Interim Project Report

ADS-B Phase Overlay

Data Link Performance Evaluation

Document information	
Date:	November 8, 2019
Work package:	WP1 (Phase Overlay Evaluation)
Project title:	Authentication and Integrity for ADS-B
Project funding:	SESAR JU grant agreement no. 783287 (Engage KTN)
WP lead:	SeRo Systems GmbH
Contributors:	M.Sc. Markus Engel (TU Kaiserslautern)
	Dr.-Ing. Michael Arndt (SeRo Systems)
	Dr.-Ing. Matthias Schäfer (SeRo Systems)
	Prof. Dr.-Ing. Jens B. Schmitt (TU Kaiserslautern)
Author/Contact:	Dr.-Ing. Matthias Schäfer (schaefer@sero-systems.de)

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. Based on the results of our performance evaluation, we then devise a protocol that relies on the phase overlay to authenticate the information provided via the ADS-B. In this document, we report our findings of the first phase of the project. In this phase, we focused on evaluating the potential real-world performance of the phase overlay extension. Therefore, we tested two alternative phase coding schemes, phase shift keying (PSK) and differential PSK. For both schemes, we measured the bit error rate for different bitrates and noise levels. Moreover, we evaluated the real-world performance by generating a realistic radio environment. The 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.

Contents

1 Overview

Huge modernization 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 exact location, velocity, and identity over a digital data link. While this new approach has many advantages, its simplicity and the associated digitalization come at a high price. Surveillance information is no longer measured 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. Only recently, 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, e.g., to provide authentication and integrity. While the SESAR JU project 15.04.06 demonstrated that such an overlay is indeed feasible, its 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 projects aims at closing this gap by first investigating the performance of the ADS-B phase overlay under realistic 1090 MHz radio frequency conditions and then using these insights to design a viable ADS-B authentication and integrity protocol. In this first work package, we developed a tailored testbed and studied the bit rate of different phase overlay configurations under the presence of noise and FRUIT. The key outputs of this work package are a testbed for performance evaluations of ADS-B phase overlay under real-world conditions, the performance evaluation of different flavors of the overlay, and the concept for a compatible secure broadcast authentication and integrity protocol.

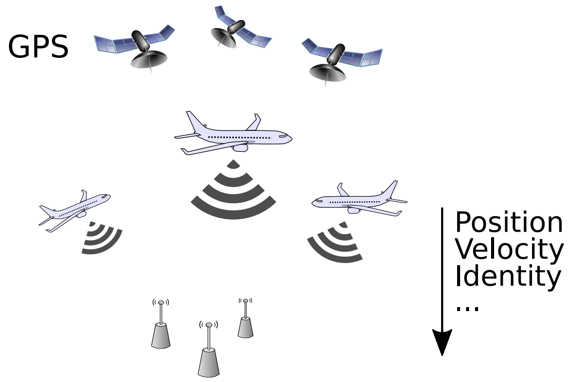


Figure 1: 1090ES ADS-B Architecture Overview. Aircraft determine their exact position using global navigation satellite systems such as GPS. Using the existing SSR Mode S data link, aircraft then broadcast their location along with other information such as their identity or status information to both ground and airborne receivers.

2 Background

2.1 Automatic Dependent Surveillance–Broadcast

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 localization requires expensive techniques such as multi-radar tracking. These shortcomings and the rapid increase in air traffic have led to major modernization 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 becomes mandatory in many parts in the world in the late 2010s (Australia[1]) and early 2020s (US[2] and Europe[3]), many airlines have already started updating their fleets with ADS-B capabilities. See Figure 1 for a simplified overview on the architecture of ADS-B.

2.1.1 Link- & Physical Layer

The ADS-B specification merely describes the function of broadcasting information [1]. Data link aspects such as the wireless medium or message structures are specified separately and there are two options. The Universal Access Transceiver (UAT) is specifically designed for supporting ADS-B and other aviation services such as the Traffic Information Service–Broadcast (TIS-B) [2]. It operates on the 978 MHz RF band. Since UAT requires aircraft to be equipped with new 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 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[5], a significant percentage of aircraft is still using ADS-B version 0 and 1 transponders. Nevertheless, since version 2 will be the prevalent version in the 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 in [3] and is the same for all three versions.

Figure 2 shows the coding and modulation used in 1090ES ADS-B. Transponders modulate 112 bit onto the carrier frequency 1090 MHz using a pulse position modulation similar to Manchester codes. The 112 bit ES format provides a 56 bit general purpose field (ME) which is filled in by the ADS-B unit of the transponder with binary coded information.

2.1.2 Security

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 in a Dolev-Yao [5] manner. With respect to the scope of this project, however, we focus on attacks that violate the integrity of spatial information. A

[1] Instrument number CASA 61/14

[2] Code of Federal Regulations §91.225

[3] Commission Implementing Regulation (EU) No 1028/2014

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

[5] According to SeRo Systems GmbH own data, the ADS-B version 2 equipage is at about 50% in Central Europe at the time of this writing.

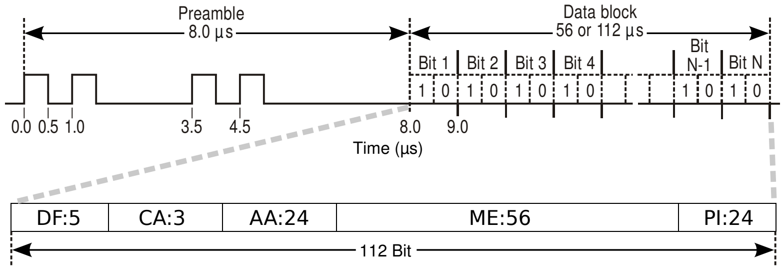


Figure 2: Modulation of Mode S replies and the Extended Squitter format according to [3]. The preamble consists of four pulses and is followed by the downlink format, which is set to 17 or 18 to indicate an Extended Squitter. The Extended Squitter provides information about the transponder capabilities (CA) and the unique aircraft address (AA). The 56 bit ME field contains the actual ADS-B data as defined in Appendix A in [4]. The parity identifier (PI) is finally used for error detection.

more complete overview of attacks, their implications, and potential countermeasures is provided by Strohmeier et al. in [6, 7, 8].

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 [8]. 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 onboard instruments [9]. A complete list of attack scenarios and physical limitations can be found in [10].

Although these vulnerabilities are known, the long development and certification cycles in aviation make the inclusion of security mechanisms into the ADS-B protocol extremely difficult in the short term[6]. 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.

2.2 Phase Overlay

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 additional capacity can then be used to, e.g., transmit authentication and integrity codes along with regular ADS-B data. This PSK extension to the regular pulse position modulation is often referred to as *phase overlay*. 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.

[6]The development and deployment of new technologies in civil aviation lasts about 20-30 years.

