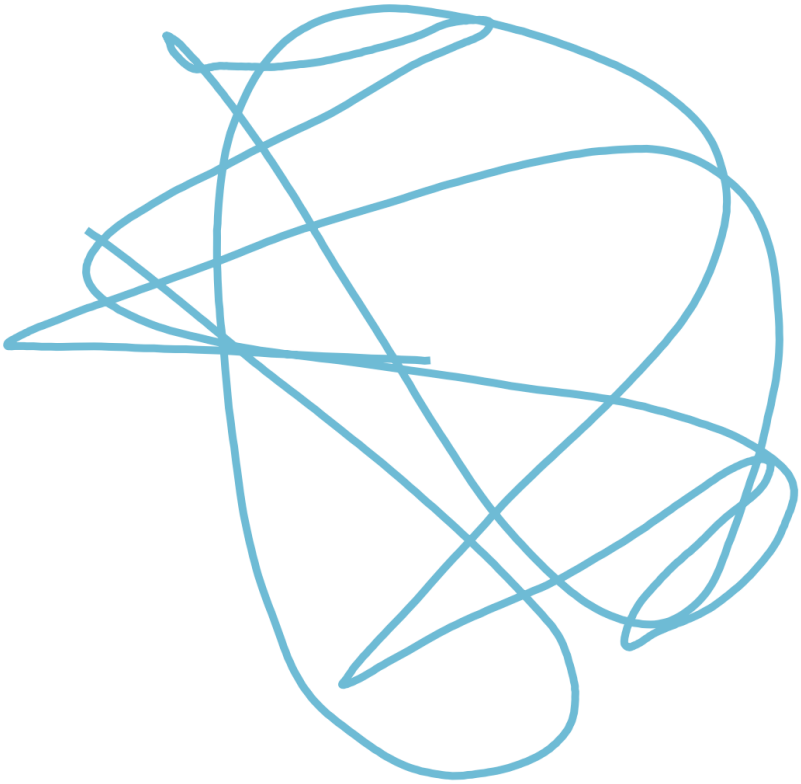
Radio Frequency Fingerprinting for Aircraft Identification

MSc Thesis Report

by

A.R. Louwen

May, 2022



TU Delft

Radio Frequency Fingerprinting for Aircraft Identification

MSc Thesis Report

by

A.R. Louwen

Student Number: 4390768
Supervisor: Dr. J. Sun
Thesis committee: Prof.dr.ir. J.M. Hoekstra
Dr. J.A.M. Vanhamel

TU Delft

Acknowledgements

This document is the result of the final thesis project to obtain the degree of master of science. The work consists of a scientific paper, accompanied by the preliminary thesis work which represents the first parts of the thesis project. I would like to thank my thesis supervisor Dr. Junzi Sun, for giving me the chance to work on this subject. I have always enjoyed our meetings and the feedback you provided me. You helped me shape this research and inspired me to approach projects using a critical mindset. I have learned some valuable lessons which will surely be of use in my later career. I would also like to thank Prof. Dr. Ir. Jacco Hoekstra for his feedback and valuable input during the final parts of my thesis.

My gratitude goes out to Ilse for her continuous company, love, and support. You gave me the encouragement I needed to do this project. Last but not least, I would like to thank my parents Kees and Astrid, and my sister Sanne, who gave me the opportunity and support to finish my studies.

A.R. Louwen
Delft, June 2022

Part I

Scientific Paper

Radio Frequency Fingerprinting for Aircraft Identification

Anton Louwen,
Supervised by: Junzi Sun and Jacco Hoekstra
Control & Simulation, Faculty of Aerospace Engineering
Delft University of Technology

***Abstract*—Radio frequency fingerprinting has been identified as a method to increase integrity in aircraft surveillance while retaining its openness. One way to uniquely determine transmitting devices is to distill the device its radio frequency (RF) fingerprint by looking at the physical features of the message signal it transmits. This physical layer fingerprint is the unique trace the transmitter leaves in the signals. This research proposes a method to RF fingerprint ADS-B and VDL2 messages to identify the transmitting aircraft using a complex-valued convolutional neural network model. Raw data from ADS-B and VDL2 messages are collected over multiple days using low-cost RTLSDR hardware. Results show that the model can identify ADS-B and VDL2 messages from up to 200 different aircraft based on the raw IQ preamble and bit synchronization samples of both signal protocols. Further analysis of the robustness of the model shows that the model accuracy can be highly affected by changing channel conditions during training and testing. This research shows that testing the RF fingerprinting model's robustness to channel conditions is necessary since the models are prone to mistakenly considering channel information as transponder RF features.**

***Index Terms*-Radio Frequency Fingerprinting, Deep Learning, Complex valued convolutional neural network**

I. Introduction

The air traffic management infrastructures in parts of the world are currently reaching their limits of capacity due to ever-increasing congestion. Besides this, the aviation industry has to increase sustainability and reduce its environmental impact dramatically in the coming decades. These are some of the major challenges for aviation. To tackle this, modernization programs are being implemented to increase capacity and efficiency such as the FAA its NextGen program and the EASA its SESAR. These projects will implement an increase in digitization, automation, and connectivity in air traffic management. Air traffic management will cross over into the digital realm.

Under these modernization programs, some new aviation surveillance and communication concepts have already been implemented. For example Controller Pilot Data Link Communications (CPDLC) represents a shift in terms of air traffic control communications from voice-based radio communication to digital communications and data links. For surveillance, there will be a shift towards more Automatic Dependent Surveillance (ADS) which means that aircraft provide surveillance data using satellite data such as GPS without the need for radar [1]. Technologies that enable these concepts are ADS-B (1090ES), which is a surveillance protocol that aims to increase safety by providing an extra means of surveillance by transmitting position information automatically between aircraft and ground stations [2], and VDL2 is a communications protocol that is the physical layer that enables CPDLC over VHF radio [3]. But this increase in digitization means the industry faces numerous challenges in cyber-security [4]. For example, the relatively new ADS-B technology, which is one of the core technologies implemented for both modernization programs, was developed as an open protocol [2]. The same holds for CPDLC (VDL2) [3]. This has many advantages, such as ease of implementation, low cost and it provides the research community with invaluable data [5].

The openness of these protocols must be preserved to uphold the many advantages it gives, but it comes at the cost of vulnerability to cyber-attacks. One of the reasons for this is because the messages in both ADS-B and VDL2 are identified or authenticated by an address that is transmitted in the message. This is the unique 24-bit ICAO code sent out by ADS-B transponders and VDL2 radios. These addresses are used to uniquely identify the transmitting aircraft. However, the problem is that these addresses can be spoofed such that an attacker is able to impersonate a device. The possibility to spoof wireless transmitting devices and impersonate aircraft or inject messages has obvious implications for the integrity of the wireless protocol. A way to uniquely identify a transmitting device by the receiver is to identify the device by its physical layer fingerprint [6]. This physical layer fingerprint, also called RF fingerprint or RFF is the unique trace the transmitter leaves in the signal it sends. Using this RF fingerprint as an extra layer of identification can possibly make both protocols more secure while retaining the openness of the protocols.

Already, it has been shown that RF fingerprinting could also be used to identify and distinguish between different aircraft ADS-B signals, without relying on the ICAO 24-bit address present in the message. Most of the methods researched use some form of deep learning. VDL2 could also, be eligible for RF fingerprinting to identify aircraft. Because of this, the goal of this research is to investigate if the VDL2 signals could be used to identify aircraft through

RF fingerprinting by using deep learning methods.

This research discusses the technical aspects and research on the security for ADS-B and VDL2, the background of RF fingerprinting, the research method used, and finally results. The main contributions of this research are as follows:

- In this research raw IQ data from ADS-B and VDL2 messages are collected over multiple days using cheap SDR hardware.
- This research proposes a complex CNN model which can identify aircraft based on the preambles of raw IQ message data for ADS-B and VDL2 messages for up to 200 different aircraft. The model avoids to use ID information within the messages as features for classification.
- This research investigates the robustness of the models to different population sizes, noise, transmitter hardware similarity, message injections and channel effects.
- This research shows the importance of investigating the channel effects when investigating RF fingerprinting methods. Results show these can have a large effect on the overall performance of classification by the model.

II. Technological Background

This section will explain the technological basics of the protocols used in this research: ADS-B and VDL2.

A. ADS-B

Compared to legacy radar surveillance methods such as the primary (PSR) and secondary surveillance radar (SSR), that determine the aircraft position using ground-based radar stations, the ADS-B system obtains positioning information from the (GNSS). This shift from independent ground-based localization surveillance or to on-board localization or dependant surveillance is intended to reduce the high costs of air traffic surveillance. ADS-B is cheaper and less maintenance-intensive compared to both primary and secondary radar equipment. It also aims to increase situational awareness for air traffic management and the safety of the entire air traffic system [7] [2]. From the acronym a lot can be distilled about the technical functionality of the ADS-B system:

- *Automatic*: The ADS-B system automatically sends its data without the need for interrogation.
- *Dependant*: ADS-B surveillance data is collected by on-board systems of an aircraft using for example GNSS.
- *Surveillance*: ADS-B provides air traffic surveillance data. For example 3D-position, velocity, and identification.
- *Broadcast*: The ADS-B protocol depends on broadcasting its surveillance data, such that every receiver in range of the signal can receive and analyze messages.

As of 2020 the ADS-B out capability is mandated to be available on most commercial passenger aircraft in European airspace [8].

The ADS-B out system periodically transmits the aircraft position, velocity, altitude, and identifier. No pilot or air traffic controller has to trigger the broadcast of information or no interrogation is needed to transmit information. Aircraft equipped with ADS-B out periodically and automatically transmit messages to ATC and other aircraft equipped with ADS-B in. Two different competing types of the ADS-B protocol exist, the UAT and the 1090ES. The UAT protocol utilizes the 978 MHz frequency, and because it requires fitting new hardware and is only being used in some countries such as the USA mostly by general aviation [9]. The (1090ES) protocol utilizes the mode S transponder. The mode-S transponder can transmit both 56-bit and 112-bit messages.

This research will only focus on 1090ES 112bit ADS-B messages. The 1090ES Mode-S/ADS-B message comprises of a preamble which is followed by a 112-bit message. This message contains the ADS-B frame information shown in table I, including the 24-bit ICAO address code used as an aircraft identifier. The ADS-B packet is amplitude modulated using PPM. This form of modulation represents a 1 bit using a $0.5\mu s$ pulse followed by a $0.5\mu s$ pause, and the opposite is true for a 0 bit. This signal is modulated on the 1090MHz carrier wave for transmission [10]. The ADS-B message frame is shown in table I:

TABLE I
ADS-B message data frame as adopted from [9]

Bit	Number of Bits	Abbreviation	Information
1-5	5	DF	Downlink Format
6-8	3	CA	Transponder Capability
9-32	24	ICAO	ICAO Aircraft Address
33-88 (33-37)	56 (5)	ME (TC)	Message, extended squitter (Type Code)
89-112	24	PI	Parity/Interrogator ID

B. VDL2

VHF data link (VDL) is the protocol that can transmit CPDLC and ACARS over VHF via the FANS-1/A systems. 4 versions of VDL have been developed. The first VDL1 was a version that utilised analog radios which is considered outdated and was thus never adopted. The second VDL2 is the only adopted and implemented VDL. The third VDL3 was a version that tried to implement a form of digitized voice communications, but airlines did not adopt this technology due to its complexity. Lastly, VDL4 was a contender to be the physical layer for ADS-B but was not implemented in favor of the Mode-S extended protocol which is discussed above. [11].

VDL2 is the physical layer that enables Controller Pilot Data Link Communications CPDLC over VHF. One of its other uses is the ability to send Aircraft Communication Addressing and Reporting System ACARS messages, which is called ACARS over Aviation VHF Link Control AVLC, AVLC is the aviation VHF link control that contains the data of the VDL2 messages [11]. ACARS messages were initially sent out over VHF analog radios, this is also referred

to as POA or plain old ACARS. As compared to POA the VDL2 system provides better performance such as a higher bit rate and is a more modern communications protocol [12]. Currently, the VDL2 datalink is the most used form of digital communication in aviation [13]. VDL2 shares the same VHF band as the VHF radio voice communication (118 [MHz] - 137 [MHz]). VDL2 uses a Differential 8-Phase Shift Keying modulation scheme (D8PSK), which encodes the message in the phase domain. The phase changes of the signal carrier wave contain the data of the message.

Before a VDL2 message is transmitted the input bits are mapped to a phase difference in the signal wave using Gray code. Using Gray code has the advantage that if a bit error occurs during for example the transmission, the error will be smaller as compared to using normal binary code [14]. Each symbol transmitted consists of three bits mapped by a phase difference. Because D8PSK does not use a reference phase to achieve phase coherence in a message, message bits are demodulated using the difference in phase with respect from the previous symbol or signaling interval, hence the name 'differential'. To do this 2 requirements have to be fulfilled, the channel effects and the transmitter oscillator have to be stable enough such that unknown phase changes very slowly such that the phase is effectively constant from one signal interval or symbol through the next. The second requirement is that the phase of the current symbol interval has to have a relationship with the previous interval [15]. The first requirement is fulfilled by using a proper transmitter oscillator and the second is fulfilled by differential encoding the phase using the current and previous phase of the signal [14]:

$$\phi_k = \phi_{k-1} + \Delta\phi_k \tag{1}$$

After the signal has been differentially encoded, the modulated signal $x(t)$ can be obtained by separately modulating the signal by its in-phase (I) and quadrature (Q) components before adding these.

A VDL2 message consists of a training sequence and the message data. Before a sequence of messages is sent the training sequence ensures a synchronization of transmitter and receiver. The training sequence consists of five parts: the transmission ramp up, bit synchronization, symbol, transmission length and header FEC showed in table II. The transmitter ramp-up is there to setup the transmitter power stabilization and receiver gain control [14], the synchronization code is there for the receiver of the message to find the synchronization point of the message and consists of a fixed known sequence of bits [11]. The FEC or forward error correction enables the receiver to detect bit errors in the message data. The message data is sent using AVLC frames. For purposes of brevity this is not discussed in detail, it is however to be noted, that the message data always includes the 24-bit ICAO address of the sender of the message.

TABLE II
VDL2 HEADER FRAME AS ADOPTED FROM [14]

Bit	Number of Bits	Number of Symbols	Information
0-15	15	3	Transmitter Ramp up
15-63	48	16	Bit Synchronisation
63-66	3	1	Reserved Symbol
66-83	17	-	Transmission Length
83-88	5	-	Header FEC
88-	1992	-	AVLC Frame + FEC

C. Security Measures

Both modern improvements in communications and surveillance, CPDLC with VDL2, and ADS-B were designed as open protocols which has many advantages in terms of ease of implementation, data for research, or investigative journalism. But this openness introduces some shortcomings in terms of confidentiality, integrity and availability of the service. This can lead to possibly dangerous situations in air traffic management and has been a subject of previous research, with many authors stressing the need for more security in ADS-B [2], [16]–[18], as well as in ACARS and CPDLC [3], [19]–[21]. Multiple security measures have been proposed for ADS-B such as encryption algorithms, spread spectrum technologies, or data verification techniques. Currently, no security measures have been implemented nor are there any plans to implement security measures in the future. Each security solution has its positive and negative sides but, not one security solution is suitable to provide full security [2]. Furthermore, it is debatable whether the openness of ADS-B should be compromised. The open nature of ADS-B has many advantages and is an essential component of ADS-B [22]. Besides this, adopting a system that does not require a change in protocol is easier to implement. This research proposes RF Fingerprinting to provide an extra method of identification for ADS-B and VDL2 messages without requiring a change in protocol and that retains the openness of both systems.

III. RADIO FREQUENCY FINGERPRINTING

Traditionally, most wireless transmitting devices are identified or authenticated by an address that is transmitted by this device. Examples of these are the unique 24-bit ICAO code sent out by ADS-B transponders or the MAC-address of a device connected to the internet. These addresses are used to uniquely identify the transmitting device. The problem is however that these addresses can be spoofed such that an attacker can impersonate a device. A way to uniquely identify and authorize a transmitting device by the receiver is to identify the device by its physical layer fingerprint [6]. The process of identifying a signal by retrieving the signal's unique physical layer features due to hardware imperfections is called Radio Frequency Fingerprinting [24]. It has been shown that due to randomness in the manufacturing process of wireless devices, small imperfections arise that affect the features of

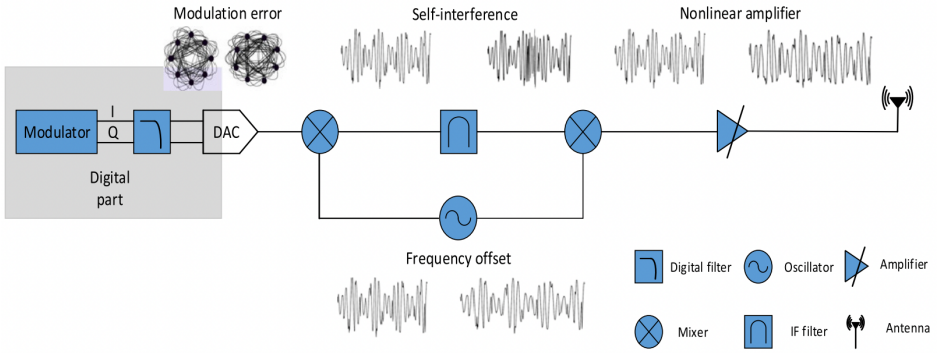


Fig. 1. Universal software radio transmission reprinted from [23]

the signals these devices transmit. These imperfections can be exploited to uniquely identify the signal's transmitter. Moreover, the likelihood that two of the same transmitters have the same fingerprint is very low [24]. This renders radio frequency fingerprints usable to provide an extra identification layer that provides more security and integrity in the wireless protocol.

A. Principles of the Fingerprint

Because there is an inherent degree of variance and tolerances in the accuracy of manufacturing radio transmitter components, no signal transmitter will be able to transmit the theoretically perfect signal. Even if the transmitting device is from the same manufacturer, it will still have some minute differences [6]. These imperfections are the actual physical constructs that enable RF fingerprinting, as can be seen from figure 1. Before transmission, several digital and analog components will have their effect on the eventual signal transmitted, with each their corresponding small error on the signal. Examples of the transmitter imperfections are the modulation errors produced by the modulator, frequency offset, and phase noise by the oscillator and non-linear distortion produced by the amplifier. During transmission traces of these effects can be found in the signal. This trace is called the RF fingerprint because these errors are inherent to the device transmitter they are very difficult to be reproduced and can thus be exploited to identify specific devices [6].

The goal of physical layer identification using the RF fingerprints is to extract the features of the origins of the fingerprinting to create a RF fingerprint of devices. A library of known devices their RF fingerprints should be created to provide a list of which devices are able to transmit messages. The receiving devices should use this library to classify if the fingerprint of the received signal compares with that of a known fingerprint. This will authenticate if a message is from a known sender. To provide a usable layer of identification, the radio frequency fingerprints and devices should fulfill the following conditions [6]:

- *Universality*: Every device should have features which are used for fingerprinting
- *Uniqueness*: Every device should have a unique fingerprint
- *Permanence*: The fingerprints should be time and environment invariant.
- *Collectability*: The fingerprints should be obtainable with existing equipment
- *Robustness*: The fingerprints should be evaluated and robust to changes in device aspects such as temperature/voltage and external environmental aspects such as effects of signal reflection or absorption

Many different features based on the protocol in signals can be exploited and combined to provide a fingerprint.

B. RF Fingerprinting for Aerospace Signals

To provide more security and identification in wireless protocols, RF fingerprinting for identification to improve security has been a topic of interest for many researchers. RF fingerprinting is possible for many different applications, such as wifi, Bluetooth, and Zigbee devices: [34], [35] and [36]. Since signals such as ADS-B and CPDLC VDL2 are periodically transmitted by aircraft, aircraft identification based on RF fingerprinting these signals is possible [32].

There has been a lot of research on specifically ADS-B fingerprinting with a great diversity in the type of fingerprinting and the features used to fingerprint. Most of the published work on ADS-B fingerprinting used IQ data to provide the features for fingerprinting with many employing machine learning techniques such as a neural network to feed IQ data directly in a neural network to provide a classification of the aircraft transponder transmitting the ADS-B signal.

Table III provides an overview of some of the research on RF fingerprinting for signals that are emitted from aircraft. As can be seen, the number of different features and input data can vary, but most use raw IQ data as input. This is useful if different signal protocols are considered for RF fingerprinting using the same classifier. Furthermore, use is made of the phase pattern and the short-time Fourier transform. The performance of the RF fingerprints can

TABLE III
RF FINGERPRINTING RESEARCH AND PERFORMANCE COMPARISON

Research	Signal	Features or Input Data	Data set (Transmitters)	Classifier	Performance (Accuracy)
[25]	ADS-B/WiFi	Raw IQ	5000	CNN/ResNet50-1D	up to 99%
[26]	ADS-B/WiFi	Raw IQ	100	Recurrent DCN	100%
[27]	ADS-B	Raw IQ/STFT	1000	Complex CNN	up to 86% (100 devices)
[28]	ADS-B	Contour Stellar Images	5	AlexNet/GoogleNet	>95%
[29]	ADS-B	Raw IQ	100	Complex CNN	81.6% (focus on preamble)
[30]	ADS-B/Wifi	Raw IQ	10000	Dilated Causal CNN	up to 99%
[31]	ADS-B	Phase Pattern	2942	kNN	- (intruder detection)
[32]	ADS-B	Phase Pattern	274	CNN	41.7%
[33]	ACARS/ADS-B	Raw IQ	5157/3022	Inception Res CNN	98.1% / 96.3%

vary widely and depends highly on the size of the datasets used. For example in [25], the performance for a dataset containing 5000 different devices was approximately 77% for the ResNet50-1D and 53% for the CNN (Baseline Model). Whereas the performance for a dataset containing 50 devices, was 86% and 92% for both models respectively. As can be seen, by the table, most of the RF fingerprinting work focused on the RF fingerprinting of ADS-B signals and not from signals other aircraft emit such as VDL2. A single example was found for ACARS (POA) messages that have been a topic of research by [28]. In the research a large ACARS (POA) data set (900,000 samples from 3143 aircraft) was used. The fingerprints were extracted from the raw signal samples using an inception residual neural network. It was furthermore shown that the network could also work for ADS-B type signals.

Most previous works on radio frequency fingerprinting of aerospace signals make no mention if training and testing data were collected over different periods to investigate channel effects. As can be seen in section VII, this can have a large influence on performance. Furthermore, some authors do not mention if ID data is used as an input for the model, this can have a very large effect on the performance since deep learning models tend to cheat by using this data to classify messages. To the best of knowledge, no research has been found on the RF fingerprinting of VDL2 or (ACARS over AVLC) signals. There is thus an apparent research gap in the RF fingerprinting of the VDL2 type of messages. The main contributions of this research are to investigate if RF fingerprinting is possible for VDL2 signals as well as ADS-B signals using a deep learning method and to test what the effect of the channel is on an RF fingerprinting model for aircraft identification.

IV. METHODOLOGY

The method for RF fingerprinting first consists of the creation of a model which can extract fingerprints based on message data collected. This can be seen in figure 2. The workflow consists, of the collection of messages of the RF signal of interest. In this research, those signals are ADS-B and VDL2. This data is collected and pre-processed such that it can be used in an RF fingerprinting deep learning model. The training of the model is done using a predefined set of training data consisting of pre-processed and labeled sets of real ADS-B and VDL2 messages from aircraft. These messages are defined as the training set. The trained model will learn to distinguish between messages from the different aircraft and assign messages to an aircraft.

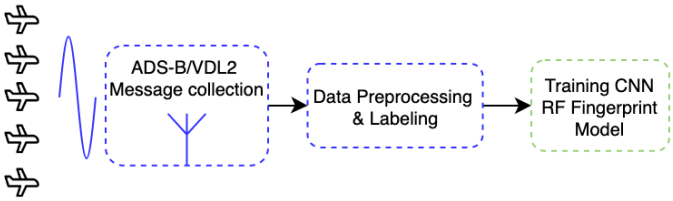


Fig. 2. Training the RF fingerprinting model.

After the model has been trained to generalize well on ADS-B and/or VDL2 messages from the aircraft in the training set. It can be employed to identify aircraft based on the RF fingerprints of these messages. This is done by collecting the message and pre-processing the message data before feeding it through the deep learning model. The deep learning model will classify from which aircraft the message is most likely to be sent, thus providing identification based on the RF fingerprint. This process can be seen in figure 3.

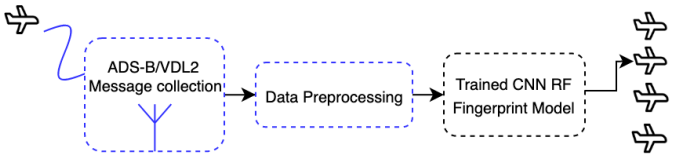


Fig. 3. RF fingerprinting for identification.

A. RF Feature Extraction Method

To develop a model that can classify aircraft based on RF fingerprints, correct features have to be extracted which fulfill the condition requirements that are explained in section III-A. Most previous work on RF fingerprinting for ADS-B data made use of raw IQ values or signal processing methods such as the short-time Fourier transform (STFT) as inputs for a deep learning model. This research will use raw IQ data as an input to extract the RF fingerprints.

1) IQ Data: Suppose we have a bandpass signal $x_{bp}(t)$, which is the RF signal, in our case, the signal containing the ADS-B or VDL2 messages. The collected signal is separated before being multiplied in the time domain by: in the in-phase (I) channel: $cos(2\pi f_c t)$ and in the quadrature channel (Q): $sin(2\pi f_c t)$. Both sinusoids have a center frequency which is equal to the center frequency f_c of the RF signal being sampled. For ADS-B center frequency is 1090Mhz and for VDL2 the center frequency is somewhere between 118-137Mhz. In the frequency domain, this centers the frequency components of the signal of interest around zero, after which a low pass filter can extract the signal of interest. This gives the complex continuous $I(t)$ and $Q(t)$ values which have to be converted to a digital sequence using a sufficient sample rate f_s. For ADS-B the signals have to be sampled at a rate $> 2MSPS$ because of the pulse cycle of ADS-B at $0.5\mu s$ [9]. This yields the discrete IQ samples of the signal $x(n)$:

$$x(n) = I(n) + jQ(n) \tag{2}$$

from which a lot of information regarding phase $\phi(n)$, frequency $f(n)$ and magnitude or amplitude $a(n)$ of the sampled signal can be distilled. [37]:

$$a(n) = \sqrt{I^2(n) + Q^2(n)} \tag{3}$$

$$\phi(n) = tan^{-1}\left(\frac{Q(n)}{I(n)}\right) \tag{4}$$

$$f(n) = \frac{1}{2\pi}\frac{\phi(n) - \phi(n-1)}{\Delta n} \tag{5}$$

Besides the signal features described above, the raw IQ data can contain lots of latent features of the origins of the fingerprint described in section III-A. The deep learning model has to extract these features hidden within the IQ data.

B. Model Selection

As can be seen in table III there is a high number of possible classification models that can be used to perform RF fingerprinting even for the same signal protocol. Deep learning provides a high number of advantages over traditional classification methods. Such as automatic feature extraction [38]. Deep learning methods generally perform well in automatically extracting features from data as compared to traditional classification methods. In RF fingerprinting problems, features are to be extracted from the message signals collected. These collected signal are subject to a high number of distortions coming from different sources. Examples are channel impairments, such as multi-path effects, noise, and interference [38]. Because of this, the choice is often made to develop a deep learning model for RF fingerprinting. CNN's have proven to be very effective in the fields of computer vision, natural language processing and as of recently the field of RF fingerprinting, therefore this research utilizes a CNN to extract the RF fingerprints. Furthermore, because the input data consists of the complex IQ values, the choice is made to develop a complex neural network. This has been shown to improve classification performance over real-valued networks in RF fingerprinting for ADS-B and WIFI messages in [29] as well as in [27]. The model is implemented using Tensorflow [39] and the complex-valued neural network package CVNN by [40].

C. Model Architecture

The model architecture consists of the input layer, the feature extraction layers, the classification layers, and can be seen in figure 4.

*1) **Input Layer**:* The input to the neural network is the complex IQ data. Most neural network architectures can only handle real-valued inputs. Complex data first had to be converted to real values. Recent developments have made the implementation of complex-valued neural networks possible. This research implements a complex-valued convolutional neural network that directly utilises the complex IQ data as an input. The difference between a real-valued network and a complex valued network is that the complex input data is not split into two real valued vectors, but rather fed in through the network directly. This requires the network layers and activation functions to handle complex values.

*2) **Feature Extraction layers**:* The feature extraction layers consist of two complex 1D convolutional layers coupled with a complex average pooling layer. The complex convolutional layers perform complex convolutions according to the equation [41]:

$$I_z * K_z = (I_R * K_R - I_J * K_J) + j(I_R * K_J + I_J * K_R) \tag{6}$$

Where I_z is the complex input vector with $Re(I) = I_R$ and $Im(I) = I_J$ and K_z the convolution kernel containing the weights. The output is afterward activated using the complex cartesian ReLu defined as [40]:

$$CReLu(z) = \max(Re(z), 0) + j\max(Im(z), 0) \tag{7}$$

From which the output is again a complex vector. Two convolutional layers with kernel sizes $k1$, $k2$ number of filters: $f1$, $f2$ are connected with a complex average pooling layer with a pool size of $p1$. The feature extraction blocks are connected n_{stack} times.

*3) **Classification Layers**:* After the feature extraction layers, the data is fed in the classification layers consisting of a flatten layer, which flattens the feature maps and passes these through to a complex dense layer with a number of neurons: $(n1)$. The number of hidden layers are defined as (n_{hidden}). The output layer is first converted to a real number by taking the absolute values, before feeding through to the last layer which has the amount of classes as the number of neurons activated by a softmax activation function, which outputs a probability distribution of an input message belonging to a certain aircraft. See figure 4 for the entire model.

*4) **Model Performance, Training & Validation**:* The model will have to be trained to approximate the function f which is able to determine the correct y_{label} using the input $\mathbf{x_{IQ}}$.

$$y_{label} = f(\mathbf{x_{IQ}}) \tag{8}$$

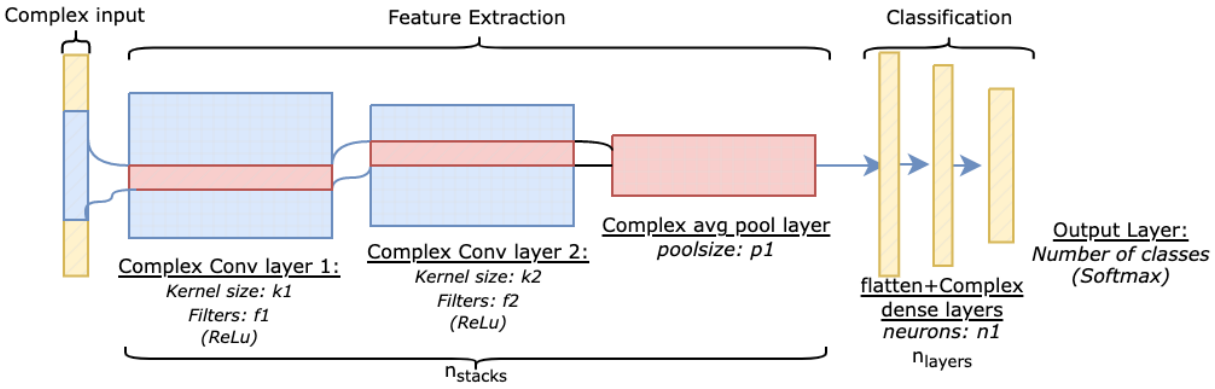


Fig. 4. RF Fingerprinting complex neural network model.

The model weights will be trained using the sgd optimizer algorithm using categorical cross-entropy as the loss function. the training data set consists of the data set: $\mathcal{D} = \{(\mathbf{x_{IQ,i}}, y_{label,i})\}$ where $\mathbf{x_{IQ,i}}$ represents the IQ data of a message i and the $y_{label,i}$ represents the ICAO 24-bit address which is the label of the message i. The model performance will be evaluated using classification accuracy as the metric. The classification accuracy is the percentage of correctly classified $\mathbf{x_{IQ,i}}$ to the correct label.

*5) **Model Parameters**:* The model parameters are tuned and adjusted for optimal performance. For this, a small subset of data was extracted from dataset 1 for both signal protocols containing messages from 50 separate aircraft. The data is split into a separate training, validation, and test set (80/10/10). The model parameters were tuned and selected using the training and validation set. No testing data was used to select the model. The model parameters are shown in table: IV

TABLE IV
MODEL PARAMETERS FOR THE DIFFERENT MESSAGE PROTOCOLS

Parameter:	VDL2	ADS-B
input size	512	32
$k1$	11	7
$k2$	9	5
$f1$	32	32
$f2$	32	32
n_{stacks}	1	1
$p1$	2	2
$n1$	256	256
n_{layers}	1	1

D. Data Pre-Processing

Before the IQ data can be used as an input for the deep learning model described above, the data is to be pre-processed to be of fixed size. Furthermore, input data has to be sliced in such a way that the RF fingerprinting Complex-CNN model is unable to use ICAO ID information as features for classification. If ID information was present within the data, the model can learn to cheat using this ID information, which defeats the purpose of RF fingerprinting. If ID information was present within the input data, both for VDL2 and ADS-B the performance resulted in a near impossible testing accuracy greater than 99%. Furthermore, min-max scaling is used between messages to improve model performance and discards the message amplitude which can be an effect of the channel or aircraft location with respect to the receiver.

*1) **ADS-B**:* For each ADS-B message, 242 IQ samples were collected. The sample number and how it relates to the message bits or contents is shown in figure 5. As can be seen, the ID information is mainly within samples 32-80. Furthermore, flight information is also within the message part, this could also hold ID information such as flight number [9]. Because of this, bits $0-32$ are chosen as input for the complex-CNN. These samples are responsible for the preamble of the ADS-B messages. These are exactly the same for all ADS-B messages, thus data from the message content can not be used as a possible feature to classify an aircraft. The input size for the ADS-B model is 32 samples.

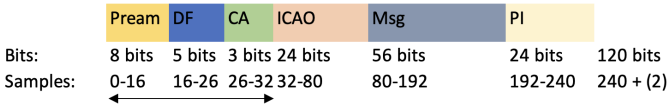


Fig. 5. ADS-B message sample selection

*2) **VDL2**:* For each VDL2 message, more than 5000 IQ samples were collected. The sample number and how it relates to the message bits or contents is shown in figure 6. The ID information is within the samples starting at bit 2400. Because the bit sync is a sequence of symbols that is the same for all VDL2 messages (samples 0-1600), this part is used as an input for our complex-CNN. Again, data from the message content can not be used as a possible feature to classify an aircraft. Because an input size of 1600 is rather large, the samples are split and sliced in two parts of 512 samples. The input size for VDL2 is 512 samples.

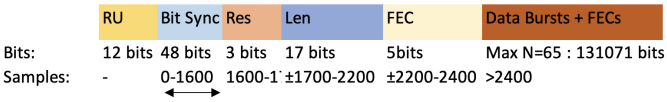


Fig. 6. VDL2 message sample selection

V. Datasets

With the model parameters tuned, data is collected to test the performance in terms of accuracy and robustness of the model in collecting RF fingerprints. ADS-B and VDL2 message data is collected using a software-defined radio. This research makes use of the relatively cheap RTLSDR (RTL2832U). This SDR can collect samples at sample rates up to 3.2 MSPS, with some decrease in stability after 2 MSPS. This maximum sampling rate is sufficient to collect the data but can be a possible bottleneck, if used for RF fingerprinting. Certain works on radio frequency fingerprinting used very high sampling rates ($\geq$ 100 MSPS) which are not achievable by the RTLSDR.

