STAP Techniques for GNSS Jamming and Spoofing Mitigation: Experimental Analysis

Noori BniLam[†,*], Samah Chazbeck[‡], Xurxo Otero Villamide[†], Luciano Musumeci[†], Raffaele Fiengo[‡], Paolo Crosta[†]
[†]ESA/ESTEC, Keplerlaan 1, 2201 AZ Noordwijk, the Netherlands.
[‡]National Instrument NI-EMERSON.
[*]noori.bnilam@ext.esa.int

***Abstract*—In this paper, we present an experimental analysis of multiple jamming and spoofing mitigation techniques. The techniques have been applied to real-life jamming and spoofing attacks on Global Navigation Satellite Systems (GNSS) services. The experimental setup constitutes Uniform Rectangular Array (URA) that was connected to fully coherent 4 RF-chains (to convert the RF signals to the base-band IQ samples). Various mitigation techniques that depend on the spatial-only diversity and the Space-Time Adaptive Processing (STAP) have been adopted. The spatial-only techniques are the Eigen subspace decomposition and the Minimum Variance Distortionless Response (MVDR); while the STAP techniques are the Power Inversion (PI-STAP) and the Linear Constraint (LC-STAP). The results show that STAP techniques have outperformed spatial-only techniques; furthermore, LC-STAP has provided the most jamming and spoofing signal attenuation compared to the other three techniques.**

***Index Terms*—Space-Time Adaptive Processing (STAP), Array antennas, Controlled Reception Pattern Antennas, CRPA, GNSS, GPS, Galileo, Resilient Navigation, Jamming and spoofing attacks, Jammertest in Norway.**

I. Introduction

Over the past decades, Global Navigation Satellite Systems (GNSS) have become the cornerstone to many industries that facilitate our modern life style. Therefore, GNSS technology has been adopted by many systems such as the United States Global Navigation System (GPS), the European Galileo, the Russian Global Navigation Satellite System (GLONASS) and the Chinese BeiDou Satellite System (BDS) [1]. As we become more dependent on this technology, we also become more vulnerable to its limitations. For example, the satellites of these systems are mainly located in the Medium Earth Orbit (MEO), which is at an altitude of approximately 20,000 km; therefore, due to the long communication link, the signal-to-noise ratio (SNR) of the received signals is very low. As a result, GNSS services degrade in indoor, urban, canyons, and forest-like environments. Furthermore, GNSS systems share the same frequency bands, therefore, GNSS signals are susceptible to interference signals (including spoof attacks) [2]–[4]. Accordingly, several solutions have been proposed in the literature to overcome the GNSS limitations using array antennas [5].

The ability of exploiting the spatial dimensions has allowed array antennas to be exploited in various applications, e.g., multipath and interference mitigation; spatial diversity; and localization [6]–[10]. Consequently, over the past years, array antennas have been deployed in GNSS receivers either to provide a spatial filter or to improve the SNR level using beamforming techniques.

In this paper, we exploit the array antenna system to protect GNSS signals against jamming and spoofing attacks. The paper presents an experimental analysis of four beamforming techniques to mitigate the effect of the jamming and spoofing signals on the genuine GNSS signals. The experimental data sets have been collected during the jammertest 2024 campaign in Norway [11]. The results of two elaborate scenarios have been considered, the first scenario represents a 3 simultaneous jammers attack for 10 minutes (the jammers were placed 50 meters away around the receiver). The second scenario, on the other hand, represents a GPS spoofing attack for 20 minutes, both the spoofer and the receiver were dynamic and the spoofing location was static.

In the following, the experimental analysis is presented; followed by the paper's conclusions; but first we present, in the following section, the adopted array signal processing techniques.

II. Array Signal Processing

In this section, we present a thorough theoretical background of the array signal model and the interference mitigation techniques.