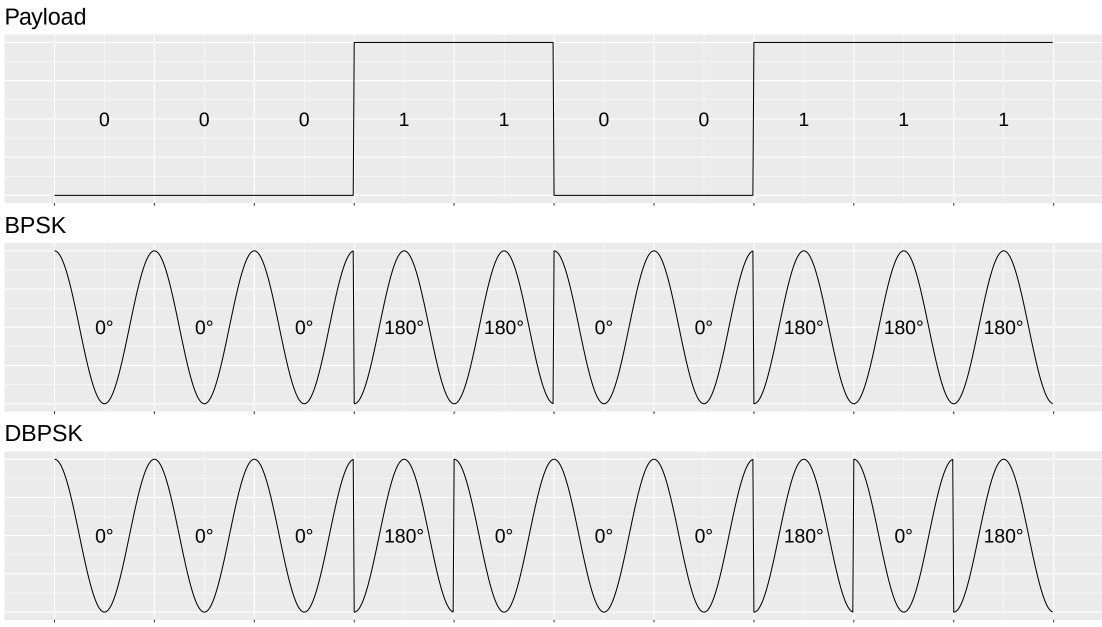


Figure 3: Example binary PSK and differential PSK modulation.

PSK-based modulations generally encode one or multiple bits by shifting the carrier signal phase. These phase shifts can be relative to either a fixed reference phase or to the phase of the prior symbol. The latter is referred to as differential PSK and the different possible shifts are referred to as symbols. The number of all possible phase shifts, i.e., the number of symbols, determines the number of bits per symbol. Given M different symbols, the number of bits per symbol is $\log_2 M$. Common values for M are 2 for binary PSK (BPSK), 4 for quadrature PSK (QPSK), and 8 (8PSK). An example for $M = 2$ is shown in Figure 3. In BPSK, the phase is one of two levels that are $360°/M = 180°$ apart. Without loss of generality, we assume that the reference is $0°$ encoding a binary 0 and $180°$ encoding a binary 1. On the other hand, in differential BPSK (DBPSK), the phase is the same as for the previous symbol if a 0 is encoded and changes by $180°$ whenever a 1 is encoded. Note again that in practice the M phase levels do not necessary have to be aligned with $0°$ but will always be separated by $360/M$ degrees to achieve best noise resistance.

When it comes to designing a phase overlay for ADS-B, two basic parameters need to be determined. First, the optimal number of symbols M needs to be found. While a higher number provides a higher theoretical bit rate, transmissions become more susceptible to bit errors due to noise or carrier frequency offsets since the phase distance between symbols becomes smaller. As a consequence, instead of simply looking at the bit error rate as a primary metric, the net data rate including possible redundancy for error correction needs to be considered when evaluating different M. Moreover, in order to find the optimal M, this net rate must also be evaluated in a realistic radio environment.

The second parameter that needs to be determined is whether to use absolute or differential coding. If “absolute” PSK is used, a synchronization mechanism is needed since the

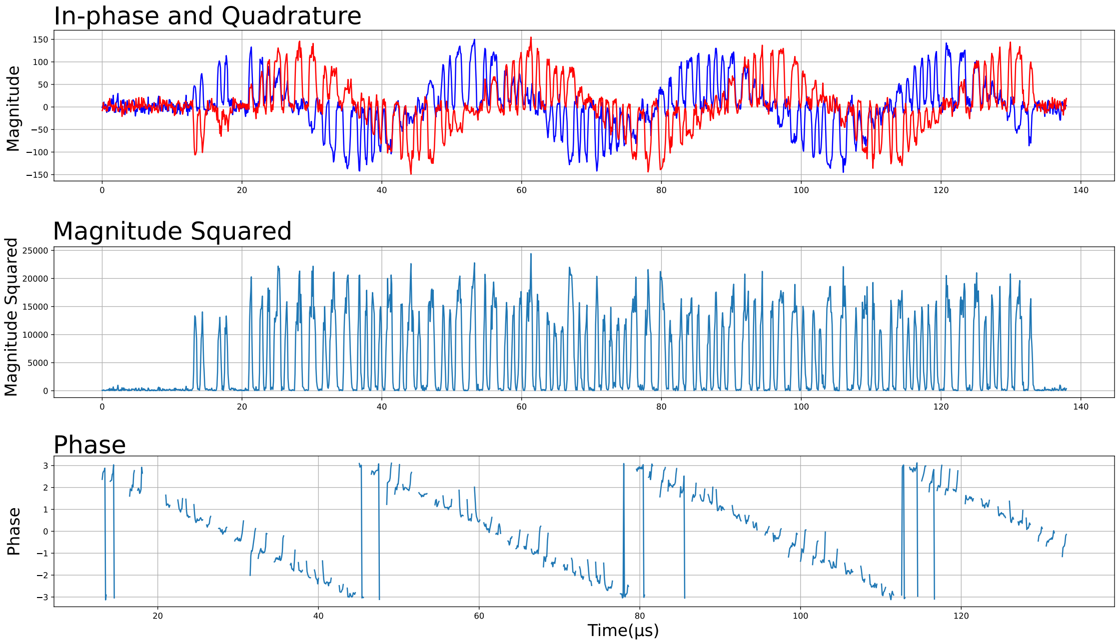


Figure 4: Real-world example for phase drift. These are the samples of a recorded ADS-B frame. The top plot shows the in-phase and quadrature of the frame. The "waves" indicate a phase drift, which is also confirmed by the bottom plot showing the phase. The drift is so high that the phase changes almost by four full rotations over the duration of the frame.

receiver/sender phase offset is unknown at signal reception. Moreover, ADS-B signal reception is always affected by significant carrier frequency offsets, mostly caused by Doppler shifts or sender/receiver oscillator inaccuracies. These frequency offsets result in phase drifts during the reception of a single frame. If this drift exceeds the tolerance of the PSK modulation (e.g., max. $45°$ over a period of 1 μs for $M = 4$), phase measurements will be misinterpreted which results in systematic decoding errors.

