LiU-ITN-TEK-G--18/069--SE

Security and Privacy of Controller Pilot Data Link Communication

Max Wernberg

2018-06-19

Department of Science and Technology
Linköping University
SE-601 74 Norrköping, Sweden

Institutionen för teknik och naturvetenskap
Linköpings universitet
601 74 Norrköping

LiU-ITN-TEK-G--18/069--SE

Security and Privacy of Controller Pilot Data Link Communication

Examensarbete utfört i Logistik
vid Tekniska högskolan vid
Linköpings universitet

Max Wernberg

Handledare Scott Fowler
Examinator Scott Fowler

Norrköping 2018-06-19

Linköpings universitet | Institutionen för teknik och naturvetenskap
Bachelor thesis | Flygtrafik och Logistik
2018

Security and Privacy of Controller Pilot Data Link Communication

Max Wernberg

Supervisor: Tatiana Polishchuk
Examiner: Scott Fowler

Linköpings universitet
SE-581 83 Linköping, Sverige
013-28 10 00, www.liu.se

Abstract

Newly implemented technologies within the aviation lack, according to recent studies, built in security measures to protect them against outside interference. In this thesis we study the security and privacy status of the digital wireless Controller Pilot Data Link Communication (CPDLC) used in air traffic management alongside other systems to increase the safety and traffic capacity of controlled airspaces. The findings show that CPDCL is currently insecure and exposed to attacks. Any solutions to remedy this must adhere to its low levels of performance. Elliptical Curve Cryptography, Protected ACARS and Host Identity Protocol have been identified as valid solutions to the system's security drawbacks and all three are possible to implement in the present state of CPDLC.

Acknowledgements

First, I would like to thank Tatiana Polishchuk, my supervisor, for her support, helpful guidance and continuous encouragement. I also wish to thank professor Andrei Gurtov, I am in debt to him for taking time to share his expertise with me. I wish to thank Anna Nilsson for her support and help. Lastly, I'd like to thank my forever faithful companion Tingeling for always putting a smile on my face, even in the most dire of times.

Table of contents

Table of Figures

Table of tables

1.1 List of abbreviations

Abbreviation	Explanation
ACARS	Aircraft Communications Addressing and Reporting System
ADS-B	Automatic Independent Surveillance-Broadcast Protocol
AIP	Aeronautical Information Publication
ANSP	Air Navigation Service Provider
ATN	Aeronautical Telecommunications Network
ATSU	Air Traffic Services Unit
AVLC	Aviation VHF Link Control
CA	Certificate Authority
CDA	Current Data Authority
CNS	Communication, Navigation and Surveillance
CoAP	Constrained Application Protocol
CPDLC	Controller Pilot Data Link Communication
CSMA	Carrier Sense Multiple Access
D8PSK	Eight-Ary Differential Phase-Shift Keying
DLS	Data Link Service
ECC	Elliptical Curve Cryptography
ECDLP	Elliptical Curve Discrete Logarithmic Problem
FANS	Future Air Navigation System
FEC	Forward Error Correction
HDLC	High-level Data Link Control
HIP	Host Identity Protocol
HIT	Host Identity Tag
ICAO	International Civil Aviation Organization
IETF	Internet Engineering Task Force
IPsec ESP SA	IPsec Encapsulating Security Payload Security Associations
KMP	Key Management Protocols
LACK	Logical Acknowledgment message
LHIP	Lightweight HIP
LME	Link Management Entity
LoWPAN	Low power Wireless Personal Area Network
MAC	Media Access Control
NDA	Next Data Authority
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSI	Open Systems Interconnection
PACARS	Protected Aircraft Communications Addressing and Reporting System
PANS-ATM	Procedures for Air Navigation Services - Air Traffic Management
PKC	Public Key Cryptosystem
PKI	Public Key Infrastructure
RSA	Rivest-Shamir-Adleman
SARPS	Standards and Recommended Practices
SDR	Software Defined Radios
VDL2	Very High Frequency Data Link Mode 2
VHF	Very High Frequency

1 Introduction

This study aims to investigate the wireless communication technology Controller Pilot Data Link Communication (CPDLC) used in today´s air traffic control with the perspective of security and privacy risks. New Communication, Navigation and Surveillance (CNS) systems are introduced to withstand the problems of congested air spaces due to an increase in air traffic. According to [1] air traffic will continue to grow. CPDLC is one of the systems introduced, as a secondary communication means, next to Very High Frequency (VHF) radio. It is meant to reduce the amount of non-critical communication via VHF radio and thereby allow for an increase in traffic capacity.

These newly introduced systems are according to [2] insecure on a conceptual level due to the lack of security consideration while designing them. The focus has instead been put on safety, a key factor within aviation, but to uphold and improve today´s safety standards the aviation industry will need to start looking at the security of the CNS systems, as recent incidents have shown the potential of malicious interference. With the widespread access to cheap and powerful tools, e.g. software-defined radios, the aviation community have lost a considerable technical advantage that up until recently protected it. External attacks pose a larger and larger threat to every new system introduced lacking built-in security measures.

In 2013 a report on the security risks of Automatic Independent Surveillance-Broadcast Protocol (ADS-B) was published [3]. The report illustrates how the lack of built-in security in the design of the system has made it possible to eavesdrop, delete, modify and create fake messages. ADS-B is currently mandatory for all newly registered aircraft in European airspace and existing aircraft is planned to be retro fitted by December 7, 2017. The Federal Aviation Association mandates that ADS-B will be installed in all entitled aircraft by 2020 in US airspace.

The safety of air traffic control is built around procedural measures which has been carried over into the technology of today. The responsibility of the safety rests on the vigilance of the air traffic controllers and pilots. This includes noticing an external attack. Both pilots and Air Traffic Control (ATC), possessing sufficient situational awareness, continuously anticipates the flow of traffic in the present airspace at any given time. The more an attack would divert from these expectations the more feasible it is that either the pilot or the controller detects it. ATCs expect pilots not to divert from given instructions, clearances and flight plans. In return, the pilots expect and trust the ATC to give instructions and clearances that will not divert the aircraft away from its intended destination. In the light of this, an attack must first be successfully initiated on order for it to be detected. It is most likely to be detected if its consequences divert from what is expected. [4] gives an excellent view of this when a controller remarks on the sudden and unexpected increase of speed during a simulated attack. However, therein lies the risk in that it has to be detected and countermeasures need to be applied in time for these procedures to protect against an attack, unless the system itself was designed to protect against intrusions.

1.1 Problem description and purpose

The purpose of the thesis is to study the security and privacy risks of the wireless communication technology CPDLC. We study CPDLC characteristics and review existing security methods within digital communication and assess applicability to CPDLC and air traffic control. The thesis aims to study possible alternatives and adjustments to the current system and propose a set of solutions regarding the security risks uncovered during the project.

1.2 Research questions

- What security and privacy risks are possible against CPDLC technology?
- Are there any possible changes or adjustments that could be applied to the technology in its current state to decrease vulnerability?
- Is it possible to remedy the weaknesses of CPDLC identified within a plausible time frame?

2 Background

Wireless communication has experienced a rapid growth the last decades. We have, according to [5], in recent years experienced an explosion of the new radio systems and a rapid development of the existing technology along with it. The expansion of wireless cellular telecommunication is an example of this, from the analog narrowband first-generation (1G) in the 1980´s to the current digital broadband fourth-generation (4G). In 2002 the mobile phones began to outnumber fixed-line phones. With all the recent advancement in wireless communication technology the main method of communication in aviation is still analog VHF radio.

Wireless communication uses electromagnetic waves to transmit information through open space and with it comes the main problem with securing it since the medium is open to anyone to with the right equipment to both transmit and receive while a wired network requires the attacker to gain physical access to the network [6]. Access to a physical network can more easily be restricted by screening it off using fences, security buildings and other physical means. When a breach is detected in a wired network it is also easily located and remedied due to the its required stationary situation whereas an attacker in a wireless system is likely mobile and able to roam inside the wireless region. It is therefore necessary to protect the information within communication networks using other means beside physical. The communication system will have to be designed so that the transmitted information is secure even if it is accessed by an unauthorized party. According to [6] and [7] secure communication system should support the following:

- Authentication, which creates a mean to verify the transferred information´s origin and users' identity.
- Confidentiality, which is needed to assure that information is kept hidden from unauthorized users.
- Integrity, to control that the information is secured in such a way that no external user may modify transmitted information.
- Non-repudiation, so that users should not be able to deny their involvement in the communication.
- Availability, which is defined as a mean to secure continuous availability of information even during a denial of service situation.

Communication network design is often based on the widely used reference model known as Open Systems Interconnection (OSI) model. It is a layered protocol structure which divides the structure into 7 layers: Physical layer, Data link layer, Network layer, Transport layer, Session layer, Presentation layer and Application layer as shown in Figure 1. Data is sent via the transmission path through each layer, from the transmitter down through the application layer to the physical layer where it is transmitted as bitstream. When received, the data is transported up through each layer until it is presented to the intended receiver. Each layer uses a protocol which adds its own piece of additional information, called header (H) which contains metadata describing how the rest of the data is to be parsed. The data link layer also adds a piece to the end of the data called trailer (T) which contains information about the data intended destination.

