Impact of Pilot Jamming Attacks on Digital Aeronautical Data Communications

Daniel M. Mielke*, Thomas Gräupl†, and Ayten Gürbüz‡
Institute of Communications and Navigation,
German Aerospace Center DLR e. V.
Wessling, Germany
Email: *daniel.mielke@dlr.de, †thomas.graeupl@dlr.de, and ‡ayten.guerbuez@dlr.de

***Abstract*—Digitization of wireless communications has reached aviation, requiring reliable high-throughput wireless data links. However, wireless communication systems can be attacked with jamming, threatening digital aviation. Fortunately, jamming attacks are, in practice, limited by the radio hardware and energy available to the attacker. It is therefore important for an attacker to use its energy budget efficiently to perform a practical attack.**

In this paper we discuss the efficiency, impact, and mitigation of jamming attacks on modern OFDM-based aeronautical communication systems. Orthogonal Frequency Division Multiplex (OFDM) uses pilot symbols to estimate the channel's frequency response which is the base of the channel equalization process. Bad channel estimation degrades the performance of the channel equalization, resulting in serious distortions of the received data frame. This makes pilot symbols an attractive target for attackers. For our analysis, we define multiple jamming strategies and analyze their performance with respect to several assumptions on the jammer's synchronization capabilities. We show that targeted jamming attacks on pilot symbols can outperform classic jamming attacks, like broadband continuous wave jamming, not only in terms of the degradation of the system performance, but also in terms of the jamming efficiency. Finally, we discuss possible countermeasures against these types of attacks.

I. Introduction

The number of manned and unmanned aircraft in operation increases rapidly and congestion in the air space is expected to saturatate legacy air-ground communication in high-density areas. This situation endangers the reliabiltiy of data links exchanging information related to safety and regularity of flight.

The air-ground communication infrastructure must therefore be modernized to ensure the sustainable growth and safety of the air transportation system. For crewed aircraft, legacy analog VHF voice communication is going to be replaced with modern digital systems like the L-Band Digital Aeronautical Communication System (LDACS) [1], AeroMACS [2], and satellite communication. The C-Band Digital Aeronautical Communication System (CDACS) has been introduced as a potential command control data link for unmanned aircraft. Technically these systems share many similarities e.g. many features of CDACS have been derived from LDACS, AeroMACS, and comparable systems.

In the particular case of aeronautical command and control data links the absence of a crew in unmanned aircraft makes it crucial to establish a reliable and secure data connection between the remote pilots and the aircraft. AeroMACS, LDACS and CDACS employ OFDM due to its bandwidth efficiency, high data rates, and robustness in multi-path environments. However, OFDM is also vulnerable where wireless communication is subject to adversarial interference [3]. In OFDM systems, pilot symbols are distributed within a data frame to estimate the channel frequency response as a base for the channel equalization process. In case these pilot symbols are interfered, the channel estimation process is degraded and – consequently – the channel equalization is likely to perform poorly. This can even lead to the situation in which the channel equalization adds more distortions to the data frame than the actual channel did during transmission. A jammer can exploit this circumstance to increase the efficiency of its attack: An efficient jamming strategy aims to achieve a certain Frame Error Rate (FER) by expending the lowest possible jamming signal energy. Since jamming only the pilot symbols of a signal requires less energy than traditional jamming methods like wideband barrage jamming [4], while still having a severe effect on the communication system [5], pilot symbols are attractive targets to jammers.

The sensitivity of OFDM systems towards channel estimation errors and different strategies to attack pilot symbols have been studied in [5], [6], [7], [8]; however, aeronautical communication systems have not been investigated yet.

The objective of this paper is to quantify the impact of targeted jamming attacks on pilot symbols in OFDM-based wireless systems in aviation, using the example of CDACS, while taking different assumptions on the jammer's synchronization capabilities into account.

The paper is structured as follows: We introduce the reader to our system model in Section II and the simulation framework in Section III. The different jammers and jamming strategies we investigate are described in Section IV. We present and discuss our results in Section V and Section VI, respectively. The paper is concluded with a conclusion and outlook in Section VII.

II. System Model

In the following, we assume that $\boldsymbol{s}_{\{\mathrm{D,J}\}} \in \mathbb{C}^K$ denotes the discrete baseband time-domain representation of the desired signal and the jamming signal, respectively. We furthermore use the indices Tx and Rx to indicate if a signal vector, power, etc. represents a transmitted or a received signal, power, etc.

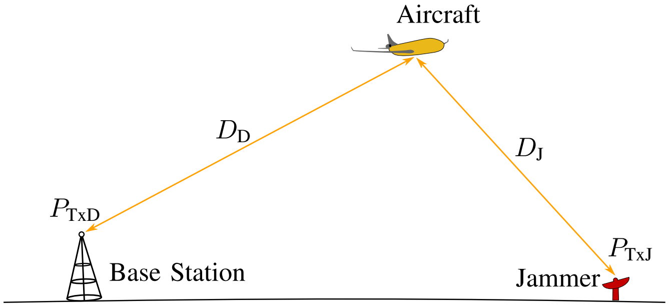

Fig. 1: Geometric setup: D_D denotes the distance between the base station (emitting the desired signal with power P_TxD), to the aircraft. D_J denotes the distance between the jammer (emitting the jamming signal with power P_TxJ), to the aircraft.

A. Geometry

The basic geometry that is assumed for this paper is sketched in Fig. 1. In our scenario, where only the Forward Link (FL) i.e. ground-to-air transmission, is subject to jamming attacks, we focus on the following three parties:

- The base station that emits the so called desired signal with a transmission power of P_TxD,
- the jammer that emits a jamming signal with a transmission power of P_TxJ, and
- the aircraft that aims to receive and process the desired signal from the base station, however, it also receives the jamming signal. We understand the aircraft as the victim of the jamming attack.

The distance between the base station and the aircraft is denoted by D_D, the distance between the jammer and the aircraft is denoted by D_J. As the Free Space Path Loss (FSPL) is the main contributor to the signal losses, these distances have a direct impact on the receiving power of the signals at the aircraft, P_RxD and P_RxJ, respectively.

