Master Thesis

ADS-B Signal Integrity and Security Verification Using a Coherent Software Defined Radio

Wouter Huygen - 4313305

Delft University of Technology

TU Delft Delft University of Technology

Challenge the future

This page is intentionally left blank.

MASTER THESIS

ADS-B SIGNAL INTEGRITY AND SECURITY VERIFICATION USING A COHERENT SOFTWARE DEFINED RADIO

by

W.J.M. Huygen - 4313305

In partial fulfilment of the requirements for the degree of

Master of Science
in Aerospace Engineering

at the Delft University of Technology

Final report date:	29-06-2021	
Graduation date:	13-07-2021	
Readers:	Dr. J. Sun	TU Delft - AE (daily supervisor)
	Prof.dr.ir. J.M. Hoekstra	TU Delft - AE
	Dr. R.T. Rajan	TU Delft - EEMCS

TU Delft Delft University of Technology

ACKNOWLEDGEMENTS

This report is written as part of the completion of the Master of Science in Aerospace Engineering. The report contains an overview of the study and work done over the last year. During the process, I have received a great deal of support and assistance from different people. First, I would like to thank my supervisor, Dr. Junzi Sun, whose expertise is exceptional, and his dedication kept me motivated to bring the work to the current level. Secondly, I would like to acknowledge the open and natural conversations and support from prof. dr. ir. Jacco Hoekstra. The very personal treatment and subsequent assignment definition have committed me to the work that I had to do. Without their help, I could not have completed this thesis in these kinds of strange times while working from home.

Furthermore, arriving at the end of my journey in Delft, I would call it a milestone. I would like to express my acknowledgments to my current flatmates, Mike and Koen, and all my former flatmates from the Spoorsingel, who brought a lot of fun and stability over the previous years in Delft. They were always open to socializing in good and bad times and allowed me to develop various skills and qualities. In addition, I would like to thank David and Annette for providing valuable guidance both in terms of content and practices. Last but not least, I want to thank my parents, Frank and Janine, who always supported me over the previous years, both mentally and financially. And of course, my siblings, Lisa, Stijn, and Kristien, for being the warm family I need.

W.J.M. Huygen
Delft, June 2021

CONTENTS

List of Figures

List of Tables

I

SCIENTIFIC PAPER

This part of the report contains the scientific paper, providing an overview of the work done. The paper is structured as follows: First the research objective and scope are discussed in the introduction. Followed by section II provides an overview of the state-of-the-art previous and related work, followed by the methodology (section III), containing the proposed solution, the experimental setup, and related technical content for the proposed solution. The method used for signal integrity verification is defined in section IV. In section V the results of the experiments are shown. The paper concludes with a discussion and conclusion in section VI and VII respectively.

ADS-B Signal Integrity and Security Verification Using a Coherent Software Defined Radio

Wouter Huygen, Junzi Sun, Jacco Hoekstra
Faculty of Aerospace Engineering,
Delft University of Technology,
Delft, the Netherlands

***Abstract*—Automatic Dependent Surveillance – Broadcast (ADS-B) is an operational enhancement as part of next-generation air transportation systems in Air Traffic Control. It enables aircraft and airport vehicles to periodically broadcast the information from their on-board equipment, like their identification, GPS location, velocity, and intent. Compared to classical radar surveillance, the service implementation has increased the renewal time, reduced costs, and increased safety and accuracy already. Nowadays, Mode S 1090 Extended Squitter is the most predominant adopted technology ADS-B service implementation. However, the ATC system has not been developed with security in mind and is vulnerable to a number of different radio frequency attacks by malicious parties. ADS-B is planned for long-term use but lacks the minimal and necessary inherent security integrity mechanisms. This study suggests a possible and cost-effective solution that improves the security and integrity of raw ADS-B signals by designing a tool which can verify and validate the low-level signal. In this paper, in order to mitigate the threat of maliciously injected signals, a method is proposed where two variables of direction of arrival are independently determined using a multi-channel coherent receiver. First, a calculated angle using signal decoding and trigonometry and secondly, an estimated angle using phase relationships and spatial correlation. Finally, an integrity verification method has been proposed and successfully applied.**

***Keywords* –** ADS-B integrity verification, Malicious attacks, Injection, Direction of arrival estimation, Coherent KerberosSDR, ADS-B, Mode S, 1090 MHz

I. Introduction

Automatic Dependent Surveillance - Broadcast (ADS-B) is a well-performing operational enhancement in Air Traffic Control (ATC) applications. It enables aircraft and airport vehicles to periodically broadcast the information from their onboard equipment, like their identification, status, GPS location, velocity, and intent [1]. As a result, the ATC can use it for surveillance purposes, and additionally, spacing and separation are enabled for airborne traffic [2]. The system is part of a trend to modernize the ATC, where over many years, the ATC has made a move from independent and uncooperative to dependent and cooperative surveillance systems [3]. The service implementation is a dependent surveillance system containing two services: 1) 'ADS-B out' the capability to broadcast the equipped aircraft parameters and 2) 'ADS-B in' the capability to receive information from nearby aircraft [4]. In May 2010, the Federal Aviation Administration (FAA) [5] set up the ADS-B performance requirements and technical amendment. In that final rule, the FAA set the equipment requirements of ADS-B mandatory for certain air spaces classes by January 1, 2020.

Nowadays, ADS-B 1090 Mode S Extended Squitter (ES) is the most predominant adopted technology ADS-B service implementation and has increased the renewal time, reduces costs, and increases safety and accuracy already in comparison to classical radar surveillance [4]. However, ADS-B is developed for long-term use but lacks the necessary inherent integrity check mechanisms. The ATC system has not been made with a security ground and is vulnerable to multiple radio frequency attacks by malicious parties. The different vulnerabilities are commonly described in the literature, and many potential feasible countermeasures are proposed. For instance, according to Manesh et al. [6], compared to classical radar surveillance, the two fundamental disadvantages are: 1) dependency on onboard derived navigation data, and 2) the open and straightforward ADS-B protocol. Nowadays, regulations are the primary prevention method for this lack of security since there are no feasible implemented mechanisms for verifying the integrity of navigation parameters in the current ADS-B protocol [7]. Multiple studies have mapped the vulnerabilities and proposed/developed technical mitigation techniques. However, to become part of the ADS-B protocol and global standard, these are yet to prove their effectiveness.

This study's main objective is to suggest a possible and cost-effective solution, which improves the security and integrity of raw ADS-B signals, by designing a tool that can verify and validate the low-level signal. This general purpose is defined to mitigate the security drawbacks of the ADS-B protocol by exploring characteristics of low-level signals. However, to define the area to be explored, a scope is set, where only the malicious frequency attack, message injection, is taken into account. The related work part of this paper discusses this scope more thoroughly. Subsequently, a method is proposed where two variables of the direction of arrival are independently determined using a multi-channel coherent receiver. First, a calculated angle using signal decoding and trigonometry and secondly, an estimated angle using phase relationships and spatial correlation. In order to prove the concept, experiments are done using real raw ADS-B data (1090 MHz) collected by a multi-channel receiver located in Delft, the Netherlands. Note, due to governmental regulations, the transmission of the raw signal is done at a different frequency. Lastly, the methods and analysis are limited to a one-year duration of the study.

The paper is structured as follows: section II provides an overview of the state-of-the-art previous and related work, followed by the methodology (section VI), containing the proposed solution, the experimental setup, and related technical content for the proposed solution. The method used for signal integrity verification is defined in section IV. In section V the results of the experiments are shown. The paper concludes with a discussion and conclusion in section VI and VII respectively.

II. Related Work

The state-of-the-art of previous and related work is summarized in this section to suggest a mitigation method for malicious injection in ADS-B networks. First, relevant knowledge about the ADS-B protocol is outlined. Secondly, an overview of the vulnerabilities and potential threats identified from the literature are presented, followed by the current state-of-the-art taxonomy of ADS-B security. Finally, although this study is scoping on malicious injection, multiple security drawbacks and mitigation methods are considered in this section. The information is valuable to find a feasible candidate method to mitigate malicious ADS-B signal injection.

A. Background of the ADS-B protocol

Automatic Dependent Surveillance - Broadcast is a satellite-based surveillance system used for ATC purposes, which operates dependently and cooperatively. Using the Global Navigation Satellite System (GNSS), accurate navigation data, including GPS position and velocity, are processed and transmitted by the ADS-B transmitter via the 1090ES/UAT data link. ATC, ground stations, and neighbor aircraft can receive and process the data via the 'ADS-B in' and 'ADS-B out' data-link [8]. This service implementation enhances pilot, and air traffic control services situational awareness, in-flight collision, runway incursion avoidance, and precise air traffic control surveillance in areas without radar coverage [6].

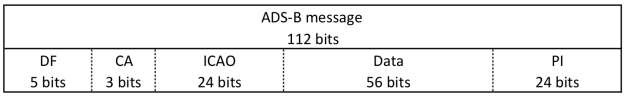

Fig. 1. ADS-B message structure

A standard message format has been established for the ADS-B 1090ES protocol. This message consists of a five-part 112-bit long structure. In figure 1, the schematic overview of this structure is shown, divided into five blocks. The first 5 bits are used for the down-link format (DF). Typically, the 1090 Mode S ES uses DF = 17 or 18, which means the 56-bit data block is permitted [9]. The following block (6-8 bits) is used for capabilities (CA) of the mode S transponder, such as the additional identifier. The following 24-bit block contains the aircraft address field. From this part of the message, the ICAO address can be decoded, used for aircraft identification. The information from the on-board systems is located, from 33 bit till 88 bit, in a 56-bit data block. The last 24-bit long data block is used for parity and interrogator ID (PI) [6].

ADS-B 1090 ES signal messages have DF 17 or 18. The type code (TC) can identify the information contained in the ADS-B signal. For instance, an aircraft identification message has TC 1 to 4. For airborne position and airborne velocity determination, TC 9 to 18 and TC 19 are used, respectively [9].

B. The security issue of ADS-B

As stated in the introduction, this study scopes on countermeasures to malicious injection in ADS-B networks. While regulation is the primary method to prevent this incidence, some of the security drawbacks can be mitigated by exploring the characteristics of the low-level signal. To understand the relevance of this problem, Manesh et al. [6] have presented an overview of the ADS-B risk analysis by considering the likelihood of an attack and its potential impact. This overview is reprinted below in table I and shortly explained below.

TABLE I
ADS-B risk analysis - Based on [6]

		Attack Impact		
		Low	Medium	High
Attack Feasibility	High	Eaves-dropping (Low Risk)		
	Medium		Jamming (Medium-High Risk)	Message Injection (High Risk)
	Low		Message Deletion (Medium Risk)	Message Modification (Medium-High Risk)

Eavesdropping is a passive attack where the malicious attacker can listen to the unencrypted and unsecured broadcasted messages causing privacy concerns [4]. Jamming is an active attack method, where a ground station or aircraft is disabled from its operation (sending and receiving messages) by adding a signal with sufficiently high power, and the same frequency into the network [7]. According to McCallie et al. [10], message deletion is an attack method to 'delete' legitimate messages from the carrier frequency. Message modification can be described as changing the message's content [6]. Lastly, Leonardi et al. [4] defined message injection as the intentional transmission of non-legitimate ADS-B signals on the same frequency and encoded following the ADS-B protocol using erroneous information. This results in displaying false aircraft in ATC applications. Due to its relatively high attack feasibility and impact, countermeasures for injection are a valuable part of the state-of-the-art knowledge body. This is endorsed by McCallie et al. [10], who also stated that the combination of multiple attacks could create more complex attacks. However, combined attacks have a lower attack feasibility since those are much more challenging to perform.

C. Related work on countermeasures of ADS-B injection

The described vulnerabilities are commonly described in the literature, and many potential countermeasures are proposed. According to Stomeiher et al. [7], [11], the state-of-the-art

of ADS-B security research is currently divided into two approaches: secure broadcast authentication and secure location verification. Multiple researchers use this distinction as the baseline of their research problems or literature reviews [12].

In figure 2, the blue blocks overview the main research fields in the current state-of-the-art of countermeasures for ADS-B security threats. This taxonomy is partly reprinted from [7].

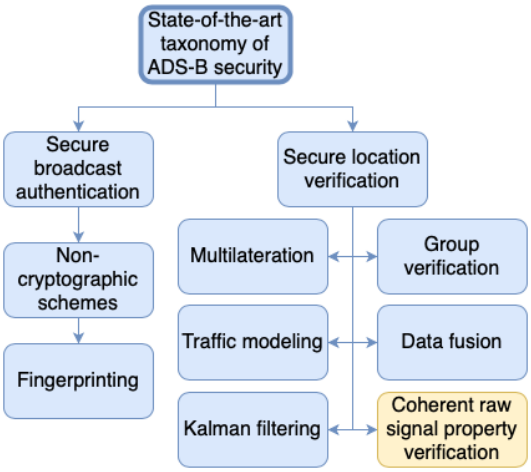

Fig. 2. ADS-B security research taxonomy [7]

Since both the pictured research fields and proposed solutions can be relevant topics, a short overview of some related work is given below in chronological order:

In 2006, Baud et al. [13] proposed a method called data fusion. This is a common technique using multiple independent data sources to obtain higher accuracy than using one single data source. The author applied position verification by using data from classical radar systems.

In 2006, Leinmüller et al. [14] used traffic modeling for signal verification, using the derivation of the next states of the flight path based on earlier known states. The estimation of the flight path can be validated between multiple ground stations to validate the position claims. The author concludes that traffic modeling can detect deviations from standard ADS-B profiles containing flight behavior.

In 2010, Sampigethaya et al. [15] proposed a method using group verification to verify the broadcasted ADS-B position. The concept is to verify the location of a single aircraft by a group of aircraft flying in coalition. For instance, in the proposed method, multilateration is used to verify the position information. When an aircraft's position message is received by four or more aircraft, the position can be estimated based on the time difference of arrival.

In 2012, Kovel et al. [16] did a comparative analysis of using Kalman filtering techniques to assess its performance on location verification. A distinction has been made between Kalman filtering the ADS-B position messages, Kalman filtering the signal strength and direction on the antenna, and Kalman filtering the on-board aircraft signal for real-time position verification. Scoping on the last one, the verification method using Kalman filtering involves sorting out missing or noisy ADS-B messages to estimate the aircraft's state. Kovel et al. conclude that the method can distinguish the particular features of the flight path. This enables the mitigation of data with physically impossible flight paths.

In 2012 Johnson et al. [17] use wide-area multilateration in challenging areas, where robust power and communication are not available. Performance results show that wide-area multilateration is a robust and adaptable surveillance solution when the network is set correctly.

In 2015, Monteiro et al. [12] implemented wide-area multilateration as a mitigation tool for malicious attacks. The author proposed a method based on known GPS errors and clock precision inaccuracies. First, a receiver placement optimization using multilateration was established to increase the accuracy of the coverage area. Then, a reliability evaluation of the ADS-B position message is done for two specific cases. 1) A legitimate and present aircraft and 2) the same legitimate and present aircraft forging false position messages.

In 2017, Zeng et al. [18] categorizes different fingerprinting techniques into three parts: 1) software-based fingerprinting, 2) hardware-based fingerprinting, and 3) channel-based fingerprinting. Software-based fingerprinting is specifically based on the unique characteristics of the protocol software. Hardware-based fingerprinting is based on the unique properties of waveforms caused by the chosen hardware. Moreover, channel-based fingerprinting has its groundwork in channel state information and signal strength. It is proven that wireless signals decorrelate rapidly in space, so a physical layer algorithm could determine whether multiple signals are from the same source.

These different approaches could potentially be helpful for the mitigation of malicious signal injection. However, to become part of the ADS-B protocol and global standard, most of these methods are yet to prove their effectiveness. In the literature, most proposed solutions require changes in the ADS-B protocol or changes in the existing hardware, entailing high costs. Part of the objective is to find a cost-effective solution.

D. A software defined radio approach

In several ADS-B signal processing researches, Software Defined Radio (SDR) approaches are used. Jondral et al. [19] provide a brief overview of the concept and development of the SDR and describes the system as a radio communication system in which the components, traditionally implemented in hardware, are implemented as software radio. According to Piracci et al. [20], an SDR permits flexibility and modularity for the easy development of prototypal devices for evaluation and testing cost-effective novel enhancements for ADS-B receivers. The author tests a multi-channel SDR approach by testing an algorithm to generate 1090 MHz ADS-B signals and interference, such as noise and jamming.
Following [21] and [22], Software-Defined-Radios are proven successful in ADS-B signal processing. Having multiple channels available enables additional signal properties to process

ADS-B signals, which can be used, for instance, for Direction of Arrival (DOA) estimation. Since the DOA can also be calculated via signal decoding, the described DOA estimation techniques enable another independent correlating variable, making DOA estimation potentially useful for ADS-B signal validation and verification. Using DOA estimation could be a feasible candidate to mitigate malicious ADS-B signal injection. In 2012, Reck et al. [23] already published about verification of ADS-B positioning by direction of arrival estimation. They objected to filter out error-prone caused by wrong information coming from on-board systems. In 2020, Li et al. [24] used a coherent SDR (KerberosSDR) to estimate the heading angle of a drone transmitting at a particular frequency.

The validation and verification of decoded ADS-B messages for integrity and security reasons using a low-cost coherent SDR is potentially useful. Using the direction of arrival might be a feasible candidate to mitigate the threats of malicious ADS-B signal injection. To the best of knowledge, nobody has done this before, using a low-cost coherent SDR. In figure 2, the yellow block is added as a potential mitigation method under secure location verification.

III. Methodology

This section contains the proposed solution based on the main research objective and related work part. Furthermore, the experimental setup and supporting technical content for the proposed solution are described more thoroughly. The corresponding theoretical content has been divided into four main subjects. To start with signal (pre-)processing and analysis, followed by ADS-B signal decoding and position interpolation. Thirdly, the DOA calculations based on the claimed GPS positions are explained, and finally, the DOA estimation methods for multi-channel antenna arrays. Note the made distinction between the calculated DOA and the estimated DOA. These two independent procedures to obtain an angle are used to verify and validate the signal.

A. Proposed method

The concept proposed in this study is to use the claimed positions of aircraft and the receiver's known position to calculate the incoming direction of arrival of the signal. For integrity verification reasons, a second calculation of the direction of arrival is provided using the characteristics of the coherent signal. In figure 3, an overview of the research methodology has been pictured schematically. Using a coherent SDR, incoming ADS-B signals can be registered and decoded. The signals containing a position message can be used to estimate the broadcast position of the signals not containing a position message. Thus, for each incoming signal, two uncorrelated values of the DOA in degrees can be determined. In addition, a method for reliability classification is implemented to calculate a confidence rate for each signal to validate the claimed position based on the DOA. All corresponding methods for both data handling and verification reliability are explained more thoroughly in second part of this section.

B. Experimental setup

To validate the performance of the chosen method and the developed validation and verification model, there is chosen to conduct an experiment using real ADS-B data. Using actual ADS-B data and different attack scenarios enables a realistic and comparable environment to potential injection threats in the operation of ADS-B. Below, a schematic overview of the experimental setup is shown in figure 4. The experiment's goal is to prove the practical implication of the concept described in the previous section. Therefore, two malicious injection attack scenarios are established. These scenarios can be simulated realistically by rebroadcasting earlier received signals.

- Static message injection: A signal is transmitted from a set location. The reference between the transmitter and the receiver is constant. There can be assumed that the attacker can create correctly formatted ADS-B messages, covering the correct message types, message order, legitimate, and reasonable flight parameters.
- Dynamic message injection: A signal is transmitted from a moving object. The reference between the transmitter and receiver is not constant. For this threat, the same assumption as for static message injection can be made.

For this experiment, there is chosen to make use of the Othernet's KerberosSDR Board - 4 Channel Coherent RTL-SDR. This multi-channel receiver enables multiple new options for data handling and allows receiving of ADS-B signals

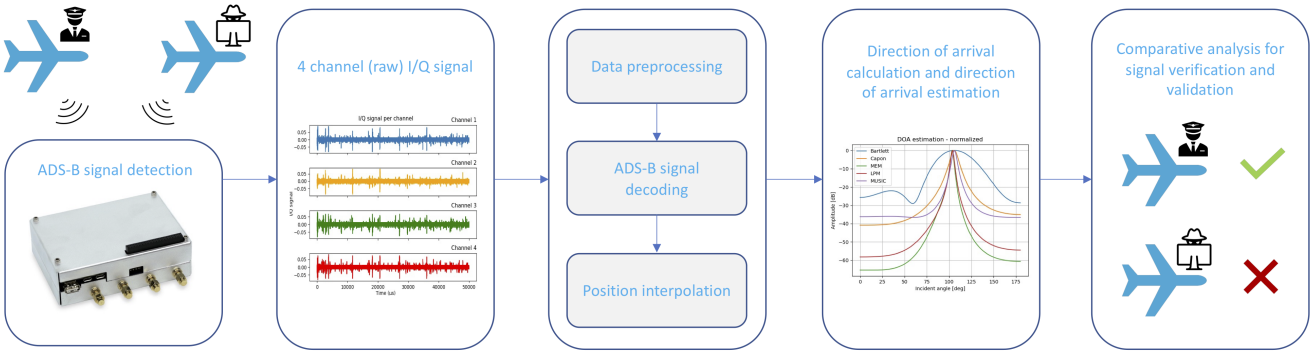

Fig. 3. Schematic research overview

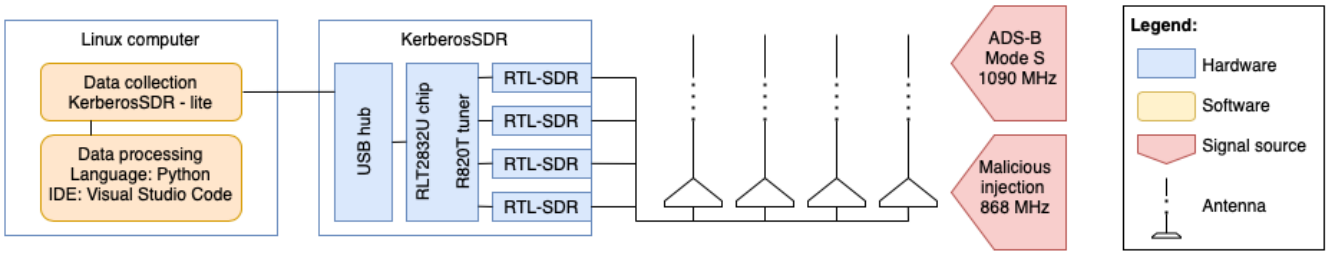

Fig. 4. Schematic overview of experimental setup.

at 1090MHz. Furthermore, an 868 MHz transmitter is needed to conduct the experiment, since broadcasting at 1090MHz is obligated by law. Chosen is to use a LimeSDR 868 MHz single-channel transceiver.
The software tools are mainly Python-based or can make or read the same data formats. The signal processing software - KerberosSDR Lite - is used to save raw signal data from a multi-channel software-defined radio and has been established for the chosen hardware.

C. Antenna array setup

Both the KerberosSDR hardware developer [25] and Zuokun Li et al. [26] describe two possible antenna setups and their advantages and disadvantages. The two antenna setups are uniform linear array (ULA) and uniform circular array (UCA). The ULA setup contains four omnidirectional antennas placed in a straight line in an equidistant manner. In figure 5, a schematic overview of the setup is shown, where the inter-element spacing (d) can be determined by $\lambda * s$. Here λ is the frequency wavelength, and s is the interelement spacing factor. To avoid ambiguities, the possible calculation of multiple directions, $s = 0.33$ is used [25]. The ULA setup enables the one-dimensional direction of arrival estimation. This means the heading or pitch angle of the signal source with regards to the antenna's position can be estimated [25].

The UCA setup contains four omnidirectional antennas placed in a circular or squared setup. In figure 6, a schematic overview of the setup is shown. Like the ULA setup, the interelement spacing (d) can be determined by $\lambda * s$, with the same restrictions as ULA for the interelement spacing factor s to avoid ambiguities. In addition, the UCA setup enables the three-dimensional direction of arrival estimation [25].