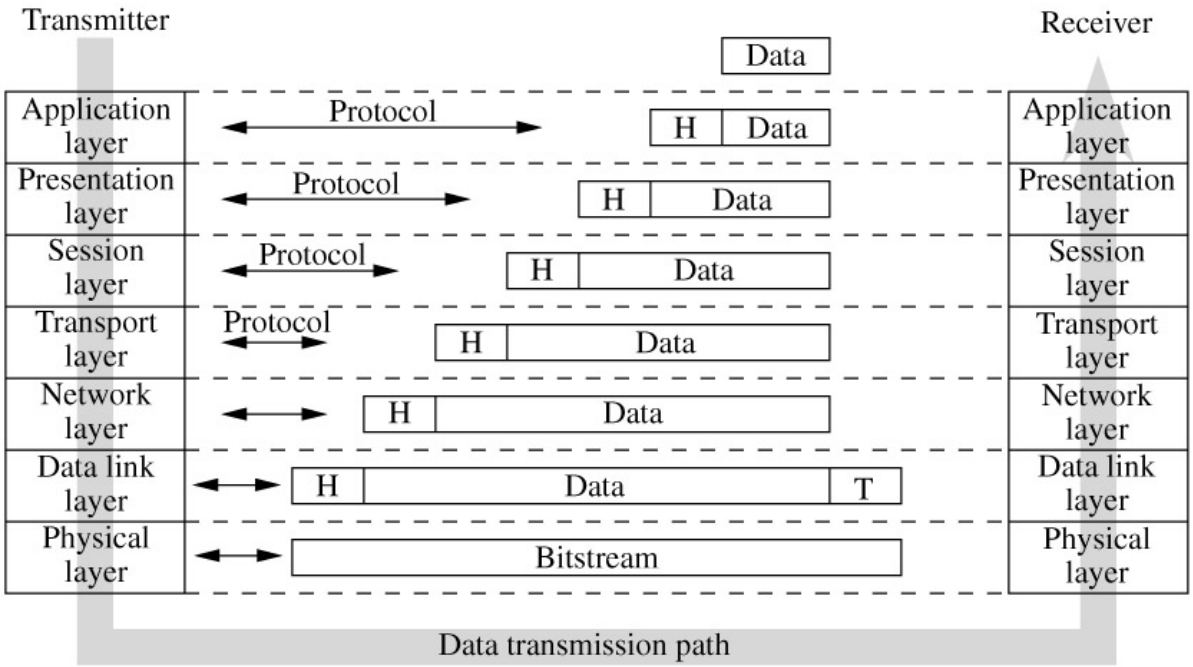

Figure 1 – OSI reference model [5]

2.1 Controller Pilot Data Link Communication (CPDLC)

CPDLC is a wireless digital communication system, first introduced in the nineties and used in parts of today´s ATC, enabling ATC and pilots to communicate via data link. It is a message-based system provides users with easy-to-read-messages and is used to convey clearances, instructions and requests between ATC and pilots. It is currently used as a secondary communication method, next to the primary VHF radio [8]. VHF radio is voices-based, half-duplex, and works only as fast as human speech allows. Since the amount of air traffic has had a steady increase the last years and is predicted to continue to increase in the future [1], the problem of airspaces congested by voice communication arises. CPDLC provides the needed benefit of freeing up transmitting time for critical voice communication. Initial experiments have shown up to as much as 84% reduction of channel occupancy time [9]. The system reduces the risk of mishearing a clearance or instruction by using text messages that are read instead of being heard and re-read without unnecessary re-transmissions. This is especially useful when a message contains multiple elements [10]. The workload of both air traffic controllers and pilots is reduced with the automation of event driven reports and updating flight plans [11].

The basis of the system is built around messages being sent between an Air Traffic Services Unit (ATSU) and an aircraft. Messages addressed from an ATSU to an aircraft are defined as the uplink traffic while the opposite, messages addressed from an aircraft to an ATSU, are defined as the downlink traffic. Any message, unless specified not to, will be answered by the receiver with a Logical Acknowledgment message (LACK) if the received message is deemed acceptable for display by the receiving system.

CPDLC connects through either Aeronautical Telecommunications Network (ATN) using Very High Frequency Data Link Mode 2 (VDL2) for, mainly European, continental airspace and Future Air Navigation System (FANS-1/A), a system that also enables the possibility to connect through satellite communications network to provide the service in oceanic airspace [11]. Figure 2 shows the data link systems used for CPDLC.

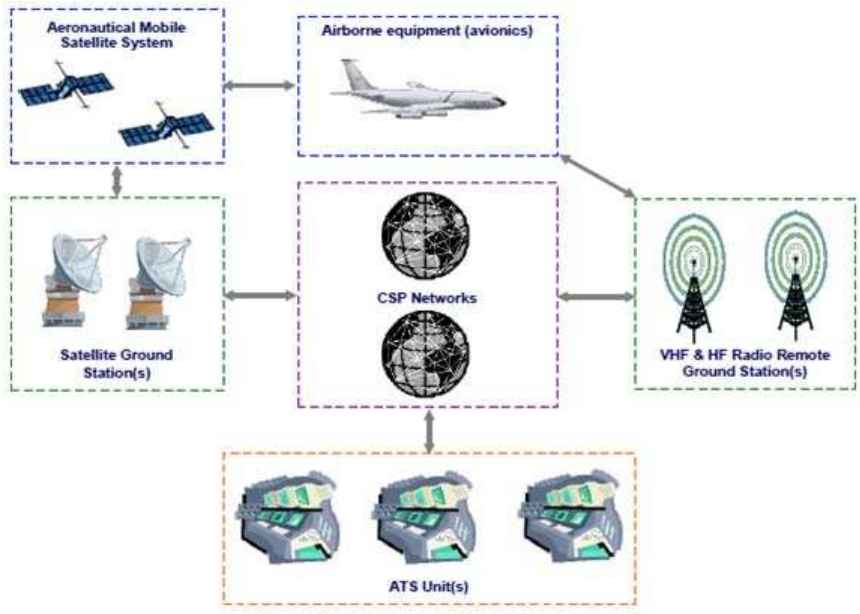

Figure 2 – Overview of CPDLC data links using either ground based system of VHF and HF ground stations network or the existing AMSS network [24]

2.1.1 Very High Frequency Data Link Mode 2

VDL2 is a signal delivery system whose architecture has been specified in the Standards and Recommended Practices (SARPS) by the International Civil Aviation Organization (ICAO). It operates on frequency 118.000 to 136.975 MHz with a data rate of 31.5 kilobits/sec [12]. VDL2 is associated with the three lower layers of the OSI model [12], as seen in Figure 3:

- Layer 1 – Physical layer
- Layer 2 – Data Link layer
- Layer 3 – Network layer

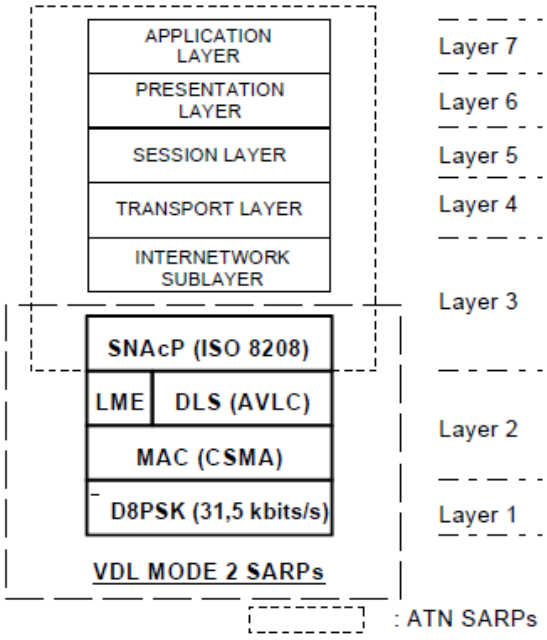

Figure 3 – VDL2 SARPS in ATN/OSI Organization [12]

The physical layer provides radio and modulation functions, such as frequency control and bit exchanges. It facilitates data encoding and a Forward Error Correction (FEC) mechanism based on interleaving and Reed Solomon coding. VDL2 uses Eight-Ary Differential Phase-Shift Keying (D8PSK) modulation with a raised cosine filter and an excess bandwidth factor of 0.6. The input data that is to be transmitted is differentiated by splitting it into groups of 3 bits, Gray Coding method, putting the least significant bit first while padding zeros is to be added to the end of transmission if needed [12]. This is meant to protect the transmitted data against the most likely errors caused by noise, since only a single bit error is likely to occur in the 3-bit sequence when using the Gray Coding method. All transmission includes a training sequence to allow for synchronization and a FEC header [12]. The Reed-Solomon code allows any correction of 1-bit errors but only corrects around 25% of possible 2-bit errors [13].

The data link layer oversees the transferring of data between two network entities by providing services such as assembling and disassembling of frames, establishes frame synchronization, and selects radio frequency channels. This is done using the sublayers:

- Media Access Control (MAC)
- Link Management Entity (LME)
- Data Link Service (DLS)

The MAC layer provides access to the physical layer using a Carrier Sense Multiple Access (CSMA) designated "P-Persistent CSMA". Data is sent with the probability of p and if the data wasn't transmitted, a timer, *TM1,* counts the time until another transmission attempt with the probability of $1 - p$. If the channel is busy during the next transmission attempt, the timer resets and another attempt is made.

The LME establishes and maintains link connection with its peer LME. A common signaling channel is used on the frequency 136.975 MHz and is used by the service providers to announce the availability of VDL2 as well as a channel to establish data link level connection when needed [13].

The second part of the layer is DLS. The DLS uses Aviation VHF Link Control (AVLC) that is derived from the High-level Data Link Control (HDLC). HDLC was primarily designed for stationary networks with greater bandwidth, and so AVLC is an optimized version to support the mobile environment of aviation and its limited bandwidth. Its main function are frame exchanges and processing as well as error detection [12].

The third layer, Network Sublayer, specified by the VDL2 SARPs in the OSI model, uses a SubNetwork Access Protocol, which is compliant with the ATN and conforms to ISO 8208. It is also known as X.25 and controls data packet flow. It connects the upper layers with the data transmission of the lower layers [13]. X.25 was developed in during the 1970's and got a breakthrough in the 1980's as protocol to be used in automatic teller machines and is partly still used but is considered a legacy system.

2.1.2 Logon and service unit switching process

The following information in this section is available in the second edition of the Global Operational Data Link Document [11] published by the International Civil Aviation Organization in 2013 but vital for understanding the low level of security.

