A Hardware-Efficient Hybrid Approach for Suppression of Multiple Jammers in GNSS Receivers

Kevin E. Drenkhahn¹, Markus Landmann², Ali Rashidifar¹, Christoph W. Wagner¹, and Renato Zea Vintimilla¹

¹Technische Universitat Ilmenau Fakultat fur Elektrotechnik und Informationstechnik
²Fraunhofer-Institut fur Integrierte Schaltungen IIS

May 27, 2024

Abstract

A majority of modern positioning solutions are based on global navigation satellite systems (GNSS). These systems provide an exact, reliable, flexible and cheap solution for the related tasks, like sea navigation, aviation or the automotive sector. However, they are vulnerable to deliberate or collateral disturbance by means of jammer or spoofer signals. Hardening the systems in an environment of ever increasing demand for reliability is therefore one of the big challenges in the field. This work presents a solution focused on an analog beamforming solution, due to its cost effectiveness. A prototype of a four antenna receiver is shown with a measured jammer suppression of above 30 dB . The measurement results were obtained in a realistic over the air scenario. The presented work functions as a proof of concept for an integrated version to be implemented in future.
RESEARCH ARTICLE

A Hardware-Efficient Hybrid Approach for Suppression of Multiple Jammers in GNSS Receivers

Kevin E. Drenkhahn¹,²  |  Renato Zea Vintimilla¹,²  |  Markus Landmann²  |  Ali Rashidifar¹  |  Christoph W. Wagner¹

¹Fachgebiet Elektronische Messtechnik und Signalverarbeitung, TU Ilmenau, Ilmenau, Germany
²Abteilung Elektronische Messtechnik und Signalverarbeitung, Fraunhofer IIS, Ilmenau, Germany

Correspondence
Kevin E. Drenkhahn:
Email: kevin-etienne.drenkhahn@tu-ilmenau.de
Present address
Helmholzplatz 2
98693 Ilmenau
Germany

Funding Information
This research was supported by the Free State of Thuringia in the framework of the project “HyLOC” (2019 FGR 0100) financed through the European Social Fund

Abstract
A majority of modern positioning solutions are based on global navigation satellite systems (GNSS). These systems provide an exact, reliable, flexible and cheap solution for the related tasks, like sea navigation, aviation or the automotive sector. However, they are vulnerable to deliberate or collateral disturbance by means of jammer or spoofer signals. Hardening the systems in an environment of ever increasing demand for reliability is therefore one of the big challenges in the field. This work presents a solution focused on an analog beamforming solution, due to its cost effectiveness. A prototype of a four antenna receiver is shown with a measured jammer suppression of above 30 dB. The measurement results were obtained in a realistic over the air scenario. The presented work functions as a proof of concept for an integrated version to be implemented in future.

KEYWORDS
GNSS, Jammer, Null-steering, Phased Array

1  |  INTRODUCTION

1.1  |  Problem Description

Navigation and time synchronisation are two closely related problems, almost as old as humankind itself. In modern times the solution often relies on the use of GNSS services, such as the American Global Positioning System (GPS), the European Galileo and the Russian Global Navigation Satellite System (GLONASS). Here, the basic technique for determining the time and position of a user is to measure the signal runtimes and therefore distance from a network of satellites. The position and time fix is done by solving a system of equations with four unknown components (three space and one time variable). The modern environment usually provides more than the minimum of four simultaneously received satellite signals, especially for multi band receivers. This in turn leads to low positioning errors at all times and locations, making these systems an invaluable tool. Reliability of positioning is however challenged by various intentional and unintentional interfering sources. Due to cheap and easily available radio frequency (RF) components and software defined radios (SDRs), Jamming and Spoofering of signals can be achieved easier than ever before. Civil GNSS is especially vulnerable due to the low transmission power, publicly accessible codes with less correlation gain and low cost integrated receivers. The resulting problems together with the growing demand of the accuracy of positioning systems due to increasing automation leads to extensive research in the field of GNSS interference.
As a part of this effort, development of robust receiver systems is crucial, yet challenging, especially in the price driven
civil market. This work proposes as solution a Discrete Beamforming Network (DBFN), a prototype for a jammer and spoofer
suppressing hybrid, meaning combined analog-digital, system. The focus of this work is on the analog part and to suppress
jammer and spoofer early in the receiver. This reduces the complexity and power consumption of the digital part of the GNSS
receiver and can allow the deployment of standard low bit depth receivers even in disturbed environments. The developed system
mainly serves as a prototype for testing and gathering experience for an integrated circuit realization and its analog control loops
to be developed based on the findings in realistic environments. In this way the proposed work paves the way for a real low
cost and robust GNSS receiver. The prototype successfully suppresses even multiple jammers in a realistic Over the Air Testing
Facility (OTA) setting and enables deployed commercial off-the-shelf (COTS) GNSS receivers to recover the full signal quality in
case of a jammer attack. The device will automatically suppress any jammer signal registered with help of a novel null-steering
algorithm. This algorithm adjusts automatically to changes like movement and needs no a priory knowledge of the scenario.

1.2 GNSS Signal Properties

GNSS saw huge expansions of frequency bands in the last two decades. This is due to the availability of multiple new services
on the civil marked in addition to GPS and the progressive development of all services. In the following, we will focus on the
publicly available parts of the three services GPS, GLONASS and Galileo, as they are available globally and see the widest use.
Specifications for the current GPS signals can be found in[7–9], for GLONASS in[10] and for Galileo in[11,12]. The basic function is
the same for all of them. A ranging code is transmitted by satellites, distributed on well defined orbits. These codes are known
by the receiver and can be used to estimate the traveling time of the signal by means of finding the time of the maximal peak
of the autocorrelation function. This autocorrelation function is build by correlating the incoming signal with a copy of the code
generated by the receiving device itself. By finding the peak of this function the time delay between satellite and receiver can
be measured and the distance can be estimated. This technique makes precise satellite navigation with cheap user equipment
possible. The correlation of the codes grant a significant Signal-to-noise ratio (SNR) gain so that the signal to be processed
will have a sufficient SNR in most cases. Furthermore most signals used send a specific code per satellite leading to a Code
Division Multiple Access (CDMA) transmission in the same frequency band. These codes have a low cross correlation allowing for
unambiguous identification of satellites. One exception here are the older GLONASS signals in the bands L1 and L2, using the
same code for all satellites, but different carrier frequencies, leading to Frequency Division Multiple Access (FDMA) transmission.
By identifying the time shifts of at least four different satellites a position can be estimated. All three considered services transmit
multiple signals on different frequency bands at the same time. This has the advantage of processing a multitude of signals, with
different characteristics like carrier frequency or ranging code length and -modulation, allowing for advanced correction of errors
caused, e.g., by ionospheric effects. Furthermore some signals can be transmitted encrypted to restrict access for military or
government services. An overview of all current signals used by the discussed services is shown in Figure[1]. To further increase
precision and acquisition times needed, additional to the ranging code, some signals carry data streams containing information
about the satellite and system status like deviation from the orbits and the related correction data. This data is send by modulating the ranging code at a quite low data rate in the tens of Hz.

