Pre-Correlation GNSS Spoofing Mitigation

Antônio Pedro S. D. Carvalho[1], Felix Antreich[2]
[1] Centro de Guerra Acústica e Eletrônica da Marinha (CGAEM), Rio de Janeiro, Brazil
[2] Electronic Warefare Laboratory (LAB-GE), Aeronautics Institute of Technology (ITA), São José dos Campos, Brazil

***Abstract*— Global navigation satellite systems (GNSS) can be used to provide continuous, safe, and reliable positioning, speed measurement, and timing services. Generating or replicating GNSS signals, a spoofer can trick the receiver into believing it is located elsewhere and, unlike in the case of jamming, the user can not easily detect such an attack. A pre-correlation spoofing mitigation approach that considers an antenna array is presented. A loosely integrated receiver is considered with an anti-spoofing subsystem processing the signals received by an antenna array and afterwards passing a spoofing-free signal to a connected state-of-the-art single-antenna GNSS receiver. This approach is independent of the specific GNSS signals or constellations and applies to both open and authorized (military) services.**

***Keywords*— Spoofing, Pre-correlation, GPS, GNSS, Satellites**

I. Introduction

Jamming and spoofing represent a serious threat to all users of global navigation satellite systems (GNSS), but especially to safety-critical and military applications [1], [2]. GNSS receivers, which are vital for positioning nowadays and numerous applications, even though well-developed, can easily be deceived, experiencing interference known as spoofing. A spoofer transmits replicas of satellite signals to control the position, velocity, and time (PVT) estimation of a victim GNSS receiver and thus can manipulate the positioning and timing information presented to the user [3].

In contrast to jamming, for which the operation of the receiver is significantly distorted and positioning is even denied, a spoofing attack is very difficult to be detected by the GNSS receiver, especially if the launched spoofing attack is well-crafted and slowly introduced. Spoofing is considered a cyberattack as it can infiltrate systems through the GNSS receiver and manipulate the system's behavior [4]. Therefore, the detection and mitigation of spoofing attacks became an important field of research and development in the last years [5], [6]. The development of appropriate countermeasures is also one of the major topics addressed by the e-Navigation strategy launched by the International Maritime Organization (IMO) [6]. Additionally, also aeronautical and military applications have a high demand for spoofing mitigation, as incidents of attacks are increasingly encountered and the they are becoming more and more sophisticated [7].

In this work, in contrast to most of the works using antenna arrays that can be found in the literature, e.g. [8], a loosely integrated receiver is considered where the anti-spoofing subsystem is processing signals of the antenna array and then passes a spoofing-free signal to a connected state-of-the-art GNSS receiver with no specific features [5]. The only approach found in the literature that could also be applied in pre-correlation was presented in [9]. However, this proposed approach does not estimate the DOAs of the spoofing signals and its spatial filter (beamformer) is based on post-correlation signal processing and knowledge of the directions of arrival (DOAs) of the received satellite signals. In contrast, the approach that is presented in this work performs spoofing detection only pre-correlation and based on DOA estimation of the spoofing signals with subsequent mitigation by an adaptive beamformer which tries to amplify the received satellite signals as much as possible without knowledge of their DOAs.

Antônio Pedro S. D. Carvalh, pedro.antonio@marinha.mil.br; Felix Antreich, fean@ita.br. This work was partially supported by the Brazilian National Council for Scientific and Technological Development (CNPq) under grant 312394/2021-7 PQ-2.

II. Data Model

The discrete complex baseband GNSS signal is received by an antenna array of $m = 1, \ldots, M$ sensor elements. The received signal of the mth sensor element is

$$\begin{aligned}\mathbf{x}_m[k] = &\sum_{i=1}^{I} a_m(\varphi_i[k], \vartheta_i[k])\sqrt{P_i[k]} \\ &\quad (\mathbf{c}_i[k;\tau_i[k]] \odot \mathbf{d}[k;\nu_i[k],\phi_{\nu,i}[k]]) \\ &+ \sum_{q=1}^{Q} a_m(\varphi_q[k], \vartheta_q[k])\sqrt{P_q[k]} \\ &\quad (\mathbf{c}_q[k;\tau_q] \odot \mathbf{d}[k;\nu_q[k],\phi_{\nu,q}[k]]) \\ &+ \mathbf{n}_m[k], \end{aligned} \tag{1}$$

where

$$\begin{aligned}\mathbf{x}_m[k] = &[x_m(kN\,T_s), \ldots, x_m((kN+n)\,T_s), \\ &\ldots, x_m((kN+N-1)\,T_s)]^{\mathrm{T}} \in \mathbb{C}^{N\times 1} \end{aligned} \tag{2}$$

$$\begin{aligned}\mathbf{n}_m[k] = &[n_m(kN\,T_s), \ldots, n_m((kN+n)\,T_s), \\ &\ldots, n_m((kN+N-1)\,T_s)]^{\mathrm{T}} \in \mathbb{C}^{N\times 1} \end{aligned} \tag{3}$$

$$\begin{aligned}\mathbf{c}_i[k;\tau_i[k]] = &[c_i(\tau_i[k]), \ldots, \ldots, c_i(nT_s - \tau_i[k]), \\ &\ldots, c_i((N-1)T_s - \tau_i[k])]^{\mathrm{T}} \in \mathbb{R}^{N\times 1} \end{aligned} \tag{4}$$

$$\begin{aligned}\mathbf{c}_q[k;\tau_q[k]] = &[c_q(\tau_q[k]), \ldots, \ldots, c_q(nT_s - \tau_q[k]), \\ &\ldots, c_q((N-1)T_s - \tau_q[k])]^{\mathrm{T}} \in \mathbb{R}^{N\times 1} \end{aligned} \tag{5}$$

$$\begin{aligned}\mathbf{d}[k;\nu_i,\phi_{\nu,i}[k]] = &[\mathrm{e}^{\mathrm{j}\phi_{\nu,i}[k]}, \ldots, \mathrm{e}^{\mathrm{j}(2\pi\nu_i[k]nT_s+\phi_{\nu,i}[k])}, \\ &\ldots, \mathrm{e}^{\mathrm{j}(2\pi\nu_i[k](N-1)T_s+\phi_{\nu,i}[k])}]^{\mathrm{T}} \in \mathbb{C}^{N\times 1} \end{aligned} \tag{6}$$