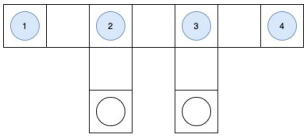

Fig. 5. Uniform linear array setup

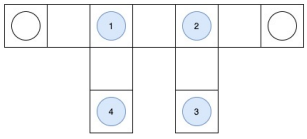

Fig. 6. Uniform circular array setup

Two disadvantages of the ULA setup are the resolution of 180 degrees and its ability for the one-dimensional DOA estimation. In other words: the setup cannot determine whether the signal transmitter is coming from the front or behind of the setup, and the setup allows (heading) DOA estimation under the assumption that the signal has a pitch angle of 90 degrees. This assumption is made due to the distance between the receiver and transmitter. Therefore, there can be expected that this setup will not work appropriately for closeby aircraft.

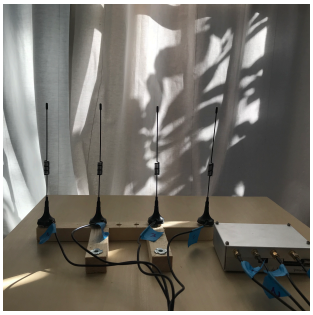

Fig. 7. Uniform linear array setup

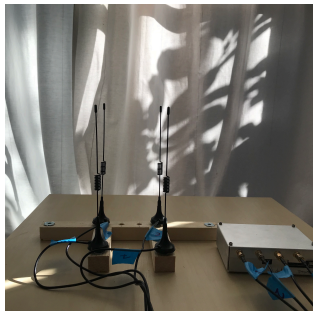

Fig. 8. Uniform circular array setup

On the other hand, the UCA setup is more vulnerable to multipath effects, which obviously could produce more wrong information. Zuokun Li et al. prefer the ULA setup to be used instead of the UCA setup. Moreover, the ULA setup gives the bearings less affected by multipath effects [25], [26]. Multipath effects occur when signals reflect on surrounding objects, causing the appearance of signals coming from another direction. Figure 7 and 8 show the receiver and antenna setups used in this research. Note that the pictures are made inside a building, but during the experiments the antenna setup was located outside to limit the multipath effects.

D. Signal (pre-)processing and analysis

Using the four-channel coherent SDR, a (*4* x *number of samples*) complex data set is generated, which allows signal (pre-)processing and analysis. This includes decoding and raw signal properties analysis. Below a received sample of incoming I/Q signal (100000 samples) has been pictured in figure 9:

Using the PyModeS library [27] in Python, the intermittent signals can be selected (using the amplitude and phase jumps) and decoded. Equations 1 and 2 are used to calculate the amplitude [dB] and phase [rad] respectively [28], [29]. Here, I and Q are the in-phase components of the incoming I/Q signal (real and imaginary parts). This results in the following amplitude and phase plot for one channel.

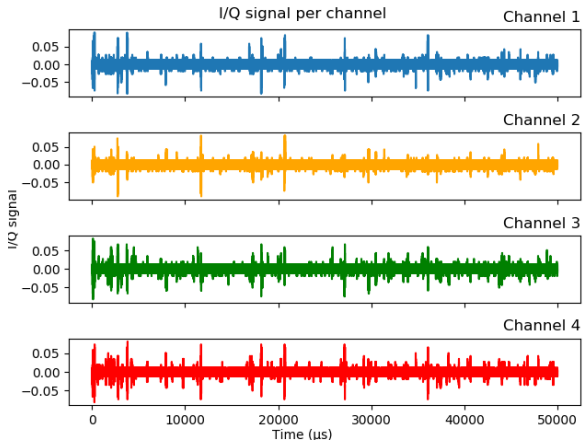

Fig. 9. 100000 samples of incoming I/Q signal at 1090MHz.

$$amplitude = \sqrt{I^2 + Q^2} \tag{1}$$

$$phase = tan^{-1}(\frac{Q}{I}) \tag{2}$$

E. Signal decoding and position interpolation

For decoding ADS-B and Mode S data, the open available Python library pyModeS [27] is used. The identification-, velocity- and position-message can be decoded from the signal using this library. By calculating the amplitude and phase, a significant jump or shift can separate the single signals. Not only error-free messages can be used, which generally can cause a significant loss of signal.

The decoded position messages provide coordinates in the EPSG:4326 WGS 84 decimal notation coordinate system. There is chosen to convert these values to a (Cartesian) EPSG:3034 coordinate system. Coordinate conversion is done for two reasons: 1) to get more accurate results of the direction of arrival calculations, and 2) the position interpolation in meters is more practical due to the unit of the velocity parameter.

Since only position messages provide position information to calculate the DOA, a method called 'kinematic path interpolation for movement data' is used to calculate the position of the other received messages. Just like the position messages, all messages have a known time of arrival. The assumptions made are that the travel time of the signals is identical for each signal, and that the velocity information can be saved for the next position message. This can be assumed due to the short time intervals. To define the actual flight path the two dimensional kinetic motions in one time step are used in forms: position: $\mathbf{z}(t) = (z_x(t), z_y(t))$ and velocity: $\mathbf{v}(t) = (v_x(t), v_y(t))$ and an array with the actual time stamps of the other incoming signals. The following equations (3, 4 and 5) are used to solve the actual flight path.

$$position : \mathbf{z}(t) = \mathbf{z}(t) + \int_{t1}^{t2} \mathbf{v}(t)\, dt \tag{3}$$

$$velocity : \mathbf{v}(t) = \mathbf{v}(t) + \int_{t1}^{t2} \mathbf{a}(t)\, dt \tag{4}$$

$$acceleration : \mathbf{a}(t) = \frac{\Delta \mathbf{v}}{\Delta t} = \frac{\mathbf{v} - \mathbf{v}_0}{\Delta t} \tag{5}$$

An example of performing kinematic path interpolation for one flight is shown in figure 10. Here the green dots are the received position messages, and the blue dots are the calculated positions of the other incoming signals from the same aircraft. Using these positions, the DOA per signal can be calculated.

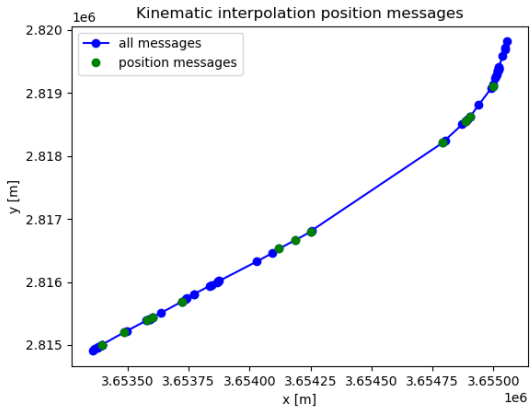

Fig. 10. Example flight path, where kinematic interpolation has applied

(*Note the distinction made between the calculated DOA and the estimated DOA, both in degrees, in subsections III-F and III-G*)

F. Direction of arrival calculation

In order to calculate the angle of arrival from the claimed position in the ADS-B position message, equation 6 can be used. Here is θ the direction of arrival, δx the distance in x-direction and δy the distance in y-direction between the transmitter and receiver, which can be calculated using $(x_{aircraft} - x_{receiver})$ and $(y_{aircraft} - y_{receiver})$, respectively. The arctan2-function returns the angle in the plane between the positive x-axis and the ray between the transmitter and receiver. Its functionality is described more thoroughly below equation 6 [30].

$$\theta = \text{atan2}(\delta y, \delta x) \tag{6}$$

, where:

$$\text{atan2}(y, x) = \begin{cases} \arctan(\frac{y}{x}) & \text{if } x > 0 \\ \arctan(\frac{y}{x}) + \pi & \text{if } x < 0 \text{ and } y \geq 0 \\ \arctan(\frac{y}{x}) - \pi & \text{if } x < 0 \text{ and } y < 0 \\ +\frac{\pi}{2} & \text{if } x = 0 \text{ and } y > 0 \\ -\frac{\pi}{2} & \text{if } x = 0 \text{ and } y < 0 \end{cases}$$

To obtain the right angle value, in the same reference as the reference of the direction of arrival estimation, the results must be corrected. For both the ULA and UCA setup, the reference axis is the positive y-axis instead of the positive x-axis, so the correction is a 90 degrees subtraction from the calculated angle. For the ULA setup, a correction has to be done for the resolution of 180°. This results in the following mathematical equations (7, 8):

$$\theta_{ULA} = 180^\circ - \theta, \text{ for } \theta \leq 180^\circ \tag{7}$$

$$\theta_{ULA} = \theta - 180^\circ, \text{ for } \theta > 180^\circ$$

$$\theta_{UCA} = \theta - 90^\circ, \text{ for } 0 > \theta > 360^\circ \tag{8}$$

G. Direction of arrival estimation

Based on different signal properties, multiple methods are available to estimate the direction of an incoming propagating wave source relative to a set of antennas. The DOA estimation is also known as spectral-, angle of arrival- or bearing estimation. These techniques are widely applied in research areas of time series analysis [31]. Using a received sample of the output of an antenna array with N antennas, the DOA can be estimated for the investigated direction angles. Bhuiya et al. [32] describe the working principle of some applicable methods: the elements of the antenna array collect signals from a propagating wave source at a different time due to the spacing of the antenna array. Here, the first antenna is used as the reference point. Assuming the incoming signal is narrowband, the delay of arrival can be defined as phase shift. The total signal and noise received by the antenna array can be expressed as in equation 9, where **x**(t) is a N x *number of samples* array.

$$\mathbf{x}(t) = \mathbf{a}(\boldsymbol{\theta})\mathbf{S}(t) + \mathbf{n}(t) \tag{9}$$

Here, $\mathbf{a}(\boldsymbol{\theta})$ denotes the steering matrix with angles $\boldsymbol{\theta}$, $\mathbf{S}(t)$ denotes the signal column vector and $\mathbf{n}(t)$ the uncorrelated additive white Gaussian distributed noise vector. Note that in this study noise vector is assumed to be constant. The total signal an noise received per antenna (N^{th} element) at time *t* can be found in equation 10 below.

$$x_N(t) = S(t) \sum_{k=1}^{K} e^{j(N-1)\mu_i} + n_N(t) \tag{10}$$

With the spatial correlation matrix $\bar{R}_x$ and the scanning vector of the array $\bar{a}$, the earlier mentioned DOA estimation algorithms could be implemented. The software has an implementation based on the earlier mentioned PyArgus library [33]. However, there is no conclusion yet on the accuracy of the DOA implementation using this library.

Five methods for DOA estimation are described in the next section, and the calculations require knowledge about the spatial direction, signal gain, and expected phase relations:

1) Spatial correlation matrix: The first input element to be calculated is the spatial correlation matrix $\bar{R}$. This matrix contains the correlation of the spatial direction of the signal and the average receiver signal gain. For each number of samples (one complete ADS-B signal) found using the PyModeS library, the raw N-channel I/Q signal ($\mathbf{x}(t)$) can be transformed into the spatial correlation matrix by using equation 11:

$$\bar{R} = \frac{1}{N} \sum_{0}^{N-1} \mathbf{x}(t) \cdot \mathbf{x}(t)^H \tag{11}$$

In the case of a four-channel coherent SDR, for each sample of the multi-channel raw signal, this results in a spatial correlation matrix with size 4 x 4.

2) Steering matrix: The second input element to be calculated is the steering matrix. Bhuiya et al. [32] describes the steering matrix as m steering arrays, where each array contains the expected phase relationships for all channels. The steering arrays are defined to store the expected phase relations for the specific incident angles m. The specific incident angles are the angles within the resolution of measurements. These steering vectors are based on the interelement spacing d and the expected incident angles (θ). The ULA setup results in an array of shape N x 180, and for the UCA setup, this results in an array of shape N x 360. Using equation 12, the m*th* array element of the steering vector can be calculated. The sinus part of the exponent equals zero for the ULA setup.

$$\bar{a}(\theta_n)_m = e^{j2\pi d_x * cos(\theta_n) + d_y * sin(\theta_n)} \tag{12}$$

$\forall m = 0 \ldots (M-1)$

H. Direction of arrival estimation algorithms

A pseudo spectrum, $P(\theta)$, of the incoming signal can be determined with the required knowledge about the average signal gain, spatial direction, resolution, and expected phase relationships. This contains the relationship between the signal strength and the incident angle. Locating the corresponding incident angle of the maximum amplitude, an estimated value for the DOA can be found. Five commonly used algorithms [34], both linear DOA estimation algorithms and algorithms based on the decomposition of sub-spaces, are explained and described in the following sections. In figure 11 an example of the pseudo spectrum plot of one complete ADS-B signal for the five used algorithms is pictured. The investigated resolution is 180 degrees in this figure, and locating the maximum amplitude gives an estimated DOA value of 102 degrees.

1) Bartlett method: The Bartlett (Fourier) method consists of power spectra estimation and is known as the first developed DOA estimation technique [26]. The method provides a reduction of the variance of the periodogram in the cost of reduced resolution [35]. This is done by maximization of the output power $\bar{R}_x$ for a certain direction. Equation 13 shows the calculation of the pseudo spectrum of Bartlett's method, where $\bar{R}_x$ is the spatial correlation matrix and $\bar{a}(\theta)$ is the scanning vector of the array.

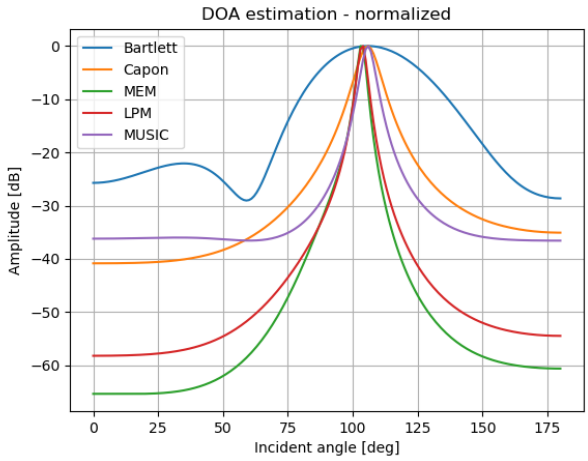

Fig. 11. Combined pseudo spectrum plot - multiple methods (normalized)

$$P(\theta) = \bar{a}^H(\theta)\bar{R}_x\bar{a}(\theta) \tag{13}$$

A main limitation of Bartlett's methods is the ability to solve the angles is limited by the array half-power beam width [36].

2) Capon's method: Capon's method is also known as the maximum variance distortionless response. The method is a maximum likelihood estimate of the power arriving from one direction (θ) [37]. This is done while considering that all other sources are considered as interference. The signal to interference ratio had to be maximized while passing the source signal undistorted in amplitude and phase [34]. Equation 14 is the pseudo spectrum of Capon - or maximum variance distortionless response - method, where $\bar{R}_x$ is the spatial correlation matrix and $\bar{a}(\theta)$ is the scanning vector of the array.

$$P(\theta) = \frac{1}{\bar{a}^H(\theta)\bar{R}_x^{-1}\bar{a}(\theta)} \tag{14}$$

Godara et al. state that the method has better resolution properties than the earlier described Bartlett method [35].

3) Burg's Maximum Entropy Method: To implement Burg's Maximum Entropy Method (MEM), a power spectrum has to be found such that its Fourier transform equals the measured correlation. This correlation is subjected to the maximized entropy constraint [38]. Equation 15 is the pseudo spectrum of Burg's maximum entropy method, where $\hat{\bar{w}}$ is the weight of the optimal beamformer and $\bar{q}(\theta)$ is a vector denoting outputs of auxiliary beams of a beam-space processor. The number of outputs equals the number of dimensions of the vector $\bar{q}(\theta)$ [35].

$$P(\theta) = \frac{1}{\hat{\bar{w}}^T\bar{q}(\theta)} \tag{15}$$

Godara et al. state that the method has better resolution properties than the earlier described Bartlett and Capon method. Additionally, this method can estimate the direction of arrival with a lower signal-to-noise ratio [35].

4) Linear prediction method: Linear prediction method (LPM) is a method, which estimates the output from one antenna using linear combinations of the other antenna outputs. The mean square error between the estimation and the true output is minimized [36]. Equation 16 is the pseudo spectrum of LPM, where $\bar{R}_x$ is the spatial correlation matrix, $\bar{a}(\theta)$ is the scanning vector of the array and $\bar{u}_m^T$ is the Cartesian basis vector, which is chosen for prediction.

$$P(\theta) = \frac{\bar{u}_m^T\bar{R}_x^{-1}\bar{u}_m}{\left|\bar{u}_m^T\bar{R}_x^{-1}\bar{a}(\theta)\right|^2} \tag{16}$$

Islam et al. described the LPM has again a higher resolution than all the other methods described above (Bartlett, Capon, and MEM) [34].

5) Multiple Signal Classification: Multiple Signal Classification (MUSIC) is described as an efficient eigenstructure variant. The estimation of the direction of arrival, number of signals and signal strength [35]. Equation 17 is the pseudo spectrum of MUSIC method, where $\bar{E}_N$ is the noise subspace eigenvector and $\bar{a}(\theta)$ is the scanning vector of the array.

$$P(\theta) = \frac{1}{\bar{a}(\theta)\bar{E}_N\bar{E}_N^H\bar{a}(\theta)} \tag{17}$$

In the above-written part, the equation needs a calculation of the noise subspace eigenvectors, which can be determined from the spatial correlation matrix. Equation 18 is the equation to apply, where D is the number of signals, and M is the number of array elements.

$$E_N = [e_1 e_2 ... e_{M-D}] \tag{18}$$

IV. Reliability Model

Monteiro et al. [12] have proposed a method for reliability classification for two estimated values in order to validate claimed ADS-B information. In their study, the validation of the claimed ADS-B position is done by a comparative analysis using position information estimated by using multilateration. However, the method used for the verification reliability classification can also be applied in this study. Using the estimated angle of arrival to verify the calculated angle of arrival based on the claimed ADS-B position information.

A. Error in the calculated DOA

The error found in the calculated angle of arrival is caused by a GPS error $\overrightarrow{G} = (g_x, g_y)$ of the transmitter and the receiver. In this case, the GPS error is a standard deviation in meters, typically provided by the equipment manufacturer. It is assumed to have a Gaussian distribution with zero mean and variances σ^2 [39].

In order to find the standard deviation of the calculated direction of arrival, there is chosen to sample equation . Since the direction of arrival calculations are dependent on the GPS position of the receiver and transmitter, these two values can be sampled using a Gaussian distribution. As described by Schäfer et al. [39] there can be assumed that GPS observations are Gaussian distributed with zero mean and variances σ_{gps}^2.

Typically, the GPS error is provided by the manufacturer of the equipment. However, the standard deviation of the GPS parameter is set as $\sigma = 30$ m [12]. By using a Monte Carlo simulation, the histogram and corresponding standard deviation (σ) of the angle calculation can be found and is pictured in figure 12.

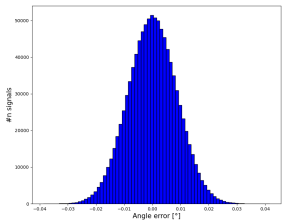

Fig. 12. Calculated DOA error

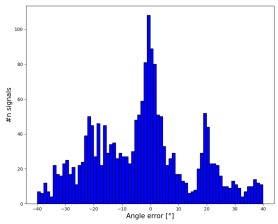

Fig. 13. Estimated DOA error (Bartlett algorithm)

B. Error for direction estimation

In figure 13, the histogram of the error from the estimated direction of arrival (Bartlett algorithm in this case) is pictured. There is no clear conclusion possible on the behavior of the error distribution yet. However, based on [23] there can be assumed that the errors of the estimated DOA, using the DOA algorithms, have the characteristics of a Gaussian distribution. Therefore, using a normal fit function in Python, the standard deviation can be determined, and the corresponding results are for all five algorithms presented in table II in section V (Experiments and Results).

C. Verification reliability classification

As mentioned in the previous section, the reliability classification method used in this study was earlier proposed by Monteiro et al. [12] with a slightly different application. In this research, the estimated direction of arrival ($\theta_{estimation}$) parameter is used to validate the calculated direction of arrival ($\theta_{calculation}$). The absolute error between the two independent parameters for each incoming signal (n) can be calculated using equation 19.

$$z_n = |\theta_{estimation} - \theta_{calculation}| \tag{19}$$

As found in the previous section both $\theta_{est.}$ and $\theta_{cal.}$ are Gaussian distributed with zero mean and variances $\sigma^2_{\theta_{est.}}$ and $\sigma^2_{\theta_{cal.}}$, respectively. Therefore, the standard deviation of both distributions can be expressed as $\sigma = \sigma_{\theta_{est.}} + \sigma_{\theta_{cal.}}$. Consequently, the probability density function of random variable $Z_n = z_n$ can be described as a half-normal distribution due to the absolute values taken from two Gaussian distributed parameters. This distribution can be expressed as in equation 20. The corresponding cumulative distribution function can be found underneath in equation 21.

$$f_{Z_n}(z_n;\sigma) = \frac{\sqrt{2}}{\sigma\sqrt{\pi}} \exp\left(-\frac{z_n^2}{2\sigma^2}\right), z_n > 0 \tag{20}$$

$$F_{Z_n}(z_n;\sigma) = \text{erf}\left(\frac{z_n}{\sigma\sqrt{2}}\right) \tag{21}$$

Similar to Monteiro et al. [12] the confidence rate can Γ of a measurement z_n can be retrieved from equation 22.

$$\Gamma(z_n) = 1 - 0.5\left[\arctan\left(\frac{z_n - z_n^{max}}{\delta}\right) + 1\right] \tag{22}$$

Where δ is the spacing factor which can be explained as the derivative of reliability, and z_n^{max} is a point of the curve at which a change in the direction of curvature occurs (equation 23), with ϵ defined as the occurring error rate of wrong classification. The typical value of ϵ is 10^{-3}.

$$z_n^{max} = \text{erfc}^{-1}(\epsilon)\sigma\sqrt{2} \tag{23}$$

V. Experiments and Results

Based on the data collected, signal processing, and the conducted experiments, this section gives an overview of the model's performance and some examples of applying the model of the proposed message injection mitigation method.

Note that during the experiments, the real ADS-B signals are received at 1090MHz. However, due to governmental regulations, the malicious transmitting experiments are done at 868MHz. Recommended by the manufacturer of the KerberosSDR, the interelement spacing factor (s) is set to 0.33. Calculating the interelement spacing (d) in meters (using: $d = \lambda * s$) gives $d = 0.0908m$ for frequency 1090 MHz and $d = 0.114m$ for 868 MHz.

The overall performance of the model can be expressed using the standard deviation (σ) of the DOA error. The standard deviation is obtained using real ADS-B signal in order to determine these values. As earlier described, the values (in degrees) are determined for all five DOA algorithms and both antenna setups. The results are pictured in table II.

TABLE II
Performance table: standard deviation for DOA algorithms and antenna setups

	ULA	**UCA**
	σ_{ula}	σ_{uca}
Bartlett	64.52°	17.41°
Capon	67.96°	18.41°
LPM	65.80°	24.76°
MEM	65.80°	24.72°
MUSIC	64.43°	17.67°

Conducting the experiments should prove the practical implication of the concept described in the methodology. Next to the application using real ADS-B data, two earlier described scenarios were tested, static and dynamic injection. Here, a 1090 MHz sample of real ADS-B data was rebroadcast at 868MHz. Using the reliability classification method the following parameters were chosen: spacing factor δ = 50 and misclassification rate $\epsilon = 0.01$. Figure 14 shows an example of the results using real ADS-B data. For all five algorithms, a similar flight path is shown.