The flight crew will have to perform a logon request to be able to connect and use CPDLC. The logon request is either an initial logon done by flight crew or a part of the forwarding procedure when the aircraft is to switch between two ATSUs, where a logon needs to be sent to the next ATSU. An initial logon is done by the flight crew through entering the four-character identifier of the ATSU that the crew intends to connect to. When the aircraft in flight is about to switch ATSU the system allows for a contact request to be sent. This request triggers an automatic logon with the next ATSU, specified in the contact request message, and is initiated by the current ATSU.

The logon request message contains the following information [11]:

- Aircraft identification, item 7 of the flight plan.
- Aircraft registration and/or aircraft address, both contained in item 18 of the flight plan. Either needs to be preceded by its indicator REG/ and CODE/
- Departure and destination aerodromes, items 13 and 16 of a flight plan.

Figure 4 shows a flight plan form and its contents, each identified as numbered items. Items preceding item 7 is to be filled by ATC. All aircraft are registered and given a unique ID, aircraft registration letters. These letters are frequently used as aircraft identification, e.g. SE123. Alternatively, the company designator followed by the flight number can also be used as aircraft identification, e.g. SAS123. Aircraft address is a unique 24-bit address, represented as six character long hexadecimal code, assigned to every aircraft upon registration of a Mode S compatible transponder. None of this information is classified.

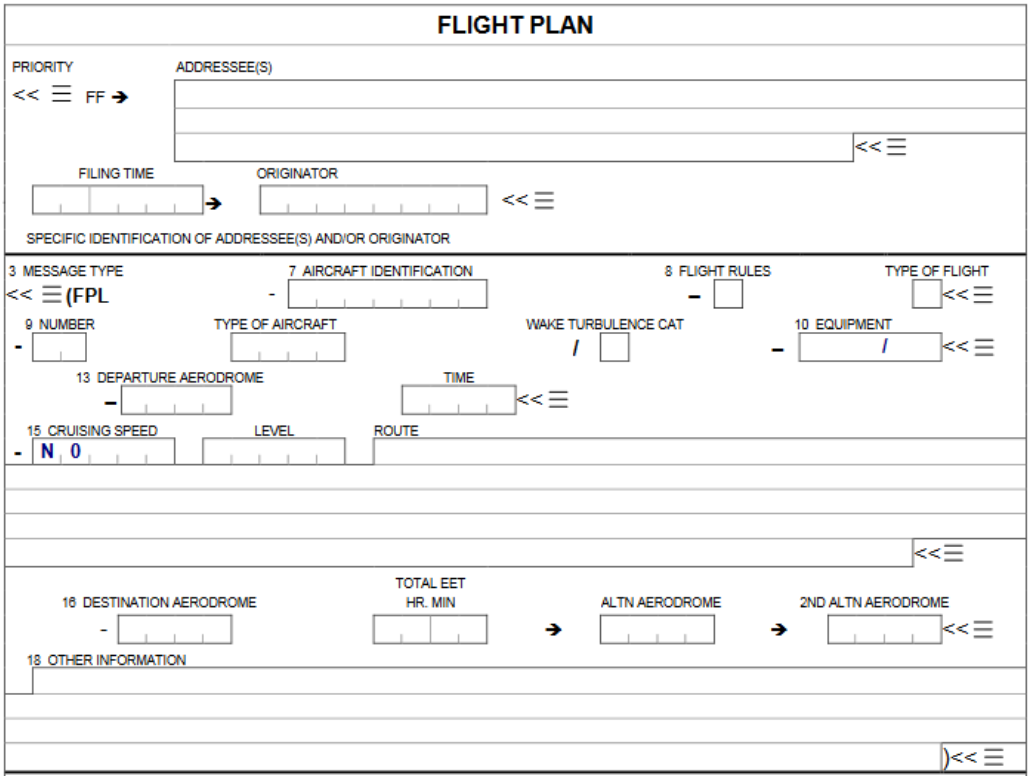

Figure 4 – ICAO Flight plan

The logon request is made to provide the ATSU with information about which data link applications is supported by the aircraft system, identifying the aircraft to ensure that future messages will be delivered to the correct aircraft, and updates are made in the correct flight plan. The identification is done by the ATSU through correlation of the information given to it by the aircraft system in the logon request message and flight plans held by the ATSU. If the aircraft identification, item 7, and either aircraft registration and/or aircraft address, item 18, can be matched with the information in a submitted flight plan, then the logon request is successful. The ATSU system automatically sends a response to the aircraft system which states if the logon was successful or unsuccessful. Figure 5 shows the process of a logon request between an aircraft and ATSU.

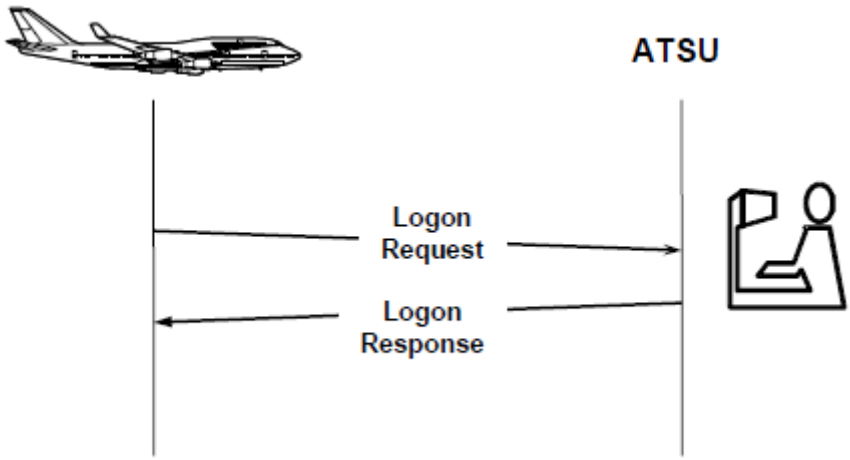

Figure 5 – Process of a logon request

Figure 6 shows the process of automatic logon requests, used when an aircraft is to switch from one ATSU to another. The process is initiated by ATSU 1, the Current Data Authority (CDA), by sending a contact request to the aircraft system which automatically initiates a logon request with the ATSU 2, the Next Data Authority (NDA). The aircraft will then finally reply to ATSU 1 with the result of the logon request. The two ways differs regarding who initiats the process.

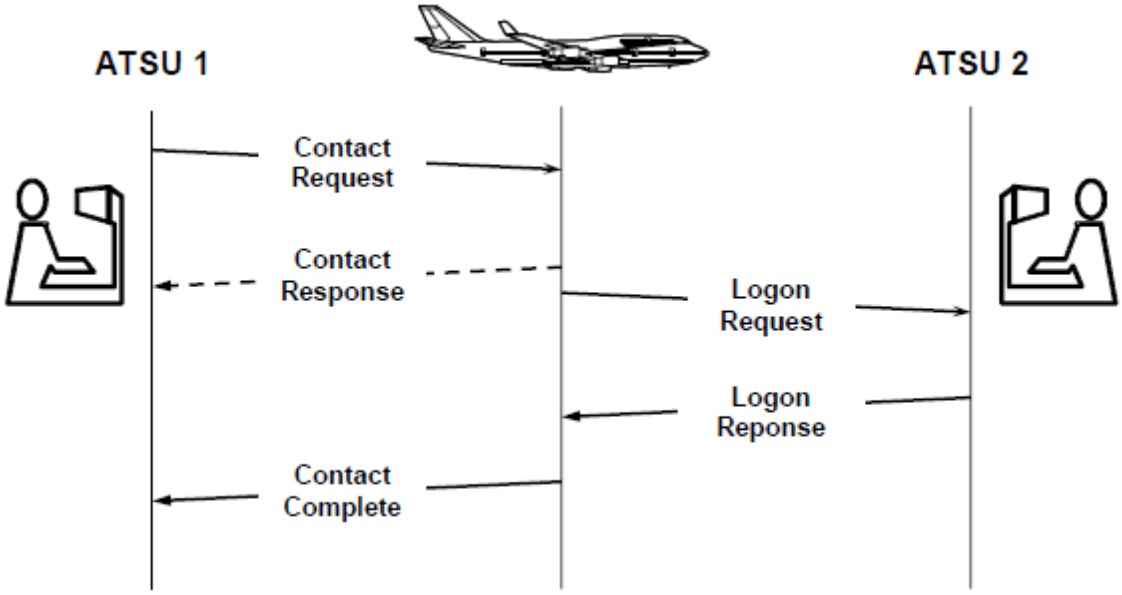

Figure 6 – Process of an automatic logon request used when transferring an aircraft between two ATSUs

CPDLC allows the aircraft client to have a maximum of two simultaneous connections, an active connection referred to as CDA and an inactive connection referred to as NDA. This is to allow for the aircraft client to be able to process the logon with a second ATSU while still being connected to its current ATSU. The active connection is the only one that allows for exchange of CPDLC messages while the inactive connection is dormant as long as there is an active connection.

After the logon request has been successful, and only then, can a connection request be sent by the ATSU to the aircraft to establish a connection. The aircraft client will, if no other connection already exists, accept the request and establish an active connection. If the aircraft client already has an active connection but verifies the requesting ATSU as the NDA, it will accept the request and establish an inactive connection. Lastly, in both cases, a confirmation reply will be sent by the aircraft to the CDA. Only the CDA can send a valid NDA message which specifies the NDA by its four-character ICAO identifier. In any other case the aircraft will reject the connection request and reply the requesting ATSU with a rejection message.

The process, of sending a contact request to the aircraft to initiate a logon request to the next ATSU en-route, can be omitted and instead imitated by the CDA. This is not a globally implemented, but available in in areas where conditions allow it. This means that the CDA sends a logon forwarding message, containing the same information as the logon request, to the next ATSU directly through ground channels and thereby omitting the need to involve the aircraft client. This allows the NDA to send a connection request to the aircraft without first processing a logon request as it has already been done. The aircraft client will accept this request if it is able to verify the ATSU sending the request as the NDA which it does through a NDA-message from the CDA.

