Proceedings of the 5th Conference of the Society for the Advancement of Positioning Technologies (SAPT), Osaka, Japan, Sep. 1, 2023

DOA Estimation and Removal of GNSS Spoofing Using MUSIC Algorithm with Nullspace Projection

Maumu YONEYAMA and Toshiaki TSUJII
Osaka Metropolitan University

Abstract GNSS (Global Navigation Satellite System) is widely used in various aspects of our daily life. In the near future, GNSS is expected to be used more in situations where reliability is important. GNSS signals, however, are susceptible to unwanted radio waves, resulting in poor positioning performance. The antenna array, a spatial-domain methodology, has been studied as an effective countermeasure to this problem. In this paper, we applied the Nullspace Projection method to the DOA (direction of arrival) by MUSIC (MUltiple SIgnal Classification) algorithm and validated its efficacy through the actual spoofing experiment. As a result, the Nullspace Projection can remove the spoofing signal, i.e., the signal in a specific direction from the DOA estimation result.

1 Introduction

GNSS (Global Navigation Satellite System) such as GPS is currently used in various aspects of society. In the near future, GNSS is expected to be used more and more in situations where reliability is important, such as in the automatic operation of ships, aircraft, automobiles, and Advanced Air Mobility (AAM). However, the signal strength of the signals used for satellite positioning is so weak that unwanted radio waves can easily cause serious problems such as deteriorating positioning accuracy, disabling positioning, and hijacking position information. In this research, we assume the spoofing and the multipath as unwanted radio waves (Fig.1). The multipath is a problem in which positioning signals from GNSS satellites are reflected or diffracted by objects, resulting in multiple reception paths, which deteriorates positioning accuracy. The spoofing, the other unwanted signal, is a malicious imitation of signals that interferes with normal positioning and hijacks location information. Compared to jamming, which is a simple jamming by strong radio waves, the spoofing requires far more complex procedures such as signal generation, but it is pointed out that recent developments in the field of electronics have reduced the technical hurdles. Especially, the emergence of software-defined radio (SDR), which can change the frequency and modulation scheme of the radio waves they transmit and receive based on software, has been noted. As a matter of fact, C4ADS reports the spoofing activities affecting civilian GNSS receivers [1]. One idea to counter these unwanted radio waves is the use of array antennas as a spatial-

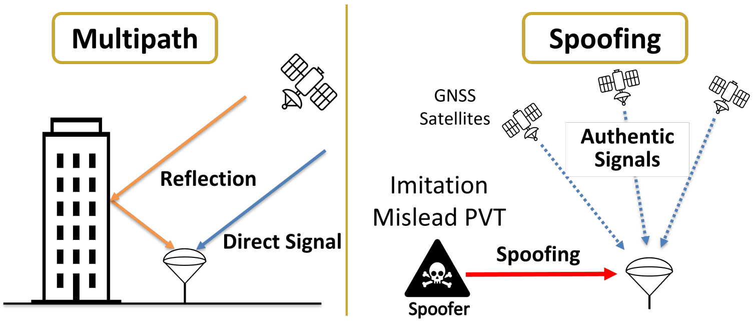

Fig. 1: Weakness in GNSS (Left：Multipath, Right：Spoofing)