A special role is allocated to the signals sent in L1, especially the C/A signal of GPS. Even though this signal is the oldest still in use and is therefore lower in power and simpler in structure, using Binary Phase Shift Keying (BPSK) modulated Gold Codes for ranging, it is still quite relevant. Newer signals, e.g., the broad band signals send in L5/E5 band, allow for more precise positioning, but most receivers rely on the L1 signal for first acquisition and synchronization. As a lot of receivers therefore rely on L1, most jammers for the civilian market are focusing on disrupting this band as well. For this reason and as the finding of the proof of concept can also be applied for other bands, this work concentrates on the L1 band.

1.3 Jammer

The main goal of jammers is to disturb reception of the GNSS signals, which leads to an increase of the positioning error or even results in the loss of positioning. In most cases the transmitted signal has a power level that is well above the GNSS signal to be received. GNSS-services are especially prone to be attacked due to the low signal power and often cheap and low dynamic range receivers. Dedicated jammers exist in a variety of models. The first kind are cheap plug-in devices, often meant to prevent the position tracking of the user himself, but as a secondary effect disturbing the reception of surrounding users. The second kind are high power military grade systems to jam large areas of hardened targets. This work focuses on automotive and customer electronics, where only low power/cost jammers are relevant. The purchase of these is often not regulated, while usage is prohibited. These devices are cheap and easily available, as the signal characteristics of GNSS allow for easy disruption for most customer grade receivers. In[13,14] a large number of different jammers were tested and measured in regard to their signal properties. The signals used are usually continuous wave (CW) or swept CW-signals in the L1-Band, differing widely in power. Other bands are less prone to jamming. As mentioned above a lot of receivers will not work correctly without L1 signals, even when having undisturbed access to, e.g., E5-signals. Furthermore a high power signal at one band might disturb other bands, depending on the inner structure of the receiver. It is also expected that jammer technology will evolve with the GNSS-systems. Consequently, a detection and suppression of the interfering signal is needed to guarantee reliable GNSS signal reception and positioning. The frequency tuning of jammers has been shown to be not very accurate and might even be out of the signal band, but the high transmission powers together with limited input filtering of GNSS-receivers will still lead to reception problems. Next to jammers, spoofers may be encountered. These systems focus on the feeding of false positioning data instead of loss of reception in the target device. Even though detection of such systems may be more challenging, they can generally be suppressed in a similar manner. While the proposed system can therefore be used for spoofer suppression, the focus of this work is on jammers.

1.4 Spatial Filtering for Jammer Suppression

Combining multiple antenna signals with added delay or phase shifts to suppress reception of unwanted signals from a certain direction is a technique discovered more than 100 years ago[12]. However, its appeal for suppression of disturbances still stands. The underlying hardware structure consisting of N antennas is shown in Figure 2 and is called a phased array. Sending and receiving from/to an array behave similarly due to reciprocity. As in GNSS the antennas on the user side are not used for transmission, we will focus on the receiving case for simplicity. Here \( x(t, \Omega) \) is a signal impinging on the array from a source in the far field such that

\[
x(t) = x_1(t) \cdot \mathbf{e}_\Omega(\Omega) + x_2(t) \cdot \mathbf{e}_{\omega t}(\Omega), \quad x_1(t) = a_1 \cdot \cos(2\pi f_\omega t + \theta_1), \quad x_2(t) = a_2 \cdot \cos(2\pi f_\omega t + \theta_2),
\]

where \( \Omega = (\Phi, \Theta) \in [0, 2\pi] \times [0, \pi] \) is the spherical angle of the impinging wave and \( x_1(t), x_2(t) \) are the two canonical orthogonally polarized signal components. The parameters \( a_1, a_2 \in \mathbb{R} \) are the corresponding amplitudes, \( f_\omega \in \mathbb{R} \) the carrier frequency of the

---

**Figure 2** General phased array principle for a receiving structure without any geometric restrictions other than being in the far field.
signal and \( t \in \mathbb{R} \) is the time. The following description for the individual signal received at each antenna signals holds:

\[
\begin{align*}
    s_n(t, \Omega) &= \gamma_n(\Omega) \cdot x_1(t) + \gamma_{n2}(\Omega) \cdot x_2(t), \\
    \gamma_n(\Omega) &= p_n(\Omega) \cdot \phi_\Omega, \\
    \gamma_{n2}(\Omega) &= p_{n2}(\Omega) \cdot \phi_\Omega.
\end{align*}
\] (2)

The terms \( \gamma_n, \gamma_{n2} \) can further be divided in an angle dependent antenna pattern part \( p_n, p_{n2} \in \mathbb{C} \) and an antenna position dependent relative phase shift \( \phi \in \mathbb{R} \). Under narrow band assumption this phase shift is equivalent to a delay between the reception of the impinging wave at each antenna due to traveling route length distances. Therefore adding an artificial phase shift of \( \phi \in [0, 2\pi] \) before combination, can directly influence the amplitude of the combined received signal in correlation to its direction. The combined signal and its power \( P \) can also be called a beam and can be expressed as

\[
y(t, \Omega, w) = \sum_{n=0}^{N} s_n(t, \Omega) \cdot d_n e^{j\gamma_n} = \sum_{n=0}^{N} s_n(t, \Omega) \cdot w_n = A_y(\Omega, w) \cdot \cos(2\pi f t + \phi_\Omega, w)),
\]

\[
P(\Omega, w) = \frac{1}{Z_0} \cdot y_{\Omega}(\Omega, w)^2 = \frac{1}{2Z_0} \cdot A_y(\Omega, w)^2.
\] (3)

The vector \( w \in \mathbb{C}^N \) contains all phase shifter weights \( w_n \) representing the added phase shift \( \gamma_n \) and an additional amplitude compensation \( d_n \in \mathbb{R} \). In cases where only a phase shift is applied without additional amplitude gain \( d_n \) is set \( d_1 = d_2 = \ldots = d_N = 1 \). The output signal \( y(t) \) is a sine wave signal just like the input signal \( x(t) \). The power of this signal is \( P \), with \( Z_0 \) being the impedance, acting as a fixed preterm. Equation (3) describes the spatial filter implementation through the applied weights \( w \).