$$\begin{aligned}\mathbf{d}[k;\nu_q,\phi_{\nu,q}[k]] = &[\mathrm{e}^{\mathrm{j}\phi_{\nu,q}[k]}, \ldots, \mathrm{e}^{\mathrm{j}(2\pi\nu_q[k]nT_s+\phi_{\nu,q}[k])}, \\ &\ldots, \mathrm{e}^{\mathrm{j}(2\pi\nu_q[k](N-1)T_s+\phi_{\nu,q}[k])}]^{\mathrm{T}} \in \mathbb{C}^{N\times 1}, \end{aligned} \tag{7}$$

with $\odot$ denoting the Hadamard-Schur product (element-wise multiplication), the sampling instant $n = 0, 1, \ldots, N-1$, the period $k = 0, 1, \ldots, K-1$, the sampling duration T_s, receiving $i = 1, \ldots, I$ satellite signals, receiving $q = 1, \ldots, Q$ spoofing signals, the pseudo-random binary sequences (PRBS) $c_i(t)$ and $c_q(t)$, the time-delays $\tau_i[k]$ and $\tau_q[k]$, the Doppler shifts $\nu_i[k]$ and $\nu_q[k]$, the Doppler phases $\phi_{\nu,i}[k]$ and $\phi_{\nu,q}[k]$, the mth element of the array steering vectors $a_m(\varphi_i[k], \vartheta_i[k])\mathbb{C}$ and $a_m(\varphi_q[k], \vartheta_q[k])\mathbb{C}$ with azimuth angles $\varphi_i[k] \in [-\pi, \pi]$ and $\varphi_q[k] \in [-\pi, \pi]$ and elevation angles $\vartheta_i[k] \in [0, \pi/2]$ and $\vartheta_q[k] \in [0, \pi/2]$, and the signal powers $P_i[k]$ and $P_q[k]$. In the present scenario the spoofer is receiving the same satellite signals as the receiver and thus is retransmitting the same PRBS in a amplify and forward fashion. Such a spoofing attack is called repeater or meaconing attack [2]. The antenna array response of the received satellite signals are

$$\mathbf{a}(\varphi_i[k], \vartheta_i[k]) = [a_1(\varphi_i[k], \vartheta_i[k]), \ldots a_m(\varphi_i[k], \vartheta_i[k]), \ldots, a_M(\varphi_i[k], \vartheta_i[k])]^{\mathrm{T}} \in \mathbb{C}^{M\times 1} \tag{8}$$

and the array response of the received spoofing signals are

$$\mathbf{a}(\varphi_q[k], \vartheta_q[k]) = [a_1(\varphi_q[k], \vartheta_q[k]), \ldots a_m(\varphi_q[k], \vartheta_q[k]), \ldots, a_M(\varphi_q[k], \vartheta_q[k])]^{\mathrm{T}} \in \mathbb{C}^{M\times 1}. \tag{9}$$

Furthermore, we assume $||\mathbf{c}_i[k; \tau_i[k]]||_2^2 = ||\mathbf{c}_q[k; \tau_q[k]]||_2^2 = N$, while in general $||\mathbf{c}_i[k; \tau_i[k]]||_2^2 \neq N, \forall \tau_i[k]$ and $||\mathbf{c}_q[k; \tau_q[k]]||_2^2 \neq N, \forall \tau_q[k]$ [1]. As the PRBS of all GNSS have good cross-correlation and autocorrelation properties, the the PRBS of different satellite are uncorrelated

$$\mathbf{c}_i^{\mathrm{T}}[k; \tau_i[k]]\mathbf{c}_p[k; \tau_p[k]] \approx 0, \quad \text{for } \; i \neq p \tag{10}$$

and thus also the spoofing signals are also uncorrelated with

$$\mathbf{c}_q^{\mathrm{T}}[k; \tau_q[k]]\mathbf{c}_p[k; \tau_p[k]] \approx 0, \quad \text{for } \; q \neq p. \tag{11}$$

Additionally, as the transmitter of the spoofing signals is assumed to have a distance of more than cT_c to the receiver, where c denotes the speed of light and T_c is the chip duration of the PRBS, the satellite signals and the spoofing signals with the same PRBS are all uncorrelated as well with

$$\mathbf{c}_i^{\mathrm{T}}[k; \tau_i[k]]\mathbf{c}_q[k; \tau_q[k]] \approx 0, \quad \text{for } \mathbf{c}_i[k, 0] = \mathbf{c}_q[k, 0], |\tau_i[k] - \tau_q[k]| > T_c. \tag{12}$$

The noise is complex Gaussian $\mathcal{CN}(0, \sigma_n^2)$ with

$$\mathrm{E}\left[||\mathbf{n}_m[k]||_2^2\right] = \sigma_n^2 \tag{13}$$

$$\mathrm{E}\left[\mathbf{n}_m^{\mathrm{H}}[k]\mathbf{n}_p[k]\right] = 0, \quad \text{with } \; m \neq p \tag{14}$$

$$\mathrm{E}\left[\mathbf{n}_m[k]\mathbf{n}_m^{\mathrm{H}}[k]\right] = \sigma_n^2 \mathbf{I}_N, \tag{15}$$

where $\mathbf{I}_N$ denotes a $N \times N$ identity matrix. In this work we consider a 7-element circular array with a central element. An antenna with 7 elements arranged in a circle is interesting due to its spatial resolution and radiation coverage. In general more elements could be added, which would enhance the performance of the later presented algorithms, but would also increase the complexity of the system. The antennas of the array are located in the x-y-plain with Cartesian coordinates

$$\mathbf{p}_1 = \left[p_{x,1}, p_{y,1}, p_{z,1}\right]^{\mathrm{T}} = [0,0,0]^{\mathrm{T}} \tag{16}$$