To terminate an active connection the CDA sends a termination request. This request can be sent with or without the need of a response from the flight crew. Only the active connection can be terminated, and only by the CDA as the aircraft will not listen to messages from the NDA on the inactive connection. An attempt by the NDA to terminate the inactive connection will be replied to with a rejection message stating the NDA is not the CDA. Upon a successful termination of an active connection the aircraft client will automatically activate any currently inactive connection and establish it as an active connection.

The process of transferring an aircraft between two CPDLC-capable ATSUs broken down into three steps.

- The CDA starts with sending a next data authority message to the aircraft specifying the identity of the next ATSU permitted to establish a connection.
- Secondly, the CDA initiates the address forwarding; this can be done by either sending a contact request message instructing the aircraft to initiate a logon request itself, or by sending logon forwarding message to the next ATSU.
- Finally, the CDA send a termination request which terminates the active connection and forces the aircraft system to establish an active connection with the next ATSU, converting the NDA to the new CDA.

2.2 Security measures

There are several ways to protect one's communication with others. Hiding the communication itself from prying eyes is especially difficult when using a public media and simply disallowing unauthor-

ized access will only create an illusion of security. A natural step is to hide it in plain sight through encryption and therefore limit access to the useful information.

2.2.1 Network cloaking

Network cloaking means that the network access point is not broadcasting itself publicly. This is not a true form of security as no information is made unavailable to prying eyes. It does not make the network undetectable. The basics behind the security is based on security through obscurity which in a way the aviation industry up until now have used as a mean of security by relying on the unavailability of the necessary equipment to the public. This is no longer the case as software defined radios are now easily available to the public.

2.2.2 ID/Address filtering

ID filtering is based on keeping a list of IDs, of devices or users, that are authorized to connect to the network and blocking connection attempts coming from sources that are not on the list. Its disadvantage is that spoofing an ID makes it easy to circumvent the filter as no authentication is made.

2.2.3 Authentication

Authentication is used to stop unauthorized users from gaining access to the system by verifying the identity of the user. In fact, both the user and the system the user is authenticating towards should verify its identity towards each other, by mutual authentication. This is to make sure that the user and the system can trust each other and prevent an adversary to masquerade an attack by pretending to imposter the user or system to gain unauthorized information [14]. This is possible to achieve through a well-designed encryption protocol.

2.2.4 Encryption

This method of security aims to make it possible for parties to communicate without any outsiders gaining understanding of the content of the communication. It is a powerful mean to protect data in transit from being compromised [7].

If encryption is successfully applied, it will be able to provide [14]:

- Unauthorized outsiders to be unable to make any useful meaning of the data.
- The receiver of the data can be assured of the integrity of the data.
- The receiver of the data can be assured of the authenticity of the data.
- That the sender of the data will be unable to deny its authorship, non-repudiation.

It is common when explaining encryption to denote the three interacting parties; sender, receiver and outsider as Alice, Bob and Eve [14, 7, 6], as it simplifies talking about communicating party A and B and a third party, the Eavesdropper, easier.

Encryption is on the most basic level easily described metaphorically as passing a message inside a box locked using a padlock which only the two communicating parties Alice and Bob have the combination to. Alice places the information she wants to send to Bob inside the lockbox and locks it. She then sends it to Bob who can access the content by unlocking the box using the combination key. Thus, securing the content from being read or edited by Eve during the transfer between Alice and Bob. Even if Eve would to get her hands on the box, it would still be safe, as Eve does not know the correct combination key to unlock the box. Bob can also be sure that the content in the lockbox is

from Alice, and Alice cannot deny that she was the one that put it there as she is the only one who can lock the lockbox using her own combination key [6].

Lockboxes is of course not used in digital communication but instead the message itself is concealed, often in plain sight, in such a way that Eve cannot make any sense of the message. The message is said to have been ciphered and needs to be deciphered for anyone to understand its content. Two types of ciphers are mainly used, transposition and substitution ciphers. A transposition cipher changes the message by rewriting it, using predefined rules, to create a displacement of the characters in the message. Substitution ciphers, as the name suggests, substitute each character with another character also using predefine rules. Used together in complex combinations, called product ciphers, a high level of security can be achieved [6]. Cryptologist Claude Shannon, famous for his work in cryptography, stated in his works that a good cryptosystem needs to confuse and diffuse. Confusion aims to create a complex relationship between the un-encrypted and encrypted information while diffusion aims to remove any statistical similarities [14].

These predefined rules for how the information is to be encrypted becomes the encryption algorithm (mathematical function). What needs to be shared between the two communicating parties, Alice and Bob, is the algorithm for how the information is encrypted so that Bob can decrypt the information by executing the algorithm backwards. This is in the wider view of things not easily manageable as a new algorithm needs to be constructed for each new communication. This is solved by introducing what is called keys. The mathematical encryption algorithm is created so that it is dependent on a specified key that can vary between sessions and is easily changed. The algorithm can in that way be distributed openly as the key is the secret that protects the information. The key is the only thing needed to be shared secretly between the two communicating parties, Alice and Bob. Metaphorically, the algorithm becomes the padlock and the key is the combination needed to unlock it. Alice can use the same algorithm and simply change the key when she instead communicates with Eve without risking revealing the information to Bob [7]. The idea for this is based on Kerckhoff´s Principle*; a cryptosystem should be secure even if everything about the system, except the key, is public knowledge* [6]*.*

There are two different systems of keys, symmetrical or asymmetrical. A symmetrical system means that the two parties share the same key; it can be used to both encrypt and decrypt information. An asymmetrical system means that different keys are used to encrypt and decrypt. The two system has their own pros and cons. The symmetrical system's benefit, and at the same time its flaw, is that the same key can both encrypt and decrypt. If an adversary gains access to the key, it will have the possibility to access the content without the two communicating parties acquiring knowledge about this security breach. This is because the adversary can both decrypt, gaining access to the information, and encrypt it again afterwards. It is however less expensive, faster and more easily used than an asymmetrical system, but will give rise to multiple keys assuming separate keys are used for each individual party Alice communicates with [14].

An asymmetrical system can preferably be used when there is a need for many parties to talk to Alice in a one-way direction. It is also an effective way to make sure that the information is not re-encrypted after being decrypted. An example of the asymmetrical key system is the public key cryptosystem. One of the communicating parties publicly shares its public key with everyone and keeps the other key, the private key, secret to itself. In this way, anyone with access to the public key will

be able to encrypt something only decryptable by Alice or the other way around. Alice will be able to encrypt messages that only her public key will can decrypt and thus making sure that the content really is from Alice. A major benefit of this system is that it is possible to secure communication in an insecure channel this way [7]. According to [14] the use of asymmetrical systems is computationally very expensive and tends to become impractical to use on larger amount of information. Instead, a combination is employed where a symmetrical key for the specific session of communication is shared through an asymmetrical system.

It is possible to use encryption not only to conceal the message itself but also to make sure that the recipient of the message can be sure of its integrity, since no eavesdropper has had the chance to edit the information. This is done by digitally signing a document using Alice's private key. By encrypting a hash of message (explained later) using Alice´s private key any receiver of Alice´s messages can be sure that it was in fact Alice that signed the document, since only her public key will decrypt the hash [14].

The main issue with the system is that it is only true if Bob can be sure that the public key he has been given is in fact Alice's public key, and not a fraud key. A fraud key could have been handed to Bob by Eve, tricking Bob into believing they key belongs to Alice. Eve could by doing this create a man-in-the-middle-situation where all communication between Alice and Bob passes through Eve. This issue can be solved by implementing a public key infrastructure using trusted third parties giving to confirm that some one's public key is valid.

Integrity is ensured using a one-way hash function. These functions use an input, which can vary in length but produces an output of a fixed length. The sender of the information, Alice, calculates the hash of the information and signs the hash digitally by encrypting it using her private key. She then attaches the hash to the messages being sent. When the recipient, Bob, receives the message he can himself decrypts the hash message and compares it with the calculated hash, which he calculates the same way as Alice did, of the message. If the two hashes compare, Bob can be certain that no changes have been made by anyone else and the integrity of the information is maintained [14]. The one-way hash functions have two properties that is beneficent for it; avalanche effect and duplication avoidance. The avalanche effect makes sure that a minor change in the message would produce a vastly different hash. The duplication avoidance protects against the risk that two different messages produces the same hash, keeping the risk to a low level. This creates a strong defense against attacks that aims to modify the information as it will create a different hash [7].

A digital signature of a message´s hash is not only a way to secure the integrity of the information but also a form of authentication, by proving the information's origin. There is another way to authenticate, besides digital signatures, called challenge and response-system. It is a more elaborated system which includes the usage of digital signatures. Bob sends a challenge, an un-encrypted message, to Alice who digitally signs it, using her private key, before sending it back to Bob. Bob can then decrypt the message and check if the content of the returned message is the same as the one he sent to Alice. Alice can in return do the same to Bob and mutual authentication has been accomplished. This is all based on the assumption that both Alice and Bob can be sure that the public keys they have originates from each other and that they have not been tampered with [7].

Challenge-response systems and digital signatures are variations of the same technique. Whereas the challenge-response system requires a single separate message to ensure authentication, the digital

signature does it on a per-message basis. Even though the digital signatures appear to be more secure, the challenge-response system is well suited for connection-oriented networks where the authentication can be done once, at connection setup, thus saving the per message over-head [7].

2.2.5 Trapdoor functions for encryption

Encryption is based on mathematical trapdoor functions that are easy to calculate but difficult to solve. The functions chosen for this are based on mathematical problems that are believed to take a very long time to find the solution, yet no mathematical proof exists to prove it that is does. The two most common ones are:

- Factoring of large integers
- Elliptical Curve Discrete Logarithmic Problem (ECDLP)

Factoring of large integers is based on multiplying two prime integers of comparable size with each other and the problem starts when attempting to factoring which two integers were used. The problem itself is not impossible but is strongly believed to take a very long time to solve. It is a well-known problem and no algorithm has been published that can solve the problem in a feasible amount of time, given of course that large enough integers are being used. One of the most commonly used integer factoring algorithm is the Rivest-Shamir-Adleman (RSA).