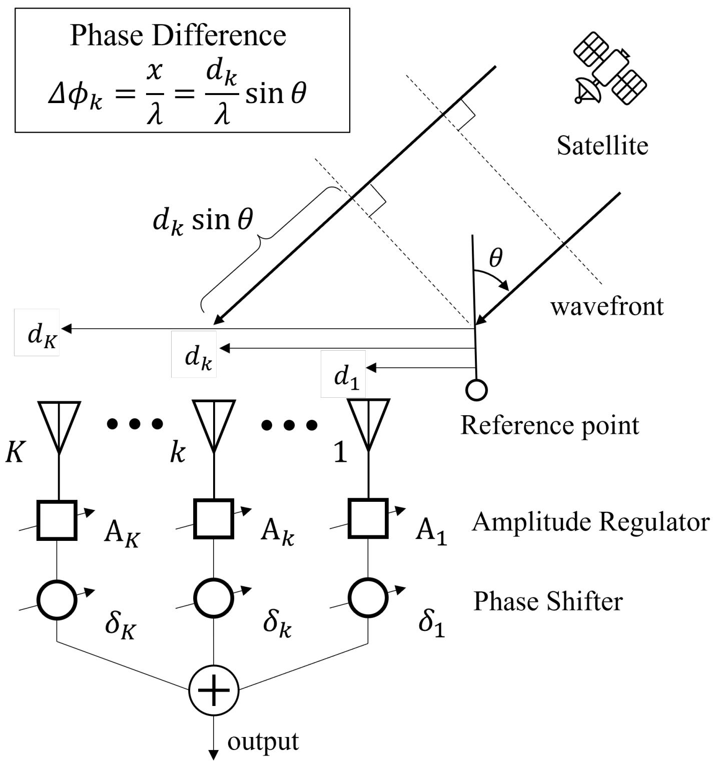

Fig. 2: The principle of antenna array

domain solution [2][3]. The characteristic of array antennas, which will be described later, is their ability to control a radiation pattern, and this property can be used to improve the quality of GNSS observations by preventing unwanted signals from being received. In this paper, we focus on the spoofing and try to eliminate the spoofing signal by the Nullspace Projection. We examined its effectiveness by the direction of arrival (DOA) estimation using the MUltiple SIgnal Classification (MUSIC) algorithm.

2 Methodology

2.1 Antenna Array

An antenna array is a kind of antenna that utilizes multiple antenna elements by combining the signal of each element. Fig.2 shows the basic idea of the antenna array. It can control its beam pattern by combining radio waves from every antenna element by applying specific weights, δ_k, described in Fig.2.

2.2 Algorithm

In this section, the algorithms used in this research are presented. MUSIC algorithm is used for the DOA estimation, and "Nullspace Projection [4]" is used for the removal of GNSS spoofing. This section also includes a signal model, assumptions, etc.

2.2.1 MUSIC [3] [5]

The MUSIC algorithm is one of the methods for the DOA estimation of incoming signals using an antenna array. Fig.3 shows the geometric relationships of antenna elements and an incident signal with respect to a reference point, which is the origin O. We assume that a K-element antenna array receives

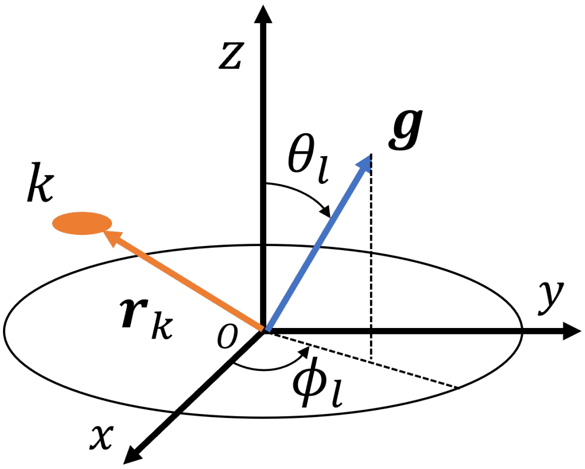

Fig. 3: Geometric relationships of antenna elements and incident signals

L signals and the incident direction of the l-th signal is described with an angle pair, the zenith angle, θ_l, and the counter-clockwise angle off the x-axis within the x-y plane, ϕ_l. A signal model is shown below. $\boldsymbol{s}(t)$ is the vector of L incoming signals at the reference point, A is the matrix containing $\boldsymbol{a}$ vectors. Herein, $\boldsymbol{a}$ vector is a what is called a "steering vector". $\boldsymbol{n}$ is the thermal noise vector. The thermal noise is considered to follow a complex Gaussian process with a mean of 0 and a variance of σ_n^2 across all elements. We assume that $\boldsymbol{x(t)}$ is the signal obtained from measurement.

$$\boldsymbol{x(t)} = A\boldsymbol{s}(t) + \boldsymbol{n}(t) \tag{1}$$

$$\boldsymbol{s(t)} = [s_1(t), \cdots, s_l(t), \cdots, s_L(t)]^{\mathrm{T}} \tag{2}$$

$$A = [\boldsymbol{a}(\theta_1, \phi_1), \cdots, \boldsymbol{a}(\theta_l, \phi_l), \cdots, \boldsymbol{a}(\theta_L, \phi_L)] \tag{3}$$

$\boldsymbol{a}(\theta_l, \phi_l)$ is defied as follows. $\Psi_k(\theta_l, \phi_l)$ denotes the received phase difference at the k-th element with respect to a reference point. $\boldsymbol{g}(\theta_l, \phi_l)$ is an incident direction vector and $\boldsymbol{r}_k$ is the position vector of the k-th element (Fig.3). c and f denote the speed of light and the frequency of signals, respectively. As presented below, the steering vector is determined by the geometry of antennas and each incident direction of incoming signals.