2.2.1 Differential PSK

Figure 4 shows an example of a recorded real-world ADS-B signal. The bottom graph shows the phase of the signal over the duration of the ADS-B transmission. Due to the carrier frequency offset between the received signal and the receiver's radio front-end, the phase is rotating almost four times during that period. A PSK modulation based on an initial phase synchronization (e.g. using the preamble as devised in [11]) might not be suited for this communication environment unless the carrier frequency offset limit becomes much stricter or some carrier tracking loop is implemented to compensate the drift. Note that such a carrier tracking loop can be susceptible to errors in environments with high levels of interference. If we assume the most noise-resistant case of $M = 2$ and a perfect phase synchronization in the 4 preamble pulses of Mode S signals, the carrier frequency offset Δf must not exceed

$$\Delta f < \frac{1}{\Delta t \cdot M} = \frac{1}{117\,\mu s \cdot 2} = 4274\,\text{Hz} \quad , \tag{1}$$

where Δt denotes the maximum time difference between the phase synchronization and the last payload symbol. In contrast, differential PSK has the advantage that phases are only compared between neighboring pulses which mitigates the effect of drift significantly since the Δt is reduced to $1\,\mu s$.

The current Mode S specification allows carrier frequency offsets for Mode S downlink transmissions of up to $1\,\text{MHz}$ [3, 3.1.2.2.1]. Given that two pulses can be separated by up to $1\,\mu s$, the carrier frequency offset limits of a differential PSK modulation based on pulse-to-pulse demodulation can still be exceeded if such soft limits are applied. For example, with $M = 4$ the theoretical limits for the carrier frequency offset (Equation 1) needs to be limited to at least $250\,\text{kHz}$. In practice, the limit for transmitter carrier frequency offsets needs to be even lower due to the presence of noise, Doppler shifts, and carrier frequency offsets of receivers. Hence, a more viable carrier offset limit for transponders with phase overlays would be in the $10\,\text{kHz}$ region used for the Mode S uplink which uses a differential phase coding [3, 3.1.2.1.1]. In fact, the authors of [11] mention that a frequency offset compensation is needed such that "a frequency offset of $+/-$ $42\,\text{kHz}$ relative to the receiver will still yield correct phase demodulated data".

While its better robustness against carrier frequency offsets is a major advantage, differential PSK has a disadvantage that might negatively affect its real-world bit error rate. Since the decoding of a symbol is always based on the phase of the preceding symbol, an error (e.g., due to overlapping signals) in one symbol always affects its succeeding symbol as well leading to an amplification of the bit error rate by a factor of 2.

2.3 Related Work

In 2013, Stayton and Pegano presented some theoretical considerations about a possible phase modulation technique for ADS-B to the International Civil Aviation Organization (ICAO) [11]. They propose using 8PSK modulation where the phase synchronization is done using the preamble bits and a phase drift compensation method is applied. However, the proposal is rather conceptual and does not define the specifics for a real-world evaluation. It is worth noting here that additional mechanisms such as the specific phase drift compensation or forward error correction (FEC) have significant effects on the actual performance of the modulation in a realistic environment. Since it is beyond the scope of this project to test all different implementations and extensions, we focus on evaluating the basic underlying techniques, i.e., PSK and differential PSK.

Following this proposal, several organizations and technology providers in the domain conducted a joint study in the SESAR Joint Undertaking Project 09.22 and 15.04.06 which ended in 2016. In [12], the project members outline the requirements for a prototype receiver with phase overlay capabilities. This prototype was then implemented and laboratory measurements were conducted in [13]. The implementation is mostly in accordance with the proposed modulation from [11]. However, implementation details such as the phase drift compensation that was used were not provided in the report.

In parallel to these projects, Yeste-Ojeda and Landry took a different approach in [14]. They proposed using a differential 16PSK phase overlay to add security services to ADS-B. Although they did not conduct a experimental evaluation, they did test the spectrum compliance of their approach, a feature that was neglected in [13]. Nguyen et al. later extended this work by implementing a hardware-in-the-loop simulation of the proposed differential 16PSK modulation in [15] and [16]. The lab measurement setup was composed of two SDRs, one for sending the other for receiving, and a certified ADS-B receiver to test backwards compatibility.

2.4 Research Goals

To conclude this section, we summarize the open questions and design parameters that need further evaluation in order to assess the net capacity provided by a phase overlay under realistic conditions. First, an optimal parameter M needs to be determined for the differential PSK modulation. This M must provide the highest possible net data rate while maintaining sufficient robustness against carrier frequency offsets and other sources of noise. As mentioned in subsection 2.3, other researchers and technology providers have conducted research and experiments with PSK modulations as well. While Yeste-Ojeda and Landry proposed $M = 16$ in [14], $M = 8$ was used in the lab demonstrator by Indra in [13]. These works, however, rather constitute feasibility studies with a focus on prototypes. They did not provide elaborate studies comparing the performance for different M under diverse conditions.

Another aspect that is not covered by previous works is the performance of different PSK schemes under the presence of interference from other transmissions. Since the $1090\,\text{MHz}$ frequency is heavily overused in key airspaces such as Central Europe, reception of overlapping (so called garbled) signals is immanent. Hence, interference resistance is a key property that needs to be considered in order to design a viable PSK modulation scheme.

Under consideration of the works that have been done previously, we identify the following open research questions that need to be tackled next and are the main focus of this research project:

- What is the optimal PSK parameter M?
- What is the expected net capacity increase with a phase overlay?

The remainder of this report aims at providing answers to these questions. Therefore, we first design and implement a testbed for evaluating the respective aspects. Using this testbed, we then perform extensive measurements which test the performance of different PSK configurations in different scenarios.

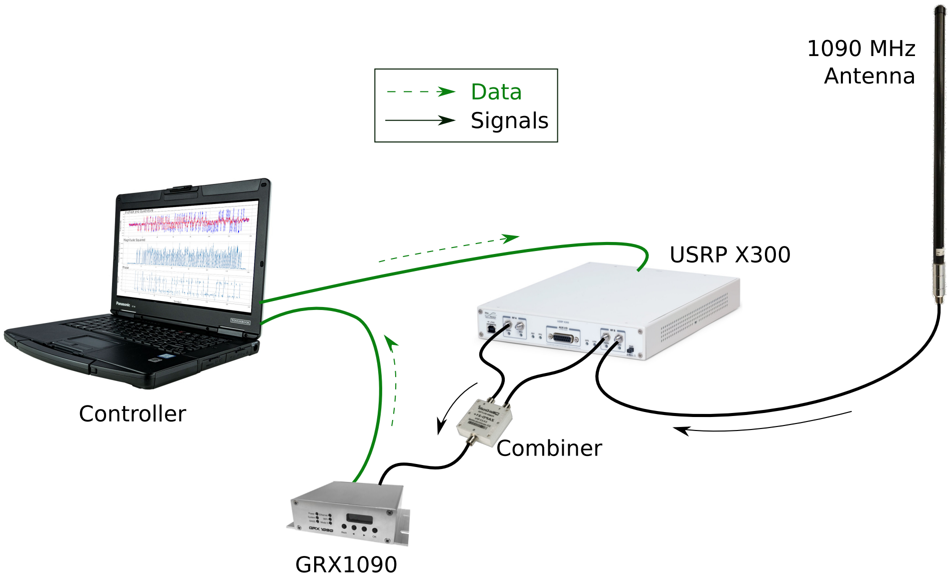


Figure 5: Testbed developed for the experimental evaluation of different phase overlay configurations. Note that additional attenuation was added to the TX connectors of the USRP to reduce signal leakage from internal oscillators.