A. ADS-B Data set

The ADS-B IQ data collected was done using the RTL-SDR (RTL2832U) at the TU Delft faculty of aerospace engineering in Delft, the Netherlands. ADS-B data collection was done over a 24h period from 10/01/2022 till 11/01/2022. This data will be referred to as dataset 1 - ADS-B (**D1-ADSB**).

To compare data over different days another set of data was collected from 24/02/2022 till 28/02/2022. This dataset will be referred to as dataset 2-ADS-B (**D2-ADS-B**).

The RTLSDR was set at a center frequency f_s of 1090Mhz and a sampling rate of 2MSPS. Each message was decoded using the pyModeS library. From each message the following data was retrieved:

- 24-bit ICAO code
- Date & time message received
- 242 IQ samples

In total there are about 6mln ADS-B messages collected from different aircraft. To utilise the message data in a deep learning model, the model has to be trained using enough messages per aircraft to learn to extract the fingerprints. Because of this, only aircraft which transmitted more than 500 messages during the collection periods were selected from the data.

B. VDL2 Data

The VDL2 IQ data was again collected at the TU Delft faculty of aerospace engineering in Delft, the Netherlands. Like ADS-B, the VDL2 data was collected on a 24h period from 10-01-2022 till 11-01-2022. This data will be referred to as dataset 1 - VDL2 (**D1-VDL2**).

And to compare data over different days another set of data was collected from 24-02-2022 till 28-02-2022. This dataset will be referred to as dataset 2-VDL2 (**D2-VDL2**)

The RTLSDR was set at a center frequency f_s of 136.775MHz and a sampling rate of 1.05MSPS. Each message was decoded using the pyVDL2 library. From each message the following data was retrieved:

- 24-bit ICAO code
- Date & time message received
- IQ samples ($>$ 5000 samples per message)
- Message type (ACARS/X.25 etc.)
- Type of source (ground station or aircraft)

In total there are about 400k messages collected from different aircraft. To utilise the message data in a deep learning model, the model has to be trained using enough messages per aircraft to learn to extract the fingerprints. Because of this, only aircraft which transmitted more than 200 messages during the collection periods were selected from the data.

VI. Experiments

With the model parameters tuned and data collected. A number of experiments are defined to investigate the performance and robustness of the model in extracting the RF fingerprints. All experiments will be evaluated using model accuracy in terms of correctly classified messages to the test set. For all data used in the experiments the data is randomly split into a training and testing set at a ratio of (90/10).

A. Experiment 1: The Effect of the Population Size

The goal of this experiment is to test if amount of different aircraft the model can classify, has an effect on the accuracy of the model in identifying messages. To test how many aircraft the model can distinguish. The model is trained and tested on subsets of messages from a different amount of distinct aircraft. For this a random selection is made from message data collected from 10/01/2022-11/01/2022 or dataset **D1**. For each experiment a subset of message data containing different amounts of aircraft is used to train and test the model. For each subset the model is trained using 180/450 training messages per aircraft, and tested using 20/50 testing messages per aircraft for VDL2/ADS-B respectively. The model is trained and tested using subsets of message data for 4 different amounts of aircraft:

- 1.A: 25 aircraft
- 1.B: 50 aircraft
- 1.C: 100 aircraft
- 1.D: 200 aircraft

This is an inquiry into the universality and uniqueness requirement of RF fingerprints. The results from this experiment will be used as a baseline to compare results for the following experiments.

B. Experiment 2: The Effect of Noise

The models robustness to noise is evaluated by adding white Gaussian noise to the raw message data. The goal of this experiment is to test the effects of noise on the model accuracy in extracting RF fingerprints. It should be noted that noise is already present currently in the input data since the input are

real collected messages. The effects of noise are measured at a signal to noise ratio (SNR) of 10dB. For this experiment the same subset of messages from 50 aircraft used in experiment 1B is used. The subset is contaminated with noise and used to train and test the model. Results are compared with the subset which is not contaminated with noise (experiment 1.B).

- 2.A: Messages without added noise (Experiment 1.B)
- 2.B: Messages with added noise at an SNR of 10dB.

The noise is added by adding artificial white Gaussian noise (AWGN) to the I and Q parts of the data at an SNR of 10dB.

C. Experiment 3: The Effect of Hardware Similarity

In the aviation industry use is made of a large number of different hardware devices to transmit either ADS-B or VDL2 messages. There could be the possibility that the model does not extract RF fingerprints from a specific unique device, but rather from a certain type of device. Because of this, the effects of hardware similarities are investigated. Here the assumption is made, that operator fleets of the same aircraft, operate similar hardware. The RF fingerprinting model should be able to distinguish between different devices of the same type of hardware. For this, the collected message data from 10/01/2022 is merged with data from the Opensky database [7]. This database contains aircraft data such as: registration, type and operator as well as the ICAO 24-bit address. From this data a subset was selected containing messages from 25 different 737-8K2 WLs from the same operator. The model was trained and tested using this subset. Results are compared with experiment 1A, where the model is trained and tested on a subset of message data from different types of aircraft and operator. Again 180/450 (VDL2/ADS-B) training messages per aircraft were used. And the model was tested using 20/50 (VDL2/ADS-B) messages per aircraft.

- 3.A: Training and testing messages from 25 aircraft of a different type and operator (Results from experiment 1.A).
- 3.B: Training and testing messages from 25 aircraft of the same type and from the same operator.

D. Experiment 4: Message Rejections

The model is trained to distinguish messages from a small subset of aircraft (max 200 in experiment 1.D), but it could very possibly be that messages encountered in the real world are from aircraft which are not within this smaller subset, or could be from possible malicious message injections such as ghost aircraft injections by ground stations. The model should be able to reject these messages if it is used as a possible means of security. To do this the model is slightly adjusted to include an extra class which is the *reject* class. The training set will contain 180/450 (VDL2/ADS-B) messages per aircraft from 50 different *legitimate* aircraft, and 180/450 messages per aircraft from 25 *unknown* aircraft, which will be labeled as the reject class. Using this the model will learn to reject messages from aircraft. The model will afterward be injected with 20/50 messages per aircraft from 25 unknown aircraft which were not in the training set. If these messages are rejected, the model will be able to reject messages from previously unidentified aircraft or possibly malicious message injections from ground stations. The data set used in this experiment is (D1). This experiment is compared with the results from experiment 1.B where the model is not trained to reject messages.

- 4.A: Model not trained to reject messages (Results from experiment 1.B).
- 4.B: Identifying Aircraft while trained to reject messages.
- 4.C: Rejecting injected messages.

E. Experiment 5: The Effect of the Channel

The model should be trained such that it generalizes to the origins of the RF fingerprint instead of the signal channel which can also influence the IQ signal data. Examples of these are multi-path effects or interference. The goal of this experiment is to investigate if the channel influences on the input data have an effect on the model accuracy in classification. To investigate the effects, the model will be trained using data from a single period (D2) but tested using data from a different period (D1). The assumption in this is that the channel effects will vary in time, such that training and testing the fingerprinting model on different days will show the effects of the channel on the accuracy of classification. This experiment will show if the model tends to focus on the channel instead of the origins of the fingerprint. This is an inquiry into the permanence and robustness requirement. For this experiment dataset 2 which are messages collected on 24-28/02/2022 are joined with messages from dataset 1 which are messages collected on 10-11/01/2022. 50 distinct aircraft were transmitting messages on both periods. This data is subdivided into separate training and testing sets such that the model is trained using messages from period 24-28/02/2022, but tested using messages from 10-11/01/2022. There are 180/450 (VDL2/ADS-B) training messages and 20/50 (VDL2/ADS-B) testing messages per aircraft. The model is thus trained using data collected on a separate day from the testing data. Any difference in performance will indicate the model is influenced by the channel effects in the data.

- 5.A: Training and testing the model on a single day (Experiment 1.B)
- 5.B: Training and testing the model over different days

VII. Results

The results from the experiments are measured in terms of accuracy to the testing set and are shown separately for each experiment in tables V-VIII.

A. Experiment 1: The Effect of Population Size

The data set used is separated in a test and training set before messages are selected from 25, 50, 100, and 200 aircraft. As can be seen by the testing accuracy results shown in table V, for ADS-B the testing performance decreases slightly with the introduction of more aircraft. This decrease in performance shows that the model will probably be limited in use if a high amount of different aircraft are to be distinguished. Because it seems the accuracy decreases, where this limit

actually is and at which level of accuracy the model is still usable is not clearly defined and a possible topic for future research. Furthermore, the decrease in performance with the increase of more aircraft is not as prevalent as with VDL2. The performance for VDL2 is also worse as compared to ADS-B, this could be because of a number of reasons:

- The signal type VDL2 could be inherently less prone to RF fingerprinting errors as compared to ADS-B due to the modulation type and way the signal is transmitted by hardware used.
- The amount of training samples per aircraft is lower for VDL2 as compared to ADS-B, which could have an effect on the testing accuracy.
- As we will see in experiment 5, VDL2 is very prone to use the channel as a feature for classification, thus not much can be said about the models ability to extract RF fingerprints.

TABLE V
ACCURACY OF THE MODEL TO THE TESTING SETS IN EXPERIMENT 1 FOR DIFFERENT AMOUNTS OF AIRCRAFT.

Experiment:	Description:	n-Aircraft:	VDL2:	ADS-B:
1.A	Low Population	25	0.81	0.88
1.B	Medium Population	50	0.80	0.86
1.C	Mid/high Population	100	0.80	0.80
1.D	High Population	200	0.79	0.70

B. Experiment 2: The Effects of Noise

To test if noise affects the extraction of fingerprints, the messages used in experiment 1.B are subjected to artificial white Gaussian noise (AWGN) at a signal to noise ratio of 10 dB. The model is trained and tested using the noisy data and results compared with experiment 1.B. As can be seen in table VI, the model performs worse for both ADS-B and VDL2 messages. The effect on the testing accuracy is for ADS-B a decrease of 49% whereas VDL2 shows a decrease of only 27%. This implies noise does have a detrimental effect on the model's accuracy to extract RF fingerprints.

TABLE VI
ACCURACY OF THE MODEL TO THE TESTING SETS IN EXPERIMENT 2 FOR INJECTED NOISE.

Experiment:	Description:	n-Aircraft:	VDL2:	ADS-B:
2.A (1.B)	No added noise	50	0.80	0.86
2.B	Added noise	50	0.57	0.44

C. Experiment 3: The Effect of Hardware Similarity

For this experiment, the effects of similar hardware are investigated. A small set is selected which only contain message from 25 different 737-8K2WLs from the same operator. The assumption made here is that similar aircraft from the same operator utilise similar hardware components and thus that the hardware responsible for transmitting ADS-B and VDL2 messages is similar for all aircraft in this dataset. The RF fingerprinting model could have a harder time extracting fingerprints if the messages are from the same type of devices. As can be seen by the results shown in table VII, the model does not perform worse which indicates that the model can make the distinction between messages from similar devices.

TABLE VII
ACCURACY OF THE MODEL TO THE TESTING SETS IN EXPERIMENT 3 FOR THE SAME AIRCRAFT AND OPERATOR.

Experiment:	Description:	n-Aircraft:	VDL2:	ADS-B:
3.A (1.A)	Different types/ operators	25	0.80	0.86
3.B	Similar type/ operator	25	0.84	0.89

D. Experiment 4: Message Rejections

The goal of this experiment is to determine if the model could be trained in such a way that it can reject messages from aircraft which are unknown. The experiment consisted of a training set containing messages from 50 aircraft which are considered legitimate, and 25 aircraft from aircraft which the model has to reject. The model is both tested using a set of messages from the 50 legitimate aircraft, and tested using a set of messages from 25 aircraft which the model has to reject. Note that the 25 reject aircraft are different from the 25 in the training set.

- **Training set:** 180/450 (VDL2/ADS-B) messages per aircraft from 50 known aircraft + 25 unknown aircraft
- **Testing set 1:** 20/50 (VDL2/ADS-B) messages per aircraft from the 50 known aircraft in the training set.
- **Testing set 2:** 20/50 (VDL2/ADS-B) messages per aircraft from 25 reject aircraft that are not in the training set.

The accuracy for testing set 1 is for VDL2 37% and for ADS-B 71%. The accuracy for testing set 2 is for VDL2 56% and for ADS-B 68%. This means for ADS-B the model is able to reject messages at an accuracy of 68% while still being able to distinguish messages from 50 different known aircraft at an accuracy of 71%. Comparing these results with experiment 1.B means that the performance in identifying aircraft decreases when the model is trained to also rejected messages from previously unidentified aircraft. For VDL2 the performance is again lower as it utilises channel conditions for classification. To accept or reject messages, models that are binary classifiers or anomaly detectors to either accept or reject messages are probably better suited for this task such as the models proposed in the study of [42]. Messages which are accepted by the binary classifier could be passed on for identification of the aircraft using this model.

TABLE VIII
ACCURACY OF THE MODEL TO THE TESTING SETS WHILE REJECTING MESSAGES.

Experiment:	Description:	n-Aircraft:	VDL2:	ADS-B:
4.A (1.B)	Identifying legitimate Messages.	50	0.80	0.86
4.B	Identifying legitimate (trained to reject)	50	0.37	0.71
4.C	Rejecting non-legitimate	25	0.56	0.68

E. Experiment 5: The Effect of the Channel

In this experiment the model is trained and tested on different days for both signal protocols. The goal of this experiment is to investigate if the model utilizes the channel effects on the data as a feature to identify the message transmitter. As can be seen by the results shown in table IX, the accuracy of the test set drastically decreases for VDL2 at a test accuracy of only 12% which is slightly better than chance. This indicates that the model utilizes the channel effects during training instead of the RF fingerprints. ADS-B also shows a decrease in performance but is still able to perform at a test accuracy of 60%. The results of this experiment show that the model can use channel effects as features to classify messages. This has implications for the usability of the model since channel conditions are varying over time the usability is thus limited for multiple days. Furthermore, for the VDL2 model accuracy seems to be highly affected by changing channel conditions. This could indicate that for VDL2 the model does not extract RF fingerprints but identifies the messages based on the channel effects which influence the raw message data.

TABLE IX
ACCURACY OF THE MODEL TO THE TESTING SETS IN EXPERIMENT 5 FOR TRAINING AND TESTING ON DIFFERENT DAYS.

Experiment:	Description:	n-Aircraft:	VDL2:	ADS-B:
5.A (1.B)	Training/testing same period.	50	0.80	0.86
5.B	Training/testing/ different periods	50	0.12	0.60

VIII. DISCUSSION

The goals of the experiments were to investigate if the model was able to extract RF fingerprints for both ADS-B and VDL2 and if the requirements set out in section III-A were fulfilled. As can be seen by the results set out in table V the model is able to correctly identify aircraft ADS-B messages at a maximum accuracy of 88% and for VDL2 messages 81%. But these accuracy figures do not tell the whole story.

Experiment 5 shows that a change in channel conditions can have a large effect on the model's ability to correctly classify messages. This holds especially for VDL2 at a test accuracy of 12% when the channel changes. The results of 5 suggests that the model utilizes the features of the channel to classify the messages, and does not extract RF fingerprints, but rather identifies messages based on the channel in which this message propagated to the receiver. This channel is inherently varying which results in this unstable performance over time. This effect is not examined in most previous literature for aerospace signals (ADS-B), such as in [30] which mentions that the channel does not vary for ADS-B. But as can be seen by the results shown in this research, the temporal conditions of the channel can have a large effect on the performance of an RF fingerprinting model for aircraft identification.

Since for VDL2, the performance is only slightly higher than chance if the channel is changed, it is safe to assume that for VDL2 no RF fingerprints are extracted and the model utilizes the channel as the main feature for classification. The model is thus not able to extract RF fingerprints for VDL2 but it extracts the channel information within the message data. The results of the other experiments for VDL2 should be viewed with this notion in mind.

For ADS-B the effect of changing channel conditions is lower as compared to VDL2. Performance decreases as can be seen by comparing the results of experiment 5.B with 1.B, but the model is still able to classify messages at a higher accuracy than chance at 60%. There is a decrease in performance when the channel is changed which indicates the model utilises the channel information as a means of classification for ADS-B as well, but this is of a lower influence as compared to VDL2.

The results from the other experiments are influenced by the model's use of channel information to identify messages. For example in experiment 3, there is no apparent difference in the models accuracy with similar hardware, this could be because the model partly uses the channel effects on the IQ data to classify the transmitter. So there could be an effect of hardware similarities, but these are not measurable if the channel effects are mistakenly taken as RF fingerprinting features.

The reason the model focuses almost fully on the channel effects instead of the RF fingerprints for VDL2 could be because there are no features present within the raw IQ data which can be utilized to make a distinction between transmitters. This could be because the hardware is inherently less prone to produce distinctive origins of a fingerprint. Another reason could be that the RF fingerprinting features can not be extracted from the IQ data directly and other feature extraction methods which can possibly be more robust to channel effects, such as the periodogram should be investigated.

It can furthermore be possible that the sampling rate used is not sufficient enough to collect features. The hardware used in this research consisted of a low spec RTL SDR which is only able to sample at a maximum stable rate of 2MSPS. The VDL2 messages were sampled utilising a sampling rate

of 1MSPS which could be too low to provide RF fingerprint origin features. This could also explain the performance difference for ADS-B as compared with previous work. Some research utilised sampling rates of ≥ 100MSPS such as [25] and [30]. A higher sampling rate could possibly increase the performance of RF fingerprint extraction, but this should be investigated. This research furthermore investigated if the model could be trained to reject messages outside of the trained aircraft set. As can be seen, the model could be able to reject messages at a test accuracy of 68% whilst still being able to correctly identify the trained set at a rate of 71%. Models which are specifically designed for the task to either accept or reject messages are probably better suited for this task. Messages which are accepted by such a model could be passed on for identification of the aircraft using this model.

The main result of the investigation on the effect of the channel has some implications for previous work on the RF fingerprinting subject. It shows that channel variability can have a large effect and thus should always be investigated if new RF fingerprinting methods are proposed. Furthermore, more investigation into the fingerprinting for VDL2 or ADS-B should be investigated using different feature extraction methods such that the models are unable to utilise the channel effects as features for identification. The authors of [25] state that generative adversarial networks could possibly increase robustness to channel effects. The highest population size used in this experiment was for 200 distinct aircraft. Even larger classification for more devices could be possible using hierarchical classifiers which structure the messages into multiple subsets before classifying. The results of experiment 4 show that the model is able to reject messages from previously unidentified aircraft to a certain degree (68%), but it could be that binary classifiers or anomaly detectors which either accept or reject messages work better for this purpose. Besides this, the overall feasibility of implementing a possible RF fingerprinting framework to identify aircraft to improve security should be considered. Implementing an RF fingerprinting model for aircraft identification requires implementing a library of *approved* aircraft fingerprints which will have to be updated constantly if transmission hardware changes. This can be impractical. Furthermore, there should be a consensus among responsible authorities in the minimal degree of certainty needed to accept or reject messages if such a model were to be implemented.

IX. Conclusion

RF fingerprinting could possibly be used as a method to provide secure identification of aircraft messages. In this research, a complex CNN model was implemented which utilized a low spec SDR to sample IQ data from ADS-B and VDL2 messages. This IQ data is used as an input to classify the transmitting aircraft ADS-B and VDL2 messages whilst being unable to utilize ID information within the data. This research tests RF fingerprinting model's scalability, robustness to noise, channel effects, hardware similarities, and message injections. It shows that for VDL2 the model was scalable to an increasing population but not robust to a changing channel, whereas ADS-B was more robust to changing channel effects as compared to VDL2. It was found that the model utilised channel features as a means of classification for both ADS-B and VDL2 messages. Furthermore, added noise seemed to negatively influence the performance of the model for both ADS-B and VDL2. Hardware similarity does not seem to influence the accuracy of the model but this could be because the model does not only use hardware induced RF fingerprinting features for identification, but also uses channel information. This research also proposes a method to reject messages from unknown aircraft whilst still being able to identify messages from a known set of aircraft.

The main contribution of this research is that it shows the necessity of investigating channel effects since these can have a very large influence on the overall performance of RF fingerprinting models for ADS-B and VDL2. Little can be said about the effectiveness of an RF fingerprinting model without investigating to what extent the model is possible to use the channel as a feature for classification. In most previous research, the effects of channel variability for RF fingerprinting aerospace signals are not investigated.

The results show the model is highly affected by the channel for VDL2 and to a lesser extent ADS-B. More research is needed to investigate the usefulness and feasibility of implementing an RF fingerprinting for aircraft identification to improve security.

References

[1] M. S. Nolan. *Fundamentals of air traffic control*. Delmar Cengage Learning, Clifton Park, N.Y, 5th ed edition, 2011. OCLC: ocn609813680.

[2] M. Strohmeier et al. Security of ADS-B: State of the Art and Beyond. *IEEE Communications Surveys & Tutorials*, 17, July 2013.

[3] C. Bresteau et al. On the security of aeronautical datalink communications: Problems and solutions. In *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, pp. 1A4–1–1A4–13, April 2018.

[4] P. Cooper et al. *Aviation cybersecurity: scoping the challenge*. 2019. OCLC: 1143251182.

[5] M. Strohmeier. Research Usage and Social Impact of Crowdsourced Air Traffic Data. *Proceedings*, 59(1):1, 2020. Number: 1 Publisher: Multidisciplinary Digital Publishing Institute.

[6] N. Soltanieh et al. A Review of Radio Frequency Fingerprinting Techniques. *IEEE Journal of Radio Frequency Identification*, 4(3):222–233, September 2020. Conference Name: IEEE Journal of Radio Frequency Identification.

[7] M. Schäfer et al. Bringing up OpenSky: A large-scale ADS-B sensor network for research. In *IPSN-14 Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*, pp. 83–94, April 2014.

[8] EASA. Amendment to the Airspace Requirements on ADS-B and Mode S, May 2020.

[9] J. Sun. The 1090 Megahertz Riddle: A Guide to Decoding Mode S and ADS-B Signals. 2021. Publisher: TU Delft OPEN.

[10] R. Calvo-Palomino et al. Nanosecond-precision Time-of-Arrival Estimation for Aircraft Signals with low-cost SDR Receivers. *arXiv:1802.07016 [cs, eess]*, February 2018. arXiv: 1802.07016.

[11] S. Lundström. Technical details of VDL Mode 2. Technical report, 2016.

[12] J. Kitaori. A performance comparison between VDL mode 2 and VHF ACARS by protocol simulator. In *2009 IEEE/AIAA 28th Digital Avionics Systems Conference*, pp. 4.B.3–1–4.B.3–8, October 2009. ISSN: 2155-7209.

[13] J. Jiránek and J. Bajer. Aeronautical VHF Data Link mode 2 receiver based on RTL-SDR. In *2017 International Conference on Military Technologies (ICMT)*, pp. 643–647, May 2017.

[14] S. M. Musa and Z. Wu. *Aeronautical Telecommunications Network: Advances, Challenges, and Modeling*. CRC Press, August 2015. Google-Books-ID: GGFECgAAQBAJ.

[15] R. E. Ziemer and W. H. Tranter. *Principles of communication: systems, modulation, and noise*. John Wiley & Sons, Inc, Hoboken, New Jersey, seventh edition edition, 2015.

[16] T. Kacem et al. Security Requirements Analysis of ADS-B Networks. *undefined*, 2014.

[17] Z. Wu et al. Security issues in automatic dependent surveillance-broadcast (ADS-B): A survey. *IEEE Access*, 8:122147–122167, 2020. Publisher: IEEE.

[18] M. Schäfer et al. Experimental Analysis of Attacks on Next Generation Air Traffic Communication. In D. Hutchison et al., editors, *Applied Cryptography and Network Security*, volume 7954, pp. 253–271. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013. Series Title: Lecture Notes in Computer Science.

[19] M. Smith et al. On the security and privacy of ACARS. pp. 1–27, April 2016.

[20] M. Smith et al. Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS. April 2017.

[21] S. Eskilsson et al. Demonstrating ADS-B AND CPDLC Attacks with Software-Defined Radio. In *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*, pp. 1B2–1–1B2–9, September 2020. ISSN: 2155-4951.

[22] ICAO. ADS-B IMPLEMENTATION AND OPERATIONS GUIDANCE DOCUMENT - CNS SG/24 Appendix O to the Report. Technical Report Edition 13.0, September 2020.

[23] J. Li et al. Differential Contour Stellar-Based Radio Frequency Fingerprint Identification for Internet of Things. *IEEE Access*, 9:53745–53753, 2021. Conference Name: IEEE Access.

[24] S. U. Rehman et al. Radio frequency fingerprinting and its challenges. In *2014 IEEE Conference on Communications and Network Security*, pp. 496–497, October 2014.

[25] T. Jian et al. Deep Learning for RF Fingerprinting: A Massive Experimental Study. *IEEE Internet of Things Magazine*, 3(1):50–57, March 2020. Conference Name: IEEE Internet of Things Magazine.

[26] I. Agadakos et al. Chameleons' Oblivion: Complex-Valued Deep Neural Networks for Protocol-Agnostic RF Device Fingerprinting. In *2020 IEEE European Symposium on Security and Privacy (EuroS P)*, pp. 322–338, September 2020.

[27] J. Stankowicz et al. Complex neural networks for radio frequency fingerprinting. In *2019 IEEE Western New York Image and Signal Processing Workshop (WNYISPW)*, pp. 1–5. IEEE, 2019.

[28] H. Zha et al. Real-World ADS-B signal recognition based on Radio Frequency Fingerprinting. In *2020 IEEE 28th International Conference on Network Protocols (ICNP)*, pp. 1–6, October 2020. ISSN: 2643-3303.

[29] S. Gopalakrishnan et al. Robust Wireless Fingerprinting via Complex-Valued Neural Networks. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Waikoloa, HI, USA, December 2019. IEEE.

[30] J. Robinson et al. Dilated Causal Convolutional Model For RF Fingerprinting. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0157–0162, January 2020.

[31] M. Leonardi and F. Gerardi. Aircraft Mode S Transponder Fingerprinting for Intrusion Detection. *Aerospace*, 7(3):30, March 2020.

[32] A. Nicolussi et al. Aircraft Fingerprinting Using Deep Learning. In *2020 28th European Signal Processing Conference (EUSIPCO)*, pp. 740–744, January 2021. ISSN: 2076-1465.

[33] S. Chen et al. Deep Learning for Large-Scale Real-World ACARS and ADS-B Radio Signal Classification. *IEEE Access*, 7:89256–89264, 2019. arXiv: 1904.09425.

[34] K. Merchant and B. Nousain. Enhanced RF Fingerprinting for IoT Devices with Recurrent Neural Networks. In *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, pp. 590–597, November 2019. ISSN: 2155-7586.

[35] J. Hall et al. Detection of transient in radio frequency fingerprinting using signal phase. *Wireless and Optical Communications*, pp. 13–18, 2003. Publisher: ACTA Press.

[36] F. Galtier et al. A PSD-based fingerprinting approach to detect IoT device spoofing. In *2020 IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC)*, pp. 40–49, December 2020. ISSN: 2473-3105.

[37] Y. Tu et al. Research on the Internet of Things Device Recognition Based on RF-Fingerprinting. *IEEE Access*, 7:37426–37431, 2019. Conference Name: IEEE Access.

[38] S. Zheng et al. Big Data Processing Architecture for Radio Signals Empowered by Deep Learning: Concept, Experiment, Applications and Challenges. *IEEE Access*, 6:55907–55922, 2018. Conference Name: IEEE Access.

[39] M. Abadi et al. TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems. *arXiv:1603.04467 [cs]*, March 2016. arXiv: 1603.04467.

[40] J. A. Barrachina. Complex-Valued Neural Networks (CVNN), January 2021. original-date: 2020-09-16T14:02:08Z.

[41] C. Trabelsi et al. Deep Complex Networks. *arXiv:1705.09792 [cs]*, February 2018. arXiv: 1705.09792.

[42] R. Karam et al. A Comparative Study of Deep Learning Architectures for Detection of Anomalous ADS-B Messages. In *2020 7th International Conference on Control, Decision and Information Technologies (CoDIT)*, volume 1, pp. 241–246, June 2020. ISSN: 2576-3555.

Appendix to Paper

This section is meant to provide some extra background into the design choices made to develop the complex-convolutional neural network model for RF fingerprinting. (The references used in this section can be found at the end of this document in the preliminary thesis).

Complex-Valued Convolutional Neural Network

In the preliminary thesis work, use was made of a real-valued convolutional neural network, the real and imaginary parts of the input sequence were treated as a separate real-valued part in the neural network. But since the input vector used in this research is the complex sequence IQ data that represents the sampled signal, it makes sense to treat the values as such. The real and imaginary parts of the input sequence have a degree of correlation, but by treating the input vector as separate real parts, this correlation is mitigated, in other words, more degrees of freedom for the network to possibly exploit are introduced [9]. This could have a detrimental effect on the generalization performance of the neural network. A complex-valued neural network treats arithmetic operations such as convolutions differently as compared to real valued neural networks. As can be seen by equation (6) in the scientific report, the convolution operation of a complex number is different from that of a a real-valued counterpart. The downside of using complex-valued convolutional neural networks is that there are not many libraries available in which complex-valued machine learning could be applied easily. Keras for example does not provide a library for complex-valued layers or activation functions. Furthermore, there are limitations regarding the training algorithms and layers available.

The choice was made to test the performance of a complex-valued convolutional neural network using the library provided by [7]. The model was trained and validated using the subset of training data containing messages from 50 distinct aircraft (data from experiment 1.B). The training data from experiment 1.B was first split in a training and validation set (90/10) the test data was not used to select the model but only used to test the final model for the results presented in the paper. As can be seen from the figures 1, both for ADS-B and VDL2 the validation performance is better for the complex convolutional neural network as for the real-valued neural network used in the preliminary thesis. Because of this, the choice was made to convert the real-valued neural network into a network which is able to use a complex vector as input.

Designing the Model

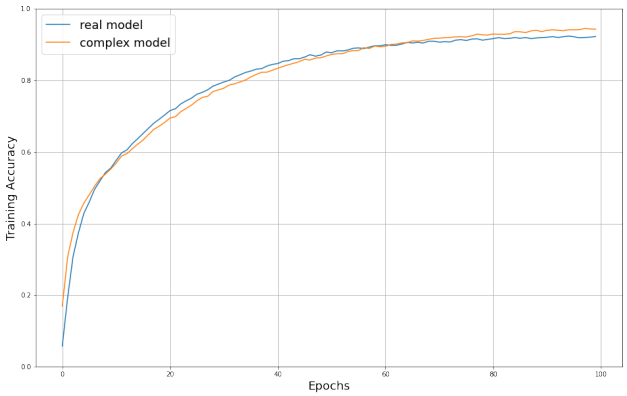
The model chosen is based of a shallower form of AlexNet which proved to perform well for RF-Fingerprinting ADS-B messages under different conditions in the research from the authors of [44]. The model is converted to a complex-valued convolutional neural network for the reasons discussed above. As compared to AlexNet the model used in this research is 1-dimensional, since the input vector is a single 1D complex vector. The model parameters are tuned using the same training and validation data used to compare performance between the complex an real-valued model.

Model Parameters

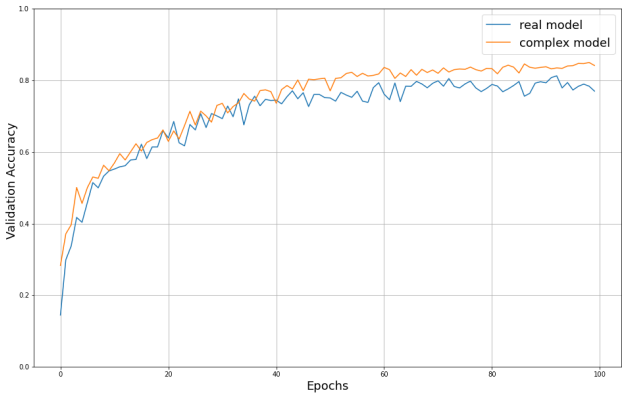
The model parameters chosen are similar to which the model was based upon. The model consists of the input layer, the feature extraction layers and the classification layers. The feature extraction layers consists of two 1D convolutional layers coupled with an average pooling layer which extracts the feature maps. The kernel size chosen for the first convolutional layer for VDL2 is $k1 = 11$ and for ADS-B $k1 = 7$, the kernel is chosen to be larger for VDL2 since the input size is larger. The second kernel size is fixed at $k2 = k1 - 2$. The number of filters is chosen at a fixed $f_{12} = 32$. The pool size of the average pooling layer is set at $p1 = 2$ which is a standard choice in most convolutional neural networks networks. The feature extraction layer is stacked a single time for both signal protocols, $n_{stacks} = 1$, any deeper network resulted in worse performance in terms of validation accuracy as can be seen in figure 2. The activation function in the convolutional layers is the complex cartesian ReLu.

The output of the feature extraction stack is flattened before moving through the hidden layers. The number of hidden layers in the classification part of the network is reduced to a single layer. Again, here the validation performance did not seem to be influenced by the amounts of hidden layers, this can be seen in figures 3. So $n_{hidden} = 1$. The activation function used in the neurons is again the

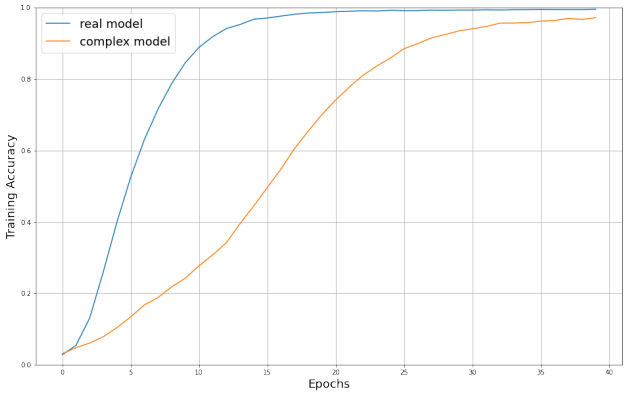
complex cartesian ReLu function. The amount of neurons in the hidden layers is set at $n1 = 256$. This leads to the parameters of the network shown in table IV of the paper.