We scale our model such that it represents a typical en-route scenario: In our simulations, we assume fixed values for the geometry and set $D_\mathrm{D} = 80\,\mathrm{km}$ and $D_\mathrm{J} = 10\,\mathrm{km}$. The transmitters' Equivalent Isotropically Radiated Powers (EIRPs) are set to $P_\mathrm{TxD} = 46\,\mathrm{dBm}$ and $P_\mathrm{TxJ} = 25\,\mathrm{dBm}$, respectively. We chose a carrier frequency of $f_c = 5.06\,\mathrm{GHz}$, as this is the center frequency of the Microwave Landing System (MLS) band, a band discussed for the deployment of a Command and Control (C2) link for Unmanned Aircraft (UA) like CDACS.

In our simulations, we perform the power scaling of the involved baseband signals according to the methods described in Appendix A.

B. Channel Model

In contrast to our recent study in [9], where a simple Additive White Gaussian Noise (AWGN) channel was assumed, we apply a more advanced channel model in this paper. Our decision is motivated by the fact that this paper specifically discusses attacks on the channel estimation process. The wireless air-ground/ground-air channel is known to highly depend on the current flight scenario of the air vehicle [10].

TABLE I: Parameters of an CDACS OFDM frame

Parameter	Value
Sub-carrier Spacing	24.41 kHz
FFT Length	64
Cyclic Prefix Length	11.52 µs
OFDM Symbols per Frame	14
Pilot Dist. Time	209.92 µs
Pilot Dist. Frequency	73.24 kHz
Frame Length	734.72 µs
Modulation Scheme	Quadrature Phase Shift Keying
Forward Error Correction	Interl. Convolutional Code, $R = 1/3$

In the remainder of this paper, we focus on the en-route scenario and use the corresponding model proposed in [11]. The channel model is implemented such that it generates one impulse response per OFDM symbol.

As the channel between the transmitter of the desired signal and the aircraft *D-channel* and the channel between the jammer and the aircraft *J-channel* are different, we use two independent instances of the channel model as it is sketched in Fig. 2. The model states of both channel model instances are updated after the transmission of an OFDM frame according to the given statistics.

C. Waveform

Throughout this paper, we use an OFDM based communication system based on the C-Band Digital Aeronautical Communication System (CDACS) described in [11], [12]. CDACS is designed as a C2 link for UA and is based on LDACS. However, our model also applies to OFDM-based aeronautical communication systems in general. While our previous study in [9] focused on a special type of OFDM frame – the Cell Entry Request (CER) – we now consider regular data frames. The parameters of such an OFDM frame as used for the simulations are summarized in Table I.

An OFDM frame in frequency domain is represented by a matrix $\boldsymbol{X} \in \mathbb{C}^{N_\mathrm{FFT} \times M}$, where N_FFT denotes the length of the Inverse Fast Fourier Transform (IFFT) and M denotes the amount of OFDM symbols of the frame. The elements $X^{(n,l)}$ of $\boldsymbol{X}$ are the symbols of the OFDM frame in frequency domain, where n denotes the symbol's index along the frequency axis (sub-carrier index) and l denotes the symbol's index along the time axis (number of OFDM symbol). The frame is transformed into the time domain by applying an IFFT along its columns. After adding the Cyclic Prefix (CP) of length N_CP at the beginning of each OFDM symbol, the time domain signal vector $\boldsymbol{s}_\mathrm{TxD} \in \mathbb{C}^{(N_\mathrm{FFT}+N_\mathrm{CP})M}$ is generated by concatenating the columns of the expanded matrix.

In this paper, we assume perfect signal synchronization with respect to time and frequency in the receiver. No measures for the reduction of the Peak to Average Power Ratio (PAPR) are applied to the OFDM signal.

D. Channel Estimation and Equalization

As in many other OFDM-based communication systems, pilot symbols are used to estimate the communication channel in order to allow a channel equalization in the receiver before a data frame is demodulated. Pilot symbols do not transmit any information and in a public standard, as they are common in aviation, both their position in the OFDM frame and their actual value are publicly known – including the desired receiver. By comparing the received pilots with the expected pilots, the receiver learns about the distortions the signal has received during transmission.

The channel estimation is performed in frequency domain. The pilot symbols $X_P^{(n,l)}$ are equidistantly distributed over the OFDM frame resulting in a grid structure; the pilot distances are given in Table I. The estimate of the channel coefficient at position (n,l) is determined according to

$$\hat{H}^{(n,l)} = \frac{X_{P,\text{Rx}}^{(n,l)}}{X_{P,\text{Tx}}^{(n,l)}}. \tag{1}$$

The remaining estimates are computed by a two-step linear interpolation: As suggested in [13], we first interpolate the channel coefficients along the time axis of the OFDM frame and then perform the interpolation along the frequency axis in a second step. Once all estimates of the channel coefficients are available, the actual channel equalization is performed according to

$$\hat{X}^{(n,l)} = \frac{X_{\text{Rx}}^{(n,l)}}{\hat{H}^{(n,l)}}. \tag{2}$$

The Mean Squared Error (MSE) between the estimated channel coefficients $\hat{\boldsymbol{H}}$ and the actual channel coefficients $\boldsymbol{H}$ can be used as a simple performance measure of the channel estimation process.

E. Protocol Structure

For data transmission we use a stop-and-go Automatic Repeat Request (ARQ) protocol synchronized to multi-frames of 8 OFDM frames duration. In each multi-frame the ARQ protocol will only either send or receive a data or acknowledgement frame, but not send and receive at the same time. It is further assumed that the frame processing time is not zero i.e. the protocol cannot respond to a received frame immediately. In the best case the protocol can thus respond after one multi-frame. The duration of a multi-frame is $7.137\,\text{ms}$, with a data capacity of $573\,\text{Byte}$.

Each time the ARQ protocol sends a data frame, it starts a retransmission timer T_ret set to $T_\text{ret} = 4$ multi-frames. This is the minimum value for the retransmission timer, equivalent to one ARQ cycle of transmission and acknowledgement assuming a multi-frame of processing time for each protocol frame. The expiration time T_Exp has been set to $T_\text{Exp} = 57.6\,\text{s}$. After this time, the protocol will no longer attempt to retransmit an unacknowledged data frame, but discard it. Data frames that have expired in the transmission queue of the protocol are also discarded.

Data traffic has been modeled with 10 data frames per second on average. The time between the data frames is exponentially distributed. The size of the data frames is set to exactly one OFDM frame. It is assumed that acknowledgement frames do not experience jamming on the Reverse Link (RL) and are always received without errors. Upon generation each data frame is put into the transmission queue of the ARQ protocol and sent when all previous data frames have been acknowledged or discarded. There is one instance of the ARQ protocol for each pair of aircraft and ground-stations.

