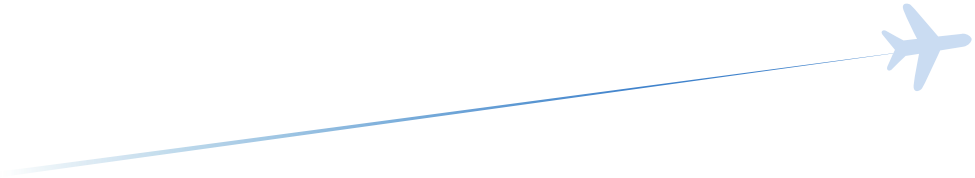

D4.3 Authentication and integrity for ADS-B

Deliverable ID:	**4.3**
Dissemination Level:	**PU**
Project Acronym:	**Engage**
Grant:	**783287**
Call:	**H2020-SESAR-2016-2**
Topic:	**SESAR-ER3-01-2016 Knowledge Transfer Network**
Consortium Coordinator:	**University of Westminster**
Edition date:	**07 April 2021**
Edition:	**01.00.00**
Template Edition:	**02.00.02**

Founding Members
EUROPEAN UNION EUROCONTROL

SESAR JOINT UNDERTAKING

Engage

THE SESAR KNOWLEDGE TRANSFER NETWORK

This deliverable is part of a project that has received funding from the SESAR Joint Undertaking under grant agreement No 783287 under European Union's Horizon 2020 research and innovation programme.

Abstract

This is the final technical report of the *Authentication and integrity for ADS-B* project, which was awarded funding through the Engage KTN's first Call for catalyst funding.

Founding Members

EUROPEAN UNION EUROCONTROL

SESAR Engage KTN – catalyst fund project final technical report

Project title:	Authentication and Integrity for ADS-B
Coordinator:	TU Kaiserslautern
Consortium partners:	SeRo Systems GmbH
Thematic challenge:	TC1 Vulnerabilities and global security of the CNS/ATM system
Edition date:	30 September 2020
Edition:	1.0
Dissemination level:	Public
Authors:	Prof. Jens B. Schmitt
	Dr.-Ing. Matthias Schäfer

This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 783287.

1. Abstract and executive summary

1.1 Abstract

The main objective of this project is to provide the means to improve the security of the Automatic Dependent Surveillance-Broadcast (ADS-B), a critical backbone of future surveillance systems. More specifically, we evaluate the data link capabilities of the so-called phase overlay, a backwards-compatible extension to the current implementation of ADS-B. Our results indicate that 8PSK performs best in a realistic radio environment, reliably providing up to 218 additional bits for each ADS-B message at a carrier frequency offset tolerance of about 40 kHz. Based on these insights, we propose a protocol that relies on the phase overlay to authenticate the information provided via the ADS-B.

1.2 Executive summary

Huge modernisation programs such as SESAR in Europe and NextGen in the U.S. have the ambitious goal to increase the safety, capacity, and efficiency of air traffic management (ATM) while at the same time decrease its ecological footprint and overall cost. A key component of these efforts is the transition from ground-based air traffic surveillance to a more accurate and more cost-efficient cooperative and dependent system, the Automatic Dependent Surveillance-Broadcast (ADS-B). Transponders equipped with ADS-B periodically broadcast surveillance information such as location, velocity, and identity over a digital data link. While this new approach has many advantages, its simplicity and the associated digitalisation come at a high price. Surveillance information is no longer provided by trusted ground infrastructure but by remote devices that are beyond control of the end user (e.g. air navigation service provider). Combined with the widespread availability of cheap yet powerful tools such as software-defined radios, this shift of trust poses a serious security threat as fake surveillance information can be injected into the ATM system over this wireless interface rather easily.

In order to fix the security problems of ADS-B in a sustainable way, authentication and data integrity must become an integral part of future versions of the protocol. This goal, however, constitutes a major challenge since the data link characteristics and the strong need for legacy compatibility render most cryptographic solutions unusable. ATM stakeholders and technology providers have jointly conducted several projects within the SESAR JU work package 15 with the goal to increase the capacity and security of the ADS-B data link. Project 15.04.06 in particular tested the feasibility of an additional legacy-compatible phase shift keying (PSK)-based ADS-B overlay. Such an overlay would increase the data volume that can be transferred in a single ADS-B transmission while preserving backwards compatibility. It could be used to add security-relevant information to ADS-B transmissions to provide authentication and integrity services. The SESAR JU project 15.04.06 demonstrated that such an overlay is indeed feasible and since then, the phase overlay has become a part of the ongoing standardisation efforts for the next ADS-B version that is likely to be published in the coming months. However, the performance in a realistic environment and the specific design of an authentication and integrity service based on such an overlay remain open questions. In fact, these two questions are strongly interdependent since existing broadcast authentication schemes need to be adapted based on the characteristics of the underlying data link.

This project aimed at answering these questions by first investigating the performance of the ADS-B phase overlay under real-world 1090 MHz radio frequency conditions and then using these insights to design a realistic ADS-B authentication and integrity protocol. More specifically, we integrated SeRo Systems' PSK-enabled ADS-B receiver GRX1090 into the testbed used by DISCO Lab in 2012 to evaluate attacks on ADS-B under realistic conditions. Using this testbed, we studied the bit error rate (BER) of different phase overlay configurations in a realistic radio environment and analysed the

expected net data rate under the assumption that typical error correction codes such Reed-Solomon codes are used.

Based on the insights gained throughout these experiments, we devised a modified version of the Time Efficient Stream Loss-tolerant Authentication (TESLA) protocol that was originally proposed by Perrig *et al*. in 2002. We modified the original protocol with respect to trade-offs that account specifically for the missing (loose) time synchronisation required by TESLA, the comparably low number of bits that can be accommodated in the new phase overlay, the computational load at the receiver which may track high numbers of aircraft simultaneously, and a simplified key management scheme.

2. Overview of catalyst project

2.1 Operational/technical context

Today's civil air traffic surveillance is typically based on secondary surveillance radar (SSR). A key characteristic of SSR is that transponders only transmit information upon requests from ground or airborne interrogators. Ground radars typically consist of rotating antennas which transmit interrogations in a directed beam. Once the aircraft transponder receives an interrogation, it immediately responds with the requested information. By measuring the time between transmission of the request and reception of the reply, the interrogator estimates the distance to the aircraft (ranging). This distance combined with the direction in which the request was sent and the altitude contained in the reply provides the interrogating ground radar with the three dimensional position of the aircraft.

A major drawback of this approach is that update rates for information are limited to the rotation period of the antenna. A full rotation usually lasts about 4-12 seconds. In addition, determining the round-trip time and angle of arrival of an interrogation is susceptible to measurement errors and precise localisation requires expensive techniques such as multi-radar tracking. These shortcomings and the rapid increase in air traffic have led to major modernisation programs such as NextGen in the US and SESAR in Europe.

A key component of these efforts is the ADS-B protocol. In principle, ADS-B elicits the periodic or event-driven transmission of special SSR transmissions without the need for interrogations. Since ranging is not possible with autonomously transmitted messages, and to achieve a better accuracy, the design of ADS-B requires aircraft to determine their exact locations themselves using satellite-based navigation systems such as GPS. The obtained position and velocity data are then periodically broadcast over the SSR downlink along with other surveillance information.

All receivers that are in line of sight of the aircraft can then simply receive and process the aircraft's spatial state without the need for expensive radars infrastructure. As ADS-B has become mandatory in many parts in the world in the late 2010s (Australia[1]) and early 2020s (US[2] and Europe[3]), many airlines have updated their fleets with ADS-B capabilities. See Figure 2.1 for a simplified overview on the architecture of ADS-B.

