UNIVERSITEIT VAN AMSTERDAM

System and Network Engineering

MSc Security and Network Engineering
Research Project II

Securing the Automatic Dependent Surveillance-Broadcast (ADS-B) protocol against spoofing

July 5, 2020

Tim de Boer
tim.deboer@os3.nl

Assessor
Prof. dr. ir. C.T.A.M. de Laat
University of Amsterdam

Supervisor
Dr. ir. J.J.P. van Es
Koninklijk Nederlands Lucht- en Ruimtevaartcentrum

Abstract

Automatic Dependent Surveillance-Broadcast (ADS-B) is a supplementary surveillance technique to improve safety in air transport. The protocol itself is an extension of earlier, older transponder techniques where security, in terms of authenticity, have not been taken into account. With the expected extra aircraft movements for the next decades, reliable and more accurate surveillance techniques are necessary. Because the protocol is vulnerable to spoofing, and the dependency on this protocol is growing, this research focuses on the possibility to detect spoofed ADS-B messages. Background on the ADS-B protocol is provided, and what fingerprintable parameters of the Radio Frequency (RF) signal could be used as assessable parameters. This study analysed the signal quality and the Doppler shift to verify values claimed by transmitted ADS-B messages, by moving aircraft. To improve the protocol itself, a revised version of ADS-B protocol, with integrity in mind, is proposed. This is done by signing the ADS-B messages with the use of asymmetric cryptography together with a Public Key Infrastructure (PKI).

Contents

1 Introduction

Since commercial aviation is ever-growing, there is a need for additional and accurate visibility for Air Traffic Control Specialists (ATCS). In 1943, the military air traffic controllers started to use the first radar. However, they are accurate up to a few hundred meters [1]. Only in the 1970s, aviation started to use transponders (short for transmitter-responder).

Together with the developments of the Traffic Alert and Collision Avoidance System (TCAS), the ADS-B was finally introduced in 2005. Aircraft equipped with ADS-B periodically transmit their position and other information (such as registration number, flight number, speed, altitude, course, and intentions) to ground stations and neighbouring ADS-B equipped aircraft.

ADS-B is primarily intended as a means for Air Traffic Control (ATC) to determine the position of an aircraft. The system was born out of the realisation that modern aircraft, thanks to Global Navigation Satellite Systems (GNSSs) such as the Global Positioning System (GPS), know their position much more accurately than can be determined with radar systems on the ground [2].

To this day, the ADS-B protocol itself has no way to guarantee the authenticity and integrity of the messages, as it has no built-in security. As a result, the protocol is sensitive to so-called replay-attacks, making it possible to provide false information to ATCs. Replay-attacks are a type of attack in which valid data transmission is maliciously or fraudulently repeated.

This research focuses on finding possible attacks against ADS-B, specifically, the replay-attacks that can mislead ATCS. These attacks will be researched from a theoretical point of view. To improve upon the ADS-B protocol, a new extended version of the protocol is proposed, that uses the advantages of modern cryptography to safeguard integrity.

2 Research Question

With this research, we aim to determine if it is possible to detect malicious ADS-B messages. This relatively old protocol was never made with security in mind and the ATC and other aircraft depend on this protocol, especially in busy airspaces.

The main research question for this project is defined as follows:

> How can malicious broadcasts of the ADS-B be detected to protect ATC from Denial-of-Service (DoS) and disinformation attacks?

To support the main research question the following sub-questions are defined:

- What types of attacks are possible in terms of DoS and disinformation?
- How can detection and filtering algorithms aid in signal integrity and authenticity validation?
- What kind of advantages can signal fingerprinting offer for the detection of malicious broadcasts?

To answer the research question a literature study is conducted on the protocol, its weaknesses are investigated and known theoretical attacks explored. Exploratory research is used to identify potential attack vectors that may aid in disinformation towards ATCS.

In addition, an investigation whether it is possible to detect these attacks will be carried out. These results will be used to analyse, which aspects can be potentially improved. For instance, the detection and filtering based on location using triangulation and/or trilateration, other forms of fingerprinting, and adaptations of transponder equipment.

3 Related Work

Over the past years research has been done on the two main topics regarding ADS-B; detecting malicious broadcasts and improving/securing the ADS-B protocol.

Costin et al. investigated the (in)security aspects of the ADS-B protocol and demonstrated that attacks are both easy and feasible for a moderately sophisticated attacker. Attacks range from passive attacks (eavesdropping) to active attacks (message jamming, replaying of injection). Attacks have been executed with the use of Universal Software Radio Peripheral (USRP), a widely available Software-Defined Radio (SDR) in combination with open-source software GNU Radio [3].

McCallie et al. analysed the security vulnerabilities of the ADS-B implementation and described the potential impact that the attacks may have on air transportation operations. The research describes a comprehensive understanding of the threats related to the ADS-B implementation and risk analysis. In addition, the research provides recommendations that could enhance security if integrated into the ADS-B implementation plan [4].

Xuhang Ying et al. created a ADS-B message classifier based on a Deep Neural Network (DNN), to enhance detection of unauthorised broadcasts. This is done using raw in-phase and quadrature components (IQ)-samples from the physical layer, namely the Radio Frequency (RF) broadcast, combined with the decoded ADS-B data [5].

Also, Strohmeier et al. comprehensively analysed vulnerabilities and existing attacks. Afterwards, they surveyed the existing research on countermeasures and categorise it into approaches that are applicable in the short term and research of secure new technologies deployable in the long term [6].

Cindy Finke et al. briefly described two basic encryption principles (asymmetric vs symmetric encryption) and the advantages and disadvantages of these principles in general. The encryption principles could be fundamental for security enhancement for ADS-B broadcasts [7].

Wei-Jun Pan et al. looked closer into an enhancement of ADS-B and proposed signing the ADS-B messages with a public key certificate (X.509) to prevent replay attacks and verification of the authenticity of the message [8].

4 Background

This section provides relevant background on the available surveillance techniques (Section 4.1) and the ADS-B protocol itself (Section 4.2).

4.1 Surveillance Techniques

For the purpose of safe (air) traffic control guidance, surveillance is required for the ATCS. The most common and oldest surveillance technique is the radar. The radar is mostly referred as Primary Surveillance Radar (PSR) and works on the principle of reflecting electromagnetic waves. Together with the time delay between transmitting and receiving a reflected wave, the distance can be calculated. The PSR works independently, as it works on almost every object that reflects the waves. The disadvantage of PSR is the fact it is limited in terms of range and accuracy.