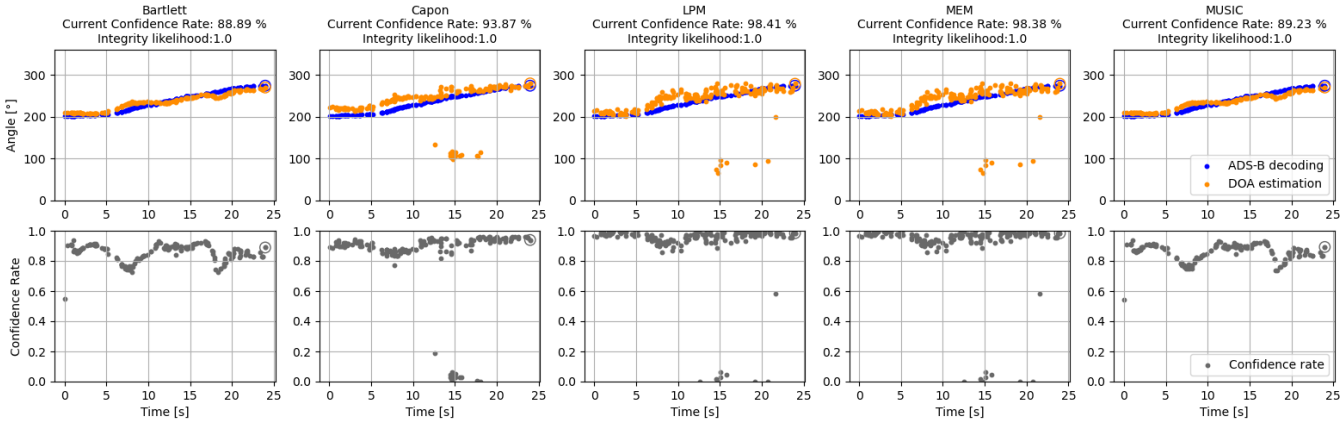

Fig. 14. Example confidence rate for different DOA algorithms for real ADS-B injection (UCA setup)

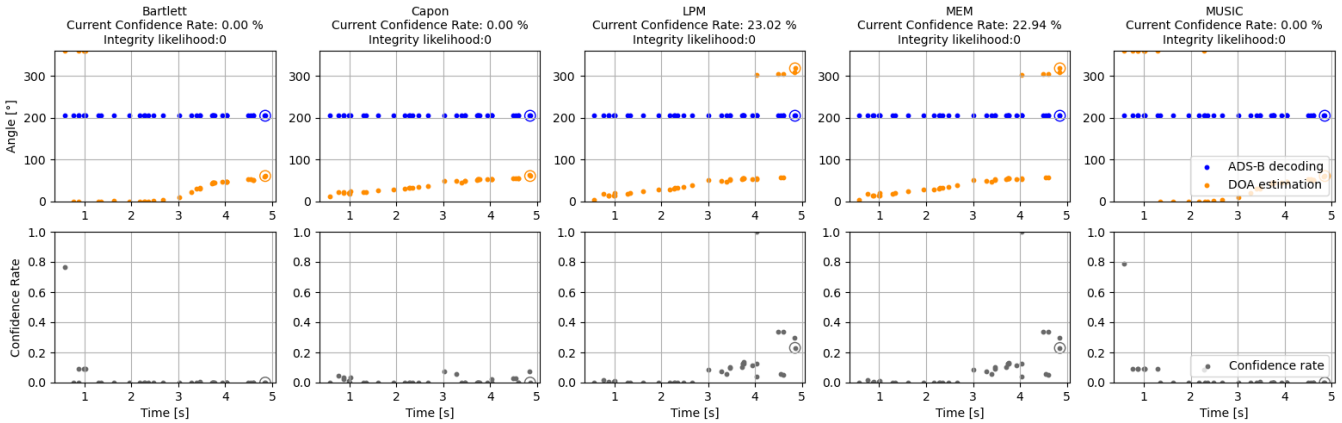

Fig. 15. Example confidence rate for different DOA algorithms for malicious signal injection (UCA setup)

In the top row, the DOA based on the claimed position (blue) and the estimated DOA (orange) are plotted against time in seconds. Each dot refers to one complete incoming ADS-B or Mode S signal. In the bottom row, the confidence rate for each signal is plotted. The current confidence rate is pictured above the figures, and the confidence rate values are nearing one.

Figure 15 shows an example of the application of the different DOA algorithms while being maliciously injected. This example contains the results of the dynamic injection scenario during the experiments. The estimated DOA values (orange) move over time, while the angle based on the claimed position remains constant. There can be seen that the given confidence rate nears zero. For the static injection scenario, the results are comparable. However, if the DOA based on the claimed position remains constant and is close to the estimated DOA, there is a probability of obtaining a high confidence rate. In actual operations, the DOA will probably not remain constant over time due to the aircraft's movement. Therefore, an additional analysis is done in order to determine an integrity likelihood over time. In other words: whether or not to confirm the integrity of a series of incoming signals from one aircraft. In figure 14, there can be found that this integrity likelihood becomes one for the real flight and in figure 15 zero for the maliciously injected flight.

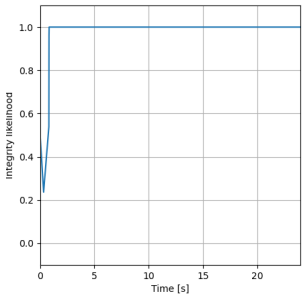

Fig. 16. Integrity verification real flight

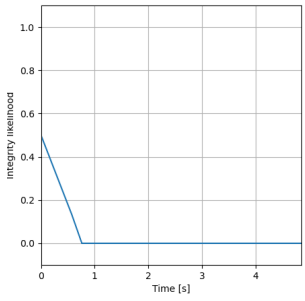

Fig. 17. Integrity verification injected flight

Using the obtained values of the confidence rate provides a conclusion on whether or not to confirm the integrity of an incoming ADS-B signal. However, misclassifications can cause wrongly verified results. Therefore, in order to get a verification conclusion for an individual flight (series of signals), as pictured in figure 14 and 15, the obtained values

of the confidence rate can be actively monitored. This is done using the confidence rate (in range 0 to 1) by first translating the values by adding 0.5, followed by a multiplication of this value by the previous one. The initial start value is set to one. If the value exceeds the upper (1.5) or lower (0.5) bound, the value will be limited to this bound. Finally, by subtracting 0.5, the calculations give a convergence over time to one for real flights (figure 16) and convergence to zero for maliciously injected flights (figure 17).

VI. Discussion

In this paper, different direction of arrival algorithms have been tested using two different antenna setups. All methods used and experiments done would benefit from further research. Due to governmental regulations, it turned out to be not realistic to set up an experiment where both real and injected ADS-B signals were received simultaneously at the operating frequency of ADS-B. This makes the standard deviation of the estimated DOA error the best indicator of the model's performance. Further research would benefit the support for possible implementation in real operations. Overall, there can be seen that the UCA setup performs much better than the ULA setup. As earlier described in section the ULA setup can only estimate the DOA in one dimension. This probably causes the high standard deviation of the DOA error. Furthermore, the results show that the Bartlett and MUSIC algorithm performs comparable and best for the UCA setup, followed by Capon's method. Looking at the results in figure 14, there can be noticed that there are signals labeled with a confidence rate nearing zero. These values are misclassifications caused by, for instance, multi-path effects and other inaccuracies of the model. Contrarily, in figure 15, the confidence rate nears one for maliciously injected signals. Also caused by several limitations of the proposed model:

First, the proposed method has been applied post-processing, which means that the model has not been implemented in real-time. Since the data collection requires large amounts of storage, the typical duration of one sample collection takes a maximum of three minutes. The primary limitation raising is that there is a relatively high data loss. To calculate the angle of the claimed position, at least one position message is required. Currently, the model can only verify the signal if position information is available. Furthermore, the application of the PyModeS toolbox, and all DOA algorithms, except for the MUSIC algorithm, limits the processing to correctly decoding only one signal at a time. This is causing more data loss, for instance, if two or more signals arrive simultaneously at the antenna array. However, using real-time processing instead of post-processing makes the proposed mitigation method more trustworthy since the measuring time is not limited to storage.

Secondly, conducting the experiments, a variance of the angle estimation was found per individual measurement. This was probably caused due to inaccuracies in the antenna setup. First, the assumption has been made that the antenna array was perfectly pointed to the magnetic north, and second, the inter-element spacing was considered accurate. However, in reality, there is probably an error in the exact positioning of the antennas. Weather and possible vibrations also contribute to this. Furthermore, during the experiments, the setup showed to be vulnerable to multi-path effects, which causes many uncertainties and must be solved for operational applications. Moreover, the sample and phase calibration of the KerberosSDR is a time-consuming process. This is because the antennas need to be manually disconnected. Adding a relay switch could improve the process. However, in April 2021, the successor of the KerberosSDR is announced [40]. Currently, in crowdfunding phase, the KrankenSDR is a 5-channel coherent capable RTL-SDR. Since this SDR has five channels, instead of four, a better accuracy is expected for the direction estimation. Also, multi-path reflections are expected to be increased. The literature describes an increase in accuracy of DOA estimation when more channels are available and the opportunity to experiment with other antenna setups, such as the trapezium or cross setup [41].

Another reason for some misclassifications, visible in the results, could be caused due to the modulation of the signals. The ADS-B protocol describes rules for the amplitude modulation of the signal but not for the phase properties and relationships. Further research is needed to determine whether certain types of transmitting equipment have phase irregularities or inconsistencies that make these kinds of DOA estimations not consistently accurate.

Finally, one of the goals of this study was to find a cost-effective method. Using a $200 coherent SDR and cheap antennas enables low cost, but the accuracy does not meet professional equipment standards. Recommended is that there can be chosen to use active antennas with more +DBI, increasing the received signal gain.

VII. Conclusion

In this paper, a possible and cost-effective solution for malicious frequency injection is proposed, which improves the security and integrity of raw Mode-S/ADS-B signals. Throughout the paper, a tool is designed, which can verify and validate the low-level signal. Using a low-cost software-defined coherent receiver, two independently determined variables of the direction of arrival of incoming ADS-B signals can be calculated. Five different direction of arrival algorithms have been tested for two different antenna setups. Furthermore, this paper shows how to apply the proposed method successfully in different experiments using real and maliciously injected ADS-B signals. Lastly, an earlier in the literature proposed reliability classifier has been applied using the standard deviations of the errors found in the experiments. In order to do this, real ADS-B data was used, and two malicious injection attack scenarios were tested for validation and verification reasons.

From the results, there can be concluded that the best performance of the model is obtained using the uniform circular antenna setup and Bartlett's direction of arrival estimation method. The corresponding standard deviation was

found 17.41 degrees. There is found that both static and dynamic injected signals can be classified as a malicious injection attack, and the integrity of real ADS-B data can be verified using the reliability model. This conclusion can be seen as a proof of concept. The used cost-effective method can be readily implemented into actual operations based on the reliability results of the real and maliciously injected signals.

Nevertheless, the limitations and recommendations show that further research is possible and could improve the model's accuracy. Future research is possible and could improve the accuracy of the model. Having found a standard deviation of 17.41 degrees, the model can be operated at a certain accuracy level in actual operations. Undoubtedly, more smart or combined methods of injection raise questions about the current accuracy. The mitigation of this threat would benefit significantly from more accurate data handling and equipment.

REFERENCES

[1] F. A. Administration, "Legal information institute. (2010, may 28). 14 cfr § 91.227 - automatic dependent surveillance-broadcast (ads-b) out equipment performance requirements." 2010.

[2] EUROCONTROL, "Automatic dependent surveillance – broadcast (ads-b)," 2020.

[3] Wikipediacontributors, "Automatic dependent surveillance – broadcast," 2020.

[4] M. Leonardi, L. Di Gregorio, and D. Di Fausto, "Air traffic security: Aircraft classification using ADS-B message's phase-pattern," *Aerospace*, 2017.

[5] *Federal Aviation Administration, DOT. (2015, February). Automatic Dependent Surveillance-Broadcast (ADS-B) Out Performance Requirements To Support Air Traffic Control (ATC) Service; Technical Amendment (2015–02579). Federal Register. Retrieved from https://www.federalregister.gov/documents/2015/02/09/2015-02579/automatic-dependent-surveillance-broadcast-ads-b-out-performance-requirements-to-support-air-traffic.*

[6] M. Riahi Manesh and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system," 2017.

[7] M. Strohmeier, V. Lenders, and I. Martinovic, "Security of ADS-B: State of the Art and Beyond," *arXiv preprint arXiv:1307.3664*, 2013.

[8] T. Li and B. Wang, "Sequential collaborative detection strategy on ADS-B data attack," *International Journal of Critical Infrastructure Protection*, 2019.

[9] J. Sun, "The 1090MHz Riddle (GNU GPL open-source license ed., v2)," 2020.

[10] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, 2011.

[11] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Communications Surveys and Tutorials*, 2015.

[12] M. Monteiro, A. Barreto, T. Kacem, D. Wijesekera, and P. Costa, "Detecting malicious ADS-B transmitters using a low-bandwidth sensor network," in *2015 18th International Conference on Information Fusion, Fusion 2015*, 2015.

[13] O. Baud, N. Honore, and O. Taupin, "Radar / ADS-B data fusion architecture for experimentation purpose," in *2006 9th International Conference on Information Fusion, FUSION*, 2006.

[14] T. Leinmüller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Communications*, 2006.

[15] *K. Sampigethaya, R. Poovendran and L. Bushnell, "Assessment and mitigation of cyber exploits in future aircraft surveillance," 2010 IEEE Aerospace Conference, Big Sky, MT, 2010, pp. 1-10, doi: 10.1109/AERO.2010.5446905.*

[16] B. Kovell, B. Mellish, T. Newman, and O. Kajopaiye, "Comparative Analysis of ADS-B Verification Techniques," *GPS Solutions 20(3)*, 2012.

[17] J. Johnson, H. Neufeldt, and J. Beyer, "Wide area multilateration and ADS-B proves resilient in Afghanistan," in *ICNS 2012: Bridging CNS and ATM - Conference Proceedings*, 2012.

[18] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Communications*, 2010.

[19] F. K. Jondral, "Software-defined radio - Basics and evolution to cognitive radio," 2005.

[20] E. G. Piracci, G. Galati, and M. Pagnini, "ADS-B signals reception: A Software Defined Radio approach," in *2014 IEEE International Workshop on Metrology for Aerospace, MetroAeroSpace 2014 - Proceedings*, 2014.

[21] A. Vesa and A. Iozsa, "Direction - Of - Arrival estimation for uniform sensor arrays," in *2010 9th International Symposium on Electronics and Telecommunications, ISETC'10 - Conference Proceedings*, 2010.

[22] C. Reck, U. Berold, J. Schür, and L. P. Schmidt, "Direction of arrival sensor calibration based on ADS-B airborne position telegrams," in *European Microwave Week 2009, EuMW 2009: Science, Progress and Quality at Radiofrequencies, Conference Proceedings - 6th European Radar Conference, EuRAD 2009*, 2009.

[23] C. Reck, M. S. Reuther, A. Jasch, and L. P. Schmidt, "Verification of ADS-B positioning by direction of arrival estimation," *International Journal of Microwave and Wireless Technologies*, 2012.

[24] Z. Li, D. Zhang, Q. Zhu, H. Gu, S. Huang, Y. Kuang, and Y. Liu, "Application Research on DOA Estimation Based on Software-Defined Radio Receiver," in *Journal of Physics: Conference Series*, 2020.

[25] RTL-SDR.COM, "KerberosSDR Quickstart Guide," *Retrieved 21 September 2020, from https://www.rtl-sdr.com/ksdr/*, 2020.

[26] Z. Li and D. Zhang, "Application Research on DOA Estimation Based on Software-Defined Radio Receiver," *J. Phys.: Conf. Ser. 1617 012047*, 2020.

[27] J. Sun, H. Vû, J. Ellerbroek, and J. M. Hoekstra, "pymodes: Decoding mode-s surveillance data for open air transportation research," *IEEE Transactions on Intelligent Transportation Systems*, 2019.

[28] J. Sun and J. Hoekstra, "Analyzing Aircraft Surveillance Signal Quality at the 1090 Megahertz Radio Frequency," 2020.

[29] *Whiteboard Web, I/Q Data for Dummies, Retrieved 27 October 2020, http://whiteboard.ping.se/SDR/IQ. http://whiteboard.ping.se/SDR/IQ, (2020).*

[30] H. E. Haber, "Physics 116a: The argument of a complex number," 2011.

[31] L. C. Godara, "Applications of antenna arrays to mobile communications, part I: Performance improvement, feasibility, and system considerations," *Proceedings of the IEEE*, 1997.

[32] S. N. Bhuiya, F. Islam, and M. A. Matin, "Analysis of Direction of Arrival Techniques Using Uniform Linear Array," *International Journal of Computer Theory and Engineering*, 2012.

[33] *Peto, Tamas, PyArgus. GitHub. Retrieved 30 August 2020, from https://pypi.org/project/pyargus/*, 2020.

[34] A. I. Islam, Ren, "Performance Study of Direction of Arrival (DOA) Estimation Algorithms for Linear Array Antenna," *https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=5166789*, 2009.

[35] L. C. Godara, "Application of antenna arrays to mobile communications, part II: Beam-forming and direction-of-arrival considerations," in *Adaptive Antennas for Wireless Communications*, 2009.

[36] *S. Chandran, "Smart Antennas for Wireless Communications (with MATLAB) (Gross, F.; 2005) [Reviews and Abstracts]," in IEEE Antennas and Propagation Magazine, vol. 51, no. 3, pp. 134-134, June 2009, doi: 10.1109/MAP.2009.5251212.*

[37] J. Capon, "High-Resolution Frequency-Wavenumber Spectrum Analysis," *Proceedings of the IEEE*, 1969.

[38] *Burg. J., Maximum entropy spectral analysis, presented at the 37th Annu. Meeting, Society Exploration Geophysics, Oklahoma city, OK, (1967).*

[39] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm, "Bringing up OpenSky: A large-scale ADS-B sensor network for research," in *IPSN 2014 - Proceedings of the 13th International Symposium on Information Processing in Sensor Networks (Part of CPS Week)*, 2014.

[40] RTL-SDR.COM, "KrakenSDR: A phase-coherent software defined radio with five RTL-SDRs," *Retrieved 21 June 2021, from https://www.crowdsupply.com/krakenrf/krakensdr*, 2020.

[41] M. G. Pralon, "Compact antenna arrays for efficient direction of arrival estimation," Ph.D. dissertation, Technischen Universitat Ilmenau, 2017.

II

MASTER THESIS (MID-TERM) REPORT

This part of the report contains the mid-term report, providing an overview of the work done, including the literature study (previously graded under AE4020), a more thoroughly description of the research motivation and proposal.

1

INTRODUCTION

Automatic Dependent Surveillance - Broadcast (ADS-B) is a well-performing operational enhancement in Air Traffic Control (ATC) applications. It enables aircraft and airport vehicles to periodically broadcast the information from their on-board equipment, like their identification, status, GPS location, velocity, and intent [9]. The ATC can use it for surveillance purposes, but additionally, spacing and separation is enabled for airborne traffic [10]. The system is part of a trend to modernize the ATC, where over many years, the ATC has made a move from independent and uncooperative (primary surveillance radar, PSR) to dependent and cooperative (secondary surveillance radar, SSR, and Automatic Dependent Surveillance - Broadcast, ADS-B) surveillance systems [11]. The service implementation is a dependent surveillance system containing two services: 1) 'ADS-B out', the capability to broadcast the equipped aircraft parameters, and 2) 'ADS-B in' the capability to receive information from nearby aircraft [2]. In May 2010, the Federal Aviation Administration (FAA) [12] set up the ADS-B performance requirements and technical amendment. In that final rule, the FAA set the equipment requirements of ADS-B mandatory for certain air spaces classes by January 1, 2020.

1.1. RESEARCH MOTIVATION

Nowadays, ADS-B 1090 Mode S Extended Squitter (ES) is the most predominant adopted technology ADS-B service implementation. The service implementation increased the renewal time, reduces costs, and increases safety and accuracy already in comparison to classical radar surveillance [2]. However, ADS-B is planned for long-term use but lacks the minimal and necessary inherent security mechanisms. The ATC system has not been developed with security in mind and is vulnerable to a number of different radio frequency attacks by malicious parties. The different vulnerabilities are commonly described in the literature and numbers of potential countermeasures are proposed. According to Manesh et al. [6], compared to classical radar surveillance, the two fundamental disadvantages are: 1) dependency on on-board derived navigation data, and 2) the open and straightforward ADS-B protocol. Nowadays, regulations are the primary prevention method for this lack of security. The current ADS-B standard does not provide mechanisms for verifying the integrity of navigation standards [3]. Multiple studies have mapped the vulnerabilities and proposed/developed technical mitigation techniques. However, to become part of the ADS-B protocol and global standard, these are yet to prove their effectiveness.

1.2. RESEARCH AIM

The aim of this preliminary research is to get a better understanding of the problem and to define a research proposal. Therefore, an initial research objective for this has been formulated to define this research's starting scope:

> *"To suggest a possible and cost-effective solution, which improves the security and integrity of raw Mode-S/ADS-B signals, by designing a tool which can verify and validate the low-level signal".*

To specify and structure the literature review and preliminary study initial question has been further specified in sub-questions. These aim to gather all relevant knowledge and to see the research objective from a broader perspective. Assumed, the attacker is able to create correctly formatted ADS-B messages, covering the correct message types, message order, legitimate and reasonable flight parameters; this study focuses on signal injection since it is medium-difficult to implement, but it has a high disruption level and it is hard to detect [6]. The sub-questions are functional to better understand how (cost-efficient) methods can verify and validate ADS-B signal integrity and what is promising in the literature for both ADS-B verification research and standard signal processing. Note: this is just a starting point; the final research proposal will be discussed later on.

1. What does the Mode-S/ADS-B signal looks like?
   (a) What are the raw ADS-B signal properties, and what variables are available?
   (b) What does the ADS-B protocol looks like?
2. How is the protocol vulnerable for malicious signal injection?
3. What is the definition validation and verification of a signal?
4. What methods are currently being used in malicious signal injection mitigation?
   (a) What methods have been applied in ADS-B research?
   (b) What methods have been applied in signal processing research?
5. What method is the most feasible candidate to mitigate malicious ADS-B signal injection?

1.3. RESEARCH SCOPE

Validation and verification of ADS-B mode S 1090 ES signals is fundamental for the secure long-term use of this protocol. The lack of minimal and necessary inherent security mechanisms, different vulnerabilities and possible solutions and countermeasures are widely described in the literature. Understanding the protocol and potential security threats is essential knowledge, where this study scopes on a cost-effective countermeasure against malicious injection while airborne.

Therefore, an background of relevant knowledge about ADS-B Mode S 1090 Extended Squitter is given in chapter 2. Chapter 3 gives a detailed overview of the related work within the scope of this research, as described above. Both the background and related work are written as part of the literature review course of the master Aerospace Engineering. This literature study aims to cover a relevant overview of the research field of verifying and validating Mode-S/ADS-B signals and mitigating malicious injected ADS-B signals. Both the historical perspective up till the current state-of-the-art are included.
Furthermore, an assessment of the literature is present to find out significant trends and potential for further research. This comes together in the final part, where a research question and a final thesis research plan are described. A research proposal is written in chapter 4. Note: the final research objective and sub-goals are written in this proposal. Chapter 5 explains the related technical content, and in chapter 6, the preliminary results are given in the hope of starting a discussion on ideas and suggestions not stated in this report so far.

2

BACKGROUND OF ADS-B MODE S 1090 EXTENDED SQUITTER

The aim of this chapter is to introduce the reader to the earlier mentioned service implementation: Automatic Dependent Surveillance-Broadcast mode S 1090 Extended Squitter. This background of ADS-B can be seen as relevant and necessary information for this research. In section 2.1 the ADS-B standard, protocol and its characteristics will be generally explained. Then, in section 2.2 the airborne ADS-B messages are explained more thoroughly.

2.1. AUTOMATIC DEPENDANT SURVEILLANCE-BROADCAST

ADS-B is a satellite-based surveillance system, which operates dependent and cooperative. The implementation is part of a trend in air traffic control (ATC) of moving from independent and uncooperative service implementations - for instance: primary surveillance radar (PSR) - to dependent and cooperative service implementations - for instance: secondary surveillance radar (SSR) and ADS-B [3].