The ADS-B specification (DO-242A) merely describes the function of broadcasting information. Data link aspects such as the wireless medium or message structures are specified separately and there are two options. The Universal Access Transceiver (UAT; DO-282B) is specifically designed for supporting ADS-B and other aviation services such as the Traffic Information Service-Broadcast (TIS-B). It operates on the 978 MHz RF band. Since UAT requires aircraft to be equipped with new

[1] Instrument number CASA 61/14
[2] Code of Federal Regulations §91.225
[3] Commission Implementing Regulation (EU) No 1028/2014

hardware, the FAA decided to use UAT only in general aviation[4]. In contrast, scheduled air transportation re-uses existing SSR transponders to broadcast ADS-B. More specifically, they use a general purpose SSR Mode S downlink format which is broadcast by transponders without prior interrogation. This downlink format is called Extended Squitter (ES) and the combination of ADS-B and SSR Mode S operating on the 1090 MHz frequency is referred to as 1090ES ADS-B.

There are three versions of 1090ES ADS-B. While version 2 is the version targeted by the mandates and although most aircraft operators have updated their transponders to version 2, a significant percentage of aircraft is still using ADS-B version 0 and 1 transponders. Nevertheless, since version 2 is and will remain the prevalent version in the foreseeable future, we will assume 1090ES ADS-B version 2 for the remainder of this report. It is worth noting, however, that the most relevant aspect of ADS-B for this project, i.e., the physical layer, is specified by SSR Mode S and is the same for all three versions.

ADS-B has evolved from technologies dating back to World War II, when sophisticated RF technology was not as widely available as it is today. This led to a negligence of security and ultimately to the complete absence of security mechanisms in ADS-B. In fact, security has never been a design goal of ADS-B at all. The result of this historical development is that transmissions can be injected, modified or deleted by any attacker who has full control over the wireless channel.

While passive attacks are mainly affecting privacy and might not result in severe risks for air traffic safety, active attacks on ADS-B can result in life-threatening situations caused by misguided pilots, controllers, and avionics. Moreover, advances in wireless technology such as the widespread availability of cheap off-the-shelf software-defined radios have made crafting and transmitting valid ADS-B signals cheap and simple. With no data integrity and origin authentication in place, ADS-B without the support of other technologies is vulnerable to a range of attacks based on transmitting fake transponder signals, including the injection of non-existing (“ghost”) aircraft and the delusion of on-board instruments.

Although these vulnerabilities are known, the long development and certification cycles of 20-30 years in aviation make the inclusion of security mechanisms into the ADS-B protocol extremely difficult in the short term. As a consequence, any viable solution must be at least backwards compatible since a complete replacement of ground infrastructure and airborne receivers is practically impossible in the short or even medium term.

One approach to seamlessly integrate security services into ADS-B is by increasing the data capacity of ADS-B transmissions using the currently ignored signal phase. More specifically, phase shift keying (PSK) techniques can be used to transmit more than one bit within a single pulse. This PSK extension to the regular pulse position modulation is often referred to as phase overlay and is in fact part of the current draft for version 3 of the 1090ES ADS-B specification. The major advantage of this approach is that it is fully backwards compatible since the current modulation feature (the pulse positions) is not changed by varying the signal phase.

2.2 Project scope and objectives

The additional capacity gained through the phase overlay technique could be used (among other things) to transmit authentication and integrity codes along with regular ADS-B data. In this project, we explore the capabilities and limitations of this new data link. We evaluate its performance under a realistic radio frequency conditions and evaluate the effect of different factors and parameters on its performance. Based on the insights gained during these experiments, we design a protocol that could bring authentication and integrity to ADS-B through the phase overlay.

[4] General aviation refers to all civil flights which do not belong to scheduled air transports.

Our overall objective is to provide valuable insights for future standardisation and to helps the ATM ecosystem to benefit from the advantages of ADS-B without suffering from its security weaknesses in the long term. We summarise the three objectives for this project as (i) improving the security of the ATM system, (ii) advancing existing research with real-world data, and (iii) conceptualising a sustainable long-term security solution for ADS-B.

2.3 Research carried out

The research in this project was conducted in two major steps. First, we evaluated different modulation parameters of the phase overlay and their effect on the expected performance. We designed and implemented a testbed that allowed us to conduct controlled experiments under conditions matching those in the real radio frequency environment. In the second step, we modified the design of an existing broadcast authentication protocol (TESLA) to match the limitations and conditions of the ADS-B phase overlay that we learned during our measurements.

2.3.1 Phase-Overlay Evaluation

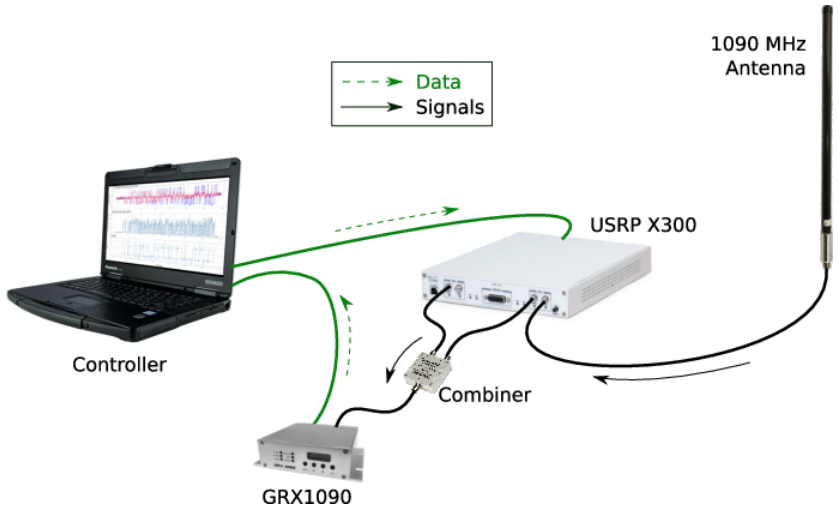

Figure 2.1: Testbed used for our experiments

An overview of the testbed is provided in Figure 2.1. At its core, the SeRo Systems GRX1090 receiver is used to receive the ADS-B frames with phase overlay. It provides an API that allows retrieving the synchronised raw I/Q signal data for received Mode S and ADS-B frames for a specific set of aircraft and transmission types. The I/Q data provided by the GRX1090 API has a resolution of 12 bit and a sample rate of 12 MHz. The receiver's oscillators are GPS-disciplined, providing a highly accurate carrier frequency synchronisation. Using a software defined radio (USRP X300), we generated ADS-B signals with different types of phase overlays and fed them into the GRX1090's RF input through a cable. The GRX1090 detected, decoded and forwarded these signals along with their I/Q data to the controller PC, where the phase overlay was extracted from the I/Q data in a final post-processing step. Using a combiner, the setup allowed us to also mix interferences that come in from a separate antenna or from recordings into the transmissions during our experiments. In this way, we could conduct our measurements under realistic radio frequency and interference conditions.

Using this testbed, we conducted a series of measurements with the goal to test the net performance of different phase overlay configurations and radio environments. Our primary performance metric was the bit error rate of the payload of the phase overlay. The primary configuration parameter for the phase overlay was the number of bits per symbol, typically denoted by M. Other parameters of the setup were the signal-to-noise ratio (or transmit power), the signal's carrier frequency offset, and whether interferences were present in the radio channel (noisy

channel) or not. For the noisy channel, we replayed and mixed continuous signal recordings from Frankfurt am Main airport into the stream of phase-overlay ADS-B signals.