A. Signal Model

Assume a GNSS signal impinges on an array antenna system that is constructed of N antenna elements. Then the received sampled signal vector, at the time index k, can be expressed as

$$\mathbf{x}(k) = [x_1(k) \dots x_n(k) \dots x_N(k)]^T, \tag{1}$$

in which

$$x_n(k) = r_m s_m(k - \tau_m) e^{i(2\pi \Delta f_m k + \Theta_m)} e^{i\psi_n(\phi,\theta)} + \Omega_n(k), \tag{2}$$

where $()^T$ is the transpose notation, r_m and s_m are respectively the received signal's amplitude and the transmitted GNSS signal from the m[th] satellite. s_m is a CDMA signal

that exploits the Direct Sequence Spread Spectrum (DS-SS) technique, which can be expressed as

$$s_m(k) = d_m(k)c_m(k), \tag{3}$$

where $c_m(k)$ is the spreading waveform or Pseudo-Random Number (PRN) of the m$^{\text{th}}$ satellite. The symbols $d_m(k)$ form the navigation message, which contains all the essential information to calculate the receiver position. It is important to mention that the data rates of the two data sequences are not equal, yet they are synchronized. The navigation data symbol period T_s comprises p chips[1], each of duration T_c, i.e., $p = T_s/T_c$.

Δf_m, in (2), is the frequency offset between the m$^{\text{th}}$ satellite and the receiver (including the Doppler frequency shift); $\Omega_n(k)$ is the identically independently distributed (iid) complex-valued Gaussian noise; τ_m is the time delay of the received sample $s_m(k)$ and Θ_m is the carrier phase. Finally, $\psi_n(\phi, \theta)$, in (2), is the phase difference between the n$^{\text{th}}$ element in the array antenna and a reference point in space. Clearly, $\psi_n(\phi, \theta)$ is a function of ϕ and θ, where $\{\phi \in \mathbb{R} : -\pi \leq \phi \leq \pi\}$ is the azimuth angle and $\{\theta \in \mathbb{R} : 0 \leq \theta \leq \frac{\pi}{2}\}$ is the elevation angle. Accordingly, the phase response can be expressed as follows

$$\psi_n(\phi, \theta) = \frac{2\pi}{\lambda} \begin{bmatrix} p_n^x & p_n^y & p_n^z \end{bmatrix} \begin{bmatrix} \cos(\phi)\cos(\theta) \\ \sin(\phi)\cos(\theta) \\ \sin(\theta) \end{bmatrix}, \tag{4}$$

where λ is the operational wavelength and p_n^x, p_n^y and p_n^z are the positions of the n$^{\text{th}}$ antenna element (in x, y and z axes) with respect to a specific point in space.

In array antenna systems, the received signal can be expressed as follows [12]

$$y(k) = \mathbf{w}^T \mathbf{x}(k) \ , \tag{5}$$

the complex vector $\mathbf{w} \in \mathbb{C}^{N\times 1}$ controls the look direction of the array antenna. The array antenna output power can be given by

$$|y|^2 = \mathbf{w}^H \mathbf{R}_{xx} \mathbf{w} \ , \tag{6}$$

in which $\mathbf{R}_{xx}$ is the received signals covariance matrix and it is given by

$$\mathbf{R}_{xx} \approx \frac{1}{K} \sum_k \mathbf{x}(k)^H \mathbf{x}(k) \ , \tag{7}$$

where K is the number of samples (the sample size) that are used to construct $\mathbf{R}_{xx}$ and $()^H$ is the conjugate transpose operator. It is worth mentioning that (7) is the approximation of $\mathbf{R}_{xx}$ for a finite sample size.

The covariance matrix $\mathbf{R}_{xx}$ is a positive definite Hermitian matrix, consequently, it can be diagonalized by a nonsingular orthogonal transformation matrix $\mathbf{Q}$ as follows [13]

$$\mathbf{Q}^H \mathbf{R}_{xx} \mathbf{Q} = \mathbf{\Lambda} \ , \tag{8}$$

where $\mathbf{\Lambda} \in \mathbb{R}^{N\times N}$ is a diagonal matrix, its diagonal elements are positive real eigenvalues $\lambda_1, \ldots \lambda_n, \ldots \lambda_N$, and the corresponding eigenvectors are:

$$\mathbf{Q} = [\mathbf{e}_1, \mathbf{e}_2, \ldots \mathbf{e}_N] \ , \tag{9}$$

where $\mathbf{e}_n \in \mathbb{C}^{N\times 1}$ is the n$^{\text{th}}$ eigenvector that corresponds to the n$^{\text{th}}$ eigenvalue λ_n. If the eigenvalues are sorted from the smallest to the largest, matrix $\mathbf{Q}$ can be divided into two subspace matrices such that $\mathbf{Q} = [\mathbf{Q}_\zeta \mathbf{Q}_r]$. The first subspace matrix $\mathbf{Q}_\zeta$ is defined as the noise subspace matrix and it is composed of $N - D$ eigenvectors associated with the channels thermal noise, the relating eigenvalues are $\lambda_1 \approx \lambda_2 \approx \ldots \lambda_{N-D} \approx \sigma_\zeta^2$. D is the number of received signals and σ_ζ^2 is the noise variance. The second subspace matrix $\mathbf{Q}_r$ is defined as a signal subspace matrix and it is composed of D eigenvectors that are associated with the received signals.