To identify the aircraft more easily the transponder was invented, where the ATC is able to interrogate the aircraft to reply with requested data. Different modes of the transponder have been developed over time;

- Mode A; 4-digit octal identification code assigned by the ATCS via radio communication
- Mode C; the aircraft pressure altitude
- Mode S; multiple information types are possible (speed, altitude, course, position) combined with an unique 24-bit address assigned by the International Civil Aviation Organization (ICAO)

Given that commercial aviation is still growing in its popularity, extra information and especially more accurate data is needed in order to cope with the extra traffic in busy airspaces. For this purpose the Automatic Dependent Surveillance-Broadcast (ADS-B) and Traffic Information Service - Broadcast (TIS-B) were invented.

4.2 ADS-B protocol

ADS-B is based on the Mode S transponder squitter (unsolicited downlink transmissions), with the difference that additional data is added to the message. This is known as the Extended Squitter (1090ES). The ADS-B protocol enhances the safety by broadcasting the position and speed every second, which makes air-traffic visible for ATC and other aircraft. Where the PSR is completely independent, as it does not require any cooperation of the aircraft itself, the ADS-B is dependent on data provided by other avionics and requires cooperative equipment (transponder) to participate in the surveillance.

The Extended Squitter (1090ES) transponder format is illustrated in Figure 1 and Table 1, which always starts with a $8\mu s$ preamble. The preamble is always constructed as illustrated in Figure 2 and is used for clock synchronisation on the receiving side and to identify both high and low amplitude transmissions in a congested frequency band. The transmission is modulate using the Pulse Position Modulation (PPM); where the combination of half a microsecond high amplitude, followed by half a microsecond low amplitude, represents a logical 1. The logical 0 is exactly the opposite. The following 112 μs contains the actual transponder data and always starts with the 5 bit Downlink Format (DF). To distinguish ADS-B messages from other transponder replies, DF 17 is used. Other transponder replies could be for example the TIS-B or military purposes with DF 18 and respectively 19. Next is the 3 bit Capability block and differ per DF and can be seen as a subtype of the DF [9].

The selective transponder mode (Mode-S) has the possibility to interrogate the transponders based on a $24bit$ uniquely assigned address by the ICAO. This is followed by the additional data used for the ADS-B message format.

8 μs	112 μs				
	5 bits	3 bits	24 bits	56 bits	24 bits
Preamble	**Downlink Format**	**Capability**	**Aircraft Address**	**ADS-B Data**	**Parity check**

Figure 1: Mode-S Extended Squitter (1090ES) message format

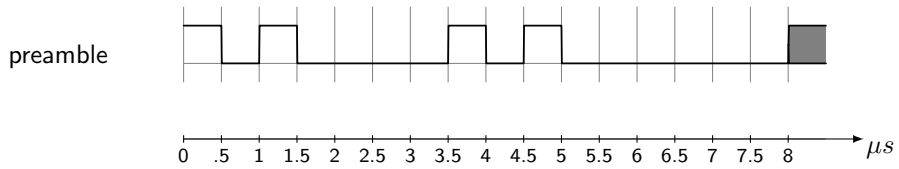


Figure 2: ADS-B preamble timing diagram

Field	Bits	Format	Value
Preamble	-		Preamble for synchronisation of receiving party (see Figure 2)
Downlink Format	5	17 18 19 *	Extended Squitter (ADS-B) Extended Squitter, supplementary (TIS-B) Military Extended Squitter Other format codes are for other purposes (TCAS, transponder messages, communications)
Capability	3		Subtype of Downlink Format (DF)
Aircraft Address	24		Unique ICAO airframe address
ADS-B Data	56		Data
Parity check	24		Cyclic redundancy check (CRC) of the message to detect transmission errors

Table 1: Mode-S Extended Squitter (1090ES) message format

The ADS-B data block start with a $5bits$ Type Code, followed by a $51bits$ long Type Code specific data block, as illustrated in Figure 3. All current addressed Type Code's used in the current ADS-B standard are listed in Table 2.

Type Code	Content
1-4	Aircraft identification
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: ADS-B Type Code's currently in use

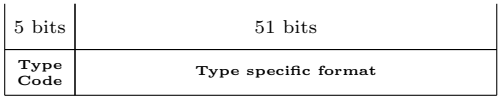


Figure 3: General ADS-B message format

4.3 Types of attack

According to literature, the ADS-B protocol is vulnerable to a variety of attack types, such as DoS and disinformational attacks. By suppressing the RF signals used by ADS-B, it is fairly easy to achieve a complete DoS attack by transmitting white or pink noise on the used $1090MHz$ frequency. This will "delete" all the aircraft on the map of the ATC as all ADS-B signals are suppressed and is easy noticeable.

Disinformational attacks are a bigger threat for the ATCS, as they are more complicated to detect. Recording an ADS-B transmission and simply replaying this message would result in outdated information being sent to the ATC, which is possible due to the fact there is no timestamp within the ADS-B message. By generating fake ADS-B messages, specific disinformation could be send towards the ATCS, resulting in "ghost" aircraft. This targeted approach forms an even higher threat because the ATC could make different decisions based on this false information.

By combining both the DoS and disinformational attacks, it is possible to "delete" specific aircraft, or even alter the flight path. This could be done by suppressing all ADS-B transmissions

with the use of a jammer, which transmits white or pink noise on a specific frequency, and retransmit specific ADS-B messages at a higher power, to overcome the earlier introduced noise.

5 Approach

To be able to fingerprint the ADS-B protocol for the purpose of assessing the authenticity of a transmission, captures of RF signals are required to identify measurable parameters. In this section, a description of the used lab environment that was used to capture RF signals of the ADS-B transmissions is given. Further more, the experiments that where performed to answer the research questions are posed in Section 2. Also, the theoretical expected values are presented in the end of this section.

5.1 Experiments theory

5.1.1 Signal quality

The first experiments will focus on ADS-B transmissions and the change of quality in signals, as the aircraft, during flight, is expected to transmit from different locations. By using raw in-phase and quadrature components (IQ) samples from *Gqrx* in combination with *dump1090-fa*, the ADS-B messages could be decoded with the corresponding Received Signal Strength Indicator (RSSI), expressed in decibels relative to full scale (dBFS). With the aircraft moving towards, or away from the receiver, an increase or decrease in RSSI is expected respectively. The so-called Free Space Path Loss is expressed as; $FSPL = \left(\frac{4\pi d}{\lambda}\right)^2$, with d the distance in metres, and λ the signal wavelength.