The resulting bit error rates could then be mapped to the net capacity of the phase overlay by subtracting the capacity consumed by appropriate error correction mechanisms such as Reed-Solomon codes or low-density parity-check codes (LDPC). Note that the capacity needed by such codes (i.e., the level of redundancy) generally depends on the expected error rate and could therefore be estimated once the bit error rate was determined.

2.3.2 Authentication and Integrity Protocol Design

In the second phase of the project, we devised a protocol that provides authentication and integrity to ADS-B. We modified the existing TESLA protocol with respect to the findings of the research described in the previous section. The modifications in particular targeted the following aspects of the original protocol.

Surveillance Requirements

In TESLA, keys are disclosed in regular time intervals according to a schedule. A receiver can only very the authenticity of received messages once the respective key has been disclosed shortly after. Since information received via ADS-B should only be used once its authenticity has been verified, the disclosure schedule has to be chosen in a way such that surveillance requirements in terms of update rates are not violated.

Protocol Overhead

TESLA requires the transmission of potentially large message authentication codes (MACs). Depending on the phase overlay configuration and assumptions, the phase overlay may not provide sufficient capacity for this.

CPU Overhead

TESLA may put a lot of computational burden on a receiver processing ADS-B messages from more than 100 targets at a time. Due to the chained processing of commitment-keys, the receiver may have to compute the one-way function many times for each received ADS-B message in order to validate their origin and integrity.

Limited Transponder Capabilities

Transponders can be limited in their computational resources and available memory. Hence, an instance of TESLA should include have low requirements in these regards. This is particularly important when it comes to choosing the right parameters for the key schedule and key chain generation.

Key Management

While the sole use of TESLA can already defend against so called modification attacks, i.e., the injection of ambiguous or false information on real ADS-B targets, a complete authentication and therefore a complete protection against any attack based on the injection of fake signals would require a key management that is light weight and does not require too much coordination between entities such as ANSPs.

2.4 Results

The results of this project can be split into two different categories. First, we gained significant insights into the inner workings and limitations of the ADS-B phase overlay technique. Using the testbed presented above, we were able to evaluate the performance of the phase overlay in terms of bit error rates under different conditions. Second, we identified the TESLA protocol as a valid candidate for providing authentication and integrity to ADS-B users based on the additional bandwidth that will become available with the phase overlay. In addition, we propose modifications to the original protocol to match the limitations of the phase overlay.

The results of both categories will be presented in more detail in the following subsection.

2.4.1 Setup Calibration

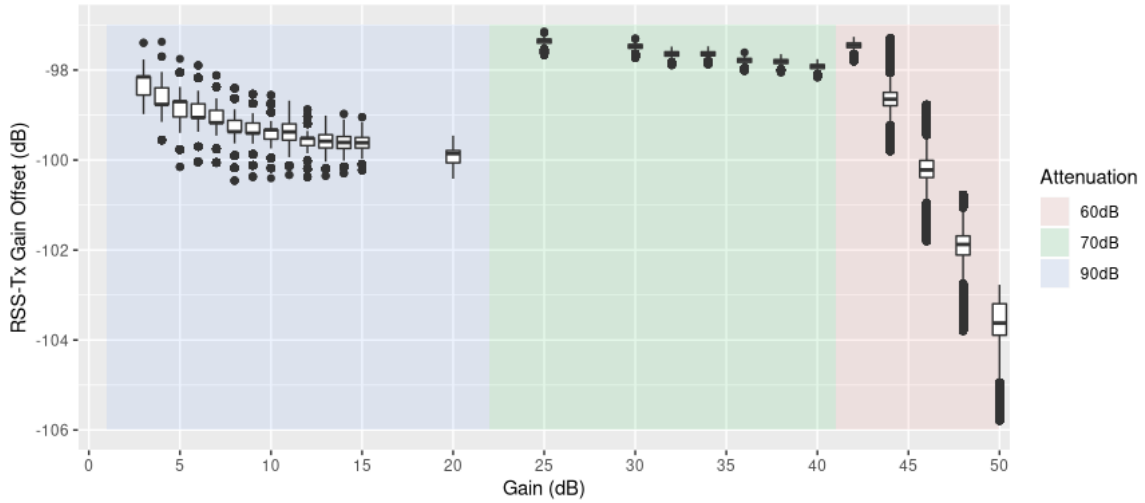

Figure 2.2: Setup calibration

In the first series of measurements, we validated that the testbed is working correctly in terms of generating signals at the desired signal strengths. The transmitter (Ettus USRP X300 software-defined radio with 2 UBX160 daughterboards) is initially not calibrated and only allows to change its transmit gain (in dB). To determine the unknown offset between gain and received signal strength in our setup, we first measured the received signal strength of ADS-B signals generated with different gains and analysed the offset. To increase the range of signal strengths to match the dynamic range of the GRX1090, we used three different configurations of static attenuators (60dB, 70dB and 90dB) and varied the signal strength using the USRP's gain setting.

Figure 2.2 shows the results of these measurements. There is a slight drift in the offset between the two values as the transmit gain increases. It seems to converge at higher gains and the drift over the full used transmit gain range of 20 dB is about 1 dB. Note that for this effect, the measurements with different attenuations need to be considered separately. Since we did not change any settings of the GRX1090 and since it was previously calibrated, we assume that the drift is solely caused by the transmitter. Moreover, the overall drift is smaller during the measurements with 70 dB attenuation which suggests that a large part of the drift in the lower gain region of the measurements with 90 dB attenuation was also affected by the low SNR. The figure also shows that the attenuators used to cover the full dynamic range were not perfect. After reducing the initial attenuation of 90 dB by 20 dB, the overall offset between the received signal strength and the gain increased on average by almost 2 dB, suggesting that the attenuator actually attenuated the signals by 22 dB instead of the specified 20 dB. The left- and right-most regions of Figure 2.2 show that the dynamic range of the GRX1090 without clipping ranges from -96 dB to -56 dB. Especially the measurements with a reduced attenuation of 60 dB clearly show the effect of the saturation of the receiver's radio front-end, resulting in a higher variance of power measurements (phase dependent) and an increasing offset due to the maximum measurable signal level. Finally, the resolution of the receiver's ADC of 12 bit limits the number of discrete signal levels and phases that can be measured by the receiver. Figure 2.2 shows the effect of this limitation on the received signal strength. While for higher signal levels (higher gains), the offset is very stable, variance becomes higher for lower gains.

We conclude that the setup generally behaves as expected with slight inaccuracies that can be compensated. However, we consider these inaccuracies negligible since only the calibrated received signal strength counts. We note, however, that an analogue PSK receiver implementation might

have a better performance when dealing with very weak signals due to the ADC resolution limitation.