$$\mathbf{p}_2 = \left[p_{x,2}, p_{y,2}, p_{z,2}\right]^{\mathrm{T}} = \left[-\tfrac{\lambda}{4}, \tfrac{\sqrt{3}\lambda}{4}, 0\right]^{\mathrm{T}} \tag{17}$$

$$\mathbf{p}_3 = \left[p_{x,3}, p_{y,3}, p_{z,3}\right]^{\mathrm{T}} = \left[\tfrac{\lambda}{4}, \tfrac{\sqrt{3}\lambda}{4}, 0\right]^{\mathrm{T}} \tag{18}$$

$$\mathbf{p}_4 = \left[p_{x,4}, p_{y,4}, p_{z,4}\right]^{\mathrm{T}} = \left[\tfrac{\lambda}{2}, 0, 0\right]^{\mathrm{T}} \tag{19}$$

$$\mathbf{p}_5 = \left[p_{x,5}, p_{y,5}, p_{z,5}\right]^{\mathrm{T}} = \left[\tfrac{\lambda}{4}, -\tfrac{\sqrt{3}\lambda}{4}, 0\right]^{\mathrm{T}} \tag{20}$$

$$\mathbf{p}_6 = \left[p_{x,6}, p_{y,6}, p_{z,6}\right]^{\mathrm{T}} = \left[-\tfrac{\lambda}{4}, -\tfrac{\sqrt{3}\lambda}{4}, 0\right]^{\mathrm{T}} \tag{21}$$

$$\mathbf{p}_7 = \left[p_{x,7}, p_{y,7}, p_{z,7}\right]^{\mathrm{T}} = \left[-\tfrac{\lambda}{2}, 0, 0\right]^{\mathrm{T}}, \tag{22}$$

where λ is the wavelength of the carrier frequency $f_c = c/\lambda$ of the received satellite and spoofing signals. This work considers isotropic elements and we assume that the far-field and the narrowband assumption are fulfilled, such that the array response vectors are equivalent to the so-called steering vectors and include the relative phase shifts at the sensor elements

$$\mathbf{a}(\varphi[k], \vartheta[k]) = \begin{bmatrix} \mathrm{e}^{\mathrm{j}\frac{2\pi}{\lambda}(u_x[k]p_{x,1} + u_y[k]p_{y,1} + u_z[k]p_{z,1})} \\ \mathrm{e}^{\mathrm{j}\frac{2\pi}{\lambda}(u_x[k]p_{x,2} + u_y[k]p_{y,2} + u_z[k]p_{z,2})} \\ \vdots \\ \mathrm{e}^{\mathrm{j}\frac{2\pi}{\lambda}(u_x[k]p_{x,M} + u_y[k]p_{y,M} + u_z[k]p_{z,M})} \end{bmatrix} \tag{23}$$

with

$$\mathbf{u}[k] = \begin{bmatrix} \cos(\varphi[k])\cos(\vartheta[k]) \\ \sin(\varphi[k])\cos(\vartheta[k]) \\ \sin(\vartheta[k]) \end{bmatrix} = \begin{bmatrix} u_x[k] \\ u_y[k] \\ u_z[k] \end{bmatrix}. \tag{24}$$

Performing correlation between the received signal of antenna $m = 1$ with the $M-1$ signals received by all other antennas of the array yields

$$\mathbf{y}[k] = \begin{bmatrix} \frac{1}{N}\mathbf{x}_1^{\mathrm{H}}[k]\mathbf{x}_2[k] \\ \vdots \\ \frac{1}{N}\mathbf{x}_1^{\mathrm{H}}[k]\mathbf{x}_m[k] \\ \vdots \\ \frac{1}{N}\mathbf{x}_1^{\mathrm{H}}[k]\mathbf{x}_M[k] \end{bmatrix} \in \mathbb{C}^{M-1\times 1}. \tag{25}$$

Correlations are collected over K periods in the matrix

$$\mathbf{Y} = [\mathbf{y}[1] \cdots \mathbf{y}[k] \cdots \mathbf{y}[K]]^{\mathrm{T}} \in \mathbb{C}^{M-1\times K}. \tag{26}$$

Now, assuming that the DOAs of the received signals are constant during K observations and considering that $a_1(\varphi_i[k], \vartheta_i[k]) = 1$ the post-correlation signal in a matrix notation can be written as

$$\mathbf{Y} = \tilde{\mathbf{A}}\mathbf{P} + \tilde{\mathbf{A}}_s\mathbf{P}_s + \tilde{\mathbf{N}}, \tag{27}$$

where

$$\tilde{\mathbf{A}} = [\tilde{\mathbf{a}}(\varphi_1, \vartheta_1) \cdots \tilde{\mathbf{a}}(\varphi_I, \vartheta_I)] \in \mathbb{C}^{M-1\times I} \tag{28}$$

$$\tilde{\mathbf{A}}_s = [\tilde{\mathbf{a}}(\varphi_1, \vartheta_1) \cdots \tilde{\mathbf{a}}(\varphi_Q, \vartheta_Q)] \in \mathbb{C}^{M-1\times Q} \tag{29}$$

$$\tilde{\mathbf{a}}(\varphi, \vartheta) = [\tilde{a}_1(\varphi, \vartheta), \ldots, \tilde{a}_{M-1}(\varphi, \vartheta)]^{\mathrm{T}} \in \mathbb{C}^{M-1\times 1} \tag{30}$$

and

$$\tilde{a}_m(\varphi, \vartheta) = a_1^*(\varphi, \vartheta)a_m(\varphi, \vartheta). \tag{31}$$

[1] In many cases, e.g., in case of GPS C/A PRBS with bandwidth $B \geq 1.023$ MHz, it's assumed that $||\mathbf{c}_i[k; \tau_i[k]]||_2^2 \approx N, \forall \tau_i[k] \;\; \forall k$ and $||\mathbf{c}_q[k; \tau_q[k]]||_2^2 \approx N, \forall \tau_q[k] \;\; \forall k$.

