JPNT 11(3), 181-189 (2022)
https://doi.org/10.11003/JPNT.2022.11.3.181

JPNT Journal of Positioning, Navigation, and Timing

Performance Analysis of the Anti-Spoofing Array Antenna with Eigenvector Nulling Algorithm

Kihoon Lee†, Min Kyu Song, Jang Yong Lee

Satellite Navigation Team, Agency for Defense Development, Daejeon 34186, Korea

ABSTRACT

The public open signals from Global Navigation Satellite System (GNSS) including Global positioning system (GPS) are used widely by many peoples in the world except for the public regulated restriction signals which are encrypted. Nowadays there are growing concerns about GNSS signal spoofing which can deceive the GNSS receivers by abusing these open services. To counter these spoofing threats, many researches have been studied including array antenna techniques which can detect the direction of arrival by means of Multiple Signal Classification (MUSIC) algorithm. Originally the array antenna techniques were developed to countermeasure the jamming signal in electronic warfare by using the nulling or beamforming algorithm toward a certain direction. In this paper, we study the anti-spoofing techniques using array antenna to overcome the jamming and spoofing issues simultaneously. First, we will present the theoretical analysis results of spoofing signal response of Minimum Variance Distortionless Response (MVDR) algorithm in array antenna. Then the eigenvector algorithm of covariance matrix is suggested and verified to work with the existing anti-jamming method. The modeling and simulation are used to verify the effectiveness of the anti-spoofing algorithm. Also, the field test results show that the array antenna system with the proposed algorithms can perform the anti-spoofing function. This anti-spoofing method using array antenna is very effective in the view point of solving both the jamming and spoofing problems using the same array antenna hardware.

Keywords: GNSS, spoofing, anti-spoofing, jamming, eigenvector, array antenna

1. INTRODUCTION

The recent advances in civil autonomous systems and military weapon systems have been achieved based widely on the precise position and timing information provided by Global Navigation Satellite System (GNSS) like global positioning system (GPS) of USA (Spilker, Jr. et al. 1996, Kaplan & Hegarty 2006).

As these sophisticated systems rely heavily on GNSS, the threat to GNSS becomes a growing concern, because GNSS signals are vulnerable due to lower power than the noise floor in general. There are two types of threats to GNSS discussed in this paper:

Jamming: it disturbs reception of signals by just emitting malicious interferences (usually uncorrelated to authentic GNSS signals) with high power;

Spoofing: it also disturbs reception of signals. But, unlike jamming, it is performed by emitting genuine-like signals so that an anonymous attacker can mislead an innocent user to where he wants it to be.

Spoofing is usually more severe than jamming because not only is it disruptive, but also it forces recipients to act according to the attacker's intentions (Pullen et al. 2012, Akos 2012, Humphreys et al. 2008, Psiaki & Humphreys 2016, Bhatti & Humphreys 2017).

It is well-known that, when using multiple number of antennas, signals from different directions have distinct signatures in spatial domain. So, by handling spatial signatures properly, it is possible to detect/classify signals

Received Jun 10, 2022 **Revised** Jun 17, 2022 **Accepted** Jul 01, 2022
†**Corresponding Author**
E-mail: hanbee75@hanmail.net
Tel: +82-42-821-4468 Fax: +82-42-823-3400
Kihoon Lee https://orcid.org/0000-0003-3618-7324
Min Kyu Song https://orcid.org/0000-0002-5481-9180
Jang Yong Lee https://orcid.org/0000-0002-5652-3084

Table 1. Comparison of spoofing detection techniques (Li et al. 2019).

Method	Characteristics	Capabilities required	Implementation difficulty	Effectiveness	Applicability
Signal encryption recognition	Unencrypted signal	Decryption ability	High	High	High
Ephemeris/Almanac check	Discontinuous ephemeris/almanac changes	Store ephemeris and almanac	Low	Medium	High
Satellite clock Check	Discontinuous ephemeris/almanac changes	Store clock information	Low	Medium	Medium
C/N_0 detection	Higher signal to noise ratio	C/N_0 monitoring	Low	Medium	Medium
Absolute power monitoring	Higher amplitude	Standardized absolute power	Low	Medium	High
Direction of arrival detection	Same signal direction	Multiple antennas array	High	High	High
Doppler shift detection	Unchanged Doppler frequency	Known satellite Doppler	Medium	Medium	Medium
Code/carrier consistency detection	Inconsistent code/carrier rates	With Code/carrier Doppler	Low	Low	Low
Dual frequency power comparison	Spoofing single frequency	Dual frequency signals	Medium	Low	Low
AGC detection	Power greater than noise	Calibrated AGC gain	Low	High	Medium
Signal quality monitoring	Signal correlation peak distortion	With multiple correlators	Medium	Medium	Low
Auxiliary informationcomparison detection (INS, sensors, etc.)	Inconsistent with the measurement results	With related auxiliary equipment	High	High	High
RAIM	Only for the few spoofing signals	Autonomous integrity detection	Medium	Medium	Medium