Elliptical Curve Cryptography (ECC) was first suggested by Neal Koblitz [15] and Vinctent Miller [16] but did not become widely used until around 2005. It's based on "dotting" points along an elliptic curve over finite field and is most easily described as multiplying a point along the curve n amount of times which is quick and easy mathematical wise. While it is assumed to be very time consuming to solve n, even if the starting point is known. The result of this is that the size of the keys beings used is smaller and the computational power needed is less.

Table 1 – Key size and strength comparison [17]

Symmetric Key size (bits)	Symmetric key algorithms	Asymmetric Prime Factoring Key Size, RSA (bits)	Elliptic Curve Key Size (bits)
80	2TDEA	1024	160
112	3TDEA	2048	224
128	AES-128	3072	256
192	AES-192	7680	384
256	AES-256	15360	521

3 Methodology

3.1 Literature study

Literature study is the main source of information for this study and is according to [18] often overlooked as a method since it is considered the most common form of data gathering. The point of a literature study is to build a knowledge base for the chosen field of study. The need for constant documentation and ease of access through digital distribution makes it possible to gather a great deal of data in a short period of time which is a major benefit of the method. This can create a problem in the sense that it may result in too much information gathered which is near impossible to go through in a way that is both efficient and valid within the time frame of the study. The method risks a biased selection of sources, because only a portion of available sources will be used, making the result of the study seem deliberately angled. To minimize this risk, it is consequently important to review every source critically [19].

3.2 Interview

Interviews is another very common way to gather information, often primary data, from the source itself. Interview is in the literature described as conversation between two parties, where one party (the interviewer) aims to gain information from the other party (the interviewed). Each party is made up of one or more persons [18] & [20].

There is no set of rules describing exactly how an interview is to be executed, but instead common and agreed guidelines which divides the method into three separate ways of structuring an interview, commonly named as ‘structured’, ‘unstructured’ and ‘semi-structured’ [21]. They differ in terms of how the interviewer’s work of preparation is planned and done. A structured interview may vary in the degree of how strong it is structured and planned around the set or list of specific questions that the interviewer has prepared beforehand. The interviewer simply wants the interviewed party to answer these questions until a satisfying level of information has been obtained [18]. On the other end of the scale there is the unstructured interview where the interviewer has an open mindset towards what is to be obtained as information from the interviewed party. The interviewed party is given a subject, which the party then can speak freely about [20]. This type of interview carries most resemblance to a conversation between two parties.

The semi-structured interview is a mix of both, where the interviewer has prepared a bit more specified subject or subjects compared to the unstructured interview. As the interview continue the interviewer may also have follow-up question regarding each subject but this type of interview is still not as strongly structured as a structured interview [20]. This study includes an interview with Andrei Gurtov, professor at Linköping University, Computer and Information Science (IDA), and expert in wireless communication security.

4 Literature study

Security within aviation has up until recent years not been a priority of the community due to the publicly inaccessible equipment [10]. Recent studies focused mostly on the security of the surveillance system known as ADS-B [3] [22] [23] [24], a system used as a cost-effective alternative to both Primary and Secondary Surveillance RADAR. Studies and experiments have shown that ADS-B is a very insecure system, lacking any authentication or encryption capabilities, and therefore susceptible to both passive and active attacks. The spectrum of studies that has been done regarding CPDLC is far from as extensive as for ADS-B. Strohmeier [10] mentions CPDLC as a likely weak system and DiMarco et. al [4] gives an interesting view on how the CPDLC system is vulnerable to external attacks.

Safety has been a predominant factor in the aviation industry, which over the years has resulted in it being built around redundancy and procedural safety. It has been important to show the public that it is safe to fly by minimizing the risk of accidents. Security has been used to increase the level of safety and heavily focused on preventing physical attacks, e.g. bombing and hijacking, by implementing extensive security checkpoints, screening of passengers and other security measures to restrict access to certain areas and air traffic control structures. Redundancy has, as an example, led to the usage of multiple aircraft engines. A flight is not critically compromised if one engine should fail as the remaining engine(s) still provides enough power to continue until a controlled descent and landing can be executed. There should always be another unit available in the case of failure to avoid emergencies. The same is true for communication, as dependence on redundancy has led to aircraft always carrying multiple radio transceivers. This is to avoid the very discomforting situation of loss of communication with ATC. Loss of communication is an emergency handled by having pre-defined procedures to fall back, for both ATC and pilots. Procedural processes have been developed, as a result of the safety being structured around redundancy, to support and help dismantle cases of emergencies where redundancy fails. But redundancy and procedural processes is not a safeguard against external interference and will not prevent an attack by an external entity on one of the CNS systems. Pre-defined procedures are structured around detecting threats in progress and suppress further negative effects once detected. Procedural security will not activate if a threat is not detected, no matter how advanced the procedures is designed to be. The importance of built in security measures to prevent attacks will continue to increase, especially when air traffic controllers are instructed not to question the information presented by the system, as in the case of the German ATC regarding the usage of ADS-B [2]. Procedural security will still contribute as an important back-up to rely on and increase the systems resilience if an attack is detected.

Strohmeier [10] showed that CPDLC, along with other systems, is inherently insecure as it provides unauthenticated and unencrypted data links which are easy to eavesdrop and attack. [4] provides an interesting look at an experimental attack done in a testing environment showing that the CPDLC system is vulnerable to a man-in-the-middle attack using freeware and open source tools. Although they did allow the attacker to have physical access to the network, which the authors considered to be unlikely to happen in real life, it does show that the system is insecure on an application level even before it goes into the wireless medium. According to [25], ICAO has specified in a draft of their guidance material that ATN systems should support authentication of both peers and data traffic, as well as securing the data integrity to ensure that the information has not been modified or duplicated. These questions are not new and proposals on how to secure the ATN has been presented as early as 2001. [25] puts forward a proposal on how to secure the communication through encryption

using an asymmetric key system to securely communicate a symmetric session key. In the same year [26] suggests a complete model for how secure the ATN while minimizing security overhead. Some years later, [27] publicizes a suggestion on how to secure the authentication process of CPDLC using an elliptic curve-based protocol.

4.1 Backup procedures in the event of failure of CPDLC

ICAO Doc 4444 Procedures for Air Navigation Services - Air Traffic Management (PANS-ATM) [28] states the agreed upon procedures to be taken in in the event of a CPDLC failure.

In the event of a failure the following procedures takes precedence:

- Revert to voice communication and alert affected parties of CPDLC failure.
- Aircraft in communication with ATC shall be informed via voice of CPDLC in the event of an intentional shutdown of CPDLC.
- ATC will inform affected stations and flights in the event of discontinuation of the use of CPDLC.
- The resumption of CPDLC shall be advised by ATC.

A detected deviation will most likely be dealt with in a procedural manor by having the ATC temporary restricting the usage of CPDLC until later notice, and fully commit to voice communication. This may lead to a decrease in air traffic capacity in certain airspaces if the ATC is heavily dependent on CPDLC to complement VHF-radio.

Availability can be easily detected by the user. It becomes obvious to the users that the system is experiencing issues with its availability when the general response time increases above normal limits or even times out in the event of complete denial of service attack. It is in these kinds of events that thoroughly developed procedural security will be able to quickly step in and help the traffic system to recover and proceed without CPDLC.

4.2 CPDLC threat model

An unsecure communication network is threatened by several types of attacks. In Table 2 we summarize the present threat model associated with CPDLC technology. Each threat is identified by its threat type, actor type, affected attributes and an example on how the threat could affect CPDLC.

Table 2 – Overview of possible types of attacks on CPDLC

Threat type	Actor type	Affected Attributes	Example Attack
Eavesdropping	Passive	Confidentiality	Reading messages
Jamming	Active	Availability	Channel blocking
Flooding	Active	Availability	Ground Station / aircraft Flooding
Injection	Active	Availability, confidentiality, integrity, non-repudiation	Ground Station / aircraft ghost messaging
Alteration	Active	Integrity	Modification of Message content
Masquerading	Active	Authentication, non-repudiation	Ghost aircraft / ground station identity

4.2.1 *Eavesdropping*

Eavesdropping means listening to the data traffic without authorization to do so [14]. Eavesdropping is widely considered the simplest attack as it does not involve any active actions by the attacking party other than the necessary equipment to receive the signal. Eavesdropping is made even easier as the CPDLC data is not encrypted. The information is sent in plain text for the receiver to read. It is easy to think of it as an innocent form of attack since it does not directly influence any data. It is a straightforward way to map the usage of CPDLC, looking for normal and usual patterns in the local area of the attack.

4.2.2 Jamming

Jamming intends to deny the affected victim access to the service. This is done by filling the medium with enough noise to make it impossible to get any useful data through to a receiving party. All users connected to the network through a jammed node is affected by a jamming attack and bottleneck connections is extra vulnerable with this kind of attack. Wireless technology allows for directed attacks to jam specific areas and/or targets when a mobile and wireless transmission medium is used. The coverage of the attack is dependent on the reach of the transmission of the attacker. A wireless jamming attack is easy to detect and find using a directional receiver to probe for the jamming signals origin.

4.2.3 Flooding

Flooding, in contrast to jamming, is done by sending multiple packets of readable data to the same receiving party instead of filling the channel with noise. If the receiving user receives more queries than it can handle per given time frame, incoming queries will start to queue up. Other actions will likely be left unattended as the queue is being managed thus preventing valid data to be processed in

time. Ultimately a system might time out under the stress or even completely come to a standstill due to overload.

4.2.4 Injection

Injection is closely related to flooding and is performed in a similar way. The difference is that information is not injected if it is sent from an authorized point of access to the network. Injection is defined as sending, possibly faulty, unauthorized messages. By not originating from an authorized source the information is said to be injected into the network. This type of attack can be very severe and difficult to detect if the system lacks necessary protection to check the information's source of origin.