This can be rewritten to $FSPL = \left(\frac{4\pi df}{c}\right)^2$, with f the transmitted frequency in hertz and c, at the propagation speed of waves in the medium, which is for a RF waves assumed to be equal to the Speed of Light; 299,792,458 m/s. Variations in density and temperature can cause some variations over distance, but Earth's atmosphere is relatively thin and the distances relatively short that these variations are negligible. As the RSSI is given in decibels, the frequency f and propagation speed c are known, the formula can be rewritten in terms of decibels as a function of the distance d. This is shown in Figure 4.

$$
\begin{aligned}
FSPL &= \left(\frac{4\pi df}{c}\right)^2 \\
FSPL(dB) &= 10\log_{10}\left(\left(\frac{4\pi df}{c}\right)^2\right) \\
&= 20\log_{10}\left(\frac{4\pi df}{c}\right) \\
&= 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right) \\
&= 20\log_{10}(d) + 20\log_{10}\left(1.09 * 10^9\right) + 20\log_{10}\left(\frac{4\pi}{299,792,458}\right) \\
&= 20\log_{10}(d) + 180.7485 - 147.5522 \\
&= 20\log_{10}(d) + 33.1963
\end{aligned}
$$

Figure 4: FSPL formula in decibels as function of distance d

5.1.2 Doppler shift

The second experiment will focus on the Doppler shift, which is the change in observed frequency of a wave in relation to a moving wave source relative to the observer, or vice versa. The following diagram (Figure 5) illustrates how the observed velocity v_{ra} changes during a simplified scenario in which the receiver is stationary ($u_{ra} = 0$) while a transmitting aircraft (whose position relative to the listener at any point in time is denoted by the vector p) flies by at a constant velocity v:

- When the transmitting aircraft is in position 1, v_{ra} is negative; therefore, the frequency of the source is increased.
- When the transmitting aircraft is in position 2, the position vector p is perpendicular to the source's velocity v, so v_{ra} is zero; therefore, there is no Doppler pitch shift.
- When the transmitting aircraft is in position 3, v_{ra} is positive; therefore, the frequency of the source is decreased.

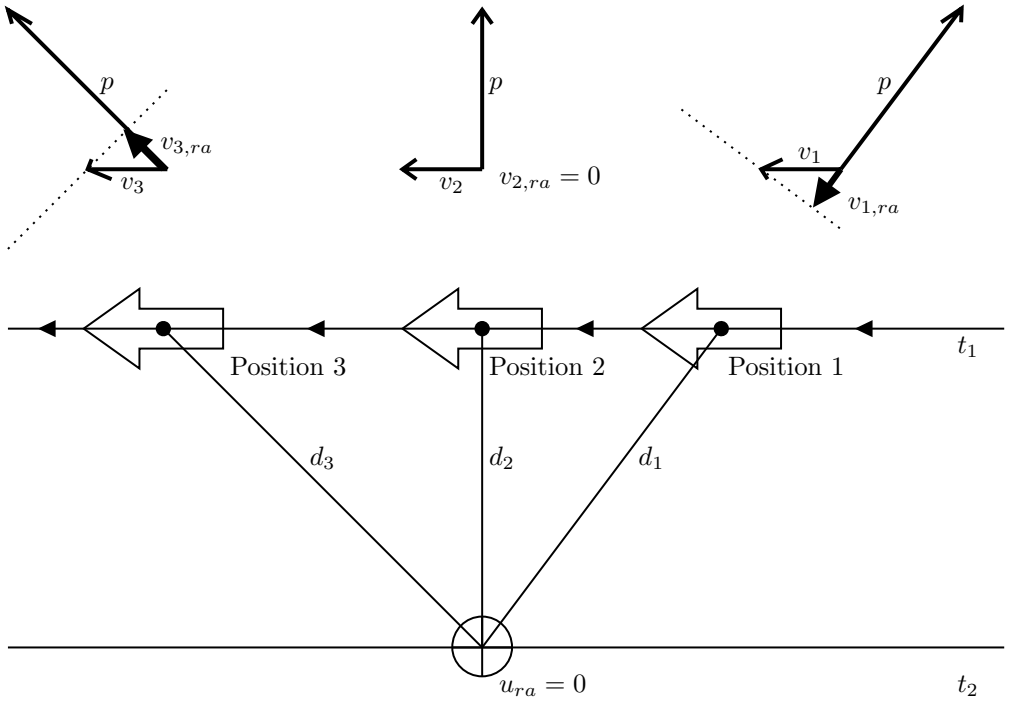


Figure 5: Illustration of changing observed velocity perpendicular on the line between Receiver and Aircraft (v_{ra}), with a constant velocity of the Aircraft itself (v)

The observed frequency, due to the Doppler shift, depends on the propagation speed of waves in the medium (denoted as c), which is for a RF-signal equal to the speed of light and the frequency used for broadcasting the ADS-B message (denoted as f_a), which is 1,090 MHz. The formula is given in Figure 6. For example, an aircraft flying towards the receiver with $450km/h$ ($= 125m/s$) results in an observed frequency of; $\left(\frac{299,792,458}{299,792,458-125}\right) 1,090 = 1,090.0004545MHz$.

$$
\begin{aligned}
f_r &= \left(\frac{c + \cancelto{0}{v_{ra}}}{c + v_{ra}} \right) f_a \\
&= \left(\frac{c}{c + v_{ra}} \right) f_a \\
&= \left(\frac{299,792,458}{299,792,458 + v_{ra}} \right) 1,090
\end{aligned}
$$

Figure 6: Observed frequency, as seen from the receiver as function of the relative velocity

5.1.3 Theoretical expected values

With the theory of Sections 5.1.1 and 5.1.2, Figure 7 represents the values that are expected along the trajectory t_1 as shown in Figure 5. Also the theoretical values of a trajectory t_2 of Figure 5 are expressed in Figure 7 in dashed lines. Positions 1 to 3 are represented with the vertical dotted lines as a reference to the corresponding positions in Figure 5. Each diagram the;

- straight lines represent the t_1 trajectory, where the aircraft follows a straight line with $5km$ distance, perpendicular to the receiver.
- dashed lines represent the t_2 trajectory, where the aircraft follows a straight line directly over the receiver.