This model captures the best case scenario in terms of robustness. Any other configuration utilizing larger data frames and more efficient ARQ variants is less robust against increased transmission time due to frame loss.

We define the time span between the first transmission of a data frame and the time of the first successful reception of this data frame as the transmission time T_suc. We define the logarithmic ratio between the transmission time resulting from jamming conditions $T_\text{suc}^\text{(Jam)}$ and the corresponding transmission time under jamming-free conditions $T_\text{suc}^\text{(noJam)}$ as

$$T_\text{suc}\big|_\text{dB} = 10\log_{10}\left\{\frac{T_\text{suc}^\text{(Jam)}}{T_\text{suc}^\text{(noJam)}}\right\}. \tag{3}$$

III. Simulation Framework

The simulations are performed in two steps: First, the effect of the proposed jamming strategies on the physical layer are simulated. In a second step, the resulting consequences on the protocol layer are investigated.

A. Physical Layer

The structure of the simulation framework's implementation is given in Fig. 2: The signal that is fed into the OFDM receiver (located in the aircraft) corresponds to a superimposition of the received desired signal $\boldsymbol{s}_\text{RxD}$, the received jamming signal $\boldsymbol{s}_\text{RxJ}$, and White Gaussian Noise (WGN) represented by $\boldsymbol{n}$. The mean power of the noise is computed according to $P_\text{wgn} = k_\text{B} T B_\text{chan}$, where k_B denotes the Boltzmann constant, T denotes the temperature of the receiver given in K, and B_chan denotes the channel bandwidth that is assumed to equal the receiver bandwidth.

The signals require scaling that is performed according to their computed powers at the receiver P_RxD, P_RxJ, and P_wgn using the approach given in Appendix A.

The baseband representation of the received desired signal $\boldsymbol{s}_\text{RxD}$ corresponds to the noise-free transmission of the transmitted desired signal $\boldsymbol{s}_\text{TxD}$ over the channel between the desired transmitter (base station) and the aircraft (denoted by D-Channel). The baseband representation of the received jamming signal $\boldsymbol{s}_\text{RxJ}$, however, corresponds to the noise-free transmission of the transmitted jamming signal $\boldsymbol{s}_\text{TxJ}$ over the channel between the jammer and the aircraft (denoted by J-Channel), shifted by a time offset τ_Δ and a frequency offset ν_Δ. The tuple $(\tau_\Delta, \nu_\Delta)$ is used to model the synchronization error of the jammer with respect to the desired signal in the receiver. The actual offsets depend on how precise the jammer is able to estimate the victim's location, speed, and heading. We assume the jammer is able to retrieve this information up to some level of precision, e. g. based on a tracking of

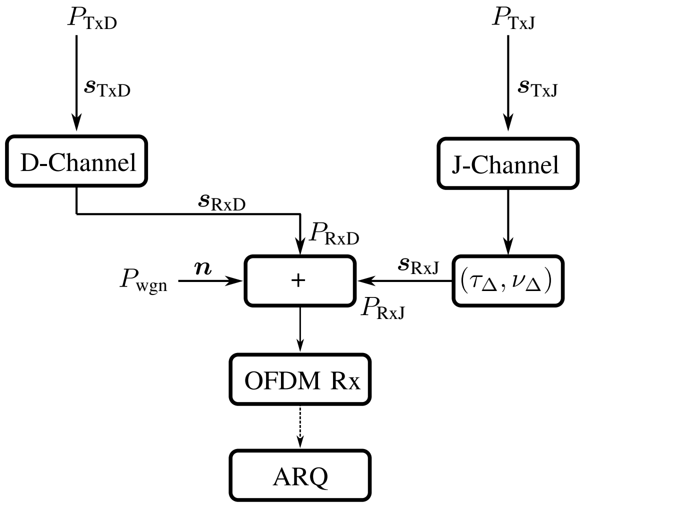

Fig. 2: Block diagram of the simulation model: $P_{\text{Tx},\{\text{D,J}\}}$ denotes the transmission power of the desired signal and the jamming signal, respectively. $P_{\text{Rx},\{\text{D,J}\}}$ denotes the received power of the desired signal and the jamming signal, respectively. P_{wgn} denotes the noise power of the noise signal $\boldsymbol{n}$. {D,J}-Channel represents the channel model used for the desired signal and the jamming signal, respectively. The tuple $(\tau_\Delta, \nu_\Delta)$ denotes the offset in time and frequency of the jamming signal w. r. t. the desired signal. The Automatic Repeat Request (ARQ) box below the OFDM receiver symbolizes the effect on the underlying protocol.

ADS-B messages or radar. The position of the other two parties involved – the base station and the jammer itself – are assumed to be known to the jammer without any significant error.

In our simulations, we assume multiple Synchronization Precision Levels (SPLs), where level *A* represents the (unrealistic) case of perfect synchronization, hence $(\tau_\Delta, \nu_\Delta) = (0, 0)$. Table II shows the definition of all SPLs used throughout this paper[1].

B. Protocol Layer

After the simulation of OFDM, the estimated FER is applied to determine the ARQ data transmission time using the Framework for Aeronautical Communications and Traffic Simulations 2 (FACTS2) [14]. Each configuration is simulated for $500\,\text{s}$. Only a single transmitting aircraft is assumed per simulation, thus no contention can appear on the data channel.

IV. Jamming Strategies

As a measure to compare the efficiency of different jamming strategies, we define the jamming efficiency η similar to [9]. First we define the jamming efficiency with respect to the FER:

TABLE II: Synchronization Precision Levels (SPLs)

Level	Time Offset $\tau_\Delta\,[\mu\text{s}]$	Frequency Offset $\nu_\Delta\,[\text{Hz}]$
A	0	0
B	$\mathcal{N}(0, 8^2)$	$\mathcal{N}(0, 300^2)$
C	$\mathcal{N}(0, 8^2)$	$\mathcal{N}(0, 500^2)$
D	$\mathcal{N}(0, 8^2)$	$\mathcal{N}(0, 1000^2)$
E	$\mathcal{N}(0, 8^2)$	$\mathcal{N}(0, 2000^2)$
F	$\mathcal{N}(0, 16^2)$	$\mathcal{N}(0, 300^2)$
G	$\mathcal{N}(0, 16^2)$	$\mathcal{N}(0, 500^2)$
H	$\mathcal{N}(0, 16^2)$	$\mathcal{N}(0, 1000^2)$
I	$\mathcal{N}(0, 16^2)$	$\mathcal{N}(0, 2000^2)$
J	$\mathcal{N}(0, 32^2)$	$\mathcal{N}(0, 300^2)$
K	$\mathcal{N}(0, 32^2)$	$\mathcal{N}(0, 500^2)$
L	$\mathcal{N}(0, 32^2)$	$\mathcal{N}(0, 1000^2)$
M	$\mathcal{N}(0, 32^2)$	$\mathcal{N}(0, 2000^2)$

$$\eta_{\text{FER}} = \frac{\text{FER}}{E^{(\text{SF})}_{\text{JamTx}}}, \tag{4}$$

where $E^{(\text{SF})}_{\text{JamTx}}$ denotes the average energy per super frame emitted by the jammer during its attack on an OFDM frame of the desired signal.