4.2.5 Alteration

An alteration attack is when the attacker alters the legitimate data. It manifests as data being modified, re-directed to another recipient or delayed. Since the data is being altered and not injected it keeps its original validity which makes this type of attack even more harder and mischievous to detect.

4.2.6 Masquerading

Masquerading means that the attacker impersonates an authorized user, be it aircraft or ATC, and gains unauthorized privileges. Unless detected, a successful masquerading attack has the means to commit to a full conversation with its victim. In the case of CPDLC sending and receiving several commands [14].

4.3 Analysis of CPDLC security

To create security that is preventive regarding the threat of an attack on the system it will have to be built into the system itself through security-by-design. CPDLC lacks this as the foundation of the system originates from a time when security was not thought of as important as it is today.

CPDLC will need to fulfill all five of the requirements for a secure communication fulfilled:

1. Authentication
2. Confidentiality
3. Integrity
4. Non-repudiation
5. Availability

4.3.1 Authentication

As seen in [11] CPDLC has a very weak authentication process implemented at the moment. Attackers with malicious intent can easily fool it and a simple undetected mistake can lead to an incorrect logon being processed and completed, as was reported by [29]. In 2009 a simple mistake in the input of the flight plan details in the flight management computer resulted in an aircraft completing a logon process as another aircraft. The solution to how to avoid it from happening again is done procedural by asking pilots to be vigilant of errors when configuring the flight management computer. In its current state, the pilot is not the entity that authenticates towards the ATSU but the aircraft computer. This might need to change so that every active pilot in the aircraft makes a personal authentication, and thereby remove the connection between authentication and the plane's flight plan.

It is today common that the aircraft is authenticated or identified by the ATC, i.e. how voice and radar identification work. This assumes that the pilot submitting to ATC services is authorized to do so. If the pilot, instead of the aircraft, authenticates it would result in the assurance that the authenticating entity is in fact authorized to operate the system. A pilot authentication system will have to allow for the dynamic variance of pilots piloting different aircraft at various times. If instead the authentication is put on the aircraft, the system will probably not have the need for as a dynamic setup and might result in a less complicated key management system. The issue of key management and who should be in charge of handling it will need to be solved alongside the implementation of authentication.

4.3.2 Confidentiality

The confidentiality of the CPDLC is not covered, as everything is sent in plain text without any encryption enforced, and according to [30] not something ICAO is currently consider a security risk. It is possible to receive and decoded the CPDLC signals using cheap equipment and free software, while how to-instructions is made available online by enthusiasts, leaving CPDLC exposed to the threat of eavesdropping. Recent advancements in technology allows for active attacks, which is deemed more dangerous due to its tampering with information than passive attacks, to be carried out much more easily. This demonstrates a need and makes it is easy to understand why the military prefers CPDLC to be completely confidential.

4.3.3 Integrity

Integrity is not guaranteed by the system. The forward error correction protocol, a lightweight version of the Reed-Solomon code, is only meant to correct apparent errors upon delivery of the information. Information tampering, if done properly, could go unnoticed by the system itself if the received information is completely made up of valid data. The task to validify of the information is put on human recipient, which is unlikely to question the information if it is not considered to be contradicting in comparison to the aircraft/ATC original intentions. Integrity combined with authentication is a robust foundation to aim for when securing the communication of CPDLC. It will provide a much-needed trust that a message received is valid and true. Yet both pilots and ATCs remain human and mistakes can be made but it will rule out the need to actively worry about a possible threat of attack on the system.

4.3.4 Non-repudiation

The last requirement that encryption can fulfill is non-repudiation. It is important to note in what point of view the non-repudiation requirement is to be fulfilled. According to [31], there is a debate regarding the possibility to achieve this. It is based on the two viewpoints; legality wise and cryptographic wise, and the way to deal with this issue depends on the viewpoint. A human can always legally repudiate, i.e. claiming forgery of signature or identity theft. This extends to digital communication cases, whereas for example an asymmetric key setup has been used to cover non-repudiation, by claiming that the person's secret key has been compromised. The cryptographic viewpoint only secures the fact that a public key was used to verify the digital signature and that it has been scientifically proven to be associated with its corresponding secret key used to sign the information. It does not cover the cases where a secret key would be compromised [31].

4.3.5 Availability

The system currently lacks any means to protect itself against an attack aimed at disrupting its availability. This kind of attack will most probably render the system useless during the attack. The consequences of an attack aimed at the systems availability will vary depending on if single aircraft is denied services or if a ground unit is targeted, comparable to client or a server being attacked. An attack targeting an aircraft will only affect that single aircraft while an attack on a ground station will affect all connected aircraft. The systems availability will in the event of an attack most likely be restricted to a specific geographical area as long as the attacker lacks physical access to the network, such as the aeronautical telecommunication network.

5 Interview with an expert

An interview was conducted with Andrei Gurtov, professor at Linköpings Universitet. Professor Gurtov has previously been an adjunct professor at Aalto University, University of Helsinki and University of Oulu, visited ICSI in Berkeley multiple times and is an ACM Distinguished Scientist, IEEE ComSoc Distinguished Lecturer and Vice Chair of IEEE Finland section. The interview was planned as a semi-structured interview based on an introduction text composed and e-mailed to professor Gurtov in advance. Gurtov provided useful information and insights on the current state of CPDLC and gave the recommendation that the next generation of CPDLC should be based on IEFT/IEEE standardized protocols, seeing as the current is one of few remaining links that is yet to switch to IEFT standards. Gurtov continued that he sees potential for Internet of Things protocols as IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) or Constrained Application Protocol (CoAP) as protocols to be used since they were designed to specifically fill the need for lightweight sensor networks where low overhead and simplicity is critical factors. Even if the IPv4 or 6LoWPAN would be implemented, there are still things to consider when it comes to selecting what type of cryptographic solution to use to secure the system.

Developing authentication for CPDLC will need a public key infrastructure and a source of trust to ensure a public key's origin. Public keys, or host identities in the case of Host Identity Protocol (HIP), can easily be self-generated. It is there for common to use a Certificate Authority (CA) to digitally sign and distribute public keys to minimize the risk of counterfeit public keys being distributed and kept in circulation. Such keys could, for instance, be used to initiate a man-in-the-middle attack. Each state's Air Navigation Service Provider (ANSP) could be assigned the role of CA in a public key infrastructure for CPDLC. However, due to the heavyweight nature of certificates an alternative approach should be sought after. One approach is to use a compact HIT to represent a hash of an aircraft's or airport's public key. This HIT is sufficient to validate the authenticity of a public key during a key exchange. These HITs can also be stored in public and distributed through the Aeronautical Information Publication (AIP). The short length of the HIT allows it to be used in the already existing flight plan system, which uses short text fields.

IEEE recently published a new Recommended Practice specification 802.15.9 for Key Management Protocols (KMP) for constrained links [32], such as IEEE 802.15.4. Currently, the following KMPs are supported: HIP BEX, Diet HIP, 802.1X, PANA, IKEv2, and Dragonfly. A special message layer is defined that allows security encapsulation without presence of IP headers. It makes this specification highly relevant for securing constrained CPDLC.

6 Proposed solutions for CPDLC security

A crucial factor regarding implementation of an encryption protocol into the CPDLC system is to consider the limited available bandwidth. CPDLC allows for up 31.5 kb/s and according to [33] the net performance of the data link can drop down to only 4 kb/s. Any suggested protocol will have to consider this and avoid adding unnecessary extra overhead data.

6.1 Elliptical Curve Cryptography

ECC shows potential as an encryption for CPDLC in its current state as it uses smaller keys while at the same time provides the same level of security as encryption techniques based on factoring of large prime numbers do. This results in less computational power needed to encrypt and decrypt the information, which in itself is beneficial. According to [6] the computational overhead of ECC, using state of the art implementations in 2002, was 10 times faster than RSA. Table 3 shows how ECC could help keep the overhead bandwidth usage down, as the size of short encrypted messages is about a third compared to RSA. Table 4 shows the sizes of a signature on a larger message of 2000-bit. Thus, ECC has a much smaller impact.

Table 3 – Overhead estimations due to encryption of small messages [6]

Encryption	Encrypted message (bits)
1024-bit RSA	1024
160-bit ECC	321

Table 4 – Signature sizes on long messages (e.g. 2000-bit) [6]

Encryption	Signature size (bits)
1024-bit RSA	1024
160-bit ECC	320

In 2004, [34] claims that 163-bit ECC is roughly 5 to 10 times as fast as a 1024-bit RSA private key operation. Further comparisons show that as the key size increase so does the performance difference. At 256-bit ECC compared to its equivalent 3072-bit RSA the difference increases to span between 20 to 60 times faster. At the level of 512-bit ECC compared to 15360-bit RSA the average difference is expected reach a ratio of 400.

However, the history of ECC is not only surrounded by good news. Back in 2007 it was reported by Dan Shumow & Niels Ferguson, two Microsoft employees, that there might have been a known back door in one of the National Institute of Standards and Technology (NIST) pseudo random number generator called SP800-90 [35]. This back door could possibly nullify the security of the ECC, which uses the suggested standard. As Nick Sullivan [36] says, this does not change the level security that the ECC in itself can provide but instead brings the level trust towards the creators of the standards into question.

ECC uses the mathematical ECDLP which has only been researched for about 30 years and is because of this not as surveyed as for example factorization of large composite integers. This does not discredit the problem of ECDLP since it is still believed to be a difficult one, but it should be known that the possibility of a faster way to solve the problem is yet to be found.

In 2015, the National Security Agency (NSA) announced its intentions to move to a new set of cryptographic algorithms resistant to Post-Quantum Cryptography. NSA also advised vendors who is yet to make the transition to their current set, Suite B which includes ECC, of algorithms not to do so but instead await their next upcoming set. The reason for this has been a questioned within cryptography community but is still unanswered [15]. It is important to acknowledge this information if it is decided to develop ECC for CPDLC.