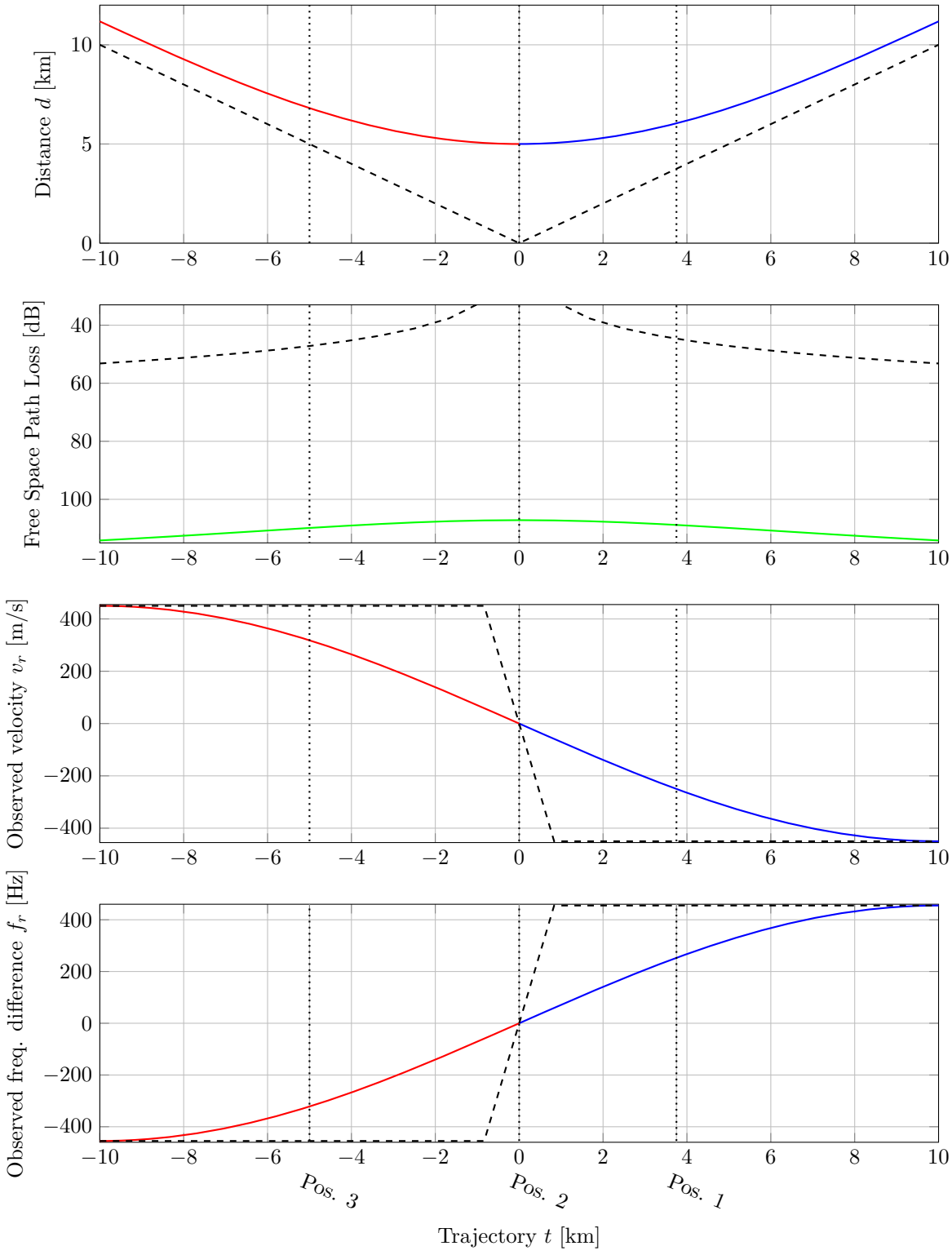


Figure 7: Theoretical values along the trajectories t_1 and t_2 in Figure 5

5.2 Lab Environment

To be able to determine if RF signals can be used to detect unauthorised transmissions by looking into the signal quality and Doppler shift, we need to capture the ADS-B messages which are broadcasted live. This can be achieved by the use of a Software-Defined Radio (SDR). The setup of the experiments is shown below.

- Ettus Research USRP2 - Universal Software Radio Peripheral, with;
  - Ettus Research WBX - Wide Bandwidth Transceiver daughterboard ($50MHz-2.2GHz$),
  - NooElec $1090MHz$ ADS-B Antenna ($5dBi$, $1090MHz$, SMA mount, 1.5 : 1 Voltage Standing Wave Ratio (VSWR)).
- Kali Linux 2020.1a, with:
  - GNU Radio Companion (version 3.8.1.0)
  - Gqrx (version 2.12.1-1)
  - dump1090-fa (version 3.7.0)
- Test locations at:
  - University of Amsterdam (UvA), FNWI
  - Building near Schiphol-Oost apron

6 Results

This section contains the results from the experiments done using the setup as described in Section 5. The experiments were conducted from two different locations both with their advantages and disadvantages. For example, at the UvA, the building blocks most ADS-B transmissions due to the concrete which affects the signal quality majorly. On the other hand, when an aircraft passes by, the only received signal is from that aircraft, which helps a lot in terms of noise. The other location was next to the Schiphol-Oost runway with a clear view over the Schiphol-Oost apron. This resulted in many more ADS-B transmissions and better signal qualities. The major disadvantage of this location is the noisiness in terms of simultaneously transmitted ADS-B messages. The following experiments are described against one example flight path, as shown in 9 and the corresponding speed and altitude graph in Figure 8.