and even more to enhance /eliminate them. With the growing importance of PNT information in modern society, this array signal processing has been attracted as the key to develop GNSS receivers robust against threats (Di & Tian 1984, Schmidt 1986, Jafarnia-Jahromi et al. 2012, Appel et al. 2015, Broumandan & Curran 2017, Broumandan & Lachapelle 2018, Seo et al. 2020, Park & Seo 2020, Lee et al. 2021).

Since the jamming signals are easy to detect due to their high power, anti-jamming technique based on array signal processing have been well-studied (Fante & Vaccaro 2000, Moore 2002, Berefelt et al. 2003, Haefner et al. 2003, Monzingo & Miller 2004, De Lorenzo et al. 2005, Vo el al. 2007). It is done by steering null to the estimated direction of jammer while forming a beam to each GNSS satellite. Herein, thanks to the high power of jamming signals, it is possible to estimate the direction to a jammer easily.

But, it is difficult to estimate direction of a spoofed signal because its power is not as high as a jamming signal. Fortunately, due to the complexity of building a spoofing system, it is reasonable to assume that a single spoofer emits multiple number of spoofing signals at the same time. Under the assumption, multiple number of spoofing signals come from the same direction. As a result, the total power of signals from that direction becomes much higher than before, and hence, it is also possible to detect and to eliminate spoofing signals.

In this paper, we study the anti-spoofing techniques using array antenna to overcome the jamming problem and the spoofing issue simultaneously. First, we will present the theoretical analysis results of spoofing signal response of Minimum Variance Distortionless Response (MVDR) algorithm in array antenna. Then the new eigenvector algorithm of covariance matrix is suggested and verified to work with the existing anti-jamming method. The modeling and simulation technique is used to confirm the effectiveness of the combined algorithm. Also, the field test results show that the array antenna system with the proposed algorithms can perform the anti-spoofing function.

2. CONVENTIONAL ANTI–SPOOFING ALGORITHM

The GNSS receiver receives a variety of signals, besides the real satellite signals, and other signals can be considered as interference signals. Natural interference always exists in the electromagnetic environment, but has small effect on the receiver and man-made interference has certain threats to the receiver. In addition, man-made interference can be divided into suppressed interference and spoofing interference. This paper will focus on spoofing interference mainly. Spoofing interference is to induce the receiver to lock the spoofing signal by transmitting the generated false signal or the related real satellite signal to the target device, so that the misleading target obtains the wrong time, position, speed and other information which indicates that the spoofer have achieved the purpose of interfering.

The various anti-spoofing methods have been proposed to alleviate the threats from the malicious spoofing attacks of GNSS (Jafarnia-Jahromi et al. 2012, Konovaltsev et al. 2014, Broumandan et al. 2016, Dempster & Cetin 2016, Konovaltsev et al. 2019, Li et al. 2019). Table 1 shows the comparison of the spoofing detection technologies. Presently, many progresses have been made in the research of anti-spoofing technology, but these methods of anti-spoofing technology for most part usually based on the detection only and the

characteristics of signals such as doppler shift, carrier-to-noise ratio (C/N0), signal correlation peak. Many researchers have analyzed GNSS spoofing detection technologies from different perspectives, such as signal power, direction of arrival, delay detection, encryption authentication, and other navigation methods. The anti-spoofing interference detection technology that has been proposed can be summarized into three categories, namely, the spoofing detection technology based on navigation data, the fraud detection technology based on signal feature and the fraud detection technology based on inertial information assistance (Li et al. 2019).