6.2 Protected Aircraft Communications Addressing and Reporting System (PACARS)

The commercial company ARINC supplies a standard for what they call PACARS. Aircraft Communications Addressing and Reporting System (ACARS) was developed in the 1970's as a digital data link system to enable to send short and simple messages to and from aircraft using radio or satellite. The standard is according to [37] able to be used for CPDLC and provide encrypted data link for FANS 1/A as well as ACARS. PACARS was originally developed for the military to protect their communication. But it is also stems from a desire by the aviation industry to address the known lack of security of ACARS using a standardized solution and because of that it is now an available standard [38]. It supports data confidentiality, integrity and authentication using ECC and Secure Hash Algorithm (SHA-256) and is claimed to have no measurable message latency, all of which is favorable due to the CPDLC's performance constraints. PACARS is meant to be software solution which implies that no changes to the current hardware is needed for it to function. It is still in development and currently lacks certification. Its development has been divided into three phases, where the first phase included a proof of concept in a lab environment. The second phase was aimed at having a hardware prototype tested for over-the-air communication. How far the development has come of a fully functional system is yet unknown.

According to [39], FANS 1/A uses ACARS as its network while ATN-B1 uses the ATN and VDL Mode 2 as its networks. PACARS will not secure CPDLC as a whole if it only supports ACARS even though it is widely used. It PACARS cannot be modified to support ATN-B1 then it will not be a valid option for continental Europe along with other areas where ATN-B1 is used.

6.3 Host Identity Protocol (HIP)

The HIP is a new internetworking architecture developed at the Internet Engineering Task Force (IETF) which had its first stable version was introduced in 2007. It has been developed to counter the problems that has arisen over the years with the ever growing, and without directional management, wildly evolving Internet [40].

HIP has mainly been developed to be used seamless with IPv6, but is fully backwards compatible with present infrastructure of IPv4 to make it possible to implement in an already existing environment, without major changes needed to be done to either applications within the routing infrastructure or the network. A HIP host and non-HIP host are able to communicate. HIP aims to cover:

- Universal connection losses
- Mobility and multi-homing support
- Multicast
- Unwanted traffic
- Authentication, privacy and accountability

By implementing a new name space in the TCP/IP stack, a public key known as Host Identifier, it disconnects the two roles of identifier and locator in the current IP address. The Host Identifier assumes the role of identifying the host and the IP address continues to work as a locator. This enables among several things a connection between two hosts, that is to be kept open even if the two hosts are mobile and continuously changes locations and thereby enhancing connectivity and mobility [41].

Data packets will use the Host Identity as source address by having it converted into a Host Identity Tag (HIT), which looks like an IPv6 address using a predefined prefix, called Orchid. This HIT follows the packets through to the Internet Protocol Security (IPsec) Encapsulating Security Payload (ESP) Security Associations (SA) where it is yet again converted into an IP-address and added to the header. This makes it possible for any non-HIP nodes in between the two communicating nodes can handle the packets like a normal IPsec ESP transport mode packet. When the packet is received on the other end it goes back through the IPsec module. If the packet passes verification and integrity checks then the IPsec module discards the IP-address and reapplies the HIT as the source address to assure upper layers of the packet's validity. This ensures that the packet was created using the correct cryptographic protocol where the private key corresponding to the HIT was used which in turn also protects against IP spoofing.

Multicast is not yet covered by HIP but according to [41] it would be explored if HIP can support making IP multicast more accessible in the future. Multicast is in the current state of CPDLC not needed unless a fundamental change is made in the amount of data being sent within the system.

HIP can approach unwanted traffic in two separate ways: either directly by hiding or make the recipients directly inaccessible by forcing the sender to gain the consent of the recipient before a connection is established. The second way is to increase the cost of sending data, or inversely minimize it. Both is partly accomplished by introducing a four-way handshake between the sender and recipient before any other data can be sent. Hiding the hosts is done by creating an overlaying system that takes care of the handshake between sender and receiver, and only lets the sender get in direct connection with the recipient after this handshake has been accepted by the recipient and allowed a direct path through a HIP-firewall. Even if the sender would know the direct address to the recipient, any incoming data would be dropped at the HIP-firewall as no path has been opened through a handshake. To increase the cost of sending data the four-way handshake is introduced to produce a CPU demanding process that is handed to the sending party to compute while the receiving party remains stateless. By processing this request, the sender shows its commitment to the connection. This also minimizes the risk of a denial-of-service attack by CPU-overloading simply by handing the CPU-load back to the sender [41].

When using Host Identifiers anonymity is not guaranteed, even though it is possible for a host to use different identifiers for each contact, it is still possible to reveal the host's identity using a simple cookie. Instead, accountability is reinforced. Ways to keep the identity hidden has been suggested such as using a hash of the Host Identity, which is not revealed until after a handshake has been accepted, to counter this loss of privacy.

The Host Identity Protocol has a potential to, if implemented, not only solve the first four requirements but also partially cover the availability requirement through its way to handle unwanted traffic. It will function as a counter to the two types of attacks, flooding and injection. A HIP-enabled host will discard any unauthorized data but will not protect against a jamming attack filling the medium

with noise. Though the source of origin of a jamming attack is easily pinpointed using direction finding, it still poses a risk. HIP appears to be very effective considering that it covers every aspect of secure communication. Though it is worth mentioning that it has been shown that HIP has a considerable throughput overhead cost when used on mobile devices such as a tablet or PDA with reduced computational power compared to a PC. In a comparing experiment done in 2007 [42] a 32% reduction in throughput, from 4.86 Mbit/s down to 3.27 Mbit/s, was measured when using HIP on tablet compared to only a 0.4% decrease when used on a laptop. The HIP measured to have an average increase of round trip time by 37% compared to a 15% increase when used on a laptop. This goes to show that HIP has a greater negative impact on a system running under computational constraints compared to a PC.

6.3.1 Lightweight HIP (LHIP)

LHIP has been developed to counter and reduce the impact of the increased overhead cost caused by HIP when applied on computational constrained devices, i.e. mobile device such as smartphones and PDA's [40]. Devices as these are lacking in CPU performance compared to PCs and laptops, and bound by its smaller battery as a resource of power, they require a simpler approach toward the base exchange procedure of HIP.

Gurtov [40] has identified four requirements that will have to be satisfied by LHIP to be considered a useful lightweight alternative to HIP.

- Increased performance
- Protocol security
- Namespace security
- Compatibility

By replacing the public-key cryptography, used for host authentication, in HIP with Interactive Hash Chain authentication(IHC) LHIP reduces the computational cost of HIP to less than 2.5% of the cost of a base exchange of normal HIP with 1024-bit RSA [40]. Removing the use of an asymmetrical key system results in lower level of security which is solved by signing distinct kinds of messages, update, close and upgrade messages, with IHC signatures to reinforce the protection against man-in-the-middle attacks, as important control messages cannot be forged. It does however support the use of RSA signatures but it not dependent on its usage. Namespace security is an important part to prevent impersonation attacks and namespace conflicts. Both issues are simply solved by using RSA signatures. LHIP is considered compatible as it does not change the way HIP works in general and has the ability to interact with HIP implantations

6.4 Analysis of the proposed solutions

It has been shown in 4.3 that CPDLC lacks built-in security and privacy. One answer to this problem is to apply a cryptographic solution on the existing system. All three opportunities presented in chapter 6 share the fact that they offer the possibility to be applied within the already existing system through modification existing system. For an already performance restricted environment as CPDLC I suggest an ECC solution to be considered as choice encryption during connection setup until a secure connection has been established. Once a connection has been established and a symmetric key can securely be shared between the clients, the communication can fall back to the more cost-effective symmetric key system for the remaining duration of the connection. This is to keep the

computational and overhead costs to a minimum and the shorter keys presented within ECC offers that over an asymmetric prime factoring system. By deciding on an ECC as a solution would include the process of designing and developing an encryption system for CPDLC from scratch, whereas PACARS offers an already defined standard to secure CPDLC. PACARS offers a standard which uses an ECC solution for both encryption and authorization but seems to lack improvement regarding the system's availability. By the available information it comes with full support for the FAN-1/A but lacks any information about the ATN-B1 used in continental Europe which might imply that it lacks support for it. It must be confirmed that it supports both FANS-1A and ATN-B1 or allows for modifications to support both before this solution becomes viable worldwide. PACARS appears to be the quickest way to apply an encryption and authorization solution as it is already available. HIP, and its lightweight version, offers a broader solution. It gives an opportunity to improve and fulfill all the five requirements of a secure communication. It incorporates the tools to encrypt the information, but it also brings a secure authentication, including a foundation on how to handle keys using secure DNS-servers. The safekeeping of public keys could become a major issue come the implementation of an asymmetric system and would preferably needed to be handled by a centralized entity. This could be assigned to each states Air Navigation Service Provider (ANSP). HIP offers the availability to continue using it in future generations of digital datalinks within aviation, including new versions of CPDLC, whereas PACARS is limited to the current legacy design of CPDLC and ACARS.

Lastly, there is the option of redesigning the entire communication system. This provides the opportunity to select newer standards and protocols, if only to catch up with current standards of wireless technology and mobility. This will obviously not solve the security shortcoming in the current iteration of CPDLC and it will most likely take another 20 to 30 years before it could be ready for the commercial market.

7 Conclusions

The importance of improving CPDLCs security and privacy stems from the need to create a secondary communication channel, trustworthy enough, to alleviate an already congested communication VHF voice communication and enable ATC and its airspace capabilities for continued growth. Without an acceptable level of trustworthiness, CPDLC will work against its intended purpose by adding more workload in the already stressed environment of air traffic control managing system.

I investigated CPDLC communication functions and its level of security and privacy in order to identify the risks and possible security threats. We have concluded that CPDLC communications lacks the appropriate level of cybersecurity. Improvements within a system are constrained by the aging structure of the foundation of the system, designed using legacy protocols. Implementation of any encryption methods therefore needs to have as small impact on the system's performance as possible while still providing an all-round security protection.