3 Evaluation

In order to tackle the aforementioned research problems, we designed and implemented a testbed for evaluating different phase overlays. Using this testbed, we then conducted a series of measurement campaigns with the ultimate goal is to gain insights on the provided real-world performance of a phase overlay in terms of gained data link capacity. Therefore, we used the *bit error rate* as our primary metric during the measurements. The results can 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 can therefore be estimated once the bit error rate has been determined.

3.1 Testbed

Figure 5 shows the overall architecture of the testbed that was developed for our measurements. 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 synchronized 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 synchronization.

The ADS-B signals with phase overlay are transmitted using an Ettus USRP X300 software-

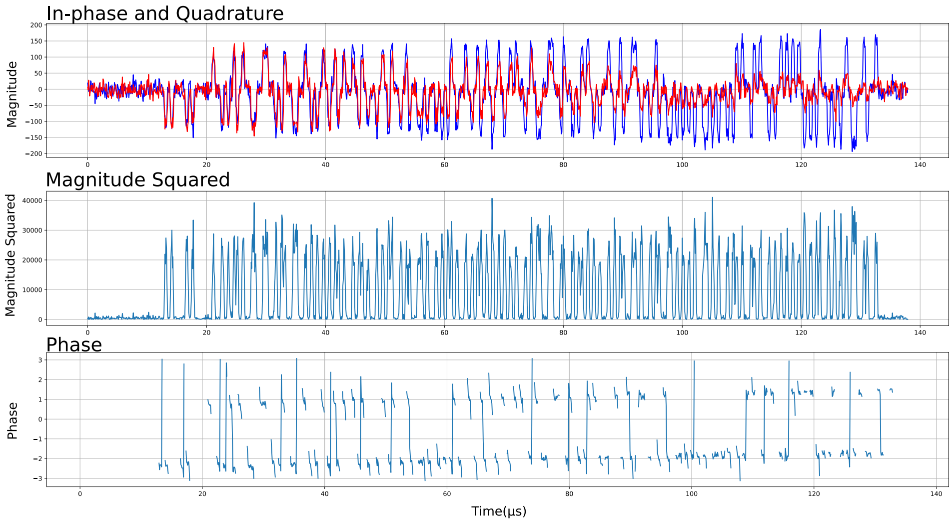


Figure 6: Example recording of an ADS-B frame with a BPSK phase overlay. The phase overlay can be interpreted as BPSK and differential BPSK at the same time resulting in two different payloads. For BPSK, we used the four preamble pulses for phase synchronization. It is worth noting that a slight carrier frequency offset is still left although both devices were tuned to 1090 MHz. This is likely caused by a slight oscillator inaccuracy since the transmitting SDR is not GPS-disciplined.

defined radio. The device is equipped with two full duplex radio front-ends (UBX160 daughterboards) which allow the transmission of two independent signals. The two signals are mixed using a combiner and then fed into the GRX1090. At the same time, the USRP can receive signals from an outdoor antenna which can then be mixed into the artificial signals to create a realistic radio environment. Moreover, the setup allows replaying and injecting I/Q recordings from remote GRX1090 receivers. This enables us to realistically reproduce a radio environment from a remote location (e.g., near a major airport). To avoid amplifying pure noise, a squelch is applied to the recording before mixing the received real-world signals with the generated ADS-B signals.

A controller host runs a Mode S signal generation application developed by SeRo Systems. It allows crafting Mode A/C/S signal data for many SDR platforms, including the USRP X300. The application generates a fixed-rate reference signals with arbitrary payloads and amplitudes. Moreover, the tool allows replaying transmissions from a CSV file and the generation of overlapping interference signals with predefined time and phase offsets to the reference signal. These interference signals are then either mixed with the reference signal in software or the application sends them to a second SDR. In our case, we use the second radio front-end of the USRP X300 to transmit the interference signals. For every pulse, the application also allows specifying the exact phase. This functionality is used to implement the phase overlay.

While the signal generator is producing the reference signals, another application running on the controller retrieves the decoded ADS-B frames along with their I/Q data from the

GRX1090. It then demodulates the phase overlay using differential PSK for a given M. An example for the data provided by the GRX1090 receiver for an ADS-B signal with BPSK overlay is shown in Figure 6. Since the USRP is not GPS-disciplined or otherwise synchronized with the GRX1090, a minor carrier phase offset is still visible. However, this is consistent with a real-world scenario since there will always be a carrier frequency offset due to Doppler shifts and inaccurate oscillators.

Transmission power: A major part of our experiments is to test the phase overlay performance at different signal-to-noise ratios. Therefore, we had to vary the transmission power during experiments to simulate different transmitter-receiver distances. To cover the full dynamic range of the GRX1090 (-96 dBm to -56 dBm where clipping starts[7]), we use a combination of attenuators and the variable hardware gain provided by the USRP's UBX160 daughterboards. The initial attenuation used to generate signals close to the detection threshold of about -96 dBm was 90 dB. We have chosen a rather high attenuation to additionally suppress leakage of constant signals close to 1090 MHz from internal oscillators. While the transmit gain of the UBX160 daughterboard ranges from 0 dB up to 31.5 dB, saturation is achieved at about 25 dB. Hence, we did not use any gain higher than that but rather reduced the attenuation to achieve stronger signals at the receiver. For the sake of simplicity, we will always refer to the combination of the transmitter's hardware gain and the attenuation simply as gain with the following definition:

$$\text{Gain [dB]} = 90\,\text{dB} - \text{Attenuation} + \text{UBX160 TX Gain}$$

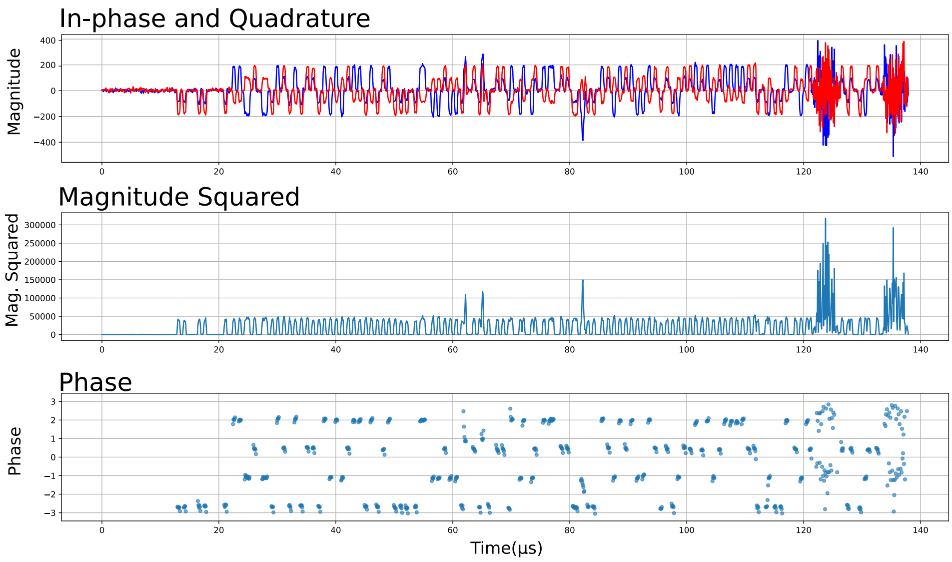
For more details, see the calibration of the testbed in subsubsection 3.3.1, in particular Figure 8a.