$$\boldsymbol{a}(\theta_l, \phi_l) = [\exp\{j\Psi_1(\theta_l, \phi_l)\}, \cdots, \exp\{j\Psi_K(\theta_l, \phi_l)\}]^{\mathrm{T}} \tag{4}$$

$$\Psi_k(\theta_l, \phi_l) = 2\pi \frac{f}{c} \boldsymbol{r}_k^{\mathrm{T}} \boldsymbol{g}(\theta_l, \phi_l) \tag{5}$$

$$\boldsymbol{g}(\theta_l, \phi_l) \triangleq [\sin\theta_l \cos\phi_l, \sin\theta_l \sin\phi_l, \cos\theta_l]^{\mathrm{T}} \tag{6}$$

R_{xx} is the covariance matrix of the received signal data and R_{ss} is the signal covariance matrix, defined as :

$$R_{xx} \triangleq E[\boldsymbol{x}(t)\boldsymbol{x}^{\mathrm{H}}(t)] \tag{7}$$

$$R_{ss} \triangleq E[\boldsymbol{s}(t)\boldsymbol{s}^{\mathrm{H}}(t)] \tag{8}$$

where $E[\cdot]$ denotes the expected value (mean) of its argument, and H denotes the complex conjugate transpose. Hence, an eigenvalue decomposition of R_{xx} is presented as below :

$$R_{xx} = AR_{ss}A^{\mathrm{H}} + \sigma_n^2 I \tag{9}$$

$$= \sum_{i=1}^{K} \lambda_i \boldsymbol{e}_i \boldsymbol{e}_i^{\mathrm{H}} \tag{10}$$

where λ_i is the i-th eigenvalue, here, in descending order, $\boldsymbol{e}_i$ is the normalized eigenvector, and σ_n^2 is the thermal noise power. We can obtain the eigenvalue structure through eigenvalue decomposition on R_{xx} from measurement data $\boldsymbol{x(t)}$. If there are L incoming signals, the eigenvectors : $E_S = [\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_L]$ span the signal subspace while the other eigenvectors : $E_N = [\boldsymbol{e}_{L+1}, \boldsymbol{e}_{L+2}, \cdots, \boldsymbol{e}_K]$ span the noise subspace. The eigenvalues corresponding to the noise subspace represent the value of the noise power. Therefore, regarding eigenvalues, it can be expressed as follows :

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_L \gg \lambda_{L+1} = \cdots = \lambda_K = \sigma_n^2 \tag{11}$$

Regarding eigenvectors, the key points are that they are orthogonal to each other and that the steering vectors of incoming signals can be represented as a linear combination of the vectors of signal subspace. Thus, the steering vectors of the received signals are also orthogonal to the vectors of noise subspace, expressed in Eq. (12). The MUSIC algorithm employs this property to estimate the signal DOA by searching for peaks of the function, called “MUSIC spectrum”, defined in Eq. (13)

$$\begin{gathered} \boldsymbol{e}_i^{\mathrm{H}} \boldsymbol{a}(\theta_l, \phi_l) = 0 \\ (i = L+1, \cdots, K; l = 1, 2, \cdots, L) \end{gathered} \tag{12}$$

$$P_{MUSIC}(\theta, \phi) = \frac{\boldsymbol{a}^{\mathrm{H}}(\theta, \phi)\boldsymbol{a}(\theta, \phi)}{\sum_{i=L+1}^{K} |\boldsymbol{e}_i^{\mathrm{H}} \boldsymbol{a}(\theta, \phi)|^2} = \frac{\boldsymbol{a}^{\mathrm{H}}(\theta, \phi)\boldsymbol{a}(\theta, \phi)}{\boldsymbol{a}^{\mathrm{H}}(\theta, \phi) E_N E_N^{\mathrm{H}} \boldsymbol{a}(\theta, \phi)} \tag{13}$$

The steering vector is determined by the arrangement of elements and the direction of arrival, as shown in Eq. (4) and (5). In this case, with the arrangement of elements known, the task is to perform peak searching for the direction of arrival. Since the norm of the noise subspace must be greater than or equal to one, the number of elements K and the number of signals L must fulfill the condition $K > L$.