2.4.2 Noise-free Channel Performance

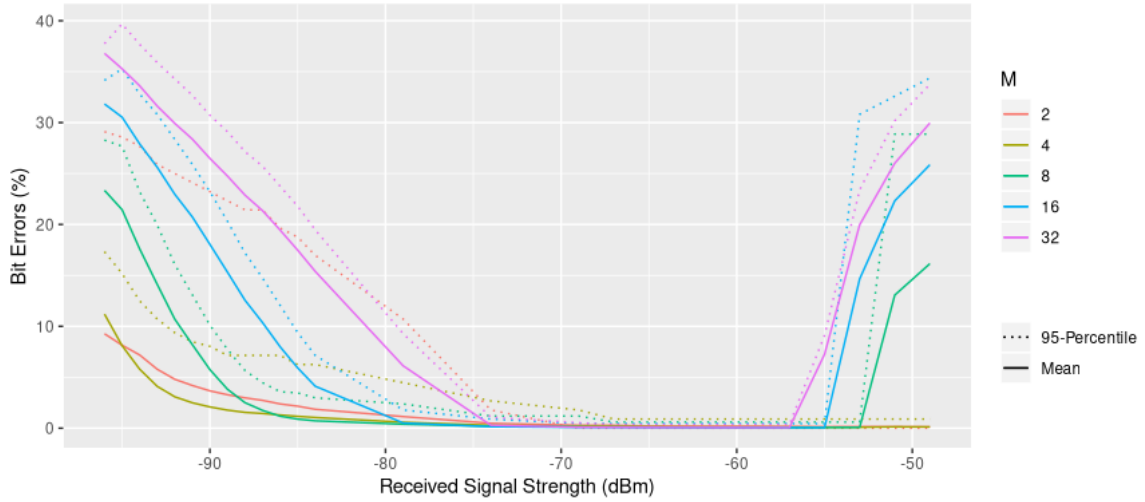

Figure 2.3: Bit Error Rate vs. RSS (Noise-free Environment)

The second series of measurements was conducted with a noise-free channel model, that is without adding interferences. We varied the gain over the full clipping-free dynamic range of the GRX1090 and repeated the measurements for M = 2, 4, 8, 16, and 32. As mentioned before, our main performance metric is the bit error rate, or, percentage of erroneously decoded bits per transmission.

The results are shown in Figure 2.3. As expected, the bit error rate increases with weaker signals and higher M are more susceptible due to a smaller tolerance to phase measurement errors. The latter is caused by the smaller phase-spacing between symbols. On the other end, bit errors rise abruptly at -56 dBm when the receiver's radio front-end is saturated (clipping). Note that unless there is a systematic error, the bit error rate should never exceed 50% since bits can only be either 1 or 0, so a random error distribution would result in 50% bit errors.

Overall, we conclude that given the 12-bit ADC resolution used by the GRX1090, the average bit error rate drops below an acceptable level of 10% for M<16 at signal levels as low as -91 dBm. If a wider dynamic range or higher M is required, an ADC with a higher resolution or an analogue PSK detector is recommended. However, we argue that for most scenarios, the performance achieved with the GRX1090 is sufficient. Moreover, using codes that support forward error correction (FEC), bit errors can be detected and corrected by the receiver. This will effectively increase the dynamic range. However, the net capacity decreases if more bit errors need to be corrected due to a higher required code redundancy.

2.4.3 Noisy Channel Performance

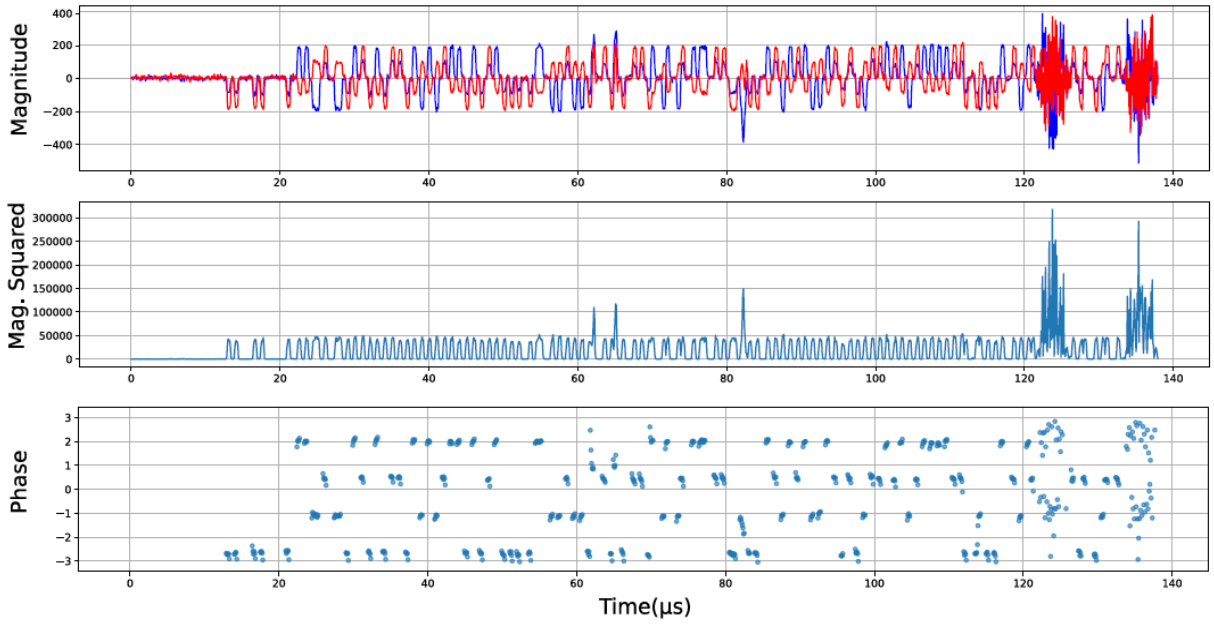

Figure 2.4: Example of received I/Q Data (top) with noise

The previous experiments can be considered the base line performance that is provided by the present hardware. However, a lower performance is expected in a real-world scenario due to the presence of interferences from other transmitters. Therefore, we continue our analysis with an evaluation of the impact of realistic interferences on the bit error rate of the phase overlay. For that purpose, we used a continuous 10 seconds I/Q recording received from another GRX1090 deployed 2 km from Frankfurt airport. The recording was captured on a Saturday during peak traffic hours (9am UTC), hence representing a very challenging radio environment with a large number of transmitters within the receiver's range. About 200 aircraft were tracked by the receiver at the time of recording and interference from other technologies such as DME were also captured. The recording was continuously mixed into the generated phase overlay signals during each experiment. Figure 2.4 shows an example for the I/Q data of an ADS-B signal with phase overlay that was captured during these experiments. This frame collided with DME interferences at its rear symbols.

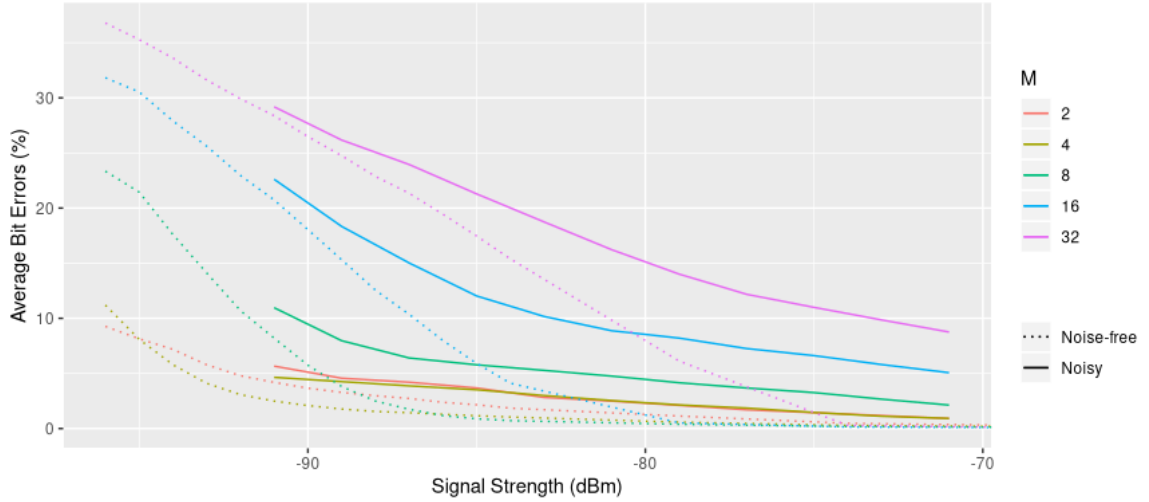

Figure 2.5: Bit error rate in a noisy environment

The results of this series of experiments in comparison to the base line experiments (noise free) is shown in Figure 2.5. As before (and unsurprisingly), weaker signals and higher M are more susceptible to bit errors due to interference from other transmissions. Interesting is, however, that the difference between the base line results and the new results is rather small for low signal strengths. This indicates that the dominating factor causing bit errors in these regions was the low signal-to-noise ratio and/or limited resolution of the ADC. This condition changes for higher signal strengths where the difference increases.