3.2 Experiments

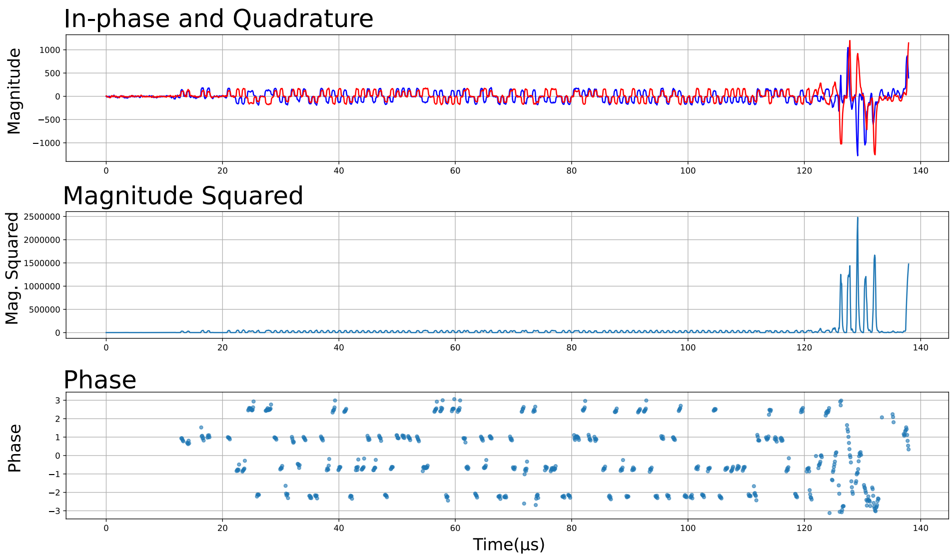
Using the above testbed, we performed a series of automated measurements with the goal to find the best M and gain insights on the additional capacity provided by the phase overlay. In all measurements, we generated a reference signal at a constant rate of 100 Hz with payload `8dffffff204c548f000000178992` (transponder address 0xffffff, downlink format 17, typecode 4, callsign "SERO"). For every successfully received transmission, we also decoded the respective PSK payload and stored the number of bit and symbol errors. Each individual experiment (i.e., for each configuration) was running for a duration of 120 seconds, i.e., 12,000 reference frames were transmitted for each combination of M and gain.

To be able to distinguish the influence of different factors such as M, signal-to-noise ratio (SNR), and the presence of noise on the phase overlay performance and to be able to assess its performance in a realistic radio environment, we repeated our experiments for $M \in \{2, 4, 8, 16, 32\}$ and different gains using three different radio channel models.

[7] Note that the GRX1090 receiver can receive signals with strengths up to 10 dBm, but any signal stronger than -56 dBm is subject to clipping which negatively affects phase information in the signal.



(a) Noisy channel example 1: the reference signal was mixed with some weak Mode A/C interference at about 65 μs and a stronger DME transmission (X channel) at the end.



(b) Noisy channel example 2: the reference signal was mixed with a strong Mode A/C transmission at the end.

Figure 7: Examples of recorded reference signals with $M = 4$ during experiments in which a continuous I/Q sample recording from FRA was replayed.

Noise-free channel: only the reference signal with phase overlay for different M and different transmit gains was generated. The goal of these measurements was to evaluate the experimental setup and to learn more about the impact of M and the SNR on the phase overlay performance.

Noisy channel: the reference signal with phase overlay for different M and different transmit gains was mixed with a continuous I/Q recording from Frankfurt am Main Airport (FRA) during peak traffic hours. The goal of these measurements was to see the performance of the phase overlay under realistic radio conditions. Figure 7 on page 14 shows two snapshots of successfully received reference signals during these experiments.

Carrier frequency offsets: the reference signal with phase overlay for $M \in \{2, 4, 8, 16, 32\}$ was generated with different carrier frequency offsets ranging from -250 kHz to 250 kHz in 10 kHz steps. The goals of these measurements was to investigate the robustness of the differential PSK schemes against carrier frequency offsets.

3.3 Results

We summarize our most important findings in this section. More details and further analyses are available in this notebook:

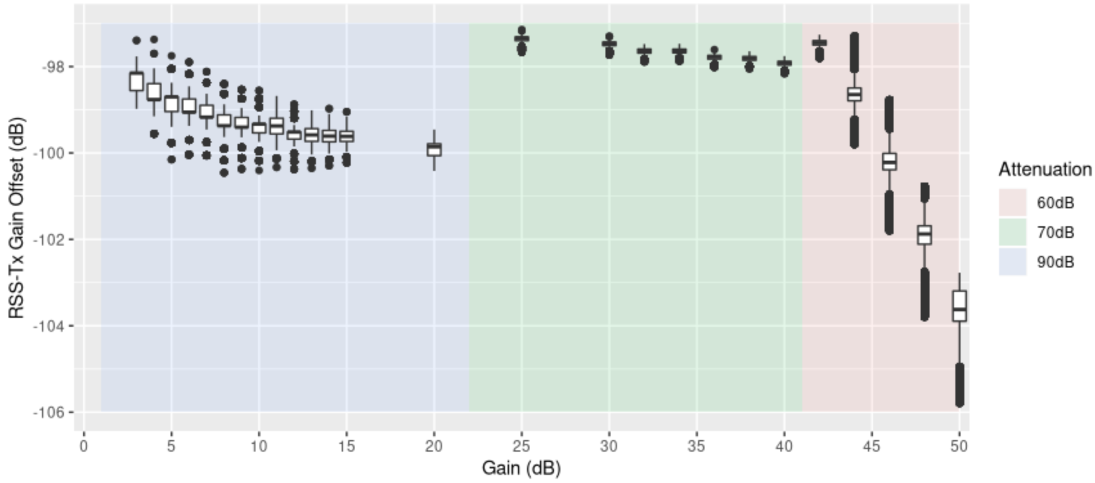
`https://doc.sero-systems.de/phase_overlay.html`