2.2.2 Nullspace Projection [4]

The Nullspace Projection, hereinafter referred to as ’NSP’, generally known as subspace projection [2] [3], is the way to remove the signal in a specific direction by projecting the received signal onto its null space. Assume that two signals : $s_1(t)$, $s_2(t)$ arrive from different directions : $\boldsymbol{a}_1 = \boldsymbol{a}(\theta_1, \phi_1), \boldsymbol{a}_2 = \boldsymbol{a}(\theta_2, \phi_2)$, then received signal can be expressed as :

$$\boldsymbol{x(t)} = s_1(t)\boldsymbol{a}_1 + s_2(t)\boldsymbol{a}_2 + \boldsymbol{n}(t) \tag{14}$$

Herein, we can obtain the orthogonal projection matrix, projecting onto the null space of s_1, as :

$$P_{\perp 1} = I - \boldsymbol{a}_1 \boldsymbol{a}_1^{\mathrm{H}} / (\boldsymbol{a}_1^{\mathrm{H}} \boldsymbol{a}_1) \tag{15}$$

$$P_{\perp 1} \boldsymbol{a_1} = 0 \tag{16}$$

The key point, here, is that the property of the projection matrix $P_{\perp 1}$ can remove the signal $s_1(t)$ as expressed in Eq. (16). The projected signal $\boldsymbol{z}(t)$ can be obtained as :

$$\boldsymbol{z}(t) = P_{\perp 1}\boldsymbol{x}(t) = s_2(t) P_{\perp 1} \boldsymbol{a}_2 + P_{\perp 1} \boldsymbol{n}(t) \tag{17}$$

In this paper, the obtained projected signal $\boldsymbol{z}(t)$ is utilized for the DOA estimation in the MUSIC algorithm.

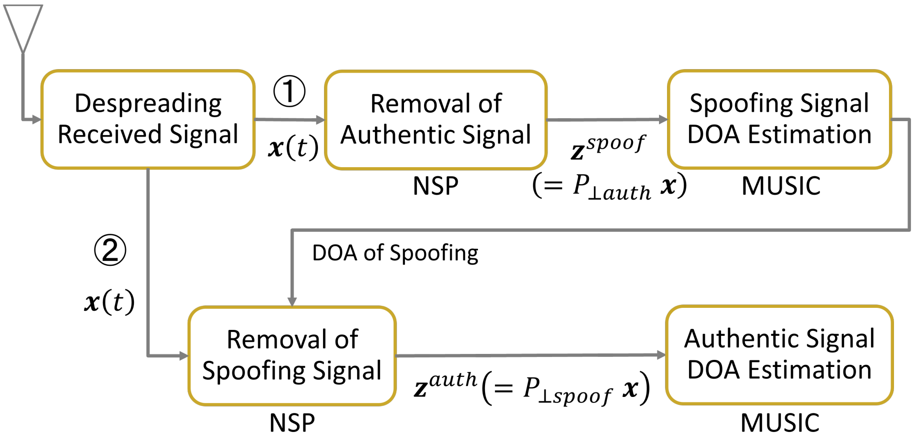
Despreading Received Signal
①
$x(t)$
Removal of Authentic Signal
NSP
z^{spoof}
$(= P_{\perp auth}\, x)$
Spoofing Signal DOA Estimation
MUSIC
②
$x(t)$
DOA of Spoofing
Removal of Spoofing Signal
NSP
$z^{auth}(= P_{\perp spoof}\, x)$
Authentic Signal DOA Estimation
MUSIC

Fig. 4: Diagram of process flow

2.2.3 Process flow

Fig. 4 depicts the process flow of the DOA estimation and the NSP. In this paper, we assume that the received signals include authentic signals and spoofing signals on the condition that the PRN numbers of the spoofing signals correspond to those of the actual satellites. In preparation, the despreading using an authentic replica signal is performed and we consider the despreaded signal as $\boldsymbol{x}(t)$. Firstly, the authentic signal is removed by NSP based on the GNSS ephemeris, and the DOA of the spoofing is estimated with MUSIC algorithm (in Fig. 4, ①). In the following stage, the spoofing signal is removed with NSP based on the DOA of spoofing obtained in the previous stage (in Fig. 4, ②). The goal of this research is to get the PVT solution, but it has not yet been conducted.

3 Spoofing Experiment in Outdoor Environment

In this section, the overall configuration of the spoofing experiment is explained.