To investigate the effect of the jamming attacks on the underlying protocol, we also define

$$\eta_{95\%} = \frac{T^{(95\%)}_{\text{suc}}}{E^{(\text{SF})}_{\text{JamTx}}}, \tag{5}$$

where $T^{(95\%)}_{\text{suc}}$ denotes the $95\,\%$ percentile of the transmission time T_{suc}.

In the following, we assume a fixed geometric setup as described in Section II-A, thus the transmit powers and the path distances do not change with time. We furthermore assume the exact same setup (same jamming power, same path distances etc.) for all jamming strategies we investigate to allow a fair comparison.

We compare the different strategies not only with respect to the resulting impact on the communication system and their efficiency, but also with different assumptions on the quality of the time and frequency synchronization of the jamming signal with respect to the desired signal represented by the SPLs as defined in Table II.

A. Continouous Wave Jammers

A Continouous Wave (CW) jammer continuously emits a noise signal with a certain bandwidth. The continuous transmission makes the CW jammer impervious to an imprecise timing synchronization (i. e. large values for τ_Δ) for obvious reasons. However, it is sensitive to frequency offsets, as the jammer is limited in its bandwidth and its power. The larger the bandwidth of the CW signal is, the lower is the power density for a specific frequency, as we assume the overall power to be constant. On the other hand, a larger bandwidth makes the CW jammer less sensitive to an imprecise frequency

[1] Please note that the actual offset distributions depend on the geometry. The authors have chosen the special case of a normal distribution for the sake of simplicity.

synchronization. Nevertheless it is very unlikely for the given scenario and the assumed SPLs that the CW jammer completely "misses" the desired signal in frequency domain. We define the jamming strategies *cw-bw080*, *cw-bw100*, and *cw-bw120*, having a bandwidth of $80\,\%$, $100\,\%$, and $120\,\%$ of the Fast Fourier Transform (FFT) bandwidth of the OFDM signal, respectively. The signal of the CW jammer is modeled by (band-limited) white Gaussian noise.

B. Pulsed Jammers

Since the pilots of the given OFDM system are arranged in a grid structure, the OFDM symbols containing pilot symbols in the time domain transmission signal appear in periodical pulses. The pulsed jammer tries to emit its pulses of band-limited white Gaussian noise such that they arrive at the receiving victim at the same time as the pilot-symbol containing OFDM symbols of the desired signal. Consequently, the pulsed jammer is more sensitive to an erroneous time synchronization than the CW jammer.

As for the CW jammers, we investigate different bandwidths for the pulsed jammers and name these jamming strategies *pulsed-bw080*, *pulsed-bw100*, and *pulsed-bw120*, again having a bandwidth of $80\,\%$, $100\,\%$, and $120\,\%$ of the FFT bandwidth of the OFDM signal, respectively.

C. OFDM Pilot Jammers

A frame of an OFDM pilot jammer has basically the same design as the frame of the signal under attack (i. e. desired signal). However, the pilot symbols are the only symbols in the frame the jammer assigns power to. As no power is assigned to the symbols on other sub-carriers, more power is available to "boost" these jamming pilot symbols. However, the pilot jammer is sensitive to erroneous time and frequency synchronization.

We assume a fixed amplitude with a uniformly distributed random phase for the jamming pilot symbol. Consequently, we do not consider pilot nulling attacks as they are discussed in [5] since we see them as not applicable to real-world aeronautical scenarios.

We distinguish between jamming strategies where all pilot symbols of the OFDM frame are attacked (*pilots-full*) and those where just a randomly chosen subset ($25\,\%$, $50\,\%$, and $75\,\%$) of the pilots are attacked. We denote this latter group of jamming strategies by *pilots-rand25*, *pilots-rand50*, and *pilots-rand75*, respectively.

V. Results

The results generated by the simulation frameworks described in Section III are presented in Tables III to VI. The tables show different measures, however, they all have the same structure: The investigated measure for jamming strategy number x under the assumption of SPL number y is given in row x and column y. All tables use color coded cell-backgrounds to provide guidance to the reader: blue color denotes low values (less dangerous), red color denotes high values (more dangerous). As all tables contain different measures, the scaling of the color coding is done table-wise.

The number of OFDM frames simulated per jamming strategy and SPL is 8000. The ARQ protocol has been simulated for $500\,\mathrm{s}$ in each scenario. In case of the jamming-free scenario, we have observed a FER below $0.01\,\%$ and $T_{\mathrm{suc}}^{(95\%)} = 30\,\mathrm{ms}$.

A. Frame Error Rate

The resulting Frame Error Rates (FERs) for the investigated jamming strategies and SPLs are presented in Table III. It is observed, that the FERs caused by all CW based jamming strategies do not vary significantly for the investigated SPLs. The same applies to the pulsed jammers. It is also observed, that none of the pulsed jammers can achieve an FER larger than $4.9\,\%$, which is a very low value compared to all other FERs.

The resulting FERs for the different pilot jammers, however, show a strong dependency on the SPL: The highest FERs are achieved for SPL A, thus the case of perfect synchronization. For the other SPLs, it can be observed that the results are roughly divided into three groups covering the SPLs from B to E, the SPLs from F to I, and the SPLs from J to M. The performance of the pilot jammers for SPL F to I is in a similar range than the performance of the CW jammers.

Comparing the amount of pilot symbols that are jammed by the respective pilot jamming strategy, it can be observed that the FER decreases with a decreasing amount of jammed pilot symbols for all SPLs: Where the *pilots-rand75* strategy achieves FERs that are just $4\,\%$ to $5\,\%$ (absolute percentage points) below the *pilots-full* strategy for all SPLs, the *pilots-rand25* strategy performs significantly worse as its resulting FERs are just roughly half of the *pilots-full* strategy's performance for all SPLs.