B. Interference Mitigation Techniques

Four different interference and spoofing mitigation techniques have been adopted in this paper, the first two depend only on the spatial diversity of the received signals; while the other two methods depend on the Space-Time Adaptive Processing (STAP) techniques.

1) Subspace-based interference mitigation: it has been proven that the weight vector $\mathbf{w}$ can be substituted by an eigenvector, of the covariance matrix $\mathbf{R}_{xx}$, to provide beamforming capability [14]. Thus, the optimal weight vector $\mathbf{w}^{opt}$ that corresponds to a received signal is equal to the eigenvector $\mathbf{e}_N$ that is associated with the largest eigenvalue λ_N. Hence, $\mathbf{e}_N$ contains the appropriate phase response that is associated with the AoA parameter of the received signal [14]. Accordingly, in order to mitigate the received jamming signals (above noise floor), the selected weight vector $\mathbf{w}$ can be equal to the eigenvector that is associated with the noise subspace (i.e., the egien vector that is associated with the lowest eigenvalue). Therefore, the weight can be expressed as

$$\mathbf{w} = \mathbf{e}_1 \ . \tag{10}$$

2) MVDR interference mitigation: the Minimum Variance Distortionless Response (MVDR) depends on minimizing the output power in (6) while passing the signal, that impinges at the look direction, undisturbed. Accordingly, the weight vector of the MVDR beamformer can be expressed as

$$\mathbf{w} = \frac{\mathbf{R}_{xx}^{-1} \mathbf{c}^*(\theta, \phi)}{\mathbf{c}^H(\theta, \phi) \mathbf{R}_{xx}^{-1} \mathbf{c}(\theta, \phi)} \ , \tag{11}$$

where $()^*$ is the conjugate operator and $\mathbf{c}(\theta, \phi)$ is the array steering vector and it is equal to

$$\mathbf{c}(\theta, \phi) = [c_1(\theta, \phi) \ldots c_n(\theta, \phi) \ldots c_N \theta, \phi)]^T \ , \tag{12}$$

in which

$$c_n(\theta) = e^{i\psi_n(\phi,\theta)} \ . \tag{13}$$

In our analysis, the zenith angles were considered as the look direction of the MVDR beamformer (i.e., $\phi = 0$ and $\theta = \frac{\pi}{2}$).

3) STAP interference mitigation: Space-Time adaptive antenna for GNSS receiver is an array antenna of which the signal from every antenna in the array is delayed by a

[1]The PRN data sequence is often referred to as chips to distinguish them from the navigation message bits.

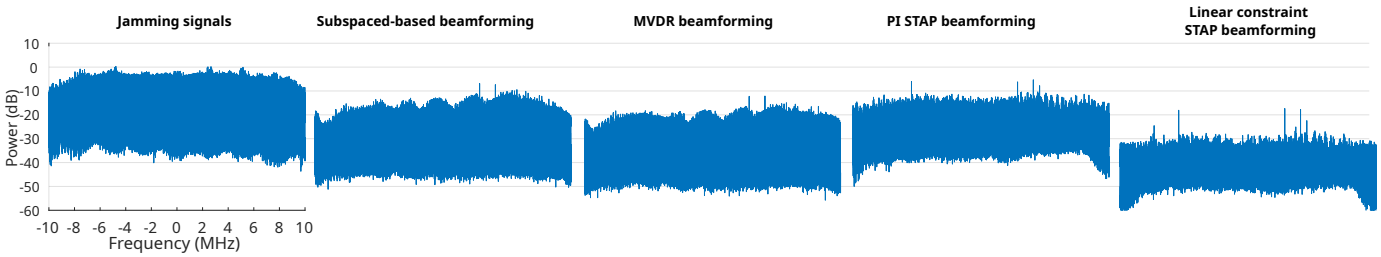

Fig. 1: The frequency spectrum of the jamming signals before and after interference mitigation process using various beamforming techniques. It is clear that LC-STAP has provided the most jamming mitigation of approximately 30dB of jamming suppression.