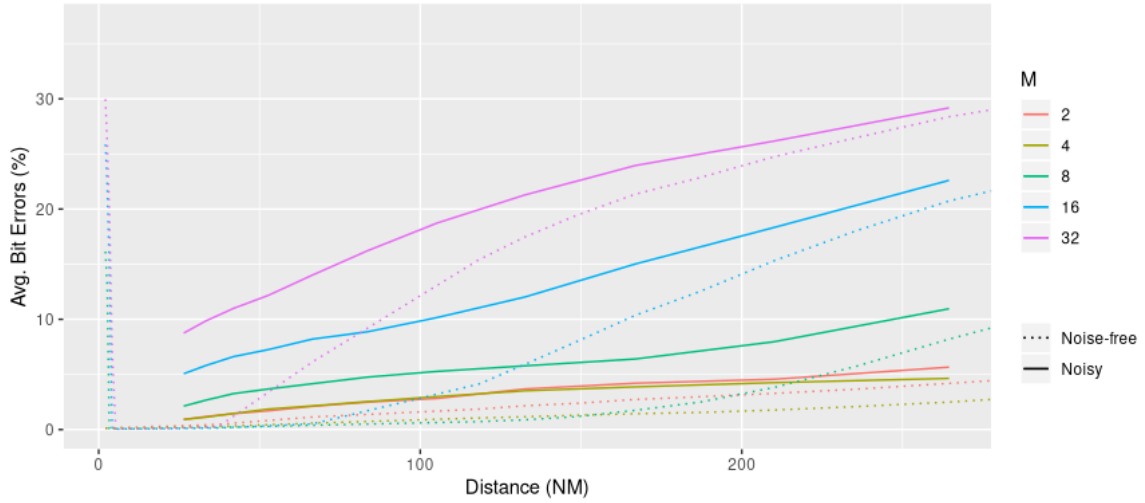

Figure 2.6: Average bit error rate over distance between receiver and transponder

To put these results into perspective, we mapped the received signal strengths to distances between transmitter and receiver using the free-space path loss model. Therefore, we assumed a transmission power of 56 dBm, which is common for transponders used by airliners. The results are shown in Figure 2.6. This analysis shows that for M<16, the average bit error rate stays below 10% up to 250 NM. Note that this analysis is simplified since it ignores factors such as antenna gains and cable losses at the receiver.

Based on these results, we finally estimate the capacity of the phase overlay within a noisy environment. We therefore assume that Reed-Solomon (RS) codes are used for forward error correction. RS codes require approximately twice the number of bits overhead that the code is able to *correct*. We now assume that a real-world phase overlay implementation is supposed to correctly decode 95% of transmissions from a transponder transmitting at 56 dBm over a distance of 250 NM. Based on our results shown in Figure 2.6, we can subtract the number of bits needed by an RS code to correct the expected 95%-percentile of the bit errors at a distance of 250 NM from the total number of bits in a frame for a given M.

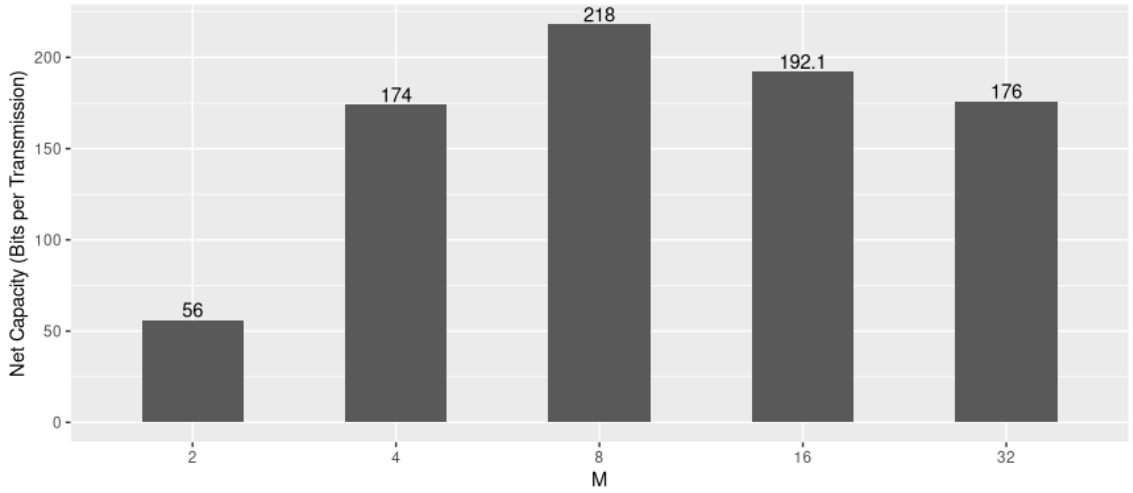

Figure 2.7: Net capacity of phase overlay in a noisy environment

The results of this analysis are shown in Figure 2.7. We can conclude that under the above assumptions, a phase overlay with M=8 performs best, providing an additional net capacity of 218 bit for each ADS-B message with at least a 95% chance of successful PSK decoding within a range of 250 NM.

2.4.4 Carrier Frequency Offsets

While the results provided in the previous section is certainly the most important one in this study, we also did experiments that analysed the resistance of the phase overlay against carrier frequency offsets. A carrier frequency offset between transmitter and receiver results in a phase drift, whereas the amplitude of the offset determines the drift rate. If this drift rate exceeds the tolerance of the phase overlay configuration and without applying any drift compensation method, symbols cannot be decoded properly anymore, resulting in systematic bit errors.

In this final series of experiments, we varied the carrier frequency offset of the transmitter over a range from -250 kHz to +250 kHz in 10 kHz steps. We used the noise-free channel model in these measurements to be able to clearly separate the effect of the phase drift from the effect of noise.

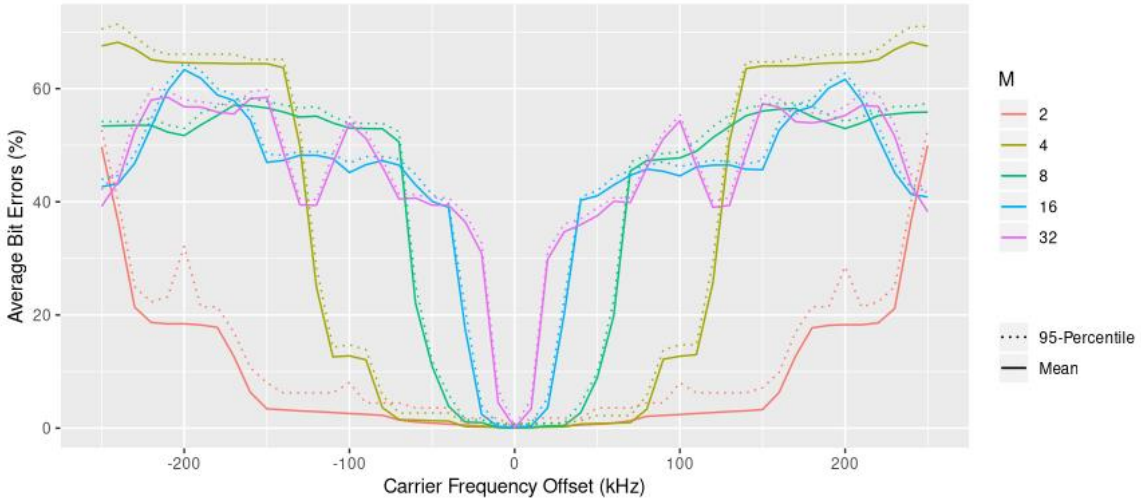

Figure 2.8: Effect of carrier frequency offsets on the phase overlay performance

The results are shown in Figure 2.8. As expected, the bit error rate has a symmetric behaviour as the absolute drift rate is the factor determining the bit errors and the sign of the offset only determines the direction of the phase drift. The results also clearly demonstrate that smaller M have a much better robustness against carrier frequency offsets. The most promising configuration M has a