Generally two techniques for deployment of phased arrays and phase shifter weight selection can be differentiated: Beamforming and null-steering. The former is sometimes used as a synonym for all phased array techniques, we are however differentiating between the two here. Beamforming has the goal of maximizing reception or transmission in a certain direction by combining all received signals from this direction constructively. All signals from this direction should therefore have the same phase when combined. There is exactly one solution for selecting weights achieving this goal, selecting the weights \( w \) such that the added phase shift \( \gamma_n \) is the inverse phase of the received signal \( s_n(t, \Omega) \) for all \( n \). Usually a side constraint is no ambiguity caused by the formation of multiple main lobes, due to having time differences between two neighboring antennas larger than a single period. Here, the same phase relation would occur for more than one spherical angle \( \Omega \). This can be guaranteed by sufficiently low distances between neighboring antenna elements, usually lower than \( \frac{\lambda}{2} \). In null-steering the goal is exactly the opposite. Here, the target is to chose all weights \( w \) such that the received power \( P \) from a direction \( \Omega \) is minimal. Multiple solutions for \( w \) generating the same desired destructive superposition of antenna signals can be found. While the distance of the antenna elements is still influencing array behaviour, in null-steering it is not as crucial, as additional nulls caused by ambiguity are not avoidable and often not problematic. Ways to calculate the phase shifter weights \( w \) to hit this target are discussed in Section 3.

1.5 State of the Art and Contribution

Hardware capable of beamforming and null-steering in this way can generally be divided into three sub categories. First, there is pure analog beamforming. Here, the phase shift is applied before digitizing the received signal. This has the advantage that the recombination of the signals can be done in the analog domain and close to the antenna. This in turn leads to an early suppression of jammers in case of null-steering, limiting the need for high dynamic range in all following components including the analog-to-digital converters (ADCs). Furthermore the number of signals can be reduced through the combination. The second variant is digital beamforming. Phase shifting and combination is subsequently done after digitizing, allowing for precise beam steering. Due to the digital nature of the signals they are also easily multiplied and distributed, allowing separated beams specifically for each satellite. This can be applied to GNSS, but is limited to high cost systems, as the dynamic range of the ADC has to be high enough to allow reception of the GNSS signal and jammer signal at the same time. The third possibility is to combine both to obtain a hybrid beamformer. Here, the analog beamformer, used to suppress strong jammers before digitization, is followed by a digital stage, allowing for further signal processing. This second stage allows, e.g., beamforming in direction of satellites to improve reception or the suppression of spoofers, which is both not possible with a purely analog design. In comparison to a fully digital approach this has still the advantage of lowering the needed dynamic range of the ADCs significantly, while keeping the advanced digital signal processing. A prerequisite for this method is the usage of multiple beams, where the signal from the antennas is split, allowing for multiple analog beamformers to work in parallel.

In the field of GNSS jammer and spoiler suppression currently available solutions based on multi antenna receivers apply mostly digital beamforming. This in turn limits their application to high cost, e.g., military applications[33]. Due to rising demand on automation applications in the price driven civil market, e.g., in the automotive sector, are more relying on precise and robust GNSS based localization than ever. As described in 1.2 and Section 1.3 this is problematic due to the ease in which the GNSS signal can be disturbed. This work aims to address this by showing an alternative for exactly these applications. The system to be
A Hardware-Efficient Hybrid Approach for Suppression of Multiple Jammers in GNSS Receivers

developed is an integrated hybrid beamforming receiver. However, the focus here is on the first analog stage, allowing for a second, digital stage to be added later. The main idea is to proof that the analog stage significantly reduces the interfering power so that the digital part can be designed or even reused with a minimum complexity and power consumption. For instance lower bit ADCs could be applied, that leads to lower complexity in the processing part, lower power consumption and on large scale to lower costs. In the following Section 2 the developed HYLOC DBFN, a prototype for a analog beamforming unit is described. To allow for the later addition of digital stages, a four beam design was chosen. Furthermore possible analog control loop algorithms were developed and optimized for deployment with the DBFN and future integrated circuit (IC) solutions (see Section 3). Finally, the DBFN was deployed together with the algorithms in realistic OTA testing scenarios and measured (see Section 4).

2 | HYLOC DBFN PROTOTYPE

2.1 Hardware Structure

The DBFN is the prototype for testing the null-steering approach for jammer suppression in GNSS receivers, as described theoretically in Section 1. It can be used as a flexible platform for testing algorithms and the application in realistic measurement scenarios. A photo of the main hardware block without cover can be seen in Figure 3b. It is build modular, with the overall structure shown in Figure 3a. The structure realizes a 4x4 beamformer, meaning it possesses inputs for four antenna signals and output for four individually controlled beams. As mentioned before, the multi beam design allows further digital processing. In the current development stage only one beam is actively used, acting as a purely analog beamformer. The first component for analog signal processing is the front plane, where the RF-connectors are mounted. Afterwards four power splitter printed circuit boards (PCBs) are mounted, using the GP2S+ power splitter IC from Mini-Circuits to split every antenna signal in four identical signal copies. The next step are the four beamformer PCBs, adding an individually controlled phase shifts by means of MAPS-010163 phase shifters from MACOM to the received signals. The phase shifter control signals are generated by the controlling main board, with added signal distribution on the back plane PCB. At the last step the four antenna signals with phase shifts are combined on these PCBs into one beam, once again using the GP2S+ circuit and relayed to the Subminiature version A (SMA) output connectors on the front plain. All individual PCBs are shown as blue building blocks and are build as single units, granting maximal reconfigurability.