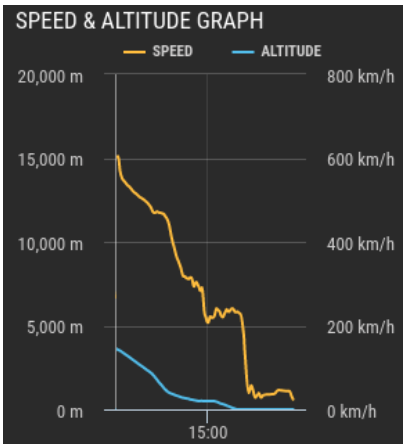


Figure 8: Figure 9's corresponding speed and altitude graph by Flightradar24

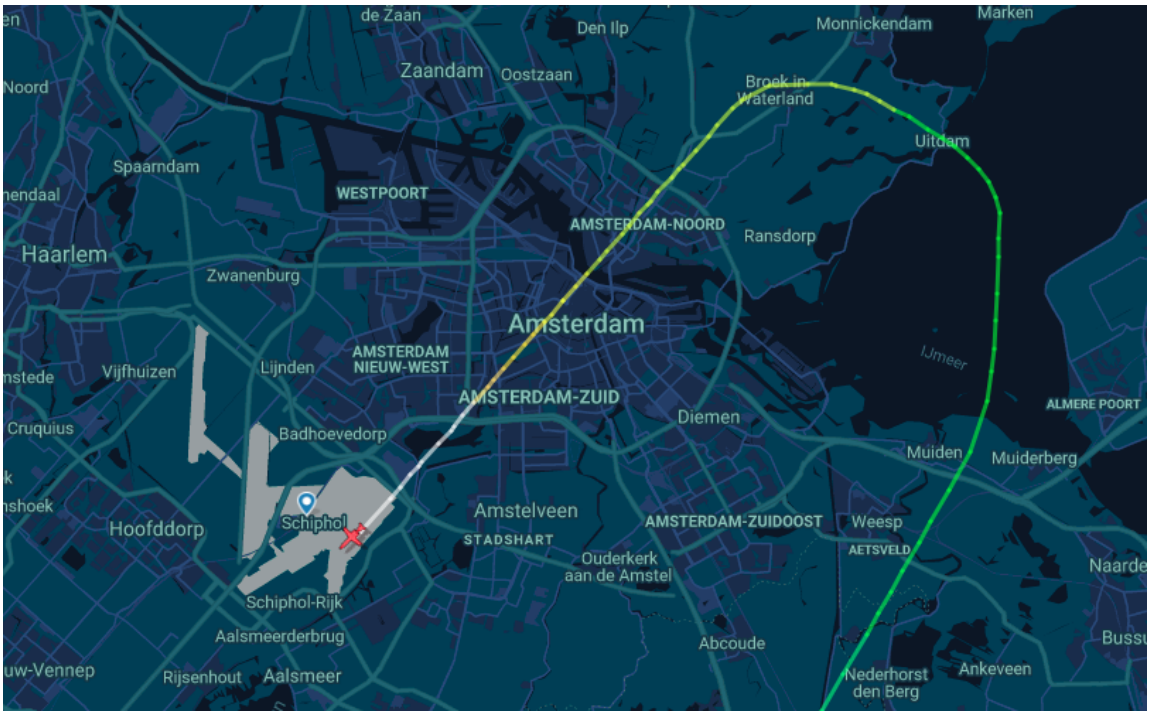


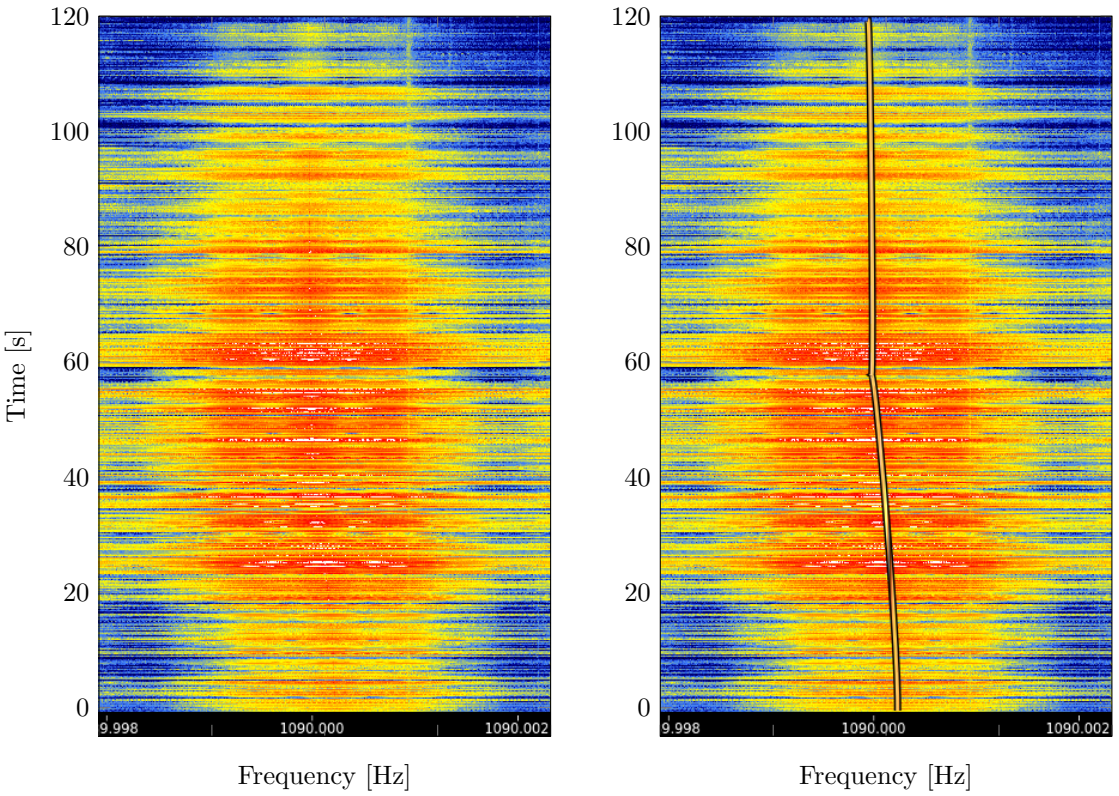
Figure 9: Tracked flight-path, visualised by Flightradar24

6.1 Signal quality

The first experiment observes the signal quality in terms of signal strength, measured in decibels. With the hypothesis the signal strength decreases when the aircraft is further away. The theory behind this is supported by the free space path loss formula, as described in Section 5.1.1. As seen in Figure 10a, we could clearly see an increase in signal strength, as the aircraft approaches the receiver. Also, a decrease in signal strength is observable, as the aircraft flies by, with maximum in the middle. This diagram shows the received signal strength, historically along the vertical axis, where the last received signal is on the top. The horizontal axis represents the received frequencies. The signal strength is an assessable parameter, which could be used to correlate the ADS-B message received from a moving aircraft. The change in signal strength is expected when an aircraft is moving and can be used to examine whether this is a moving sender. In other words, to verify an actual flying aircraft instead of a stationary sender.

6.2 Doppler shift

The second experiment observes the Doppler shift, with the hypothesis that the frequency shifts with the change of velocity between the sender and the receiver, as described in Section 5.1.1. As seen in the Fast Fourier Transform (FFT) waterfall diagram in Figure 10a, we can clearly see a higher observed frequency 2 minutes earlier, than in the middle where the observed velocity remain the same. The centre frequency is highlighted in Figure 10b.



(a) Original capture

(b) Original capture, with centre frequency highlighted

Figure 10: Signal Strength and Doppler shift observed in FFT waterfall with live aircraft

7 Security enhancement

In the results of the experiment (Section 6) a practical solution to identify unauthorised transmissions that is based on measurable parameters is given. The parameters provide insights whether the transmission is from a moving aircraft. The degree of certainty heavily depends on the reliability of the used hardware and other external factors. This is not always in the power of the assessing party, as the transmitting equipment of the aircraft could suffer from external factors, which could lead to a non-perfect $1090MHz$ transmission. When a potential attacker knows the location of the receiving antenna, these parameters could in theory be used to imitate a real broadcast, by changing the clock frequency and antenna gain on purpose.

As ADS-B messages are trusted by multiple systems, such as Secondary Surveillance Radar (SSR), TCAS, and other aircraft receiving ADS-B, it would be recommended to have a mechanism to verify these broadcasted messages. The information security industry primarily focuses on the balanced protection of the confidentiality, integrity and availability of the information; in this case

the ADS-B message data [10]. Each security property can be explained as;

- **Confidentiality** Protection against unauthorised data disclosure
- **Integrity** Prevention against unauthorised data modification
- **Availability** Prevention against delays
- **Authenticity** Authentication of data source
- **Non-repudiation** Prevention against any party from denying on an agreement after the fact
- **Privacy** Provision of data control and disclosure

The confidentiality, non-repudiation and privacy concepts are not covered in the protocol, because the ADS-B messages are meant to be broadcasted for any application that could benefit from it, and should not be kept secret. Besides that, the integrity, availability, and authenticity security properties are desirable in the fight against disinformation. In other words, eavesdropping, masquerading, and tracking is not a security attack on the protocol by its design. However, Denial-of-Service (DoS), replaying, and impersonation attacks are a threat for the trustworthiness of the ADS-B message.