<table>
<tr><td colspan="3"></td><td colspan="2">ADS-B Protocols</td></tr>
<tr><td colspan="3"></td><td>1090ES</td><td rowspan="2">UAT</td></tr>
<tr><td>Mode 3/A</td><td>Mode C</td><td>Mode S</td></tr>
<tr><td colspan="3">Transponder Protocols</td><td></td></tr>
</table>

Table 2.1: *Relationship between ADS-B protocols and transponders - Reprinted from [6].*

There are two competing ADS-B standards: 978 MHz Universal Access Transceiver (UAT) and 1090 MHz Mode S Extended Squitter (1090ES). UAT has specifically been developed for ADS-B applications, but requires a renewal of the aviation hardware. Instead, 1090ES can make use of general aviation hardware. This enabled the integration of ADS-B in standard Mode S transponders. Table 2.1 demonstrates the hierarchy and between transponders and ADS-B protocols 1090ES and UAT [6].

Nowadays, the most adopted ADS-B standard is the 1090 MHz Mode S Extended Squitter. The aircraft position, identification, and velocity - determined by the on-board systems and receivers - are transmitted through the ES. The messages can also integrate further fields and are continuously transmitted at a frequency of 1090 MHz by the majority of the aircraft [13].

The service implementation enhances pilot and air traffic control services situational awareness, in-flight collision, runway incursion avoidance, and precise air traffic control surveillance in areas without radar coverage [6]. In figure 2.1, the ADS-B transmission flow has been schematically shown. There can be seen of what different parts the service implementation consists.

From the Global Navigation Satellite System (GNSS), accurate navigation data, including GPS position and velocity, are processed and transmitted by the ADS-B transmitter via the 1090ES/UAT data link. The ATC center, ground stations, and neighbor aircraft can receive and process the data via the 'ADS-B in' and 'ADS-B out' data-link [1].

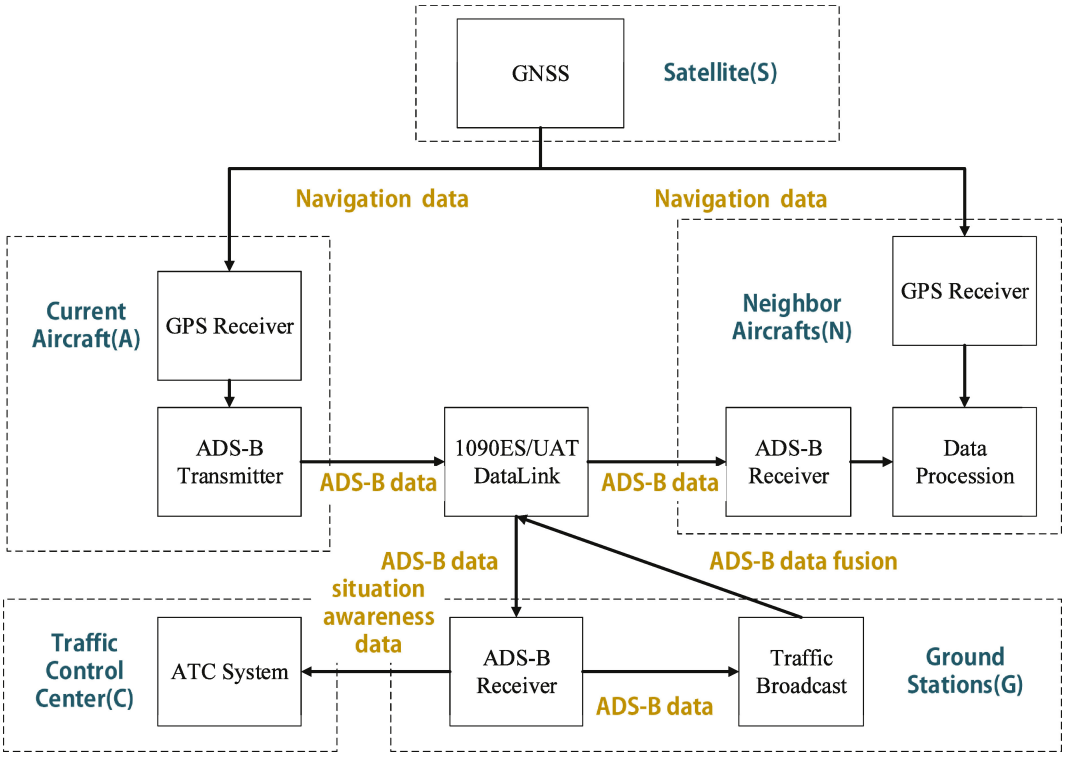

Figure 2.1: *ADS-B transmission flow - Reprinted from [1].*

2.2. ADS-B MESSAGE

This section describes the ADS-B message more thoroughly. This information is valuable to determine the possible message content, which can be retrieved from the signal. Since the protocol is open available, anyone can decode and generate these signals.

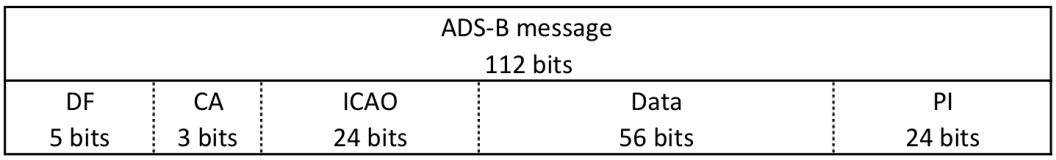

Figure 2.2: *ADS-B message structure.*

A standard message format has been established for the ADS-B 1090ES. This message consists of a five part 112-bit long structure. In figure 2.2, the schematic overview of this structure is shown, divided into five blocks. The first 5 bits are used for the downlink-format (DF). Normally, the 1090 Mode S ES uses DF = 17, which means the 56-bit data block is permitted. Furthermore, in case of TIS-B messages: DF = 18 [7].
The following block (6-8 bits) is used for capabilities (CA) of the mode S transponder, for instance the additional identifier. The next 24-bit block contains the aircraft address field. From this part of the message, the ICAO address can be decoded, which is used for aircraft identification. The information from the onboard systems is located from 33 bits till 88 bits a 56-bit data block. This will be discussed more thoroughly below. The last 24-bit long data block is used for parity and interrogator ID (PI) [6].

ADS-B 1090 ES signal messages have DF 17 or 18. The type code can identify the information contained in the ADS-B signal. For instance, an aircraft identification message has type code 1 to 4. For airborne position determination type code 9 to 18 and for airborne velocity determination type code 19 is used. An overview of the type code and its content can be found in table 2.2.

Type code	Content
1 - 4	Aircraft identification
5 - 8	Surface position
9 - 18	Airborne position (w/ Baro Altitude)
19	Airborne velocities
20 - 22	Airborne position (w/ GNSS Height)
23 - 27	Reserved
28	Aircraft status
29	Target state and status information
31	Aircraft operation status

Table 2.2: *Type code and content - Reprinted from [7].*

As shown, there are multiple data formats designed to meet the required navigation performance [1]. Since this research initially scopes on the airborne protocols, the more thorough explanation of the 56-bit data frames is limited to aircraft identification (TC 1-4), airborne position determination (TC 9 - 18), and airborne velocity determination (TC 19) [7].

2.2.1. AIRCRAFT IDENTIFICATION

In this section, the ADS-B aircraft identification protocol is further explained. The ICAO states in 'Technical Provisions for Mode S Services and Extended Squitter' the primary purpose is: "to provide aircraft identification and category" [8]. After confirming the type code the aircraft type and aircraft call sign can be decoded. The composed messages are shown in table 2.3.

Data bits	MSG bits	Content
33 - 37	1 - 5	Format type code
38 - 40	6 - 8	Aircraft category
41 - 46	9 - 14	Character 1
47 - 52	15 - 20	Character 2
53 - 58	21 - 26	Character 3
59 - 64	27 - 32	Character 4
65 - 70	33 - 38	Character 5
71 - 76	39 - 44	Character 6
77 - 82	45 - 50	Character 7
83 - 88	51 - 56	Character 8

Table 2.3: *1090 ES aircraft identification message bits and content - (Partially) reprinted from [8].*

2.2.2. AIRBORNE POSITION

In this section, the ADS-B airborne position protocol is further explained. The ICAO states in 'Technical Provisions for Mode S Services and Extended Squitter' the primary purpose is: "to provide accurate airborne position information" [8]. Just like for the aircraft identification - after confirming the type code the airborne position information can be decoded. The composed messages are shown in table 2.4.

Data bits	MSG bits	Content
33 - 37	1 - 5	Format type code
38 - 39	6 - 7	Surveillance status
40	8	Single antenna flag
41 - 52	9 - 20	Altitude
53	21	Time
54	22	CPR format
55 - 71	23 - 39	Latitude
72 - 88	40 - 56	Longitude

Table 2.4: *1090 ES airborne position message bits and content - (Partially) reprinted from [8].*

In principle, decoding different types of messages can be done similarly. From the signal, a hexadecimal message is retrieved and converted into a binary number. From this number, the message content can be decoded. The information contained in the airborne position message is used in several studies for location verification. Therefore, a more thorough clarification and explanation of an actual (example) ADS-B raw airborne position message in hexadecimal and the converted one to a binary message are shown below:

Raw message in hexadecimal:

```
8D48C22658C902BBC2EAEB6B22B5
```

Raw message converted to binary numbers:

```
10001101010010001100001000100110010110001100100100000010
10111011110000101110101011101011011010110010001010110101
```

Using the ADS-B message structure, as pictured in figure 2.2, the 112-bit message in binary numbers can be divided into parts. This is shown in figure 2.3. The example signal is divided into the earlier described five parts in the top half of the figure. In the bottom half, the 56-bit data block is divided into the parts described in table 2.4.

	DF	CA	ICAO	Data	PI
HEX	8D		48C226	58C902BBC2EAEB	6B22B5
BIN	10001	101	010010001100 001000100110	01011000110010010000000101011 10111100001011101010111010 11	011010110010 001010110101

	Type	..	.	Altitude	Time	.	Latitude	Longitude
BIN	01011	00	0	110010010000	0	0	10101110111100001	01110101011101011

Figure 2.3: *Example of a raw message and its information parts*

2.2.3. AIRBORNE VELOCITY

In this section, the ADS-B airborne velocity protocol is further explained. The ICAO states in 'Technical Provisions for Mode S Services and Extended Squitter' the primary purpose is: "To provide additional state information for both normal and supersonic flight based on airspeed and heading" [8]. After confirming the type code, the airborne velocity information can be decoded just like for the aircraft identification and position. The composed messages are shown in table 2.4.

Data bits	MSG bits	Content
33 - 37	1 - 5	Format type code
38 - 40	6 - 8	Subtype
41	9	Intent flag change
42	10	Capability flag
43 - 45	11 - 13	Uncertainty navigation velocity
46	14	Heading status
47 - 56	15 - 24	Magnetic heading
57	25	Airspeed type
58 - 67	26 - 35	Airspeed
68	36	Vertical rate source
69	37	Vertical rate sign
70 - 78	38 - 46	Vertical rate
79 - 80	47 - 48	Turn indicator
81	49	Baro altitude sign
82 - 88	50 - 66	Baro altitude

Table 2.5: *1090 ES airborne velocity message bits and content - (Partially) reprinted from [8].*

3

LITERATURE REVIEW

This chapter was written as part of the literature review course of the master Aerospace Engineering. This literature review aims to cover a relevant overview of the research field of verifying and validating Mode-S/ADS-B signals and mitigating malicious injected ADS-B signals. The review is limited to the scope described in the introduction. Both the historical perspective up till the current state-of-the-art are included. Furthermore, an assessment of the literature is present to find out significant trends and potential for further research. The above written comes together in the next chapter, where a research question and a final thesis research plan are described.

This chapter is divided into three main sections to explain the relevant knowledge from related work briefly. To underline the problem statement, in section 3.1, an overview is given of potential malicious attack threats. Furthermore, in section 3.2, the current state-of-the-art taxonomy of ADS-B security, scoping on malicious injection, is provided. Moreover, the final section (section 3.5) goes into more detail about a relatively new approach used for signal processing and jamming mitigation in the literature.

3.1. THE SECURITY ISSUE OF ADS-B

As stated in the introduction, this study scopes on countermeasures to malicious injection in ADS-B networks. However, to understand the relevance of the problem, this section gives an overview of multiple malicious attacks suggested in the literature. Multiple authors summed up potential vulnerabilities and attacks. These different vulnerabilities are commonly described in the literature and numbers of potential countermeasures are proposed. Manesh et al. [6] present an overview of the ADS-B risk analysis by considering the likelihood of an attack and its potential impact. This overview is reprinted below in table 3.1:

		Attack Impact		
		Low	Medium	High
Attack Likelihood	High	Eavesdropping (Low Risk)		
	Medium		Jamming (Medium-High Risk)	Message Injection (High Risk)
	Low		Message Deletion (Medium Risk)	Message Modification (Medium-High Risk)

Table 3.1: *ADS-B risk analysis - Reprinted from [6]*

The presented overview functions also as an overview of different scopes within this research field since different attacks are commonly based on different properties or weaknesses of the service implementation. Below the different types of attacks are shortly summed up and explained. For further information and a more thorough explanation, the reader is recommended to read the referred studies.

Eavesdropping
Eavesdropping is a passive attack where the malicious attacker can listen to the unencrypted and unsecured

broadcasted messages [2]. In the literature, eavesdropping is also known as message interception of aircraft reconnaissance and is a known issue since the early stages of ADS-B development. There is no technical countermeasure against unintended recipients. Instead, different countries chose to regulate this by law enforcement [6]. According to Strohmeier et al. [3], next to privacy considerations, eavesdropping forms the basis for more advanced active attacks. According to the risk analysis of Manesh et al. [6] the attack has a high attack likelihood but a low attack impact.

Jamming
Jamming is an active attack method, where a ground station or aircraft is disabled from its operation (sending and receiving messages) by adding an additional signal with sufficiently high power and the same frequency into the network [3]. Leonardi et al. [2] explain jamming would cause denial of services for any aircraft or airports in a geographical area. Furthermore, specifically targeting single objects, such as aircraft, using jamming is proven feasible by Wilhelm et al. [14]. According to the risk analysis of Manesh et al. [6] the attack has a medium attack likelihood and medium attack impact.

Message deletion
Message deletion is an attack method to 'delete' legitimate messages. McCallie et al. [15] distinguish two types of message deletion: 1) constructive message deletion and 2) destructive message deletion. Performing constructive message deletion, the attacker causes sufficient errors in the bits of the message. Since the receiver system marks the message as corrupted and will drop it. Performing destructive message deletion, the attacker transmits the inverse of the legitimate message to cancel out the message. Since this method requires a high level of precise and complex timing, it is difficult to set up a message deletion attack, according to [2]. This is in line with the risk analysis of Manesh et al. [6], who states: the attack has a low attack likelihood and medium attack impact.

Message modification
Message modification can be distinguished into three different approaches during transmission over the physical layer: 1) Overshadowing, 2) bit-flipping, and 3) combined message deletion and injection (discussed below) [6]. Overshadowing is an approach where the attacker transmits a message over the legitimate message. Using a higher-powered signal and timing rightly, the attacker would be able to modify specific bits or the whole legitimate message. As discussed in the section about jamming above, targeting a single node instead of an entire network, is more or less the method described by Wilhelm et al. [14]. Bit-flipping causes switches in the modulated signal described in the previous chapter. Bits can be switched from zero to one and vice versa. The third approach, combined message deletion and injection, is obviously a combination of the two described attacks. The malicious attacker would be able to replace an aircraft or it parameters. Strohmeier et al. [16] sets message modification of an ADS-B message as the most difficult executable form of attack. According to the risk analysis of Manesh et al. [6] the attack has a low attack likelihood but a high attack impact.

Message injection
Leonardi et al. [2] defined message injection as the intentional transmission of non-legitimate ADS-B signals on the same frequency and encoded following the ADS-B protocol using erroneous information. This results in displaying false aircraft. Since there is no data link authentication layer and no encryption, it relatively simple to generate and transmit these signals. Assumed the attacker is able to create correctly formatted ADS-B messages, covering the correct message types, message order, legitimate and reasonable flight parameters, the false aircraft in the network are hard to detect and can cause high disruption. Schäfer et al. [17] shows it is relatively simple to perform a message injection attack with limited knowledge and cheap hardware. According to the risk analysis of Manesh et al. [6], the attack has a medium attack likelihood and high attack impact.

Concluding, McCallie et al. [15] stated that the combination of multiple attacks creates more complex attacks. However, combined attacks have a lower attack likelihood since those are much more challenging to perform. As part of the relevant knowledge and within this study's scope, the vulnerable parts or the ADS-B taxonomy, as described in chapter 2 are pictured and highlighted by Leonardi at al. [2]. This schematic overview is reprinted in figure 3.1 below:

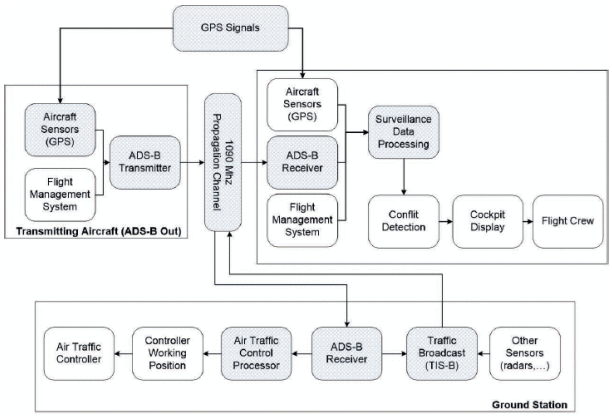

Figure 3.1: *Most vulnerable areas (highlighted) within the ADS-B transmission flow - Reprinted from [2]*

The classified and described malicious attacks above find its ground in the processing elements of the transmission flow. If the aircraft sensors or signal transmissions (GPS and ADS-B) are targeted by a malicious attacker, the system is corrupted for malicious scopes [18].

3.2. RELATED WORK ON COUNTERMEASURES OF ADS-B INJECTION

According to Stomeiher et al. [3], [16], the state-of-the-art of ADS-B security research is currently divided into two approaches: secure broadcast authentication and secure location verification. Multiple researchers use this distinction as the baseline of their research or reviews [4], [6]. This part of the literature review focuses on the related work done, focusing specifically on the malicious attack: injection.

As baseline for this literature review, the taxonomy set by Stomeiher et al. is used and can be found in figure 3.2 below. Note: not all security approaches in this taxonomy are relevant or capable against malicious injection attacks. Only the capable ones are discussed and colored blue in figure 3.2. Additionally, some subjects are discussed, clarified and explained more thoroughly than others, since this research scopes on a cost-effective solution, where an actual redesign of the ADS-B protocol is not feasible. To define a gap in the literature, there is assumed the taxonomy is not complete. The current state-of-the-art research mainly used this taxonomy as a baseline, but other opportunities are added and discussed below.

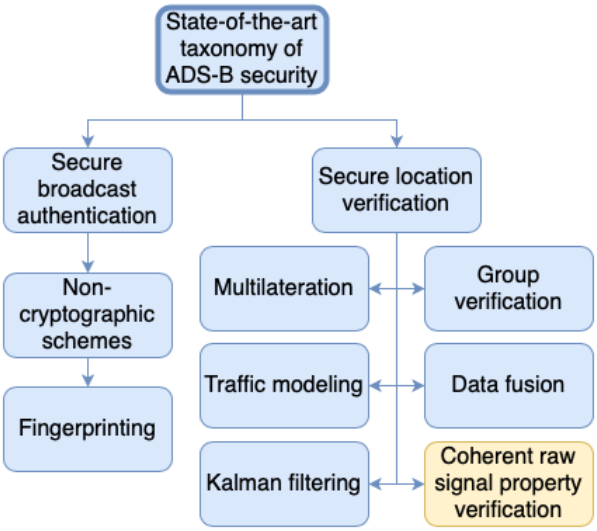

Figure 3.2: *ADS-B security research taxonomy - Partly reprinted from [3]*

3.3. SECURE BROADCAST AUTHENTICATION

Physical layer authentication can be distinguished in cryptographic and non-cryptographic physical layer authentication. An example of non-cryptographic physical layer authentication is fingerprinting.

3.3.1. NON-CRYPTOGRAPHIC PHYSICAL LAYER AUTHENTICATION

An example of non-cryptographic physical layer authentication is fingerprinting. This method includes possibilities in order to verify ADS-B messages while the network has been maliciously injected. Fingerprinting is a commonly used subject in research for wireless networks. The goal is to identify imperfections and characteristics of a network [6]. Zeng et al. [19] categorizes these techniques into three parts: 1) software-based fingerprinting 2) hardware-based fingerprinting, and 3) channel based fingerprinting. Software-based fingerprinting is specifically based on the unique characteristics of the protocol software. Hardware-based fingerprinting is based on the unique properties of waveforms caused by the chosen hardware. Moreover, channel-based fingerprinting has its groundwork in channel state information and signal strength. It is proven that wireless signals decorrelate rapidly in space, so a physical layer algorithm could determine whether multiple signals are from the same source [19].

Strohmeier et al. [16] discuss differences in the implementation of aircraft transponders to fingerprint their wireless drivers. The work on fingerprinting can be used as an anomaly detection system to identify inconsistencies in the ADS-B protocol. There have been created a number of different features to classify multiple transponder classes. All those features are time interval based, for instance: slot width, first slot and last slot. This is done by hand-crafting clusters by observation and an unsupervised clustering approach, using the k-mean clustering algorithm. By mapping those classes in different aircraft types or fleet class databases, it creates an overview of the installed hardware. Strohmeier suggests the implementation of this technique on network intrusion, including injection. The received signals can be validated by comparing its features to the expected features

Leonardi et al. [2] proposes to use the transmitter carrier phase as feature to classify different aircraft. This provides a way to distinguish legimate messages from fake messages. By neglecting the preamble, so only using the 112-bit data block (see figure 2.2), the transmitted signal can be represented mathematically:

$$s_t(t) = A \cdot \left[\sum_{m=1}^{112} rect\left(\frac{t - 2mT + c_m T + T/2}{T}\right) \right] sin[2\pi f_c t] \tag{3.1}$$

Here $s_t(t)$ is the phase pattern of the 112-bit data block. A is the message amplitude, c_m is the bits sequence, f_c is the carrier frequency and T is the pulse width. For 1090ES these two are 1090MHz and 0.5μs, respectively.

Due to tolerances in different transmitting devices, the phase pattern can differ per transponder. Therefore, the author compensates in the equation below by adding the tolerance of the carrier phase , carrier frequency and additive white Gaussian noise.

$$s_r(k) = s_r(kT_s) = A(kT_s) \cdot \left[\sum_{m=1}^{112} g(kT_s - 2mT + c_m T + T/2) \right] sin[2\pi(f_c + \delta f)kT_s + \phi(kT_s)] + n(kT_s) \tag{3.2}$$

Here, k represents samples, T_s the sample time, $n(kT_s)$ is the additive white Gaussian noise, δf the allowed tolerance of the carrier frequency and $\phi(t)$ the carrier frequency. Knowing this, the Maximum Likelihood estimation can be used for the estimation of the ADS-B message's phase pattern ($\hat{\phi}_m$). The author uses the following equation, where K represent the relative samples of the pulses and m the pulse itself:

$$\hat{\phi}_m = arctan\left[\frac{\sum_K s_r(kT_s) sin(2\pi(f_c + \delta f)kT_s)}{\sum_K s_r(kT_s) cos(2\pi(f_c + \delta f)kT_s)} \right] \tag{3.3}$$

Leonardi et al. choose to use a neural network (NN) to classify the aircraft into seven different classes. To overcome the not homogeneously distribution of $\hat{\phi}_m$ in time, interpolation has been used to remove the empty spaces. By training the NN with data from the first day and testing with data from the second day, a 91.4% correct classification probability is achieved. There can be concluded that more than 50% of the aircraft have a representative $\hat{\phi}_m$.
Combining the information from the classification, $\hat{\phi}_m$ and the decoded ICAO code, an intruder detection algorithm is proposed. There can be concluded that two types of attacks can be detected 1) legitimate aircraft not present but receiver under attack and 2) legitimate aircraft present and under attack. A 3) class is available for legitimate and present aircraft. The proposed method is able to assign 62-64% of the aircraft to one of the classes.