At the inputs four additional external ZX60-P103LN+ low noise amplifiers (LNAs) from Mini-Circuits with 12 dB gain at the L1 band are used to pre-amplify the antenna signals, thus compensating for the power loss in the power splitting stage.

The main board for controlling the DBFN consists of a SAM-E70 Xplained evaluation kit board from Microchip with a custom firmware flashed onto it. Other equivalent microcontrollers and boards could be used, which is part of the modularity doctrine. The firmware and a developed module for python allow for direct control of the DBFN device from a high level language. Controlling of the beamforming settings is done by a PC connected via USB. The firmware has an integrated error detection on board and compares the sent phase shifter states with the actually selected. The connected PC runs a Python script managing the algorithmic calculation (see Section 3) of the phase shifter weights from the measured DBFN beam output signals and the communication with the rest of the measurement setup further explained in Section 4.1.
2.2 | DBFN Characterization

On the controlling PC side the software running is python based. To allow for the development of the DBFN in tandem with the controlling software and the algorithms, this software was first developed based on simulation. Later the simulated parts was replaced by the possibility for a hardware in the loop setup with the DBFN and OTA measurement chamber described in Section 4.1. It is planned to develop a custom IC design on bases of the results and experiences gathered from the DBFN. The simulation and control software is advanced side-by-side with the hardware to allow for early assessment of the system performance. This serves as a high level supplementation to the circuit level simulation done in Cadence, maximising the chances for a first-time-right design. To allow this development precise characterization and modelling of the DBFN is needed as a reference. This allows predictions of performance of future hardware on the basis of the measurements taken in Section 3.

This characterization is done with stand alone measurements of the device independently of the over the air jammer suppression measurements. These measurements are conducted with a ZNB vector network analyzer (VNA) from Rhode & Schwarz measuring the S-Parameter characteristics from antenna inputs to beam outputs. A challenge of these measurements are the numerous possible setting combinations. The device contains 16 phase shifters with $2^8 = 64$ possible states, respectively. To measure all possible combinations and describe the device fully would mean to test for $64^{16} \approx 8 \times 10^{28}$ states. As this is not viable a heavy preselection of interesting states is needed. This is done by taking into account the inner workings of the switch based phase shifters and the most likely parasitic effects. Overall the number of points measured representing the whole setting space of the device are brought down to 12064. The detailed results are not discussed here, as they go beyond the scope of this article.

3 | DYNAMIC JAMMER SUPPRESSION

3.1 | Null Steering

Next to the physical structure and hardware described above, the performance of the system build is heavily dependent on the algorithms used to calculate the weight states $w$ for the phase shifters. The main goal is to calculate these settings without any a priori knowledge about the position of the jammer signal in a way to suppress said signal. Even though the hardware is capable of four simultaneous and independent beam outputs, the algorithms discussed here are only single beam/ null-steering solutions. Selection of weights for multiple beams or orthogonal null-steering solutions to be combined in the digital domain are an extension on this and are not discussed here, as the focus of this work is purely the analog null-steering part with default digital signal processing later.

Overall there are over $16^{16\text{ mio}}$ different combinations of the four 6bit phase shifters of the DBFN. As it is not possible to do an exhaustive search for every change in the scenario an intelligent search approach for finding a sufficiently good solution in a acceptable low time is needed. As a starting point a general solution with ideal phase shifters, possessing phase states with infinitely fine resolution, paired with perfect antennas can be defined. In this case total deconstructive superposition can be treated as a jammer signal. As all of these signals shall be suppressed, $g$ can be chosen according to considerations of algorithm timing and noise. The more samples of the $u$ possible states, respectively. To measure all possible reception direction. There are even multiple solutions for reaching this result. A general way to calculate these ideal weights for beamforming and null-steering phased arrays is (3):

$$\lambda^H = g^H(C^H R^{-1} C)^{-1} C^H R^{-1}$$

$$C = [b_1, b_2, \cdots, b_J]$$

$$R = \text{cov}(m_{0,u}, m_{1,u}, \cdots, m_{N,u}) = MM^H$$

The goal is to calculate a single ideal weight vector, containing a solution for the targeted beamforming result, we call $\hat{w} \in \mathbb{R}^N$. The input for the algorithms are the $N$ digitized antenna signals. The calculation is based on a least squares approach with the covariance matrix $R \in \mathbb{R}^N$, containing the received signal properties. This is calculated from the row vectors of the $N \times U$ measurement matrix $M$ containing the individual measurements $m_{n,u}$, with the antenna index $n \in [0, \cdots, N]$ and the sample index $u \in [0, \cdots, U]$. The value of $U$ can be chosen according to considerations of algorithm timing and noise. The more samples of the antenna signals are considered, the larger the measurement time and the heavier the calculation load, but the lower the influence of noise. An upper limit is set by the dynamics of the scenario, as during the measurement time the reception situation is assumed static. For a case involving movement of either the receiver or the jammer (or both), the time spend measuring has to be kept sufficiently low. The other inputs used are coding the treatment of incoming signals. The constraint matrix $C$ contains the J steering vectors $b_j$ of received and either desired or interfering signals with $j \in [0, 1, \cdots, J]$. These can as well be calculated from $R$ by means of a single value decomposition (SVD). The vector $g$ defines for each $j$, if the associated signal should be attenuated (0) or amplified (1). In our case we have no specific desired direction of reception, as the satellite positions are distributed at different positions and no specific satellite direction should be selected. Only a certain number of jammers are to be attenuated. Due to the power of the GNSS signals being below the noise floor before correlation, every signal with power over the expected noise level can be treated as a jammer signal. As all of these signals shall be suppressed, $g$ only containing zeros and J going up to the
number of received jammer signals. This pure null-steering can efficiently be calculated by solving the simplified equation

$$C \cdot \hat{w} = 0_v.$$  \hspace{1cm} (5)

In case of \( N > J \) multiple solutions for \( \hat{w} \) are possible. The solution of Equation (5) \( \hat{w} \) is defined as the kernel of \( C \), containing the vector space with all possible individual solutions for \( \hat{w} \).