frequency offset tolerance of about 40 kHz. Hence, transponders with phase overlay must have a much narrower carrier frequency offset requirement than those without (offsets up to 1 MHz allowed).

2.4.5 Authentication and Integrity Protocol

As mentioned above, the basis of our authentication and integrity protocol for the phase overlay is based on the Timed Efficient Stream Loss-tolerant Authentication (TESLA)-Protocol that was presented by Perrig *et al*. in 2002. The basic principle behind TESLA is to add authentication codes to broadcast messages that can only be computed with a key that is only known to the original transmitter. Then, after a pre-defined period of time, the sender discloses the key and by that enables the receiver to confirm the authenticity and integrity of the previously received messages retrospectively. The keys are connected via a one-way key chain and can therefore be related to each other. Whenever the receiver learns a new key, it can check whether that key was generated by the same entity that also created the one before.

Key Generation and Management

The keys used in this scheme for authentication are generated using a one-way key chain. A chain of length L is established by first selecting a random element K_L which serves as the last element of the chain. The chain is then created in a backwards fashion by applying a one-way function (e.g., a cryptographic hash function such as SHA-256) (L-1) times to K_L. Each intermediate result of the function serves as an element of the chain in a decreasing order. Note that whenever a key K_i becomes known, it is possible to deduce all keys K_j with $j < i$ by applying the one-way function to it. This property is called commitment in the sense that K_j commits to K_i if $j < i$ since whenever K_i is revealed, it is also revealed whether K_j belongs to the same chain as K_i or not.

TESLA uses each key K_i for a fixed period of time to authenticate messages and then reveals the key to enable the recipient to verify the authenticity of those message. In the context of ADS-B, trade-offs have to be made with respect to the (fixed) length of the disclosure interval. On the one hand, a longer disclosure interval allows the sender to pre-calculate and store less intermediate keys to cover a certain amount of time with a single key chain. This would have the operational benefit of lowering the resources (memory, CPU) needed in the transponder to use the same key chain for a whole flight. If this was possible, the key management could be significantly simplified as will be explained later. On the other hand, intervals must be short enough to support surveillance requirements. More specifically, in the ADS-B environment, surveillance information should become available to the users within at most 1 second. To make sure that only authenticated information becomes available to the user, the disclosure interval must be shorter than this 1-second limit. For the remainder of this report, we will assume a 0.5 second disclosure interval which should satisfy the latter requirement in practice.

Time Synchronisation

To coordinate the disclosure interval mentioned in the previous paragraph between the sender and receiver, the TESLA protocol requires a loose time synchronisation between sender and receiver. In the case of ADS-B, a tight time synchronisation could be achieved by relying on GPS on both sides. The reader should note that this assumption can generally be made for aircraft using ADS-B since they usually use GPS anyway to determine their exact location. Also ground stations are usually synchronised for a variety of reasons such as event logging, exact timestamping of messages, and so on. This is usually also achieved using GNSS such as GPS. However, for the purpose of this protocol, a lighter synchronisation mechanism such as NTP would suffice.

Should the protocol avoid any dependence on external timing sources for reasons such as system complexity or security, ADS-B could be extended such that it broadcasts a timestamp in a regular interval (e.g. at 1 Hz). This timestamp could then be used by the ground station to determine the

offset between its own and the transmitters clock, resulting in a light synchronisation. The implicit assumption here is that the drift of the sender and receiver clocks are sufficiently stable over the transmission interval.

It is worth mentioning here that this authentication protocol is not secure against stronger attacker models, where the attacker can also manipulate the time synchronisation. A coordinated attack on the synchronisation between sender and receiver and the authentication protocol at the same time can make the protocol vulnerable to (temporary) injection of false information. However, secure time synchronisation is beyond the scope of this work.

Message Authentication Codes

In order to authenticate single messages, so called message authentication codes (MACs) must be attached to each message. The phase overlay provides additional capacity for each ADS-B transmission that could be leveraged for this task. Moreover, a MAC algorithm has to be chosen that is easy to compute since avionics and transponders are likely to be limited in their resources and, while usually more powerful, ground stations will have to process data from several hundred targets in a busy airspace. At the same time, the algorithm should provide robust security and good hardware support.

One group of algorithms which satisfies these needs are cipher-based MACs (CMACs). In general, CMACs leverage symmetric encryption algorithms to encrypt data using a secret key and then use the encrypted output of this process to generate a MAC. The big advantage of using symmetric ciphers is their computational efficiency and hardware support.

For our protocol here we propose using AES-CMAC5 due to its excellent security and wide hardware support. In AES-CMAC, a message is split up into blocks of 128 bits. Since an ADS-B message M only has a length of 112 bits (the full DF17 frame), the algorithm first extends it to 128 by appending a 1-bit followed by 15 0-bits. Then it uses the Advanced Encryption Algorithm (AES) to encrypt that block to cipher text C = AES-128(K, M), which then serves as our MAC.

C also has a length of 128 bits and will be truncated to a smaller size by just using the desired number of most significant bits. This mechanism will be used below to be able to combine both the authentication code and the disclosure of the previous key in the same message.