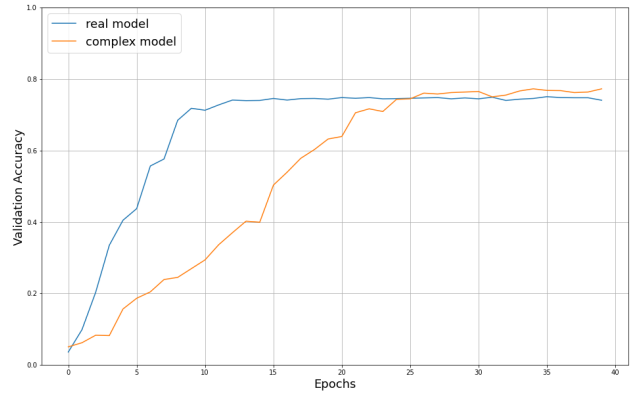
(a) ADS-B Training



(b) ADS-B Validation

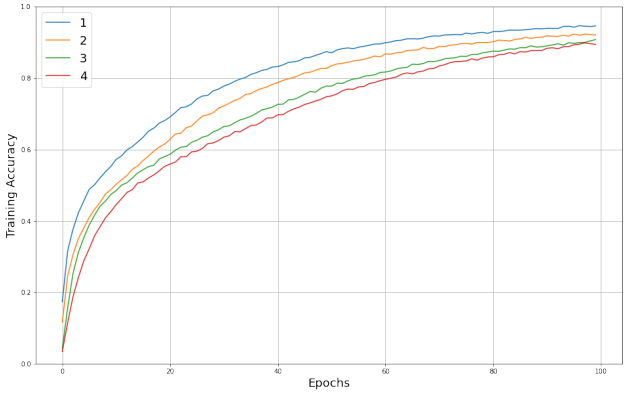


(c) VDL2 Training

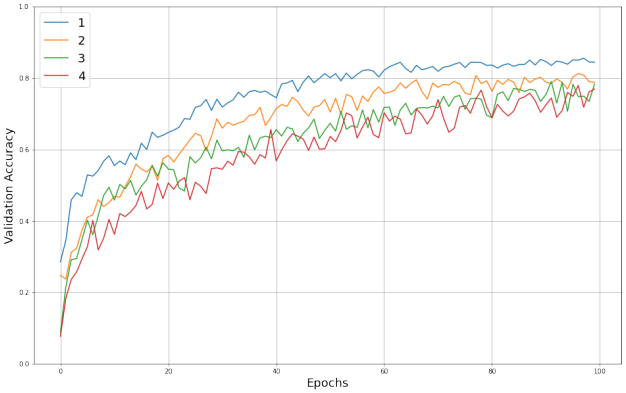


(d) VDL2 Validation

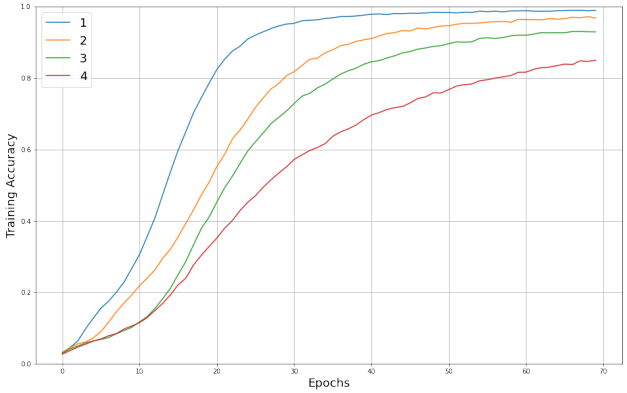
Figure 1: Comparison of accuracy Complex vs. Real CNN



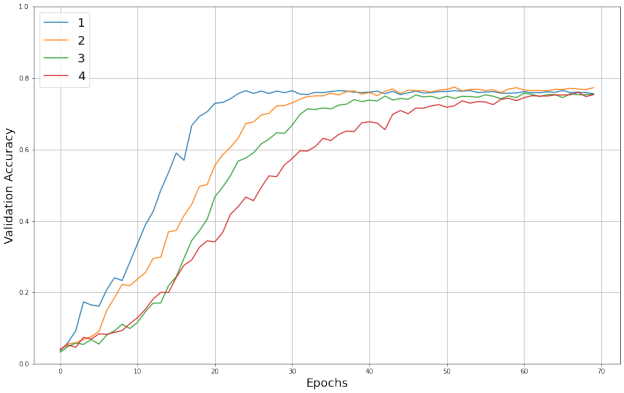
(a) ADS-B Training



(b) ADS-B Validation

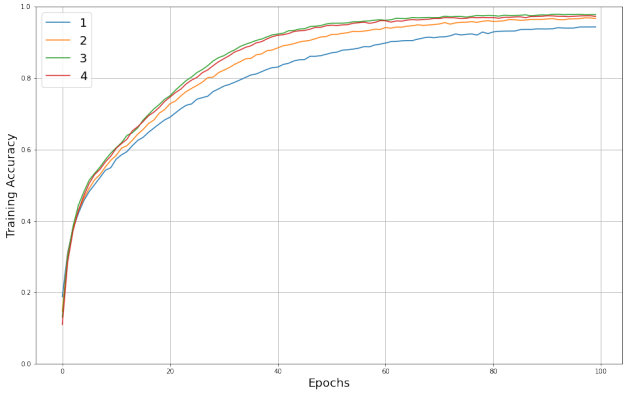


(c) VDL2 Training

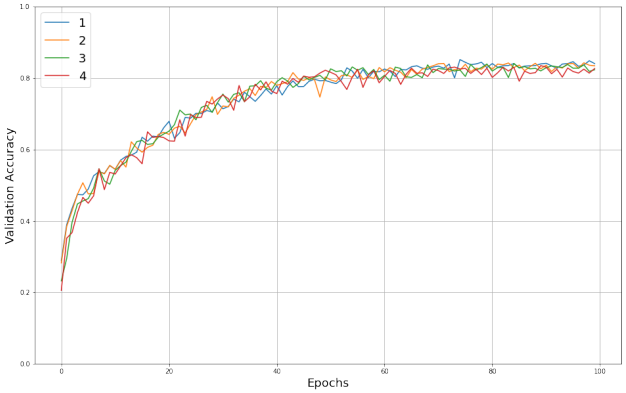


(d) VDL2 Validation

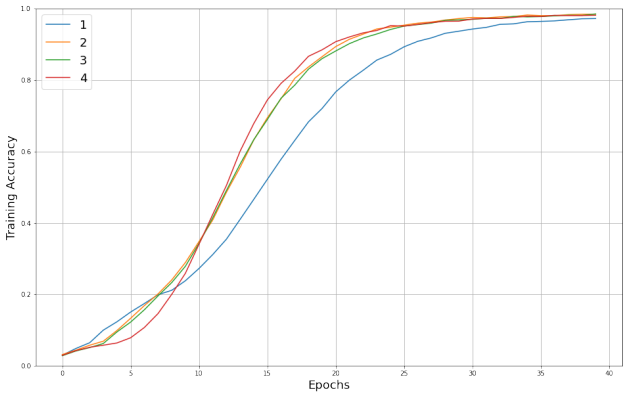
Figure 2: Comparison of training and validating different amounts of feature extraction stacks: $n_{stacks} = [1, 2, 3, 4]$.



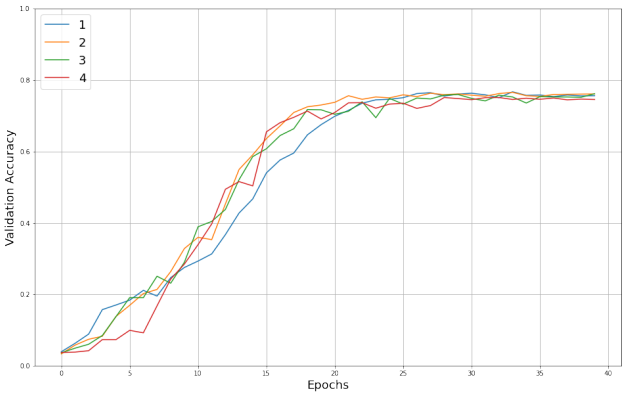
(a) ADS-B Training



(b) ADS-B Validation



(c) VDL2 Training



(d) VDL2 Validation

Figure 3: Comparison of training and validating for different amounts of hidden fully connected layers in the the complex-CNN: $n_{layers} = [1, 2, 3, 4]$

Part II

Preliminary Thesis Report (Graded)

Summary

Due to modernisation programs in air traffic management, some relatively new surveillance and communication protocols have been adopted: ADS-B surveillance and VHF data link communications (VDL2). Both technologies aim to increase safety in ATM, and are designed as open protocols. This has many advantages but can lead to vulnerabilities in terms of cyber-security. A method to increase integrity in the mentioned wireless surveillance and communication technologies while retaining the openness, can be radio frequency fingerprinting for physical layer identification. A way to uniquely identify transmitting devices is to distill the device its radio frequency (RF) fingerprint by looking at the physical features of the message signal it transmits. This physical layer fingerprint is the unique trace the transmitter leaves in the signal it sends. This thesis proposes a method to RF fingerprint ADS-B and VDL2 messages to identify aircraft using a convolutional neural network model (CNN). Initial results show the model is able to identify aircraft based on raw message IQ data as input, but more research is needed to determine if this model could be used to provide a robust identification for multiple aircraft. This report starts with an introduction of the research questions and objective. This is followed by a detailed background in chapters 2-4 of the technical aspects of ADS-B and VDL2 including some security issues highlighted in previous research. Furthermore, the paradigm of RF fingerprinting and machine learning for RF fingerprinting will be explained. In chapter 5 the methodology is discussed. Here the CNN model used for RF fingerprinting is introduced and six experiments to test the robustness and performance of the model explained. The six experiments consist first of the effect of model parameters, secondly of the model performance for different aircraft population sizes, the effect of training and testing on different days, the effect of noise on the samples, the effect of hardware similarities and lastly the robustness of the model to message injections. This preliminary report discusses the results of experiments one to two in chapter 6. The initial results show that the model is capable of identifying aircraft using raw IQ message data as an input, furthermore the results of experiments two show the model is scalable with increasing population size but an increase in different aircraft in the data set slightly reduces the accuracy of aircraft identification. The next steps are to conduct the experiments 3-6. These will show if the model is capable of a robust RF fingerprinting for ADS-B and VDL2 messages to identify aircraft.

Contents

List of Figures

List of Tables

List of Acronyms

ADS Automatic Dependant Surveillance . . . 1
ACARS Aircraft Communication Adressing and Reporting System . . . 17
VHF Very High Frequency . . . 2
ATC Air Traffic Control . . . 8
AOC Air Operation Control . . . 2
ADS-B Automatic Dependent Surveillance - Broadcast . . . 1
NextGen Next Generation Air Transportation System . . . 2
GNSS Global Navigation Satellite System . . . 2
UAT Universal Access Transceiver . . . 7
EASA European Aviation Safety Agency . . . 1
SSR Secondary Surveillance Radar . . . 2
PSR Primary Surveillance Radar . . . 2
ACAS Airborne Collision Avoidance System . . . 8
SDR Software Defined Radio . . . 9
ATM Air Traffic Management . . . 9
PPM Pulse Position Modulation . . . 7
CRC Cyclic Redundancy Check . . . 8
NBAA National Business Aviation Association . . . 10
PIA Privacy ICAO Address . . . 10
FAA Federal Aviation Administration . . . 1
ICAO International Civil Aviation Organisation . . . 2
NGOs Non-Governmental organizations . . . 10
FPE Format Preserving Encryption . . . 12
PKI Public-Key Infrastructure . . . 12
RF Radio Frequency . . . 1
CA Certificate-Authority . . . 12
MAC Media Access Control . . . 12
DSSS Direct Sequence Spread Spectrum . . . 13
FHSS Frequency-Hopping Spread Spectrum . . . 13
PSN Pseudo Random Noise . . . 13
VFR Visual Flight Rules . . . 5
AOC Airline Operations Control . . . 2
VDL VHF Data Link . . . 1
FANS Future Air Navigation System . . . 18
RFF Radio Frequency Fingerprint . . . 22
PSD Power Spectral Density . . . 23
MLP Multi-layer Perceptron . . . 31
1090ES 1090 Extended Squitter . . . 7
CPDLC Controller Pilot Data Link Communications
SESAR Single European Sky ATM research . . . 1

1 Introduction

The air traffic management infrastructures in parts of the world are currently reaching their limits of capacity due to ever increasing congestion. Furthermore, the aviation industry will have to increase sustainability and reduce its environmental impact dramatically in the coming decades. These are some of the major challenges for aviation and to tackle this, modernisation programs are being implemented to increase capacity and efficiency such as the Federal Aviation Administration (FAA) its NextGen program and the European Aviation Safety Agency (EASA) its Single European Sky ATM research (SESAR). These projects will implement an increase in digitisation, automation and connectivity in air traffic management. The aviation industry will cross over into the digital realm.

Under these modernization programs, some new concepts have already been implemented, for example CPDLC which represents a shift in terms of air traffic control communications from voice based radio communication to digital communications and data links. For surveillance there will be a shift towards Automatic Dependant Surveillance (ADS) which means that aircraft provide surveillance data using satellite data such as GPS without the need for radar [69]. A technology which enables one of these concepts is Automatic Dependent Surveillance - Broadcast (ADS-B), which is a surveillance protocol that tries to increase safety by providing an extra means of surveillance by transmitting position information automatically between aircraft and ground stations [95]. Another technology is VHF Data Link (VDL) 2 a communications protocol which is the physical layer that enables CPDLC over VHF radio [15].

But this increase in digitization means the industry faces numerous challenges in cyber-security [22]. For example, the relatively new ADS-B technology which is one of the cornerstones for both modernisation programs, was developed as an open protocol [95]. The same holds for VDL2 [15]. This has many advantages, such as ease of implementation, low cost and provides the research community with invaluable data. The openness must be preserved, but it comes with a cost of vulnerability to cyber-attacks. One of the reasons of this is because, the messages in both ADS-B and VDL2 are identified or authenticated by an address which is transmitted in the message. This is the unique 24-bit ICAO code sent out by ADS-B transponders and VDL2 radios. These addresses are used to uniquely identify the transmitting aircraft. The problem is however that these addresses can be spoofed such that an attacker is able to impersonate a device. The possibility to spoof wireless transmitting devices and to impersonate or inject messages has obvious implications for the integrity of the wireless protocol. A way to uniquely identify a transmitting device by the receiver is to identify the device by its physical layer fingerprint [91]. This physical layer fingerprint, also called Radio Frequency (RF) fingerprint or (RF-fingerprint) is the unique trace the transmitter leaves in the signal it sends. This RF fingerprint could be used as an extra layer of identification, which can possibly make both protocols more secure while retaining the openness of the protocols.

Already, it has been shown that RF fingerprinting could also be used to identify and distinguish between different aircraft ADS-B signals, without relying on the ICAO 24-bit address present in the message. With most of the methods researched using some form of deep learning. VDL2 could also be

eligible for RF fingerprinting to identify aircraft. Therefore, the goal of this thesis research is to investigate whether the VDL2 signals could be used to identify aircraft through RF fingerprinting by using deep learning methods. Furthermore it will be investigated if the combination of both ADS-B and VDL2 can be used in a mixed input deep learning model such that both signals can be utilised to identify aircraft.

This preliminary thesis will first discuss the technical aspects and research on the security for ADS-B and VDL2 in chapter 2. It will afterwards discuss the background of RF fingerprinting and introduce some machine learning concepts in chapters 3 and 4. Chapters 2-4 will consist of the background and the research foundation for this thesis. Chapter 5 will discuss the research method used and Chapter 6 the preliminary results. In the last chapter some initial conclusions are drawn.

1.1. Summary of Background

The increase in air traffic over the last decades has led authorities to develop future proof air traffic management systems. Examples of such initiatives are the implementation of the modernisation of U.S. airspace: Next Generation Air Transportation System (NextGen), and its European counterpart: the Single European Sky. One of the cornerstones of both modernisation programs is the development and implementation of ADS-B. Compared to legacy radar surveillance methods such as the Primary Surveillance Radar (PSR) and Secondary Surveillance Radar (SSR), that determine the aircraft position using ground-based radar stations, the ADS-B system obtains positioning information from the Global Navigation Satellite System (GNSS). This shift from ground based localisation or independent to onboard localisation or dependant surveillance is intended to reduce the high costs of air traffic surveillance. ADS-B is cheaper and less maintenance intensive compared to both primary and secondary radar equipment. It also aims to increase the situational awareness for air traffic management and increase the safety of the entire air traffic system [85],[95].

Currently, the primary means of communication in aviation is the Very High Frequency (VHF)-radio voice communication. VHF-radio voice communication is an analog AM form of radio communication which enables aircraft to communicate by voice with among others, air traffic control and other air traffic. The VHF voice communications demand a high cognitive workload from the pilots and air traffic controllers. To further meet the increase in aviation traffic and volume, a transition is needed from the voice-only communication to a long term solution utilising data communications [48]. This has lead to the development of data links between aircraft and ground stations. The first form of data link communications in aviation was implemented with the ACARS. ACARS was implemented in the late 1970s to accommodate communications between the Airline Operations Control (AOC) and aircraft. The ACARS system is a data-link between the aircraft and ground stations which makes it possible to send text data over VHF. ACARS is mostly used by the airlines operation control but in the last two decades the system was extended to be used by ATC [48]. To further improve, modernize and promote the usage of controller/pilot data links the International Civil Aviation Organisation (ICAO) recommended new standards. This has lead to the development of the Future Air Navigation System (FANS). FANS is a system which enables CPDLC over either VHF, HF or Satcom. Both Boeing (FANS-1) and Airbus (FANS-A) developed implementations of the system, therefore FANS is usually referred to as FANS-1/A. To improve the capability of CPDLC over the earlier ACARS implementation, new VHF datalink schemes have been implemented such as VDL2 which provides some advantages over ACARS such as a higher bit-rate [15].

Both modern improvements in communications and surveillance, CPDLC with VDL2 and ADS-B were designed as open protocols which has many advantages in terms of ease of implementation, data for research or investigative journalism. But this openness introduces some shortcomings in terms of security. This can lead to possible dangerous situations in air traffic management and has been a subject of previous research, with many authors stressing the need for more security in ADS-B [47, 111, 95, 84], as well as in ACARS and CPDLC [87, 88, 15, 28]. Multiple security measures have been proposed for ADS-B such as: encryption algorithms, spread spectrum technologies or data verification techniques. Each security solution has its positive and negative sides but not one security solution is suitable to provide full security [95]. Furthermore, it is highly debatable whether the openness of ADS-B should

be compromised. The open nature of ADS-B has many advantages and is an essential component of ADS-B [40]. This thesis will focus on a security measure for ADS-B and VDL2 which preserves the openness, radio frequency fingerprinting. RF fingerprinting has already been demonstrated to be able to identify ADS-B transmitters for aircraft identification without needing a change in signal protocol or transmitter devices. Besides this it will be investigated if RF fingerprinting is possible for VDL2 messages.

Physical layer identification or radio frequency fingerprinting is providing the identity of transmitting devices through the physical signal characteristics of the messages [91]. The RF fingerprint of the signals transmitter is based upon imperfections of the hardware. Examples of these transmitter imperfections are due to the analog elements of the device which can be extracted as features to produce fingerprints. Some examples of the elements which can be features for fingerprints are [91]: Phase noise, digital to analog converters, band pass filters, frequency mixers and power amplifiers.

Many research has been done on RF fingerprinting, and it could be used to provide an extra physical layer identification for many different devices [91]. This research will focus on RF fingerprinting for aircraft signals, ADS-B and VDL2 to identify aircraft. Currently there has been lots of research on the fingerprinting of ADS-B signals such as: [55, 92, 113, 46, 116]. There is a great difference in the types of methods used. Even for a single signal type. However, most fingerprinting methods have the commonality that they employ some deep learning method such as convolutional neural networks,recurrent neural networks or denoising autencoders. Most papers have common parameters which should be evaluated to determine the performance and robustness of the radio frequency fingerprinting. Namely: classification accuracy, the size of the data set or number of devices, the number of samples per device, sampling rate of the signal receiver, features considered, deep learning method and signal to noise ratio.

Aircraft transmitter identification using radio frequency fingerprinting based on ADS-B signals has already been shown to be possible. However, there has been little focus on other signals aircraft emit, such as VDL2. To the best of the authors knowledge, there is no research on the fingerprinting of the VDL2 protocol to provide aircraft identification or on how both VHF signals such as VDL2 fingerprinting can be combined with ADS-B signal fingerprinting to provide aircraft identification. Radio frequency fingerprinting has however been done with signals comparable to VDL2, such as [117] which used DQPSK modulated signals as radio frequency fingerprints. A form of PSK (D8PSK) is the modulation scheme of VDL2 signals. It is thus to be expected that fingerprinting VDL2 signals is a feasible undertaking. Therefore this thesis proposes to investigate radio frequency fingerprinting of VDL2 signals for aircraft identification, and to see if the combination of ADS-B and VDL2 can provide an accurate aircraft identification based on radio frequency fingerprinting.

1.2. Research Objectives

1.2.1. Research Questions

The main topic of research is divided into one main question and five sub-questions. The questions are formulated as:

- Q1 Can the paradigm of radio frequency fingerprinting be used to identify aircraft based on ADS-B and VDL2 signals to provide an accurate aircraft identification?
  - SQ1 Which deep learning algorithm can be effectively applied to achieve an accurate radio frequency fingerprint from ADS-B and VDL2 signals to identify the aircraft transmitting this signal?
  - SQ2 What is the effect of noise on the accuracy of the extracted the radio frequency fingerprints?
  - SQ3 What is the effect of hardware similarity on the accuracy of the extracted the radio frequency fingerprints?
  - SQ4 Is the RF fingerprinting model able to reject message injections from previously unidentified transmitters?
  - SQ5 Is the model usable over multiple days?

1.2.2. Research Objective

The main research objective of this thesis is:

> *"To develop a method to radio frequency fingerprint aircraft ADS-B and VDL2 signals to identify an aircraft, by using radio frequency fingerprinting methods which employ deep learning."*

The research objective can be divided into multiple specific sub-goals. The first one being the goal to fingerprint aircraft based on ADS-B and VDL2 signals by using deep learning. This can be subdivided in to firstly determine which signal features are suitable to provide a fingerprint and secondly to select a deep learning algorithm which is able to achieve a high accuracy fingerprinting. Furthermore the goal is to investigate if the model focuses on the correct features and investigate the robustness of the fingerprints to noise and on the accuracy of the fingerprints. Besides investigating fingerprinting for the ADS-B & VDL2 signals, another goal is to identify aircraft by combining the VDL2 fingerprints with that of ADS-B signal fingerprints, to see if the combination of both provides a more accurate aircraft identification.

2

Aviation Communications and Surveillance

Before the 1930s, aviation air traffic control was still in its infancy. There was no need for a large air traffic control system because most aircraft flew only during daytime and in good weather under Visual Flight Rules (VFR). With the increasing growth of aviation, the first forms of air traffic control in terms of communication were the use of light signals. This had the drawback that pilots had no way of responding to signals coming from the early air traffic controllers and a new two-way system of communication had to be adopted. This was solved with the implementation of radio communication. The outbreak of world war two had a profound impact on aviation, with numerous adaptations of new technologies such as radar and transponders. These early forms of surveillance technologies were implemented in the years following the war, which saw an immense growth in aviation and air traffic. Radio communication and radar surveillance are at present still the primary sources of information and data for air traffic control. But due to ever increasing congestion, airspace modernisation programs are currently being implemented such as the FAA its NextGen program and the EASA its Single European Sky. These programs will implement a shift in terms of communication from voice based radio communication to digital communications and data links. In terms of surveillance there will be a shift towards automatic dependant surveillance which means that aircraft will provide surveillance data using satellite data such as GPS without the need for radar. [69].

These paradigm shifts to the digital realm hold some new challenges in terms of cyber-security. This chapter will discuss the newly implemented technologies in aviation communications and surveillance and their security implications. It will furthermore discuss the dilemma of openness and security and some proposed mitigation measures to increase security.

2.1. Surveillance

Aircraft surveillance initially relied fully on the PSR [101]. The primary surveillance radar is a rotating radio transmitter which consecutively transmits a radio signal and listens to the reflections to determine the slant-range of an aircraft. This is done by measuring the time difference between transmitting and receiving the signal. The aircraft azimuth angle is determined by the rotation angle of the radar. Because the primary radar alone does not give enough information to for example, determine aircraft elevation, the secondary radar was introduced. The secondary radar is used to interrogate aircraft transponders by sending out interrogation messages on the 1030 [Mhz] frequency band and listens for replies on the 1090 [Mhz] frequency band replied by an aircraft transponder [101]. The latest type of aircraft transponder is the mode S transponder, mode S (Mode Select Beacon System) can be selectively interrogated, which means that the SSR can interrogate different types of information such as altitude, identification and velocity from different aircraft [101].

2.1.1. ADS-B

The increase in air traffic over the last decades has led authorities to develop future proof air traffic management systems. Examples of such initiatives are the implementation of the modernisation of U.S. airspace: NextGen, and its European counterpart: the Single European Sky. One of the main technological implementations of both modernisation programs is the development of ADS-B. Compared to legacy radar surveillance methods such as the before mentioned primary PSR and secondary surveillance radar SSR, that determine the aircraft position using ground-based radar stations, the ADS-B system obtains positioning information from the GNSS . This shift from ground based localisation or independent to on board localisation or dependant surveillance is intended to reduce the high costs of air traffic surveillance. ADS-B is cheaper and less maintenance intensive compared to both primary and secondary radar equipment. It also aims to increase the situational awareness for air traffic management and the safety of the entire air traffic system [85][95]. From the acronym a lot can be distilled about the technical functionality of the ADS-B system:

- *Automatic*: The ADS-B system automatically sends its data without the need for interrogation.
- *Dependant*: ADS-B surveillance data is collected by on-board systems of an aircraft using for example GNSS.
- *Surveillance*: ADS-B provides air traffic surveillance data. For example 3D-position, velocity and identification.
- *Broadcast*: The ADS-B protocol depends on broadcasting its surveillance data, such that every receiver in range of the signal can receive and analyse messages.

As of 2020 the ADS-B out capability is mandated to be available on most commercial passenger aircraft in European airspace [26].

2.1.2. ADS-B Overview

The ADS-B out system periodically transmits the aircraft position, velocity and other data such as the altitude and identifier. As mentioned ADS-B is automated, which means that no pilot or air traffic controller has to trigger the broadcast of information or no interrogation is needed to transmit information. Aircraft equipped with ADS-B out periodically and automatically transmit messages to ATC and other aircraft equipped with ADS-B in. Two different competing types of the ADS-B protocol exist, the Universal Access Transceiver (UAT) and the 1090 Extended Squitter (1090ES). The UAT protocol utilizes the 978 MHz frequency, and because it requires fitting new hardware and is only being used in some countries such as the USA, mostly by general aviation [101]. The (1090ES) protocol utilises the mode S transponder. The mode-S transponder can transmit both 56-bit and 112-bit messages. This thesis will only focus on 1090ES ADS-B. The 1090ES ADS-B format utilises the 112-bit mode-S message format to automatically transmit aircraft data without the need for selective interrogation [96]. An overview of the entire surveillance system is shown in figure 2.1. As can be seen, the positional data of the aircraft is transmitted over the ADS-B data link to both other aircraft and ground stations.

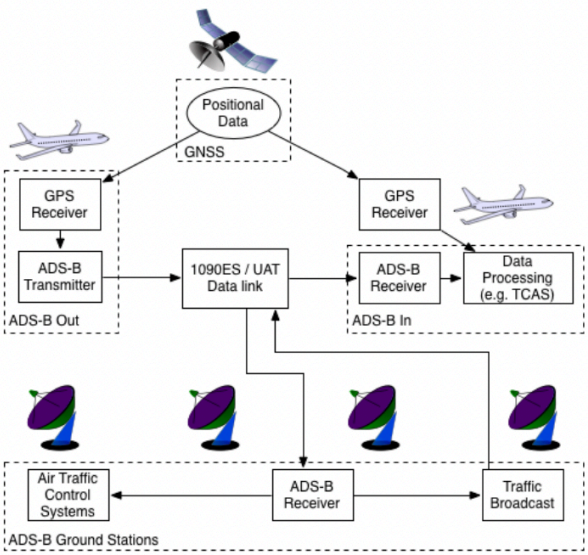


Figure 2.1: ADS-B surveillance system overview as reprinted from [94]

2.1.3. 1090ES Message Format

The 1090ES Mode-S/ADS-B message comprises of a preamble which is followed by a 112-bit message. This message contains the ADS-B frame information shown in 2.1, including the 24-bit ICAO-address code used as an aircraft identifier. The message format is shown in figure 2.2. The ads-b downlink packet is amplitude modulated using Pulse Position Modulation (PPM). Shown in figure 2.2, this form of modulation represents a 1 bit using a $0.5\mu s$ pulse followed by a $0.5\mu s$ pause, and the opposite is true for a 0 bit. This signal is modulated on the 1090MHz carrier wave for transmission [18]. The ADS-B message frame is shown in table 2.1.

Bit	Number of Bits	Abbreviation	Information
1-5	5	DF	Downlink Format
6-8	3	CA	Transponder Capability
9-32	24	ICAO	ICAO Aircraft Address
33-88 (33-37)	56 (5)	ME (TC)	Message, extended squitter (Type Code)
89-112	24	PI	Parity/Interrogator ID

Table 2.1: ADS-B message data frame as adopted from [101]

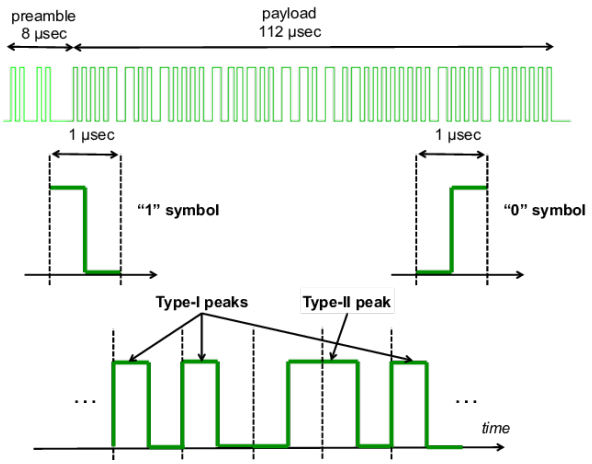


Figure 2.2: ADS-B packet format reprinted from [18]

The first five bits correspond to the message down-link format, the number 17 indicates the receiver that the message is an ADS-B extended squitter message [101]. The next sequence is the transponder capability, which indicate the transponder level. The 24-bit aircraft ICAO address indicates a unique identifier for the transmitting aircraft which will be discussed further in section 2.1.4. Bits 33-88 contain the message data, the first five bits (33-37) contain the type code which indicate what kind of information is transmitted in the message, possible message types include: airborne position, surface position, airborne velocities and aircraft status [101]. The last 24 bits are reserved for the CRC-remainder which is used to check if messages were corrupted during transmission [101]. Cyclic Redundancy Check (CRC) is an authentication method which uses in the case of ADS-B, a 24-bit number together with a predefined division number to calculate the remainder of a message. The message sender calculates the 24-bit remainder such that the entire 112-bit message remainder with the division number is equal to zero. The message receiver checks upon receiving if the message has attained errors during transmitting by calculating the remainder. If the remainder is not zero, some bits have been lost or adjusted. The CRC can also correct up to 5 bit errors in the received message [101].

2.1.4. ICAO-Address

Aircraft Mode-S and ADS-B messages can be identified by their ICAO aircraft address. The ICAO-address is a unique 24-bit code which is assigned to each aircraft when equipped with a mode S transponder. All ADS-B and mode S messages contain the transmitters unique 24-bit ICAO code. The EASA have expressed concerns that there is a large number of aircraft in European airspace with the wrong setting of the ICAO-24 bit address. According to [27] this can lead to possible hazardous situations when two aircraft with the same ICAO 24-bit address are in the range of a single mode-S interrogator. This can lead to aircraft being ignored from Air Traffic Control (ATC) displays, creates the possibility of misidentification and it could potentially degrade the performance or even disable the Airborne Collision Avoidance System (ACAS) (II) system [27].

2.2. ADS-B Security Implications

With the before mentioned shift from an independent to a dependant form of Air Traffic Management (ATM) and the introduction and roll out of ADS-B, arise some security implications. Since ADS-B was not designed with security as a main focus point, it can be attacked using easy to obtain hardware and software [95]. An example of this is the development of the Software Defined Radio (SDR). SDRs make it very easy for everyone to transmit or receive RF transmissions at a very low cost. This makes the non-encrypted ADS-B protocol vulnerable for attacks [111]. Furthermore, a number of attacks on the ADS-B system have already been demonstrated by research, for example [84] which demonstrated among others, the successful injection of a ghost ('fake') aircraft into the ADS-B system using a SDR. The vulnerability and ease in which the ADS-B system can be attacked, call for a need to mitigate these security issues. A number of security threats and requirements have been identified by [59, 95, 111, 60, 63]:

2.2.1. Eavesdropping

Message interception or eavesdropping is the collection of signals with malicious intent. ADS-B is an un-encrypted protocol which means that signals are sent out using plain text, such that everyone with an ADS-B receiver can read these signals. According to [111] this could be used to achieve "complex-attacks", although no concrete examples are given. Collecting ADS-B data is mostly done by non-hostile actors, which visualize ADS-B data, such as `planefinder.net`. Eavesdropping can lead to privacy implications which will be discussed in section 2.3.

2.2.2. Message Injection

The before mentioned lack of a secure authentication protocol in the ADS-B system makes it possible for attackers to construct and inject fake messages into the system. Because the ADS-B message sends its own 3D location information, the ADS-B receiver can not authenticate if the location of the received message is the actual location of the ADS-B transmitting device. Therefore, Constructing and injecting an entire ADS-B message will appear to be an aircraft which does not actually exist ('ghost aircraft'). A legitimate ADS-B receiver can not distinguish real from a fake messages and whether the location sent out by this message is the actual location of the sender [95]. [84] has demonstrated the systems vulnerability to these types of attacks by injecting messages which represent a ghost aircraft. Injecting false ADS-B messages could lead to confusing and potentially dangerous situations. Such as unnecessary go-arounds, diversions and ACAS systems could give false warnings. This leads to a higher workload and increased situational complexity for pilots an air traffic control, which could lead to dangerous situations [84]. Injecting multiple ghost aircraft could have an overwhelming effect on the surveillance system [60]. [84] proved this could be possible by injecting 100 ghost aircraft that appeared at random locations, this lead to a total loss in situational awareness and system failures.

2.2.3. Message Deletion

Deleting of legitimate ADS-B messages sent out by aircraft can be a potential security hazard. An attacker can interfere with the sent out messages by aircraft. A strategy could be implemented to cause a high amount of bit errors in the message. The CRC discussed in section 2.1.3, can correct up to 5-bit errors, any higher number of errors and the message will be considered invalid and neglected [95], this is called "Constructive Interference" [63]. Another method could be to transmit the inverse of message also known as "Destructive Interference" [63]. This however, is very complex in terms of timing and precision. This type of attack can thus be very challenging [95, 111]. A concrete attack scenario utilising message deletion is posed by [84] is total aircraft disappearance by deleting all ADS-B messages from an aircraft. This will suspend the functionality of collision avoidance systems utilising ADS-B, which can lead to dangerous situations [84].

2.2.4. Message Modification

Modifying an ADS-B message can be done using multiple methods, [95] gives two different approaches, namely: overshadowing and bit-flipping. Overshadowing is the transmission of a high powered signal to modify or replace parts of the message being transmitted by the legitimate transmitter. Bit flipping can be done by inverting bits of the message, such that information is changed. [84] demonstrated a message modification attack utilising the overshadowing approach. The trajectory of an aircraft was

modified by sending modified position updates. If ADS-B is the only data-source ADS-B data modification is hard to recognize [84].

2.2.5. Jamming

Jamming the entire Mode-S/ADS-B service can be another possible security hazard. Jamming ADS-B and Mode S can be done by sending a high powered signal over the same frequency that utilises ADS-B and Mode S: 1090Mhz. [60], gives two feasible forms of jamming the ADS-B system. Ground station flood-denial, in which a simple jamming signal is sent out in range of an ADS-B ground station. This will block all ADS-B signals to the ground station. Materials to do this are readily available at low-cost [60]. Another method could be aircraft flood denial. This method is similar to the one ground station flood denial mentioned above only here the aircraft in and outgoing messages are being denied. Depending on the altitude and location of the aircraft, this requires high powered jamming equipment, but is still feasible [60]. Jamming is a common vulnerability in almost all wireless networks, but due to the air traffic managements inherent large uncontrollable open spaces coupled with its critical nature of the system, jamming parts of the system can have a severe impact [95].

2.3. Privacy & Openness Implications

As mentioned before, the open nature of ADS-B makes it possible for anyone with an ADS-B ground station to receive and read ADS-B messages. ADS-B messages contain the airplanes unique ICAO 24-bit address and combining this with aircraft ownership data in publicly available aircraft registries, targeted tracking can be possible. Since flight plans are openly available, this is usually not a concern for commercial flights but it can have an impact on military or privately owned/company aircraft [62]. Aircraft tracking can be done by different types of interested parties, such as: Hobbyists, journalists, planespotters, the military, business and criminals [100]. An Examples of flight tracking by investigative journalism are highlighting the personal movements of company executives by private or company owned aircraft [100]. Collecting ADS-B data can also be used for more complex privacy infringements, which can provide valuable business information or information about governments and upcoming world events. This is demonstrated by [100] where ADS-B data from state or business owned aircraft can be used to detect government events and even predict mergers and acquisitions of companies.