3.3.1 Setup Calibration

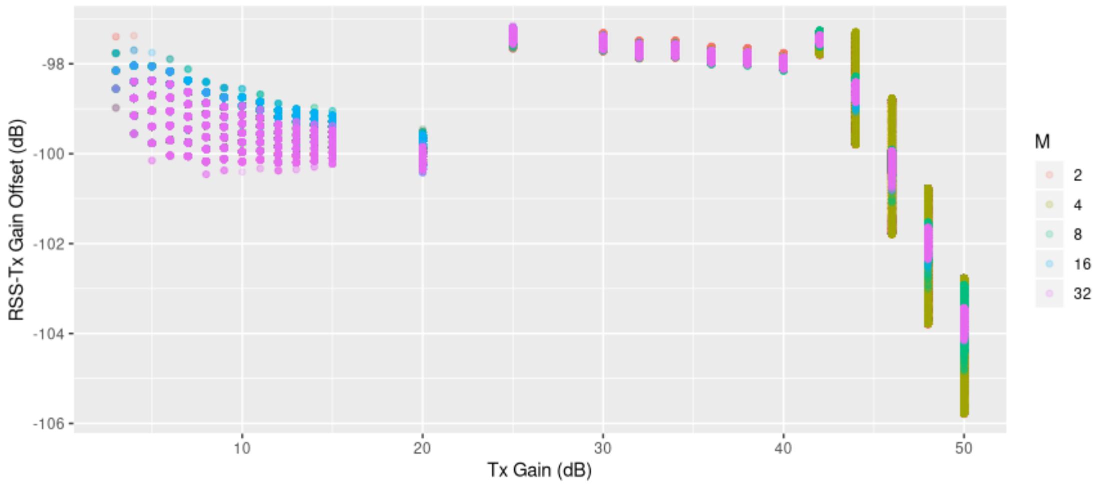
In the first series of measurements, we validated that the testbed is working correctly in terms of generating signals at the desired signal strengths. The results of these measurements are shown in Figure 8 as the the differences between the gain[8] in dB and the received signal strength in dBm. There are several interesting observations.

Non-linearity of the TX Gain: Figure 8a shows that the relationship between received signal strength and the UBX160's transmit gain is not perfectly linear. 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.

[8] see also the comment on transmission power in subsection 3.1



(a) Gain vs. received signal strength. The measurements were conducted with three different attenuations to be able to cover the full clipping-free dynamic range of the GRX1090.



(b) Scatter plot of the single measurement values for the offset between the gain and the received signal strength. The limitation of the GRX1090's 12 bit ADC resolution becomes visible for signals weaker than 80 dBm (gain of less than 20 dB).

Figure 8: Results of our setup calibration measurements. We compared the received signal strength to the gain, whereas gain is a combination of the UBX160's variable transmit hardware gain and the attenuation added to the output connector of the USRP.

Attenuator inaccuracies: Figure 8a 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.

Dynamic range: The outer regions of Figure 8a 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.

Limited ADC resolution: 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 8b 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. Moreover, the discrete levels become more visible for small gains as the ratio between the step width of the discrete values and signal level become smaller. Note that this effect also holds for the transmitter's DAC. However, since we used analog gain to vary the transmit power, the signals generated by the DAC were always at maximum power such that this effect is minimized for the transmitter.

We conclude that the setup generally behaves as expected with slight inaccuracies on the transmitter side. We consider these inaccuracies negligible since only the calibrated received signal strength counts. We note, however, that an analog PSK receiver implementation might have a better performance when dealing with very weak signals due to the ADC resolution limitation.

3.3.2 Noise-free Channel

The second series of measurements was conducted with a noise-free channel model, i.e., without adding interferences. We varied the gain over the full clipping-free dynamic range of the GRX1090 and repeated the measurements for each M. Our main performance metric was the bit error rate in terms of percentage of erroneously decoded bits per transmission.

The results are shown in Figure 9. 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. 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 can conclude that with 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 analog PSK detector is recommended. However, we argue that for

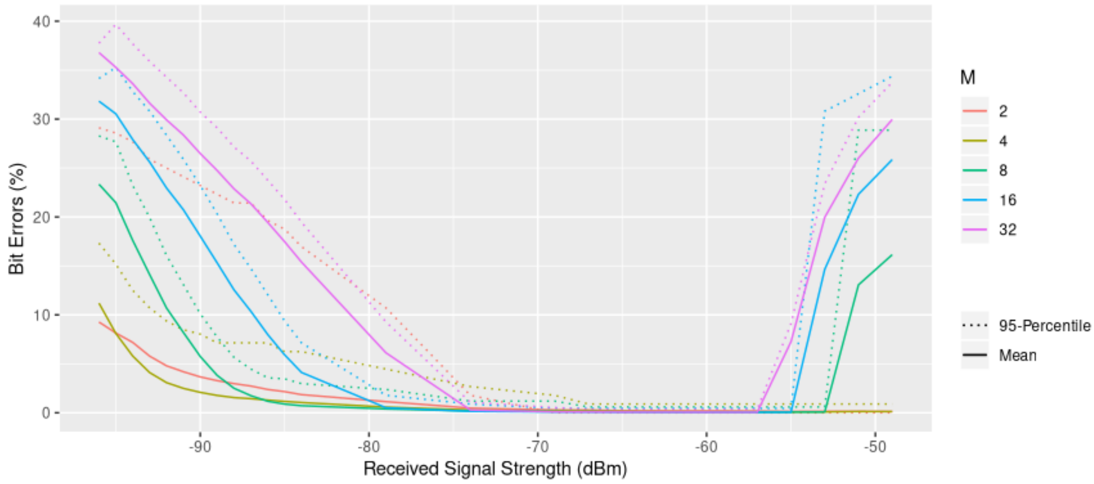


Figure 9: Phase overlay performance in a noise-free environment. Note that the bad 95-percentile for 2PSK is likely a result of the receiver's ADC resolution limitation.

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 the more bit errors need to be corrected due to a higher required code redundancy.

3.3.3 Noisy Channel

In this third series of measurements, the phase overlay performance under realistic radio channel conditions was evaluated. Therefore, SeRo Systems provided a continuous $10\,\mathrm{s}$ I/Q recording received from another GRX1090 deployed $2\,\mathrm{km}$ from FRA. 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. More precisely, about 200 aircraft were tracked by the receiver at the time of recording and interference from other technologies such as DME were also captured (see Figure 7). The recording was repeated for two minutes during each experiment.

The results of this experiment are shown in Figure 10. We also compared the phase overlay performance in the noise environment to the results of the noise-free measurements in Figure 11. As before, weaker signals are more susceptible to bit errors due to interference from other transmissions. However, as Figure 11a shows, the bit error rate is only slightly higher for very low signal strengths. This indicates, that the major factor causing these signal errors in weak signals is the limitation due to the resolution of the GRX1090's ADC. The difference becomes larger as the signals become stronger, meaning that the impact of the new factor (i.e., interferences) becomes higher than that of the resolution.

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 $56\,\mathrm{dBm}$, which is common for transponders used by airliners.