[5] https://tools.ietf.org/html/rfc4493

ADS-B Authentication Protocol

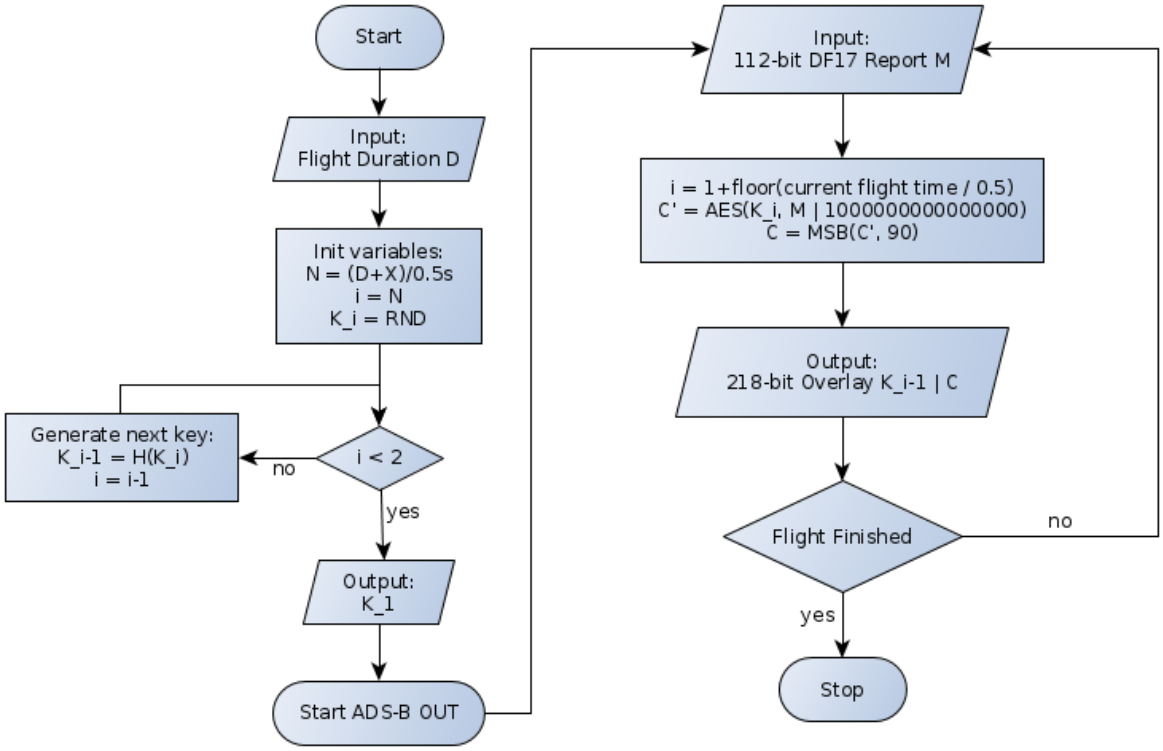

Figure 2.9: On-board Generation of Overlay Payload

The flowchart for the process generating the payload ADS-B phase overlay according to the TESLA protocol is provided in Figure 2.9. Given the above assumptions (0.5 s key disclosure schedule, loose time synchronisation), the first step of the protocol is the initialisation at the transmitter, i.e., at the ADS-B transponder. Before it starts broadcasting ADS-B transmissions it generates a key chain that is long enough to cover the whole flight (duration D) plus some margin for delays (X, e.g. 1 hour).

Once this key chain is generated, the transponder outputs the last key K_1 that can then be added to the flight plan or provided to any other trusted third party for authentication (see below). The transponder then starts broadcasting its ADS-B messages and adds the following information to each message in the phase overlay:

- the disclosed 128-bit key K_{i-1} of the previous key schedule period (all zeroes in the first period), concatenated with
- the (218-128 =) 90 most significant bits of the MAC generated for the message with the currently active key Ki

On the receiver side, the receiver buffers all incoming messages until it receives the first message of the next key scheduling period. It then extracts the disclosed key from that message and verifies the authenticity of the buffered messages by first checking whether the key is part of the key chain and then re-calculating all MACs using the revealed key. It then compares whether the MACs are equal. If so, it considers the messages authenticated and publishes or forwards them for further processing. This process is depicted in Figure 2.10 on the next page.

While the mere use of the protocol can already prevent some attacks (e.g., attacks that aim at modifying information on an existing target), a trusted third party would be required to provide means for verifying that the used key chain actually belongs to the identity (transponder) that uses it. This could be realised with a low footprint on the operational processes by, for example, adding

the last key of the chain, that is, the key that is used in the first key schedule period, to the flight plan. Since flight plans are usually passed on to ANSPs prior to handling the flight, a key chain could be authenticated by an ANSP by re-generating they keychain all the way to the last key upon reception of the first ADS-B message (which includes the key of the last key schedule period).

Security

The security of the scheme is provided by the fact that an attacker trying to spoof messages would have to guess the key used in the current key scheduling period. Under the assumption that the attacker cannot break the one-way function used to produce the key chain nor is in the possession of any of the keys used in this or any future period of the flight, it will be nearly impossible to brute-force the currently used key within the rather short key scheduling period of 0.5 seconds. Hence, the attacker will not be able to generate valid MACs for the current key scheduling period and will therefore not be able to inject any fake ADS-B message.

A nice side effect of the protocol design is that the freshness of the data is also assured through the time-based key disclosure schedule. The short disclosure periods of 0.5 seconds prevent the injection of outdated information through replay attacks.

Message Loss

Many ADS-B transmissions are lost in a realistic radio environment due to, among other things, interferences from other transponders. To cope with such loss, the above protocol is designed such that the verification process is not interrupted by loss of single messages. Since the key of the previous key scheduling period is provided with every message, a single message from the current period is sufficient to authenticate all messages received in any of the earlier periods.

Sender Requirements

Ignoring the hardware needed to generate the signals and the phase overlay, the resources needed by the transmitter to apply the protocol are mainly memory. For a flight lasting 6 hours and a key length of 128 bits, the transponder would have to generate 43,200 keys that would amount to a data volume of about 0.7 megabytes. If necessary, the volume can be reduced, or rather traded for CPU, by only storing every x-th key and re-calculate the intermediate keys when they are needed. We consider the calculations needed when generating the messages to be rather negligible since being a symmetric cipher, AES can be implemented very efficiently in hardware and only a single block needs to be encrypted for each message.