More recent research from Leonardi et al. [20] proposes an intrusion detection mechanism based on radio frequency fingerprinting. Combining the carrier phase features (as described above), carrier frequency features and time features, the aircraft fingerprint is composed. By applying Kolmogorov-Smirnov, Anderson and Darling, and Lillifors-Gaussian-test, the features can be extracted and tested. A new intrusion algorithm is proposed, which is able to detect aircraft without a (stable) signature. The method is reaching a low probability of false alarm and a high detection probability.

Manesh et al. [6] discuss the implementation of fingerprinting. Compared to other methods, the implementation might have a medium difficulty of implementation. No changes of the ADS-B protocol are needed, but due to required additional hardware the expected costs are high. Instead, Strohmeier et al. [3] concludes that both cost and implementation difficulties are variable.
Leonardi et al. [2] [20] discuss the weaknesses of the applied fingerprinting methods. The use of historical data to create the signature reduces the detection to only very slow changes in the aircraft signature. However, these weaknesses can be resolved by sharing aircraft databases between different ground stations. Also, a mechanism to reduce fake information in aircraft databases is proposed to reduce the limitations of these fingerprinting methods.

3.3.2. CRYPTOGRAPHIC SCHEMES
Since cryptographic physical layer authentication requires more than slight changes in the protocol, it is out of the scope of this study. Commonly used examples are lightweight PKI & μTesla [3].

3.4. SECURE LOCATION VERIFICATION
3.4.1. WIDE-AREA MULTILATERATION
(Wide-area) multilateration is a position estimation technique based on measuring the differences in time of arrival of radio signals with a known propagation speed. Multilateration requires multiple antenna receivers on different known locations. According to Liu et al. [21], a commonly used method to determine the unknown position of the transmitter, with reference to ground stations, is the time-difference-of-arrival (TDOA). Monteiro et al. [4] explain there are multiple signal properties to be explored, such as signal strength, frequency and angle of arrival. However, the TDOA is chosen and explained since the aviation use case makes this convenient. The author has explained and summarized clearly the Wikipedia page about multilateration [22]. A network of K antennas is considered. The coordinates (known positions) of the antennas are expressed by $K \times 3$ matrix $\mathbf{S}$, which is visible in equation 3.4.

$$\mathbf{S} = \begin{bmatrix} s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,1} & s_{2,2} & s_{2,3} \\ \vdots & \vdots & \vdots \\ s_{K,1} & s_{K,2} & s_{K,3} \end{bmatrix} \tag{3.4}$$

To computation of the transmitter's position can be written into a linear equations (3.5), where $\hat{\mathbf{x}}$ is (x, y, z) and the components A and b are expressed in equation 3.6.

$$\hat{\mathbf{x}} = A^{-1} b \tag{3.5}$$

$$A = \begin{bmatrix} a_3 & b_3 & c_3 \\ a_4 & c_4 & d_4 \\ a_5 & c_5 & d_5 \end{bmatrix}, B = \begin{bmatrix} -d_3 \\ -d_4 \\ -d_5 \end{bmatrix} \tag{3.6}$$

The example given by Monteiro et al. [4] requires $K = 5$ antennas. Equations 3.7 solve the components of the equations above, where the time of arrival is $t_1, ..., t_5$, the reveiver position is $s_1, ..., s_5$ and v is the propagation speed of the signal.

$$\begin{aligned} a_m &= \frac{2s_{m,1}}{v(t_m - t_1)} - \frac{2s_{2,1}}{v(t_2 - t_1)} \\ b_m &= \frac{2s_{m,2}}{v(t_m - t_1)} - \frac{2s_{2,2}}{v(t_2 - t_1)} \\ c_m &= \frac{2s_{m,3}}{v(t_m - t_1)} - \frac{2s_{2,3}}{v(t_2 - t_1)} \\ d_m &= v(t_m - t_1) - v(t_2 - t_1) - \frac{s_{m,1}^2 + s_{m,2}^2 + s_{m,3}^2}{v(t_m - t_1)} + \frac{s_{2,1}^2 + s_{2,2}^2 + s_{2,3}^2}{v(t_2 - t_1)} \end{aligned} \tag{3.7}$$

The explained method is a widely used subject in ADS-B data collecting and processing [23]. Schäfer et al. [24] did an implementation and analysis of wide-area multilateration of ADS-B data to demonstrate the ability of confirming the ADS-B position messages. There is chosen multilateration as a benchmark for Opensky [24]. Since dedicated multilateration systems are expensive and difficult to implement the author proposes with Opensky a low-cost solution available for researchers. Johnson et al. [25] uses wide area multilateration at challeging areas, where robust power and communication are not available. Performance result show when the network is properly set wide area multilateration is an robust and adaptable surveillance solution.

Nevertheless, Monteiro et al. [4] states security is not the main focus of earlier research and proposes to use multilateration to detect malicious ADS-B attacks based on known GPS errors and clock precision inaccuracies. First, a receiver placement optimization, using multilateration, is established to increase the accuracy of the coverage area. Following, a reliability evaluation of the ADS-B position message is done for two specific cases. 1) A legimate and present aircraft and 2) the same legimate and present aircraft forging false position messages. The results are plotted by the author in two plots. Above the actual flightpath is compared to the flightpath determined by decoding the ADS-B signal and the determined flight path using multilateration. The bottom plot shows the confidence rate. In figure 3.3 the legimate and present aircraft is visible. The confidence rate is near to 1 (100%) over the samples. In figure 3.4 the confidence rate of the malicious transmitter is shown. Here, the confidence rate is near to zero and the signal can be identified as malicious. There is concluded by the author validating the position message shields against malicious message injections

Manesh et al. [6] and Strohmeier et al. [3] discusses the implementation of wide area multilateration and there can be concluded that compared to other methods the implementation might have a low difficulty of implementation. No changes of the ADS-B protocol are needed and the costs to implement are at a medium level. Two additional disadvantages of multilateration mentioned in ICAO research are summerized by Manesh et al. [6]: 1) Multilateration is vulnarable for multi-path effect and 2) the signal has to be received correctly and by multiple receivers. Furthermore, Monteiro et al. [4] discusses the required measurement of time of arrival at different locations. The accuracy of the estimation is highly dependent on the location of the antennas. The cost-effective solution of reuse of existing infrastructure is correlated to the accuracy of the system. Nevertheless, the proposed optimisation placement of ADS-B receivers tool improves the accuracy and reduces the error.

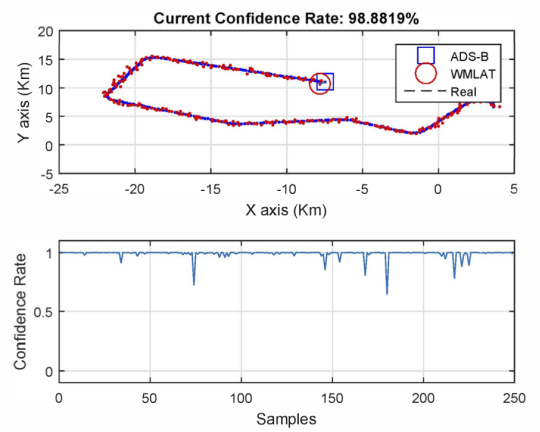

Figure 3.3: *Confidence rate for a legimate present aircraft, Reprinted from [4]*

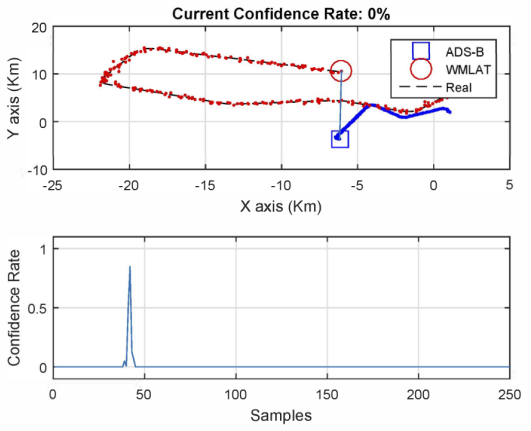

Figure 3.4: *Confidence rate for malicious transmitter, Reprinted from [4]*

3.4.2. KALMAN FILTERING

Kalman filtering is a widely used method in ATC applications. For instance, GPS position data can be smoothened by applying a Kalman filter [3]. The filtering method was introduced in the early '60s by Kalman et al. [26] and is also known as linear quadratic estimation. It is used to observe time series of measurements containing noise and generates statistically optimized variables for the unknown parts, based on a series of observations instead of single measurements. Moreover, Fox et al. [27] describes how the Kalman filter is based on Bayesian inference, a process based on historical data to estimate guesses about future steps.

According to Welch et al. [28] the method consists of three steps: 1) prediction, 2) observation, and 3) update. In the prediction step, the state variables and uncertainties are predicted depending on the system inputs, the current state and the transition information from the previous state to the current state. In the observation step, the estimation is computed with the observed variable of the observed state. In the update step, the estimations are weighted based on the error found in step 2.

Kovel et al. [29] did a comparative analysis of this technique to assess its performance on location verification. A distinction has been made between Kalman filtering the ADS-B position messages, Kalman filtering the signal strength and direction on the antenna and Kalman filtering the onboard aircraft signal for real-time position verification. The author scopes on the last one. The verification method using Kalman filtering involves sorting out missing or noisy ADS-B messages to estimate the aircraft's state. The estimated state is validated by comparing this to the actual trajectory. Kovel et al. conclude that the method can distinguish the particular features of the flight path. This makes it possible to discriminate signal data with physically impossible flight paths.

3.4.3. GROUP VERIFICATION

According to Sampigethaya et al. [30], group verification is a useful method to verify the broadcasted ADS-B position. The proposed method uses multilateration to verify its own position. When an aircraft's position message is received by four or more aircraft the position can be estimated based on the time difference of arrival. This independently estimated location can be verified with the location determined by the onboard systems. To make this possible, the author proposes to use an internet protocol airborne network. Kovel et al. [29] uses this method in a comparative analysis and proposes multiple air-to-air communication techniques, which meet the requirements ([31], [32], [33]). However, the authors note the central vulnerability of this method comes with the new malicious attack threats in the air-to-air communication system. Also, one can inject multiple targets due to the relatively big line-of-sight of air-to-air communication. This can result in stressing the processing capabilities of the equipment.
Strohmeier et al. [3] note that the method is medium-difficult to implement. However, there is concluded the cost-effectiveness of this solution scores bad. High costs are involved due to a required new protocol and communication network.

3.4.4. DATA FUSION

Data fusion is a common technique using multiple independent data sources to obtain higher accuracy than using one single data source. Comparative analysis of correlating data, also called data fusion, are generally based on probabilistic modeling and analysis [6]. For verification and validation of ADS-B signals, multiple solutions have been proposed in the literature. For instance, position verification can be done using data from PSR and SSR [34] or by comparing the flight path to the initial flight plan [35]. Also, map-based verification (no-fly zones) or maximum capacity limits are used as independent data sources in the literature [36]. Strohmeier et al. [3] note that the method is simple to implement. However, since separated systems are required, due to the need for independent sources, the method is hard to scale up.

3.4.5. TRAFFIC MODELING

Traffic modeling is a proposed technique, using the derivation of the next states of the flight path, using earlier known states. The estimation of the flight path can be validated between multiple ground stations to validate position claims the aircraft does. According to Leinmüller et al. [36], traffic modeling is able to detect deviations from standard ADS-B profiles, containing flight behavior. For instance, historical ATC data can be used as a verification tool. On the ground side of this solution, a lot of processing hardware is required, entailing high costs.

3.4.6. CONCLUSION ON STATE-OF-THE-ART TAXONOMY

There can be concluded that past research in validation and verification of ADS-B signals, while the network is maliciously injected, is mainly focused on secure broadcast authentication and secure location verification. The discussed methods and corresponding working principle and estimated implementation difficulty, cost, and effectiveness have been summarized in table 3.2. The different approaches could potentially be useful for the mitigation of malicious signal injection. However, to become part of the ADS-B protocol and global standard, most of these are yet to prove their effectiveness. In the literature, most proposed solutions require changes in the ADS-B protocol or changes in the existing hardware, both entailing high costs. Looking at table 3.2, there can be concluded Kalman filtering and data fusion might be the most feasible approaches to mitigate malicious injection since these are the most cost-effective and best-performing approaches. Since both haven't proved their efficiency yet, there cannot be made a recommendation on including these methods in the research proposal. However, a combination of these two can be added to a multi-layer solution.

Method	Working principle	Difficulty	Cost	Effectiveness	References
Non-Cryptographic Physical Layer Authentication	Fingerprinting	1) Medium - since additional hardware and software are required. 2) Difficult - if a world wide data base system is required	Dependent	Good performance on providing data and location integrity	[2], [19], [18]
Wide Area Multilateration	Multilateration	Low - existing protocol and hardware can be used. Note: for optimal area coverage additional hardware is required	Medium	Well performing on location integrity, However, new data links make this solution vulnerable for new threats	[4], [20], [21], [22], [23]
Kalman Filtering	Bayesian inference	Low - existing protocol and hardware can be used	Low	Medium performance on providing data and location integrity	[24], [25], [26], [27]
Group Verification	Multilateration	High - new protocol and hardware required	High	Good performance on location integrity and possibly on data integrity	[27], [28], [30], [31]
Data Fusion	Data correlation	Low - existing protocol and hardware can be used	Medium	Good performance on location integrity and possibly on data integrity	[32], [34]
Traffic Modeling	Flight path estimation	Medium - additional entities required	Low	Good performance on location integrity	[5], [34]

Table 3.2: *Comparison of ADS-B countermeasures with respect to coverage of malicious injection*

3.5. A SOFTWARE DEFINED RADIO APPROACH

In numbers of ADS-B processing research Software Defined Radio (SDR) approaches are used. Jondral et al. [37] provide a brief overview of the concept and development of SDR and describes the system as a radio communication system in which the components, traditionally implemented in hardware, implemented as software radio. The SDR is a practical version of the Software Radio (SR), enabling digital signal generation and processing. According to Piracci et al. [38], a SDR permits flexibility and modularity for the easy development of prototypal devices for evaluation and testing novel enhancements for ADS-B receivers. The author states that the device is useful to analyze the traffic in a network or channel and test developed algorithms for signal processing. The author tests a multi-channel SDR approach by testing an algorithm to generate 1090MHz ADS-B signals and interference, such as noise and jamming.
Another example is presented by Leonardi et al. [39]. The authors describe a garbling reduction technique using low-cost ADS-B receivers. Garbling is the reception of superimposed signals broadcasted by multiple different aircraft. A multi-channel receiver (KerberosSDR) is applied by the author for the implementation of garbling mitigation. He is able to almost double the number of correctly decoded signals. This proves low-cost multi-channel receivers can play an essential role in ADS-B research.

3.5.1. MULTI-CHANNEL COHERENT SDR

Multiple studies in the literature make use of a coherent multi-channel SDR. For instance, Costin et al. [40] deploys a SDR for transmitting and receiving ADS-B messages to mitigate message injection and replay threats. Furthermore, Leonardi et al. [41] propose a solution against receiver jamming using a multi-channel coherent receiver. The author proposes Algebraic manipulation based on singular value decomposition (SVD). SVD is used to separate different transponder sources. Algebraic manipulation is also used in other SSR and ADS-B signal processing studies while using a coherent multi-channel receiver. For instance, another blind source separation algorithm is proposed by Zhou et al. [42], to avoid loss of replies due to overlapping replies. Petrochilos et al. [43] presents three algebraic algorithms to separate overlapping reply signals. This method enables the detection of individual parameter set of separated signals, time of arrival (TOA), and the estimation of the direction of arrival (DOA).
Based on different signal properties, there are multiple methods available to estimate the direction of arrival. The direction of arrival estimation is also known as spectral-, angle of arrival- or bearing estimation. These techniques are widely applied in research areas of time series analysis [44]. The methods consist of different methods. For instance: spectrum analysis, periodograms, eigenstructure methods, parametric methods, beamforming, array processing, and adaptive array methods [45]. Five commonly used algorithms, both linear DOA estimation algorithms and algorithms based on the decomposition of subspaces, are described below [46]:

- Bartlett (Fourier) method
- Capon's method
- Burg's Maximum Entropy Method
- Linear Prediction Method
- Multiple Signal Classification (MUSIC)

These methods have been tested and applied with different objectives in ADS-B signal processing research. For instance, Vesa et al. [47] used different DOA algorithms (Bartlett, Capon and MUSIC). The author concludes that for a uniform linear array, all three methods are promising. The Bartlett method has the disadvantage of not being able to estimate the DOA for signals sent from close directions. Overall, the MUSIC algorithm performs best with regards to the other two methods.
Furthermore, Reck et al. [48] investigate the use of position messages to calibrate the DOA. Within some limitations, the author concludes that the position message provides acceptable results for DOA estimation and the DOA estimation error is dependent on the distance between receiver and transponder.

3.5.2. CONCLUSION ON THE SOFTWARE DEFINED RADIO APPROACH

Software-Defined-Radios are proven successful in ADS-B signal processing. Having multiple channels available enables additional signal properties to process ADS-B signals, which can be used for instance for DOA estimation. Since the DOA can also be calculated via signal decoding, the described DOA estimation techniques enable another independent correlating variable, which makes DOA estimation potentially useful for ADS-B signal validation and verification. Using DOA estimation could be a feasible candidate to mitigate malicious ADS-B signal injection. To the best of knowledge, nobody has done this before

4

RESEARCH PROPOSAL

In this chapter, the research proposal is presented based on the background given in chapter 2 and the literature review in chapter 3. This chapter summarizes the literature gap written in chapter 3, the research objective, and supporting tangible sub-goals. After that, the chosen methodology, signal pre-processing, and experimental setup are described. Finally, the initial outcomes are presented. Note - as written in the introduction - this proposal and the preliminary results are given in the hope to start a discussion on ideas and suggestions not stated in this report so far.

4.1. LITERATURE GAP

Past research in validation and verification of ADS-B signals, while the network is malicious injected, is mainly focused on secure broadcast authentication and secure location verification. In the literature, most of the proposed solutions require changes in the ADS-B protocol or changes in the existing hardware, both entailing high costs. The application of low-cost software defined radios in ADS-B signal processing has been proven in multiple studies. Having multiple channels available enables additional signal properties to process ADS-B signals, which can be used in numbers of applications, such as direction of arrival estimation. This has been successfully tested in multiple studies with different objectives. For validation and verification of decoded ADS-B messages, this can be a potentially useful tool. Using direction of arrival might be the most feasible candidate to mitigate malicious ADS-B signal injection. To the best of knowledge, nobody has done this before.

4.2. RESEARCH OBJECTIVE AND QUESTIONS

The main research objective of this thesis is:

> *"To suggest a possible and cost-effective solution, which improves the security and integrity of raw Mode-S/ADS-B signals, by designing a tool which can verify and validate the low-level signal".*

This main research objective is supported by tangible sub-goals. To start with writing a literature study into Mode-S/ADS-B signal properties and current state-of-the-art methods to verify and validate Mode-S/ADS-B signals or applicable methods that can be used potentially. The main research objective can be translated into the main research question, which is defined as:

> *"How to mitigate security drawbacks of the ADS-B protocol by exploring characteristics of low-level signals, using the direction of arrival, while scoping on malicious injection?"*

The research question has been further specified in sub-questions to specify and structure the literature review and preliminary study. Note: these sub-question functions as a guideline through the research process and will result in the proposed methodology. The sub-questions are defined as:

1. What does the Mode-S/ADS-B signal looks like?

   (a) What are the raw ADS-B signal properties, and what variables are available?
   (b) What does the ADS-B protocol looks like?
   (c) What is the definition of signal validation and verification?

2. What is the potential of direction of arrival (DOA) estimation as a countermeasure to malicious signal injection?
   (a) What parts of the incoming signal are useful for signal processing?
   (b) How can decoded information result in a DOA variable?
   (c) What role can a multi-channel coherent receiver perform in DOA estimation?
   (d) What scenarios of malicious signal injection exists?
   (e) How can the model mitigate all these scenarios?

3. How to classify incoming signals based on the DOA?
   (a) What DOA methods have been applied in ADS-B research?
   (b) What DOA methods have been applied in signal processing research?
   (c) What DOA method is the most feasible candidate to mitigate malicious ADS-B signal injection?
   (d) What are the minimal requirements and indicators of the model's performance?

4. How can the method be verified?
   (a) What procedures can be used to perform a validation?
   (b) How to measure the performance indicators
   (c) Does the performance meet the actual performance indication?
   (d) How to visualize the results and performance?

4.3. METHODOLOGY

This section aims to explain the methodological approach and theoretical content to solve the proposed solution of this study's thesis phase. To follow up the main research question and sub-questions - this research can be divided into four parts: research background, signal (pre-)processing and analysis, develop a signal verification and validation model and an experimental phase to apply and validate the model. These research parts are more thoroughly explained in subsections 4.3.3, 4.3.4, 4.3.5 and 4.3.6 respectively and a schematic overview can be found in section 4.4. First, the preliminary chosen software and hardware can be found below:

4.3.1. SOFTWARE

As written in the objective questions, the proposed method should be as cost-effective as possible. Therefore there is chosen for freely available software. Additionally, the software tools are mainly Python-based or can make or read the same data formats. Further use of Python libraries is more thoroughly explained in chapter 5. Therefore, as preliminary software for the experimental setup, the following tools are chosen:

- Programming language: Python
- Integrated Development Environment: Jupyter Notebook
- Signal (pre-)processing software: KerberosSDR Lite

The signal processing software - KerberosSDR Lite - is used to dump and save raw signal data from a multi-channel software-defined radio and has been established for the chosen hardware. The software is a Python-based software tool, which makes Python the obvious programming language. Jupyter Notebook is a functional integrated development environment (IDE) that operates online and independently - enabling easy file sharing.

4.3.2. HARDWARE

Following the conclusions written in section 4.1, a multi-channel receiver enables multiple new options to verify and validate ADS-B signals. As preliminary hardware for the experimental setup, the following equipment is chosen:

- Othernet's KerberosSDR Board - 4 channel coherent RTL-SDR
- 1090 MHz single channel transmitter

To conduct the experiment, both a signal receiver and transmitter are needed. For the transmitter, a random 1090 MHz transmitter can be chosen. For the receiver, the Othernet's KerberosSDR Board - 4 Channel Coherent RTL-SDR has been chosen. This coherent board contains four RTL-SDR R820T2 Receivers.

4.3.3. RESEARCH BACKGROUND

As part of the research background, the research problem and research objective are formulated. Relevant knowledge about ADS-B 1090MHz ES and related work done in this research field have been studied and summarized. Also, there is time and space left for 'open discovery'. This means that - within the scope of this research - there can raise additional applications, solutions, or opportunities. Some of these will be recommended for future research. However, if there are relevant findings - these can be included in this research. Both the literature review and 'open discovery' continue in the following research parts.

4.3.4. SIGNAL (PRE-)PROCESSING AND ANALYSIS

For data collection the described hardware, Othernet's KerberosSDR Board - 4 Channel Coherent RTL-SDR, is used combined with a fork of the corresponding software from the KerberoSDR [49]. The software allows the user to calibrate and synchronize the four channels with a built-in noise source. Various variables can be set, such as frequency, sampling rate, and gain settings. The fork [50], named KerberosSDR-lite, has some significant changes to enables data dumping. The ADS-B data is received with a sampling rate of 2 samples per μsecond and saved in an I/Q file, which can be easily transformed to an array of N array elements, where N is the number of antenna elements. For the KerberosSDR the number of antenna elements is four. An example of the incoming I/Q signal (100000 samples) is plotted for the four channels in figure 4.1. There can be observed that the four channels contain more or less the same data, but due to different reasons, such as noise and multi-path vulnerabilities, the I/Q information differs per channel.