3.1 Test Equipments and Configuration

The experiment is conducted in the radome, where the authentic satellite signals can be received. Fig. 5 shows the devices and the experimental environment. The spoofing simulator is the CLAW GPS Simulator manufactured by Jackson Labs Technologies, which generates GPS signals based on the ephemeris and Pulse Per Second (PPS) signal (Fig. 6). As for the antenna, a 6-elements antenna array was used (Fig. 5, left). An antenna element is 3G1215RL-AA-XS-1 manufactured by Antcom. The spacing between adjacent elements was half the L1 signal wavelength, approximately 0.095[m]. The received signal was logged as digital data in the PC via the RF frontend, which is composed of the downconverter, the AD converter, etc.

3.2 Test Conditions

The antenna is static throughout the experiment. The spoofing scenario is divided into three parts sequentially; normal(no spoofing), static spoofing, and kinematic spoofing. The kinematic spoofing means moving the location ahead to the north. The duration of each part are 3 [min], 2 [min] and 5 [min], respectively. The first 3 [min] data was also used for the array calibration. Since the spoofer, in this

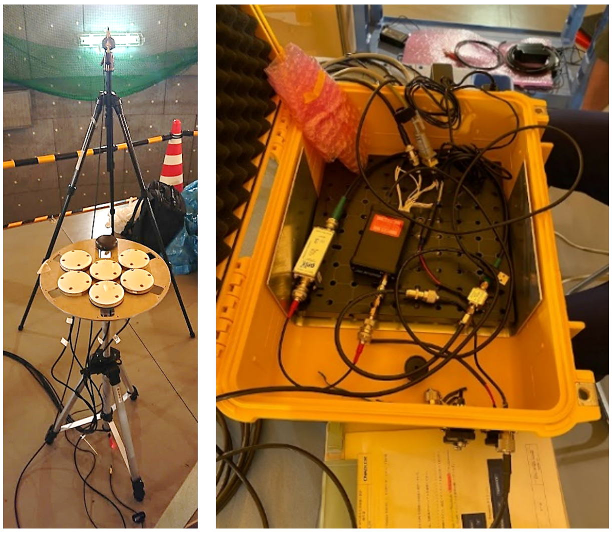

Fig. 5: Equipments and experimental environment (Left: spoofer and antenna array, Right: simulator)

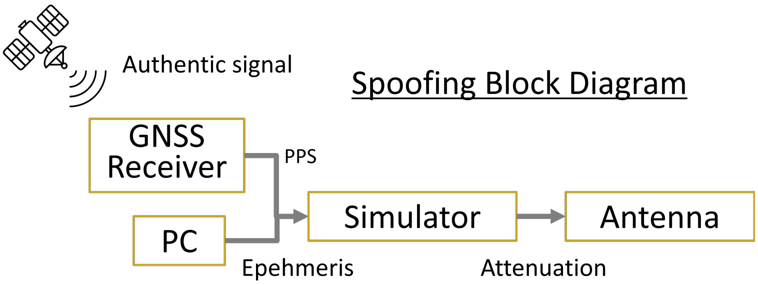

Fig. 6: Spoofing Block Diagram

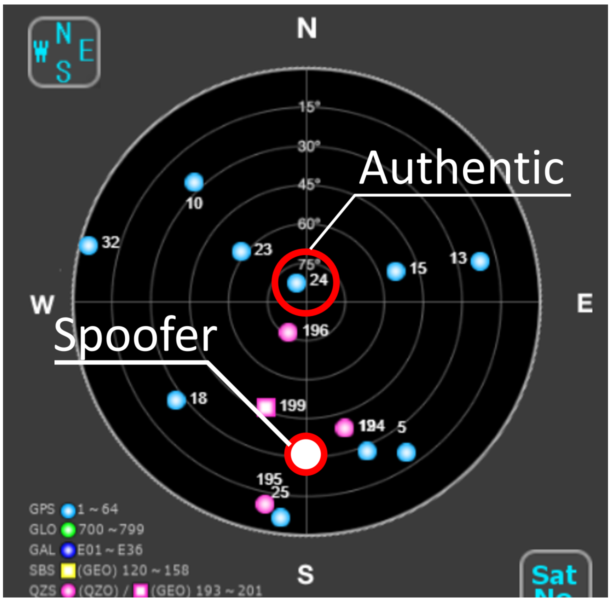

Fig. 7: Skyplot with true DOA of spoofing [6]