tapped delay line (i.e. every antenna is followed by a finite impulse response FIR filter). All the delayed signals will be multiplied by a weight vector and summed to provide the desired response.
This adaptive processing can be used usually to process a wideband signals [15]. Nonetheless, this technique can also be used to preserve the desired signal while suppressing the interference signals [16]. The STAP model constitutes N antenna elements and J tapped delay line. Therefore, the received signal vector in (1) will be transformed to a matrix of $N \times J$ size; and the received signal covariance matrix will be of the size $NJ \times NJ$.
For Power Inversion (PI-STAP), we used the same MVDR response in (11) with a steering vector equals to

$$\mathbf{c}(\theta, \phi) = [1\, 0 \ldots 0]^T \ , \tag{14}$$

where $\mathbf{c} \in \mathbb{R}^{NJ \times 1}$.
For Linear Constraint (LC-STAP) the steering vector can be expressed as follows [17]

$$\mathbf{c}(\theta, \phi) = [1_0 \ldots 1_{N-1}\, 0 \ldots 0]^T \ . \tag{15}$$

For more details regarding the full signal model of the STAP technique, the reader is referred to [15]. In our analysis, every signal from the array antenna was delayed 20 times, therefore, the tapped delay line size was 20.

III. Experimental analysis

In 2024, we have participated in the elaborate jammertest campaign in Norway. During the 5 days of the test campaign many scenarios were executed; for instances multiple jammers, high and low power jamming, meaconing and spoofing the GNSS signals, static and dynamic conditions were considered. In this section, we will present the experimental setup and the experimental results, successively.

A. Experimental setup and processing platforms

A record and playback system consists of 4 synchronized Vector Signal Transceivers (VST) to acquire GNSS signals from 4 RF ports; the local oscillators (LO) of the VSTs were shared from a common LO source to ensure the phase and amplitude coherency among the RF ports and across the recorded bandwidth. The deployed VSTs system was connected to 4 antenna elements that were distributed as a square with a side length of 10 cm. The recorded bandwidth, the sampling rate and the center frequency were respectively 32 MHz, 40 Msps and 1575.42 MHz.
All the array signal processing has been conducted offline using MATLAB implementation.

B. Experimental scenarios and analysis

Two data sets are presented in this paper, the first scenario represents 10 minutes of a 3 simultaneous jamming attack (the non synchronized jammers were placed 50 meters away around the receiver). The second scenario, on the other hand, represents a GPS spoofing attack for 20 minutes, where the spoofer and the receiver were dynamic and the spoofing location was static.
For the jamming scenario, we have exploited the Multi-GNSS SDR Receiver (FGI-GSRx), which is based on the implementation provided by Borre et al. [18]. The FGI-GSRx MATLAB software is capable of offering a positioning solution with multiple GNSS signals; in our implementation, we have considered GPS L1 and Galileo E1b signals.
In order to extract the observables in the spoofing scenario, we have used the GNSS-SDR open source software [19].

1) Three jammers: in this scenario, we present the analysis of 5 minutes of the collected data. The data set starts with a clean signals, afterwards (approximately after 80 seconds) the jamming signals were started.
Figure 1 shows the frequency spectrum of the jamming signals and the 4 adopted beamforming techniques. It is clear that the LC-STAP has provided the most jamming mitigation with a jamming attenuation of approximately 30dB. Figure 2 shows the Carrier-to-Noise ratio (C/N_0) of the investigated techniques for GPS L1 and Galileo E1b signals. The figure reveals that all the techniques have suffered of a drop in the C/N_0 values for all the acquired GNSS signals at the start of the jamming signals. However, the techniques that depend on spatial-only diversity show a larger drop than the STAP techniques. Two important points that are worth mentioning: 1) the jamming channel has lost the track of the GNSS signal completely, while all the 4 techniques have managed to keep the tracking loop running; 2) the beamforming techniques have been deployed from the start, therefore, there is a clear difference in the amount of satellites' signals that have been acquired by each technique.
Finally, tables I and II shows clearly that the LC-STAP technique has provided the best 3D performance. The Subspace-