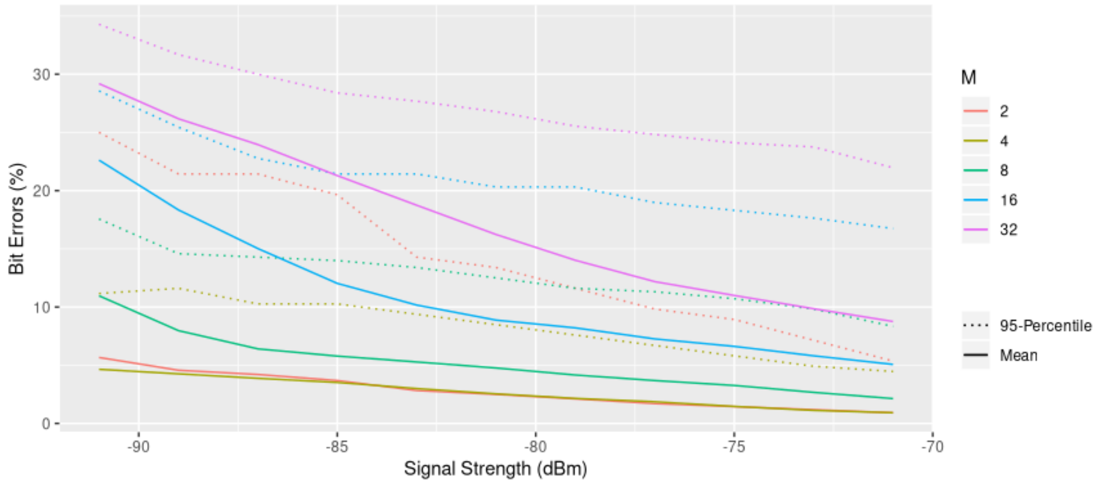


Figure 10: Bit error rate of different phase overlay configurations in a noisy environment.

The results are shown in Figure 11b. This analysis shows that for $M < 16$, the average bit error rate stays below 10% up to 250 NM for aircraft transmitting at 56 dBm. Note that this analysis is simplified since it ignores factors such as antenna gains and cable losses at the receiver.

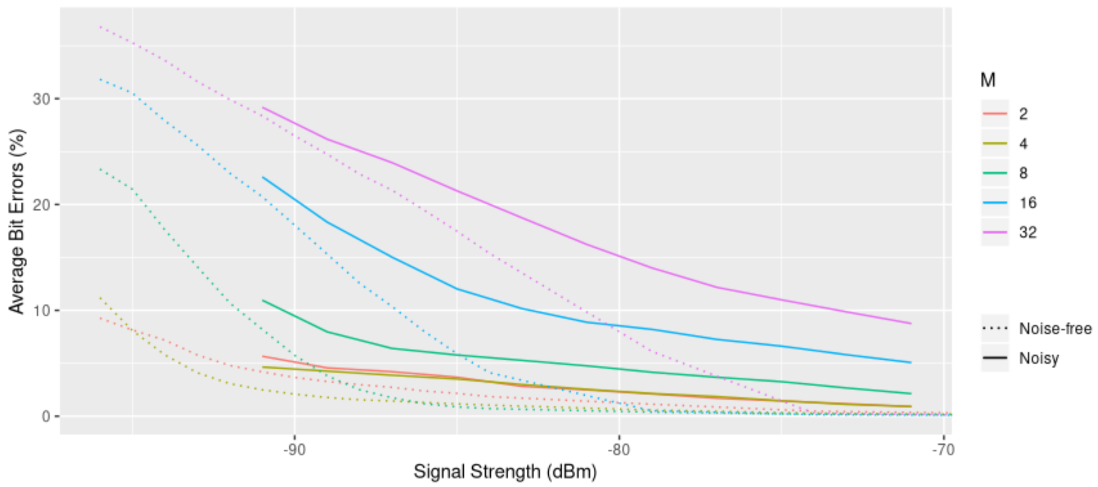
Based on these results, we finally estimate the capacity of the phase overlay within a noisy environment. We therefore assume that Reed-Solomon (RS) codes are used for FEC as proposed in [13]. RS codes require approximately twice the number of bits overhead that the code is able to correct. We now assume 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 11b, 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.

The results of this analysis are shown in Figure 12. We can conclude that under the above assumptions, a phase overlay with $M = 8$ performs best providing an additional capacity of 218 bit per transmission with a 95% chance of successful PSK decoding within a range of 250 NM.

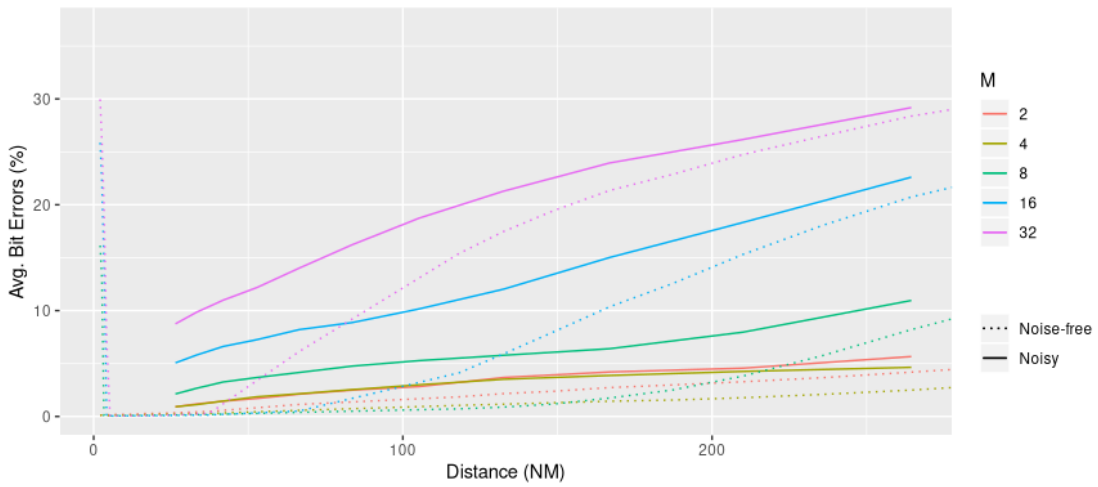
3.3.4 Carrier Frequency Offset

Our final series of measurements aimed at testing the impact of carrier frequency offsets on the phase overlay performance. Therefore, 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 separate the effect of the phase drift from the effect of noise.

The results are shown in Figure 13. As expected, the bit error rate has a symmetric behavior as the drift rate is the factor determining the bit errors and the sign of the offset only



(a) Bit error rate's dependency on the signal level.



(b) Average bit error rate over distance between transmitter and receiver. We assumed a transmission power of $56\,\text{dBm}$ and used the free-space path loss model to map received signal strengths to distances.

Figure 11: Comparison of different phase overlay configuration's bit error rates in a noisy and noise-free environment.