Furthermore,

$$\mathbf{P} = \begin{bmatrix} P_1[1] & \dots & P_1[k] & \dots & P_1[K] \\ \vdots & & \vdots & & \vdots \\ P_i[1] & \dots & P_i[k] & \dots & P_i[K] \\ \vdots & & \vdots & & \vdots \\ P_I[1] & \dots & P_I[k] & \dots & P_I[K] \end{bmatrix} \in \mathbb{R}^{I\times K} \tag{32}$$

$$\mathbf{P}_s = \begin{bmatrix} P_1[1] & \dots & P_1[k] & \dots & P_1[K] \\ \vdots & & \vdots & & \vdots \\ P_q[1] & \dots & P_q[k] & \dots & P_q[K] \\ \vdots & & \vdots & & \vdots \\ P_Q[1] & \dots & P_Q[k] & \dots & P_Q[K] \end{bmatrix} \in \mathbb{R}^{Q\times K} \tag{33}$$

$$\begin{aligned}\tilde{\mathbf{N}} =& [\tilde{\mathbf{n}}[1]\cdots\tilde{\mathbf{n}}[k]\cdots\tilde{\mathbf{n}}[K]] \\ =& \begin{bmatrix} \tilde{n}_1[1] & \dots & \tilde{n}_1[k] & \dots & \tilde{n}_1[K] \\ \vdots & \vdots & \vdots & & \\ \tilde{n}_m[1] & \dots & \tilde{n}_m[k]\dots & \tilde{n}_m[K] & \\ \vdots & \vdots & \vdots & & \\ \tilde{n}_{M-1}[1] & \dots & \tilde{n}_{M-1}[k] & \dots & \tilde{n}_{M-1}[K] \end{bmatrix} \in \mathbb{C}^{M-1\times K}\end{aligned} \tag{34}$$

with

$$\begin{aligned}\tilde{\mathbf{n}}[k] =& \tfrac{1}{N}\textstyle\sum_{i=1}^{I} \tilde{\mathbf{a}}(\varphi_i,\vartheta_i)\sqrt{P_i[k]}\mathbf{n}_1^{\mathrm{H}}[k](\mathbf{c}_i[k;\tau_i[k]]\odot\mathbf{d}[k;\nu_i[k],\phi_{\nu,i}[k]]) \\ &+\tfrac{1}{N}\textstyle\sum_{i=1}^{I} \sqrt{P_i[k]}\bar{\mathbf{N}}[k](\mathbf{c}_i[k;\tau_i[k]]\odot\mathbf{d}[k;\nu_i[k],\phi_{\nu,i}[k]])^* \\ &+\tfrac{1}{N}\textstyle\sum_{q=1}^{Q} \tilde{\mathbf{a}}(\varphi_q,\vartheta_q)\sqrt{P_q[k]}\mathbf{n}_1^{\mathrm{H}}[k](\mathbf{c}_q[k;\tau_q[k]]\odot\mathbf{d}[k;\nu_q[k],\phi_{\nu,q}[k]]) \\ &+\tfrac{1}{N}\textstyle\sum_{i=q}^{Q} \sqrt{P_q[k]}\ \bar{\mathbf{N}}[k](\mathbf{c}_q[k;\tau_q[k]]\odot\mathbf{d}[k;\nu_q[k],\phi_{\nu,q}[k]])^* \\ &+\tfrac{1}{N}\bar{\mathbf{N}}[k]\mathbf{n}_1^*[k],\end{aligned} \tag{35}$$

where

$$\bar{\mathbf{N}}[k] = [\mathbf{n}_2[k]\cdots\mathbf{n}_m[k]\cdots\mathbf{n}_M - 1[k]]^{\mathrm{T}} \in \mathbb{C}^{M-1\times N}. \tag{36}$$

Finally, the spatial covariance matrix can be defined as

$$\begin{aligned}\mathbf{R}_{\mathbf{YY}} &= \mathrm{E}[\mathbf{Y}\mathbf{Y}^{\mathrm{H}}] \in \mathbb{C}^{M-1\times M-1} \\ &= \tilde{\mathbf{A}}\mathrm{E}[\mathbf{P}\mathbf{P}^{\mathrm{H}}]\tilde{\mathbf{A}}^{\mathrm{H}} + \tilde{\mathbf{A}}_s\mathrm{E}[\mathbf{P}_s\mathbf{P}_s^{\mathrm{H}}]\tilde{\mathbf{A}}_s^{\mathrm{H}} + \mathrm{E}[\tilde{\mathbf{N}}\tilde{\mathbf{N}}^{\mathrm{H}}],\end{aligned} \tag{37}$$

where the noise covariance matrix is

$$\begin{aligned}\mathrm{E}\left[\tilde{\mathbf{N}}\tilde{\mathbf{N}}^{\mathrm{H}}\right] =& \sum_{i=1}^{I}\frac{P_i\sigma_n^2}{N}\tilde{\mathbf{a}}(\varphi_i,\vartheta_i)\tilde{\mathbf{a}}^{\mathrm{H}}(\varphi_i,\vartheta_i) + \sum_{i=1}^{I}\frac{P_i\sigma_n^2}{N}\mathbf{I}_{M-1} \\ &+ \sum_{q=1}^{Q}\frac{P_q\sigma_n^2}{N}\tilde{\mathbf{a}}(\varphi_q,\vartheta_q)\tilde{\mathbf{a}}^{\mathrm{H}}(\varphi_q,\vartheta_q) + \sum_{q=1}^{Q}\frac{P_q\sigma_n^2}{N}\mathbf{I}_{M-1} \\ &+ \frac{(M-1)}{N^2}\sigma_n^4\mathbf{I}_{M-1}.\end{aligned} \tag{38}$$