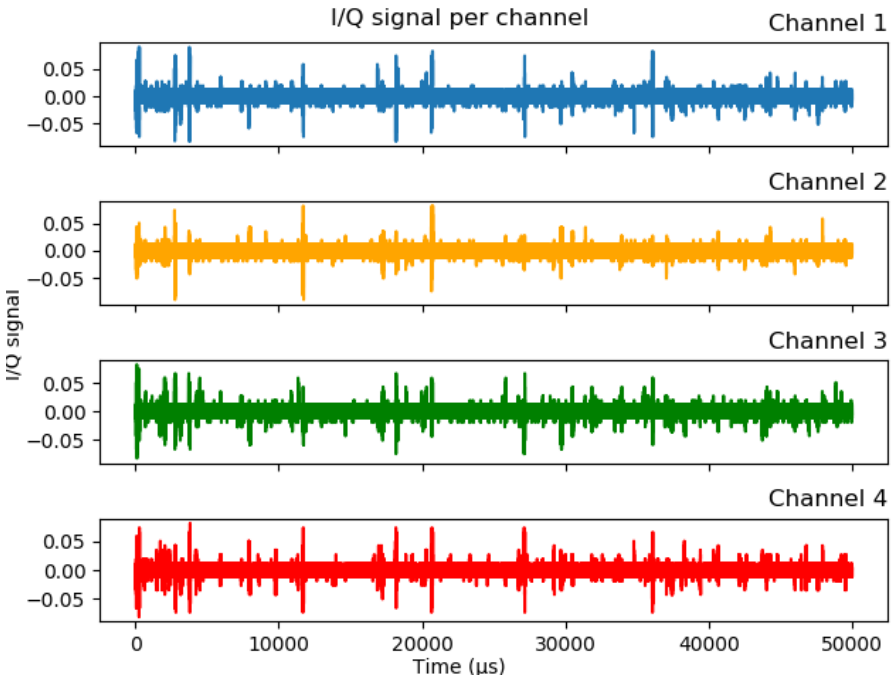

Figure 4.1: *100000 samples of incoming I/Q signal at 1090MHz.*

4.3.5. ADS-B VERIFICATION AND VALIDATION MODEL

The use of a coherent receiver enables the option to estimate the direction of arrival (DOA) via different approaches. Decoding the signal's position message and using a known own location enables the calculation of the DOA. Comparing those two angles can validate and verify the incoming ADS-B signals. Since more information is available in the different ADS-B signals, such as heading and airspeed, interpolation can be done to calculate the DOA for more message types, besides only the position message. Simultaneously, the DOA estimation can be done for all incoming messages. Additionally, to access the DOA's accuracy, the antenna elements of the coherent receiver can be used in two different setups. Chapter 5 provides a theoretical overview of the used decoding method, DOA estimation approaches and antenna element setups.

4.3.6. EXPERIMENTAL PHASE AND SETUP

To validate the performance of the chosen method and the developed validation and verification model, there is chosen to conduct an experiment using real data. Using actual ADS-B data and different attack scenarios enable a realistic and comparable environment to potential injection threats in the operation of ADS-B. Below, the chosen software, hardware and injection threat scenarios more explained more briefly, and a schematic overview of the experimental setup is shown in figure 4.2:

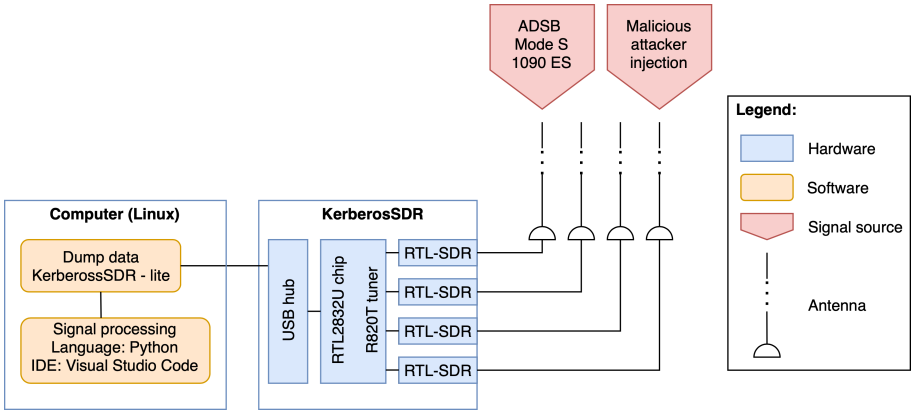

Figure 4.2: *Schematic overview of experimental setup.*

MALICIOUS ATTACKER INJECTION SCENARIOS

One of the essential elements of developing a signal validation and verification model, and to validate the performance of this model, is to list the different scenarios of threats. Within the ADS-B service implementation, an injection attacker can be classified using different properties. This research scopes on the injection of aircraft while airborne with as target a ground station. Costin et al. [40] made a distinction between three different properties: 1) place in the system, 2) physical position, and 3) the attacker's goals. McCallie et al. [15] distinguish three types of injection attacks. The first, with the ground station as a target, and the second with the aircraft as a target. The third type is the injection of multiple targets. Based on the studies mentioned above, and within the scope of this research, the following scenarios are set as potential threats:

- Static message injection: An signal is transmitted from a set location. The reference between the transmitter and the receiver is constant. There can be assumed, the attacker is able to create correctly formatted ADS-B messages, covering the correct message types, message order, legitimate, and reasonable flight parameters.
- Dynamic message injection: An signal is transmitted from a moving object. The reference between the transmitter and receiver is not constant. For this threat, the same assumption as for static message injection can be made.
- On-board equipment parameter injection: The on-board equipment can also be injected. For instance, the values of the position and velocity can be changed. If a malicious attacker changes the flight parameters in the on-board systems, the ADS-B system can still create a correctly formatted ADS-B messages, covering the correct message types and message order. Only the flight parameters are different from the actual parameters.

4.4. THESIS PROPOSAL OVERVIEW

In figure 4.3, pictured below, a flowchart is presented containing all steps to be taken from the initial problem statement and raw ADS-B data to a validated validation and verification method.

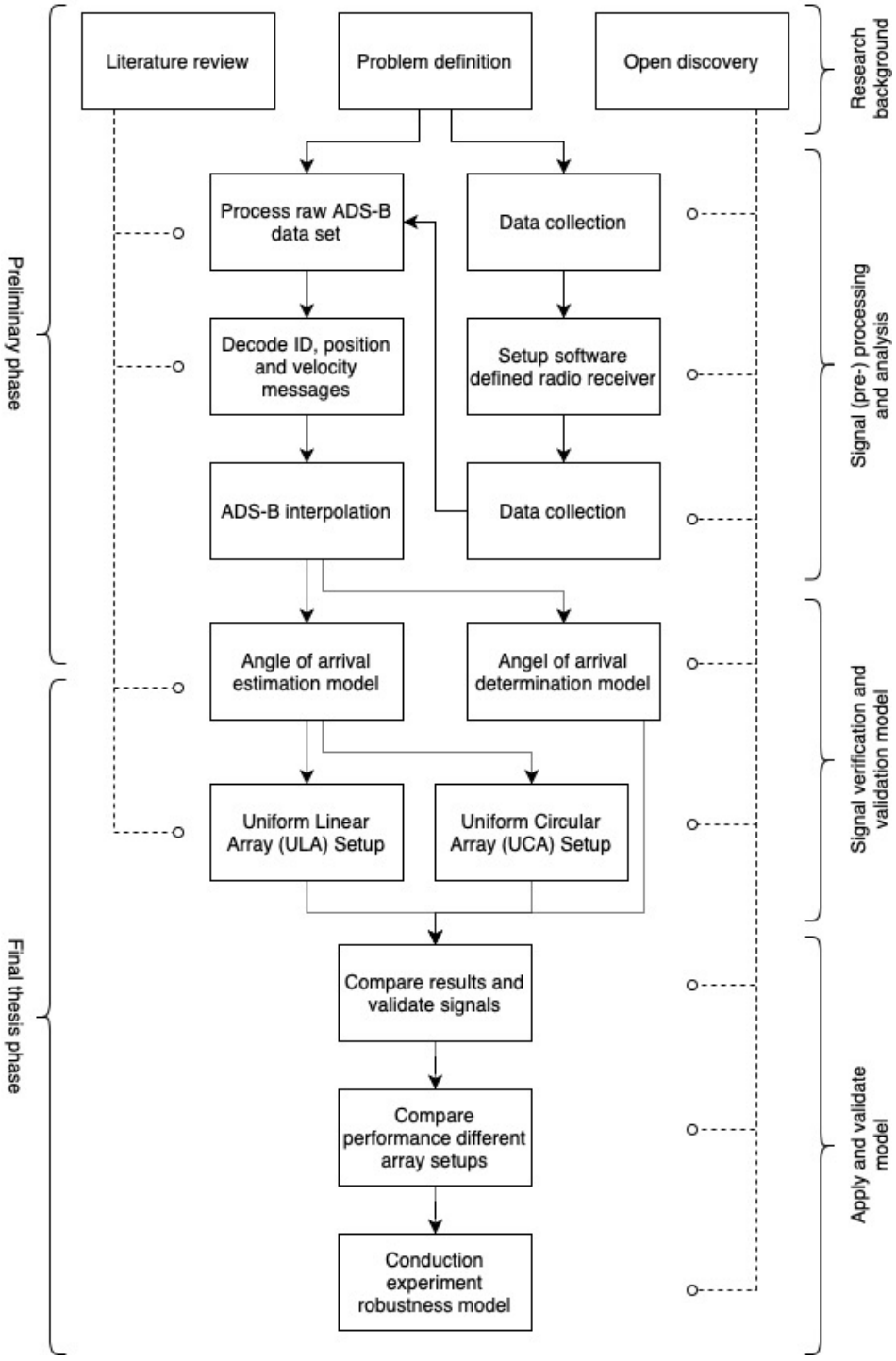

Figure 4.3: *Flowchart of research proposal: raw ADS-B data to validation and verification application*

5

THEORETICAL CONTENT

This chapter contains the theoretical content supporting the methodological approach proposed in the previous chapter. The theoretical content has been split up into three main subjects. To start with ADS-B signal decoding, followed by DOA estimation methods for multi-channel signal data sets, and last, the possible antenna element setups are presented. Note the made distinction between DOA calculation and DOA estimation.

5.1. SIGNAL DECODING AND POSITION INTERPOLATION

For decoding ADS-B and Mode S data, the open available Python library pyModeS [51] is used. The identification-, velocity- and position-message can be decoded from the signal using this library. By calculating the amplitude and phase, a significant jump or shift can separate the single signals. Not only error-free messages can be used, which generally can cause a significant loss of signal.

The decoded position messages provide coordinates in the EPSG:4326 WGS 84 decimal notation coordinate system. There is chosen to convert these values to a (Cartesian) EPSG:3034 coordinate system. Coordinate conversion is done for two reasons: 1) to get more accurate results of the direction of arrival calculations, and 2) the position interpolation in meters is more practical due to the unit of the velocity parameter.
Since only position messages provide position information to calculate the DOA, a method called 'kinematic path interpolation for movement data' is used to calculate the position of the other received messages. Just like the position messages, all messages have a known time of arrival. The assumptions made are that the travel time of the signals is identical for each signal, and the velocity information can be saved for the next position message. This can be assumed due to the short time intervals. To define the actual flight path the two dimensional kinetic motions in one time step are used in forms: position: $\mathbf{z}(t) = (z_x(t), z_y(t))$ and velocity: $\mathbf{v}(t) = (v_x(t), v_y(t))$ and an array with the actual time stamps of the other incoming signals. The following equations (5.1, 5.2 and 5.3) are used to solve the actual flight path.

$$position : \mathbf{z}(t) = \mathbf{z}(t) + \int_{t1}^{t2} \mathbf{v}(t)\, dt \tag{5.1}$$

$$velocity : \mathbf{v}(t) = \mathbf{v}(t) + \int_{t1}^{t2} \mathbf{a}(t)\, dt \tag{5.2}$$

$$acceleration : \mathbf{a}(t) = \frac{\Delta \mathbf{v}}{\Delta t} = \frac{\mathbf{v} - \mathbf{v}_0}{\Delta t} \tag{5.3}$$

An example of performing kinematic path interpolation for one flight is shown in figure 5.1. Here the green dots are the received position messages, and the blue dots are the calculated positions of the other incoming signals from the same aircraft. Using these positions, the DOA per signal can be calculated.

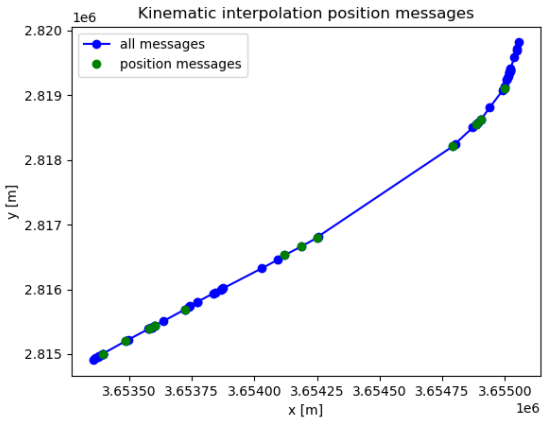

Figure 5.1: *Example flight path, where kinematic interpolation has applied*

(*Note the distinction made in DOA calculation and DOA estimation in the following sections 5.2 and 5.3*)

5.2. DIRECTION OF ARRIVAL CALCULATION

In order to calculate the angle of arrival from the claimed position in the ADS-B position message, equation 5.4 can be used. Here is θ the direction of arrival, δx the distance in x-direction and δy the distance in y-direction between the transmitter and receiver, which can be calculated using $(x_{aircraft} - x_{receiver})$ and $(y_{aircraft} - y_{receiver})$, respectively. The arctan2-function returns the angle in the plane between the positive x-axis and the ray between the transmitter and receiver. Its functionality is described more thoroughly below equation 5.4 [**?**].

$$\theta = \text{atan2}(\delta y, \delta x) \tag{5.4}$$

, where:

$$\text{atan2}(y,x) = \begin{cases} \arctan(\frac{y}{x}) & \text{if } x > 0 \\ \arctan(\frac{y}{x}) + \pi & \text{if } x < 0 \text{ and } y \geq 0 \\ \arctan(\frac{y}{x}) - \pi & \text{if } x < 0 \text{ and } y < 0 \\ +\frac{\pi}{2} & \text{if } x = 0 \text{ and } y > 0 \\ -\frac{\pi}{2} & \text{if } x = 0 \text{ and } y < 0 \end{cases}$$

To obtain the right angle value, in the same reference as the reference of the direction of arrival estimation, the results must be corrected. For both the ULA and UCA setup, the reference axis is the positive y-axis instead of the positive x-axis, so the correction is a 90 degrees subtraction from the calculated angle. For the ULA setup, a correction has to be done for the resolution of 180°. This results in the following mathematical equations (5.5, 5.6):

$$\theta_{ULA} = 180^\circ - \theta, \text{ for } \theta \leq 180^\circ \tag{5.5}$$

$$\theta_{ULA} = \theta - 180^\circ, \text{ for } \theta > 180^\circ$$

$$\theta_{UCA} = \theta - 90^\circ, \text{ for } 0 > \theta > 360^\circ \tag{5.6}$$

5.3. DIRECTION OF ARRIVAL ESTIMATION

Based on different signal properties, multiple methods are available to estimate the direction of an incoming propagating wave source relative to a set of antennas. The DOA estimation is also known as spectral-, angle of arrival- or bearing estimation. These techniques are widely applied in research areas of time series analysis [44]. Using a received sample of the output of an antenna array with N antennas, the DOA can be estimated for the investigated direction angles. Bhuiya et al. [**?**] describe the working principle of some applicable

methods: the elements of the antenna array collect signals from a propagating wave source at a different time due to the spacing of the antenna array. Here, the first antenna is used as the reference point. Assuming the incoming signal is narrowband, the delay of arrival can be defined as phase shift. The total signal and noise received by the antenna array can be expressed as in equation 5.7, where $\mathbf{x}$(t) is a N x *number of samples* array.

$$\mathbf{x}(t) = \mathbf{a}(\boldsymbol{\theta})\mathbf{S}(t) + \mathbf{n}(t) \tag{5.7}$$

Here, $\mathbf{a}(\boldsymbol{\theta})$ denotes the steering matrix with angles $\boldsymbol{\theta}$, $\mathbf{S}(t)$ denotes the signal column vector and $\mathbf{n}(t)$ the uncorrelated additive white Gaussian distributed noise vector. Note that in this study noise vector is assumed to be constant. The total signal an noise received per antenna (N^{th} element) at time t can be found in equation 5.8 below.

$$x_N(t) = S(t) \sum_{k=1}^{K} e^{j(N-1)\mu_i} + n_N(t) \tag{5.8}$$

With the spatial correlation matrix $\bar{R}_x$ and the scanning vector of the array $\bar{a}$, the earlier mentioned DOA estimation algorithms could be implemented. The software has an implementation based on the earlier mentioned PyArgus library [52]. However, there is no conclusion yet on the accuracy of the DOA implementation using this library.
Five methods for DOA estimation are described in the next section, and the calculations require knowledge about the spatial direction, signal gain, and expected phase relations:

Spatial correlation matrix
The first input element to be calculated is the spatial correlation matrix $\bar{R}$. This matrix contains the correlation of the spatial direction of the signal and the average receiver signal gain. For each number of samples (one complete ADS-B signal) found using the PyModeS library, the raw N-channel I/Q signal ($\mathbf{x}(t)$) can be transformed into the spatial correlation matrix by using equation 5.11:

$$\bar{R} = \frac{1}{N} \sum_{0}^{N-1} \mathbf{x}(t) \cdot \mathbf{x}(t)^H \tag{5.9}$$

In the case of a four-channel coherent SDR, for each sample of the multi-channel raw signal, this results in a spatial correlation matrix with size 4 x 4.

Steering matrix
The second input element to be calculated is the steering matrix. Bhuiya et al. [**?**] describes the steering matrix as m steering arrays, where each array contains the expected phase relationships for all channels. The steering arrays are defined to store the expected phase relations for the specific incident angles m. The specific incident angles are the angles within the resolution of measurements. These steering vectors are based on the interelement spacing d and the expected incident angles (θ). The ULA setup results in an array of shape N x 180, and for the UCA setup, this results in an array of shape N x 360. Using equation 5.12, the m*th* array element of the steering vector can be calculated. The sinus part of the exponent equals zero for the ULA setup.

$$\bar{a}(\theta_n)_m = e^{j2\pi d_x * cos(\theta_n) + d_y * sin(\theta_n)} \tag{5.10}$$

$\forall m = 0 \ldots (M-1)$

5.4. DIRECTION OF ARRIVAL ESTIMATION ALGORITHMS

Five commonly used algorithms, both linear DOA estimation algorithms and algorithms based on the decomposition of sub-spaces, are explained and described below [46]:

- Bartlett (Fourier) method
- Capon's method

- Burg's Maximum Entropy Method
- Linear Prediction Method
- Multiple Signal Classification

The elements of the incoming signals from the four channels are saved in an array of N array elements, which can be seen in chapter 4. After weighting each array element and having the received signal vector, the output of the array signal can be defined as $x_{rec}[n]$. Using the output of the array signal $x_{rec}[n]$ for each array element the average power for the entire array of N elements can be calculated. In PyArgus [52] this is called the spatial correlation matrix. This can be interpreted as the correlation between the spatial direction of the signal and the signal gain. The calculation can be done using equation 5.11.

$$\bar{R}_x = \frac{1}{N} \sum_{N=0}^{N-1} |x_{rec}[N]|^2 \tag{5.11}$$

To apply the DOA estimation algorithms PyArgus used, so called 'scanning vector' ($\bar{a}$) to store the expected phase relations for the specific incident angles. These scanning vectors are based on the interelement spacing d and the expected incident angles (θ). For instance, the uniform linear array setup results in an array with N x 180. Using equation 5.12, the mth array element of the scanning vector can be calculated.

$$\bar{a}(\theta)_m = e^{jm\beta dcos(\theta)}, \forall m = 0 \ldots (M-1) \tag{5.12}$$

With the spatial correlation matrix $\bar{R}_x$ and the scanning vector of the array $\bar{a}$, the earlier mentioned DOA estimation algorithms can be implemented. The software has a implementation based on the earlier mentioned PyArgus library [52]. There is no conclusion yet on the accuracy of the DOA implementation using this library.

5.4.1. BARTLETT METHOD

The Bartlett (Fourier) method consists of power spectra estimation and is known as the first developed DOA estimation technique [5]. The method provides a reduction of the variance of the periodogram in the cost of reduced resolution [45]. This is done by a maximization of the output power $\bar{R}_x$ for a certain direction. Equation 5.13 shows the calculation of the pseudo spectrum of Bartlett's method, where $\bar{R}_x$ is the spatial correlation matrix and $\bar{a}(\theta)$ is the scanning vector of the array.

$$P(\theta) = \bar{a}^H(\theta) \bar{R}_x \bar{a}(\theta) \tag{5.13}$$

A main limitation of Bartlett's methods is the ability to solve the angles is limited by the array half-power beam width [53].

5.4.2. CAPON'S METHOD

Capon's method is also known as the maximum variance distortionless response. The method is a maximum likelihood estimate of the power arriving from one direction (θ) [54]. This is done while considering all other sources are considered as interference. The signal to interference ratio had to be maximized, while passing the source signal undistorted in amplitude and phase [46]. Equation 5.14 is the pseudo spectrum of Capon - or maximum variance distortionless response - method, where $\bar{R}_x$ is the spatial correlation matrix and $\bar{a}(\theta)$ is the scanning vector of the array.

$$P(\theta) = \frac{1}{\bar{a}^H(\theta) R_x^{-1} \bar{a}(\theta)} \tag{5.14}$$

Godara et al. state that the method has better resolution properties than the earlier described Bartlett method [45].

5.4.3. BURG'S MAXIMUM ENTROPY METHOD

To implement Burg's Maximum Entropy Method (MEM), a power spectrum has to be found such that its Fourier transform equals the measured correlation. This correlation is subjected to the maximized entropy constraint [55]. Equation 5.15 is the pseudo spectrum of Burg's maximum entropy method, where $\hat{\bar{w}}$ is the weight of the optimal beamformer and $\bar{q}(\theta)$ is a vector denoting outputs of auxiliary beams of a beam-space processor. The number of outputs equals the number of dimensions of the vector $\bar{q}(\theta)$ [45].

$$P(\theta) = \frac{1}{\hat{\bar{w}}^T \bar{q}(\theta)} \tag{5.15}$$

Godara et al. state that the method has better resolution properties than the earlier described Bartlett and Capon method. Additionally, this method can estimate the direction of arrival with a lower signal-to-noise ratio [45].

5.4.4. LINEAR PREDICTION METHOD

Linear prediction method (LPM) is a method, which estimates the output from one antenna using linear combinations of the other antenna outputs. The mean square error between the estimation and the true output is minimized [53]. Equation 5.16 is the pseudo spectrum of LPM, where $\bar{R}_x$ is the spatial correlation matrix, $\bar{a}(\theta)$ is the scanning vector of the array and $\bar{u}_m^T$ is the Cartesian basis vector, which is chosen for prediction.

$$P(\theta) = \frac{\bar{u}_m^T \bar{R}_x^{-1} \bar{u}_m}{\left|\bar{u}_m^T \bar{R}_x^{-1} \bar{a}(\theta)\right|^2} \tag{5.16}$$

Islam et al. described the LPM has again a higher resolution than all the other methods described above (Bartlett, Capon, and MEM) [46].

5.4.5. MULTIPLE SIGNAL CLASSIFICATION

Multiple Signal Classification (MUSIC) is described as an efficient eigenstructure variant. The estimation of the direction of arrival, number of signals and signal strength [45]. Equation 5.17 is the pseudo spectrum of MUSIC method, where $\bar{E}_N$ is the noise subspace eigenvector and $\bar{a}(\theta)$ is the scanning vector of the array.

$$P(\theta) = \frac{1}{\bar{a}(\theta)\bar{E}_N\bar{E}_N^H\bar{a}(\theta)} \tag{5.17}$$

In the above-written part, the equation needs a calculation of the noise subspace eigenvectors, which can be determined from the spatial correlation matrix. Equation 5.18 is the equation to apply, where D is the number of signals, and M is the number of array elements.

$$E_N = [e_1 e_2 ... e_{M-D}] \tag{5.18}$$

5.5. UNIFORM LINEAR AND CIRCULAR ARRAY ANTENNA SETUP

Both the KerberosSDR hardware developer [56] and Zuokun Li et al. [5] describe two possible antenna setups and their advantages and disadvantages. Both have used the KerberosSDR hardware in combination with four omnidirectional antennas. The two antenna setups are uniform linear array (ULA) and uniform circular array (UCA).