Due to these privacy issues, the U.S. National Business Aviation Association (NBAA) and the general aviation community have expressed concerns regarding their privacy and indicated it as a barrier to equip ADS-B out systems [29]. Therefore, the FAA implemented the Privacy ICAO Address (PIA) which is a separate ICAO 24-bit address not linked to the U.S. domestic aircraft registry such that aircraft supposedly can not be tracked under the program in U.S. Airspace [29]. [62] showed that the PIA program does not fulfill the privacy requirements because flight tracking can still be done using different data-sources. Furthermore, it concludes that the achievable privacy performance of the PIA program will be weak [62]. Privacy will be very difficult to achieve without full encryption, such that new message types or new protocols would need to be developed and implemented [95]. More mitigating factors which could potentially improve on the privacy concerns are discussed in section 2.4.

On the other hand, a very large case can be made for the openness of ADS-B, mainly because the openness of ADS-B is one of the most essential components of the successful implementation and use of the system [40]. Due to the potential cost impact of implementing a completely new air traffic surveillance system, the 1090ES ADS-B system was designed around already present hardware available in most aircraft: the Mode S transponder. This has lead to a relatively cheap and quick adaptation of ADS-B in the entire aviation industry. For example, the implementation of 1090ES is considerably cheaper than that of the UAT ADS-B protocol mentioned in 2.1.2, which requires different hardware. The open nature of the protocol also provides the research community with an easy way of collecting data. An example of this is Opensky, which is an initiative that crowdsources ADS-B data which is made available for research groups [97]. This data is being used for effective research in numerous different fields with about 150 academic papers as of 2021 [90]. A recent example of the use of open ads-b data in research is investigating the change of mobility patterns in Europe due to the Covid-19 pandemic [42]. Besides the scientific advantages of crowdsourced openness in ADS-B data, it can have a positive societal impact as well. With numerous non-profits, Non-Governmental organizations (NGOs) and

journalists using the Opensky database for different purposes [93]. The broader social impact of open ADS-B data or the Opensky project can be seen in various areas [93]:

- Investigative Journalism: As mentioned before, this group focuses mostly on highlighting the movements of high profile individuals and political leaders.
- Data Journalism: ADS-B data is being used by journalists to visualise movements of aircraft to the general public or individuals without a deep knowledge of aviation. Furthermore it can highlight surveillance activities by governments, An example of this is the article about U.S. government surveillance ahead of the presidents inauguration in 2021, [82].
- (Supra)National Analysis: ADS-B data can be used for economical analysis, during the Covid-19 crisis ADS-B data was for example used to provide an overview of the economic impact of travel restrictions on aviation [41].
- Local Activism: ADS-B data can also provide information about local problems or concerns in aviation, such as noise complaints within proximity to airports.
- Recreational Use: The data is lastly being used for recreational purposes, such as the numerous websites which provide live ads-b data e.g. `https://www.flightradar24.com/` and `https://flightaware.com/`. Moreover, it can be used by flights simulators such as X-Plane to provide real-life traffic.

2.4. Securing the Protocol

Due to the apparent need for more security in ADS-B, a number of countermeasures or security protocols against the types of attacks discussed in section 2.2 have been proposed. When discussing security, a model which is often used as a baseline for discussing different levels or concepts of security is the CIA triad model, which consists of [6]:

- *Confidentiality*: This concept refers to the ability to protect the gathering of data from unauthorized persons.
- *Integrity*: Integrity is the ability to protect data from undesirably being changed or corrupted and from an authorized source.
- *Availability*: This refers to the ability to data or service remaining accessible for authorized users.

[17] summarised how the CIA model can be used to decompose the security of ADS-B:

With confidentiality meaning that it should only be accessed by its intended entities. The privacy and openness implications discussed in section 2.3 are part of this level. Full confidentiality has a negative impact on of the openness of ADS-B and will negate its advantages, but it does improve the privacy of the users of the system. Integrity within the ADS-B protocol can be decomposed into two parts, source authentication and data verification [17]. Source authentication is ensuring that data only originates from an authorized source. Without modification from an outside entity. [17] decomposes source authentication in three parts: Authentication, Content immutability and Non-repudiation. Data verification is the process of determining if the information provided is true, for example if the location information in an ADS-B message is the actual location of the aircraft transmitting [17]. Availability is the assurance of service provided to the users of ADS-B [17]. Various security solutions relating to confidentiality, integrity and availability exist and could be applied to ADS-B. These will be briefly discussed in the next section, for a complete overview of ADS-B security solutions derived from [17] see figure 2.3.

2.4.1. Security Solutions

This section discusses proposed security paradigms, which will be decomposed into the CIA model described in the section above. As mentioned by [86]: ”All countermeasures have some value, but no countermeasure is perfect.” The same holds for the security solutions proposed for ADS-B. This can be clearly seen in figure 2.3 where there is no single protocol or security paradigm which encompasses the entire CIA security model.

Cryptography Methods

Security solutions which aim to ensure confidentiality and a form of authentication in the ads-b protocol are cryptography methods. Cryptography is a method which protects information and ensures confidentiality and or authentication, such that only the intended receiver has access to the information of the

message [25]. Three main types of cryptographic methods can be identified, symmetric, asymmetric and hash [25]. As mentioned by [109], changing ADS-B to an encrypted protocol can be problematic. First of all because ADS-B is currently an international protocol which means the encryption method must adhere to existing policies and technological limitations regarding the use of ADS-B [109]. Secondly, ADS-B is bandwidth and interference constrained. The number of aircraft that the system can support is limited by interference, increasing the message length to accommodate encryption methods will further reduce this [109]. Moreover, ADS-B operates in an ”cryptographically untrusted environment” this means that all encryption hardware, software and keys will become available for possible malicious groups [109].

Symmetric Encryption Symmetric encryption algorithms derives its name by the way keys are used and shared between sender and recipient. In symmetric encryption, a single public key is used for both encryption and decryption [31]. Multiple symmetric encryption security measures have been posed for ADS-B such as [31] who proposed a Format Preserving Encryption (FPE) method. This is an encryption method which encrypts a message without changing the data format of the message [10]. This format preserving encryption will enable the ADS-B protocol to retain message format while being presented in an encrypted format. The advantages of symmetric key encryption is that data format can be kept the same. The problems however arise with key management, if the decryption key is leaked, the encryption is compromised. As stated above, the environment in which ads-b operates is ”cryptographically untrusted”, this will make key management difficult.

Asymmetric Key Encryption Asymmetric key encryption is an encryption scheme which distributes public-private key pairs through an infrastructure called the Public-Key Infrastructure (PKI) [109]. Here every user of the protocol has its own public-private key pair coupled with their own identity. This public-private key will have to be managed by the Certificate-Authority (CA). The message sender will encrypt the message with the public key and the recipient of the message will decrypt the message using their private key [109]. The drawbacks of asymmetric encryption are that the message lengths of ADS-B will have to be increased to accommodate key ciphers. Furthermore, implementing a PKI would be expensive [111]. [109], discusses a possible asymmetric key encryption paradigm to secure ADS-B, but this needs a full key management infrastructure and requires key signatures of at least 448 bits. This is four times the length of an 1090ES ADS-B message [109]. When using asymmetric encryption, the sender needs to know the recipient before the transmission, as with the SSR. This could degrade the positive effects of the ADS-B real time location data [5].

Hashing Techniques A hash or hash function is a function which will map an input of some arbitrary length, to an output of a fixed length. A cryptographic hash function will have to be non-invertible and unique in the sense that its difficult to find two of the same outputs [73]. Some cryptographic security solutions proposed to secure are built around the use of hash functions, such as blockchain methods. A blockchain is in essence a distributed database or network which records all events that have been executed in the database network. Blockchain frameworks, consist of blocks which contain information on the state of the network. Moreover, the blocks contain data and the blocks hash value including the hash value from the previous block. The blocks are linked in a chain because it incorporates the previous blocks hash value. Each entity in the blockchain will save its own copy of the blockchain. The chain coupled with the distribution will ensure security in the blockchain database [24]. This technology could be applied to provide a solution for ADS-B security issues. With for example [76] proposing a blockchain inspired PKI framework to authenticate and secure ADS-B.

Besides the three main techniques of cryptography, multiple different paradigms exist which incorporate cryptography. Such as retroactive publication, which separately sends a Media Access Control (MAC) to authenticate the sender. An example of this is the proposed protocol by [72], which aims to ensure message authentication without changing the ADS-B protocol or hardware. Furthermore hybrid cryptography techniques can also be employed, these techniques as the name suggests combine the elements of the different types discussed above. An example of such a technique proposed by [13], the technique proposed called TESLA combines both the asymmetric, symmetric and retroactive publication paradigms to authenticate ADS-B messages.

Spread Spectrum Technologies
Technologies which aim to ensure availability and in some forms authentication in the ADS-B protocol are spread spectrum technologies. Most use cases of spread spectrum technologies in wireless networks are to mitigate eavesdropping and jamming attacks [111]. Different forms of spread spectrum technologies exist such as Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS). DSSS uses a Pseudo Random Noise (PSN) code, which divides the frequency spectrum a wireless communication protocol occupies. It than uses the PRN code to modulate the transmitted signal such that it is spread over a wider bandwidth [107]. The signal received is demodulated by the receiver using the same PRN code. Because of this, there is also the need for key management and distribution (the PRN code in DSSS) [111]. However, non-coordinated spread spectrum technologies exist. Uncoordinated Spread Spectrum (UDSSS) is such a technique which does not pre-share the PRN code, but the PRN code is chosen randomly from a set of publicly available codes [71]. Everyone with the publicly available set of PRN sequences can decode the message [71]. Although this does protects from jamming and modification attacks, spread spectrum technologies have an inherent low performance and prolonged transmission times will make the implementation difficult on a large system such as ADS-B. Besides this, authentication will only be possible by implementing a public/private key infrastructure as with some forms of cryptography [95].

Data Verification Techniques
Data verification techniques in ADS-B focus on guaranteeing the integrity of location information provided by the protocol. The techniques discussed in this section provide methods to find the location of the transmission without relying on the information provided by the sender. These methods provide protection against message modification and injection attacks discussed in section 2.2. Furthermore, they can provide a layer of redundancy when systems such as GPS or primary navigation system failures [95].

Multilateration Multilateration is a technique which uses multiple ADS-B receivers at different locations to calculate the time difference of arrival, which are used to calculate hyperboloids to derive the location of the sender. To derive the full 3D position 4 receivers at different locations will have to receive the ADS-B signal, the location of the sender has to lie at the intersection of the calculated hyperbolas from the 4 receivers [95].

Group Verification Group verification is a technique which uses the same principle of multilateration, but instead of ground receivers, groups of four aircraft will verify location information by other aircraft by using multilateration [95]. To implement group validation, the protocol has to be changed and probably new hardware has to be implemented [53].

Data Fusion Data fusion techniques try to combine information from multiple sources to verify data. In the case of ADS-B this could be to combine information from the PSR ,ADS-B and even flight plan data to verify location data of aircraft.

Distance Bounding Distance bounding is a technique in which a verifier challenges a prover to prove its distance from the verifier. The distance is determined by the time difference between the verifiers challenge and the provers response and the upper limit of signal propogation which is the speed of light. Distance bounding techniques have been proposed by [49], but require a change in the ADS-B protocol [111].

Kalman Filtering The most important set of state estimation techniques used is the Kalman filter. The basic idea behind the kalman filter is the calculation of a weighted average between the measured and a predicted state,where the weight depends on the level of uncertainty in or noise statistics of the measurement. Kalman filters have many use cases, they are for example used by airborne GPS systems to smooth noisy GPS data [53]. Kalman filters can also be used to validate ADS-B data using the state vector and ADS-B trajectory change (TC) report [53]. [53] states Kalman filters have the potential to discriminate between consistant and inconsistent ADS-B data which will provide a layer of security. But mentions that the method can still be easily spoofed [53].

Radio Frequency Fingerprinting
A technique to identify the transmitter of ADS-B messages could be RF fingerprinting. This method uses the physical layer of the ADS-B signal to verify ADS-B message sources without changing the protocol. This method does not require the implementation of cryptographic infrastructures such as the PKI discussed above. Fingerprinting can be implemented with some changes to the software of the receivers, without changing the current message format as described in section 2.1.3. Fingerprinting and its different types will be extensively discussed in chapter 3.

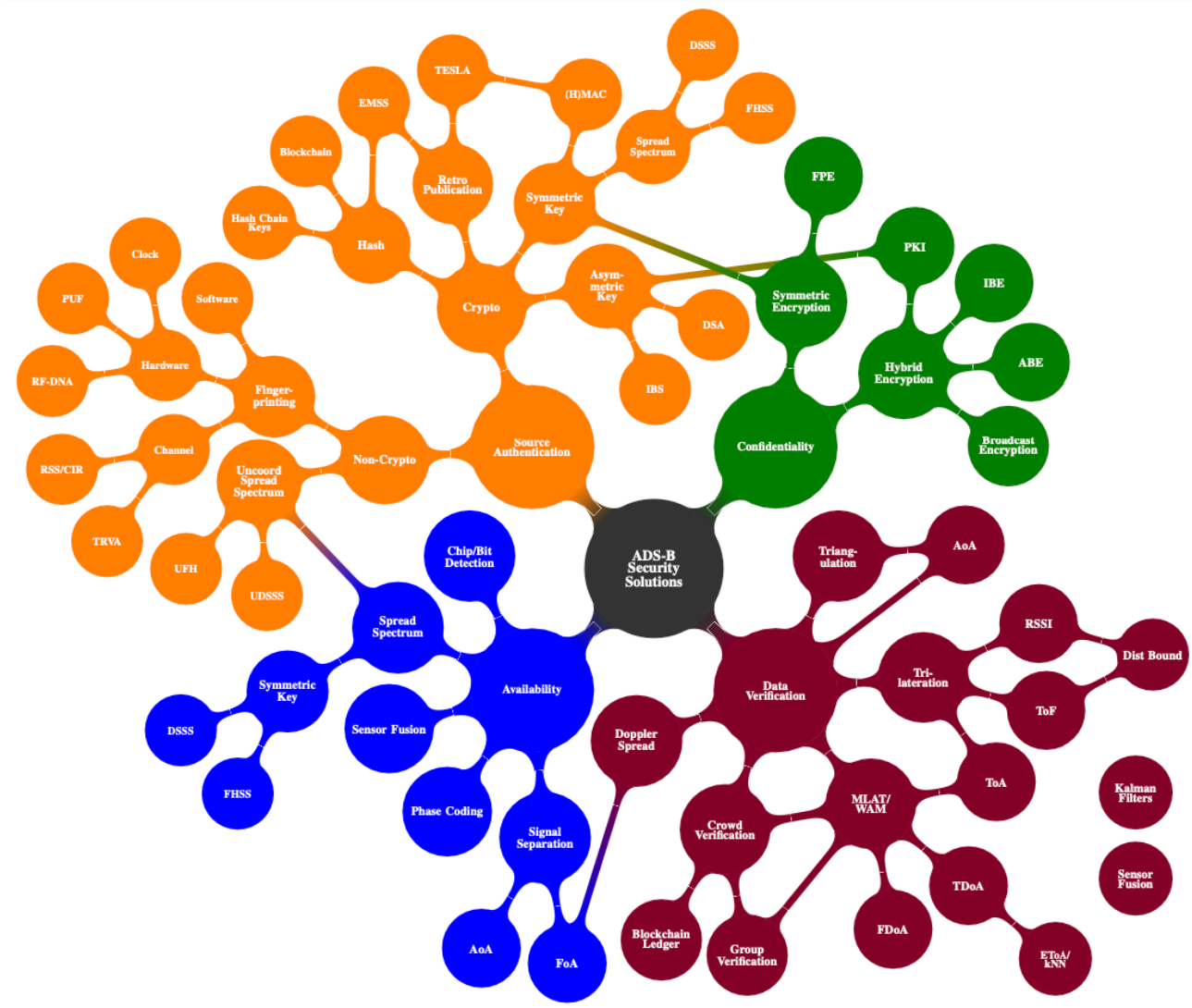


Figure 2.3: ADS-B security solutions reprinted from [17]

2.4.2. Overview

An overview of the security solutions and how they protect against the different types of attacks possible on the ADS-B system is shown in table 2.2. The security methods discussed above and how they relate to the CIA security model are shown in table 2.3. Furthermore, a large overview of most of the security protocols discussed and how they relate to the CIA model is shown in 2.3. The openness of the system is an important aspect [111], full confidentiality would mitigate the many advantages the open protocol has. Another important feature to consider is the overall cost of implementation. methods such as the cryptography and spread-spectrum methods, will need a change in communication protocol and in some instances even a change in hardware. This will make the implementation costly. As said by the [40], the implementation was done relatively quick because of the open nature of the protocol, because of this, it can be argued that an implementation requiring a large investment of money and resources by regulators and airlines will probably be difficult to implement.

As can be seen, no method will provide full security and adequate protection against all attacks. [111] proposes a multi-layer protection system which uses multiple methods to ensure security. Besides this [111] proposes that it is better to adopt a system which does not require a change in protocol, because this is easier to implement. Fingerprinting technology can be currently used to provide a secure broadcast identification layer which aims to prevent message injection, spoofing and modification attacks without a change in protocol which will retain the open nature. RF Fingerprinting to secure the ADS-B protocol will be further investigated in this thesis.

	Eavesdropping	Message: Injection/modification	Jamming/Deletion
Cryptography Methods	✓	✓	x
Spread Spectrum Technologies	✓	x	✓
Data Verification Techniques	x	✓	x
Fingerprinting	x	✓	x

Table 2.2: Attacks and security solutions derived from [95]

	Confidentiality	Integrity:Authorization	Integrity: Data	Availability
Cryptography Methods	✓	✓	✓	x
Spread Spectrum Technologies	✓	x	x	✓
Data Verification Techniques	x	x	✓	x
RF Fingerprinting	x	✓	x	x

Table 2.3: Comparison of security solutions derived from [111] and [95]

2.4.3. Openness, Privacy And Security Dilemmas

The privacy and security implications of the ADS-B system is two-sided. On the one hand there are obvious concerns and weaknesses regarding privacy and security surrounding the protocol. On the other hand, one of the key factors in the success and implementation of ADS-B is its openness. Also, as stated by [95] full security and if possible privacy would possibly require the development of new message types or new protocols. [60] highlights the dilemma that increasing security of ADS-B will reduce the functionality of the protocol, which could reduce the safety. These trade offs should be considered when implementing security solutions for ADS-B [60]. But due to the high number of security vulnerabilities in ADS-B, there is a call for the implementation of security methods in ADS-B [47, 111, 95, 23, 84]. Besides this, the likelihood of these systems being attacked by the methods mentioned in 2.2 should be considered. RF fingerprinting is a lightweight identification method, meaning that it does not require a change in protocol or a large cryptography infrastructure. Furthermore, it does not impede the advantages of the open nature of the system. Because of this, RF fingerprinting for ADS-B is investigated in this thesis.

2.5. Communication

Communication between air traffic control the air operator and aircraft is key for a safe operation. Currently almost all communication between ATC and pilots is the VHF radio voice communication [98]. More forms of message based communication include ACARS and CPDLC. This section will discuss these methods and their technical aspects and some of the security and privacy implications identified.

2.5.1. VHF-Radio Voice Communication

Currently, the primary means of communication in aviation is the VHF-radio voice communication. VHF-radio voice communication is an analog AM form of radio communication which enables aircraft to communicate by voice with among others, air traffic control and other air traffic. The VHF bandwidth reserved for aviation 118 to 137 [Mhz]. In the 1980s the bandwith was separated using a 25kHz channel which rendered about 760 channels. Each channel can be assigned to a ground station such as an air traffic control tower at an airport. The communication works on a half-duplex basis, which means that two way communication is possible, but no two stations can communicate on the same channel at the same time. This is also called ”push to talk” [48]. Most of the radio channels are assigned to air traffic control stations with the remainder assigned to AOC. The AOC uses the channels for a data service called Aircraft Communication Adressing and Reporting System (ACARS) which will be discussed in section 2.5.2. Increasing growth in aviation traffic coupled with the fixed nature of frequency spectrum allocation, has lead to a depleted spectrum. This caused the EASA to implement a new channel separation in Europe of 8,33 [KHz] instead of 25 [kHz] rendering 2280 channels [11]. The VHF voice communications demand a high cognitive workload from the pilots and air traffic controllers. To further meet the increase in aviation traffic and volume, a transition is needed from the voice-only communication to a long term solution [48].

2.5.2. ACARS

The first form of data link communications in aviation was implemented with ACARS. ACARS was implemented in the late 1970s to accommodate communications between the AOC and aircraft. The ACARS system is a data-link between the aircraft and ground stations which makes it possible to send text data over VHF. ACARS is mostly used by the airlines operation control but in the last two decades the system was extended to be used by ATC [48]. ATC uses the system to communicate with pilots to provide clearances or flight information. The advantage of text information instead of voice reduces the possibility of misinterpretation, and relieves the highly congested VHF radio communications [15]. The AOC employs the system to request maintenance information such as component, performance or flight parameter data to support their operation [120]. ACARS makes use of multiple subsystems and can also be transmitted via SATCOM and HF radio. ACARS messages are transmitted at a 2400 bps bit rate. And makes use of the Amplitude Modulation - Minimum Shift Keying [51]. ACARS has 110 different types of messages, for example: current fuel consumption, engine data, estimated time of arrival as well as free text [102]. Two different types of ACARS messages exist: uplink and downlink. The first being a ground station transmitting to an aircraft, and the other vice versa. The ACARS system has limitations such as message length constraints [48]. Therefore new improvements of the system and protocol have been developed and implemented in the form of CPDLC and ACARS over VDL2 which will be discussed in section 2.5.4.

2.5.3. CPDLC

CPDLC is text message communication with aircraft and controllers. As mentioned above the earliest form of CPDLC was over ACARS. To further improve, modernize and promote the usage of controller/pilot data links the ICAO recommended new standards. This has lead to the development of the Future Air Navigation System (FANS). FANS is a system which enables CPDLC over either VHF, HF or Satcom. Both Boeing (FANS-1) and Airbus (FANS-A) developed implementations of the system, therefore FANS is usually referred to as FANS-1/A. To improve the capability of CPDLC over the earlier ACARS implementation, new VHF datalink schemes have been implemented such as VDL-2 this provides some advantages such as higher bit-rate [15]. Furthermore, the FANS-1/A system blends with the aircraft avionics such that instructions are integrated with the aircraft its flight management system [15]. How FANS1/A compares to ACARS and how both systems are technically implemented is shown in table 2.4.

	AOC	**ATC**	**Technical Implementation**
ACARS	-Text Communication	- Text Communication - Departure Clearance - Oceanic Clearance - ATIS Information	- VHF/HF/Satcom - 2.4 kBit/s - MSK modulation - Character oriented
FANS-1/A	No usage for AOC	- ADS-C - CPDLC - ACARS over FANS-1/A (AVLC)	- VHF(VDL)/HF/Satcom - 31.5 kBit/s - D8PSK Modulation - Bit oriented

Table 2.4: Comparison of ACARS and FANS adopted from [15]

2.5.4. VDL-2

VHF data link(VDL) is the protocol which can transmit CPDLC and ACARS over VHF via the FANS-1/A systems. 4 versions of VDL have been developed. The first VDL1 was a version which utilised analog radios which is considered outdated and was thus never adopted. The second VDL2 is the only adopted and implemented VDL. The third VDL3 was a versions which tried to implement a form of digitized voice communications, but airlines did not adopt this technology due to complexity. Lastly VDL4 was a contender to be the physical layer for ADS-B, but was not implemented in favour of the Mode-S extended protocol which is discussed in section 2.1.3 [58].

VDL2 is the physical layer which enables CPDLC over VHF. One of its others uses is the ability to send ACARS messages, which is called ACARS over AVLC, AVLC is the aviation VHF link control which contain the data of the VDL2 messages [58]. ACARS messages as described in section 2.5.2 were initially sent out over VHF analog radios, this is also referred to as POA or plain old ACARS. The VDL2 system provides better performance such as a higher bit rate and is a more modern communications protocol as compared to POA [51]. Further differences in technical specifications of both systems can be seen in the table above. Currently the VDL2 datalink is the most used form of digital communication in aviation [45]. VDL2 shares the same VHF band as the VHF radio voice communication (118 [MHz] - 137 [MHz]). VDL2 uses a D8PSK modulation scheme, which encodes the message in the phase domain.

D8PSK modulation or differential 8-ary phase shift keying is the modulation method of VDL2. This is a form of phase modulation, which as the name suggests modulates the signals carrier wave, such that the phase changes of the signal contain the data of the message. Before a VDL2 message is transmitted the input bits are mapped to a phase difference in the signal wave using Gray code. Using Gray code has the advantage that if a bit error occurs during for example the transmission, the error will be smaller as compared to using normal binary code [65]. In D8PSK bits are mapped to phase differences by using the following constellation diagram and phase encoding see figure 2.4 & table 2.5.

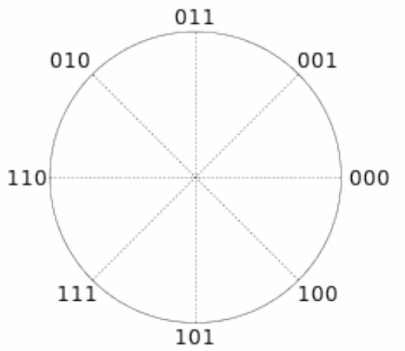


Figure 2.4: D8PSK constellation diagram reprinted from [58]

X_k	Y_k	Z_k	$\Delta\phi_k$
0	0	0	0.00π
0	0	1	0.25π
0	1	1	0.50π
0	1	0	0.75π
1	1	0	1.00π
1	1	1	1.25π
1	0	1	1.50π
1	0	0	1.75π

Table 2.5: D8PSK phase difference encoding adopted from [65]

As can be seen each symbol consists of three bits mapped by a phase difference. Because D8PSK does not use a reference phase to achieve phase coherence in a message, message bits are demodulated using the difference in phase with respect from the previous symbol or signalling interval, hence the name 'differential'. To do this 2 requirements have to be fulfilled, the channel effects and the transmitter oscillator have to be stable enough such that unknown phase changes are very slow such that the phase is effectively constant from one signal interval or symbol through the next. The second requirement is that the phase of the current symbol interval has to have a relationship with the previous interval [119]. The first requirement is fulfilled by using a proper transmitter oscillator and the second is fulfilled by differential encoding the phase using the current and previous phase of the signal [65]:

$$\phi_k = \phi_{k-1} + \Delta\phi_k \tag{2.1}$$

After the signal has been differential encoded, the modulated signal $s(t)$ can be obtained by separately modulating the signal by its in-phase (I) and quadrature (Q) components before adding these.

2.5.5. VDL-2 Message Format

A VDL2 message consists of a training sequence and the message data. Before a sequence of messages is sent the training sequence ensures consists of five sequences: the transmission ramp up, bit synchronization, symbol, transmission length and header FEC. The transmitter ramp up is there to setup the transmitter power stabilization and receiver gain control [65], the synchronisation code is there for the receiver of the message to find the synchronisation point of the message and consists of

a fixed known sequence of bits [58]. The FEC or forward error correction enables the receiver to detect bit errors in the message data. The message data is sent using AVLC frames. For purposes of brevity this is not discussed in detail, it is however to be noted, that the message data always includes the 24-bit ICAO address of the sender of the message.

Transmitter ramp up and power stabilization	Bit-Synchronisation	Reserved Symbol	Transmission Length	Header FEC	Message
5 symbols (15 bits)	16 symbols (48 bits)	1 symbol (3 bits)	17 bits	5 bits	Variable length (AVLC Frame)

Table 2.6: VDL2 transmission [65]

2.5.6. Security & Privacy Implications

Like the previously described ADS-B protocol the ACARS and CPDLC systems have not been designed with security as a main concern [15, 28]. Most ACARS messages are sent in plain text, which leaves it vulnerable for eavesdropping attacks and can lead to privacy implications. [87], demonstrated that ACARS is sometimes used by commercial aviation to transmit sensitive information such as medical data of passengers or even credit card information. Intercepting these kinds of messages can lead to obvious privacy infringements. But the undermining of privacy is mostly due misuse of the system [89]. Besides this the authors [28] demonstrated that CPDLC messages over VDL2 can be injected using relatively cheap software defined radios. The CIA security model can also be applied to evaluate the security of CPDLC and ACARS over FANS1/A.

Confidentiality As described above, if sensitive information is sent out over ACARS the message can be easily intercepted and privacy breached if privacy sensitive information is sent because CPDLC and ACARS messages are sent out using plain text. This will lead to problems if the system is not used correctly and privacy sensitive information is transmitted over these channels.

Integrity the controller and pilots need to be sure the sources of information are authentic and can be identified as the legitimate transmitters. Furthermore, the messages received should not have been modified by non legitimate actors. Clearances sent out by possible attackers can lead to dangerous situations. An example of such an attack took place with VHF-voice communications in Melbourne, where a non-authorised person gave false information to air traffic, [114]. This could also be done with CPDLC over VDL2 because the logon process of CPDLC is transparent.

Availability For ATC and AOC availability is critical. Denial of service or jamming attacks can lead to pilots not receiving clearance instructions which can have a disruptive effect on air traffic if attackers disrupt multiple channels [15]. Both the CPDLC and ACARS do not have an identification scheme robust to attacks [15] and can thus be easily spoofed. This vulnerability was also demonstrated by [28].

As with ADS-B, there are numerous of different countermeasures available to provide more security in CPDLC and ACARS over VDL2. Examples are the discussed cryptography methods such as symmetric and asymmetric encryption. Again here not a single method will be able to provide full security.

3

Radio Frequency Fingerprinting

Traditionally, most wireless transmitting devices are identified or authenticated by an address which is transmitted by this device. Examples of these are the unique 24-bit ICAO code sent out by ADS-B transponders or the MAC-address of a device connected to the internet. These addresses are used to uniquely identify the transmitting device. The problem is however that these addresses can be spoofed such that an attacker is able to impersonate a device. The possibility to spoof wireless transmitting devices and to impersonate or inject messages by non authorized transmitters has obvious implications for the integrity of the wireless protocol. A way to uniquely identify and authorize a transmitting device by the receiver is to identify the device by its physical layer fingerprint [91]. The process of identifying a signal by retrieving the signals unique physical layer features due to hardware imperfections is called Radio Frequency Fingerprinting [75]. It has been shown that due to randomness in the manufacturing process of wireless devices, small imperfections arise which have an effect on the features of the signals these devices transmit. These imperfections can be exploited to uniquely identify the signals transmitter. Moreover, the likelihood that two of the same transmitters have exactly the same fingerprint is very low [75]. This renders radio frequency fingerprints usable to provide an extra identification layer which provides more security and integrity in the wireless protocol. RF-Fingerprinting could be used to provide a fingerprint for many different devices [91]. Examples of applications are the fingerprinting of ADS-B signals [116] to identify aircraft, Wifi devices [44] and push to talk radio transmitters [104].

This chapter will discuss the paradigm of RF fingerprinting identification and requirements for RF fingerprinting fingerprinting, afterwards it will discuss some of the different types of features that can be extracted to be used to fingerprint wireless devices. Furthermore, it will be discussed how radio frequency fingerprinting can be applied to identify aviation surveillance and communication signals for ADS-B and VDL2 to provide an extra identification layer.

3.1. Origins of the RF Fingerprint

Because there is an inherent degree of variance and tolerances in the accuracy of manufacturing radio transmitter components. No signal transmitter will be able to transmit the theoretically perfect signal. Even if transmitting device is from the same manufacturer, it will still have some minute differences [57]. These imperfections are the actual physical constructs that enable RF fingerprinting. As can be seen from figure 3.1. Before transmission a number of digital and analog components will have their effect on the eventual signal transmitted, with each their corresponding small error on the signal. Examples of the transmitter imperfections are the modulation errors produced by the modulator, frequency offset and phase noise by the oscillator and non-linear distortion produced by the amplifier. During transmission traces of these effects can be found in the signal. This trace is called the RF fingerprint, because these errors are inherent to the device transmitter they are very difficult to be reproduced and can thus be exploited to identify specific devices [57].

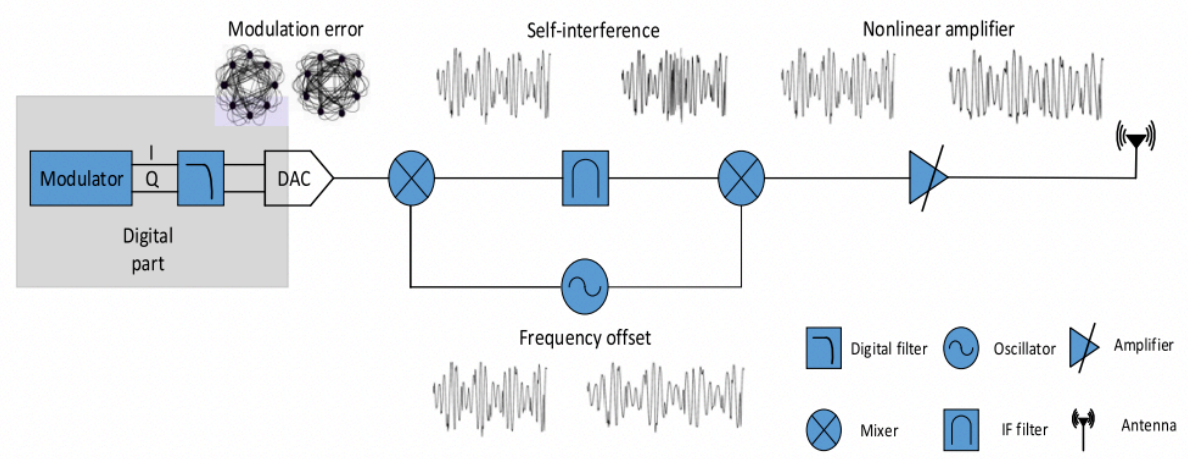


Figure 3.1: Universal software radio transmission reprinted from [57]

3.2. Physical Layer Identification

Physical layer identification is providing the identity of devices through the physical characteristics of the wireless device [91]. The physical layer fingerprint of the signals transmitter is based upon imperfections of the hardware. The goal of physical layer identification is to extract these features to create a Radio Frequency Fingerprint (RFF) of devices. A library of known devices their RFFs should be created to provide a list of which devices are able to transmit messages. The receiving devices should use this library to classify if the fingerprint of the received signal compares with that of a known fingerprint. This will authenticate if a message is from a known sender. To provide a usable layer of identification, the radio frequency fingerprints and devices should fulfill the following conditions [91]:

- *Universality*: Every device should have features which are used for fingerprinting
- *Uniqueness*: Every device should be have an unique fingerprint
- *Permanence*: The fingerprints should be time and environment invariant.
- *Collectability*: The fingerprints should be obtainable with existing equipment
- *Robustness*: The fingerprints should be evaluated and robust to changes in device aspects such as temperature/voltage and external environmental aspect such as effects of signal reflection or absorption

Many different features based on protocol in signals can be exploited and combined to provide a fingerprint. An RF fingerprinting method usually consist of multiple steps, which depend heavily on the application, type of fingerprinting in terms of features and classification strategy. But in general most of the techniques consist of the following steps [112]:

Identifying Relevant Features $\rightarrow$ Extracting and modelling Features $\rightarrow$ Device Identification

The first step to create a physical layer security system based on RF fingerprinting is to identify the relevant features which could be used to fingerprint devices. In other words, which parts of the received signal should be focused on to identify the transmitter of the signal. The next step is to extract and model these features which usually requires signal processing techniques such as the PSD, constellation diagrams or by directly utilising the sampled IQ data of the signal. The final step is to identify the device. This is usually done by training a machine learning algorithm to utilize the identified and extracted features [112]. The steps mentioned above will be further elaborated upon in the coming sections.