experiment, generated signals based on the broadcast ephemeris via the Internet and PPS from an actual GNSS receiver, the spoofing signal was synchronized 'to some extent', which means that the processing delay by computation and transmission via the cable was not compensated. Fig. 7 is the skyplot at the experiment. GPS 24 satellite was used for the DOA estimation. The true direction of the spoofer is also depicted in the figure; azimuth: 180 [deg], elevation: 30 [deg]. Note that the DOA, here, is represented by a set of angles; azimuth and elevation while the DOA of Fig. 3 is represented by a set of angles; zenith angle and counter-clockwise angle off the x-axis within the x-y plane. The reference point of the antenna array is the center element. The sampling rate of RF frontend is 20.46 [MHz]. We assume the number of signals is $L = 2$ when estimating the DOA by the MUSIC algorithm, which indicates that the number of vectors of the noise subspace used for the MUSIC is 4 ($= 6 - 2$); nevertheless, the actual number of the noise vectors of incoming signals is 5 ($= 6 - 1$) and one more noise vector can be used to calculate the MUSIC spectrum. Therefore, the effect of averaging the MUSIC spectrum like the harmonic mean in Eq. (13) is reduced. In general, the number of signals is estimated by MDL (Minimum Description Length), AIC (Akaike Information Criterion), and so on, but the number of signals was provided in advance in this study in order to compare the MUSIC spectrum results before and after NSP.

3.3 Results

The DOA estimation results after the removal of the authentic signal and after the removal of the spoofing signal by NSP are presented in this subsection. The former and the latter correspond to the process ① in Fig. 4, and the process ② in Fig. 4, respectively. In the estimation result figures, a black X mark denotes the direction of the authentic signal and a white X mark denotes that of the spoofing one.

3.3.1 Removal of Authentic Satellite Signal

The DOA estimation results with and without NSP are, herein, compared in Fig. 8 and Fig. 9. Fig. 9 shows the DOA result of the projected signal onto the null space of the authentic signal so that the authentic signal is eliminated. As seen in these figures, the normal method reveals two peaks of the MUSIC spectrum, in the directions of authentic signal and spoofing signal. In the case of with-NSP, in contrast, the peak of authentic signal disappeared and only the peak of spoofing is present. Thus, the results show that the null space projection can eliminate the authentic signal effectively.

3.3.2 Removal of Spoofing Signal

Fig. 10 shows the DOA estimation results of the projected signal onto the null space of the spoofing signal so that the spoofing signal is eliminated. It has only the peak in the direction of the authentic signal and therefore it can be said that the Nullspace Projection eliminates the spoofing signal effectively. Fig. 11 and Fig. 12 show the DOA results at 250 [s], and these results are different in the number of signals, L. When L is 2, the MUSIC spectrum has the irrelevant peak, whereas there is only one peak in the direction of the authentic signal when L is 1. When L is 2, about 80% of the DOA results of every 10 seconds have the correct peak (direction), but some of the results depict the result like Fig. 11. As mentioned in the section 3.2, it is thought that this is because the number of the noise vectors($K - L = 6 - 2 = 4$) used in this analysis is less than the maximum number of the noise vectors ($6 - 1 = 5$) assuming only one signal is impinging on the antenna array, and it is not enough to average out the MUSIC spectrum.

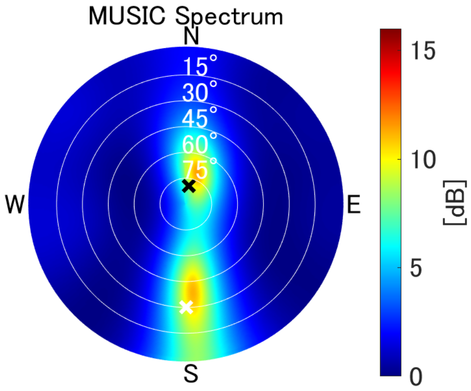

Fig. 8: MUSIC spectrum w/o NSP (G24, at 390 [s], $L = 2$)

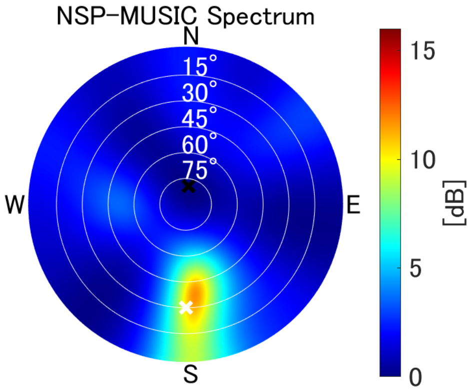

Fig. 9: MUSIC spectrum with NSP for the removal of authentic signal (G24, at 390 [s], $L = 2$)