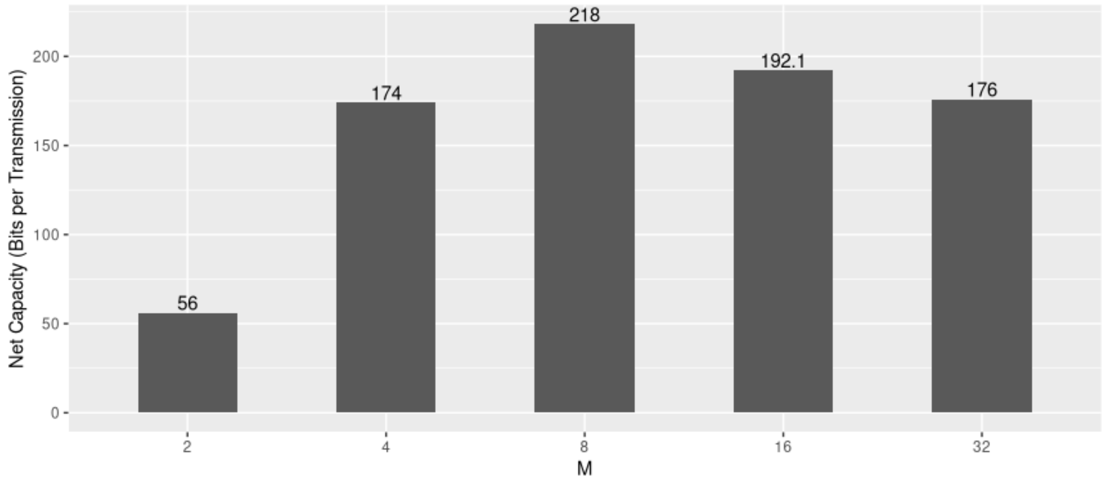


Figure 12: Net capacity of phase overlays in a noisy environment.

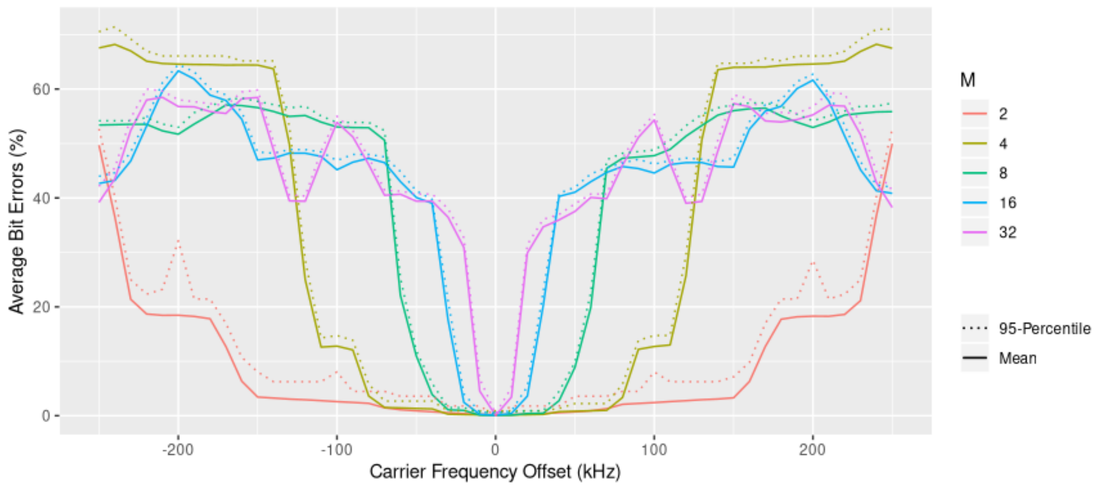


Figure 13: Bit error rate for different carrier frequency offsets and different M.

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 $M = 8$ has a frequency offset tolerance of about 40 kHz which is in line with the 42 kHz mentioned as a carrier frequency offset limit in [11].

4 Conclusion

We can conclude our measurements indicate that $M = 8$ is indeed the best choice. Our differential 8PSK coding was able to provide an additional net capacity of 218 bit for each transmission and ranges up to 250 NM. Moreover, our measurements revealed some limitations and requirements for receiver designs. For example, if a receiver with quadrature demodulation is used, the resolution of the ADC needs to be high enough to provide the respective dynamic range. While these results are only exemplary and different assumptions might be used in the actual implementation of the overlay, we believe that they demonstrate the feasibility and potential of the phase overlay under realistic conditions.

4.1 Next Planned Steps

The primary focus of this work was to gain insights on the capacity provided by the phase overlay in realistic radio environments. However, several other aspects need to be evaluated to guarantee a seamless integration of the phase overlay with existing surveillance infrastructure. First, by varying the phase of the ADS-B signal, its spectrum footprint changes. Hence, we will test its compliance with current regulations such as [3] next. A special focus will be on the amplitude and spectrum behavior of transmissions where phase reversals happen during long pulses (a 0-1 transition in the pulse-position modulation). Finally, we will evaluate the phase overlay performance in a real-world experiment using airborne transmitters. Only such an experiment can include all factors such as radio environment and antenna and setup characteristics.

References

[1] Minimum aviation system performance standards for Automatic Dependent Surveillance – Broadcast (ADS-B). Technical Report DO-242A (including Change 1), RTCA, Inc., December 2006.

[2] Minimum operational performance standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance – Broadcast. Technical Report DO-282B, RTCA, Inc, December 2011.

[3] International Civil Aviation Organization (ICAO). *International Standards and Recommended Practices, Annex 10: Aeronautical Telecommunications*, 4 edition, 2007. Volume IV: Surveillance and Collision Avoidance Systems.

[4] Minimum operational performance standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B). Technical Report DO-260B (with Corrigendum 1), RTCA, Inc., December 2011.

[5] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2), mar 1983.

[6] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Communications Surveys Tutorials*, 17(2), October 2015.

[7] Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders, and Ivan Martinovic. On Perception and Reality in Wireless Air Traffic Communication Security. *IEEE Transactions on Intelligent Transportation Systems*, 18(6), 2016.

[8] Martin Strohmeier. *Security in Next Generation Air Traffic Communication Networks*. PhD thesis, University of Oxford, 2016.

[9] Donald McCallie, Jonathan Butts, and Robert Mills. Security analysis of the ADS-B implementation in the next generation air transportation system. *International Journal of Critical Infrastructure Protection*, 4, 2011.

[10] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. Experimental Analysis of Attacks on Next Generation Air Traffic Communication. In *Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS)*. Springer Berlin Heidelberg, 2013.

[11] Greg Stayton and Thomas Pagano. Phase modulation technique receiver requirements and proposed data structure. Technical report, International Civil Aviation Organization (ICAO), October 2013.

[12] D09 - ADS-B Capacity - Phase Overlay Report. Technical report, SESAR Joint Undertaking, 2016. Work Package 15.04.06.

[13] D13 - ADS-B Capacity - Demonstration Report. Technical report, SESAR Joint Undertaking, 2016. Work Package 15.04.06.

[14] Omar Yeste-Ojeda and René Landry. ADS-B Authentication Compliant with Mode-S Extended Squitter Using PSK Modulation. In *18th IEEE International Conference on Intelligent Transportation Systems*, 2015.

[15] Anh-Quang Nguyen, Abdu Amrhar, Joe Zambrano, Georges Brown, Omar A. Yeste-Ojeda, and René Jr Landry. Application of PSK Modulation in ADS-B 1090 Extended Squitter Authentication. *International Journal of Aerospace and Mechanical Engineering*, 2018.

[16] Anh-Quang Nguyen, Abdu Amrhar, Joe Zambrano, Georges Brown, Omar A. Yeste-Ojeda, and René Jr Landry. Application of PSK Modulation for Secure ADS-B Avionics. *AIAA Aviation Forum*, 2018.