3.3. RF-Fingerprinting Techniques

The techniques used to fingerprint devices vary widely based on different types of protocols, devices and features. One of the main challenges in RFF is the selection and extraction of the features in the signal [91]. Feature extraction and selection can be divided into three different types of techniques depending on which parts of the signal the features for fingerprinting are extracted from. Namely: transient-based, steady state-based and other approaches [91]. Transient RF-fingerprinting focuses as the name suggests on the transient part of the signal, which means the part between the first reception of the transmission and the actual steady-state data packet. An example of an application of a transient based RF fingerprinting technique is by [52]. Where wifi devices were identified based on their energy in the transient part of the signal. Transient based methods can provide a very high accuracy in terms of classification performance. The problem however is that it is very difficult to extract the transient part of signals and very high sampling rates are needed [91]. This requires very expensive receivers [83]. Steady state based methods make use of the steady-state part of the signal. The obvious problem with this is that the steady state part depends on the data being transmitted and is thus subject to change with different transmissions. This can be problematic for identification. It is however possible to focus on certain parts of the transmission which do not change between transmissions, such as the preamble which is present in most wireless transmissions [83]. An example of this is the work by [35] which utilises the preamble of the signal to fingerprint ADS-B transmitters. Other approaches which can not be classified to be either a transient or steady state approach make use of specific features of a certain protocol, for example [96] proposed utilising a clock skew approach to fingerprint aircraft transponders. A clock skew method makes uses of the minute differences in timing of transmissions of data between different devices.

3.3.1. Feature Extraction

There are numerous amounts of different features that can be extracted to be utilised for fingerprinting. Features can be subdivided into both location-dependent and location-independent features [91]. To correctly RF-fingerprint devices, the permanence requirement mentioned above should be satisfied, therefore the features extracted should be mostly determined by the transmitter characteristics and not be subject to much noise coming from for example the channel in which the signal propagates. RF-fingerprinting can also be applied to localisation, therefore location dependent features are briefly mentioned as well, [115] provides an overview of the different applications of localisation using RF-Fingerprinting. This section will discuss the different methods which could be used to extract features to RF fingerprint for identification.

As mentioned before, due to imperfections in analog components of radio transmitters. Certain imperfections arise in the transmitted signal which can be exploited to extract the fingerprint of the transmitter. Despite these imperfections the transmission usually still guarantees that the signal is fully within protocol boundaries. A number of different location-independent features can be exploited from the signal to provide a fingerprint. There are a high variety of methods and features to use for fingerprinting. [91] highlights multiple useful methods to extract features for fingerprinting devices. Methods include using raw time domain IQ signal data. another method is to estimate the signals Power Spectral Density (PSD) coefficients. The PSD coefficients can be used to fingerprint the devices transmitting the signal [91]. Choosing a correct method to identify features is heavily dependant of the type of signal being considered.

3.3.2. Feature Extraction Using IQ Data

Radio frequency signals can be sampled and represented as IQ data. This complex time domain (TD) data represents the collected RF signals. The signals sampled data points (n) are represented as in phase (I) and quadrature (Q) data. With the signal represented as [106]:

$$s_{TD}(n) = I_{TD}(n) + jQ_{TD}(n) \tag{3.1}$$

This raw signal data can be directly used to extract features of the transmitter. Furthermore, from this expression a number of signal attributes such as amplitude phase and frequency can be derived [106]:

$$a(n) = \sqrt{I_{TD}^2(n) + Q_{TD}^2(n)} \tag{3.2}$$

$$\phi(n) = tan^{-1}[\frac{Q_{TD}(n)}{I_{TD}(n)}] \tag{3.3}$$

$$f(n) = \frac{1}{2\pi}\frac{\phi(n) - \phi(n-1)}{\Delta n} \tag{3.4}$$

These basic physical layer features could be used to provide fingerprints. For example, [21] used these features with a feature dimensionality reduction technique to identify transmitters. There are multiple methods to use the IQ data of signals to extract features for RF fingerprinting. Some of the more recent publications in the field focus more on the direct utilisation of IQ samples and utilise machine learning methods to extract features. Some examples of these are [43] and [44].

Features in the Modulation Domain

The radio signals of interest in this literature survey ADS-B and VDL-2. Both make use of some form of digital modulation to transmit data. During signal modulation, errors can occur due to hardware imperfections or impairments [16]. The raw IQ data collected of a signal can be used to determine different features based on modulation errors. [16] used the differences of IQ data-points collected with that of an ideal signal (the signal which is ideally modulated, also referred to as target signal). There are multiple possible features to identify a transmitter based on the differences between the collected IQ sample of the signal and an ideally modulated IQ signal. [16] makes a distinction between individual IQ data points and the entire IQ data spectrum. The features of individual IQ data points and the ideally modulated signal are. [16]:

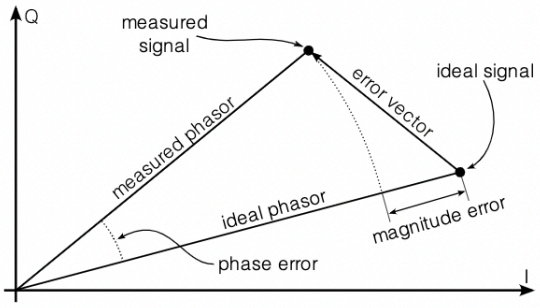


Figure 3.2: Possible features of individual IQ data points reprinted from [16].

- Phase Error
- Magnitude Error
- Error Vector Magnitude

To extract more features from the IQ data, instead of looking at individual data points the entire IQ data set can also be examined and compared with the ideally modulated signal [16]:

- IQ origin offsets: This is the distance between the origin of the ideal IQ plane and that of the observed IQ samples.
- Frequency Errors: This is the difference between the ideal carrier frequency, and the observed carrier frequency of the signal.
- SYNC Correlation: This is the correlation of signals from the SYNC section. SYNC is the part of the signal that precedes the data to synchronize the transmitter and receiver.

Some research has made use of the constellation or modulation errors to provide features for RF fingerprinting. Such as [16], [1] and [66].

Besides the feature extraction methods discussed in the sections above, many more exist such as the use of the Discrete Wavelet Transform by [36]. The variety in the different types of features used is to high to mention. And every possible method and depends heavily on the protocol or device considered for RF fingerprinting. In section 3.5 the current research on fingerprinting and feature identification and extraction for aviation communication protocols, such as ADS-B and VDL2 is discussed more specifically.

3.3.3. Location-Dependent Features

The fingerprinting feature extraction techniques discussed so far focus on device identification. But RF fingerprinting can be applied to finding the location of the transmitting device as well [91]. The features used to identify the location of transmitters must be location dependant. On of the most used feature in location identification is the radio signal strength [91]. Since this thesis focuses on an identification scheme instead of a data verification application of RF fingerprinting, it is only briefly mentioned here. [115] provides an overview of the different applications of localisation using RF-Fingerprinting.

3.3.4. Feature Extraction Using Deep Learning

The features of the fingerprint initially had to be extracted using feature extraction methods such as the ones described above. Deep learning methods can also be utilised for this task, because deep learning methods have the ability to learn and extract features based on data [118]. Furthermore, it can be very hard to engineer features by hand from the radio signals which are affected by noise from the channel, multipath effects or interference. Because features extraction methods, such as features extracted using the modulation domain, are based on the errors between the ideally modulated signal and the received signal, they are protocol specific. For example, the protocols of interest in this thesis ADS-B and VDL2 have different types of modulation, trying to extracted features based on modulation errors will require a protocol specific feature extraction method. This is where deep learning can also be very helpful, because these methods can adapt to different tasks, a single deep learning model can be utilised for multiple different signal protocols [118].

3.4. Device Identification

After relevant features have been selected and extracted to provide an RF fingerprinting. An algorithm should be devised which could identify the transmitting device. An algorithm is to be used to identify and assign the received signal to the correct transmitter [70]. Classification algorithms, utilise a set of labeled data or, in the case of RF fingerprinting, a set of devices from which the RF fingerprints are known. The algorithm then classifies from which device the signal was transmitted from. Chapter 4 will further elaborate on the machine learning methods utilised for RF fingerprinting.

3.5. RF Fingerprinting for Aerospace Signals

To provide more security and identification in wireless protocols, RF fingerprinting for radiometric identification to improve security has been a topic of interest for many researchers. RF fingerprinting has been shown to be possible for many different applications, such as wifi, bluetooth and zigbee devices: [61],[36] and [33]. As mentioned in chapter 2, most of the wireless protocols currently being used in aviation communication and surveillance, do not provide a fully secure identification scheme and can be easily spoofed. RF fingerprinting described in this chapter can provide identification by uniquely identifying the devices transmitting the signals. Since signals such as ADS-B and CPDLC VDL2 are periodically transmitted by aircraft, aircraft identification based on RF fingerprinting these signals is possible [67].

The following sections will further elaborate on the current state of the art in research of RF fingerprinting specifically for aerospace signals.

3.5.1. VHF Radio Voice Communication

As shown in chapter 2 aircraft transmit and receive numerous amounts of different types of signals for communication and surveillance. In aviation communications, the main form of communication between air traffic control and pilots is the VHF-radio voice communication. VHF voice communication is the least trusted communication paradigm in aviation [99]. Because of this, some security measures have been proposed to provide speaker verification based on watermarking [30]. Furthermore, research has been done on using voice data and machine learning to authenticate and verify the speakers in the voice channel [32]. It has been shown that RF fingerprinting on mobile VHF transmitters is possible, for example in the research of [103]. But there is an apparent gap in RF fingerprinting for aviation VHF radio voice communication, which is most likely also due to a number of impracticalities, such that device identification will not give identification of the person using the device. A better method would be to identify speakers, such as in the research of [105] where a speaker authorization module was developed using a deep neural network (DNN).

3.5.2. VHF Data Link

Chapter 2, discussed various VHF data link communications currently used in commercial aviation, namely: CPDLC(VDL-2) and ACARS. [15], showed that the lack of verification and identification leave the communications protocol vulnerable for impersonation attacks. RF fingerprinting the devices could provide a layer of physical identification of the transmitters. RF fingerprinting for ACARS (POA) messages has been a topic of research by [116]. In the research a large ACARS (POA) data set (900,000 samples from 3143 aircraft) was used. The fingerprints were extracted from the raw signal samples using an inception residual neural networks. It was furthermore shown that the network could also work for ADS-B type signals, but no research was done on if fingerprinting using the combination of both signals could be used for aircraft identification. It should also be noted that the authors make no remarks which parts of the signal were used for fingerprinting, since the machine learning method could possibly learn to cheat on the identifier (24bit ICAO) which is sent in the message. Also, the sampling rate was very high at 192MS/s. As to the best of knowledge, no research has been found on the RF fingerprinting of VDL2 or (ACARS over AVLC) signals. There is thus an apparent research gap in the RF fingerprinting of the VDL2 type of messages. There has however been research with signal types comparable to the modulation scheme of VDL2. In [39], the authors devised a RF fingerprinting method for among others DSSS-DQPSK modulated signal. This signal differs from the D8PSK scheme in that the phase differences between symbols are always $\pi/2$ instead of $\pi/4$. Furthermore D8PSK does not use DSSS.

3.5.3. ADS-B Fingerprinting

The ADS-B, or automatic dependent surveillance broadcast is one of the cornerstones in the modernisation of aviation. Many authors have expressed concerns regarding the security of ADS-B [95][60][55]. This has lead to research in numerous different kinds of possible solutions to improve security in the ADS-B protocol, among others full encryption, data verification techniques and even blockchain technologies. One of the researched techniques has been radio frequency fingerprinting. Radio frequency fingerprinting has been proven to be possible with the transmitted ADS-B signal with a great diversity in the type of fingerprinting and the features used to fingerprint. This section will discuss most of the recent publications on this subject.

ADS-B Fingerprinting Features

Most of the published work on ADS-B fingerprinting used IQ data to provide the features for fingerprinting with many employing machine learning techniques such as a neural network to feed IQ data directly in a neural network to provide a classification of the aircraft transponder transmitting the ADS-B signal. Some focused on inter arrival times of different types of ADS-B messages, such as velocity, position and identification [96] or on specific signal features such as the ADS-B signal's phase-pattern. The ICAO standards of the ADS-B protocol provide an overview of the signals requirements and tolerances, from [55]:

- Carrier Frequency should be 1090 $\pm$ 1MHz
- Pulse Width: 0.5 $\pm$ 0.05μs rise time
- message amplitude can change in $\pm$1 dB
- No phase restrictions

Carrier Phase-Pattern

Because the ADS-B message protocol described by ICAO standards does not provide a restriction on the message carrier phase, the authors of [55] and [113] used this feature as a means to classify and identify aircraft. To estimate the phase pattern of the received message, a maximum likelihood estimator which estimates the phase pattern of each received bit in a full not taking into account the preamble, 112 bit ADS-B message. Signal sampling was done at a rate of 100Msamples/s [55]. The phase pattern of each message was extracted and showed that a distinction could be made between different types of phase pattern behaviour of the carrier. The phase behaviours of different types of transponders can be separated into seven classes, linear, quadratic, oscillating, non-coherent, mixed: quadratic & linear and wave [55]. The authors state that about 50% of all aircraft have a distinct representative phase pattern. From which 93 % could be correctly classified by a neural network [55]. The authors did not identify distinct aircraft, but classified the class of phase pattern of transponder signal. This classification based solely on the carrier phase pattern thus limits itself in to only seven classes, which implies limited effectiveness [113]. The carrier phase pattern feature was used in [55] to develop an intruder detection algorithm. This intruder detection algorithm was further developed to contain more features such as the carrier frequency features in [56]. Furthermore [67] used the phase pattern to try to identify different aircraft using a convolutional neural network with four layers with an accuracy of 41.9 %. In a more recent study, [113] also used the phase pattern of the ADS-B message to classify not only seven classes, but label the aircraft as a separate class. This study used the pairs of IQ samples to calculate their phases. Using the following relationship [113]:

$$\phi[k] = tan^{-1}(\frac{x_q[k]}{x_i[k]}) \tag{3.5}$$

With k as the kth pair of IQ samples. The phases of these IQ samples contain a number of different features for classification, namely information about the carrier frequency offset and the phase offset. The ADS-B passband signal can be denoted as [113]:

$$x_p(t) = Re\{\sqrt{2}x(t)e^{j2\pi f_c t}\} \tag{3.6}$$

With $x(t) = x_i + jx_q(t)$ as the baseband signal in complex form f_c as the carrier frequency (1090MHz). With a frequency offset and a phase offset the signal becomes Δf, $\Delta\phi$, the signal becomes [113]:

$$\begin{aligned} \tilde{x}_p(t) &= Re\{\sqrt{2}x(t)e^{j2\pi(f_c+\Delta f)t+\Delta\phi}\} \\ &= Re\{\sqrt{2}\big(x(t)e^{j\phi(t)}\big)e^{j2\pi f_c t}\} \end{aligned} \tag{3.7}$$

Where the phase is denoted as: $\phi(t) = 2\pi\Delta ft + \Delta\phi$. The rate of change of the phase is the carrier frequency offset, which is a result of the doppler shift, propagation channel and the transmitter device specific frequency offset [113].

Signal Classification Using IQ Samples
Raw IQ data without specifically extracting features such as the phase pattern described above could also be used for radio frequency fingerprinting. Most of the works used raw IQ data as input for a deep learning method which extracted the features and afterwards classified the signals. This has been applied for ADS-B as well. [35] used the signals from 100 different devices with about 400 signals per device and used deep neural network with complex valued weights to classify the different devices. From an ADS-B message. The authors specifically focused on the first part of the message not containing any identification data. Moreover the authors demonstrated the sensitivity of the complex neural network to identification data in the raw IQ data points. By focusing on the ICAO 24 bit code alone, an artificially high accuracy of the network of 99% was achieved [35]. Thus to not focus on the easily spoofed identification data, only the first part of the message was considered which contains no information and is reasonably similar for all devices. The messages were sampled at 20Mhz and only the initial $16\mu s$ was considered, which lead to 320 IQ samples per message. The complex neural network consisted of real and imaginary valued weights and complex activation functions such as ModReLu and CRelu. The complex valued neural network proved to achieve an accuracy of 81.4 % in classifying the different transponders.

3.5.4. Overview

Table 3.1 provides an overview of some of the research on RF fingerprinting for signals that are emitted from aircraft. As can be seen, the number of different features and input data can vary, but most use raw IQ data as input. This is useful if different signal protocols are considered for RF fingerprinting using the same classifier. Furthermore use is made of the phase pattern and the short-time fourier transform. The performance of the RF fingeprints can vary widely and depends highly on the size of the datasets used. For example in [44] the performance for a dataset containing 5000 different devices was about 77% for the ResNet50-1D and 53% for the CNN (Baseline Model). Whereas the performance for a dataset containing 50 devices, was 86% and 92% for both models respectively.

Research	Signal	Features or Input Data	Data set (Transmitters)	Classifier	Performance (Accuracy) Depending on task
[44]	ADS-B/WiFi	Raw IQ	5000	CNN/ResNet50-1D	up to 99%
[2]	ADS-B/WiFi	Raw IQ	100	Recurrent DCN	100%
[92]	ADS-B	Raw IQ/STFT	1000	Complex CNN	up to 86% (100 devices)
[116]	ADS-B	Contour Stellar Images	5	AlexNet/GoogleNet	>95%
[35]	ADS-B	Raw IQ	100	Complex CNN	81.6% (focus on preamble)
[79]	ADS-B/Wifi	Raw IQ	10000	Dilated Causal CNN	up to 99%
[56]	ADS-B	Phase Pattern	2942	kNN	- (intruder detection)
[67]	ADS-B	Phase Pattern	274	CNN	41.7%
[20]	ACARS/ADS-B	Raw IQ	5157/3022	Inception Res CNN	98.1% / 96.3%

Table 3.1: RF Fingerprinting Research and Performance Comparison

4

Machine Learning

Machine learning is the term used to describe the set of methods which can automatically detect patterns in data. These learned patterns can afterwards be used to perform different kinds of decision making under uncertainty [64]. Machine learning can be divided into three main types. The first being supervised or predictive learning. This type aims to learn a mapping of from input **x** to output y using a labeled set of data pairs $\mathcal{D} = \{(\mathbf{x}_i, y_i)\}$. Here $\mathbf{x}_i$ in the data set $\mathcal{D}$ is known as the set of features, this could be a time series, images or in the case of radio frequency fingerprinting a received signal, or features from this received signal. y is the set of labels or target value of data, this is a categorical value in the case of classification problems. For example, in radio frequency fingerprinting, this is the label which specifies from which device y_i the signal x_i was sent. In the case that y is a continuous variable, it is called a regression problem [14]. Another main type is called unsupervised learning, here the data to be used for training the machine learning model is not labeled, and the data sets consist only of the input $\mathcal{D} = \{x_i\}$. Unsupervised learning can have the goal to find groups of similar examples within a data set, this is called clustering [14]. More examples of unsupervised learning are ways to determine the distribution of data known as density estimation. The last main type of machine learning is called reinforcement learning, here the machine learning algorithm does not use labels or optimal target values as with supervised learning, but has to discover them by using processes of trial and error [14].

This chapter will discuss the different kinds of machine learning methods that could be employed, specifically for radio frequency fingerprinting.

4.1. Classification Algorithms

Classification is a supervised learning task which is the mapping of an input x to an output class y. With y being the set of class labels. If the full set of y is two classes, we speak of binary classification, if y is larger than two it is called multi-class classification [64]. The goal of a classification algorithm is to estimate the unknown function which maps inputs x to their class labels y: $y = f(x)$. The algorithms thus acts as a function approximator to output a prediction of a class: $\hat{y} = \hat{f}(x)$ (where the hat indicates a prediction). In RF fingerprinting for identification, the classification algorithm chosen will have as an input the signal, or extracted features from this signal and as an output the probability distribution of the device labels. The eventual prediction of the model will be chosen based on the maximum a posteriori estimate or MAP, which is in other words the device label which has the highest probability of being the transmitter of the signal. A high variety of classification algorithms exist. The selection of a correct algorithm depends highly on the data considered. In RF fingerprinting, the data can be the raw IQ samples of the signal received, or an extracted subset of the data which contain the features which was obtained through feature engineering. Here a distinction can be made between classification methods which work well when features have been hand picked or processed by humans (feature engineering) or classification methods which can automatically extract features from the data. Most of the recent publications in RF fingerprinting utilise methods which can extract features automatically. Because features are extracted automatically, the algorithms can work for different signal protocols, without requiring a feature extraction based on the signal. Such as in [3], where a single type of machine learning algorithm could RF fingerprint both WIFI and ADS-B transmitters. Since automatic feature extraction is mostly the realm of deep learning methods, it will be discussed in more depth.

4.1.1. Deep Learning

RF fingerprinting discussed in chapter 3 needs some form of a learning classification algorithm to classify devices. Most of the recent published work in RFF used deep learning methods for this task, such as: [44, 74, 78]. Deep learning is a type of machine learning which has great flexibility and is very powerful, because it learns to represent the world or data as a nested hierarchy of concepts, in other words it can build complex concepts by combining or relating simpler concepts [34]. The main motivation to develop deep learning methods was because traditional machine learning methods, such as support vector machines did not generalize well enough on tasks which required to learn functions with high dimensional data such as speech recognition or computer vision [34]. Because with an increase in the number of dimensions of a machine learning problem, the problem becomes increasingly difficult, this is also known as the curse of dimensionality. One other important concept in many deep learning problems is the hypothesis that in high dimensional data, the data of interest lies on a lower dimensional space embedded in the high dimensional space, this is called a manifold, the learning algorithm should be able to discover the lower dimensional manifold representation of this useful data [34]. This section will discuss deep learning methods which have been applied for RFF, starting with the feed-forward neural network. The methods discussed are based on the theory by [34] unless stated otherwise.

4.1.2. Feed-Forward Networks

Deep feed-forward networks, feedforward neural networks or Multi-layer Perceptron (MLP) is the archetype of the deep learning methods. The feedforward network is a function approximator which tries to map an input x to an output y, or in the case of classification problems an input x to a category y. Also called MLPs neural networks consist of multiple perceptrons or neurons connected through layers. Perceptrons are the building blocks of neural networks. The perceptrons take the weighted sum of inputs of the previous layer, add a bias and pass it through an activation function ψ. Figure 4.1 shows the diagram of a perceptron. A feed-forward neural network consists of an input layer, which is connected to a hidden layer. The hidden layer takes the summed weighted input and passes it through an activation function, the weighted output of the activation function is afterwards passed through multiple hidden layers or the output layer. The depth of the network is determined by the number of hidden layers before the output layer. The hidden layers consist of multiple neurons. Within each neuron the weighted input vector is converted to a scalar, by summing the weighted inputs and passing them through an activation function, these neurons thus have the same working principle as a perceptron. The output layer also has an activation function depending on the problem considered. For a classification with more than two classes, the output layer is usually a softmax function because it gives an output between 0 and 1 yielding the probability of each class in the output [34]. Section 4.1.2 will discuss the different commonly used activation functions. The neural networks have been applied to many different problems and are very flexible in terms of application [14]. The feed-forward neural network is a universal function approximator because it can model any suitable smooth function to any desired level of accuracy, given enough hidden units [38]. Therefore they can be used for radio frequency fingerprinting purposes aswell.

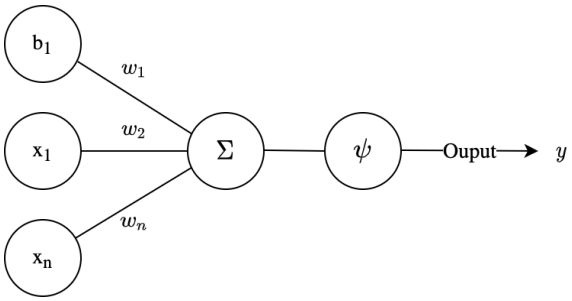


Figure 4.1: Diagram of a perceptron.

Activation Functions

The activation functions used in neural networks should be nonlinear to approximate nonlinear functions. This is because the neural network as a whole will remain a linear function if only linear activation functions are used [34]. This is because successive linear transformations are in itself a linear transformation. There are many different types of activation functions, and these are still a subject of research [34]. Choosing an activation function depends on the considered task for the neural network. Currently the most used activation function for feed-forward neural networks is the **ReLU**. Some of the most popular activation functions used in deep learning are:

Sigmoid The sigmoid function is defined by $\sigma(x) = \dfrac{1}{1+e^{-x}}$. [34] states that the sigmoids perform well with small networks, but suffer from what is known as a vanishing gradient problem. This is because with small x the functions output is very close to zero, whereas when the input x is large the output is very close to 1 and the gradient or derivative shrinks to a too small value to be useful for training. This is an important drawback, because weight updates based on the gradient will not be updated effectively and thus network training can stall if this happens.

ReLU The rectified linear unit, is currently one of the most used activation functions in neural networks. It is defined by the function $\sigma(x) = max(0, x)$. This activation function suffers less from the vanishing gradient problem. This only happens with negative input, when the gradient is always 0. The leaky

ReLU was developed specially to counter this.

Softmax The softmax function defined by $softmax(x_i) = \frac{e^{x_i}}{\sum_j^n e^{x_j}}$ is most often used as the classifier to output the probability distribution over n distinct classes in multi class classification.

Hyperbolic tangent The hyperbolic tangent: $g(x) = tanh(x)$. The hyperbolic tangent generally performs better than the sigmoid function [34]. It is often used in recurrent neural networks because the use of rectified linear functions such as the ReLU do not fulfill the requirements for these types of networks [34].

Many more activation functions exist and can be applied for neural networks, the process of selecting a correct activation function depends mostly on trial and error [34].

Training
A machine learning method usually needs to be optimized. This refers to the maximization or minimisation of the objective function. The objective function also called, cost function, loss function or error function is the metric to be maximized or minimised by the training algorithm. The algorithm used for training in deep learning is usually a gradient descent algorithm. A neural network has a number of learnable parameters such as the network weights, which are optimised by the gradient descent algorithm. A neural network also has hyper-parameters, which are the parameters that are not learned by the training algorithm, but rather are the parameters which have an influence on the performance of the model and model training. Examples of hyper-parameters are: the number of training epochs, number of neurons in the layers and learning rate of the algorithm.

Loss function As stated above, the learning algorithm needs to minimise a loss function. The loss function is a measure between the networks desired output and the actual output of the network. The data which is used during the training of the learnable parameters of the network is called the training data. This data is input in the network in a so called forward pass, the error is calculated by the loss function and the learnable parameters are updated by the training algorithm.

Radio frequency fingerprinting is usually an multi-class classification problem, and thus needs a loss function which is suitable for this. The most used implementation is the cross-entropy method. The multi class cross entropy error function with T as the matrix of target values (data labels) of $N \times K$ with targets t_k and model output y_k, for each output neuron or class k. [68]:

$$\mathcal{C} = -\frac{1}{n} \sum_{n=1}^{N} \sum_{k=1}^{K} t_{n,k} \ln (y_{n,k}) \tag{4.1}$$

Back-propagation
When the network makes a so called, forward pass. The input x is propagated through the network to result in the network output y. During training back-propagation, the information from the cost function propagates backwards in the the network to determine the gradient of the loss function with respect to the learnable parameters or weight vector using the chain rule [34]. After back propagation, the gradient descent algorithm will update the weights of the network according to an update rule depending on the type of gradient descent algorithm used. The update rule usually has a learning rate parameter, which scale the weight updates for each training step, this can be regarded as a hyper parameter [34]. Some algorithms such as Adam utilise an update rule for the learning rate parameter, such that the learning rate is adapted at each training step. Choosing a right optimization algorithm is difficult because there is no general consensus on which is the best algorithm, and it usually depends on the familiarity of the user. Adam seems to be fairly robust to choices of the hyperparameters [34].

Regularization
The goal of the machine learning model is to create a model which does not only fit well on the model training data, but is rather a model which generalises on the problem being considered. In other words, it prevents over-fitting to the training data. Regularization can be thought of as a reduction in generalization error, which is not necessarily a reduction in training error [34]. In machine learning, regularization can be done by constraining the weights of the network by introducing an error term in the cost function, which penalises the weights. Furthermore, specific for neural networks a dropout layer can be introduced, which randomly drops out neurons in the layer such that neurons do not rely on other neurons, which is also referred to as co adaptation [37].

4.1.3. Convolutional Neural Networks
Convolutional neural networks are a special kind of neural networks initially designed for computer vision or image recognition tasks [54]. In traditional pattern recognition or classification problems, features were extracted using a hand made feature extractor specific for the problem considered. These features can after extraction be classified by a trainable classifier such as a feed-forward neural network [54]. For computer vision tasks, this proved to be impractical because the number of variables would become very high with the number of weights increasing dramatically with the number of variables or pixels in images. Besides this, the high degree of variability in the location of relevant features in images leads to feature extraction becoming difficult. Fully connected feed-forward neural networks could learn to extract the features, with the weights focusing on specific locations in the input space, but to learn all variability in the inputs a very high number of training instances will probably be required [54]. This has lead to the development of convolutional neural networks, which use the mathematical convolution instead of matrix multiplication in a layer of the network, besides this, most neural networks employ a pooling operation [34].

Convolutional Layer
Convolutional layers perform a convolution of the input layer I with a kernel K. For a one-dimensional convolution the output of the convolution is [34]:

$$S(i) = (I * K)(i) = \sum_{n} I(n)K(i-n) \tag{4.2}$$

As can be seen from figure 4.2, the kernel moves over the input space and produces an output layer, in a CNN this output is usually also fed through an non-linear activation function with the remaining output layer being referred to as a feature map [34]. The coefficients in the kernel can be thought of as the weights which can be trained. In the kernel the weights are the same for each input value, this is also called weight sharing [118]. This has the advantage that the set of weights in the kernel can detect a specific feature over the entire input space. Even when there is variety in the locations of the features in the input space, the kernel can detect and extract these features. A convolutional layer usually consists of multiple kernels from which each produces an output vector. In 2D convolutions such as with image recognition problems, naturally the input space consists of pixels which are convoluted with a 2D kernel. As can be seen in the example of figure 4.2 the kernel fits exactly 5 times in the input space. The size of the kernel is constrained by the input space but can be overcome by using padding of the input space. The size of the kernel, number of kernels and padding can be regarded as hyperparameters.

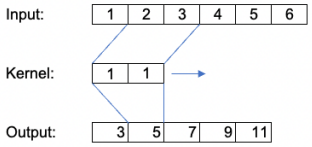


Figure 4.2: Visual Representation of a 1D convolution.

Pooling
The convolutional neural network usually also includes a number of pooling layers. The pooling layers usually come after a number of convolutional layers. This layer transforms the feature maps of the convolutions at certain locations of this feature map by comparing the values in the pool by a certain statistic such as max or average. Figure 4.3 represents a max pooling operation, it will take the max value of the pool. Here the pool size and type of statistic can also be regarded as a hyperparamter. Pooling helps the output of the network become invariant to small variations in the input [34]. Because

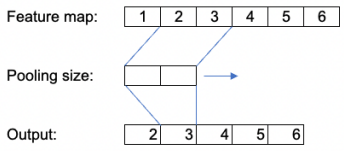


Figure 4.3: Visual Representation of a 1D max pooling layer.

the learning algorithm trains the weights in the kernels, the whole convolutional neural network can be seen as an automatic feature extractor of data [54]. Because of the weight sharing feature extraction can be done with a relatively low amount of trainable parameters, which reduces computation times. Convolutional neural networks have been and can be used for a large amount of different applications, such as: image recognition, speech recognition etc. It also has been used for many signal processing applications such as: detection of jammers, unauthorized transmissions and radio frequency fingerprinting [118].

4.1.4. Recurrent Neural Networks
Recurrent neural networks (RNNs) are another type of neural network. RNNs are specially suited for sequential input data [12]. And were designed specifically for data with a temporal relationship [108] such as natural language processes. Multiple different architectures of RNNs exist. In a recurrent neural network the input data of the previous inputs in the hidden layer is shared with the current state, such that previous information influences the current output of the network, this is a form of memory [4]. Because a classic RNN suffered from the vanishing gradient problems, the LSTM was introduced. LSTM stands for long short term memory. The horizontal line on the top of the cell, is the current cell state. This state passes information to the next recurring LSTM cell. The LSTM also consists of three gates, the forget gate "f_t", input gate "i_t and the output gate "o_t". The LSTM cell adds or removes information (data) to the current cell state via these gates and their respective activation functions. An LSTM neural network usually consists of multiple hidden layers with each neuron representing an LSTM.

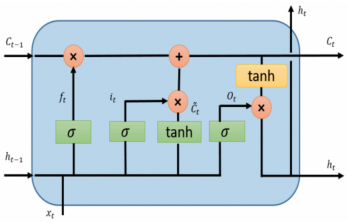


Figure 4.4: Visual Representation of an LSTM cell [4]

Recurrent neural networks and LSTMs, like the CNN, can have a wide number of applications. Recurrent neural networks have have been used for RF fingerprinting purposes in [43], [110] and [81] for a number of different types of transmitters and signal protocols.

4.1.5. Other Classification Algorithms

This chapter has provided an overview of some of the most used classification algorithms for RF-Fingerprinting. Some other RF-fingerprinting methods include but are not limited to: Denoising Autoencoders. The denoising autoencoder is an unsupervised learning method try to extract features by passing the input through first an encoder and reconstruct the data through a decoder by minimising the reconstruction error [8]. The authors of [8] used denoising autoencoders to develop an intruder detection model using RF fingerprinting. Some other classification algorithms which can not be characterised as deep learning methods but have been used for RF fingerprinting are kNN and SVMs. Both have been used by [16], but using these types methods has the downside that features have to be extracted by first developing a feature extraction method based upon the signal. This is one of the reasons why deep learning methods are so popular for RF fingerprinting, since it does not require extensive feature engineering methods based upon the signal [118].

5 Methodology

This chapter will discuss the details of the implementation of RF fingerprinting for aircraft identification. Section 5.2 will discuss the methods used to collect the data and the types and amount of data collected. The next section will describe the methods used to extract features and what type of data will be used as inputs for the classification methods described in the following section. Furthermore, the procedures to investigate the validation and robustness of the model will be discussed in the last sections.

5.1. RF-Fingerpinting Method

The method for RF fingerprinting first consists of the creation of a model which can extract fingerprints based on message data collected. This can be seen in figure 5.1. The workflow consists, first of the collection of messages of the RF signal of interest. In this thesis, those signals are ADS-B and VDL2. This data is collected and pre-processed such that it can be used in a RF fingerprinting deep learning model. This model will have to learn to distinguish between messages from different aircraft. The training of the model is done using a predefined set of training data consisting of pre-processed and labeled sets of real ADS-B and VDL2 messages from aircraft. These messages are defined as the training set.

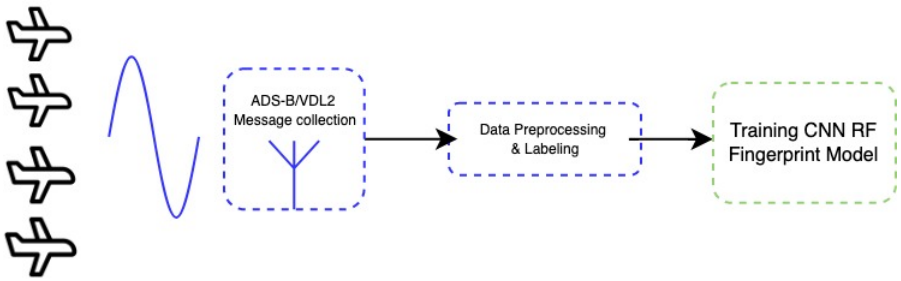


Figure 5.1: Training the RF fingerprinting model.