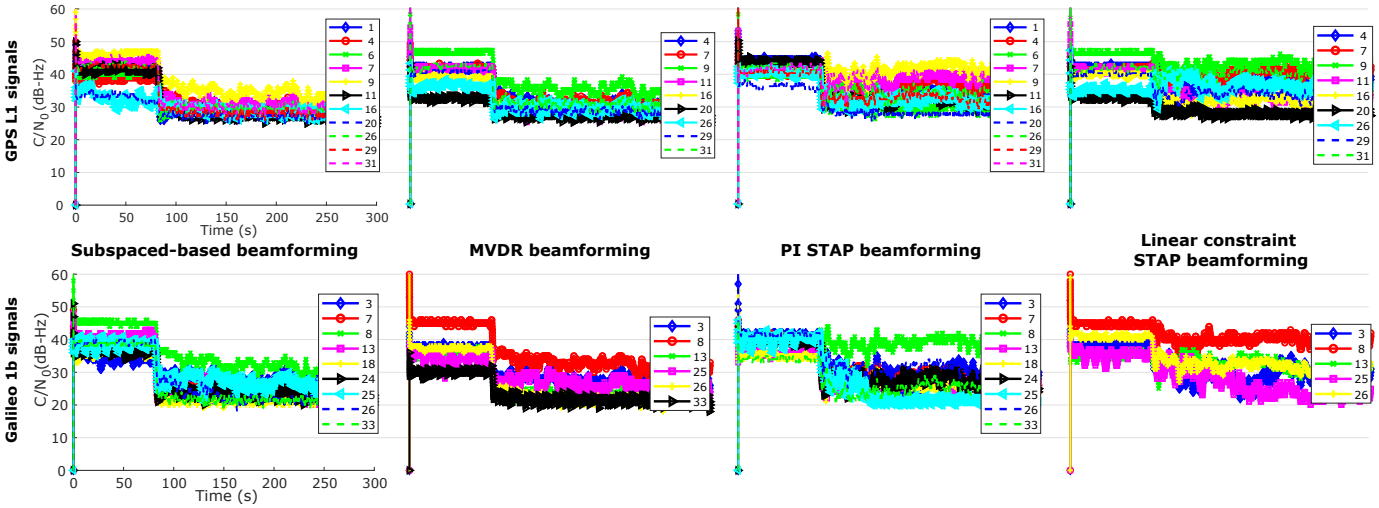

Fig. 2: The C/N_0 values of the investigated techniques for GPS L1 and Galileo E1b signals, it is clear that all the techniques have suffered of a drop in the C/N_0 values for all the acquired GNSS signals at the start of the jamming signals, however, the techniques that depend on spatial-only diversity show a larger drop than the STAP techniques.

TABLE I: 2D Estimation error of the jamming scenario using Single Point Positioning (SPP).

Deployed technique	50% error (m)	95% error (m)
Subspace	nan	nan
MVDR	8.8	105.0
PI STAP	3.59	7.9
LC STAP	5.3	11.0

TABLE II: 3D Estimation error of the jamming scenario using SPP.

Deployed technique	50% error (m)	95% error (m)
Subspace	nan	nan
MVDR	17.9	183.2
PI STAP	19.3	34.9
LC STAP	13.3	28.6

based technique, on the other hand, has failed to provide a position estimate.

2) GPS spoofing: this spoofing scenario has lasted for 20 minutes; during the first 10 minutes, the spoofer and the receiver were static, afterwards, the spoofer and the receiver have become dynamic. The spoofer objective is to keep the receiver position static at the start location. The spoofing device was transmitting GPS-only signals.

Figure 3 shows the receiver positions for the authentic GNSS navigation (the reference trajectory in black), the spoofed receiver (in red), the PI-STAP (in green) and the LC-STAP (in blue). It is clear that the spoofed receiver position shows that the dynamic receiver was static. Furthermore, the PI-STAP technique has maintained a dynamic position for a short time before it has lost the tracking of the satellites' signals. The LC-STAP, on the other hand, has lost the track for a small part of the trajectory but, after a short while, it has managed to maintain the dynamic position of the receiver correctly.

Fig. 3: The receiver positions for the authentic GNSS navigation (the reference trajectory in black), the spoofed receiver (in red), the PI-STAP (in green) and the LC-STAP (in blue).

IV. Conclusions

In this paper, we have presented an experimental analysis of multiple jamming and spoofing mitigation techniques. Two data sets were presented, the first scenario represents 10 minutes of a 3 simultaneous jamming attack (the jammers were placed 50 meters, away around the receiver); while the second scenario represents a GPS spoofing attack for 20 minutes, where the spoofer and the receiver were dynamic and the spoofing location was static. The experimental results reveal the following:

i. using STAP techniques can increase the attenuation of the jamming signals compared with the spatial diversity techniques. However, this comes with a very high computational cost. In our case, we have achieved 30dB of attenuation using 4 antennas and a tapped delay line of 20 taps.

ii. the LC-STAP outperformed the other techniques, with 95% 3D error of 28m. Furthermore, it has maintained the dynamic positioning during the spoofing attacks, while all the other techniques have failed.