Uniform linear array

This setup contains four omnidirectional antennas placed in a straight line in an equidistant manner. In figure 5.3, a schematic overview of the setup is shown [5]. The inter-element spacing (d) can be determined by $\lambda * s$, where λ is the frequency wavelength, and s is the interelement spacing factor. To avoid ambiguities, the possible calculation of multiple directions, it is recommended to use an inter-element spacing factor between 0.1 and 0.5. Commonly, 0.33 or 1/3 is used [56].
The ULA setup enables the one-dimensional direction of arrival estimation. This means the heading or pitch angle if the signal source with regards to the antenna's position can be estimated [56].

Uniform circular array

This setup contains four omnidirectional antennas placed in a circular or squared setup. In figure 5.2, a schematic overview of the setup is shown [5]. Like the ULA setup, the interelement spacing (d) can be determined by $\lambda * s$, with the same restrictions for the interelement spacing factor s to avoid ambiguities. In the UCA setup also the antenna array radius (R) has to be determined. This can be done by $\frac{\lambda * s}{\sqrt{2}}$, where λ is the frequency wavelength and s is the interelement spacing factor (0.33 recommended). The UCA setup enables the three-dimensional direction of arrival estimation [56].

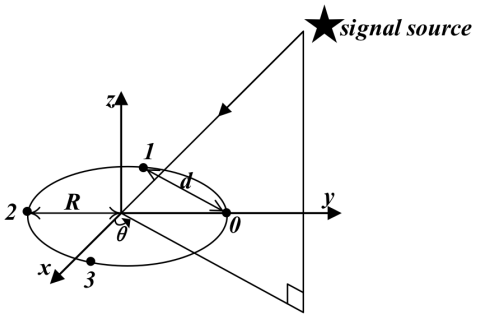

Figure 5.2: *Uniform circular array setup - Reprinted from [5]*

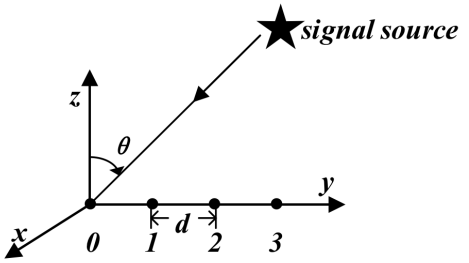

Figure 5.3: *Uniform linear array setup - Reprinted from [5]*

A disadvantage of the ULA setup is the resolution of 180 degrees. In other words: the setup cannot determine whether the signal transmitter is coming from the front or behind of the setup. On the other hand, the UCA setup is more vulnerable to multipath effects, which obviously could produce more wrong information. Zuokun Li et al. prefer the ULA setup to be used instead of the UCA setup. Moreover, the ULA setup gives the bearings less affected by multipath effects [56], [5]. Multipath effects occur when signals reflect on surrounding objects, causing the appearance of signals coming from another direction.

6

Results, Outcome and Relevance

6.1. Preliminary results and outcome

Some of the proposed applications have already been performed to indicate the working principles, as set in the research proposal and related technical content. This aims to demonstrate and prove that the solution is achievable. In this chapter, the preliminary results are pictured, including the operational signal receiving and processing setup, the decoding of incoming messages, DOA estimation for the ULA setup and, finally, an example of the outputs is given. As stated in the introduction, these are preliminary results, given in the hope of starting a discussion on ideas and suggestions not stated in this report so far.

6.2. Testing the experimental setup

The setup of the multi-channel coherent receiver, KerberosSDR, and the corresponding software is a time-consuming process. Since both the quantity and the quality of the incoming signals increase significantly, there is chosen to place the setup outside on a building's roof. This maximizes the received signal strength and the number of readable messages. Furthermore, it reduces multi-path effects. Besides, it is visible in the received data - this choice is endorsed by multiple researchers like Eichelberger et al. [57]. In figure 6.1 and 6.1 the setup is pictured being in operation.

Figure 6.1: *Experimental setup 1*

Figure 6.2: *Experimental setup 2*

In picture 6.2 there can be seen that the four antennas are aligned on a tripod. In this figure, the UCA array setup is used, as explained in chapter 5. The tripod enables both the UCA and ULA setup with an inter-element spacing of one-third or half the wavelength. The antennas can easily be attached using magnets. In figure 6.3 and 6.4, the top view of the respectively UCA and ULA tripod is shown. Note, the antenna order is numbered.

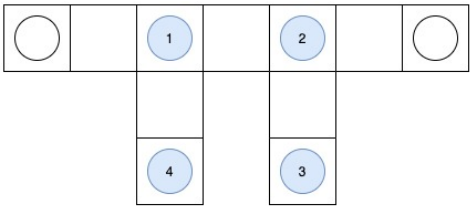

Figure 6.3: *UCA setup - schematic overview*

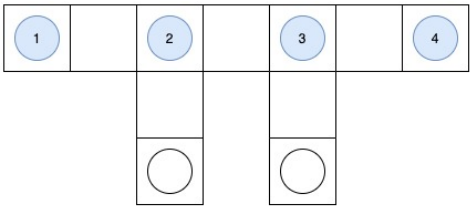

Figure 6.4: *ULA setup - schematic overview*

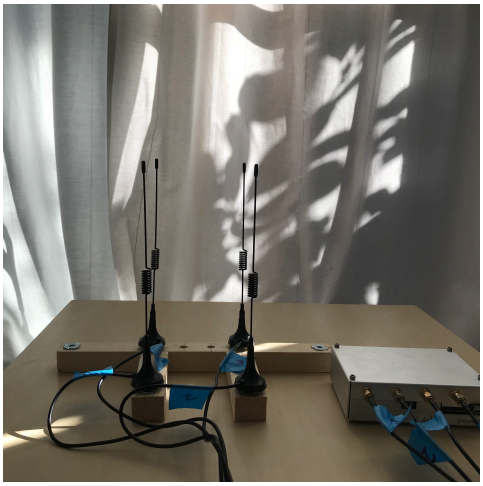

Figure 6.5: *Uniform circular array setup - KerberosSDR*

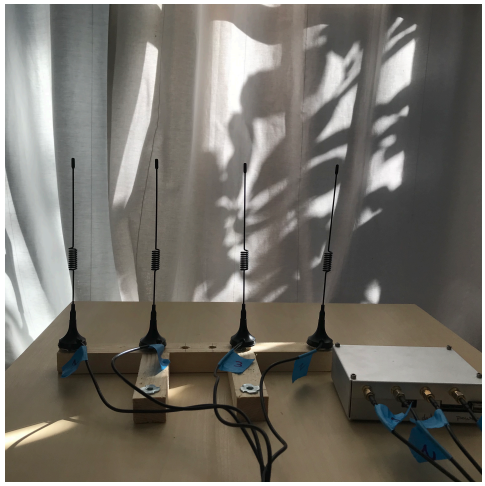

Figure 6.6: *Uniform linear array setup - KerberosSDR*

6.3. SIGNAL (PRE-)PROCESSING AND ANALYSIS

Having a properly working receiver, the next step is the signal (pre-)processing and analysis, including decoding and raw signal properties analysis. In chapter 4, research proposal, an example of the incoming I/Q signal (100000 samples) has been pictured in figure 4.1. Using equations 6.1 and 6.2, the amplitude and phase can be calculated respectively [58], [59].

$$Amplitude = \sqrt{I^2 + Q^2} \tag{6.1}$$

$$Phase = tan^{-1}(\frac{Q}{I}) \tag{6.2}$$

Here, I and Q are the in-phase components of the incoming I/Q signal. This results in the following amplitude and phase plot for one channel. In figure 6.7, the first 1000 samples (500 μseconds) have been pictured. In the amplitude plot, a clear constant noise is visible over the whole period, and three signals can be clearly seen in this sample. In the phase plot, a clear phase shift is visible at the same place of the signals in the sample. Using the PyModeS library [51] in Python, the single signals can be selected and decoded. In section 6.6, the decoded information has been pictured for an example flight.

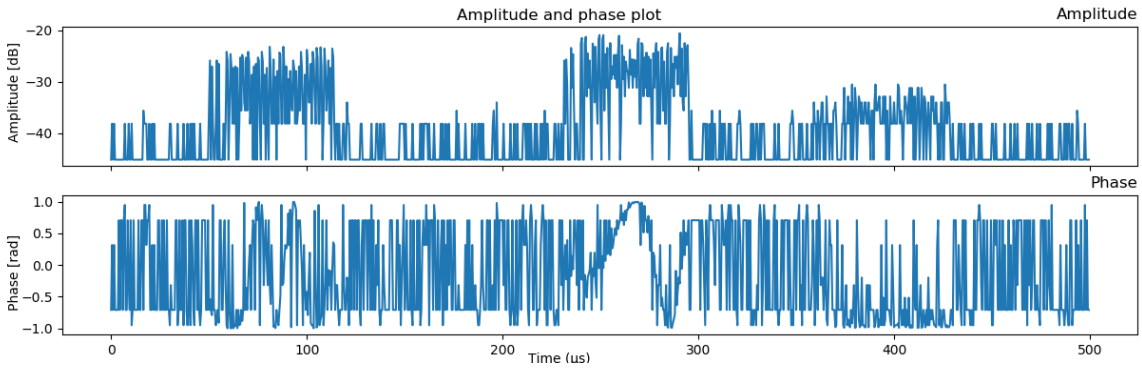

Figure 6.7: *Amplitude and phase plot for 1000 samples (= 500 µseconds)*

Using the multi-channel coherent receiver, KerberosSDR, the signal is received by four synchronized channels. In figure 6.8, the relative amplitude of a single ADS-B signal is plotted for the four channels. The signal is selected by the PyModeS library and can be decoded using this library either. In figure 6.9, the corresponding relative phase plot for the four channels is visible. Here, a small phase shift is visible per channel, caused by the different positions of the antennas, which is used for the DOA estimation later on.

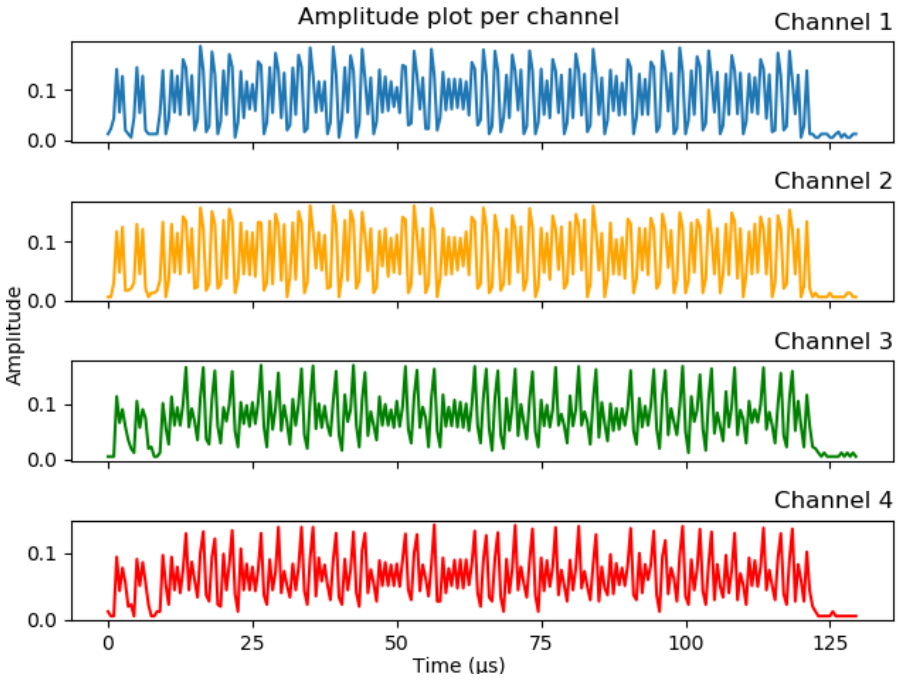

Figure 6.8: *Amplitude plot for a single ADS-B signal*

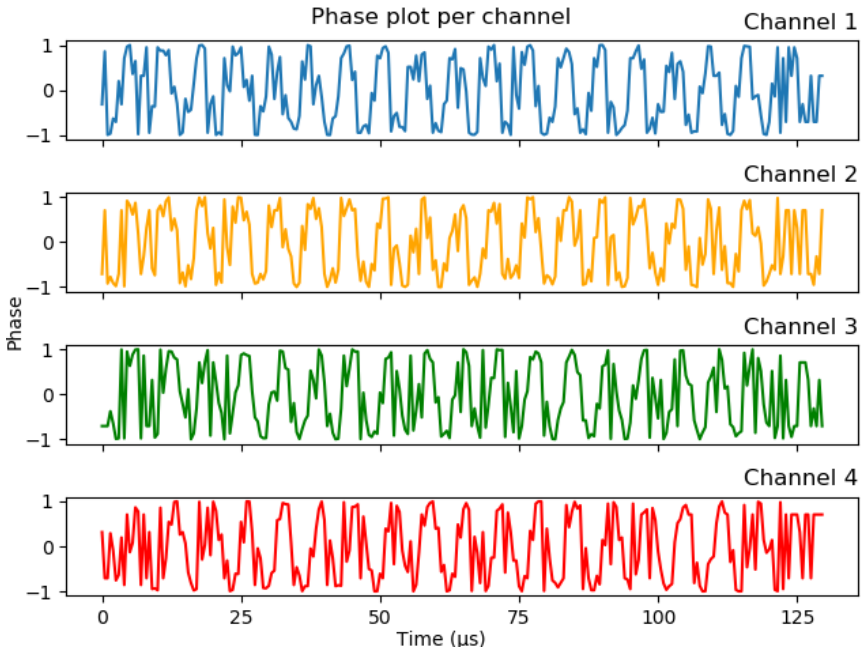

Figure 6.9: *Phase plot for a single ADS-B signal*

6.4. DIRECTION OF ARRIVAL ESTIMATION

The different direction of arrival methods, described in chapter 5, have been applied to a real data set for the ULA setup. The discussed algorithms for the ULA setup are available in the PyArgus library in Python [52]. After locating the signals in the data set, the different methods can be applied for the time period of the given signal. This results in an amplitude-incident-angle plot. By selecting the incident angle at the maximum amplitude, a single value for the DOA is found. In the thesis phase of this research, it is recommended to check whether this is valid. In this setup, the inter-element spacing was set to approximately one-third wavelength, which is equal to 0.09167965 cm. The results and corresponding observations of the different methods can be found below:

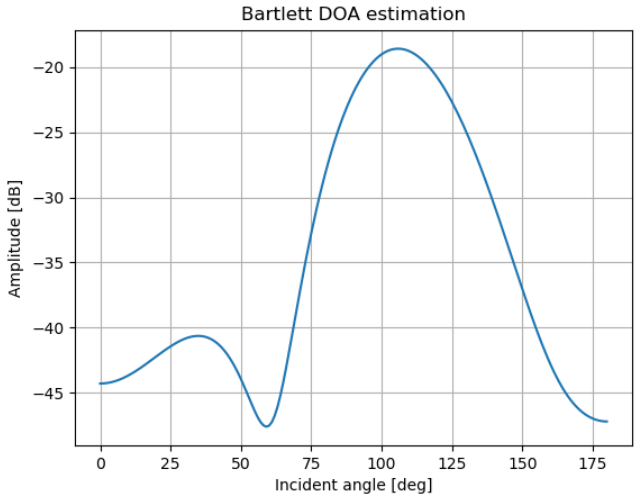

Figure 6.10: *Direction of arrival plot - Bartlett method*

In figure 6.10 the DOA plot - using the Bartlett method - is shown. Using an inter-element spacing of one third

the wavelength, four antenna elements, two samples per microsecond at a frequency of 1090MHz. The value found for the angle of arrival - using the maximum value - is 106 degrees.

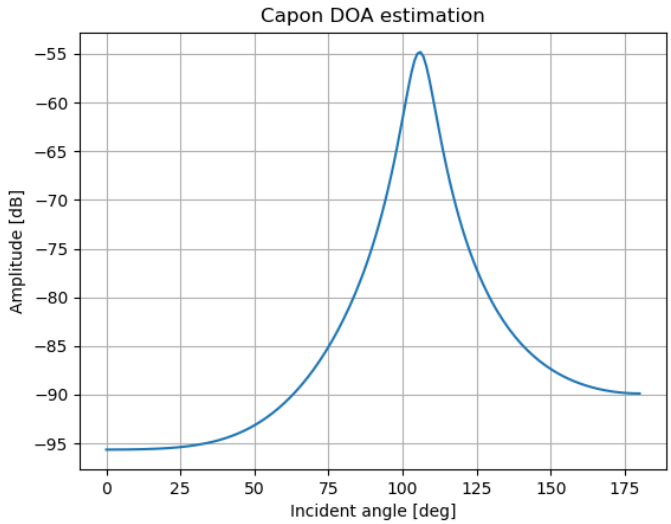

Figure 6.11: *Direction of arrival plot - Capon method*

In figure 6.11 the DOA plot - using the Capon method - is shown. Using an inter-element spacing of one third the wavelength, four antenna elements, two samples per microsecond at a frequency of 1090MHz. The value found for the angle of arrival - using the maximum value - is 106 degrees.

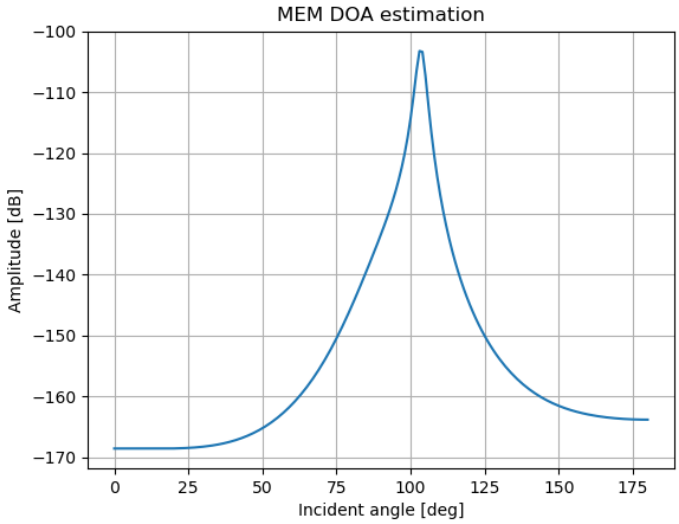

Figure 6.12: *Direction of arrival plot - MEM method*

In figure 6.12 the DOA plot - using the MEM method - is shown. Using an inter-element spacing of one third the wavelength, four antenna elements, two samples per microsecond at a frequency of 1090MHz. The value found for the angle of arrival - using the maximum value - is 103 degrees.

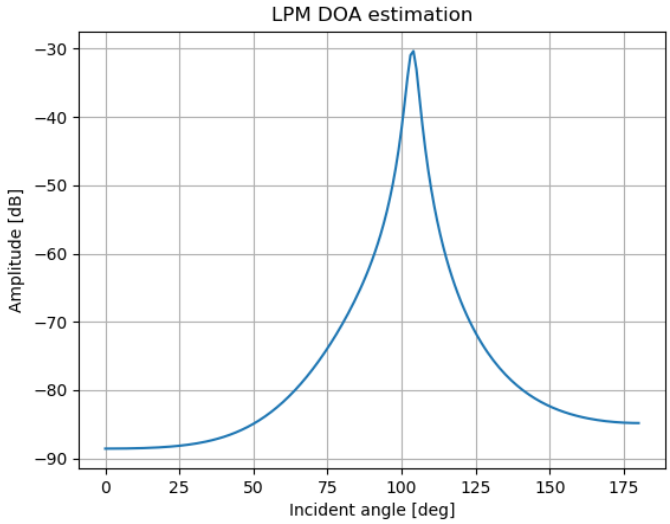

Figure 6.13: *Direction of arrival plot - LPM method*

In figure 6.13 the DOA plot - using the LPM method - is shown. Using an inter-element spacing of one third the wavelength, four antenna elements, two samples per microsecond at a frequency of 1090MHz. The value found for the angle of arrival - using the maximum value - is 104 degrees.

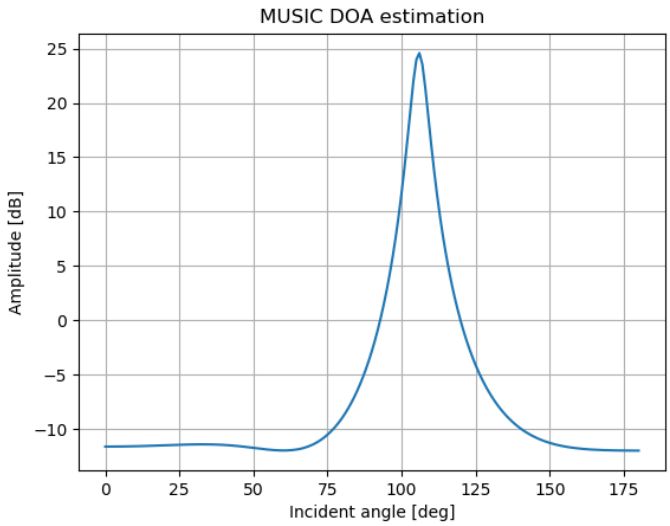

Figure 6.14: *Direction of arrival plot - MUSIC method*

In figure 6.14 the DOA plot - using the MUSIC method - is shown. Using an inter-element spacing of one third the wavelength, four antenna elements, two samples per microsecond at a frequency of 1090MHz. The value found for the angle of arrival - using the maximum value - is 106 degrees.

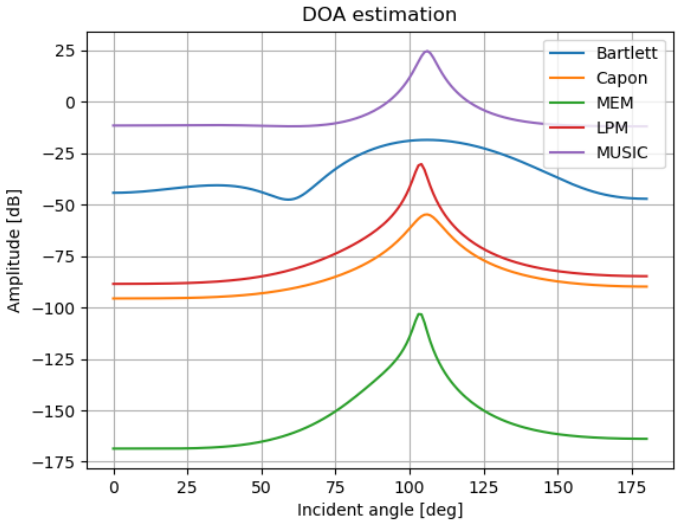

Figure 6.15: *Direction of arrival combined plot - multiple methods*

In figure 6.15, the different graphs of the used methods have been plotted in one figure. The main observation which can be done is that the estimated incident angles are close to each other. The incident angles at maximum amplitude are all within the range from 103 - 106 degrees. Furthermore, the different methods result in a different amplitude scale. This is due to the different calculation methods of the pseudo-spectra, as described in chapter 5. To compare the distribution of the incident angles fairly, it is useful to remove the varying scale. This can be done by normalization of the results. In figure 6.16, the different graphs of the used methods have been plotted normalized. In this case, the normalization is done by dividing the output array by its maximum value.