B. Efficiency w. r. t. Frame Error Rate

Table IV shows the jamming efficiency with respect to the FER η_{FER} as it is defined in (4). The overall table shows a pattern similar to Table III: The efficiency of the CW based jamming strategies appear to be independent of the SPL and the pulsed jammers show the lowest performance compared to all other jamming strategies. However, whereas the CW based jamming strategies' FERs are in a comparable range than the pilot jamming strategies' FERs for SPLs F to I, the CW based jamming strategies' η_{FER} are comparable to the pilot jamming strategies' performance for SPLs J to M, thus under worse synchronization conditions.

Comparing the pilot jamming strategies' performance along the different SPLs shows a similar behavior compared to the FER in Table III: Again, three groups can be defined and the *pilots-rand25* strategy performs significantly worse than the other pilot jamming strategies.

C. Transmission Time

The logarithmic transmission time $T_{\mathrm{suc}}^{(95\%)}\big|_{\mathrm{dB}}$ as defined in (3) is given in Table V. The applied reference value is the $95\,\%$ percentile of T_{suc} for the jamming free case: $T_{\mathrm{suc}}^{(95\%)} = 30\,\mathrm{ms}$. The logarithmic representation of the measure is motivated

TABLE III: Resulting Frame Error Rate (FER) for given jamming strategies and SPLs in $\%$.

	Synchronization Precision Level (SPL)												
Jamming Strategy	A	B	C	D	E	F	G	H	I	J	K	L	M
cw-bw080	52.4	52.7	53.2	52.9	53.0	53.5	53.3	51.5	52.7	52.6	53.1	53.0	52.5
cw-bw100	60.6	61.6	60.6	61.1	61.4	61.9	61.3	61.1	61.8	61.0	61.3	60.2	61.3
cw-bw120	46.8	47.0	47.8	47.8	45.1	46.8	47.3	47.3	48.1	45.9	46.8	47.4	46.9
pulsed-bw080	4.9	4.0	4.2	4.0	4.2	3.2	3.6	3.5	3.6	2.3	2.2	2.2	2.2
pulsed-bw100	5.3	4.4	4.4	4.8	4.5	3.9	4.0	3.3	3.6	2.3	2.3	2.4	2.5
pulsed-bw120	3.4	2.8	3.1	2.7	2.7	1.9	1.9	2.0	2.0	1.4	1.6	1.6	1.7
pilots-full	87.2	74.6	74.2	73.5	71.5	55.4	55.5	55.0	55.2	32.0	32.7	33.1	33.0
pilots-rand75	83.6	69.0	68.6	68.6	67.9	52.2	51.9	51.8	50.2	30.6	30.3	31.2	29.5
pilots-rand50	73.2	60.3	60.9	61.4	59.2	44.9	44.7	45.0	44.1	26.7	25.9	26.3	26.4
pilots-rand25	46.1	37.1	36.5	36.3	36.2	27.6	26.7	27.1	26.4	15.7	16.3	16.0	15.1

TABLE IV: Resulting jamming efficiency η_{FER} for given jamming strategies and SPLs in $\%/\text{mJ}$.

	Synchronization Precision Level (SPL)												
Jamming Strategy	A	B	C	D	E	F	G	H	I	J	K	L	M
cw-bw080	196.6	197.3	198.2	197.4	198.5	200.4	199.0	192.7	197.2	197.2	198.3	197.6	195.6
cw-bw100	216.9	220.2	216.3	218.2	219.8	220.7	219.0	218.8	220.9	218.1	219.1	215.3	219.2
cw-bw120	158.6	159.1	161.5	161.6	153.3	158.8	160.0	160.6	162.5	155.4	158.3	160.6	159.0
pulsed-bw080	53.4	43.7	45.5	44.4	46.3	35.2	39.1	38.7	39.3	24.7	24.2	23.5	24.2
pulsed-bw100	55.6	46.2	46.5	50.9	47.6	41.0	41.4	35.0	38.1	24.2	23.9	25.4	25.9
pulsed-bw120	33.4	28.4	30.5	27.1	27.1	18.8	18.7	20.2	20.3	13.8	15.9	16.4	16.5
pilots-full	813.4	694.8	691.7	683.9	669.8	517.0	519.0	513.3	514.3	298.9	304.3	309.3	307.9
pilots-rand75	786.7	651.1	646.3	647.3	639.1	492.5	488.5	485.5	475.4	289.1	285.1	293.6	277.7
pilots-rand50	704.1	577.3	584.5	588.6	566.9	431.4	431.5	432.5	421.8	256.0	248.6	252.6	253.2
pilots-rand25	450.9	362.3	357.2	356.1	353.8	269.6	262.2	265.7	258.2	154.0	159.3	156.2	147.0

by the super-exponential effect of an increasing FER on the protocol as described in Section II-E and thus on the transmission time.

The table, again, shows a similar pattern than the previous tables: The performance of the CW jamming strategies is more or less independent of the SPL and the pulsed jammers perform poorly compared to the other jamming strategies.

The performance of the pilot jamming strategies can be grouped as described above. However, the group from SPL B to E performs noticeable better compared to the other SPLs.

D. Efficiency w. r. t. Transmission Time

Table VI shows the jamming efficiency with respect to the $T_{\text{suc}}^{(95\%)}$ as it is defined in (5). The basic structure of the table looks similar to Table IV, however, the values given here, represented by $\eta_{95\%}$, show a much higher variance compared to the alternative efficiency measure η_{FER}.

E. Frame Error Rate vs. Efficiency

The scatter plot in Fig. 3 shows the FER versus the resulting logarithmic transmission time $T_{\text{suc}}^{(95\%)}\big|_{\text{dB}}$. The size and color of the data points indicate the jamming efficiency $\eta_{95\%}$; the applied color coding is the same that is used in Table VI. The horizontal red line indicates the protocol's timeout time of $57.6\,\text{s}$ corresponding to $32.8\,\text{dB}$ in logarithmic scale.

The plotted data points show a nearly linear[2] increase in the FER interval from $5\,\%$ to $65\,\%$. However, for even higher FERs, the curve shows rapid – probably exponential – growth up to a saturation level that is caused by ARQ retransmissions.