In the current ADS-B standard only the integrity is ensured by the use of a CRC [11]. The CRC only ensures the integrity of the data-transmission itself, in order to prevent transmission errors. It is therefore self-evident that also this parity check could be altered by an attacker and does not prevent against unauthorised data modification.

Using cryptographic hash functions could aid in creating verifiable ADS-B messages, especially when a Public Key Infrastructure (PKI) is used. PKI is a framework used in the information security industry for end-to-end protection of communications. The framework includes the infrastructure, policies, (separation of) roles, hardware/software, and policies, required to distribute the public keys among other participating parties and the possibility and administration of revocation of the public keys. It is also known as asymmetric cryptography, where the fundamentals of this principle rely on the use of two different cryptographic keys; the public key and the private key.

With the use of asymmetric cryptography a sender is able to encrypt the message with the public key of the receiving party, where only the receiving party is able to decrypt the message with the private key, which should kept secret. This is relevant for secure communications in terms of confidentiality, non-repudiation and privacy, which are not the security properties that have to be addressed. However, by using the private key, at the sending party, the messages can be signed, which could be verified by everyone who has the public key. Signing ADS-B messages, which are verifiable together with the public key, addresses the security problems in terms of integrity and authenticity. With regards to the availability, the backwards compatibility should be taken into account during the transition phase. The required backward compatibility is especially true for the aerospace industry, where the adoption of a new standard could take multiple years. The ADS-B version 2 is still ongoing as seen in Figure 11, where the SESAR Deployment Manager expects an acceptance by the end of 2025. Version 2 of ADS-B is mandated by the European Commission in November 2011 (CIR 1207/2011) [12].

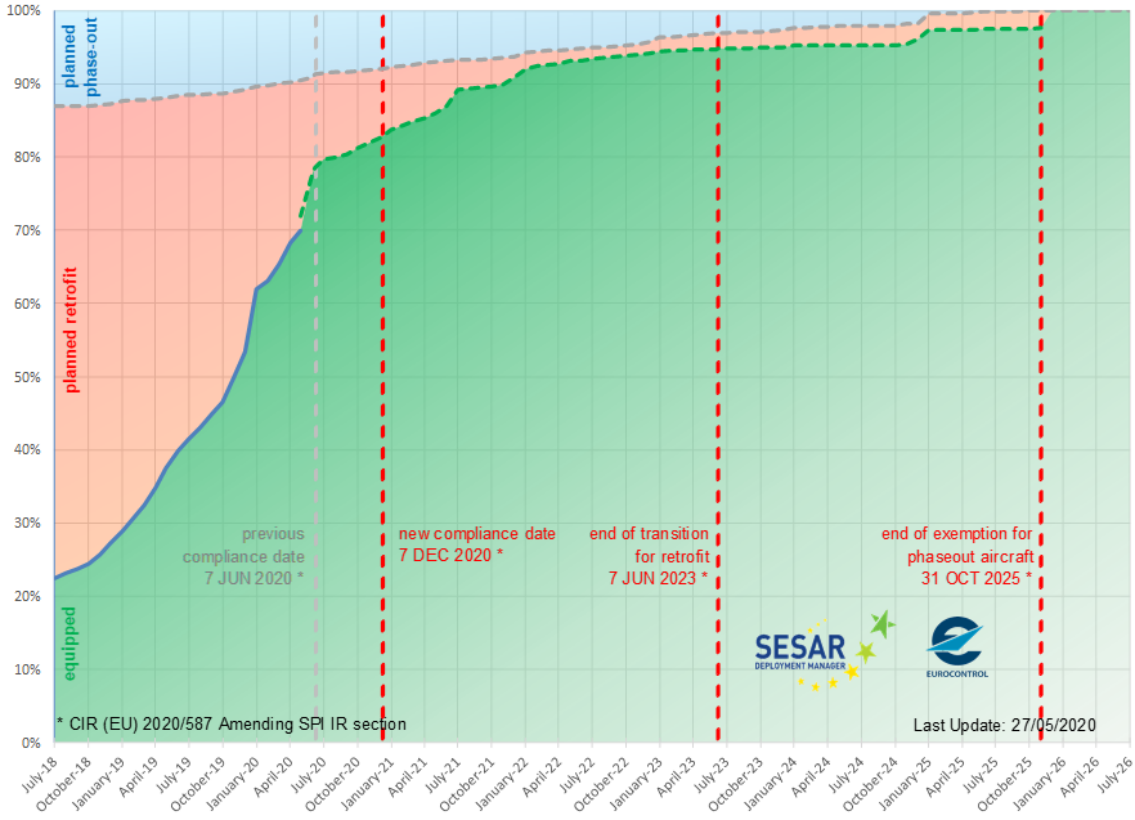


Figure 11: ADS-B Implementation Status [12]

Allowing a phased transition, mainly two options are available; create a new protocol which could co-exist with the current version or create a backward compatibile protocol, where current equipment is still able to cooperate with the enhanced version. As explained in Section 4.2, the ADS-B transmissions are expected to be transmitted in a $120\mu s$ time frame, which could be extended for the purpose of signing, provided that current equipment is not disturbed by extra transmission time.

To overcome a possible replay attack, where authentic and verifiable ADS-B messages are recorded and replayed later on, a timestamp should be added. By using timestamps received from a mutual trusted source, for example GPS, makes it fairly easy to verify whether the message has been replayed. This introduces a minor pitfall in terms of time stamp roll over. The GPS time stamps are represented in the Time of Week (ToW), which is a 19 bit representation of amount of 1.5 seconds passed since the beginning of the week with the Coordinated Universal Time (UTC) as reference. The week number is represented as a 10 bit value, which gives us $2^{10} = 1024$ weeks, since the counter started at the first full week of 1980 (6th of January). With a maximum of 1024 possible weeks, a roll over happens every 19.7 years. In theory it is possible to replay a 19.7 years older, valid signed ADS-B message [13]. To overcome this issue, a public/private key pair should not be used, after the maximum representable time frame, for the signing messages. This can be done by a key roll over; regenerate a new public/private key pair, where the private key will be replaced in the aircraft and the public key published to accessible databases. This could be done during the required service intervals for the transponder equipment. To reduce the required extra transmission time, in the already congested frequency band, a shorter time stamp notation could be chosen, if the key rollover is done more frequently.

Together with the data field and the timestamp, a cryptographic signature could be generated and appended to the current standard ADS-B message. By choosing a modern hashing algorithm like Secure Hash Algorithm (SHA)-1, an additional 189 bits will be appended to the current ADS-B message, as shown in Figure 12. Newer versions of SHA are available, which have advantages in terms of security, but will result in longer signatures, and therefore longer transmission time is required.