After the model has been trained to generalize well on ADS-B and/or VDL2 messages from the aircraft in the training set. It can be employed to identify aircraft based on the RF fingerprints of these messages. This is done by collecting the message and pre-processing the message data before feeding it through the deep learning model. The deep learning model will classify from which aircraft the message is most likely to be sent from and thus providing identification based on the RF fingerprint. This process can be seen in figure 5.2.

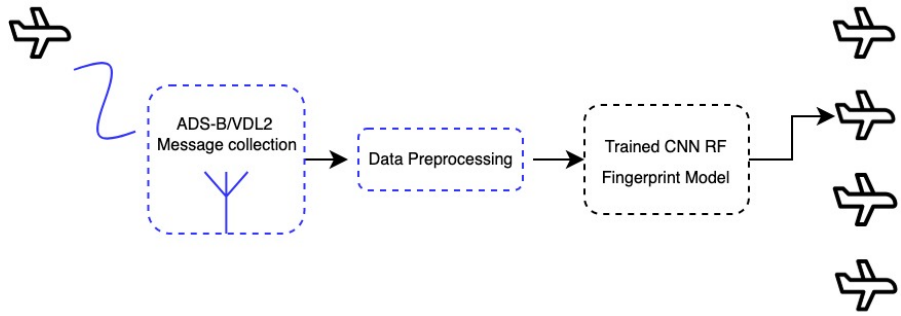


Figure 5.2: RF fingerprinting for identification.

5.2. Data Collection

This section will describe the methods which were used to collect the data. The data was collected using a software defined radio. A software defined radio is described by [80] as: *"a radio in which some of the physical layer functions are software defined"*. This means that the radio can be programmable to be able to adjust to multiple types of signals, frequencies, bandwidths, wave-forms, sampling rates etc. For this thesis, use was made of the following software defined radio hardware:

- RTLSDR (RTL2832U)
  - Frequency Range: 24.0 [MHz] - 1.76 [GHz]
  - Max Sampling Rate: 3.2 [MSPS]
  - Cost: $\pm$20 [USD]

The software defined radio is capable of tuning to the correct frequencies for both ADS-B (1090[MHz]) and VDL2 ($\pm$118-137[MHz]). Both maximum sampling rates are sufficient for RF-fingerprinting, but can be a possible bottle neck. Certain works on radio frequency fingerprinting used very high sampling rates which are not achievable by the RTLSDR. For example the authors of [2] used a sampling rate of 100[MSPS]. The signal bandwidth of ADS-B both devices however are able to sample above the minimum sample rate for both signals, the SDR is connected to a suitable antenna for both types of signal. Both SDRs use quadrature or IQ sampling to sample the VDL2 and ADS-B signals, which will be discussed in section 5.3.1.

5.3. Fingerprinting Implementation Hardware & Software

The collection and demodulation of data will be done using the python libraries pyModeS and pyVDL2. The fingerprints will be extracted using a deep learning model. This model will be built using tensorflow 2.80. The training and testing will be done using a virtual machine utilising 4vCPUs, 15GB of RAM and a NVIDIA Tesla T4 GPU.

5.3.1. IQ Sampling

The following describes the method of IQ sampling bandpass signals based on the article by [50]. The signals of interest ADS-B and VDL2 are both modulated such that they can be transmitted over VHF radio, modulation is needed because the signal can not be sent directly as this would require an impractically large antenna to transmit the low frequency contents of the signal [19]. The resulting signal after modulation can be referred to as the bandpass signal and the signal before modulation can be referred to as the baseband signal. The bandpass signal is thus transmitted over VHF. To sample a signal, the sampling rate should be at least or higher twice the frequency of the highest occurring frequency in the signal according to the Nyquist theorem such that aliasing does not occur. For an ADS-B bandpass signal the highest frequency is at ± 1090MHz (50kHz bandwidth). The sampling theorem thus states that this signal would have to be sampled at a rate of $f_s > 2180$MHz. As we can see in the section above, the SDRs used do not even remotely come near that a high sampling frequency, and sampling at such high rates would probably be quite a costly undertaking in terms of sampler hardware and data storage. Thus direct sampling is not a practical method to receive these signals. Therefore quadrature or IQ sampling is used to retrieve the baseband of the signal. The block diagram of quadrature sampling is shown in figure 5.3.

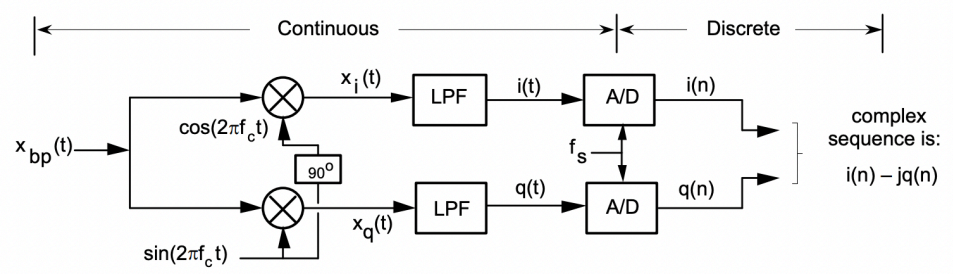


Figure 5.3: Quadrature sampling block diagram [77].

Suppose we have a bandpass signal $x_{bp}(t)$, which is the RF signal which is in our case, the signal containing the ADS-B or VDL2 messages. The signal is seperated before being multiplied in the time domain by: in the in phase (I) channel: $cos(2\pi f_c t)$ and in the quadrature channel (Q): $sin(2\pi f_c t)$. Both sinusoids have a center frequency which is equal to the center frequency f_c of the RF signal being sampled. For ADS-B: 1090Mhz and VDL2 somewhere between 118-137Mhz. In the frequency domain, this centers the frequency components of the signal of interest around zero, after which a low pass filter can extract the signal of interest. This gives the complex continuous $i(t)$ and $q(t)$ values which have to be converted to a digital sequence using a sufficient sample rate f_s. For ADS-B the signals have to be sampled at a rate $> 2MSPS$ because of the pulse cycle of ADS-B at $0.5\mu s$ [101]. This yields the IQ samples of the signal from which a lot of information regarding phase, frequency and magnitude of the sampled signal can be distilled. [106]:

$$a(n) = \sqrt{I^2(n) + Q^2(n)} \tag{5.1}$$

$$\phi(n) = tan^{-1}\left(\frac{Q(n)}{I(n)}\right) \tag{5.2}$$

$$f(n) = \frac{1}{2\pi}\frac{\phi(n) - \phi(n-1)}{\Delta n} \tag{5.3}$$

Besides the signal features described above, the raw IQ data can possibly contain lots of latent features of the origins of the fingerprint described in section 3.1. In this thesis, the deep learning model will try to extract these features. The IQ data is collected for both ADS-B and VDL2.

5.3.2. ADS-B Data

The ADS-B IQ data collected was done using the RTL-SDR (RTL2832U) at the TU Delft faculty of aerospace engineering in Delft, the Netherlands. ADS-B data collection was done from 10-01-2022 till 11-01-2022. The RTLSDR was set at a center frequency f_s of 1090Mhz and a sampling rate of 2MSPS. This yielded approximately 1.6 million separate ADS-B messages. Each message was decoded using the pymodes library. From each message the following data was retrieved:

1. 24-bit ICAO code
2. date & time message received
3. 242 Q samples
4. 242 I samples

Because of the high number of different messages in the data, the data was divided into multiple subsets. The subsets were divided based on the message arrival times and number of distinct aircraft. The different subsets of data used in the different experiments will be explained in section 5.11.

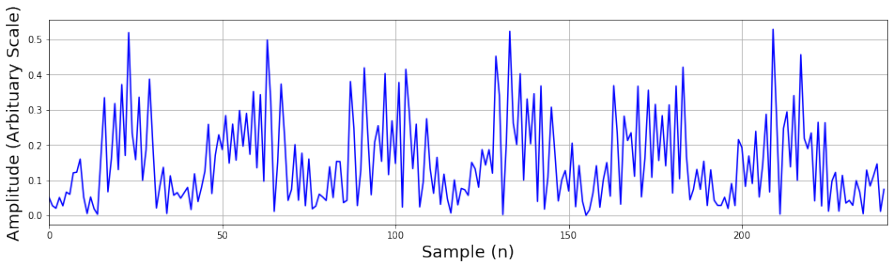
5.3.3. VDL2 Data

The VDL2 IQ data collected was done using the RTL-SDR (RTL2832U) at the TU Delft faculty of aerospace engineering in Delft, the Netherlands. Like ADS-B, the VDL2 data collection was done from 10-01-2022 till 11-01-2022. The RTLSDR was set at a center frequency f_s of 136.775MHz and a sampling rate of 1MSPS. This yielded approximately 127 thousand separate VDL2 messages. Each message was decoded using the pyvdl2 library. From each message the following data was retrieved:

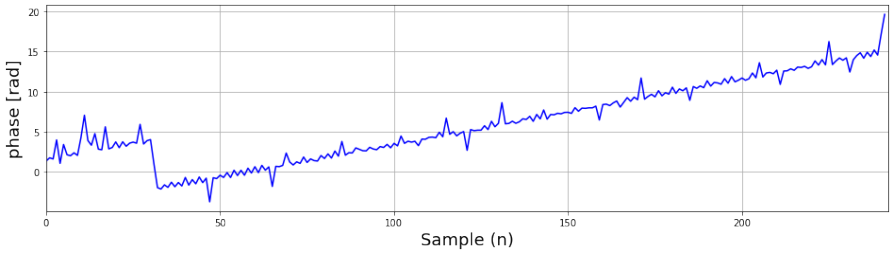
1. 24-bit ICAO code
2. date & time message received
3. Q samples (ranging from $\pm$6000-300000 samples per message)
4. I samples (same as Q samples)
5. Message type (ACARS/X.25 etc.)
6. Type of source (ground station or aircraft)

Because of the high number of different messages in the data, the data was divided into multiple subsets. The subsets were divided based on the message arrival times and number of distinct aircraft. The different subsets of data used in the different experiments will be explained in section 5.11.

The next page shows a received ADS-B and VDL2 message amplitude and phase pattern. Both originating from a single message from the data sets raw I and Q values using equations 5.1 and 5.2 . As can be seen the patterns of both signals are quite different as a result of the difference in modulation and type of signal. Furthermore both signals contain noise

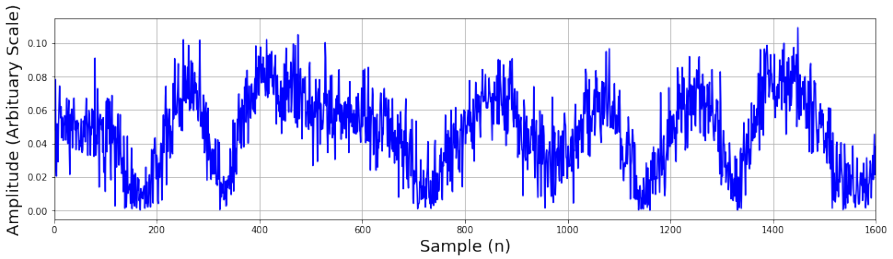


(a) Received ADS-B message amplitude pattern.

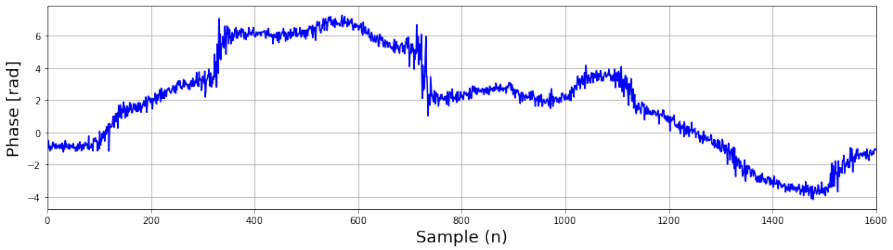


(b) Received ADS-B message unwrapped phase pattern.

Figure 5.4: Amplitude and phase patterns from a single received ADS-B message.



(a) Received VDL2 message amplitude pattern.



(b) Received VDL2 message unwrapped phase pattern.

Figure 5.5: Amplitude and phase patterns from a single received VDL2 message.

5.4. Model Selection

To perform radio frequency fingerprinting, as can be seen in table 3.1 there is a high number of possible classification models which can be used to perform RF fingerprinting. Even for the same signal protocol, there are many different classification models. Deep learning provides a high number of advantages over traditional classification methods. Such as, automatic feature extraction. Deep learning methods generally perform well in automatically extracting features from data as compared to traditional classification methods. In RF fingerprinting problems, features are to be extracted from the signal collected. These collected signal are subject to a high number of distortions coming from different sources. For example channel impairments, such as multi-path effects, noise and interference [118]. These effects are not consistent and change over time. It is very hard to select features which are subject to dynamic noise effects. Extracting these types of features by designing a feature extraction method by hand will be very hard because the locations of the features in the data can for example change over time. Deep learning methods can learn features from the radio signals without requiring such a feature extraction method. Furthermore Deep learning methods can be adaptable for different tasks. This can be seen in table 3.1, where the same deep learning method is used for multiple signal protocols. In this thesis, the RF fingerprints for two different signal protocols namely, VDL2 and ADS-B are investigated. The automatic feature extraction and adaptability of deep learning methods, are one of the reasons the choice is made to utilise deep learning methods for RF fingerprinting in this thesis.

5.4.1. CNN model

Because CNNs have proven to be very effective in the fields of computer vision, natural language processing and as of recently the field of RF fingerprinting. With publications [44, 92, 79, 67] all utilising some form of CNN to do RF fingerprinting for (among others) ADS-B. Therefore the deep learning model developed for this thesis is a CNN. Furthermore, the model is kept relatively small as compared to other RF fingerprinting deep learning models used in other works. For example ResNet50-1D in [44] or the dilated causal convolutional network used in [78]. This has the advantage that it can be trained and used on relatively low spec hardware. The model is partly based upon the baseline model by [44] which is in term based upon AlexNet. An overview of the deep learning model developed can be seen in figure 7.1. This model comprises of three main parts:

1. The input layer
2. The feature extracting CNN stacks
3. The classification & output layer

Input Layer

The input layer is made up of two different channels, namely the I and Q channels. Contrary to most works on RF fingerprinting using IQ data as an input, the input is chosen to be separated. This has the effect that the convolution layers network does not perform cross channel summations, but treats the in-phase I and quadrature Q values separately until the feature maps are concatenated in the classification layer. As we can see later in section 5.10, the model performance will be compared to a similar single channel model where the I and Q channels dimensions are jointly convoluted. The size of the input layer can be regarded as a hyperparameter. Moreover which parts of the messages will be used in the neural network as input data can be an important factor, which will be discussed in section 5.5.

Feature Extraction
The I and Q data are fed through the feature extraction layers. These layers are made up of two 1 dimensional convolutions and a max pooling layer. The convolutional layers consist of 128 different kernels which have a size of 1x7 for the first layer, and 1x5 for the second layer. The convolutional layers convolve the input such that features can be extracted by learning the weights inside the kernels. The convolutional layers are activated using a ReLu activation function. The convolutional layers are connected with a max pooling layer. The pooling layer reduces the dimension of the parameters of the network by summing the feature maps generated by the previous convolutional layers. The two convolutional and single max pooling layer are stacked n times. The classification layers have a number of hyper-parameters which can influence network performance, namely:

- Kernel size
- Number of filters
- Pool size
- Number of stacks

  These model hyper-parameters are tuned to achieve the best performance in terms of classification accuracy possible for the model.

Classification
The classification part of the model consists of three layers. The first is a flatten layer which flattens the outputs of the feature extraction stacks, next a fully connected dense layers with 256 neurons. These layers are connected with a dropout layer which randomly drops 50% percent of the neurons to regularize the network. And are afterwards connected with the output layer which has the same number of output neurons as classes in the training set. This layer is activated using a Softmax activation function, such that the output is a probability distribution for each class. Naturally the network chooses to classify the input messages to a label with the highest probability.

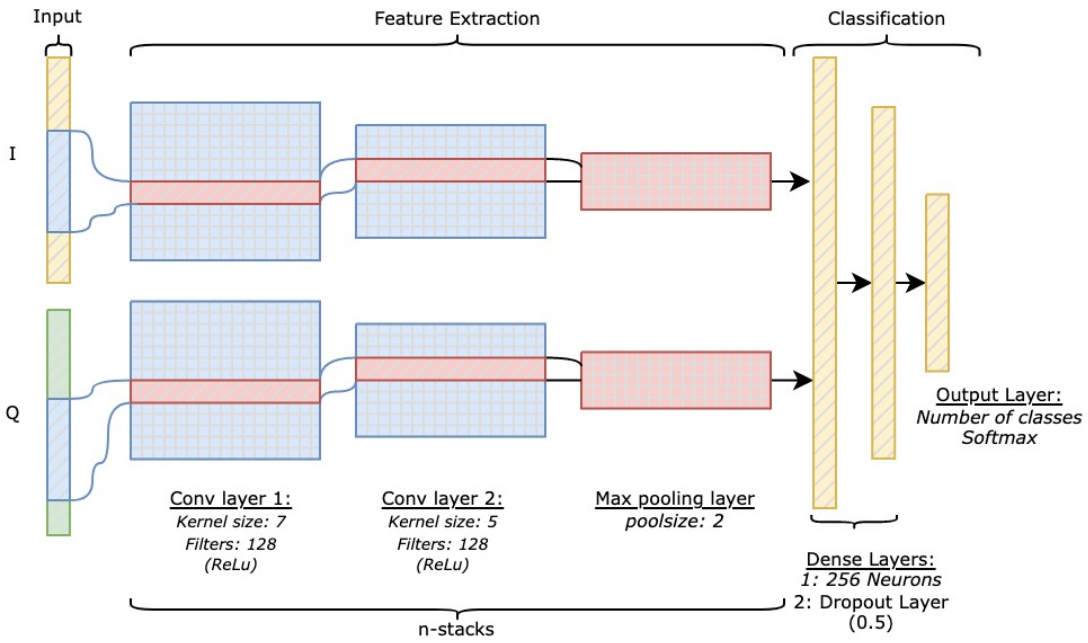


Figure 5.6: CNN model used for RF fingerprinting.

5.5. ADS-B Pre-processing

Before the data is fed into the RF fingerprinting CNN model the collected data has to be pre-processed first. The data collected consists of the ICAO code and the 242 IQ samples for ADS-B. The ICAO codes will be used as the labels for the CNN network to train. The labels are one-hot encoded to be used in the CNN. Furthermore 242 samples will be shortened and only a specific part of the IQ data will be used for training and testing. As can be seen in table 2.1 an ADS-B message consists of 112 bits, which excludes the 8 bit preamble. The preamble is also saved in the in the IQ data, the entire message thus consists of 120 bits and lasts for around 120 μs. Since the message was sampled at 2MSPS the number of raw IQ data points should be 240, the remaining 2 samples are usually added zeros as a result of the sampling in the SDR and computer. Because bits 9-32 in the message contain the 24-bit ICAO ID, these samples should not be included in the data. Therefore the input samples are sliced to not contain samples 32-80, which are the samples corresponding to the data which contain the ICAO ID. Including the ICAO ID in the data will learn the CNN model to cheat by decoding the easily spoofed 24-bit ICAO ID. This will be demonstrated and discussed in section 6.2. The choice is made to utilize the samples 80-242. This leaves us with a size of 162 samples for the ADS-B messages. Each ADS-B message used as an input in the network thus contains 162 I and 162 Q samples. And the message used is min max normalized using the function:

$$x' = \frac{x - min(x)}{max(x) - minx} \tag{5.4}$$

Where x represents the input vector. This normalization scales the samples between 0 and 1. This will ensure the neural network does not focus on the amplitudes of the signal, which can be highly influenced by the channel and location of the sender with respect to the receiver. Furthermore this can possibly improve network training and performance. The input data x_n for the neural network thus consists of 162 min/max scaled I and Q values and the target data t_n consists of the one hot encoded ICAO 24-bit aircraft address.

5.6. VDL2 Pre-processing

Like the ADS-B data, the VDL2 data collected has to be pre-processed. The collected VDL2 data consists of more than 6000 samples per message. Furthermore the ICAO 24-bit address is collected which will again be used as labels. The labels are one-hot encoded to be used in the CNN. Furthermore the more than 6000 samples will be shortened and only a specific part of the IQ data will be used for training and testing. As can be seen by table 2.6, the VDL2 message header consists of the 15 bit ramp up, the 48 bit bit sync, 17 bit transmission length and the 5 bit header FEC. The message data collected does not contain the first 15 bit ramp up so the first part in terms of raw IQ data collected starts at the bit synchronization. Because the 48 bit sync does not contain any message data, and is exactly the same for each message, this part of the data is selected as the input data for the CNN RF fingerprinting model. Because the data is the same for each message, the model will have a minimal chance to learn the contents of the messages and use this as a possible feature for RF fingerprinting. Because the samples 0-1600 in each VDL2 message correspond to the bit sync: 48 bits equals 16 symbols of 3 bits, at a symbol rate of 10500kHz sampled at 1.05GHz which equals 100 samples per symbol. Furthermore the input data is similar to the ADS-B input, min max normalized using equation 5.4. Because the input size of the CNN model at 1600 samples per input message, resulted in very slow training performance, the choice was made to slice the input into two vectors of 512 samples each.

5.7. ADS-B & VDL2 Combination

Because ADS-B and VDL2 can both be sent out by aircraft, it can be investigated if the combination of both ADS-B and VDL2 messages can be lead to a combined RF fingerprint and if this increases accuracy as compared to fingerprinting using a single protocol. The requirement here is that the same aircraft transmits both ADS-B and VDL2 messages at similar times, such that the fingerprinting can be done using the combination of both messages. To see if this combination of both ADS-B & VDL2 data can be used to provide aircraft identification using RF fingerprinting, the RF model is slightly adjusted. The model is changed to a four input channel CNN (IQ of ADS-B + IQ of VDL2) such that both VDL2 and ADS-B can be used as an input. The data is pre-processed such that each VDL2 message is accompanied by a single ADS-B message using the pre-processing steps described in the sections above. This means that the input data consists of a 512 sample part of a VDL2 message, and 162 sample part of an ADS-B message.

5.8. Model Performance, Training & Validation

The model will have to be trained to approximate the function f which is able to determine the correct y_{label} using the input $\mathbf{x_{IQ}}$.

$$y_{label} = f(\mathbf{x_{IQ}}) \tag{5.5}$$

The model weights will be trained using the adam optimizer algorithm using categorical cross-entropy as the loss function. the training data set consisting of the data set: $\mathcal{D} = \{(\mathbf{x_{IQ,i}}, y_{label,i})\}$ where $\mathbf{x_{IQ,i}}$ represent the IQ data of a message i and the $y_{label,i}$ represents the ICAO 24-bit address which is as the label of the message i. The model performance will be evaluated using classification accuracy as the metric. The classification accuracy is the percentage of correctly classified $\mathbf{x_{IQ,i}}$ to the correct label.

To investigate if the model generalises to the RF fingerprints instead of just the training set. The model has to be tested on data which is not seen by the model during training. Therefore the data is to be separated into three parts the training set, the validation set and the test set. The training and validation sets are used during the training. Where the training set is directly utilised to update the trainable parameters and the validation data set is used to update the model hyperparameters during training iterations. Because the validation data indirectly affects the model selection process, it is thus not considered an unbiased metric of model performance to unseen data. For this we have the training set, for which the model accuracy is indicative of the eventual performance of the model to unseen data.

A random training/validation and testing split of the data sets can still be biased. Because of this it is recommended to divide the data into a training and testing set. The training set is afterwards iteratively divided into both validation and training subsets. This is called k-fold cross-validation. K-fold cross validation divides the training set into k folds of training and validation data. If for example 5 folds are used, the training data is divided 5 times into a training and testing set, with each fold the validation data is a different subset, such that every sample of data is used for both training and testing. Keep in mind that the testing data is separated form the training set which is divided into k-folds. Because this gives a better indication of model performance as compared to multiple subsets of data, it is used in this research.

5.9. Requirements

Now that the CNN model has been developed and message data collected. The performance of the extraction of RF fingerprints has to be evaluated. Recall from chapter 3 that the extracted fingerprints should fulfill the following requirements [91], these requirements will be investigated using the experiments described in the next section:

- *Universality*: Every device should have the features which are used for fingerprinting.

Every device transmitting in the protocols ADS-B and VDL2 should have the features described in 3.1. This is a very hard requirement to investigate since there is a large variety in types of hardware which can transmit and receive these protocols. But it can be assumed that each device transmitting ADS-B or VDL2 utilise all or at least some of the hardware components described in section 3.1. Therefore it is assumed that each device has similar features which are extracted by the model for fingerprinting.

- *Uniqueness*: Every device should be have an unique fingerprint

To investigate if this requirement is fulfilled, the fingerprint from ideally every device or aircraft in the data set should be extracted. This is however impractical since this would require a high amount of computing power and not every aircraft transmits enough messages required to train the model. Because of this, the effect of increasing the amount of aircraft or classes in the data set is investigated to see if the messages can still be correctly classified when more aircraft are added to the data set in experiments 2.A-2.D.

- *Permanence*: The fingerprints should be time and environment invariant.

This means that each fingerprint should not change over time and at different locations or environments. To see if this requirement is fulfilled, the training and testing of the model will be done on different days in experiment 3.A.

- *Collectability*: The fingerprints should be obtainable with existing equipment

The data to extract fingerprints is collected using existing hardware, the RTLSDR. And the fingerprints are extracted using the hardware and software described in section 5.3.

- *Robustness*: The fingerprints should be evaluated and robust to changes in device aspects such as temperature/voltage and external environmental aspect such as effects of signal reflection or absorption

The robustness of the model to the aspects described above, will be investigated in both experiment 3A and 4A-4D, which will add extra noise to the signal data, which will try to model the device aspects.

5.10. Experiments

To investigate the performance of the model in extracting RF fingerprints and correctly identifying the aircraft transmitting the messages, a set of experiments is defined. To evaluate the performance and robustness of the model in extracting RF fingerprints and classifying aircraft based on raw message data a number of experiments have been identified highlighted by their experiment number, ranging from 1A-6A.

Experiment	Description:	N Aircraft:	VDL2	ADS-B	Combination	Method of Validation
1A	Number of CNN stacks	100	x	x		split
1B	Number of CNN Filters	100	x	x		split
1C	Kernel Size	100	x	x		split
1D	IQ channel separation	100	x	x		split
1E	ID information in IQ	100		x		split
2A	Low population	25	x	x	x	5-fold
2B	Medium population	50	x	x	TBD	5-fold
2C	Medium high population	100	x	x	TBD	5-fold
2D	High population	200	x	x	TBD	5-fold
3A	Channel Effects	TBD	x	x	TBD	1 train set 10/01/2022 1 test set 26/02/2022
4A - (2A)	No noise	25	x	x	x	5-fold
4B	Medium noise	25	x	x	TBD	5-fold
4C	High noise	25	x	x	TBD	5-fold
5A	Same aircraft/operator	TBD	x	x	TBD	5-fold
6A	Message Injections	TBD	x	x	TBD	TBD n testing messages

Table 5.1: Experiments and Data

5.10.1. The Model Parameters

The model design choices can have a large influence on the model training and accuracy. For this, a number of parameters are investigated. These parameters are investigated by training and testing the model and evaluating the effect of these parameter adjustments in both training and validation performance. Furthermore, the results of this experiment will lead to a model which is used in the experiments that follow afterwards (2A-5A).

- 1.A: Number of CNN feature extraction layer stacks. The number of CNN stacks can possibly have a large influence on the overall accuracy of the model. Therefore this influence is investigated by training and testing using three different stack sizes: 1, 3 and 5. The limit is set at 5 because any higher number would result in a very high and impractical training time.
- 1.B: Number of filters in convolutional feature extraction layer stacks. The number of CNN filters can possibly have a large influence on the overall accuracy of the model. Therefore this influence is investigated by training and testing using four different amounts of filters: 32, 64, 128 and 256.
- 1.C: Kernel size in convolutional feature extraction layer stacks. The kernel size can possibly have an influence on the overall accuracy and training performance of the model. Therefore this influence is investigated by training and validation using three different kernel sizes for the first convolutional layer: 5, 7 and 9.
- 1.D: Effect of IQ channel separation. The effect of separating the IQ channel is to be compared with a single channel model. This means that the model used in this thesis will be compared to a CNN model where the channels are not separated such that the input of the models are joined after a single convolutional layer.
- 1.E: Effect of ID information in IQ data. This focuses on if the model can possibly learn to demodulate the message. This experiment uses two different input vectors, each containing 162 samples from ADS-B messages. The first set includes the ICAO 24-bit ID part of the message, whereas the second set does not. If the accuracy increases dramatically using ID information in the samples, it can be assumed that the model will focus on the easily spoofed 24-Bit ICAO code present in the message. Because ID parts of information were not collected for VDL2 messages, this effect will only be demonstrated using ADS-B data.

5.10.2. The Effect of Number of Aircraft in Accuracy of Classification

To investigate the effect of the population number of different aircraft in the data the model can classify. The models are trained and tested using multiple subsets of data containing a different amount of aircraft messages:

- 2.A: 25 aircraft
- 2.B: 50 aircraft
- 2.C: 100 aircraft

- 2.D: 200 aircraft

These aircraft are randomly selected from the data collected on 10/01/2022. To function properly as a real life identification RF fingerprinting model, the model should be robust enough to provide an accurate enough classification for higher population sizes.

5.10.3. The Effect of the Channel

The model should be trained such that it generalizes to the origins of the RF fingerprint instead of the signal channel which can also influence the raw signal data. Examples of these are: multi-path effects or interference. To investigate these effects, the model will be trained using data from a single day, but tested using data from a different day. The assumption in this is that the channel effects will vary in time, such that training and testing the fingerprinting model on different days will show the effects of the channel on the accuracy of classification if the model tends to focus on the channel instead of the origins of the fingerprint.

- 3.A: training the model with data from 10-01-2022, testing with data from: 26-02-2022.

5.10.4. The Effect of Noise

The model should be robust to noise, this is evaluated by adding white Gaussian noise to the raw message data. It should be noted that noise is already present currently in the input data since the input are real collected messages. The effects of noise are measured at three different levels of noise.

- 4.A: no added noise (Results of 2A)
- 4.B: medium added noise
- 4.C: high added noise

The noise is added by adding artificial white Gaussian noise (AWGN) to the I and Q parts of the data at different SNR levels.

5.10.5. The Effect of Aircraft Type and Operator

Here the assumption is made, that operator fleets of the same aircraft, operate similar hardware. The RF fingerprinting model should be able to distinguish between different devices of the same type of hardware. For this the data is to be merged with data from the Opensky database [85]. This database contains the data of aircraft such as: registration, type and operator aswell as the ICAO 24-bit address. Because the ICAO 24 bit address is available in the Opensky data, the datasets of messages collected for this thesis and Opensky can be linked. The goal is to create a subset of data which are of similar type and operator and use this for training and testing. If the model does not show a dramatic decrease in performance in terms of accuracy, the model is thus robust to hardware similarities in RF fingerprinting.

- 5.A: Data set containing same model of aircraft from the same operator.

5.10.6. Robustness to Message Injections

For the RF fingerprinting model to be effective as an extra layer of security for the message protocols, the robustness of the model to message injections to unidentified transmitters should be investigated. For this a set of aircraft messages from different aircraft which do not have been previously identified by aircraft should be injected. The RF fingerprinting model should not be able to classify these messages with a high degree of certainty. A threshold should be set to reject messages which can not be classified with a certain degree of certainty. This threshold is yet to be determined. To test the robustness after the threshold is set, it should be evaluated if the messages from the unidentified aircraft are rejected and previously identified aircraft are not rejected.

- 6.A: Inject messages from unidentified aircraft.

5.11. Data sets & Validation Methods

The experiments described above aim to investigate the overall effectiveness and robustness of the model. Furthermore most of these experiments will be carried out for the two signal protocols of interest ADS-B, VDL2 as well as using a combined input of VDL2 and ADS-B messages. For this a number of

subsets of data are made. First two subsets of data are randomly selected from the data collected on 10-01-2022:

- VDL2 Messages from 200 distinct aircraft:
  - 200 messages per aircraft
  - 1024 (2x512) samples per message
- ADS-B Messages from 200 distinct aircraft:
  - 500 messages per aircraft
  - 162 samples per message

These subsets are chosen as the main data sets which are used for experiments 1,2, 4 and 6. This data is randomly dived into three subsets, the training, validation and testing splits at a ratio of $80/10/10$.

- VDL2 Messages from 200 distinct aircraft:
  - 160 training messages per aircraft
  - 20 validation messages per aircraft
  - 20 testing messages per aircraft
- ADS-B Messages from 200 distinct aircraft:
  - 400 training messages per aircraft
  - 50 validation messages per aircraft
  - 50 testing messages per aircraft

The data set used for experiment 3A consists of a training set from 10/01/2022 merged with the data from 26/02/2022. This means that a subset of message data is created from the same aircraft transmitting on both days. For this the data set consists of:

- Messages from at least 25 distinct aircraft VDL2:
  - 150 messages per aircraft on 10/01/2022 as training set
  - 50 messages per aircraft on 26/02/2022 as testing set
  - 1024 (2x512) samples per message
- Messages from at least 25 distinct aircraft ADS-B:
  - 400 messages per aircraft on 10/01/2022 as training set
  - 100 messages per aircraft on 26/02/2022 as testing set
  - 162 samples per message

Experiment 4 aims to investigate the effect of noise on the samples. This is done by adding artificial white Gaussian noise to the raw message data on the data set used in experiments 1 and 2. Experiment 5A aims to investigate the effect of hardware similarity. Thus a data set of collected messages which have been sent by similar hardware. The assumption is made that the same type of aircraft of the same operator operate the same type of hardware. Therefore a data set should be made which contain messages from the same aircraft type and operator. The size of this data set is to be determined, but should at least contain:

- Messages from >25 distinct aircraft utilising similar hardware for VDL2:
  - 200 messages per aircraft
  - 1024 (2x512) samples per message
- Messages from >25 distinct aircraft utilising similar hardware for ADS-B:
  - 500 messages per aircraft
  - 162 samples per message

5.11.1. Validation

The methods of validation will mostly use 5-fold cross validation with a separate test set. This is done because this will give a good estimation of eventual model performance for various training and testing splits. Experiment 1 will however be done using a 80/10/10 split in which single random sets of validation and testing data will be used. This is because experiment 1 is an investigation in the effect of model design choices which will be indicative of some of the main parameter choices used to develop the model.

The reason 5-fold cross validation is used for experiments (2A-5A) is to give a better indication of training and validation performance under the experiment conditions over multiple subsets of training and validation data, as will be the case in eventual real life use cases of this model. Because experiment 1 will explain why some of the model design choices were made for the eventual model used for the rest of the research experiments, using 5 fold cross validation was deemed unnecessary for experiment 1.

5.11.2. Combination of ADS-B & VDL2

The effect of a model utilising a combination of both ADS-B and VDL2 is to be investigated as well. Since the data set of the combination of data is very hardware intensive in terms of data size and thus RAM usage, it is decided to initially only investigate lower population of aircraft experiments such as 2A and 4A. Table 5.1 will give a full overview of all experiments and data used.

6

Preliminary Results

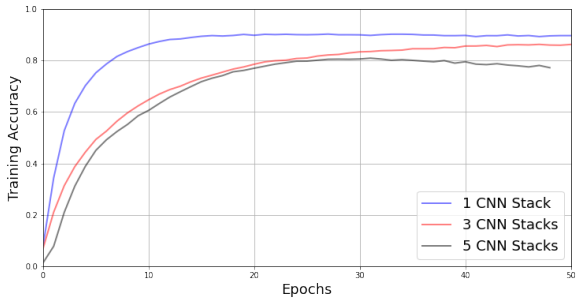
This chapter discusses the preliminary results. It starts with experiments 1.A-1.E the effects of some key model parameters on the model training and validation performance. The outcome of these experiments determined the eventual model settings used for the following experiment 2.A-2.D.