For a more realistic case some important considerations have to be taken into account. First, the antenna signals \( s_i(t) \) have to be accessible. This scales badly with the problem size considering the goal of low cost, as all antenna signals need to be digitized, instead of only the combined signal. In the DBFN this is therefore not intended.

A second major restriction is the limited resolution of phase shifters. As mentioned in the beginning of this chapter the MAPS-010163 deployed have \( i \) bit resolution, leading to \( 2^i = 64 \) fixed states, where the solution found is under the condition of infinitely high resolution. Furthermore, the phase shifters suffer from basic phase errors in the region equivalent of half a least significant bit (LSB). In our case this is equivalent to \( \pm 2.3^\circ \). Additional errors in amplitude can be expected as well. This complicates the search for optimal selectable weights \( \hat{w} \) based on theoretically ideal weights \( \hat{w} \). Even though it is planned to further develop the covariance matrix solution in the future, especially the former problem leads to the decision to go another route for the weight finding in way of power minimization in regard to the DBFN.

### 3.2 Analogue Null-Steering Approach Based on Power Minimization

Power minimization is a known approach to null-steering in GNSS applications, based on an empirical selection of \( \hat{w} \). E.g., it was done in\(^{[4]} \) As every signal above the noise can be classified as a disturbance, the goal is to minimize the power \( P \) of the combined signal \( y(t) \) (see Equation (2)), for an arbitrary array geometry, like the one shown in Figure 2. To get \( \hat{w} \) directly, a solution to

$$P(\Omega, \hat{w}(\hat{i})) = \min(P(\Omega, w(i))), \quad w(i) = \exp\left(\imath \frac{2\pi}{\lambda} s_i \cdot \hat{s} \right), \quad \hat{w}(i) = \exp\left(\imath \frac{2\pi}{\lambda} \text{MSBs old} \right), \quad i, \hat{i} \in \mathbb{N}_0^N,$$  \hspace{1cm} (6)

needs to be found, by with searching a small subset of all possible states. As discussed before the phase shifters can be set to a finite number of states. The vector \( i \) contains the selected state for each of the phase shifters used in the arbitrary weight vector \( w(i) \), while \( i \) contains the indices for the found optimum \( \hat{w}(i) \). A big advantage is that the optimization algorithm relies solely on the power \( P \) as an input and therefore a single, easily measured value. The computationally complex estimation of direction of arrival (DOA) or a priori knowledge about the jammer is not needed. As the power measurement of \( y(t, \Omega, w) \) can be done analogously, an initial overload of the ADCs will not disturb the algorithmic performance. For some hardware implementations one could also use the available automatic gain control (AGC) as a power sensor.

To solve the optimization problem for finding \( \hat{i} \) in the following a new algorithm is proposed. The algorithm uses a coarse-to-fine approach, represented in Figure 4. The gray blocks ‘Measure P’ and ‘Threshold hit?’ are optional and will be described later. As a first step, the applied weights \( w(i) \) are set to all combinations of the variation of the two most significant bits (MSBs) of \( i \), holding the other bits constant at ‘0’. The powers are measured one by one and saved. From these \( 4^i = 256 \) combinations, the \( i \) resulting in the lowest measured power \( P \) serves as preliminary solution for \( \hat{i} \) and a starting point for the next iteration step. In this step one additional bit of resolution is considered and all combinations involving the new nearest neighbours of \( \hat{i} \) are used for the next searching step. An example for step 3 of this process is shown in Figure 4. These steps are repeated until the minimal step width of the employed phase shifters is reached and a good result for \( \hat{i} \) and therefore the weights \( \hat{w}(i) \) is found. With this implementation the number of measurement points is reduced to \( 4^4 + 4 \cdot 3^4 = 580 \) measurements. To further decrease the needed measurements, a degree of freedom can be sacrificed by holding one phase shifter fixed. It does not infringe on the capabilities of the null-steering and only \( 4^4 + 4 \cdot 3^3 = 172 \) points need to be measured.
This was used for all measurements shown later. With each individual measurement consisting of 1000 samples with the SDR operating at 20 Mps, the overall time spend measuring for a full algorithm run is 8.6 ms. The main limitation is the speed of the power measurement and the phase shifter control units. Currently the time for a algorithm run in the discrete measurement setup is longer at around 2 s. This is due to the heavy limitation of the current measurement setup, where calculation is done on a separate computer with limited connection speed. Later integrated solutions will not have these problems. It is however still beneficial to limit the number of needed calculations further, as this relaxes the need for high performance, high cost processing units.

### 3.3 Tracking Null-Steering Weights

<table>
<thead>
<tr>
<th>Measured $P$ [dBm]</th>
<th>$&lt;-90$</th>
<th>$-90 \ldots -85$</th>
<th>$-85 \ldots -80$</th>
<th>$-80 \ldots -75$</th>
<th>$-75 \ldots -70$</th>
<th>$&gt;-65$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recalc. starting bit</td>
<td>no recalc.</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Max recalc. steps needed</td>
<td>–</td>
<td>27</td>
<td>54</td>
<td>81</td>
<td>108</td>
<td>172</td>
</tr>
</tbody>
</table>

**Table 1** Starting levels of precision for recalculation in tracking mode. Higher measured power is interpreted as a larger shift in positions, therefore triggering a coarser recalculation starting point.