A commercial solution called Protected ACARS, claims to be able to solve the system's lack of security using the ECC method. We argued towards a solution based on open IETF and IEEE standards. IETF protocols 6lowpan, CoAP, HIP can be adopted for design of the future aviation communication system. We proposed utilizing the current flight plan and AIP information systems to provide root of trust for authenticating CPDLC encryption.

It should be possible to have a finished solution ready for deployment well ahead of a new or redeveloped system. Especially seeing as the need for improvement has already been identified and plausible solutions have been suggested.

My recommendations for future research would be to discuss the pros and cons of the suggested solutions with security experts within aviation, and proceed with testing and prototyping of the most promising ones to adjust them to the current needs of the Swedish and global aviation infrastructure.

8 Ethical discussion

Performing a study about the security and integrity of a technology currently in partial use with plans to expand its usage within the aviation industry brings its own ethical considerations. Aviation safety is a critical matter not to be taken lightly. Millions of passengers use its infrastructure every year and its growth its predicted to continue. It is therefore vital that the industry continuously work towards maintaining a high level of safety. Part of this is the existence of reliable and secure communication, navigation and surveillance tools at the air traffic controller's disposal. The general goal is to raise awareness about the existing shortcomings of CPDLC current state and not to spread fear. It is with the hope of optimism that this study will assist in minimizing the risks of CPDLC and hopefully even future technologies.

9 Bibliography

[1] "IATA Air Passenger Forecast Shows Dip in Long-Term Demand," [Online]. Available: http://www.iata.org/pressroom/pr/Pages/2015-11-26-01.aspx. [Accessed 2018-04-09].

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

[3] M. Strohmeier, V. Lenders and I. Martinovic, "On Security of the Automatic Dependent Surveillance-Broadcast Protocol," Cornell University Library, arXiv:1307.3664v2 [cs.CR], 2014. [Online]. Available: https://arxiv-org.e.bibl.liu.se/pdf/1307.3664v2.pdf. [Accessed 2018-04-09].

[4] D. Di Marco, J. Hird, A. Manzo and M. Ivaldi, "Security Testing with Controller-Pilot Data Link Communication," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, Austria, 2016, pp. 526-531.

[5] K.-L. Du and M. N. S. Swamy, Wireless communication systems: from RF subsystems to 4G enabling technologies, New York: Cambridge University Press, 2010.

[6] R. K. Nichols, Wireless security: models, threats, and solutions, New York: McGraw-Hill, 2002.

[7] P. Chandra, Bulleftproof Wireless Security, Oxford: Newnes, 2005.

[8] R. Bone and K. Long, "Air Traffic Controller Utilization of Voice and Data Link Communication During Interval Management," *2016 Integrated Communications Navigation and Surveillance (ICNS),* pp. 2D1-1-2D1-16, Herndon, VA, 2016.

[9] P. A. Massimini, J. E. Dieudonne, L. C. Monticone, D. F. Lamiani and E. A. Brestle, "Insertion of Controller-Pilot Data Link Communication into the National Airspace System: Is It More Efficient?," *IEEE Aerospace and Electronic Systems Magazine,* vol. 15, no. 9, pp. 25-29, Sep. 2000.

[10] M. Strohmeier, "Security in Next Generation Air Traffic Communication Networks," Ph.D. Thesis, Kellogg College, University of Oxford, 2016.

[11] International Civil Aviation Organization, *Global Operational Data Link Document (GOLD),* International Civil Aviation Organization (ICAO), 2013.

[12] ETSI EN 301 841 V1.4.1, "VHF air-ground Digital Link (VDL) Mode 2; Techical characteristics and methods of measurements for ground-based equiptment; Part 1: Physical layer and MAC sub-layer," European Telecommunications Standards Institute, 2015. [Online]. Available: http://www.etsi.org/deliver/etsi_en/301800_301899/30184101/01.04.01_60/en_30184101v010401p.pdf. [Accessed 2018-04-09].

[13] ICAO Document 9776/AN970 (first edition), "Manual on VHF Digital Link (VDL) Mode 2,"

International Civil Aviation Organization, 2001.

[14] H. Imai, M. G. Rahman and K. Kobara, Wireless Communication Security, Boston: Artech House, 2006.

[15] N. Koblitz and A. J. Menezes, "A Riddle Wrapped in an Enigma," *IEEE Security & Privacy,* vol. 14, no. 6, pp. 34-42, Dec. 2016.

[16] V. Miller, "Use of Elliptic Curves in Cryptography," in *Williams H.C. (eds) Advances in Cryptology — CRYPTO '85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science*, vol 218. Springer, Berlin, Heidelberg, 1986, pp. 417-426.

[17] E. Barker, "Recommendation for Key Management Part 1: General," National Institute of Standards and Technology, 2016. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4 [Accessed 2018-04-09].

[18] J.-A. Kylén, Att få svar, Stockholm: Bonnier Utbildning AB, 2004.

[19] M. Björklund and U. Paulsson, Seminarieboken, Lund: Studentlitteratur AB, 2012.

[20] M. Dalen, Intervju som metod, Mamlö: Gleerups Utbildning AB, 2015.

[21] R. Ejvegård, Vetenskaplig Metod, Lund: Studentlitteratur AB, 2009.

[22] A. Costin and A. Francillon, "Ghost in the Air(Traffic): On Security of ADS-B protocol and practical attacks on ADS-B device," 2012. [Online]. Available: http://s3.eurecom.fr/docs/bh12us_costin.pdf. [Accessed 2018-04-09].

[23] M. Schäfer, V. Lenders and I. Martinovic, "Experiment Analysis of Attacks on Next Generation Air Traffic Communication," in *Jacobson M., Locasto M., Mohassel P., Safavi-Naini R. (eds) Applied Cryptography and Network Security. ACNS 2013. Lecture Notes in Computer Science*, vol 7954. Springer, Berlin, Heidelberg, 2013, pp. 253-271.

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

[25] T. McParland, V. Patel and W. Hughes, "Securing air-ground communication," in *20th DASC. 20th Digital Avionics Systems Conference*, Daytona Beach, Florida, 2001, vol. 2, pp. 7A7/1-7A7/9.

[26] M. L. Olive, "Efficient Datalink Security in a Bandwidth-Limited Mobile Environment - An Overview of the Aeronautical Telecommunication Network (ATN) Security Concept," in *20th DASC. 20th Digital Avionics Systems Conference*, Daytona Beach, Florida, 2001, vol. 2, pp. 9E2/1-9E2/10.

[27] D. Getachew and J. H. Griner, "An Elliptic Curve Based Authentication Protocol For Controller-Pilot Data Link Communications," in *2005 Integrated CNS Technology Conference & Workshop*,

Fairfax, Virginia, 2005.

[28] International Civil Aviation Organization, "Doc 4444 (PANS-ATM)," International Civil Aviation Organization, 2016.

[29] EUROCONTROL, "SKYbrary," 2008. [Online]. Available: https://www.skybrary.aero/index.php/CPDLC_Incorrect_Call_Sign_on_Log-on. [Accessed 2018-02-11].

[30] M. Strohmeier, M. Schäfer, M. Smith, V. Lenders and I. Martinovic, "Assessing the Impact of Aviation Security on Cyber Power," in *2016 8th International Conference on Cyber Conflict (CyCon) Cyber Conflict (CyCon)*, 2016, pp. 223-241.

[31] A. McCullagh and W. Caelli , "Non-Repudiation in the Digital Enviroment," 2000. [Online]. Available: http://www.firstmonday.org/ojs/index.php/fm/article/view/778/687. [Accessed 11/02/2018].

[32] "IEEE Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams," *IEEE Std 802.15.9-2016,* pp. 1-74, 2016-08-17.

[33] F. de Oliviera Gil, L. F. Vismari, J. Batista and C. Júnior, "Analysis of the CPDLC Real Time Characteristics and the Mode S Data Link Capacity," in *Symposium of Air Transportation*, 2008.

[34] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless Communications,* vol. 11, no. 1, pp. 62-67, February 2004.

[35] D. Shumow and N. Ferguson , "On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng," 2007. [Online]. Available: http://rump2007.cr.yp.to/15-shumow.pdf. [Accessed 2018-02-11].

[36] S. Nick, "A (relatively easy to understand) primer on elliptic curve cryptography," 2013. [Online]. Available: https://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/3/. [Accessed 2018-02-11].

[37] P. E. Storck, "Benefits of Commercial Data," in *2013 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, Herndon, Virginia, 2013, pp. 1-26.

[38] J. Salisbury, "Protected ACARS (PACARS)," in *The MITRE Corporation CNS/ATM Conference*, 2011. [Online]. Available: http://www.afceaboston.com/documents/events/cnsatm2011/Briefs/02-Tuesday/Tuesday-PM%20Track-2/01-Salibury-Protected%20ACARS-Tuesday%20Track2.pdf. [Accessed 2018-04-09].

[39] B. Burton, "Data Link Deep Dive," 2013. [Online]. Available: http://www.wxaviation.com/Data_Link_Deep_Dive_HON_Ops_Conf_2013.pdf. [Accessed 11/02/2018].

[40] A. Gurtov, Host Identity Protocol (HIP): Towards the Secure Mobile Internet, John Wiley & Sons, 2008.

[41] P. Nikander, A. Gurtov and T. R. Henderson, "Host Identity Protocol (HIP): Connectivity, Mobility, Multi-homing, Security, and Privacy over IPv4 and IPv6 Networks," *IEEE Communications Surveys & Tutorials,* vol. 12, no. 2, pp. 186-204, April 2010.

[42] A. Khurri, E. Vorobyeva and A. Gurtov, "Performance of host identity protocol on lightweight hardware," in *Proceedings of ACM SIGCOMM 2007 Workshops - 2nd ACM International Workshop on Mobility in the Evolving Internet Architecture, MobiArch'07*, Kyoto, Japan, 2007, pp. 1-8.