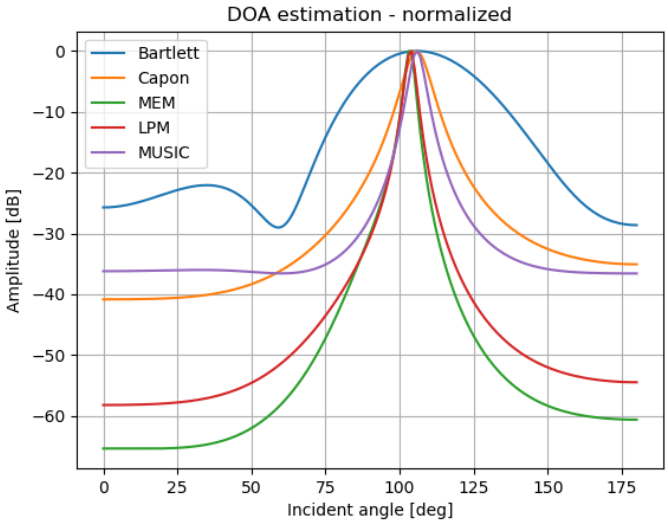

Figure 6.16: *Direction of arrival combined plot - multiple methods (normalized)*

6.5. OPEN DISCOVERY

As part of the 'open discovery' of this research, nothing has been worked out yet. However, the capabilities of the multi-channel coherent receiver and an article, found in the literature, about indoor localization using ADS-B signals [57], brought up another idea. The author used multi-lateration to determine the time of broadcasting. Based on this, he can determine the location of a single-channel receiver, with an accuracy up

to 25 meters. The research motivation is to use ADS-B signals instead of GPS signals since these have higher signal strength, enabling indoor localization. Within the discovery part of this research, there will be a possibility of determining the (multi-channel) receiver's position, based on the estimated DOA and the decoded GPS position from multiple incoming signals. Until now, this offers two opportunities: 1) The receiver could be able to verify and validate incoming signals without knowing its position. 2) During malfunction in the on-board - satellite-based - systems of an aircraft, this system would enable navigation, based on ADS-B signals coming from surrounding aircraft.

6.6. EXAMPLE APPLICATION MODEL - AIRCRAFT ICAO: '484CBA'

To provide an idea of the model to be performed, an example of the output of the current work done is given below in figure 6.17. In this screenshot from Flightradar24 [60], the actual flight path of flight ICAO '484CBA' is pictured. The two red dots are decoded position messages from the received signal, and the ULA antenna setup has been pictured. The red lines visualize the direction of arrival (α in figure) estimated by the DOA algorithms.

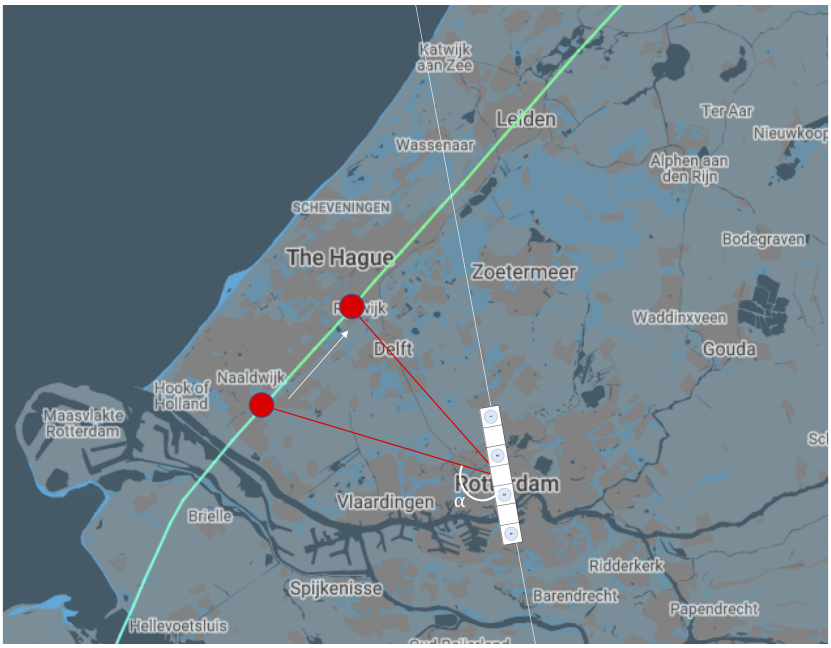

Figure 6.17: *Visualization of flight path and experimental setup*

From a received and saved four multi-channel data set, the information is decoded, and based on the known own position and the decoded GPS position, the direction of arrival is calculated. Furthermore, the direction of arrival estimation has been done using the four-channel data set. The information can be found in table 6.1 and 6.2, where the data set is filtered for one aircraft (ICAO: '484CBA'), and the columns contain the DF, the message in hexadecimal, the start and end sample from the data set, decoded latitude and longitude and the described DOA calculation and estimation. The DOA calculation has been done for the decoded position messages and the DOA estimation (MUSIC algorithm) for all incoming signals. For instance, using Kalman filtering, the position information and calculated DOA can be determined. Next to position, also velocity and heading can be decoded from these messages. This will be done in the next (thesis) phase of this research. One of the main observations is the gradual increase over time of both the calculated and estimated direction of arrival.

DF	Message in hexadecimal	Start sample	End sample	Latitude	Longitude	DOA calculation	DOA estimation
17	8D484CBAEA0DC85C797C08603EF7	332400	332660				96
21	A80001908DB00030A40000AB7E1F	869580	869840				98
17	8D484CBA582D02A68CD845A598D6	1688820	1689080	51.9759	4.2240	100.61	106
17	8D484CBA582BF2A6C2D85DBAB660	2327540	2327800	51.9771	4.2259	100.99	99
11	5D484CBAB22496	2491560	2491700				101
11	5D484CBAB22485	2698080	2698240				102
21	A80001908D69F71B7EDFDB337A38	3565040	3565300				99
21	A8000190FFF1DF2700048C54BD43	3565840	3566100				99
5	2800019061DFEC	3586440	3586580				98
4	2000053CFF7857	4136620	4136760				102
21	A80001908DB00030A40000AB7E1F	4424380	4424640				99
20	A000053C8D69F71B7EDFDBD6857E	4451840	4452100				100
21	A80001908DB00030A40000AB7E1F	4770160	4770420				99
17	8D484CBAEA0DC85C797C08603EF7	5167080	5167360				103
17	8D484CBA9910D11D185089C5C2DA	5297480	5297740				100
21	A8000190202CC371C348209E5F3C	5400240	5400520				99
20	A000053A8DB00030A40000B7A99C	5805840	5806120				108
17	8D484CBAF8230006004BB8473C78	6649920	6650180				108
11	5D484CBAB2249F	7358400	7358540				107
11	59484CBAB2249F	7376260	7376420				107
17	8D484CBA582B8614A0D31806126B	7386240	7386520	51.9873	4.2407	104.31	106
20	A00005388011DD26C0048C24900B	7594660	7594940				105
4	20000536FF1420	8578800	8578940				103
11	5D484CBAB22485	9958320	9958460				107
17	8D484CBA9910CF1CB84489BB6D39	12384660	12384940				110
20	A00005308D89F71B3EFFE0138DAD	12405260	12405540				110
4	2000051F0151F5	13110240	13110400				98
16	80A1851F5829F616E0D410D6CEF2	13311560	13311820				99
17	8D484CBA252CC371C3482041D0D2	15216420	15216680				111
4	2000051AFE9DCA	15942940	15943100				110
11	5D484CBAB2248E	15967320	15967460				111
4	2000051AFE9DCA	15974300	15974440				111
20	A000051A8D89F71B3F07E11AAC94	16364680	16364960				112
20	A000051AFFF1DF2640048ACDAFE4	16397420	16397700				114
17	8D484CBAF8230006004BB8473C78	16726160	16726440				114
17	8D484CBA5829961864D4B9A85379	16889480	16889740	52.0097	4.2735	112.97	114
11	5D484CBAB2248E	19272880	19273020				117
11	5D484CBAB2248E	19298600	19298760				117
11	5D484CBAB2248E	19324480	19324640				117
17	8D484CBA582942AD98DB5A97016C	19603940	19604220	52.0172	4.2842	116.27	115
21	A80001908D99F71B3F07E38F426C	19873960	19874240				115
21	A80001908031DF2600048A07485B	19875100	19875360				115
17	8D484CBA58293619D2D557CDBC20	19952860	19953140	52.0182	4.2859	116.79	113
11	5D484CBAB224A9	20360080	20360240				113
5	2800019061DFEC	20399980	20400140				113
20	A00005138D99F71AFF37E8AA971C	20419140	20419400				113
20	A00005138DB00030A40000E4AEB4	20446020	20446280				113
20	A00005138DA9F71AFF3FE92CB8A4	20572280	20572540				114

Table 6.1: *Example of the model's output so far - part 1*

DF	Message in hexadecimal	Start sample	End sample	Latitude	Longitude	DOA calculation	DOA estimation
17	8D484CBA5829261A46D5898537B5	20949620	20949880	52.0209	4.2898	118.06	115
11	5D484CBAB224A9	21835340	21835500				117
17	8D484CBA5829161AE0D5CCAB0CC8	22100520	22100780	52.0246	4.2950	119.80	118
4	200005110105B4	22299920	22300060				118
17	8D484CBA252CC371C3482041D0D2	22595100	22595380				115
17	8D484CBAEA0DC85C6D7C088A2BE3	23036120	23036400				116
20	A00005118051DF25C004894550CE	23105460	23105740				116
20	A00005118DB9F31AFFD7F844425E	23107940	23108220				116
20	A00005118DB00030A40000191AF0	23132840	23133120				116
17	8D484CBA582912AF8ADC34DC3E29	23366500	23366780	52.0286	4.3008	121.80	116
17	8D484CBA5829061BE4D63C90BE37	24056820	24057100	52.0306	4.3038	122.85	120
20	A00005108DB9F51AFFD7FBCF4ECA	24181900	24182180				117
17	8D484CBAE10190000000005BFD98	24182400	24182680				117
11	5D484CBAB2248E	25006480	25006660				115
20	A00005108DB00030A4000067C0D2	26122860	26123120				122
21	A80001908D99F91B3FFC005EF805	26645000	26645300				120
21	A8000190FF91DB25C0048A7CDB6D	26646100	26646380				120
20	A00005108D89F91B3FEC00DF5FA0	27446320	27446620				120
11	5D484CBAB22485	27457920	27458100				120
17	8D484CBA582902B1DCDD367E1EC6	27763740	27764020	52.0421	4.3205	129.03	120
17	8D484CBA9910C91C58048A17B34B	27793840	27794120				120
4	20000510FEF1BD	28199460	28199620				115
11	5D484CBAB2248E	28223400	28223580				116
17	8D484CBA5829061E56D7498E4189	28598240	28598540	52.0452	4.3249	130.73	120
17	8D484CBA9910C81C50048A7A1B8D	28774040	28774320				120
20	A00005108DB00030A4000067C0D2	28843120	28843400				120
20	A00005108DB00030A4000067C0D2	29150460	29150740				120
21	A80001908D79F51AE0140125A315	29171880	29172160				121

Table 6.2: *Example of the model's output so far - part 2*

7

CONCLUSION

This preliminary report presented relevant knowledge, written as an ADS-B background, related work in the literature, a research proposal, relevant theoretical content and preliminary results regarding decoding raw signals and direction of arrival estimation. As stated in the introduction, the information given in the report is in the hope to start a discussion on ideas and suggestions not stated so far.

In the literature part of this report (chapter 2 and 3) was found that to verify and validate ADS-B signals, commonly a change in protocol or hardware is required. To find a cost-effective countermeasure against malicious signal injection, the applications and opportunities of using a multi-channel coherent receiver have been studied. Combining decoded information and processing the raw-signal properties from the incoming signal enables a cost-effective validation and verification technique. Using the direction of arrival might be the most feasible candidate to mitigate malicious ADS-B signal injection. To the best of knowledge, nobody has done this before.

This conclusion led to a research proposal. This proposal contains a study about the validation and verification of ADS-B signals, while the network is attacked by different malicious injection scenarios. The objective is to suggest a possible and cost-effective solution, which improves the security and integrity of raw Mode-S/ADS-B signals, by designing a tool which can verify and validate the low-level signal. Chosen is to indicate how the functionalities of a coherent multi-channel receiver can solve the stated problem.

The related theoretical content, containing: signal decoding, direction of arrival algorithms, and two antenna setups, are explained, followed by the preliminary results and outcome. These results demonstrated that the proposed solution is potentially achievable. Both signal decoding, resulting in the calculation of the direction of arrival and the direction of arrival estimation for an uniform linear antenna array has been demonstrated to work. However, to build an accurate validation and verification model, the accuracy of these methods has to be tested and possibly increased. Using real data and active malicious injection, the model must be validated in the thesis phase of this research.

BIBLIOGRAPHY

[1] T. Li and B. Wang, *Sequential collaborative detection strategy on ADS-B data attack,* International Journal of Critical Infrastructure Protection (2019), 10.1016/j.ijcip.2018.11.003.

[2] M. Leonardi, L. Di Gregorio, and D. Di Fausto, *Air traffic security: Aircraft classification using ADS-B message's phase-pattern,* Aerospace (2017), 10.3390/aerospace4040051.

[3] M. Strohmeier, V. Lenders, and I. Martinovic, *Security of ADS-B: State of the Art and Beyond,* arXiv preprint arXiv:1307.3664 (2013), arXiv:1307.3664 .

[4] M. Monteiro, A. Barreto, T. Kacem, D. Wijesekera, and P. Costa, *Detecting malicious ADS-B transmitters using a low-bandwidth sensor network,* in *2015 18th International Conference on Information Fusion, Fusion 2015* (2015).

[5] Z. Li and D. Zhang, *Application Research on DOA Estimation Based on Software-Defined Radio Receiver,* J. Phys.: Conf. Ser. 1617 012047 (2020).

[6] M. Riahi Manesh and N. Kaabouch, *Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system,* (2017).

[7] J. Sun, *The 1090MHz Riddle (GNU GPL open-source license ed., v2),* (2020), http://mode-s.org .

[8] InternationalCivilAviationOrganization, *Technical Provisions for Mode S Services and Extended Squitter, 2nd Edition,* (2012).

[9] F. A. Administration, *Legal information institute. (2010, may 28). 14 cfr § 91.227 - automatic dependent surveillance-broadcast (ads-b) out equipment performance requirements.* (2010), Retrieved 19 October 2020, from https://www.law.cornell.edu/cfr/text/14/91.227) .

[10] EUROCONTROL, *Automatic dependent surveillance – broadcast (ads-b),* (2020), Retrieved 19 October 2020, from https://www.eurocontrol.int/service/automatic-dependent-surveillance-broadcast .

[11] Wikipediacontributors, *Automatic dependent surveillance – broadcast,* (2020), Retrieved 19 October 2020, from https://en.wikipedia.org/wiki/Automatic_dependent_surveillance_%E2%80%93_broadcas .

[12] Federal Aviation Administration, DOT. (2015, February). Automatic Dependent Surveillance-Broadcast (ADS-B) Out Performance Requirements To Support Air Traffic Control (ATC) Service; Technical Amendment (2015–02579). Federal Register. Retrieved from https://www.federalregister.gov/documents/2015/02/09/2015-02579/automatic-dependent-surveillance-broadcast-ads-b-out-performance-requirements-to-support-air-traffic .

[13] W. Coady and R. Landry, *Software-defined radio to support aviation efficiency,* Article de recherche. Substance ÉTS. https://substance.etsmtl.ca/en/software-defined-radio-support-aviation-efficiency (2014).

[14] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, *Short paper: Reactive jamming in wireless networks - How realistic is the threat?* in *WiSec'11 - Proceedings of the 4th ACM Conference on Wireless Network Security* (2011).

[15] D. McCallie, J. Butts, and R. Mills, *Security analysis of the ADS-B implementation in the next generation air transportation system,* International Journal of Critical Infrastructure Protection (2011), 10.1016/j.ijcip.2011.06.001.

[16] M. Strohmeier, V. Lenders, and I. Martinovic, *On the security of the automatic dependent surveillance-broadcast protocol,* IEEE Communications Surveys and Tutorials (2015), 10.1109/COMST.2014.2365951, arXiv:1307.3664 .

[17] M. Schäfer, V. Lenders, and I. Martinovic, *Experimental analysis of attacks on next generation air traffic communication,* in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2013).

[18] L. Purton, H. Abbass, and S. Alam, *Identification of ADS-B system vulnerabilities and threats,* in *ATRF 2010: 33rd Australasian Transport Research Forum* (2010).

[19] K. Zeng, K. Govindan, and P. Mohapatra, *Non-cryptographic authentication and identification in wireless networks,* IEEE Wireless Communications (2010), 10.1109/MWC.2010.5601959.

[20] M. Leonardi and F. Gerardi, *Aircraft mode S transponder fingerprinting for intrusion detection,* Aerospace (2020), 10.3390/aerospace7030030.

[21] H. Liu, H. Darabi, P. Banerjee, and J. Liu, *Survey of wireless indoor positioning techniques and systems,* (2007).

[22] Wikipedia contributors. (2020, September 18). Multilateration. Retrieved 19 October 2020, from https://en.wikipedia.org/wiki/Multilateration .

[23] A. Savvides, H. Park, and M. B. Srivastava, *The bits and flops of the n-hop multilateration primitive for node localization problems,* in *Proceedings of the ACM International Workshop on Wireless Sensor Networks and Applications* (2002).

[24] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm, *Bringing up OpenSky: A large-scale ADS-B sensor network for research,* in *IPSN 2014 - Proceedings of the 13th International Symposium on Information Processing in Sensor Networks (Part of CPS Week)* (2014).

[25] J. Johnson, H. Neufeldt, and J. Beyer, *Wide area multilateration and ADS-B proves resilient in Afghanistan,* in *ICNS 2012: Bridging CNS and ATM - Conference Proceedings* (2012).

[26] R. E. Kalman, *A new approach to linear filtering and prediction problems,* Journal of Fluids Engineering, Transactions of the ASME (1960), 10.1115/1.3662552.

[27] D. Fox, J. Hightower, L. Liao, D. Schulz, and G. Bordello, *Bayesian filtering for location estimation,* IEEE Pervasive Computing (2003), 10.1109/MPRV.2003.1228524.

[28] G. Welch and G. Bishop, *An Introduction to the Kalman Filter,* In Practice (2006), 10.1.1.117.6808.

[29] B. Kovell, B. Mellish, T. Newman, and O. Kajopaiye, *Comparative Analysis of ADS-B Verification Techniques,* GPS Solutions 20(3) (2012).

[30] K. Sampigethaya, R. Poovendran and L. Bushnell, "*Assessment and mitigation of cyber exploits in future aircraft surveillance,*" 2010 IEEE Aerospace Conference, Big Sky, MT, 2010, pp. 1-10, doi: 10.1109/AERO.2010.5446905. .

[31] EUROCONTROL, *Action plan 17: future communications study, brussels, belgium: Eurocontrol,* (2007).

[32] M. Sajatovi, *L-DACS 1 System Definition Proposal: Deliverable 3-Design Specifications for L-DACS 1 Prototype,* (2007).

[33] T. Gräupl, M. Ehammer, and S. Zwettler, *L-DACS1 air-to-air data-link protocol design and performance,* in *ICNS 2011 - Integrated Communications, Navigation and Surveillance Conference: Renovating the Global Air Transportation System, Proceedings* (2011).

[34] O. Baud, N. Honore, and O. Taupin, *Radar / ADS-B data fusion architecture for experimentation purpose,* in *2006 9th International Conference on Information Fusion, FUSION* (2006).

[35] W. Liu, J. Wei, M. Liang, Y. Cao, and I. Hwang, *Multi-sensor fusion and fault detection using hybrid estimation for air traffic surveillance,* IEEE Transactions on Aerospace and Electronic Systems (2013), 10.1109/TAES.2013.6621819.

[36] T. Leinmüller, E. Schoch, and F. Kargl, *Position verification approaches for vehicular ad hoc networks,* IEEE Wireless Communications (2006), 10.1109/WC-M.2006.250353.

[37] F. K. Jondral, *Software-defined radio - Basics and evolution to cognitive radio,* (2005).

[38] E. G. Piracci, G. Galati, and M. Pagnini, *ADS-B signals reception: A Software Defined Radio approach,* in *2014 IEEE International Workshop on Metrology for Aerospace, MetroAeroSpace 2014 - Proceedings* (2014).

[39] M. Leonardi and M. Maisano, *Degarbling technique for low cost ADS-B receivers,* in *2019 IEEE International Workshop on Metrology for AeroSpace, MetroAeroSpace 2019 - Proceedings* (2019).

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

[41] M. Leonardi, E. Piracci, and G. Galati, *ADS-B jamming mitigation: A solution based on a multichannel receiver,* IEEE Aerospace and Electronic Systems Magazine (2017), 10.1109/MAES.2017.160276.

[42] M. Zhou and A. J. Van Der Veen, *Improved blind separation algorithm for overlapping secondary surveillance radar replies,* in *2011 4th IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing, CAMSAP 2011* (2011).

[43] N. Petrochilos and A. J. van der Veen, *Algebraic algorithms to separate overlapping secondary surveillance radar replies,* IEEE Transactions on Signal Processing (2007), 10.1109/TSP.2007.894248.

[44] L. C. Godara, *Applications of antenna arrays to mobile communications, part I: Performance improvement, feasibility, and system considerations,* Proceedings of the IEEE (1997), 10.1109/5.611108.

[45] L. C. Godara, *Application of antenna arrays to mobile communications, part II: Beam-forming and direction-of-arrival considerations,* in *Adaptive Antennas for Wireless Communications* (2009).

[46] A. I. Islam, Ren, *Performance Study of Direction of Arrival (DOA) Estimation Algorithms for Linear Array Antenna,* https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=5166789 (2009).

[47] A. Vesa and A. Iozsa, *Direction - Of - Arrival estimation for uniform sensor arrays,* in *2010 9th International Symposium on Electronics and Telecommunications, ISETC'10 - Conference Proceedings* (2010).

[48] C. Reck, U. Berold, J. Schür, and L. P. Schmidt, *Direction of arrival sensor calibration based on ADS-B airborne position telegrams,* in *European Microwave Week 2009, EuMW 2009: Science, Progress and Quality at Radiofrequencies, Conference Proceedings - 6th European Radar Conference, EuRAD 2009* (2009).

[49] Rtlsdrblog, *Kerberossdr*. GitHub. Retrieved 14 June 2020, from https://github.com/rtlsdrblog/kerberossdr (2020).

[50] Sun, J, *Kerberossdr-lite*. GitHub. Retrieved 20 August 2020, from https://github.com/junzis/kerberossdr-lite (2020).

[51] J. Sun, H. Vû, J. Ellerbroek, and J. M. Hoekstra, *pymodes: Decoding mode-s surveillance data for open air transportation research,* IEEE Transactions on Intelligent Transportation Systems (2019), 10.1109/TITS.2019.2914770.

[52] Peto, Tamas, *PyArgus*. GitHub. Retrieved 30 August 2020, from https://pypi.org/project/pyargus/ (2020).

[53] S. Chandran, "Smart Antennas for Wireless Communications (with MATLAB) (Gross, F.; 2005) [Reviews and Abstracts]," in IEEE Antennas and Propagation Magazine, vol. 51, no. 3, pp. 134-134, June 2009, doi: 10.1109/MAP.2009.5251212. .

[54] J. Capon, *High-Resolution Frequency-Wavenumber Spectrum Analysis,* Proceedings of the IEEE (1969), 10.1109/PROC.1969.7278.

[55] Burg. J., *Maximum entropy spectral analysis*, presented at the 37th Annu. Meeting, Society Exploration Geophysics, Oklahoma city, OK, (1967) .

[56] RTL-SDR.COM, *KerberosSDR Quickstart Guide,* Retrieved 21 September 2020, from https://www.rtl-sdr.com/ksdr/ (2020).

[57] M. Eichelberger, S. Tanner, K. Luchsinger, and R. Wattenhofer, *Indoor localization with aircraft signals*, in *SenSys 2017 - Proceedings of the 15th ACM Conference on Embedded Networked Sensor Systems* (2017).

[58] J. Sun and J. Hoekstra, *Analyzing Aircraft Surveillance Signal Quality at the 1090 Megahertz Radio Frequency*, (2020), ICRAT2020.

[59] Whiteboard Web, *I/Q Data for Dummies*, Retrieved 27 October 2020, http://whiteboard.ping.se/SDR/IQ. http://whiteboard.ping.se/SDR/IQ, (2020) .

[60] Flightradar24, *Live Flight Tracker - Real-Time Flight Tracker Map*, Retrieved 27 October 2020, from https://www.flightradar24.com/data/aircraft/ph-bvf, (2020) .