Disclaimer

The content of the present article reflects solely the authors' view and by no means represents the official ESA view.

References

[1] C. J. Hegarty, "GNSS signals - An overview," in *2012 IEEE International Frequency Control Symposium, IFCS 2012, Proceedings*, 2012, pp. 87–93.

[2] T. G. Reid, A. M. Neish, T. Walter, and P. K. Enge, "Broadband leo constellations for navigation," *NAVIGATION: Journal of the Institute of Navigation*, vol. 65, no. 2, pp. 205–220, 2018.

[3] J. J. Khalife and Z. M. Kassas, "Receiver design for doppler positioning with leo satellites," in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2019, pp. 5506–5510.

[4] N. BniLam and P. Crosta, "Resilient gnss coarse positioning based of angle of arrival estimates," in *2024 11th Workshop on Satellite Navigation Technology (NAVITEC)*. IEEE, 2024, pp. 1–5.

[5] N. BniLam, F. Principe, and P. Crosta, "Large array antenna aperture for gnss applications," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 60, no. 1, pp. 675–684, 2023.

[6] N. BniLam, S. Chazbeck, R. Fiengo, and P. Crosta, "Two stages beamforming technique for gnss applications," in *the European Navigation Conference*. MDPI, 2024.

[7] C. Fernández-Prades, J. Arribas, and P. Closas, "Robust gnss receivers by array signal processing: Theory and implementation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1207–1220, 2016.

[8] N. BniLam, D. Joosens, M. Aernouts, J. Steckel, and M. Weyn, "Loray: Aoa estimation system for long range communication networks," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 2005–2018, 2020.

[9] N. BniLam, G. Ergeerts, D. Subotic, J. Steckel, and M. Weyn, "Adaptive probabilistic model using angle of arrival estimation for iot indoor localization," in *2017 International conference on indoor positioning and indoor navigation (IPIN)*. IEEE, 2017, pp. 1–7.

[10] N. Bnilam, D. Joosens, R. Berkvens, J. Steckel, and M. Weyn, "Aoa-based localization system using a single iot gateway: An application for smart pedestrian crossing," *IEEE Access*, vol. 9, pp. 13 532–13 541, 2021.

[11] Norwegian Public Roads Administration, Norwegian Communications Authority, Norwegian Defence Research Establishment, Norwegian Metrology Service, Norwegian Mapping Authority, Norwegian Space Agency, and Testnor, "Jammertest 2024," https://jammertest.no/, 2024, accessed: 2025-02-24.

[12] R. A. Monzingo, R. L. Haupt, and T. W. Miller, "Introduction to Adaptive Arrays, Scitech Pub," 2011.

[13] H. Krim and M. Viberg, "Two Decades of Array Signal Processing Research: The Parametric Approach," *IEEE signal processing magazine*, vol. 13, no. 4, pp. 67–94, 1996.

[14] N. Bnilam, E. Tanghe, J. Steckel, W. Joseph, and M. Weyn, "Angle: Angular location estimation algorithms," *IEEE access*, vol. 8, pp. 14 620–14 629, 2020.

[15] N. BniLam, J. Steckel, and M. Weyn, "2d angle of arrival estimations and bandwidth recognition for broadband signals," in *2017 11th European Conference on Antennas and Propagation (EUCAP)*. IEEE, 2017, pp. 2041–2045.

[16] Z. Hongwei, L. Baowang, and F. Juan, "Interference suppression in gnss receiver using space-time adaptive processing," in *2011 IEEE 3rd International Conference on Communication Software and Networks*. IEEE, 2011, pp. 381–385.

[17] O. L. Frost, "An algorithm for linearly constrained adaptive array processing," *Proceedings of the IEEE*, vol. 60, no. 8, pp. 926–935, 1972.

[18] K. Borre, I. Fernández-Hernández, J. A. López-Salcedo, and M. Z. H. Bhuiyan, *GNSS software receivers*. Cambridge University Press, 2022.

[19] C. Fernandez-Prades, P. Closas, and M. Navarro, "GNSS-SDR: An Open Source Tool for Global Navigation Satellite Systems Signal Processing," *Proceedings of the 6th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, pp. 153–157, 2011.