6.1. Experiment 1: Model Parameters

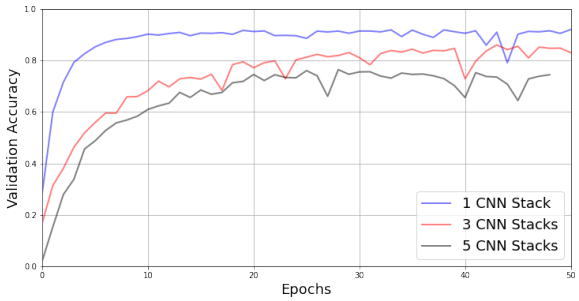
The model design choices can have a large effect on the eventual training performance and accuracy or usability of the model. A number of key model design parameters were investigated in experiment 1. The results from this experiments will determine the eventual model used for the following experiments. The data used is a subset of data containing messages from 100 different aircraft for ADS-B and 100 different aircraft for VDL2. For ADS-B 500 messages per aircraft were collected and split into three groups, 400 training messages, 50 validation messages and 50 testing messages. For VDL2 200 messages per aircraft were collected and split into three groups, 160 training messages, 20 validation messages and 20 testing messages. The first parameter investigated was the effect of the number of CNN stacks in the feature extraction layers.

6.1.1. 1.A Effect of the Number of CNN stacks in the Feature Extraction Layers

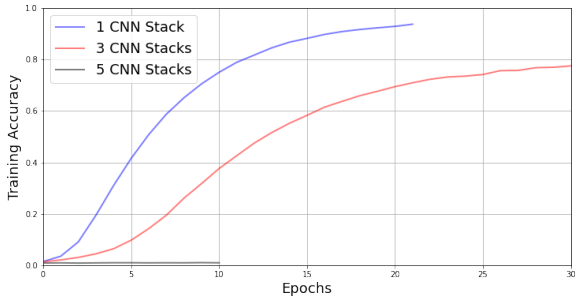
As can be seen by figure 7.1 the feature extraction layer consists of stacks of two convolutional layers connected with a max pool. These can be stacked such that feature maps are passed through extra feature extraction layers. As is the case with AlexNet. The effect of the number of stacks on the training and validation performance is investigated for three stack sizes. These are 1,3 and 5. Any number above 5 results in a very long impractical training time. The training and validation accuracy during training for ADS-B can be seen in figures 6.1. As can be seen by the figures, the training performance actually decreases with increasing number of CNN stacks. The single CNN stack achieves a higher training and validation accuracy using less epochs as compared to 3 and 5 CNN stacks. Furthermore the eventual validation accuracy is also lower as compared to the single CNN stack. The same holds for the VDL2 signal. One possible explanation of this is that more than one convolutional layer is not needed to extract features. And thus the consecutive layers try to extract more features from the feature maps of the previous feature extraction layers and thus complicate the model, which has a detrimental effect on the training of the model. Furthermore, for VDL2 the model sometimes does not converge for the higher stack sizes, as is the case in the training run performed in figure 6.1. Therefore the choice is made to include only one feature extraction stack for both VDL2 and ADS-B.



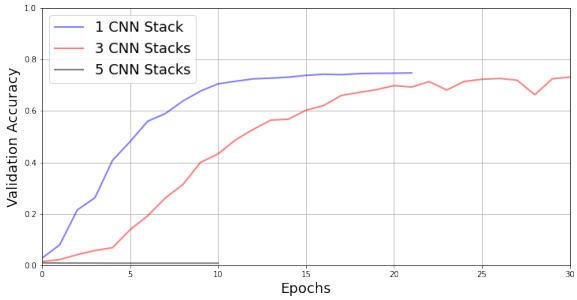
(a) ADS-B Training



(b) ADS-B Validation



(c) VDL2 Training

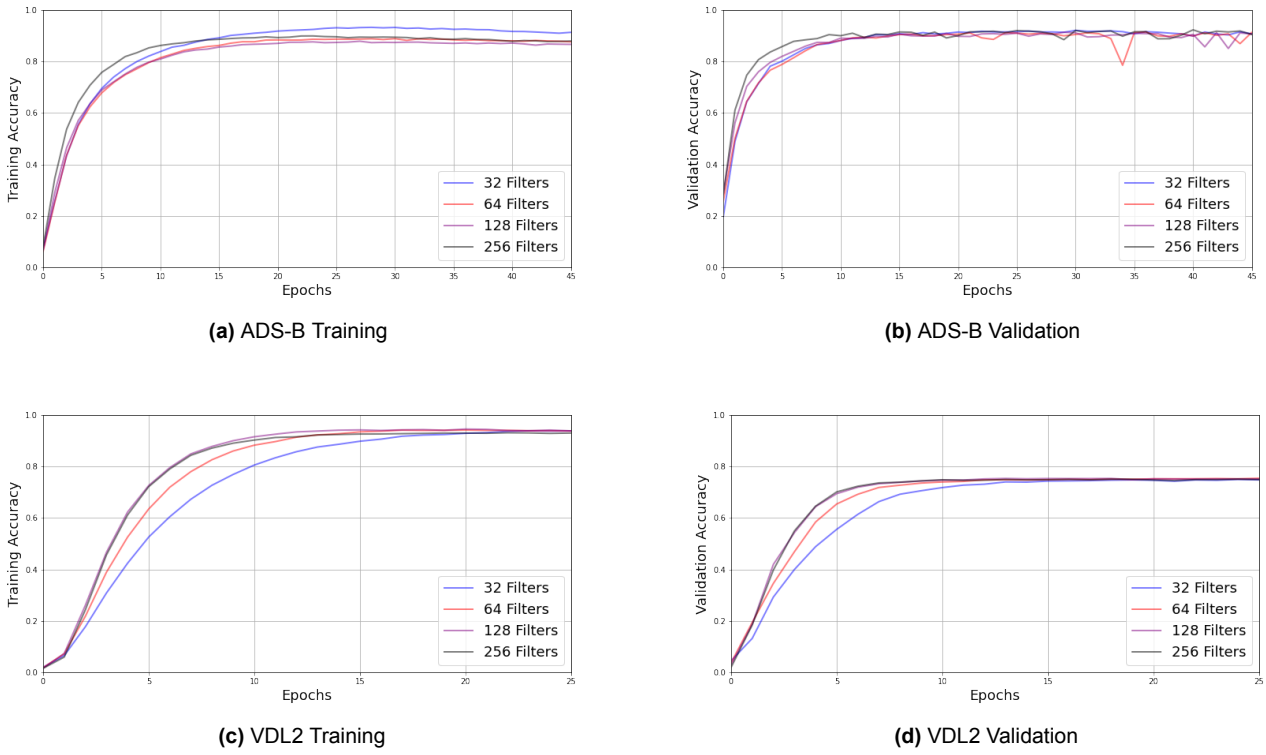


(d) VDL2 Validation

Figure 6.1: Effect of changing the number of CNN stacks

6.1.2. 1.B Effect of the Number of filters in the Feature Extraction Layers

The feature extraction layers consist of convolutional layers. These layers convolute the input data with a number of different weighted kernels or filters. The number of filters can be a parameter which influences the training and overall performance of the model The effect of the number of filters in the convolutional layers on the training and validation performance is investigated for four different amounts of filters. These are 32, 64, 128 and 256. Any number above 256 filters resulted in a very high impractical training time for the model. The training and validation accuracy during training for ADS-B and VDL2 can be seen in figures 6.2. The amount of filters per convolutional layer has some effect on the training and validation performance. Increasing the amount of filters decreases the amount of epochs needed to achieve a certain maximum training accuracy, but the training time per epoch will be longer since there are more filters to be trained. The number of filters does not have a very large effect on the eventual validation performance for VDL2 and ADS-B. The ADS-B training accuracy for a low amount of filters (32) is higher than (64-256). But the validation accuracy is not higher, this could suggest the network is slightly more 'overfit' to the training set, which is undesirable. Because of this, the number of filters chosen is set at 128.



(a) ADS-B Training

(b) ADS-B Validation

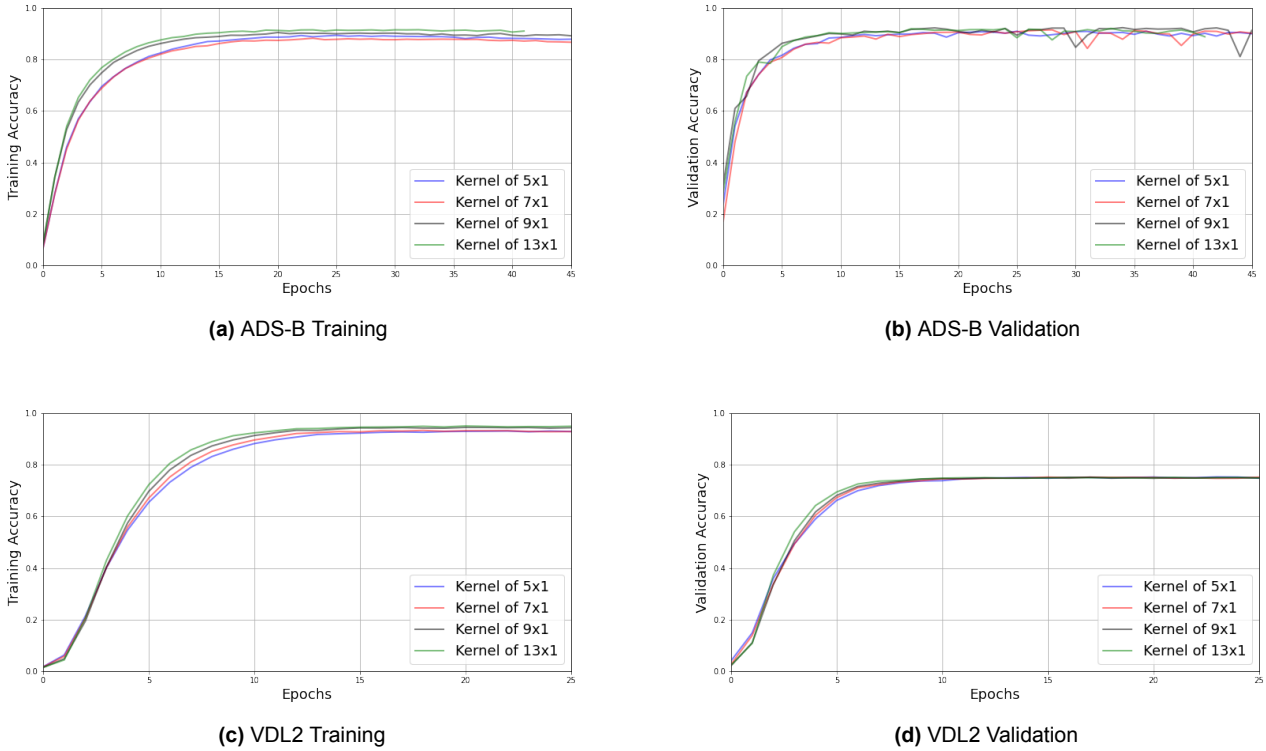
(c) VDL2 Training

(d) VDL2 Validation

Figure 6.2: Effect of changing the number of filters

6.1.3. 1.C Effect of the Kernel Size in the Feature Extraction Layers

The size of the kernels moving across the data in the convolutional layer can be of influence on the training and overall performance of the model. As can be seen by figure 7.1, the feature extraction layers consist of two convolutional layers with the first having a larger kernel size than the second. These kernel sizes are adjusted and the effect on training and validation evaluated. The kernel sizes chosen are 3, 5, 7, 9 and 13. The effect of changing the kernel size on the training and validation can be seen in figures 6.3. As can be seen in the figures, the kernel size has some effect on the training and validation performance. Increasing the kernel size decreases the amount of epochs needed to achieve a certain maximum training accuracy, the catch in this is however that training time per epoch will be longer, since the kernels in the model are larger i.e. more weights to be trained. As can be seen changing the kernel size does not have a large effect on the eventual validation accuracy of the model for VDL2 and ADS-B.



(a) ADS-B Training

(b) ADS-B Validation

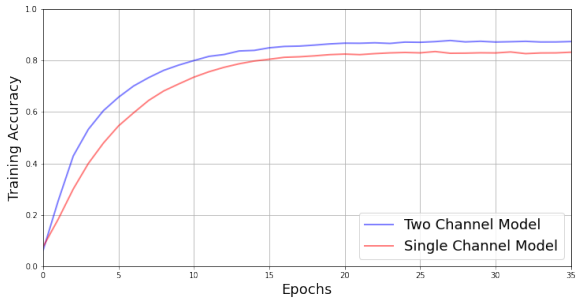
(c) VDL2 Training

(d) VDL2 Validation

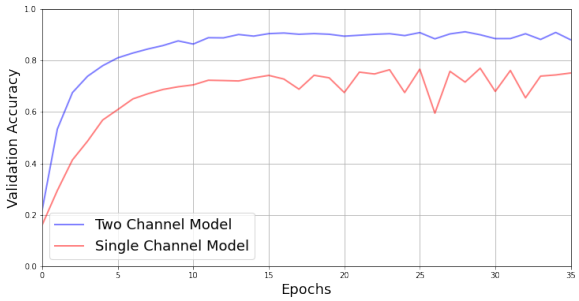
Figure 6.3: Effect of changing the kernel size

6.1.4. 1.D Effect of the Channel Separation

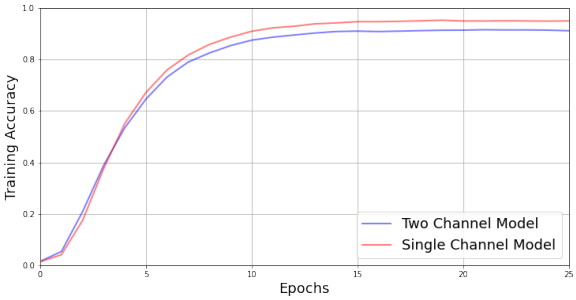
The model used separates the input data into two distinct channels, the I and Q channels. This is a different design choice as compared to the model by [44] on which this model is based. The effect of separating the input on the training and validation can be seen in figures 6.4. As can be seen by the figures, the performance of the models increases in terms of training and validation accuracy. The effect is more profound for the ADS-B messages. This comes at a slight cost of more training time and model complexity. Since the performance for the separated model is better at ± 91 and $\pm 75\%$ validation accuracy vs ± 74 and 71% for ADS-B & VDL2 respectively. Because of this clear performance increase, the choice is made to separate the channels for both protocols.



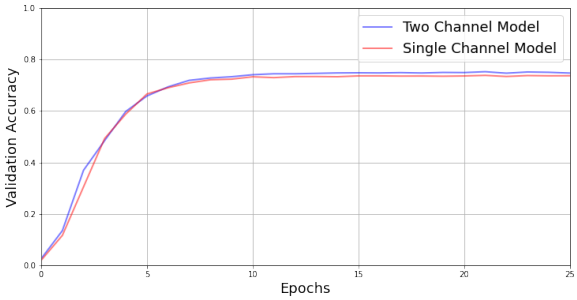
(a) ADS-B Training



(b) ADS-B Validation



(c) VDL2 Training

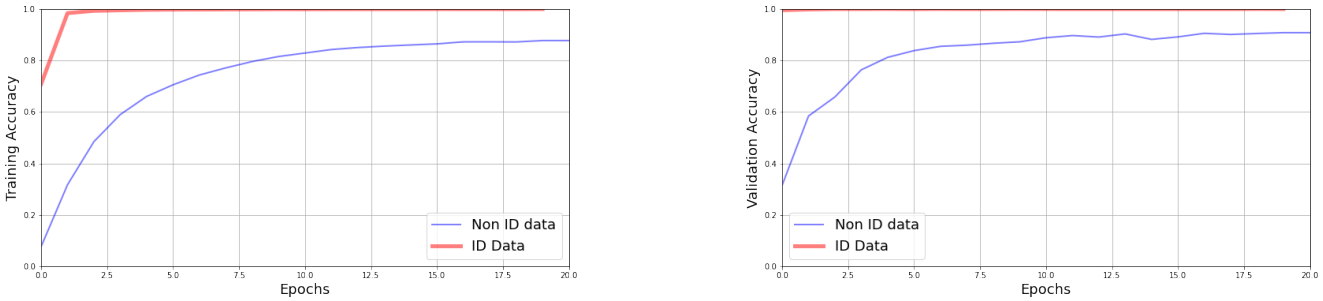


(d) VDL2 Validation

Figure 6.4: Effect of separating the channels

6.2. 1.E Effect of ID information in Input Data

In the data pre-processing step, the choice is made to not include any ID information in the raw input data. Or in other words, the raw samples which correspond with with the 24-Bit ICAO part identification in the messages are not used as input. For ADS-B the number of IQ samples per message are 242. From table 2.1, it can be seen that bits 9-32 correspond with the ICAO aircraft address. The raw message samples start at the beginning of the preamble. Thus the id information is at about $17\mu s - 40\mu s$ from the start of the preamble. Sampled at $2MSPS$ the id information thus corresponds to samples $34 - 80$. To demonstrate the effect including this information in the input data, the samples at 34-80 are selected as the only input samples. The results of this in training and validation accuracy can be seen in figure 6.5. The training and validation both almost instantly go to high accuracies of 100%. This means the network learns to cheat by demodulating the input data and extracting the ICAO 24-bit ID information. This is unwanted behaviour since the model should extract the RF fingerprints and not the message information or the easily spoofed 24-bit ICAO ID. This is a clear demonstration the model will learn to cheat if given the opportunity. Therefore it is imperative that each opportunity for cheating by the model should be mitigated to achieve valid results.



(a) ADS-B Training

(b) ADS-B Validation

Figure 6.5: Effect of including ID data in the raw input data ADS-B

6.3. Experiment 2: Population Size

The effect of the population size is investigated in this experiment. A number of subsets of message data for different amounts of aircraft are trained and tested using the RF fingerprinting model. This metric is important to consider since it will indicate how well the model is able to distinguish between messages from different amounts of aircraft. Four different amounts of aircraft are considered: 25, 50, 100 and 200. The experiment was done for both ADS-B and VDL2.

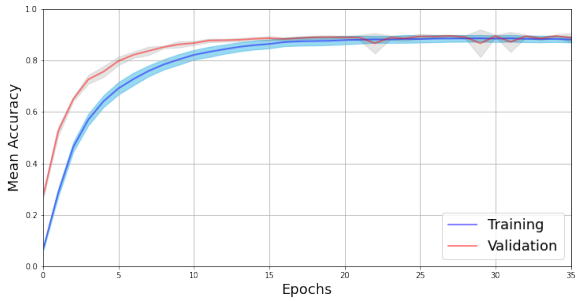
6.3.1. Experiment 2: ADS-B

The effect of the population size is investigated for 25-200 different aircraft. The data set collected consisted of 500 messages per aircraft collected on 10/01/2022. The amount of different messages collected per aircraft can be seen in table 6.1.

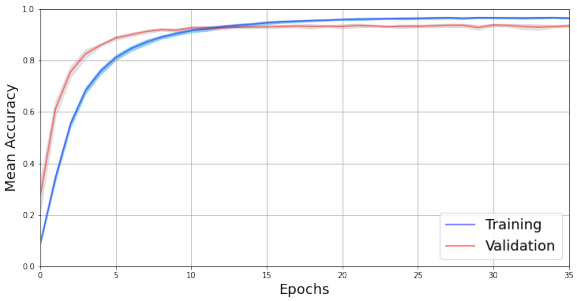
Experiment:	N Aircraft:	Training (n)	Validation (n)	Testing (n)
2.A	25	10k	1.25k	1.25k
2.B	50	20k	2.5k	2.5k
2.C	100	40k	5k	5k
2.D	200	100k	10k	10k

Table 6.1: The amount of messages per experiment for ADS-B

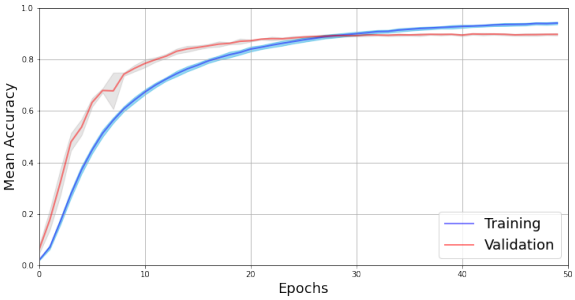
The models were trained and tuned with k-fold cross validation using 5 folds. The model training is tuned and cross validated, afterwards the model is trained using both the training and validation data. The training and validation accuracies training curves can be seen in figures 6.6. Furthermore the training and testing performance can be seen in table 6.2. From the figures it can be seen that for most models, the training and validation accuracy indicate well fitting behaviour of the models to the data. The eventual testing performance decreases slightly with the introduction of more classes. This indicates the model has a harder time in making a distinction between messages fingerprints if more aircraft are introduced to the data.



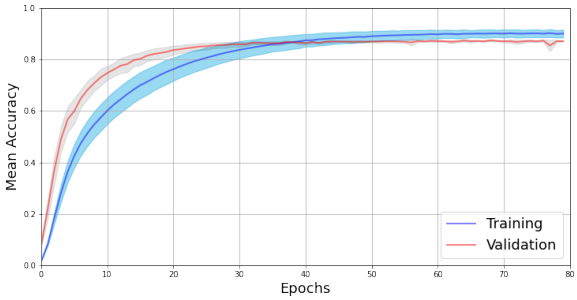
(a) 25 Classes.



(b) 50 Classes.



(c) 100 Classes.



(d) 200 Classes.

Figure 6.6: ADS-B Training and validation for different population sizes.

Experiment:	N Aircraft:	Training (%)	σ_{train}(%)	Validation (%)	σ_{val}(%)	Testing (%)
2.A	25	99	0.2	94	0.6	95
2.B	50	97	0.3	93	0.8	95
2.C	100	94	0.5	90	0.4	90
2.D	200	90	0.8	88	0.5	89

Table 6.2: Experiment 2 results for ADS-B

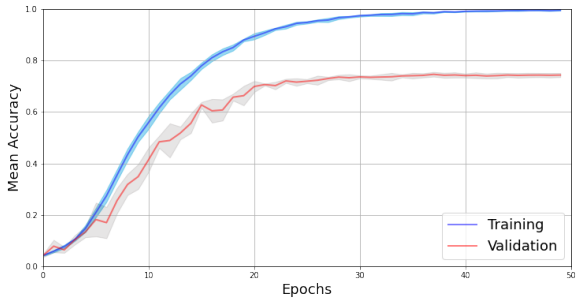
6.3.2. Experiment 2: VDL2

The effect of the population size is investigated for 25-200 different aircraft. The data set collected consisted of 200 messages per aircraft collected on 10/01/2022. The amount of different messages collected per aircraft can be seen in table 6.3. The models were trained and tuned with k-fold cross

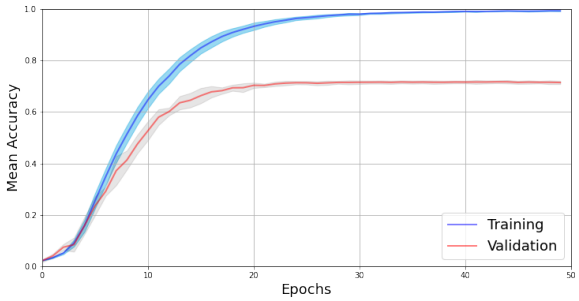
Experiment:	N Aircraft:	Training (n)	Validation (n)	Testing (n)
2.A	25	4k	500	500
2.B	50	8k	1k	1k
2.C	100	16k	2k	2k
2.D	200	32k	4k	4k

Table 6.3: The amount of messages per experiment for VDL2

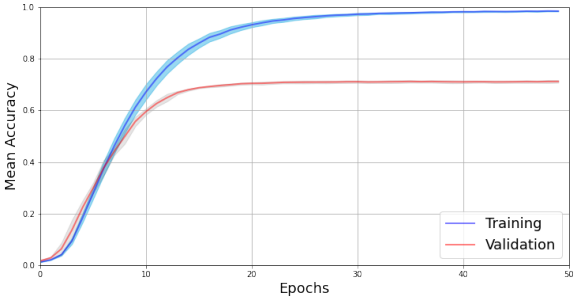
validation using 5 folds. The model training is tuned and cross validated, afterwards the model is trained using both the training and validation data and tested using the test data. The training and validation accuracies training curves can be seen in figures 6.7. Furthermore the training and testing performance can be seen in table 6.2. From the figures it can be seen that for most models, the validation accuracy is substantially lower as compared to the training accuracy, whereas the testing accuracy is higher as compared to the validation accuracy. This can be explained by the amount of data used for training, the training of the model before testing the model is done by combining the validation and training data sets, such that the amount of training data used for testing is comparatively higher. This suggests that more data or messages per aircraft used in training can increase the accuracy of the model.



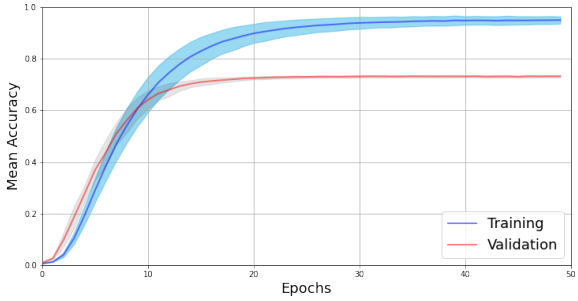
(a) 25 Classes.



(b) 50 Classes.



(c) 100 Classes.



(d) 200 Classes.

Figure 6.7: VDL2 Training and validation for different population sizes.

Experiment:	N Aircraft:	Training (%)	σ_{train} (%)	Validation (%)	σ_{val} (%)	Testing (%)
2.A	25	99	0.2	71	0.6	83
2.B	50	99	0.2	71	0.6	80
2.C	100	98	0.1	71	0.5	79
2.D	200	95	1	73	0.5	79

Table 6.4: Experiment 2 results for VDL2

6.4. Discussion of Preliminary Results

With the first two experiments done, some preliminary results can be discussed. The first experiment 1.A-1.E is an inquiry into some of the model design choices and parameters.

6.4.1. Experiments 1.A-1.D

As can be seen for experiment 1.A, the number of CNN stacks actually decrease the model training and validation accuracies for both the VDL2 and ADS-B protocols. It was expected that a deeper model would perform better, because the deeper layers could learn more different latent features, hidden within the input data as compared to shallower models. This better performance with less 'depth' could possibly be explained by the research of [44]. Here the RF fingerprints were extracted for very large amounts of different ADS-B transmitters (50-5000) using two different models, here the shallower model used, performed better till after about >250 devices where the deeper model started to perform better. It could be possible that increasing the amount of stacks can increase the model performance but only for higher population sizes, but more research will be needed to prove this. Furthermore, for a high amount of stacks, the VDL2 model did not converge.

Experiment 1B investigated the number of filters in the feature extraction stacks. The results show that lower amounts of filters will increase the amount of training epochs to achieve a certain level of accuracy, but each epoch requires less time since there are less parameters to be trained. For ADS-B however, the training accuracy was higher for a lower amount of filters as can be seen by figure 6.2(a). This did not result in a higher validation performance, thus suggesting the model is slightly more 'overfit' to the training set, which is undesirable. Because there is no large increase or decrease in model performance between the amounts of filters, the number of filters used in the model is set at 128. The same holds for the results of experiment 1C, as can be seen there is no large difference in training and validation performance with a changing kernel size.

What does show some significant increase in performance is the separation of the input channels. This is investigated in experiment 1.D. As can be seen by figures 6.4, the validation accuracy for both models increase with separating the inputs before feeding these through convolutional layers. This effect is especially apparent for the ADS-B model where the validation performance increased by about 16% against a 3% increase for VDL2. The difference between the single channel and two channel model is that in the single channel the convolutional layers summarize both channels after the convolution with a kernel. This is not the case in the two channel model, and thus the real (I) and imaginary (Q) parts of the signal are convoluted separately. This increases model performance but comes at the cost of a more complex model.

The final experiment in group 1. is an investigation into the effect of including raw samples responsible for ID information in the input data 1.E. As can be seen by figures 6.5, the model shows a dramatic increase in perfomance. With validation accuracies reaching about 100 %. This would be an unrealistically high accuracy if the model would classify based on RF fingerprints. This thus clearly shows the model will learn to demodulate the raw input data and fit the possibly spoofed 24-Bit ICAO ID. This will totally defeat the purpose of actually doing RF fingerprinting since the model does not fit the fingerprints. It should be noted that the model that the model is thus able to detect the message contents and could possibly use this as a feature. This has many implications, the 162 raw input samples used for ADS-B contain message data and thus data from the transmitting aircraft its location or velocity etc. Since the input data was collected on a single day, it could possibly be that the model tries to use message contents as a feature. Therefore it is required to investigate if this is the case, this will be done in exper-

iment 3A. Where the data used will be merged with data collected on a different day. The assumption here will be that message data for the same aircraft on a different days will be dissimilar. If the model is able to perform similarly in terms of training and testing over different days, the conclusion will be that the model does not fit the message data for ADS-B, or the channel influences on the raw input data. For VDL2 however this is already the case, since all data used as a raw input are the samples responsible for the bit synchronisation code. The bit synchronisation code is the same for all VDL2 messages. So there is no distinction between message data for different messages used and the model will be unable to use the message data as features for VDL2. For VDL2 there is however the possibility that the channel effects on the raw signal data could be used, it will be investigated if this is the case in experiment 3A.

The results from experiments 1.A-1.D were used to develop the parameters for the model used in the following experiments.

6.4.2. Experiments 2.A-2.D

The second experiment investigates the performance of the model to different data sets containing messages from different amounts of aircraft. The dataset used was first separated in a test and training set before messages were selected from 25, 50, 100 and 200 aircraft. The training data was again separated into 5 different folds of validation and training data. As can be seen by the results for ADS-B the testing performance decreases slightly with the introduction of more classes. This decrease in performance shows that the model will probably be limited in use if a high amount of classes will be used. Because it seems the accuracy decreases. Where this limit actually is and at which level of accuracy the model is still usable is not clearly defined and a possible topic for future research.

For VDL2 the decrease in testing accuracy with an increase in number of aircraft is not as prevalent as is the case with ADS-B. It can possibly be that the model is more robust to this increase as compared to ADS-B, but more research will be needed to test the model for even more classes. Furthermore VDL2 shows worse performance in terms of testing accuracy as compared to ADS-B. This could be explained by a number of reasons. The ADS-B data and VDL2 data inputs differ in a number of aspects. The VDL2 input message data is the same for all messages because the focus was on the bit synchronisation, this is not the case with ADS-B. This could explain why the ADS-B the model performs better, since the message data could be used as a feature (which is undesirable). Furthermore the number of samples used for the VDL2 input data was higher but the signal was sampled at a lower rate as compared to ADS-B, this lower sample rate could possibly 'miss' some of the RF fingerprint features. Also, the signal type VDL2 could be inherently less prone to RF fingerprinting errors as compared to ADS-B due to the modulation type and way the signal is transmitted by hardware used. And lastly, the amount of training samples per aircraft is lower for VDL2 as compared to ADS-B, which could have an effect on the testing accuracy. This effect can actually already be seen by looking at table 6.4. The validation accuracy is about ±10 % lower to the testing accuracy. This is because the model is trained on more messages per aircraft before testing as compared to validation (180/160), this results in a very large performance difference. This can also be seen in the learning curves in figure 6.7, as can be seen the validation performance differs a lot from the training performance for all classes. This can suggest that the training set is not representative enough to develop a good generalisation for the validation set. Increasing the training set slightly, as is the case with the eventual testing of the model showed a significant increase in model performance, because of this the sensitivity of the model to the of the amount of training messages per aircraft should be investigated.

7

Conclusion Next Steps

The main objective of this thesis is to develop a method to radio frequency fingerprint aircraft ADS-B and VDL2 signals to identify an aircraft, by using radio frequency fingerprinting methods which employ deep learning. The RF fingerprinting could possibly be used to provide an extra layer of security for both protocols which can possibly improve the integrity and robustness to message injection attacks. Previous research on this subject proved ADS-B messages can be utilised for RF fingerprinting. In this thesis, an RF fingerprinting convolutional neural network has been developed which utilises raw message IQ signal data as the input. This model was trained to classify the aircraft transmitting these messages based solely on the raw message data.

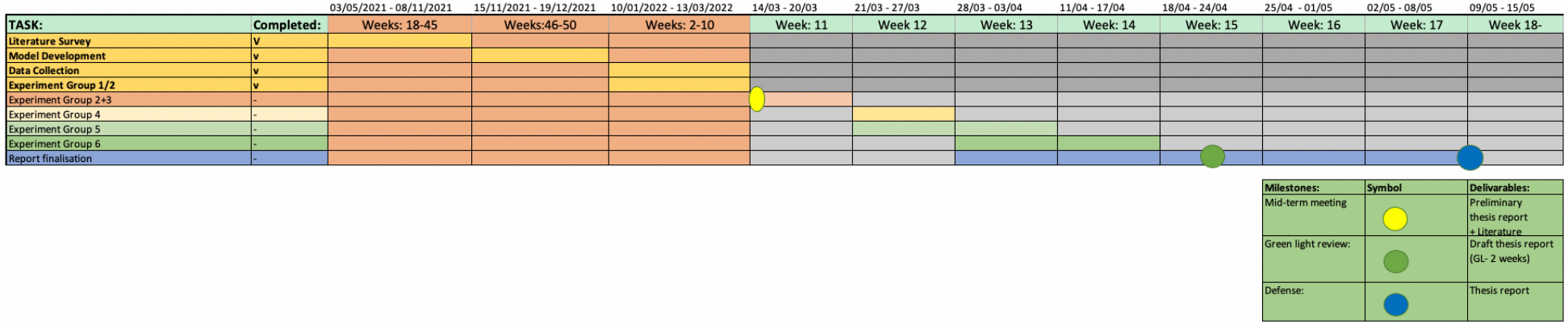
The preliminary results show the model is capable of identifying aircraft based on these raw message samples for up to 200 different aircraft for both VDL2 and ADS-B messages at a testing accuracy of 79% and 89% respectively. But still more research is needed on whether the deep learning model focuses on the correct RF fingerprinting features, instead of other elements such as the channel effects on the raw signal data or message contents. Furthermore, the model robustness to noise and message injections from previously unidentified aircraft are to be investigated. Besides this, it will be investigated if hardware similarities can have an effect on the accuracy of the model.

The initial results thus prove hopeful, but there is still no certainty the model will be able to actually be useful as a possible security measure. This will be investigated in the following part of the research. The model robustness and usability will be investigated using a number of different experiments utilising data already collected over multiple days. These experiments will check if the convolutional neural network model focuses on the correct features, it will check the model robustness and usefulness.

7.1. Next Steps & Planning

The planning to finalize the project is as follows:

- **Data Collection:** All data which is to be used in this thesis is collected. For experiments 1-2 is the data set is from messages collected on 10/01/2022 - 11/01/2022. The data set for experiment 3 will be from the messages collected on datasets from 10/01/2022-11/01/2022 and 26/02/2022-28/02/2022.
- **Development of Deep Learning Model:** completed
- **Experiment group 1:** completed
- **Experiment group 2:** completed for both protocols separately, performance of the combination of both signals to be investigated.
- **Experiment group 3:** For this data has to be merged from the data sets collected on different days. The data is already collected.
- **Experiment group 4:** Noise to be added to the data, the method is already in place but results need to be gathered.
- **Experiment group 5:** The data has to be merged with data from the open sky database and a selection of similar aircraft/operator should be made. If this is done, the results can be gathered.
- **Experiment group 6:** Robustness of model to message injections, method to determine performance and to test this need to be investigated, afterwards results can be gathered.
- **Report Finalisation**
- **Green light**
- **Defense**



		03/05/2021 - 08/11/2021	15/11/2021 - 19/12/2021	10/01/2022 - 13/03/2022	14/03 - 20/03	21/03 - 27/03	28/03 - 03/04	11/04 - 17/04	18/04 - 24/04	25/04 - 01/05	02/05 - 08/05	09/05 - 15/05
TASK:	**Completed:**	Weeks: 18-45	Weeks:46-50	Weeks: 2-10	Week: 11	Week 12	Week: 13	Week: 14	Week: 15	Week: 16	Week: 17	Week 18-
Literature Survey	**v**											
Model Development	**v**											
Data Collection	**v**											
Experiment Group 1/2	**v**											
Experiment Group 2+3	-											
Experiment Group 4	-											
Experiment Group 5	-											
Experiment Group 6	-											
Report finalisation	-											

Milestones:	**Symbol**	**Delivarables:**
Mid-term meeting		Preliminary thesis report + Literature
Green light review:		Draft thesis report (GL- 2 weeks)
Defense:		Thesis report

Figure 7.1: Project Planning.