In Section 3.2 it is shown that the process of finding optimal weights as described in Section 3.2 works fine for a situation of suddenly appearing jammers with fixed positions. For a realistic mobile scenario this is however only the case at the start of the jamming event. Afterwards the jammer and/or the GNSS receiver will change their relative positions and the null-steering weights need to be adjusted. This dynamic change in positions calls for small incremental adjustments to the weights rather than a recalculation from scratch. To accommodate for this in the algorithm a tracking mode based on a dynamic recalculation approach is implemented. Here, every recalculation of weights is triggered by a rise in measured $P$. The level of change in $P$ is corresponding to the change in position(s) of receiver, jammer or both and in turn also the needed change of the weights to find a new minimum. The recalculation is therefore not started from scratch, but is instead initialized with the previous weight indices, as the new solution for $\hat{1}$ is expected close to it. A large change in received power needs to be answered by a coarse recalculation approach and a small up rise only requires a relatively fine and fast recalculation. This is realized by starting from the previously set weights with a certain level of precision. The recalculation precision levels of the starting point are shown in Table 1 depending on the measured input power. The values were found empirically and worked the best for the current setup. Changes in the setup, e.g., antenna geometry or calculation speed, would change the optimum. For choosing the decision levels, the fundamental trade-off between possible faster speed and missing a solution completely has to be kept in mind. The former is achieved through sufficiently high power limits, triggering coarse recalculation only in case of large power increases. This however can lead to a case, where the recalculation is chosen from a too fine step by means of residing in a local minimum not reaching the global minimum of the optimization problem. As the algorithm will automatically adapt the level of recalculation, the tracking mode can be chosen as default operating mode. In Figure 4 the tracking mode is shown by including the grey block ‘Measure $P$’ at the beginning of every run before selecting the precision. This overall limits the number of iterations steps and lightens the computational load of recalculating weights. The 172 measurements from Section 3.2 are therefore the upper limit of steps needed, only required in case of a big rise of jammer power, e.g., at the beginning of a jamming event.

A further step to potentially reduce the number of measurements needed to find an optimal value for $\hat{w}$ is to define an abort condition by means of a threshold for $P$. Setting the threshold to the value of the noise floor at $-90$ dBm, the needed iterations as given in Table 1 are the maximum. In most cases the threshold is reached earlier, when $P$ is in the range of the noise level. This method has no drawback, other than the additional lightweight comparing step shown in Figure 4 as the optional ‘Threshold hit?’ decision.

### 3.4 Taking Advantage of DBFN Phase Shifter Impairments

Additional approaches for optimizing results were tested, first in the simulation and then with measurements on hardware level. The trade off is usually between finding a better solution (better jammer suppression) and investing measurement time and thus taking longer to suppress a jammer or react to changes in the scenario. We propose the so called ‘rotation optimization’ as an optional last step of the algorithm. The idea is to use the individual phase and amplitude non-idealities of the phase shifter states as a leverage point. Usually phase shifters with as close to perfect performance as possible are desirable, as they allow to predict performance from a theoretic algorithm calculation view point without calibration. However, non ideal phase shifters give an
The possible enhancement is heavily dependent on the state of the incoming antenna signals. The resulting jammer suppression performance is now dependent on all applied weights $w_i$. While this leads to only a minuscule difference for constructive beamforming with small arrays, for null-steering it will heavily influence performance. The phase and amplitude deviations between the phase shifters can therefore be used as an additional degree of freedom for mitigating the limited phase shifter resolution.

An example with values from measured phase shifters is shown in Figure 5. Here, the result of null-steering two antenna signals with phases of $0^\circ$ and $178^\circ$ with 6 bit phase shifters are shown. In blue the best possible result with ideal phase shifters is limited to $-20$ dB suppression, as the ideal weights of $\tilde{w} = [1, e^{j2\pi r/2}]$ can only be approximated by using $\tilde{w}(i) = [1, 1]$. Rotating the values and using, e.g., $w = [e^{j2\pi i/8}, e^{j2\pi 5/8}]$ (rotation index $r = 1$) is possible, but will not influence the combined signal power. While the limited number of options is true for the use of real phase shifters with errors, too, here the rotation will change performance, as the errors are not equal for each step. This can be seen by observing the orange plots, where instead of ideal phase shifters the data from the first two real phase shifters (Beam 1 Antenna 1 / Beam 1 Antenna 2) of the DBFN were used. The measurement data were taken from the characterization measurements described in Section 2.2. For most cases the additional phase shifter error leads to worse suppression performance. However, 9 rotation states perform better than the ideal phase shifter equivalent. This is due to the additional degree of freedom due to differing errors and can be understood as an equivalent to using phase shifters with higher resolution. In this particular case the performance enhances $7$ dB for the best point marked in green. The possible enhancement is heavily dependent on the state of the incoming antenna signals.

In simulation it can be shown that the deployment of this method will lead to better results for algorithms operating under the condition of unknown phase shifter errors, like the covariance based approach mentioned in Section 3.1. Here the performance of the resulting jammer suppression can often be increased $10$ dB or more. However, in the case of power minimization used for the DBFN it has no significant advantage in simulation or measurement. The phase shifter errors are included in all measurements and therefore algorithm steps. A global minimum will therefore be found without the additional rotation optimization, deeming it unnecessary here. For future development and deployment of solutions based on a theoretical solution, like the covariance based approach, it is however effective in mitigating effects of hardware errors and allowing for even better performance than with ideal limited resolution phase shifters. Furthermore, it can be considered while designing a integrated phase shifter (see Section 5.2), as not all impairments are a disadvantage and can in the contrary be beneficial, when taken into account by the algorithm.
**VERIFICATION VIA REALISTIC MEASUREMENTS**

### 4.1 General Measurement Setup

The structure of the general setup used for measurements is shown in Figure 6. All measurements described here are conducted in the OTA chamber. In order to create a GNSS scenario for the testing of the HYLOC DBFN, the OTA testing method becomes the right choice due to its benefits in terms of playback and control of the test conditions. The basis of the applied realistic GNSS scenario emulation is the combination of the OTA testing method with a technique called 3D Wave Field Synthesis (3D-WFS). This combination can integrate more features to already established OTA testing method, such as the creation of electromagnetic plane waves and the ability to set virtual signal sources at any angular position within a three-dimensional space. Details about the 3D-WFS principle and its integration to the OTA testing method have already been described in recent publications. Therefore, this contribution will focus only on the implementation of a GNSS test setup.

The OTA setup consists of a GNSS simulator, an OTA channel emulator and an anechoic chamber where the virtual electromagnetic scenario is created. The GSS9000 unit developed by Spirent Communications performs the generation of the GNSS signals. This unit is customized in a way that signals per individual satellite are sent digitally to the channel emulator inputs. The OTA channel emulator itself contains three different blocks. These are ADC units, digital signal processor (DSP) based signal processing units and digital to analog converter (DAC) units for the signal transmission inside the anechoic chamber. It is worth to mention that the ADC devices become an active part of the setup during the OTA system calibration. Finally, the anechoic chamber is composed of 16 dual-polarized antennas equidistantly distributed according to a Lebedev grid. An equidistant distribution is highly important for the efficiency of the 3D-WFS. More details on the chamber setup can be found in.