VI. Discussion

A. Continouous Wave Jammers

The performance of CW jamming strategies is independent of the investigated SPL. This finding is not surprising, since a CW jammer is robust against timing offsets by definition, and only vulnerable to frequency offsets. However, none of the defined SPLs achieved a frequency offset, that would cause a situation where the CW jamming signal misses the desired signal. Thus, all the CW jammers achieve comparatively high FERs between $41\,\%$ to $62\,\%$ causing relative transmission times of up to $12.8\,\text{dB}$. Comparing the bandwidths of the jammers shows that the *cw-bw100* jammer outperforms the other two CW jammers in all cases. We explain the poor performance of the *cw-bw120* jammer by the fact that it puts some of its power outside of the frequency band that is used by the desired signal. Since the simulated frequency offsets are not that large, this strategy results in a waste of

[2] The reader may keep in mind that the values on the y-axis are of logarithmic scale.

TABLE V: Resulting $T_{\mathrm{suc}}^{(95\%)}\big|_{\mathrm{dB}}$ for given jamming strategies and SPLs in dB; reference value is $T_{\mathrm{suc}}^{(95\%)} = 30\,\mathrm{ms}$.

	Synchronization Precision Level (SPL)												
Jamming Strategy	A	B	C	D	E	F	G	H	I	J	K	L	M
cw-bw080	9.7	10.0	10.1	9.9	10.0	10.0	10.0	9.6	9.9	9.9	10.1	10.0	9.7
cw-bw100	12.0	12.8	12.3	12.1	12.8	12.4	12.3	12.2	12.2	12.4	12.5	12.2	12.2
cw-bw120	8.6	8.8	9.0	9.0	8.5	8.6	8.8	8.7	8.9	8.5	8.6	8.8	8.8
pulsed-bw080	1.2	1.4	1.4	1.4	1.4	1.0	1.0	1.0	1.0	0.8	0.8	0.8	0.8
pulsed-bw100	1.5	1.2	1.2	1.2	1.2	1.1	1.2	1.0	1.0	0.8	0.8	0.8	1.0
pulsed-bw120	1.0	1.0	1.0	0.9	0.9	0.5	0.5	0.8	0.8	0.4	0.4	0.4	0.4
pilots-full	33.0	28.9	27.9	25.0	19.0	10.4	10.3	10.1	10.3	5.8	5.8	5.8	5.9
pilots-rand75	33.0	17.6	16.7	16.7	16.4	9.9	9.7	9.4	9.2	5.6	5.7	5.7	5.6
pilots-rand50	22.0	11.9	12.0	12.6	11.8	8.4	8.4	8.5	8.4	5.0	5.0	5.0	5.0
pilots-rand25	8.4	6.6	6.6	6.5	6.7	5.2	5.0	5.1	5.0	3.4	3.5	3.5	3.5

TABLE VI: Resulting jamming efficiency $\eta_{95\%}$ for given jamming strategies and SPLs in $\mathrm{s/mJ}$.

	Synchronization Precision Level (SPL)												
Jamming Strategy	A	B	C	D	E	F	G	H	I	J	K	L	M
cw-bw080	1054	1128	1152	1088	1117	1131	1132	1019	1108	1109	1154	1120	1048
cw-bw100	1701	2050	1822	1751	2028	1853	1831	1771	1775	1851	1915	1783	1763
cw-bw120	739	774	809	809	717	740	764	757	784	722	737	766	763
pulsed-bw080	439	450	449	451	449	418	418	417	417	396	395	394	396
pulsed-bw100	441	420	422	421	420	410	420	400	400	379	379	378	399
pulsed-bw120	379	380	380	370	368	341	340	359	360	330	330	330	330
pilots-full	563 724	216 963	171 427	88 124	22 438	3050	3030	2877	3020	1065	1061	1074	1093
pilots-rand75	566 628	16 184	13 174	13 193	12 311	2749	2637	2467	2376	1038	1055	1057	1037
pilots-rand50	45 650	4434	4597	5248	4297	2008	1989	2036	1998	911	902	911	911
pilots-rand25	2027	1351	1353	1305	1381	978	935	951	930	648	656	656	654

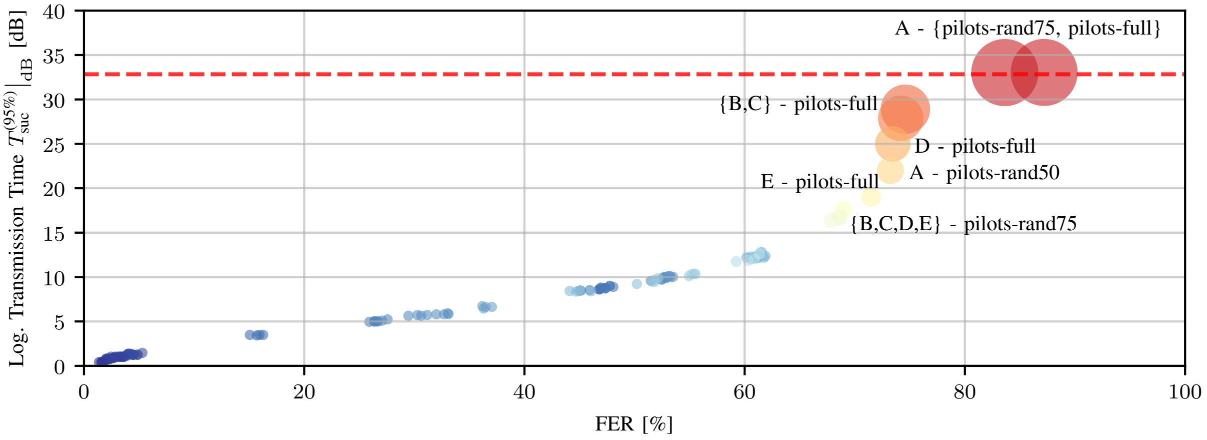

Fig. 3: Logarithmic transmission time $T_{\mathrm{suc}}^{(95\%)}\big|_{\mathrm{dB}}$ (with respect to $T_{\mathrm{suc}}^{(95\%)} = 30\,\mathrm{ms}$ in case of no jamming) vs. Frame Error Rate (FER). Size and color of a data point indicate the jamming efficiency $\eta_{95\%}$ as shown in Table VI. The horizontal red line indicates the expiration time of $57.6\,\mathrm{s}$. Jamming strategies that achieve a higher FER than $65\,\%$ for the given SPL are labeled.

jamming power. For situations with a higher frequency offset, however, this strategy is expected to be advantageous. The performance of the *cw-bw080* jammer can be explained by the robust modulation alphabet, the robust channel coding, and the applied interleaving. As only parts of the transmission band are jammed, it is ensured that parts of a transmitted data frame are not jammed and consequently are very unlikely to contain any errors. Apparently, this effect is not entirely compensated by the slightly higher band power of the jammer.