Thus, the noise after correlating the signal received by antenna element $m = 1$ with the received signals of the other antennas of the array is still Gaussian but spatially colored. The signal-to-noise ratio (SNR) before this correlation for each received satellite or spoofing signal at each receive antenna is

$$\mathrm{SNR}_{\mathbf{x}} = \frac{P_{i/q}}{\sigma_n^2} \tag{39}$$

and is in the order of -20 to -15 dB. Considering (38) the SNR for each received satellite or spoofing signal after the correlation at each receive antenna is

$$\mathrm{SNR}_{\mathbf{y}} = \frac{P_{i/q}^2}{\frac{P_{i/q}\sigma_n^2}{N} + \frac{IP_i\sigma_n^2}{N} + \frac{QP_q\sigma_n^2}{N} + \frac{M-1}{N^2}\sigma_n^4}. \tag{40}$$

In case $P_i = P_q = P$ and $N >> M$

$$\begin{aligned}\mathrm{SNR}_{\mathbf{y}} \approx& \frac{P}{\frac{\sigma_n^2}{N} + \frac{I\sigma_n^2}{N} + \frac{Q\sigma_n^2}{N}} = \frac{P}{\sigma_n^2}\frac{N}{(1+I+Q)} = \\ &\mathrm{SNR}_{\mathbf{x}}\frac{N}{(1+I+Q)}.\end{aligned} \tag{41}$$

Thus, in the case of a one-sided bandwidth of the GNSS signals $B = 1.023$ MHz with $N = 2046$ and $I = Q = 13$, the $\mathrm{SNR}_{\mathbf{y}}$ is increased by nearly 19 dB with respect to the $\mathrm{SNR}_{\mathbf{x}}$. Consequently, correlating the signals received by antennas $m = 2,\dots,M$ with the signal received by antenna $m = 1$ achieves an increase of the effective SNR and provides reasonable conditions to analyse the DOAs of the received signals while no knowledge about the signals itself, besides their bandwidth and carrier frequency, is required.

III. DOA Estimation

In this section we discuss the DOA estimation of the spoofing signals in order to subsequently design a beamformer or spatial filter to spatially mitigate these spoofing signals and to provide a *clean* signal to a state-of-the-art single antenna GNSS receiver. In the following we assume a meaconing attack and thus the received sum power received from the DOA of the spoofing signals is much higher than the power received from each satellite, as the satellite signals are received from different DOAs.

A. Convential Beamformer (CBF)

A classic direction finding method is the so-called conventional beamformer (CBF) which estimates the received power in each direction to find the signals' DOAs from the maxima of the correlation output [10]

$$\begin{aligned}V_{CBF}(\varphi,\vartheta) =& \mathrm{E}\left[|\tilde{\mathbf{a}}^{\mathrm{H}}(\varphi,\vartheta)\mathbf{y}[k]|^2\right] \\ =& \tilde{\mathbf{a}}^{\mathrm{H}}(\varphi,\vartheta)\mathrm{E}\left[\mathbf{y}[k]\mathbf{y}^{\mathrm{H}}[k]\right]\tilde{\mathbf{a}}(\varphi,\vartheta) \\ =& \tilde{\mathbf{a}}^{\mathrm{H}}(\varphi,\vartheta)\mathbf{R}_{\mathbf{YY}}\tilde{\mathbf{a}}(\varphi,\vartheta).\end{aligned} \tag{42}$$

Using an estimate of the covariance matrix

$$\hat{\mathbf{R}}_{\mathbf{YY}} = \frac{1}{K}\mathbf{Y}\mathbf{Y}^{\mathrm{H}} \tag{43}$$

and evaluating the following cost-function

$$V_{CBF}(\varphi,\vartheta) = \tilde{\mathbf{a}}^{\mathrm{H}}(\varphi,\vartheta)\hat{\mathbf{R}}_{\mathbf{YY}}\tilde{\mathbf{a}}(\varphi,\vartheta). \tag{44}$$

The CBF represents a specific case of the maximum likelihood (ML) DOA estimator in the single source case. This is particular useful for our approach because in case of a meaconing attack the spoofing signals will arrive all from the same DOA and thus can be considered as one source with accumulated power of the different spoofing signals. Thus, one only needs to search for the global maximum of $V_{CBF}(\varphi,\vartheta)$ and the respective azimuth and elevation angles are the DOAs of the spoofing signals.

B. Results for DOA Estimation

In order to evaluate the performance of the CBF in a scenario with spoofing (meaconing) we consider a typical scenario with 13 received GPS satellites. The respective skyplot is depicted in Fig. 1 and shows the DOAs of the GPS satellites by their pseudo-random code numbers (PRNs) and the DOA of the spoofing signals (in red).

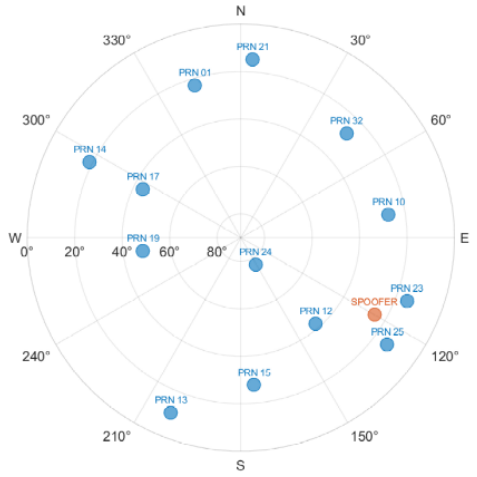

Fig. 1. Skyplot - azimuth and elevation angles of the GPS satellites and the spoofer .

The considered received power of the GPS satellites is listed in Tab. I. We also assume that the spoofing signals are amplified and they arrive at the victim GNSS receiver with a spoofing-to-signal ratio (SSR) of 3 dB in order to be considered for positioning by the victim receiver. In Fig. 2 the cost function $V_{CBF}(\varphi, \vartheta)$ is depicted for the simulated scenario. One can observe that the global maximum of the cost function (azimuth of 120º and elevation of 25º) clearly indicates the DOA of the spoofing signal.