The rest of the measurement setup consists of a controlled reception pattern antenna (CRPA) GNSS-antenna, the DBFN itself, a SDR and controlling personal computers (PCs). For measurements in Section 4.4 an additional commercial GNSS receiver is deployed. The antenna array developed by Fraunhofer IIS consists of four L1 antennas in two-by-two $\frac{\lambda}{2}$ configuration and a single L5 antenna in the middle of the structure. The later was not used and subsequently terminated with a $50\,\Omega$ resistor. The L1 antennas have symmetric antenna behaviour by means of homogeneous radiation patterns. This is important in the current configuration of the DBFN as it is limited to only phase shifting capability with no possible amplitude correction. This in turn means, that differences in received power from a certain direction between the elements will limit the null-steering capability. For deployment in a true low cost system this will need to be changed by adding a gain controlling stage, as low cost antenna arrays can not be expected to behave in a homogeneous way. After the antenna the signals are amplified by the LNAs and fed into the DBFN. Here, the antenna signals are weighted and combined to the four beam signals, as described in Section 2.1. Only one of these beams is actively used, while the others are currently not evaluated. The output of the first beam is connected to an Ettus

---

1 www.iis.fraunhofer.de/en/profil/standorte/forte
A Hardware-Efficient Hybrid Approach for Suppression of Multiple Jammers in GNSS Receivers

4.2 Jammer on Spiral

As mentioned above wave field synthesis (WFS) is used to generate arbitrary scenarios with different spatial positions of the jammer and the GNSS receiver under test. The antenna positions are shown in Figure 7a. Also realistic scenarios with a small incremental motion of the jammer and/or the GNSS receiver under test can be generated to evaluate the tracking behaviour. A prior selection of scenarios to test needs to be done, as it is impossible to test for all positions and trajectories. For sake of realism and ease of measurement a spiral form of jammer movement was chosen. Here, the azimuth is swept in a complete circle with 360 steps from the starting position. Simultaneously the elevation is swept from $0^\circ$ to $90^\circ$. As starting positions a selection of $-60^\circ$, $-30^\circ$, $0^\circ$, $30^\circ$ and $60^\circ$ was used to get some variety. The trajectories are shown in Figure 7b. The speed of position changes is varied. As the antenna array is a symmetric two-by-two structure in the x-y-plane a symmetric behaviour over $90^\circ$ shift in azimuth can be implied. It can be inferred that the taken measurements give a good idea for the overall performance on the half sphere. Measurement results for some representative measurements are shown in Figure 8a. Here, the position was changed every second. As a normal state reference and starting point the phase shifters were set to phases of $w(i) = [0, e^{j\frac{\pi}{2}}, e^{j\pi}, e^{j\frac{3\pi}{2}}]$, as the antenna has internal fixed phase offsets of $90^\circ$ between the elements. The received powers in the null-steering and the non-null-steering case are shown. For the null-steering case only the results of the algorithm are plotted and not the powers received during the algorithm runtime. This gives a good picture of the expected null-steering capability. It can be observed, that the power stays roughly at noise floor level, between 10 decibel and 30 dB below the reference, for most of the time. Exceptions can happen especially at positions, where the incoming wave characteristics change too fast for the algorithm. This leads to a
calculation of weights that is too slow for the change, which in turn leads to the power spikes in the orange plots of Figure 8a. This is expected and can be prevented by an faster integrated version of the HYLOC DBFN. Here, the 1 s steps used for jumping to the next jammer position are consistent with later measurements with GNSS signals present. The timings here are chosen as a compromise between measurement time and algorithm performance and are slowed down in comparison to scenarios encountered in reality. The current bottle neck is the waiting time for samples from the SDR over Ethernet. As a reference to optimization of calculation speeds also see Section 3.4

4.3 Multiple Jammers Test Scenario

A further measurement was conducted to evaluate performance for the simultaneous presence of two jammers. With four antennas stretching two dimensions this should be theoretically possible for all constellations of the impinging waves of the jammers. For the test setup the signals are transmitted from the OTA antenna positions. With 16 OTA antenna positions \(16 \times 15 = 240\) combinations of two different antennas active are possible. The measurements were conducted in a synchronous way, meaning enough settling time was given between the measurement points for a full algorithm run of the maximum 172 single measurement steps. This is necessary, as every measurement will change the jammer positions in large steps, preventing the tracking mode of the algorithm to work. The measured result is shown in Figure 8b. The overall suppression for the most part is again down to the noise level, around \(-90\) dBm. The received power for the fixed weights is strongly varying, as is expected, due to the either constructive or distructive superposition of the signals of the two sent jammer signals. Overall the difference between the DBFN prototype and without suppression is around \(-21\) dBm on average.

4.4 GNSS Performance with HYLOC DBFN in Jammed Scenario

The last measurement was done with a scenario close to a real application case in mind. A measurement drive on a street in the real world is recorded, to get GPS signals for a realistic measurement as a reference. A single beam stage of the DBFN with the same CRPA antenna was used as a Front-End with a Septentrio PolaRx5 receiver as GNSS backend. The recorded scenario is applied for a realistic emulation of the environment in the OTA facility at FORTE and a jammer signal at a fixed position was added to a part of the drive. This test is performed applying the same a Septentrio GNSS receiver in the chamber setup. To connect it to the DBFN one of its output signals was split with a power splitter in front of the SDR, so SDR and GNSS receiver get the same input signal (see Figure 6). The results of the received carrier-to-noise density ratio \(C/N_0\) for both cases, with fixed weights/without null-steering and with continuously calculated weights/null-steering active, are shown in Figure 9. This value determines the received signal quality. It can clearly be seen that the algorithm is quite effective in restoring most of the GNSS signal after a short reaction time. A secondary effect can be seen paying close attention to the individual satellite signals. While some of these are received with lower \(C/N_0\), others rise to even higher levels than in the not jammed case. This can be explained by the secondary beamforming effect of the null-steering weighting of antenna signals changing the gain in the satellite directions.
As the satellite positions are unknown to the receiver at this stage and therefore not taken into account by the algorithm this effect is random. However, for a full hybrid solution applying the multiple outputs one can additionally improve the $C/N_0$ for individual satellites via digital beam forming and even further suppress the jammer but with less dynamic range of the ADCs needed.