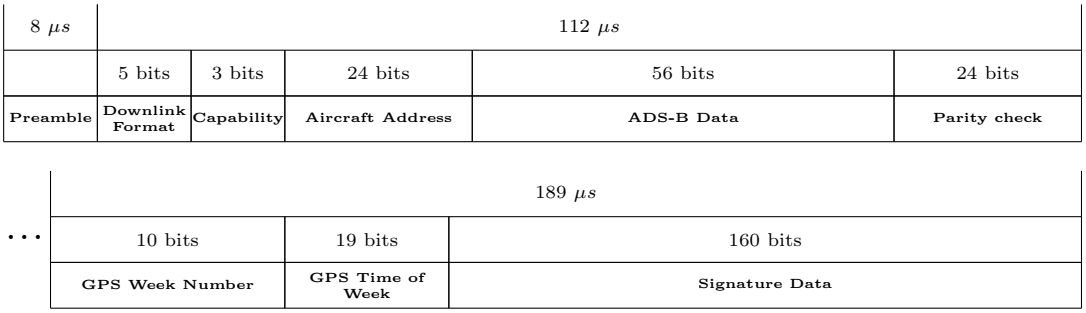


Figure 12: ADS-B message format with additional signature

In Figure 13 the process is illustrated. An aircraft receives signals from a GNSS, and is able to calculate the position and build up the ADS-B message as usual. The extra signature data could be calculated, based on the ADS-B message, the received time stamp, and the private key belonging to the transponder. This standard ADS-B message will be transmitted with the extra signature data appended. Therefore every other ADS-B capable transponder is able to decode the current ADS-B message format. Other aircraft and ATC, who follow the proposed standard, are able to verify the standard ADS-B message against the public key, belonging to the transponder private key.

The public keys should be publicly available to all concerned parties, such as ATCs and aircraft. This could be achieved by periodically updating the public key databases via transactional updates. These transactional updates could consist of new public keys when, for example a new aircraft transponder is manufactured, or a key roll over has taken place. Also, revoked public keys should be distributed via this channel for the purpose of distrusting private keys. This may be necessary at the moment a private key is compromised.

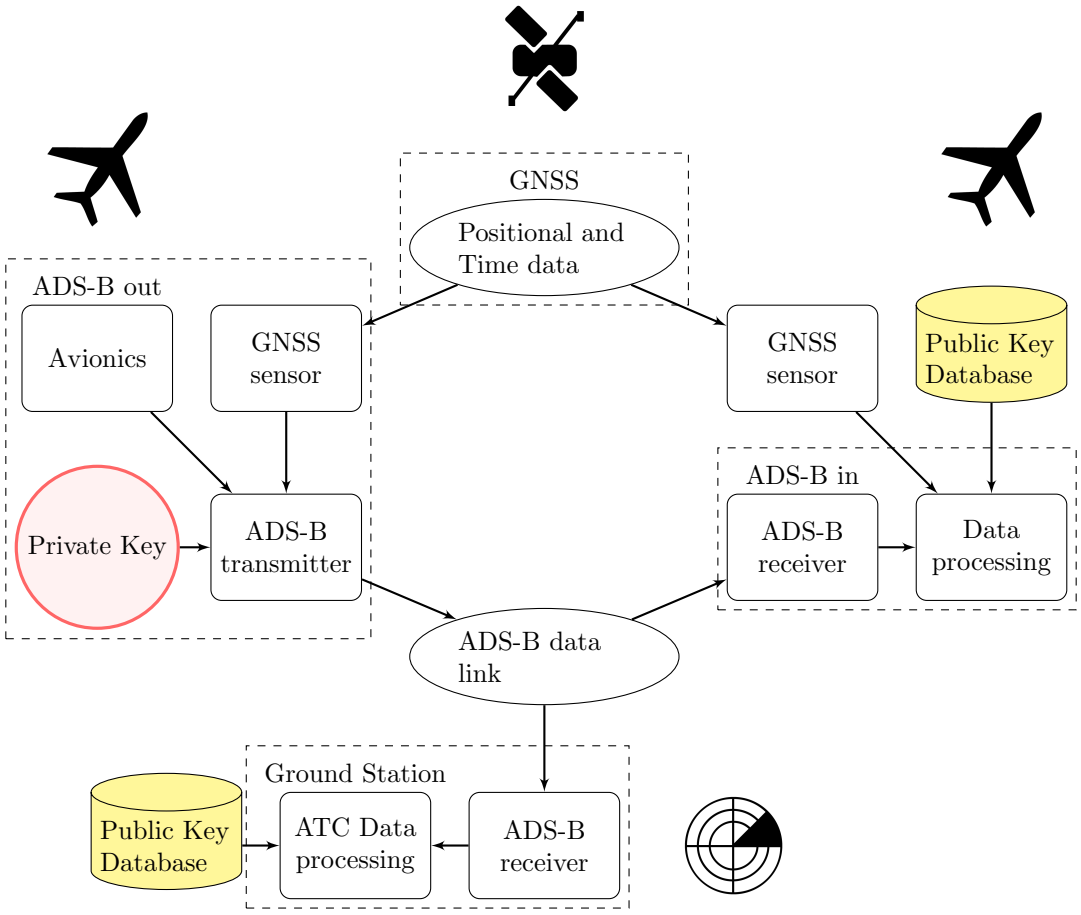


Figure 13: ADS-B process with additional signature, signed by Private Key, verifiable against the Public Key

8 Discussion

The results suggest that the signal quality and the doppler effect can be used to validate the data against the claimed values in ADS-B messages. However, high quality receiving equipment is required to increase the certainty with the RF signal analyse test. The equipment should be reliable, and the reference clock should be moree accurate to prevent extensive differences introduced due to a possible clock drift from the the receiver. The applicability of the RF signal results in this research should be taken in consideration when observing the signal quality and Doppler shift in the FFT waterfall with live aircraft.

In addition, signed ADS-B messages require longer transmission time. This results in a less available bandwidth, which could be a problem for busy airspaces. To overcome this issue, less frequent signing the ADS-B messages or only sign the ADS-B messages on request, triggered by a specific interrogation message. The singed data could also be sent over a different channel, by using a different frequency or a different modulation technique, which does not interfere with the current PPM.

By adding the GPS time stamps to the signed version of the ADS-B transmission, the protocol is vulnerable to replay attacks, as described in Section 7. In principle, the period of 19.7 years is

incredibly long, and probably not relevant as an attack vector.

9 Conclusion

The ADS-B protocol does not guarantee the authenticity and integrity of the message due to the lack of built-in security. The protocol is sensitive for replay-attacks and vulnerable for false information to ATCS.