Once the jamming efficiency is taken into account, all CW jammers perform comparatively poor. This is caused by the CW jammers' approach to add damage to the entire OFDM frame and not to focus the damage just onto critical parts of the OFDM frame. The impact on the FER is considerable, however, a comparatively high amount of energy is required.

B. Pulsed Jammers

The performance of the pulsed jammers is quite poor: The achieved FERs are very low and perform worse than any other jamming strategy observed. As the pulsed jammer is nothing but an interrupted CW jammer, we state that the pulsed jammers' duty cycles[3] are just too low to have a significant impact on the attacked transmission.

Although the pulsed jammer emits less energy per frame than the CW jammer due to its lower duty cycle, its efficiency is even worse compared to the CW jammer. This is caused by the significantly lower impact on the overall system performance that is not compensated by the lower energy consumption.

We see the pulsed jamming strategy as an unattractive choice for the attacker considering the given scenarios. The pulses neither degrade the channel estimation in a considerable way, nor significantly damage the OFDM frame like the CW jammers do.

C. OFDM Pilot Jammers

All pilot jamming strategies outperform the other strategies up to SPL I in terms of the achieved FER. However, there are significant distinctions in performance comparing the different pilot jamming strategies: Apparently, the impact of the *pilots-full* and the *pilots-rand75* jamming strategies on the channel estimation are both severe, whereas the *pilots-rand25* jamming strategy's impact is considerably lower. Even in case of perfect synchronization, the *pilots-rand25* strategy does barely achieve similar FERs than the CW jamming strategies.

In case of bad synchronization, thus with a high probability of a significant time offset (SPLs J to M), the resulting FERs of all pilot jammers are lower than the FERs achieved by the CW jammer. We therefore assume that the jamming signal's pilot symbols miss the pilot symbols of the desired signal that often, that their impact on the channel estimation process is considerably lower than in the other scenarios. However, once the jamming efficiency is considered, all but the *pilots-rand25* strategy outperform the CW jammers.

From these results, we conclude that all but the *pilots-rand25* strategy are reasonable choices for a jamming attack on a system. Only in case of a bad synchronization with respect to time, the CW strategies are more potent as long as efficiency is not an issue.

D. Effects on Protocol

The simulation of the protocol shows the expected exponential degradation of ARQ under frame loss. Jammed data frames are not acknowledged and have to be retransmitted. This increases the latency of the affected data frame and the latency of all data frames waiting in the transmission queue. In extreme cases data frames expire and are discarded. This is indicated with the red dotted line in Fig. 3. At this line the transmission latency is capped by discarding the data frame.

E. Effect of Package Timeout

Since the protocol discards packages older than $57.6\,\mathrm{s}$ – a value whose $95\,\%$-percentile is achieved starting from a FER of roughly $78\,\%$ – it is not necessary for the jammer to aim for even higher FERs. Thus, once this threshold is achieved, the jammer does not need to improve its impact on the FER, e. g. by taking more effort to minimize the synchronization error or by increasing its jamming power. The jamming strategies *pilots-full* and *pilots-rand75* therefore do not need to achieve perfect synchronization (SPL A) to realize their maximum impact (c.f. Fig. 3).

F. Possible Countermeasures

In the previous section, we have seen that pilot jamming attacks (yellow and red data points in Fig. 3) outperform classic CW and pulsed jamming (most of the blue data points in Fig. 3) both in terms of resulting FER and efficiency (for SPLs B to E) or at least in terms of efficiency (for SPLs F to I). However, the fundamental prerequisite for this kind of attack is that the jammer is aware of the exact design of the OFDM frames it aims to attack. In case the position of the pilot symbols inside of a frame is unknown to the attacker, the jammer cannot drive a targeted attack on the channel estimation.

Thus, random frame scrambling – based on a shared secret known to both the transmitter and the receiver and *not* to the jammer – offers a countermeasure against pilot jamming attacks, since it forces the attacker to use the less efficient and less effective jamming attacks shown in blue in Fig. 3.

VII. Conclusion and Outlook

In this paper we have presented several jamming strategies on digital aeronautical communication systems based on an OFDM waveform. We have compared the impact of targeted jamming attacks on the channel estimation process to straight forward jamming strategies like CW jamming and investigated the attacks' impact on the overall system performance. All strategies were investigated for different assumptions regarding the synchronization precision of the jamming signal with respect to the signal under attack. We showed that targeted

[3] From Table I it follows that four out of 14 OFDM symbols contain pilots, thus the pulsed jammer is active for four OFDM symbols per OFDM frame, which results in a duty cycle of $\frac{4}{14} \approx 28\,\%$.

pilot jamming attacks can outperform pulsed and CW jammers in terms of the achieved FER and thus the resulting transmission time up to a synchronization with a noticeable error. Once the efficiency is taken into account, nearly all of the pilot jamming attacks outperform the CW jammers for all investigated synchronization errors.

Our study has raised several questions that are beyond the scope of this paper: For example it is of great interest how more sophisticated channel estimation/equalization methods, e. g. based on a Wiener filter, perform under the described attacks. Furthermore, it is interesting how a pilot jammer can react on bad synchronization conditions, e. g. by increasing the "footprint" of the jamming pilot symbols inside of its signal to increase the probability of an overlap with the pilot symbol in the attacked signal. On the other hand, it is of great interest on how a system can be hardened against the described attacks, e. g. by randomizing the frame design.

Appendix

A. Signal Power

We compute the power of sample k of the discrete signal $\boldsymbol{s}_x \in \mathbb{C}^K$ sampled at f_{SR} according to

$$P_x[k] = \mid \boldsymbol{s}_x[k] \mid^2, \quad \forall\ 0 < k < K-1. \tag{6}$$

The peak power of a signal $\boldsymbol{s}_x$ is therefore defined as

$$P_x^{(\text{peak})} = \max_{k \in \{0,\ldots K-1\}} \{\ P_x[k]\ \} \tag{7}$$

and its mean power is defined as

$$\overline{P_x} = \frac{1}{K} \sum_{k=0}^{K-1} P_x[k]. \tag{8}$$

However, the application of the mean power of a signal as defined above can be problematic for certain waveforms, e. g. a pulsed signal.