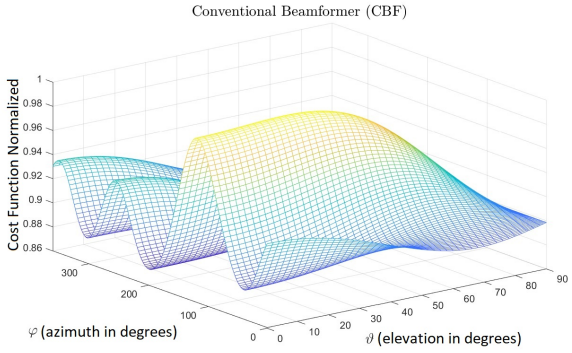

Fig. 2. Normalized cost function $V_{CBF}(\varphi, \vartheta)$.

In order to evaluate the root mean square error (RMSE) of estimating the azimuth and elevation angle of the spoofing signals with the CBF it's performed Monte Carlo simulations for different SSRs and number of periods K. The results are depicted in Fig. 3 and 4, respectively.

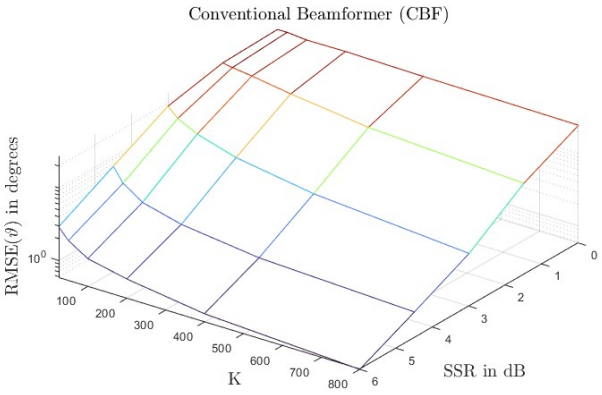

Fig. 3. RMSE of the azimuth angle of the spoofing signals.

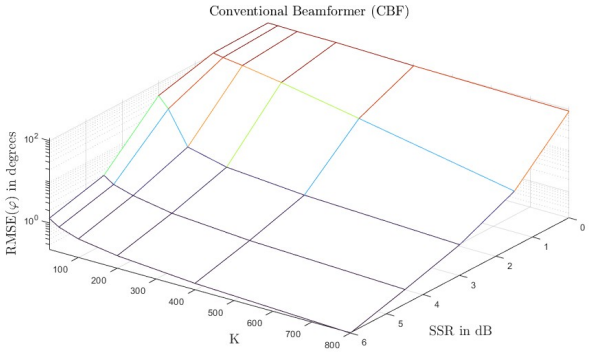

Fig. 4. RMSE of the elevation angle of the spoofing signals.

For a SSR higher than 3 dB and $K > 200$ reasonable good estimation of the DOAs of the spoofing signals can be achieved, as observed.

IV. Spoofing Mitigation

In order to mitigate the spoofing signals, we design a spatial filter or beamformer such that its output provides a *clean* signal to a standard single-antenna GNSS receiver without any specific spoofing countermeasures. The beamformer $\mathbf{w} \in \mathbb{C}^{M\times 1}$ filters the baseband signal received by antennas $m = 1, 2, \ldots M$ before correlation

$$\mathbf{z}^{\mathrm{T}}[k] = \mathbf{w}^{\mathrm{H}}\mathbf{X}[k]. \tag{45}$$

A. Beamformer

The beamformer uses the estimated DOAs of the spoofing signals to spatially mitigate them and additionally it incorporates constraints to amplify the satellite signals as much as possible for further processing. The beamformer ties to achieve a desired response over a specific region of azimuth φ and elevation ϑ angles. The covariance matrix of such a distributed source can be given as

$$\mathbf{Q} = \int_{\varphi_l}^{\varphi_u}\int_{\vartheta_l}^{\vartheta_u} \tilde{\mathbf{a}}(\varphi,\vartheta)\tilde{\mathbf{a}}^{\mathrm{H}}(\varphi,\vartheta)d\varphi d\vartheta \in \mathbb{C}^{M\times M}, \tag{46}$$

PRN	13	21	19	17	12	15	25	01	24	10	32	23	14
C/N_0 dB-Hz	42	45	42	45	42	45	42	45	42	45	42	45	42

TABLE I

CARRIER-TO-NOISE DENSITY RATIO C/N_0 IN DB-HZ OF THE GPS SATELLITES.

where the upper limit for the azimuth and elevation angles is given by φ_u and ϑ_u and the respective lower limits is given by φ_l and ϑ_l. Using the matrix $\mathbf{Q}$ the maximum power of the beamformer can be directed to the defined region by solving the problem

$$\max_{\mathbf{w}} \mathbf{w}^{\mathrm{H}}\mathbf{Q}\mathbf{w} \tag{47}$$

subject to

$$||\mathbf{w}||_2^2 = 1. \tag{48}$$

Furthermore, to suppress the spoofing signals the linear constraint

$$\mathbf{w}^{\mathrm{H}}\mathbf{a}(\varphi_s, \vartheta_s) = 1 \tag{49}$$

is introduced, where φ_s and ϑ_s are the azimuth and elevation angle of the spoofing signals. The problem given in (47), (48), and (49) can be solved by an eigenvalue problem including a linear null constraint. To solve the problem of maximizing (47) subject to (48) Lagrange multipliers can be used. The constraint is accommodated and so the corresponding Lagrangian function is

$$\mathcal{L}(\lambda, \mathbf{w},) = \mathbf{w}^{\mathrm{H}}\mathbf{Q}\mathbf{w} - \varrho(\mathbf{w}^{\mathrm{H}}\mathbf{w} - 1) - \varrho^*(\mathbf{w}^{\mathrm{H}}\mathbf{w} - 1) \tag{50}$$

with the Lagrangian multiplier $\varrho \in \mathbb{C}$. Now, the dual problem

$$\max_{\varrho} \max_{\mathbf{w}} \mathcal{L}(\varrho, \mathbf{w}) \tag{51}$$

can be solved. First, we take the derivative with respect to $\mathbf{w}^*$ and equate this to zero

$$\frac{\partial \mathcal{L}(\varrho, \mathbf{w})}{\partial \mathbf{w}^*} = \mathbf{Q}\mathbf{w} - \varrho\,\mathbf{w} - \varrho^*\mathbf{w} = \mathbf{0} \tag{52}$$

and we get

$$\mathbf{Q}\mathbf{w} = 2\mathrm{Re}\{\varrho\}\mathbf{w} = \lambda\mathbf{w}. \tag{53}$$