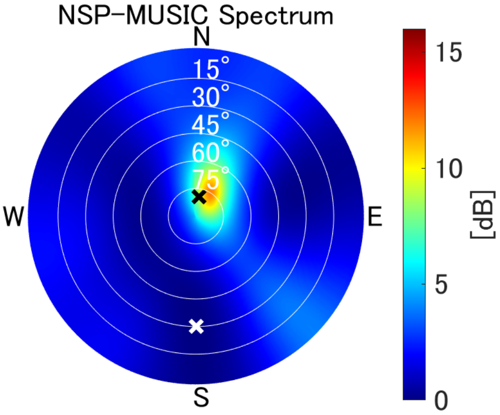

Fig. 10: MUSIC spectrum with NSP for the removal of spoofing signal (G24, at 390 [s], $L = 2$)

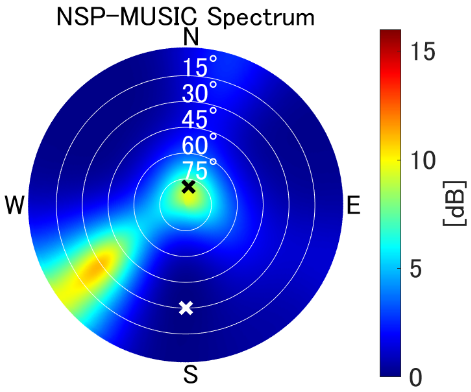

Fig. 11: MUSIC spectrum with NSP for the removal of spoofing signal (G24, at 250 [s], $L = 2$)

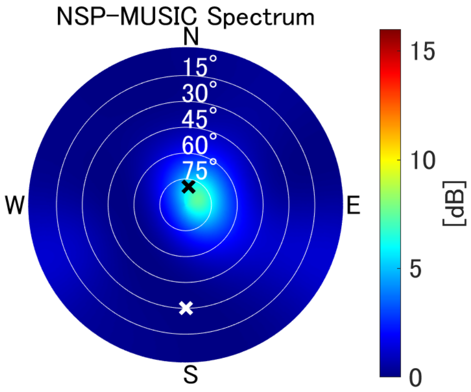

Fig. 12: MUSIC spectrum with NSP for the removal of spoofing signal (G24, at 250 [s], $L = 1$)

3.4 Conclusion

As potential threats of the spoofing have become more apparent in recent years, this paper aims to remove the spoofing signal and introduce the method called the Nullspace Projection. The spoofing experiment in the real environment was conducted, and, in conclusion, it demonstrates the effectiveness of Nullspace Projection. The goal of this research is to obtain the PVT solution, but further work needs to be done. In this paper, we handled the signal after despreading as $\boldsymbol{x}(t)$, but the pre-correlation (before despreading) signal has to be projected onto the null space of the spoofing for signal processing such as tracking and decoding the navigation data. That could make a difference in the effect of the NSP, and thus further research is needed.

References

[1] C4ADS, “ABOVE US ONLY STARS Exposing GPS Spoofing in Russia and Syria”, pp. 15-16, 2019.

[2] J. Zhang, X. Cui, H. Xu , M. Lu, “A Two-Stage Interference Suppression Scheme Based on Antenna Array for GNSS Jamming and Spoofing” , *Sensors*, 2019.

[3] G. Fan, X. Gan, B. Yu, Q. Rong , C. Sheng, “Adaptive Spoofing Suppression Algorithm for GNSS Based on Multiple Antennas Array,” *Sensors*, 2020.

[4] C. Yang, A. Soloviev, “How to mitigate a spoofing signal while tracking it for intent analysis?” , *Inside GNSS* July/August, pp. 24-30, 2021.

[5] Nobuyoshi Kikuma, [*Adaptive signal processing with array antenna*] Arei antena niyoru tekiou singousyori(in Japanese), Kagaku Gijutsu (Science and Technology Pub.), pp. 13-34, 87-114, 194-202, 247-268, 1998.

[6] Cabinet Office, Government of Japan, GNSS View [web app]. Available at :
`https://qzss.go.jp/redirect/gnssview.html`