In order to answer the main research question, we first need to elaborate on the sub-questions. The first one, focused on the possible types of attack, is answered in Section 4.3, and completely supported by a literature study. As it was not feasible to test a DoS attack nor a fake ADS-B broadcast in companion with the authorised parties. From literature study it can be concluded that the ADS-B protocol is vulnerable for disinformational attacks, such as replaying earlier broadcasted ADS-B messages or generating fake ADS-B messages. By combining DoS attacks, with disinformational ADS-B messages, the attack becomes even more dangerous.

The second sub-question was regarding the possibilities to detect, and therefore able to filter, undesired fake ADS-B broadcasts. Combined with signal fingerprinting, as stated in the last sub-question, the detection is possible to a certain extend. This is done by assessing RF signal properties, against the claimed values of the ADS-B message. From the experiments, as described in Section 5, and the results in Section 6, this research can conclude that it is possible to use the signal strength and the Doppler shift for verification of the ADS-B messages. Although there are some pitfalls regarding the Doppler shift method, as described in the previous Section 8. The advantages of using signal fingerprinting is the ability to detect, and therefore filter, ADS-B messages that do not match with the expect values.

To be able to detect and filter malicious ADS-B broadcasts, it would be advised to verify the ADS-B messages itself, instead of assessing the RF signals. From a theoretical study it is possible to sign the ADS-B messages, as such that the receiving party can verify ADS-B message, and therefore proving the integrity and authenticity. This is described in Section 7.

Based on these conclusions, malicious broadcasts of the ADS-B messages can be detected by signing and verifying the ADS-B messages and as fallback assessing RF-signals, in order to protect ATC from DoS and disinformation attacks

10 Future work

Signing the ADS-B message allows for a verifiable transmission in combination with the public key. The research explained that ADS-B transmissions are expected to be transmitted in the 120 μs time frame which could be extended for the purpose of signing. By creating a new protocol, which is able to co-exist with the current version, the protocol could be enhanced in terms of authenticity and integrity. It would be interesting to see what other signing methods are available for ADS-B messages to reduce the required transmission time.

Besides improving the ADS-B protocol, the key management could be challenging, especially for less frequent used aircraft. It would be interesting to investigate the possibilities of Over-the-Air (OTA) updating and/or updating of the transponders.

Furthermore, in this paper different security properties which are applicable for the information security industry in general, are described. The confidentiality, non-repudiation and privacy concepts are not covered in the proposed ADS-B message protocol, since the message is designed to be decoded for any application or system that could benefit from the message. To improve on these security features, it is almost inevitable to use two-way communication instead of broadcasting, which could be feasible when the ADS-B are validated selectively by periodically interrogating the

aircraft transponder. It would be interesting to reflect the other security properties with the ADS-B protocol.

Finally, it would be interesting to see what security attacks are available for Aircraft-to-Aircraft communication and how the aircraft could be prevented from disinformational attacks to improve the security enhancements for the TCAS and the overall safety in airspace.

11 Acknowledgements

I want to thank Jan-Joris van Es and Nico de Gelder for their feedback and supervision. I would also like to thank the OS3 Core-team for the feedback sessions and opportunities as well as the educational facilities that were at my disposal to perform this research. Especially the availability for the Ettus USRP2 SDR and dispensation on the COVID-19 restrictions applied by the University of Amsterdam.

References

[1] Leon Purton, Hussein Abbass and Sameer Alam. "Identification of ADS-B system vulnerabilities and threats". In: *Australian Transport Research Forum, Canberra*. 2010, pp. 1–16.

[2] Ron van Scheppingen. *Van Primaire Radar Tot ADS-B*. 9 Nov. 2018. URL: https://www.knvvl.nl/nieuws/presentaties-workshop-general-aviation-2018-ontwikkelingen-aan-de-horizon.

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

[4] Donald McCallie, Jonathan Butts and Robert Mills. "Security analysis of the ADS-B implementation in the next generation air transportation system". In: *International Journal of Critical Infrastructure Protection* 4.2 (2011), pp. 78–87.

[5] Xuhang Ying et al. "Detecting ADS-B Spoofing Attacks using Deep Neural Networks". In: *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE. 2019, pp. 187–195.

[6] Martin Strohmeier et al. "On perception and reality in wireless air traffic communication security". In: *IEEE transactions on intelligent transportation systems* 18.6 (2016), pp. 1338–1357.

[7] Cindy Finke, Jonathan Butts and Robert Mills. "ADS-B encryption: confidentiality in the friendly skies". In: *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*. 2013, pp. 1–4.

[8] Wei-Jun Pan, Zi-Liang Feng and Yang Wang. "ADS-B data authentication based on ECC and X. 509 certificate". In: *Journal of Electronic Science and Technology* 10.1 (2012), pp. 51–55.

[9] C. Binns. *Aircraft Systems: Instruments, Communications, Navigation, and Control*. Wiley - IEEE. Wiley, 2018. ISBN: 9781119259541. URL: https://books.google.nl/books?id=N5lxDwAAQBAJ.

[10] Jason Andress. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress, 2014.

[11] Jeffrey L Gertz. *Fundamentals of mode s parity coding*. Tech. rep. MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB, 1984.

[12] SESAR Deployment Manager. *ADS-B Implementation Status*. 27 May 2020. URL: https://ads-b-europe.eu/.

[13] Richard B Langley. "The GPS End-of-Week Rollover". In: *GPS World* 9 (1998), pp. 40–47.

A Acronyms

ADS-B Automatic Dependent Surveillance-Broadcast. 1–6, 10–18

ATC Air Traffic Control. 2–5, 15, 17

ATCS Air Traffic Control Specialists. 2–5, 17

CRC cyclic redundancy check. 5, 13

dBFS decibels relative to full scale. 6

DF Downlink Format. 4, 5

DNN Deep Neural Network. 3

DoS Denial-of-Service. 2, 5, 13, 17

FFT Fast Fourier Transform. 11, 12, 16

GNSS Global Navigation Satellite System. 2, 15

GPS Global Positioning System. 2, 14, 16

ICAO International Civil Aviation Organization. 4, 5

IQ in-phase and quadrature components. 3, 6

OTA Over-the-Air. 17

PKI Public Key Infrastructure. 1, 13

PPM Pulse Position Modulation. 4, 16

PSR Primary Surveillance Radar. 3, 4

RF Radio Frequency. 1, 3, 5–7, 10, 16, 17

RSSI Received Signal Strength Indicator. 6

SDR Software-Defined Radio. 3, 10, 18

SHA Secure Hash Algorithm. 15

SSR Secondary Surveillance Radar. 12

TCAS Traffic Alert and Collision Avoidance System. 2, 5, 12, 18

TIS-B Traffic Information Service - Broadcast. 4, 5

ToW Time of Week. 14

USRP Universal Software Radio Peripheral. 3, 10

UTC Coordinated Universal Time. 14

UvA University of Amsterdam. 10

VSWR Voltage Standing Wave Ratio. 10