This is a so-called eigenvalue problem and thus the $\mathbf{w}^\star$ that maximizes (47) subject to (48) is given by the eigenvector $\mathbf{u}^\star$ related to the dominant eigenvalue $\lambda^\star$ of the eigendecomposition

$$\mathbf{Q} = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^{\mathrm{H}} \tag{54}$$

whereas $\mathbf{\Lambda} = \mathrm{diag}\{[\lambda_1, \lambda_2, \ldots, \lambda_M]^{\mathrm{T}}\} \in \mathbb{R}^{M\times M}$ contains the eigenvalues and $\mathbf{U} = [\mathbf{u}_1\ \mathbf{u}_2\ \cdots\ \mathbf{u}_M] \in \mathbb{C}^{M\times M}$ is a unitary matrix containing the related eigenvectors. In general, it can stated that

$$0 \leq \mathbf{w}^{\mathrm{H}}\mathbf{Q}\mathbf{w} \leq \lambda^\star \tag{55}$$

and

$$(\mathbf{w}^\star)^{\mathrm{H}}\,\mathbf{Q}\mathbf{w}^\star = \lambda^\star. \tag{56}$$

More generally, the eigenvalue problem can also have one or even several linear constraints. In the case of one constraint, the resulting eigenvalue problem can be given as

$$\mathbf{G}^{\mathrm{H}}\mathbf{Q}\mathbf{G} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^{\mathrm{H}} \tag{57}$$

whereas the projection matrix

$$\mathbf{G} = \mathbf{I}_M - \mathbf{a}(\varphi_s,\vartheta_s)\left(\mathbf{a}^{\mathrm{H}}(\varphi_s,\vartheta_s)\mathbf{a}(\varphi_s,\vartheta_s)\right)^{-1}\mathbf{a}^{\mathrm{H}}(\varphi_s,\vartheta_s) \tag{58}$$

and $\mathbf{V} = [\mathbf{v}_1\ \mathbf{v}_2\ \cdots\ \mathbf{v}_M] \in \mathbb{C}^{M\times M}$ is a unitary matrix containing the related eigenvectors. Here, $\mathbf{w}^\star$ that maximizes (47) subject to (48) and (49) is equivalent to $\mathbf{G}\mathbf{v}^\star$, where $\mathbf{v}^\star$ is the eigenvector related to the dominant eigenvalue $\lambda^\star$.

In practice it is very useful to broaden the null in the direction of the spoofing signals as much as possible due to possible errors in the DOA estimation of the spoofing signals. In order to broaden nulls one can introduce a Toeplitz taper matrix [10]

$$[\mathbf{T}]_{i,j} = \mathrm{sinc}(|i-j|\alpha) \in \mathbb{R}^{M\times M} \tag{59}$$

where $[\mathbf{T}]_{i,j}$ denotes the i,jth element of matrix $\mathbf{T}$ and $\alpha \in \mathbb{R}$ is a design parameter. Thus, the resulting eigenvalue problem can be given by

$$\left(\mathbf{G}^{\mathrm{H}}\mathbf{Q}\mathbf{G} \odot \mathbf{T}\right) = \tilde{\mathbf{V}}\mathbf{\Lambda}\tilde{\mathbf{V}}^{\mathrm{H}} \tag{60}$$

where $\tilde{\mathbf{V}} = [\tilde{\mathbf{v}}_1\ \tilde{\mathbf{v}}_2\ \cdots\ \tilde{\mathbf{v}}_M] \in \mathbb{C}^{M\times M}$ is a unitary matrix containing the related eigenvectors. Thus, $\mathbf{w}^\star$ that maximizes (47) subject to (48) and (49) with broadening the null according to $\mathbf{T}$ is equivalent to $\mathbf{G}\tilde{\mathbf{v}}^\star$, where $\tilde{\mathbf{v}}^\star$ is the eigenvector related to the dominant eigenvalue $\lambda^\star$.

B. Results for Spoofing Mitigation

Fig. 5 and 6 show the response of the beamformer in terms of the array gain of the antenna array without using the Toeplitz matrix $\mathbf{T}$, while Fig. 7 and 8 show the response with $\mathbf{T}$ and $\alpha = 1$. We choose $\varphi_l = 0$ (0°), $\varphi_u = 2\pi$ (360°), $\vartheta_l = 0.34$ (20°), and $\vartheta_u = 1.2217$ (70°).

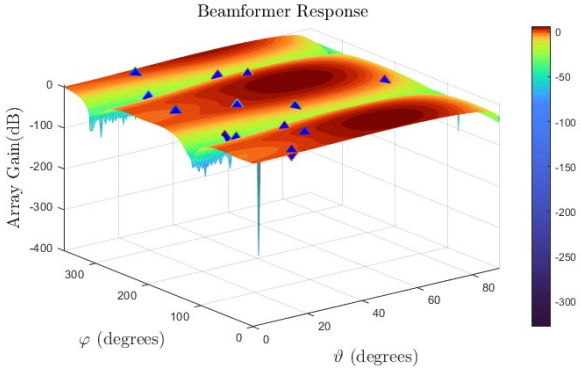

Fig. 5. Response of the beamformer without $\mathbf{T}$ in 3D.

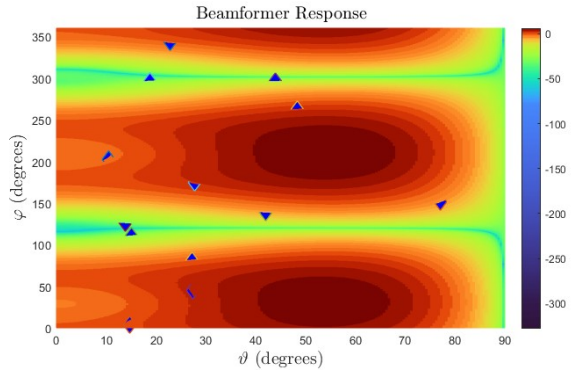

Fig. 6. Response of the beamformer without $\mathbf{T}$.