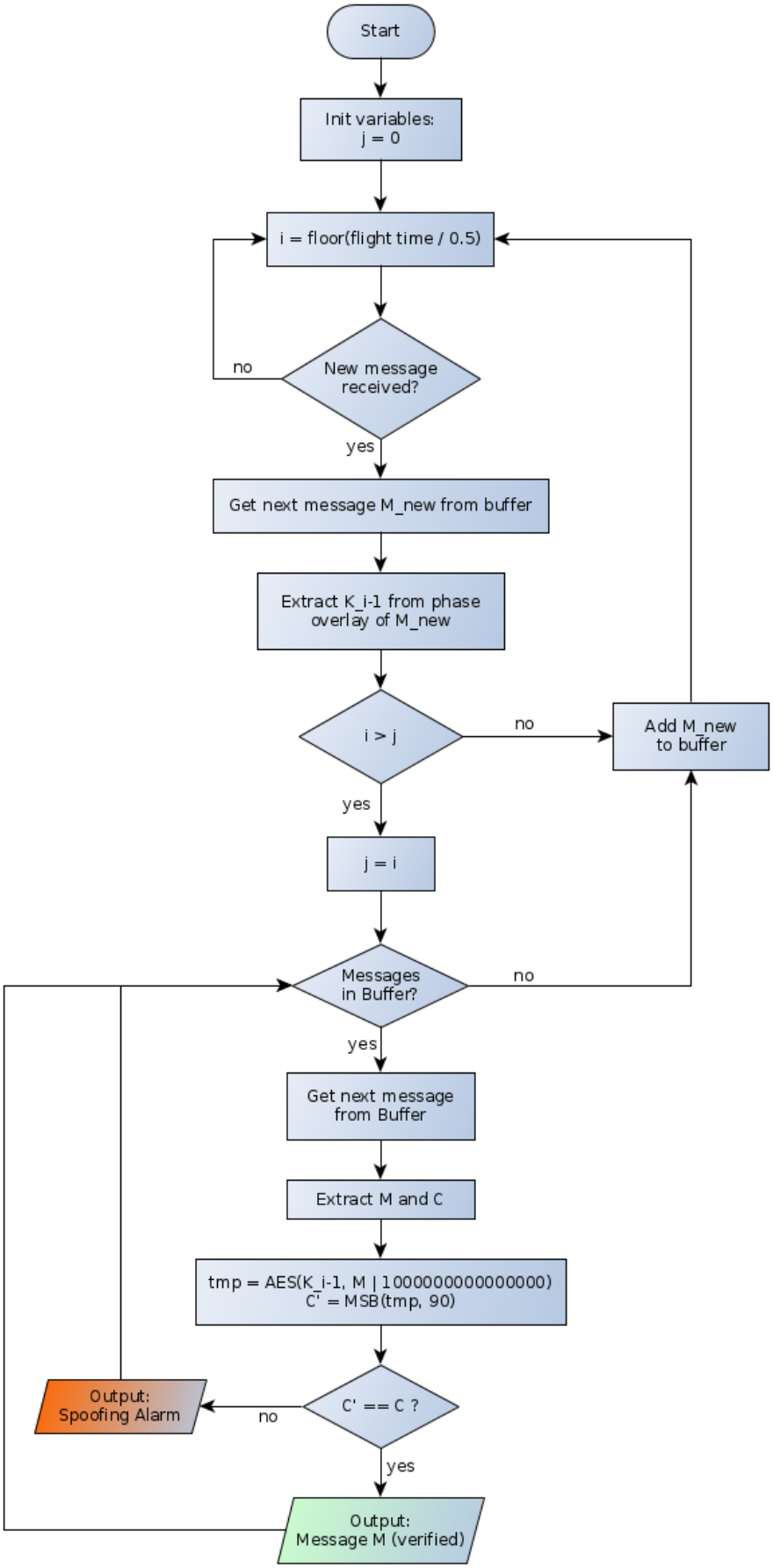

Figure 2.10: Verification Process at the Receiver

Receiver Requirements

The resources needed by the protocol on the receiver side are much higher than those required by the sender. The receiver needs to buffer all messages that are received over a single key schedule period. Based on our own observations, a single receiver can track as many as 250 aircraft at a time in airspaces with high traffic densities. If the receiver receives on average 4 ADS-B reports from each aircraft (accounting for some message loss), the receiver would have to buffer about 500 reports in a given scheduling period and then perform the same number of verifications in the subsequent period. Assuming that an ADS-B report consists of the 112 bits of the pulse position-modulated DF17 signal and the 218 bits of the phase overlay, a receiver would have to buffer about 21 kilobytes. Since the verification is as computationally efficient (encryption of a single block) as the generation of the MAC, we assume that a typical ground stations should be well able to perform the verification in negligible time, given that nowadays, most processors have built-in hardware support for AES.

3. Conclusions, next steps and lessons learned

3.1 Conclusions

In this project, we have designed and implemented a testbed that lowers the entry barrier for realistic research incorporating the phase overlay significantly. More specifically, our testbed can provide a realistic radio environment without the need for conducting expensive measurement campaigns using test flights and setting up temporary ground infrastructure. Using this testbed, we conducted extensive measurements evaluating different configurations and aspects of the new phase overlay. Our findings (see 'Lessons learned' below) can be used to select the right configuration for the phase overlay that maximises the net capacity provided by this additional data link. They also highlight the limits and challenges that are associated with the phase overlay such as backwards compatibility and the need for stricter requirements for the radio hardware.

Besides evaluating the phase overlay and determining the expected capacity that will become available through it, we have also proposed a design for integrating the TESLA protocol into ADS-B using the new phase overlay. This extension would provide ADS-B with the overdue authentication and integrity capabilities that would solve the most stringent security issues of ADS-B in a sustainable way. Our design choices proposed in this project are specifically tailored for the ADS-B environment as they respect conditions such as low hardware and key management overhead, a maximum verification delay of 1 second, and tolerant to loss of transmissions in busy radio environments.

3.2 Next steps

Some challenges associated with the integration of the phase overlay into ADS-B remain. For instance, it is unclear whether the phase overlay with the proposed configuration (M=8) is fully backwards compatible. Specifically, the configuration could exceed the limited bandwidth of receivers, resulting in drops in detected signal strength for some symbol transitions. Depending on the signal processing at the receiver, these drops may have a negative impact on the correct detection of the signals by legacy receivers. Hence, further measurements are needed with high bandwidth receivers to determine the spectrum footprint of the phase overlay and its effect on existing receivers without phase overlay capability needs to be evaluated.

Finally, only a real-world in-flight test of the phase overlay and the authentication protocol can provide the ultimate validation of the findings of this project and demonstrate the protocol's usability and benefits to the stakeholders.

3.3 Lessons learned

We demonstrated the potential that comes with the upcoming phase overlay for the security of ADS-B. In particular, our evaluations have shown that in a realistic environment, the phase overlay performs best with M=8, providing an estimated net capacity increase of 218 bits for each ADS-B transmission. This capacity increase is enough to integrate protocols that provide sustainable security to ADS-B.

However, some challenges remain. Our measurements have shown that this capacity increase requires the underlying Mode S transponders to satisfy requirements that are much stricter than those that are imposed by the current specification. In particular, the carrier frequency offset tolerance for transmitters and receivers using the phase overlay must be limited by the specification such that 42 kHz is never exceeded. This can be achieved, e.g., by limiting the allowed carrier frequency offset of both receiver and sender to 21 kHz each. In addition to that, it still needs to be determined whether the phase overlay will have negative effects on the backwards compatibility of 1090ES ADS-B.

Another challenge is the integration of a security protocol such as the one proposed in this project into the operational processes used in air traffic management. Although the organisational footprint of the protocol proposed here is small (adding a 128-bit key to the flight plan), we argue that no authentication protocol can be integrated in a completely transparent manner, i.e., without the need for modifying any of the protocols and data structures that are currently used to exchange information in the air traffic management system. The reason is the need for connecting the keys used by avionics with the actual entity that is claimed. This is required to make sure a malicious actor is not just making up key chains and hence, it is required to provide full authentication. Such authentication is typically implemented using a trusted third party that verifies the authenticity of a device using a specific key or, in our case, key chain. As proposed above, such a trusted third party could be the organisation where the flight plans are filed, given that there is a secure way for the filer to provide the key to the organisation shortly prior to the flight.

4. References

4.1 Project outputs

The following outputs were and will be generated by this project:

Title	Description
ADS-B Phase Overlay Technical Report	This report presents the design and results of the extensive measurements that were conducted as a part of this project. Besides the measurement results, it provides recommendations and potential limitations that may arise when implementing the phase overlay.
Data Analysis Notebook	The results of the phase overlay measurements were analysed beyond the aspects presented in the technical report. The notebook of the data analysis (including Gnu R code) can be found under this URL: https://sero-systems.de/resources/phase_overlay.html
Evaluation Testbed	The testbed that was built for this project continues to be maintained by the Distributed Computer Systems Group of TU Kaiserslautern for future tests and measurements. As soon as airborne equipment with phase overlay capabilities becomes available, parts of the testbed will be advanced towards TRL 5.
Measurement Data Set	During the measurements, the partners accumulated a vast amount of measurement data that could be used as input for further research. For example, it could serve as a realistic reference data set to evaluate error correcting codes that might later be integrated into the specification.
Algorithm Design	The TESLA broadcast authentication protocol was modified such that it matches the capacity and conditions of the ADS-B phase overlay. The design is presented in the final technical report.
Presentation at 2nd Engage TC1 Workshop	A presentation will be held at the 2nd Engage workshop on “Vulnerabilities and global security of the CNS/ATM system” on November 10, 2020.

4.2 Other

Perrig, Canetti, Song: Efficient and secure source authentication for multicast. Proceedings of the Internet Society Network and Distributed System Security Symposium, 2001.

Strohmeier, Lenders, Martinovic: On the security of the automatic dependent surveillance-broadcast protocol. IEEE Communications Surveys Tutorials, 2015.

RFC 4082: Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction, https://tools.ietf.org/html/rfc4082

RFC 4493: The AES-CMAC Algorithm, https://tools.ietf.org/html/rfc4493

-END OF DOCUMENT-