5 | CONCLUSION

5.1 | Results

In this article we showed an effective jammer suppression system for global navigation satellite systems (GNSS) receivers based on a four antenna analog beamforming receiver. With the Discrete Beamforming Network (DBFN) a flexible hardware platform capable of four independently set beams was developed. Together with the efficient power minimization algorithm running on a controlling PC the system proved to be effective in minimizing reception of jammer signals even from multiple directions. A testing environment for realistic GNSS scenarios based on wave field synthesis (WFS) was set up. Here real measured GNSS signals were used in combination with an artificially generated jammer signal. The DBFN proved to be capable of suppressing present jammer signals reliably more than 30 dB, while keeping satellite $C/N_0$ at level comparable with the undisturbed case. This shows that the proposed solution for a analog beamforming unit to suppress jammer signals is viable and can be deployed as is with a commercial off-the-shelf (COTS) GNSS receiver. Scalability and modularity were taken into account, so the build system can be used as a platform for future developments on the concept, like hybrid algorithms.

5.2 | Further Developments

As mentioned above the current prototype is used as a proof of concept as well as a flexible test platform. The next planned step is to take the results from these tests and use them as a basis for a integrated circuit design including the same functionality in a far smaller form factor at lower energy consumption and a scaleable price point. It is planned to implement this capability together with frequency shifting in two separated ICs first for better flexibility during development. The general high level structure is shown in Section 5.2. The first one is a RF Front-End with amplification, filtering and down conversion to bring the selected GNSS band to a defined intermediate frequency. The second is a direct conversion or low-IF receiver structure with phase shifting done at the mixing stage on the IQ-signal, implementing the beamforming capability and provision of signal to the ADCs. This IC also contains an implementations of the power minimization algorithm for weight calculation, eliminating the need for additional computational hardware. This on-board calculation will also vastly improve the calculation speed discussed in Section 4, as the current bottle neck of the SDR and Local Area Network (LAN) can be avoided. This allows for a flexible design, as the beamforming part is thus mostly independent on the used RF-band. It is also planned to use the work presented in 22 as an inspiration for the frequency planning, further decreasing cost by using one ADC for multiple bands.

Furthermore it is planned to adapt the prototype for other frequencies and applications, again as a testing platform or custom solution for specific low number applications. One idea here is to adapt to Radio-Frequency Identification (RFID) frequencies to heighten sensitivity of automatic inventory systems, as these systems struggle similarly with the high required dynamic range. With an updated algorithms and changed frequency range of the phase shifters the hardware shown here can be used to improve these systems, with relatively minor additional cost.

References


A Hardware-Efficient Hybrid Approach for Suppression of Multiple Jammers in GNSS Receivers

AUTHOR BIOGRAPHY

Kevin E. Drenkhahn studied electrical engineering at Technische Universität Ilmenau, Ilmenau, Germany from 2012, where he received the M.Sc. degree in 2018 and is currently pursuing the doctorate degree. Since 2018, he is part of the Electronic Measurements and Signal Processing (EMS) group in Ilmenau and since 2020 of Fraunhofer-Institut für Integrierte Schaltungen IIS. Current research topics are system design and signal processing for multi antenna receivers, especially for GNSS applications, as well as design of integrated analog and mixed-signal CMOS and BiCMOS circuits.

Renato Zea Vintimilla. received the BSc. degree in electrical engineering from the University of Cuenca in Ecuador and later the MSc. degree in communications and multimedia engineering from the Friedrich-Alexander-Universität Erlangen-Nürnberg in Germany in 2009 and 2016 respectively. Since 2018 he works as researcher for Fraunhofer IIS and Technische Universität Ilmenau in the development of testing techniques for wireless devices, particularly in the Over-the-Air testing method applied to GNSS devices. His research interests include signal processing, wireless communications and GNSS measurements.

Markus Landmann was born in Zeitz, Germany, in 1977. He is technical supervisor and head of the Over the Air Testing Group in the Wireless Distribution Systems Dept. —received the Dipl.-Ing. degree and Dr.-Ing. degree in electrical engineering (information technology) from the Technische Universität Ilmenau, Germany, in 2001 and 2008, respectively. From 2001 to 2003, he worked as a research assistant and instructor at Technische Universität Ilmenau. In 2004, he was developing advanced antenna array calibration methods and high resolution parameter estimation algorithm (RIMAX) for propagation studies at MEDAV Company. In 2005, he was visiting researcher and instructor at Tokyo Institute of Technology (Takada Laboratory) in the field of Channel measurement and estimation techniques. From 2006 to 2008, he was finalizing his PhD thesis while a research assistant and instructor at Technische Universität Ilmenau. Between 2008 and 2009, his projects were in wireless propagation, channel modeling, and array signal processing for Technische Universität Ilmenau and Tokyo Institute of Technology. In 2010, he started working for Fraunhofer IIS within the Department Wireless Distribution System/ Digital Broadcasting headed by Professor Giovanni Del Galdo. He is mainly responsible for the Facility for Over the Air Research and Testing.

Ali Rashidifar pursued electronics engineering with a focus on microwave and telecommunications. In 2020, he received a master degree in communication and signal processing at Technische Universität Ilmenau, (TU Ilmenau). Since then, he has been a research assistance in Electronic Measurements and Signal Processing Group at TU Ilmenau. He focuses on designing and miniaturizing antennas, as well as measuring and processing antenna data.

Christoph W. Wagner received the M.Sc. degree in electrical engineering and information technology from Technische Universität Ilmenau, Ilmenau, Germany, in 2016, where he is currently pursuing the doctorate degree. Since 2016, he has been with the Electronic Measurements and Signal Processing (EMS) group
at Technische Universität Ilmenau. His current research interests include the integrated circuit realization of sub-Nyquist signal acquisition schemes up to mm-Wave frequencies and investigating the properties of alternative analogue-mixed-signal acquisition architectures in integrated CMOS and Bi-CMOS technology for RADAR, GNSS and array signal processing applications.