Fig. 5 reports a prominent attenuation denoted by the yellow and blue regions. It is also observed that such attenuation affects some satellites as well which are denoted by the blue triangles. A more detailed analysis can be performed by observing the azimuth and elevation profile shown in Fig. 6. Applying the Toeplitz matrix $\mathbf{T}$ with $\alpha = 1$, as shown in Fig. 7 and 8, results to a much lesser suppression of the satellite signals, except for the actual spoofing signal and the satellites with DOAs close to the spoofing signals. Note that the null in the direction of the spoofing signals is significantly widened by $\mathbf{T}$ with $\alpha = 1$ introducing robustness to DOA estimation errors by the CBF.

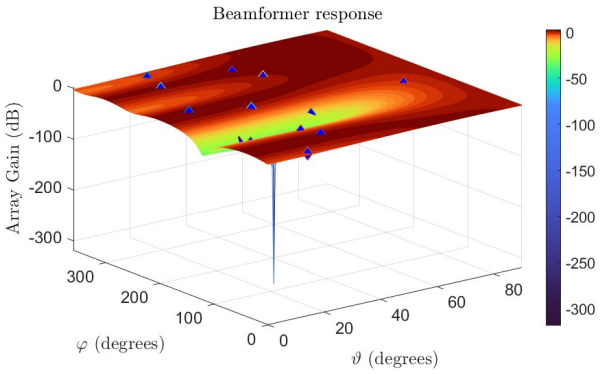

Fig. 7. Response of the beamformer with $\mathbf{T}$ in 3D.

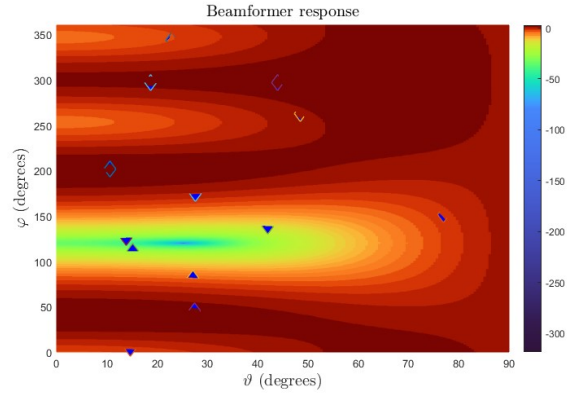

Fig. 8. Response of the beamformer with $\mathbf{T}$.

V. Conclusion

This work presented a pre-correlation spoofing mitigation approach based on a loose integration of an antenna array. The anti-spoofing subsystem detects spoofing attacks by DOA estimation of the spoofing signals and performs subsequent mitigation of the spoofing by adaptive spatial filtering. The CBF was introduced as a suitable DOA estimation algorithm. Simulation results show that for a SSR higher than 3 dB and $K > 200$ reasonable small RMSE for the azimuth and elevation angle of the spoofing signals can be achieved. The proposed beamformer achieves nulling the spoofing signals based on the DOA estimates provided by the CBF while trying to amplify as much as possible the GPS satellite signals. The proposed approach shows good performance in a realistic scenario and the beamformer manages to robustly mitigate a meaconing attack while providing GPS satellite signals with sufficient array gain to a state-of-the-art GNSS receiver.

This study, in addition to not adopting other specific anti-spoofing countermeasures, is different from most of the techniques that can be found in the literature. Most of the literature is based on post-correlation DOA estimation and requires knowledge of the spreading sequences of each satellite [6]. The only approach found in the literature that could also be applied in pre-correlation was presented in [9]. However, this proposed approach does not estimate the DOAs of the spoofing signals and its beamformer is based on post-correlation signal processing and knowledge of the DOAs of the received satellite signals.

References

[1] D. Egea-Roca, M. Arizabaleta-Diez, T. Pany, F. Antreich, J. A. López-Salcedo, M. Paonni, and G. Seco-Granados, "GNSS User Technology: State-of-the-Art and Future Trends," *IEEE Access*, vol. 10, pp. 39 939–39 968, 2022.

[2] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE*.

[3] J. R. Merwe, X. Zubizarreta, I. Lukcin, A. Rugamer, and W. F. Fraunhofer, "Classification of spoofing attack types," in *European Navigation Conference (ENC), Proceedings*, 2018, pp. 91–99.

[4] D. L. da Silva, R. Machado, O. L. Coutinho, and F. Antreich, "A Soft-Kill Reinforcement Learning Counter Unmanned Aerial System (C-UAS) With Accelerated Training," *IEEE Access*, vol. 11, pp. 31 496–31 507, 2023.

[5] A. Iliopoulos, C. Enneking, O. G. Crespillo, T. Jost, M. Appel, and F. Antreich, "Robust GNSS Ranging in the Presence of Repeater Signals," in *Proceedings of ION GNSS+ 2017*, Portland, OR , U.S.A., September 2017.

[6] M. Appel, A. Iliopoulos, F. Fohlmeister, E. P. Marcos, M. Cuntz, A. Konovaltsev, F. Antreich, and M. Meurer, "Experimental validation of gnss repeater detection based on antenna arrays for maritime applications," *CEAS Space Journal*, pp. 7–19, 2018.

[7] D. Goward, "Ukraine attacks changed russian gps jamming," *GPSWorld*, 2022. [Online]. Available: https://www.gpsworld.com/ukraine-attacks-changed-russian-gps-jamming/

[8] M. Meurer, A. Konovaltsev, M. Appel, and M. Cuntz, "Direction-of-arrival assisted sequential spoofing detection and mitigation," in *2016 International Technical Meeting (ION ITM), Monterey, Proceedings*, 2016, pp. 25–28.

[9] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A gnss structural interference mitigation technique using antenna array processing," in *IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM)*, Coruna, 2014, pp. 109–112.

[10] H. L. V. Trees, *Optimum Array Processing. Detection, Estimation and Modulation Theory, Part IV*. Wiley Interscience, 2002.