References

[1] Erkan Acar and Sule Ozev. “Low cost characterization of RF transceivers through IQ data analysis”. In: *2007 IEEE International Test Conference*. ISSN: 2378-2250. Oct. 2007, pp. 1–10. DOI: 10.1109/TEST.2007.4437641.

[2] Ioannis Agadakos et al. “Chameleons’ Oblivion: Complex-Valued Deep Neural Networks for Protocol-Agnostic RF Device Fingerprinting”. In: *2020 IEEE European Symposium on Security and Privacy (EuroS P)*. Sept. 2020, pp. 322–338. DOI: 10.1109/EuroSP48549.2020.00028.

[3] Ioannis Agadakos et al. “Deep Complex Networks for Protocol-Agnostic Radio Frequency Device Fingerprinting in the Wild”. en. In: *arXiv:1909.08703 [cs, eess]* (Sept. 2019). arXiv: 1909.08703. URL: http://arxiv.org/abs/1909.08703 (visited on 11/08/2021).

[4] Md Zahangir Alom et al. “The History Began from AlexNet: A Comprehensive Survey on Deep Learning Approaches”. In: *arXiv:1803.01164 [cs]* (Sept. 2018). arXiv: 1803.01164. URL: http://arxiv.org/abs/1803.01164 (visited on 01/07/2022).

[5] Sahar Amin et al. “Design of a cyber security framework for ADS-B based surveillance systems”. In: *2014 Systems and Information Engineering Design Symposium (SIEDS)*. Apr. 2014, pp. 304–309. DOI: 10.1109/SIEDS.2014.6829910.

[6] Jason Andress. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. en. Amsterdam ; Boston: Syngress, 2011. ISBN: 978-1-59749-653-7.

[7] J. Agustin Barrachina. *Complex-Valued Neural Networks (CVNN)*. original-date: 2020-09-16T14:02:08Z. Jan. 2021. URL: https://github.com/NEGU93/cvnn (visited on 04/20/2022).

[8] Joshua Bassey, Xiangfang Li, and Lijun Qian. “Device Authentication Codes based on RF Fingerprinting using Deep Learning”. In: *arXiv:2004.08742 [cs, eess]* (Apr. 2020). arXiv: 2004.08742. URL: http://arxiv.org/abs/2004.08742 (visited on 01/11/2022).

[9] Joshua Bassey, Lijun Qian, and Xianfang Li. “A Survey of Complex-Valued Neural Networks”. In: *arXiv:2101.12249 [cs, stat]* (Jan. 2021). arXiv: 2101.12249. URL: http://arxiv.org/abs/2101.12249 (visited on 05/19/2022).

[10] Mihir Bellare et al. “Format-Preserving Encryption”. en. In: *Selected Areas in Cryptography*. Ed. by Michael J. Jacobson, Vincent Rijmen, and Reihaneh Safavi-Naini. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2009, pp. 295–312. ISBN: 978-3-642-05445-7. DOI: 10.1007/978-3-642-05445-7_19.

[11] Mohamed Slim Ben Mahmoud et al. *Aeronautical Air–Ground Data Link Communications*. Nov. 2014. DOI: 10.1002/9781119006954.

[12] Y. Bengio, P. Simard, and P. Frasconi. “Learning long-term dependencies with gradient descent is difficult”. In: *IEEE Transactions on Neural Networks* 5.2 (Mar. 1994). Conference Name: IEEE Transactions on Neural Networks, pp. 157–166. ISSN: 1941-0093. DOI: 10.1109/72.279181.

[13] Paul Berthier, José M. Fernandez, and Jean-Marc Robert. “SAT : Security in the air using Tesla”. In: *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*. ISSN: 2155-7209. Sept. 2017, pp. 1–10. DOI: 10.1109/DASC.2017.8102003.

[14] Christopher M. Bishop. *Pattern recognition and machine learning*. en. Information science and statistics. New York: Springer, 2006. ISBN: 978-0-387-31073-2.

[15] Corentin Bresteau et al. “On the security of aeronautical datalink communications: Problems and solutions”. In: *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*. Apr. 2018, 1A4–1–1A4–13. DOI: 10.1109/ICNSURV.2018.8384830.

[16] Vladimir Brik et al. “Wireless device identification with radiometric signatures”. In: *Proceedings of the 14th ACM international conference on Mobile computing and networking*. 2008, pp. 116–127.

[17] Brandon Burfeind et al. “Confidential ADS-B”. In: *2019 IEEE Aerospace Conference*. ISSN: 1095-323X. Mar. 2019, pp. 1–11. DOI: 10.1109/AERO.2019.8742166.

[18] Roberto Calvo-Palomino et al. “Nanosecond-precision Time-of-Arrival Estimation for Aircraft Signals with low-cost SDR Receivers”. In: *arXiv:1802.07016 [cs, eess]* (Feb. 2018). arXiv: 1802.07016. URL: http://arxiv.org/abs/1802.07016 (visited on 06/04/2021).

[19] Luis Chaparro. “Chapter 8 - Sampling Theory”. en. In: *Signals and Systems Using MATLAB (Second Edition)*. Ed. by Luis Chaparro. Boston: Academic Press, Jan. 2015, pp. 493–534. ISBN: 978-0-12-394812-0. DOI: 10.1016/B978-0-12-394812-0.00008-5. URL: https://www.sciencedirect.com/science/article/pii/B9780123948120000085 (visited on 01/14/2022).

[20] Shichuan Chen et al. “Deep Learning for Large-Scale Real-World ACARS and ADS-B Radio Signal Classification”. In: *IEEE Access* 7 (2019). arXiv: 1904.09425, pp. 89256–89264. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2925569. URL: http://arxiv.org/abs/1904.09425 (visited on 01/13/2022).

[21] William E. Cobb et al. “Intrinsic Physical-Layer Authentication of Integrated Circuits”. In: *IEEE Transactions on Information Forensics and Security* 7.1 (Feb. 2012). Conference Name: IEEE Transactions on Information Forensics and Security, pp. 14–24. ISSN: 1556-6021. DOI: 10.1109/TIFS.2011.2160170.

[22] Pete Cooper et al. *Aviation cybersecurity: scoping the challenge*. en. OCLC: 1143251182. 2019. ISBN: 978-1-61977-080-5. URL: https://www.atlanticcouncil.org/wp-content/uploads/2019/12/AVIATION-CYBERSECURITY-12-19-.pdf (visited on 06/02/2021).

[23] Andrei Costin and Aurélien Francillon. “Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices”. In: *Black Hat USA* (2012), pp. 1–12.

[24] Marina Dehez Clementi et al. “When Air Traffic Management Meets Blockchain Technology: a Blockchain-based concept for securing the sharing of Flight Data”. In: *2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)*. ISSN: 2155-7209. Sept. 2019, pp. 1–10. DOI: 10.1109/DASC43569.2019.9081622.

[25] Pooja Dixit et al. “Traditional and Hybrid Encryption Techniques: A Survey”. en. In: *Networking Communication and Data Knowledge Engineering*. Ed. by Gregorio Martinez Perez et al. Lecture Notes on Data Engineering and Communications Technologies. Singapore: Springer, 2018, pp. 239–248. ISBN: 978-981-10-4600-1. DOI: 10.1007/978-981-10-4600-1_22.

[26] EASA. *Amendment to the Airspace Requirements on ADS-B and Mode S*. en. May 2020. URL: https://www.easa.europa.eu/newsroom-and-events/news/amendment-airspace-requirements-ads-b-and-mode-s (visited on 12/23/2021).

[27] EASA. *SIB_2011-14_1.pdf*. July 2011. URL: https://ad.easa.europa.eu/ad/2011-14.

[28] Sofie Eskilsson et al. “Demonstrating ADS-B AND CPDLC Attacks with Software-Defined Radio”. In: *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*. ISSN: 2155-4951. Sept. 2020, 1B2–1–1B2–9. DOI: 10.1109/ICNS50378.2020.9222945.

[29] FAA. *ADS-B Privacy*. en-us. template. Last Modified: 2020-12-15T14:16:29-0500. URL: https://www.faa.gov/nextgen/equipadsb/privacy/ (visited on 06/10/2021).

[30] R. Fantacci et al. “A secure radio communication system based on an efficient speech watermarking approach”. en. In: *Security and Communication Networks* 2.4 (2009), pp. 305–314. ISSN: 1939-0122. DOI: 10.1002/sec.70. URL: http://onlinelibrary.wiley.com/doi/abs/10.1002/sec.70 (visited on 09/13/2021).

[31] Cindy Finke, Jonathan Butts, and Robert Mills. “ADS-B encryption: confidentiality in the friendly skies”. en. In: *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop on - CSIIRW ’13*. Oak Ridge, Tennessee: ACM Press, 2013, p. 1. ISBN: 978-1-4503-1687-3. DOI: 10.1145/2459976.2459986. URL: http://dl.acm.org/citation.cfm?doid=2459976.2459986 (visited on 06/16/2021).

[32] Michael Finke and Tim H. Stelkens-Kobsch. “A practical example for validation of ATM security prototypes”. en. In: *CEAS Aeronautical Journal* 9.1 (Mar. 2018), pp. 157–170. ISSN: 1869-5582, 1869-5590. DOI: 10.1007/s13272-017-0275-y. URL: http://link.springer.com/10.1007/s13272-017-0275-y (visited on 09/13/2021).

[33] Florent Galtier et al. “A PSD-based fingerprinting approach to detect IoT device spoofing”. In: *2020 IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC)*. ISSN: 2473-3105. Dec. 2020, pp. 40–49. DOI: 10.1109/PRDC50213.2020.00015.

[34] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep learning*. MIT press, 2016.

[35] Soorya Gopalakrishnan, Metehan Cekic, and Upamanyu Madhow. “Robust Wireless Fingerprinting via Complex-Valued Neural Networks”. en. In: *2019 IEEE Global Communications Conference (GLOBECOM)*. Waikoloa, HI, USA: IEEE, Dec. 2019, pp. 1–6. ISBN: 978-1-72810-962-6. DOI: 10.1109/GLOBECOM38437.2019.9013154. URL: https://ieeexplore.ieee.org/document/9013154/ (visited on 05/31/2021).

[36] Jeyanthi Hall, Michel Barbeau, and Evangelos Kranakis. “Detection of transient in radio frequency fingerprinting using signal phase”. In: *Wireless and Optical Communications* (2003). Publisher: ACTA Press, pp. 13–18.

[37] Geoffrey E. Hinton et al. “Improving neural networks by preventing co-adaptation of feature detectors”. en. In: *arXiv:1207.0580 [cs]* (July 2012). arXiv: 1207.0580. URL: http://arxiv.org/abs/1207.0580 (visited on 01/10/2022).

[38] Kurt Hornik. “Approximation capabilities of multilayer feedforward networks”. en. In: *Neural Networks* 4.2 (Jan. 1991), pp. 251–257. ISSN: 0893-6080. DOI: 10.1016/0893-6080(91)90009-T. URL: https://www.sciencedirect.com/science/article/pii/089360809190009T (visited on 11/03/2021).

[39] Guangquan Huang et al. “Specific Emitter Identification for Communications Transmitter Using Multi-measurements”. en. In: *Wireless Personal Communications* 94.3 (June 2017), pp. 1523–1542. ISSN: 0929-6212, 1572-834X. DOI: 10.1007/s11277-016-3696-8. URL: http://link.springer.com/10.1007/s11277-016-3696-8 (visited on 01/13/2022).

[40] ICAO. *ADS-B IMPLEMENTATION AND OPERATIONS GUIDANCE DOCUMENT - CNS SG/24 Appendix O to the Report*. Tech. rep. Edition 13.0. Sept. 2020. URL: https://www.icao.int/APAC/Documents/edocs/APX.%20O%20-%20Revised%20AIGD%20Edition%2013%20-%20draft%20v2a%20-%20ENRI%2010.3.pdf.

[41] ICAO. *Effects of Novel Coronavirus (COVID□19) on Civil Aviation: Economic Impact Analysis*. Montreal, May 2020. URL: https://www.icao.int/sustainability/Documents/COVID-19/ICAO%20Coronavirus%202020%2005%2008%20Economic%20Impact.pdf.

[42] Anna Sigridur Islind, María Óskarsdóttir, and Harpa Steingrímsdóttir. “Changes in mobility patterns in Europe during the COVID-19 pandemic: Novel insights using open source data”. In: *arXiv:2008.10505 [cs]* (Aug. 2020). arXiv: 2008.10505. URL: http://arxiv.org/abs/2008.10505 (visited on 06/11/2021).

[43] Hossein Jafari et al. “IoT Devices Fingerprinting Using Deep Learning”. In: *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*. ISSN: 2155-7586. Oct. 2018, pp. 1–9. DOI: 10.1109/MILCOM.2018.8599826.

[44] Tong Jian et al. “Deep Learning for RF Fingerprinting: A Massive Experimental Study”. In: *IEEE Internet of Things Magazine* 3.1 (Mar. 2020). Conference Name: IEEE Internet of Things Magazine, pp. 50–57. ISSN: 2576-3199. DOI: 10.1109/IOTM.0001.1900065.

[45] Jakub Jiránek and Josef Bajer. “Aeronautical VHF Data Link mode 2 receiver based on RTL-SDR”. In: *2017 International Conference on Military Technologies (ICMT)*. May 2017, pp. 643–647. DOI: 10.1109/MILTECHS.2017.7988836.

[46] Nikita Susan Joseph et al. “FlightSense: A spoofer detection and aircraft identification system using raw ADS-B data”. In: *2020 IEEE International Conference on Big Data (Big Data)*. IEEE, 2020, pp. 3885–3894.

[47] Thabet Kacem et al. “Security Requirements Analysis of ADS-B Networks”. en. In: *undefined* (2014). URL: /paper/Security-Requirements-Analysis-of-ADS-B-Networks-Kacem-Wijesekera/b6dec4d8169d0a3aa08eeef1a1d2243f5ac2ae6b (visited on 06/03/2021).

[48] Behnam Kamali. “An overview of VHF civil radio network and the resolution of spectrum depletion”. In: *2010 Integrated Communications, Navigation, and Surveillance Conference Proceedings*. ISSN: 2155-4951. May 2010, F4–1–F4–8. DOI: 10.1109/ICNSURV.2010.5503256.

[49] Yoohwan Kim, Ju-Yeon Jo, and Sungchul Lee. “ADS-B vulnerabilities and a security solution with a timestamp”. In: *IEEE Aerospace and Electronic Systems Magazine* 32.11 (Nov. 2017). Conference Name: IEEE Aerospace and Electronic Systems Magazine, pp. 52–61. ISSN: 1557-959X. DOI: 10.1109/MAES.2018.160234.

[50] Johan Kirkhorn. “Introduction to IQ-demodulation of RF-data”. In: *IFBT, NTNU* 15 (1999).

[51] Jun Kitaori. “A performance comparison between VDL mode 2 and VHF ACARS by protocol simulator”. In: *2009 IEEE/AIAA 28th Digital Avionics Systems Conference*. ISSN: 2155-7209. Oct. 2009, 4.B.3–1–4.B.3–8. DOI: 10.1109/DASC.2009.5347498.

[52] Memduh Köse, Selçuk Taşcioğlu, and Ziya Telatar. “RF Fingerprinting of IoT Devices Based on Transient Energy Spectrum”. In: *IEEE Access* 7 (2019). Conference Name: IEEE Access, pp. 18715–18726. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2896696.

[53] Brandon Kovell, B. Mellish, and T. Newman. *Comparative Analysis of ADS-B Verification Techniques*. en. 2012. URL: http://www.semanticscholar.org/paper/Comparative-Analysis-of-ADS-B-Verification-Kovell-Mellish/d0eab53a6b20bfca924b85fcfb0ee76bfde6d4ef (visited on 06/30/2021).

[54] Y. Lecun et al. “Gradient-based learning applied to document recognition”. In: *Proceedings of the IEEE* 86.11 (Nov. 1998). Conference Name: Proceedings of the IEEE, pp. 2278–2324. ISSN: 1558-2256. DOI: 10.1109/5.726791.

[55] Mauro Leonardi, Luca Di Gregorio, and Davide Di Fausto. “Air Traffic Security: Aircraft Classification Using ADS-B Message’s Phase-Pattern”. en. In: *Aerospace* 4.4 (Dec. 2017). Number: 4 Publisher: Multidisciplinary Digital Publishing Institute, p. 51. DOI: 10.3390/aerospace4040051. URL: https://www.mdpi.com/2226-4310/4/4/51 (visited on 09/30/2021).

[56] Mauro Leonardi and Fabrizio Gerardi. “Aircraft Mode S Transponder Fingerprinting for Intrusion Detection”. en. In: *Aerospace* 7.3 (Mar. 2020), p. 30. ISSN: 2226-4310. DOI: 10.3390/aerospace7030030. URL: https://www.mdpi.com/2226-4310/7/3/30 (visited on 05/31/2021).

[57] Jingchao Li et al. “Differential Contour Stellar-Based Radio Frequency Fingerprint Identification for Internet of Things”. In: *IEEE Access* 9 (2021). Conference Name: IEEE Access, pp. 53745–53753. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3071352.

[58] Stefan Lundström. *Technical details of VDL Mode 2*. en. Tech. rep. 2016, p. 13. URL: https://www.commsys.isy.liu.se/TSKS03/reports/VDL-M2.pdf.

[59] M. R. Manesh and N. Kaabouch. “Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system”. In: *Int. J. Crit. Infrastructure Prot.* (2017). DOI: 10.1016/j.ijcip.2017.10.002.

[60] Donald McCallie, Jonathan Butts, and Robert Mills. “Security analysis of the ADS-B implementation in the next generation air transportation system”. en. In: *International Journal of Critical Infrastructure Protection* 4.2 (Aug. 2011), pp. 78–87. ISSN: 18745482. DOI: 10.1016/j.ijcip.2011.06.001. URL: https://linkinghub.elsevier.com/retrieve/pii/S1874548211000229 (visited on 06/02/2021).

[61] Kevin Merchant and Bryan Nousain. “Enhanced RF Fingerprinting for IoT Devices with Recurrent Neural Networks”. In: *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*. ISSN: 2155-7586. Nov. 2019, pp. 590–597. DOI: 10.1109/MILCOM47813.2019.9021080.

[62] Guillaume Michel and Martin Strohmeier. “Flying in Private Mode: Understanding and Improving the Privacy ICAO Address Program”. In: *Journal of Aerospace Information Systems* (May 2021). Publisher: American Institute of Aeronautics and Astronautics, pp. 1–9. DOI: 10.2514/1.I010938. URL: http://arc.aiaa.org/doi/10.2514/1.I010938 (visited on 06/10/2021).

[63] Kayvan Faghih Mirzaei, Bruno Pessanha de Carvalho, and Patrick Pschorn. *Security of ADS-B: Attack Scenarios*. Tech. rep. EasyChair, 2019.

[64] Kevin P. Murphy. *Machine learning: a probabilistic perspective*. en. Adaptive computation and machine learning series. Cambridge, MA: MIT Press, 2012. ISBN: 978-0-262-01802-9.

[65] Sarhan M. Musa and Zhijun Wu. *Aeronautical Telecommunications Network: Advances, Challenges, and Modeling*. en. Google-Books-ID: GGFECgAAQBAJ. CRC Press, Aug. 2015. ISBN: 978-1-4987-0505-9.

[66] Nam Tuan Nguyen et al. “Device fingerprinting to enhance wireless security using nonparametric Bayesian method”. In: *2011 Proceedings IEEE INFOCOM*. ISSN: 0743-166X. Apr. 2011, pp. 1404–1412. DOI: 10.1109/INFCOM.2011.5934926.

[67] Alessandro Nicolussi, Simon Tanner, and Roger Wattenhofer. “Aircraft Fingerprinting Using Deep Learning”. In: *2020 28th European Signal Processing Conference (EUSIPCO)*. ISSN: 2076-1465. Jan. 2021, pp. 740–744. DOI: 10.23919/Eusipco47968.2020.9287691.

[68] Michael A. Nielsen. *Neural networks and deep learning*. Vol. 25. Determination press San Francisco, CA, 2015.

[69] Michael S. Nolan. *Fundamentals of air traffic control*. en. 5th ed. OCLC: ocn609813680. Clifton Park, N.Y: Delmar Cengage Learning, 2011. ISBN: 978-1-4354-8272-2.

[70] Douae Nouichi et al. “IoT Devices Security Using RF Fingerprinting”. In: *2019 Advances in Science and Engineering Technology International Conferences (ASET)*. Mar. 2019, pp. 1–7. DOI: 10.1109/ICASET.2019.8714205.

[71] Christina Pöpper, Mario Strasser, and Srdjan Capkun. “Jamming-resistant Broadcast Communication without Shared Keys.” In: Jan. 2009, pp. 231–248.

[72] Pavana Prakash, Ahmed Abdelhadi, and Miao Pan. “Secure Authentication of ADS-B Aircraft Communications using Retroactive Key Publication”. In: *arXiv:1907.04909 [cs, eess]* (July 2019). arXiv: 1907.04909. URL: http://arxiv.org/abs/1907.04909 (visited on 06/23/2021).

[73] Bart Preneel. “Cryptographic hash functions”. en. In: *European Transactions on Telecommunications* 5.4 (1994). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/ett.4460050406, pp. 431–448. ISSN: 1541-8251. DOI: 10.1002/ett.4460050406. URL: http://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4460050406 (visited on 06/24/2021).

[74] Guangwei Qing, Huifang Wang, and Tingping Zhang. “Radio frequency fingerprinting identification for Zigbee via lightweight CNN”. en. In: *Physical Communication* 44 (Feb. 2021), p. 101250. ISSN: 1874-4907. DOI: 10.1016/j.phycom.2020.101250. URL: https://www.sciencedirect.com/science/article/pii/S187449072030327X (visited on 11/01/2021).

[75] Saeed Ur Rehman et al. “Radio frequency fingerprinting and its challenges”. In: *2014 IEEE Conference on Communications and Network Security*. Oct. 2014, pp. 496–497. DOI: 10.1109/CNS.2014.6997522.

[76] Ronald Reisman. “Blockchain serverless public/private key infrastructure for ADS-B security, authentication, and privacy”. In: *AIAA Scitech 2019 Forum*. 2019, p. 2203.

[77] Richard Lyons. *A Quadrature Signals Tutorial: Complex, But Not Complicated*. Apr. 2013. URL: https://mriquestions.com/uploads/3/4/5/7/34572113/quad_signals_tutorial-lyons.pdf.

[78] Josh Robinson and Scott Kuzdeba. “RiftNet: Radio Frequency Classification for Large Populations”. In: *2021 IEEE 18th Annual Consumer Communications Networking Conference (CCNC)*. ISSN: 2331-9860. Jan. 2021, pp. 1–6. DOI: 10.1109/CCNC49032.2021.9369455.

[79] Josh Robinson et al. “Dilated Causal Convolutional Model For RF Fingerprinting”. In: *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*. Jan. 2020, pp. 0157–0162. DOI: 10.1109/CCWC47524.2020.9031257.

[80] Tony J. Rouphael. *RF and Digital Signal Processing for Software-Defined Radio: A Multi-Standard Multi-Mode Approach*. en. Google-Books-ID: 4ca9ScU3RXAC. Newnes, Mar. 2009. ISBN: 978-0-08-094173-8.

[81] Debashri Roy et al. “RF Transmitter Fingerprinting Exploiting Spatio-Temporal Properties in Raw Signal Data”. In: *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)*. Dec. 2019, pp. 89–96. DOI: 10.1109/ICMLA.2019.00023.

[82] Tate Ryan-Mosley. *Police are flying surveillance over Washington. Where were they last week?* en. Jan. 2021. URL: https://www.technologyreview.com/2021/01/18/1016309/police-surveillance-washington-capitol-mob-riot/ (visited on 06/14/2021).

[83] Patricia Scanlon, Irwin O. Kennedy, and Yongheng Liu. "Feature extraction approaches to RF fingerprinting for device identification in femtocells". In: *Bell Labs Technical Journal* 15.3 (Dec. 2010). Conference Name: Bell Labs Technical Journal, pp. 141–151. ISSN: 1538-7305. DOI: 10.1002/bltj.20462.

[84] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. "Experimental Analysis of Attacks on Next Generation Air Traffic Communication". en. In: *Applied Cryptography and Network Security*. Ed. by David Hutchison et al. Vol. 7954. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 253–271. ISBN: 978-3-642-38979-5 978-3-642-38980-1. DOI: 10.1007/978-3-642-38980-1_16. URL: http://link.springer.com/10.1007/978-3-642-38980-1_16 (visited on 06/02/2021).

[85] Matthias Schäfer et al. "Bringing up OpenSky: A large-scale ADS-B sensor network for research". In: *IPSN-14 Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*. Apr. 2014, pp. 83–94. DOI: 10.1109/IPSN.2014.6846743.

[86] Bruce Schneier. *Beyond fear: thinking sensibly about security in an uncertain world*. en. New York: Copernicus Books, 2003. ISBN: 978-0-387-02620-6.

[87] Matt Smith et al. "On the security and privacy of ACARS". In: Apr. 2016, pp. 1–27. DOI: 10.1109/ICNSURV.2016.7486395.

[88] Matthew Smith et al. "Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS". In: Apr. 2017.

[89] Matthew Smith et al. "Undermining Privacy in the Aircraft Communications Addressing and Reporting System (ACARS)". en. In: *Proceedings on Privacy Enhancing Technologies* 2018.3 (June 2018), pp. 105–122. ISSN: 2299-0984. DOI: 10.1515/popets-2018-0023. URL: https://www.sciendo.com/article/10.1515/popets-2018-0023 (visited on 09/14/2021).

[90] *Social Impact*. URL: https://opensky-network.org/about/social-impact (visited on 06/11/2021).

[91] Naeimeh Soltanieh et al. "A Review of Radio Frequency Fingerprinting Techniques". In: *IEEE Journal of Radio Frequency Identification* 4.3 (Sept. 2020). Conference Name: IEEE Journal of Radio Frequency Identification, pp. 222–233. ISSN: 2469-7281. DOI: 10.1109/JRFID.2020.2968369.

[92] James Stankowicz et al. "Complex neural networks for radio frequency fingerprinting". In: *2019 IEEE Western New York Image and Signal Processing Workshop (WNYISPW)*. IEEE, 2019, pp. 1–5.

[93] Martin Strohmeier. "Research Usage and Social Impact of Crowdsourced Air Traffic Data". en. In: *Proceedings* 59.1 (2020). Number: 1 Publisher: Multidisciplinary Digital Publishing Institute, p. 1. DOI: 10.3390/proceedings2020059001. URL: https://www.mdpi.com/2504-3900/59/1/1 (visited on 06/11/2021).

[94] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol". In: *IEEE Communications Surveys & Tutorials* 17.2 (2015). arXiv: 1307.3664, pp. 1066–1087. ISSN: 1553-877X, 2373-745X. DOI: 10.1109/COMST.2014.2365951. URL: http://arxiv.org/abs/1307.3664 (visited on 12/23/2021).

[95] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. "Security of ADS-B: State of the Art and Beyond". In: *IEEE Communications Surveys & Tutorials* 17 (July 2013). DOI: 10.1109/COMST.2014.2365951.

[96] Martin Strohmeier and Ivan Martinovic. "On Passive Data Link Layer Fingerprinting of Aircraft Transponders". en. In: *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*. Denver Colorado USA: ACM, Oct. 2015, pp. 1–9. ISBN: 978-1-4503-3827-1. DOI: 10.1145/2808705.2808712. URL: https://dl.acm.org/doi/10.1145/2808705.2808712 (visited on 06/09/2021).

[97] Martin Strohmeier et al. “Crowdsourced air traffic data from the OpenSky Network 2019–2020”. en. In: *Earth System Science Data* 13.2 (Feb. 2021), pp. 357–366. ISSN: 1866-3516. DOI: 10.5194/essd-13-357-2021. URL: https://essd.copernicus.org/articles/13/357/2021/ (visited on 06/11/2021).

[98] Martin Strohmeier et al. “On Perception and Reality in Wireless Air Traffic Communication Security”. In: *IEEE Transactions on Intelligent Transportation Systems* 18.6 (June 2017). Conference Name: IEEE Transactions on Intelligent Transportation Systems, pp. 1338–1357. ISSN: 1558-0016. DOI: 10.1109/TITS.2016.2612584.

[99] Martin Strohmeier et al. “Surveying Aviation Professionals on the Security of the Air Traffic Control System”. In: Jan. 2019, pp. 135–152. ISBN: 978-3-319-61157-0. DOI: 10.1007/978-3-030-16874-2_10.

[100] Martin Strohmeier et al. “The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication”. en. In: *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. London: IEEE, Apr. 2018, pp. 107–121. ISBN: 978-1-5386-4228-3. DOI: 10.1109/EuroSP.2018.00016. URL: https://ieeexplore.ieee.org/document/8406594/ (visited on 06/10/2021).

[101] Junzi Sun. “The 1090 Megahertz Riddle: A Guide to Decoding Mode S and ADS-B Signals”. en. In: (2021). Publisher: TU Delft OPEN. DOI: 10.34641/MG.11. URL: https://books.open.tudelft.nl/home/catalog/book/11 (visited on 05/31/2021).

[102] Shuguang Sun. “ACARS Data Identification and Application in Aircraft Maintenance”. In: Apr. 2009, pp. 255–258. DOI: 10.1109/DBTA.2009.93.

[103] O.H. Tekbas, N. Serinken, and O. Ureten. “An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions”. In: *Canadian Journal of Electrical and Computer Engineering* 29.3 (July 2004). Conference Name: Canadian Journal of Electrical and Computer Engineering, pp. 203–209. ISSN: 0840-8688. DOI: 10.1109/CJECE.2004.1532524.

[104] J. Toonstra and W. Kinsner. “A radio transmitter fingerprinting system ODO-1”. In: *Proceedings of 1996 Canadian Conference on Electrical and Computer Engineering*. Vol. 1. ISSN: 0840-7789. May 1996, 60–63 vol.1. DOI: 10.1109/CCECE.1996.548038.

[105] Marian Trnka et al. “Speaker Authorization for Air Traffic Control Security”. en. In: *Speech and Computer*. Ed. by Alexey Karpov and Rodmonga Potapova. Vol. 12997. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, 2021, pp. 716–725. ISBN: 978-3-030-87801-6 978-3-030-87802-3. DOI: 10.1007/978-3-030-87802-3_64. URL: https://link.springer.com/10.1007/978-3-030-87802-3_64 (visited on 01/13/2022).

[106] Ya Tu et al. “Research on the Internet of Things Device Recognition Based on RF-Fingerprinting”. In: *IEEE Access* 7 (2019). Conference Name: IEEE Access, pp. 37426–37431. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2904657.

[107] C.B. Villani and R.J. Pankiewicz. “A spread spectrum digital data link for aviation”. In: *AIAA/IEEE Digital Avionics Systems Conference. 13th DASC*. Oct. 1994, pp. 498–503. DOI: 10.1109/DASC.1994.369434.

[108] Xueli Wang et al. “Radio Frequency Signal Identification Using Transfer Learning Based on LSTM”. en. In: *Circuits, Systems, and Signal Processing* 39.11 (Nov. 2020), pp. 5514–5528. ISSN: 1531-5878. DOI: 10.1007/s00034-020-01417-7. URL: https://doi.org/10.1007/s00034-020-01417-7 (visited on 01/06/2022).

[109] Kyle D. Wesson, T. Humphreys, and B. Evans. “Can Cryptography Secure Next Generation Air Traffic Surveillance?” en. In: (2014). URL: http://www.semanticscholar.org/paper/A-Practical-and-Compatible-Cryptographic-Solution-Yang-Zhou/d4fbbbce5152d4d59215eef941b567eee5eac2d0 (visited on 06/21/2021).

[110] Qingyang Wu et al. “Deep Learning Based RF Fingerprinting for Device Identification and Wireless Security”. In: *Electronics Letters* 54 (Dec. 2018). DOI: 10.1049/el.2018.6404.

[111] Zhijun Wu, Tong Shang, and Anxin Guo. “Security issues in automatic dependent surveillance-broadcast (ADS-B): A survey”. In: *IEEE Access* 8 (2020). Publisher: IEEE, pp. 122147–122167.

[112] Qiang Xu et al. “Device Fingerprinting in Wireless Networks: Challenges and Opportunities”. In: *IEEE Communications Surveys Tutorials* 18.1 (2016). Conference Name: IEEE Communications Surveys Tutorials, pp. 94–104. ISSN: 1553-877X. DOI: 10.1109/COMST.2015.2476338.

[113] Xuhang Ying et al. “Detecting ADS-B spoofing attacks using deep neural networks”. In: *2019 IEEE conference on communications and network security (CNS)*. IEEE, 2019, pp. 187–195.

[114] Emma Younger. *Melbourne Airport hoax caller Paul Sant pleads guilty to making fake flight calls, aborting Virgin landing - ABC News*. May 2017. URL: https://www.abc.net.au/news/2017-09-05/melbourne-airport-hoax-caller-paul-sant-pleads-guilty/8873984 (visited on 08/27/2021).

[115] Tao Yu et al. “A Guide of Fingerprint Based Radio Emitter Localization using Multiple Sensors”. In: *arXiv:1804.02124 [cs, eess, math]* (Apr. 2018). arXiv: 1804.02124. URL: http://arxiv.org/abs/1804.02124 (visited on 09/02/2021).

[116] Haoran Zha, Qiao Tian, and Yun Lin. “Real-World ADS-B signal recognition based on Radio Frequency Fingerprinting”. In: *2020 IEEE 28th International Conference on Network Protocols (ICNP)*. ISSN: 2643-3303. Oct. 2020, pp. 1–6. DOI: 10.1109/ICNP49622.2020.9259404.

[117] Caidan Zhao et al. “A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks”. en. In: *Computer Networks*. Survivability Strategies for Emerging Wireless Networks 128 (Dec. 2017), pp. 164–171. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2017.05.028. URL: https://www.sciencedirect.com/science/article/pii/S1389128617302347 (visited on 11/22/2021).

[118] Shilian Zheng et al. “Big Data Processing Architecture for Radio Signals Empowered by Deep Learning: Concept, Experiment, Applications and Challenges”. In: *IEEE Access* 6 (2018). Conference Name: IEEE Access, pp. 55907–55922. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2872769.

[119] Rodger E. Ziemer and William H. Tranter. *Principles of communication: systems, modulation, and noise*. en. Seventh edition. Hoboken, New Jersey: John Wiley & Sons, Inc, 2015. ISBN: 978-1-118-07891-4.

[120] Juan Zuluaga-Gomez et al. “Automatic Call Sign Detection: Matching Air Surveillance Data with Air Traffic Spoken Communications”. en. In: *Proceedings* 59.1 (2020). Number: 1 Publisher: Multidisciplinary Digital Publishing Institute, p. 14. DOI: 10.3390/proceedings2020059014. URL: https://www.mdpi.com/2504-3900/59/1/14 (visited on 06/04/2021).