Therefore, to allow a fair comparison of signal powers, we first define a new measure that gives the average power of a signal over a certain integration time T_{int}[4]:

$$P_{x,a}^{(T_{\text{int}})} = \frac{1}{K_{\text{int}}} \sum_{k=a}^{a+K_{\text{int}}} P_x[k], a \in \mathbb{N},\ 0 \leq a < K - K_{\text{int}}, \tag{9}$$

where $K_{\text{int}} = \lceil T_{\text{int}} f_{\text{SR}} \rceil$. We then apply (9) to all parts of the signal and take the maximum value:

$$P_x^{(T_{\text{int}})} = \max_{a \in \{0, K_{\text{int}}, 2K_{\text{int}}, \ldots\}} \{\ P_{x,a}^{(T_{\text{int}})}\ \}. \tag{10}$$

We understand the definition of (10) as a compromise between the extreme cases (7) and (8):

$$\lim_{T_{\text{int}} \to 0} P_x^{(T_{\text{int}})} = P_x^{(\text{peak})}$$
$$\lim_{T_{\text{int}} \to \frac{K}{f_{\text{SR}}}} P_x^{(T_{\text{int}})} = \overline{P_x}.$$

We finally define the ratio between the peak power $P_x^{(\text{peak})}$ of $\boldsymbol{s}_x$ and its mean power $\overline{P_x}$ as the Peak to Average Power Ratio (PAPR) (usually given in logarithmic scale):

$$\text{PAPR}\big|_{\text{dB}} = 10 \log_{10} \left\{ \frac{P_x^{(\text{peak})}}{\overline{P_x}} \right\}. \tag{11}$$

B. Scaling of Signals

The equations presented in the previous section all apply to digital signals that represent relative powers that are not given in physical units. However, as we take physical parameters from the environment (e. g. Line of Sight (LOS) distance, transmission power) into account, we have to connect the domain of digital signals with the real world setup. This is performed by an appropriate scaling of the involved signals.

When a signal $\boldsymbol{s}_{\text{Tx}}$ is physically transmitted with an EIRP of P_{Tx}, we use (10) with a reasonable T_{int} to compute the signal's power for the required signal scaling in the receiver. This is motivated by the fact, that in a real world scenario, the average operating point of a High Power Amplifier (HPA) is set below its actual $1\,\text{dB}$ ($3\,\text{dB}$, respectively) compression point to avoid distortions to the amplified signal or even damage to the HPA. Therefore, the average power of the emitted signal is below the maximum power the transmission hardware is capable of and cannot be used as a base for the signal scaling in the receiver.

Since the received power of a signal depends on the transmission power, this principle is applied to received signals, too, as a matter of consequence: In case a receiver receives two signals $\boldsymbol{s}_A$ and $\boldsymbol{s}_B$ with the received powers $P_{\text{Rx},A}$ and $P_{\text{Rx},B}$, respectively, the signal vectors are scaled before superimposing them such that

$$\frac{P_A^{(T_{\text{int}})}}{P_B^{(T_{\text{int}})}} = \frac{P_{\text{Rx},A}}{P_{\text{Rx},B}} \tag{12}$$

is fulfilled.

C. Signal Energy

The common way to compute the energy of a continuous signal is by integrating its power along time. Another way is to multiply the signal's mean power by its duration. The latter approach can be applied directly to a discrete signal $\boldsymbol{s}_x$ – however, once the physically emitted power is of interest, the transmission power P_{Tx} of the signal comes into account. As described above, we understand P_{Tx} as the real world power corresponding to $P_x^{(T_{\text{int}})}$, the scaling is performed with respect to this power:

$$E_x = \underbrace{P_{\text{Tx}}}_{\substack{\text{transmission}\\\text{power}}} \underbrace{\frac{\overline{P_x}}{P_x^{(T_{\text{int}})}}}_{\substack{\text{power}\\\text{scaling}}} \underbrace{\frac{K}{f_{\text{SR}}}}_{\text{duration}}. \tag{13}$$

[4] We suggest to choose T_{int} such that it is at most half as long as the pulse length of the shortest pulse of all signals inside of the observed system.

References

[1] M. Schnell, U. Epple, D. Shutin, and N. Schneckenburger, "Ldacs: future aeronautical communications for air-traffic management," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 104–110, 2014.

[2] J. Budinger and E. Hall, *Aeronautical Mobile Airport Communications System (AeroMACS)*, 09 2011.

[3] J. Grimes, "Commercial wireless metropolitan area network (wman) systems and technologies," *Memo 8–39*, 2009.

[4] C. Patel, G. Stuber, and T. Pratt, "Analysis of ofdm/mc-cdma under channel estimation and jamming," in *2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No.04TH8733)*, vol. 2, 2004, pp. 954–958 Vol.2.

[5] T. C. Clancy, "Efficient ofdm denial: Pilot jamming and pilot nulling," in *2011 IEEE International Conference on Communications (ICC)*, 2011, pp. 1–5.

[6] C. Shahriar, S. Sodagari, and T. C. Clancy, "Performance of pilot jamming on mimo channels with imperfect synchronization," in *2012 IEEE International Conference on Communications (ICC)*, 2012, pp. 898–902.

[7] C. Shahriar, R. McGwier, and T. C. Clancy, "Performance impact of pilot tone randomization to mitigate ofdm jamming attacks," in *2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, 2013, pp. 813–816.

[8] C. Mueller-Smith and W. Trappe, "Efficient ofdm denial in the absence of channel information," in *MILCOM 2013 - 2013 IEEE Military Communications Conference*, 2013, pp. 89–94.

[9] D. M. Mielke and T. Gräupl, "On the vulnerability of random access channels in aeronautical communications," in *2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)*, 2020, pp. 1–7.

[10] P. Hoeher and E. Haas, "Aeronautical channel modeling at vhf-band," in *Gateway to 21st Century Communications Village. VTC 1999-Fall. IEEE VTS 50th Vehicular Technology Conference (Cat. No.99CH36324)*, vol. 4, 1999, pp. 1961–1966 vol.4.

[11] D. M. Mielke, "C-band digital aeronautical communication for unmanned aircraft systems," in *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, Sep. 2017, pp. 1–7.

[12] D. M. Mielke, "Frame structure of the c-band digital aeronautical communications system," in *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, April 2018, pp. 2C4–1–2C4–12.

[13] U. Epple and M. Schnell, "Channel estimation in ofdm systems with strong interference," 09 2010.

[14] T. Gräupl, "Facts2: A service oriented simulation framework for aeronautical communication system evaluation," 09 2016.