Table 1 shows that some effective anti-spoofing techniques are as the signal encryption recognition, the direction of arrival detection, and the auxiliary information comparison detection (such as inertial navigation, sensors, etc.) The most effective anti-spoofing method is to use the encrypted signal like GPS P(Y) code. But the encrypted signal is under the control of the government who own the navigation satellite system. Therefore, most civilian or some military applications are limited considerably. Another effective method is to detect the direction of arrival of the spoofing signals using the array antenna. This method is difficult to implement because of the multiple antennas, RF channels, and the high speed digital signal processor. But the array antenna technique has been widely used in the field of anti-jamming system. So the use of the array antenna is feasible for the anti-spoofing function addition to the existing anti-jamming system.

The representative spoofing detection algorithm of the direction of arrival is the Multiple Signal Classification (MUSIC) algorithm (Schmidt 1986). The main idea of the MUSIC algorithm is to conduct eigen decomposition for the covariance matrix of the array input data. In this paper, our goal is to research not only the detection but also the elimination for the spoofing signal with the array antenna.

A typical GNSS array antenna schematic for anti-jamming is shown in Fig. 1. GNSS satellite and spoofing signals are collected by antenna element 1 to K, and then converted to low-frequency signals by a RF down-converter. After digital sampling using an analogue-to-digital converter (ADC), the signals are processed using an anti-jamming algorithm, such as a nullifying or beamforming algorithm in a field-programmable gate array (FPGA). The array antenna system generates the final output by multiplying the number of input signals by a weight vector and adding them together. In the next section, we will assume this digital signal processing architecture, and propose the anti-spoofing algorithm which can eliminate the spoofing signal securely.

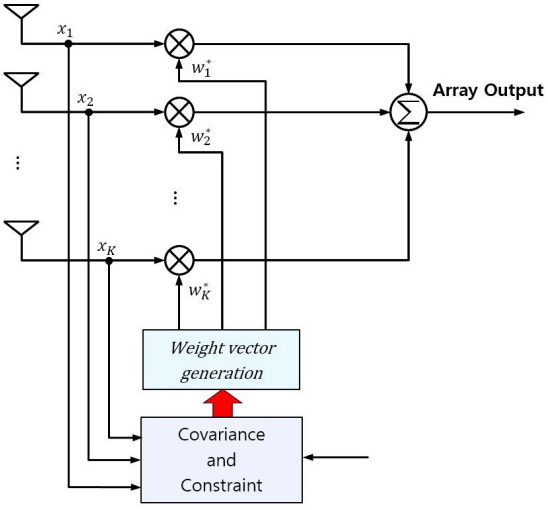

Fig. 1. Signal processing block diagram of array antenna system.

3. EIGENVECTOR ANTI–SPOOFING ALGORITHM

3.1 Received Signal Model

Before we begin, we fix the following notation for convenience:

- Any symbol expressed in boldface implies a vector or a matrix;
- All the vectors are column vectors;
- The identity matrix of order K is denoted by $\boldsymbol{I}_K$;
- The Hermitian (or conjugate) transpose of a vector of a matrix is denoted by $(\cdot)^H$.

Let us consider a reception of signals by using an array of K antennas. The received signal vector at the receiver is

$$\boldsymbol{r}(t) = \sum_{i=1}^{L} s_i(t)a(\boldsymbol{\theta}_i) + \boldsymbol{n}(t) \tag{1}$$

where $s_i(t)$ is the i-th incoming signal, $a(\boldsymbol{\theta}_i)$ is the steering vector for the direction $\boldsymbol{\theta}_i$ toward source of the i-th signal, and $n(t)$ is the receiver noise vector. For positive integers N,P,M such that $L=N+P+M$, we assume that, among those L signals, the first N signals are interferences, the following P signals are spoofed, and the rest M signals are authentic. Then, Eq. (1) can be expressed as

$$\boldsymbol{r}(t) = \underbrace{\sum_{i=1}^{N} s_i(t)a(\boldsymbol{\theta}_i)}_{\text{interferences}} + \underbrace{\sum_{j=N+1}^{N+P} s_j(t)a(\boldsymbol{\theta}_j)}_{\text{spoofed signals}} + \underbrace{\sum_{k=N+P+1}^{L} s_k(t)a(\boldsymbol{\theta}_k)}_{\text{authentic signals}} + \boldsymbol{n}(t). \tag{2}$$

In the literature of array signal processing with GNSS

signals, a general assumption is that each interference has much higher power than that of any authentic one. Furthermore, when spoofed signals considered, one more reasonable assumption is usually considered: All the spoofing signals comes from a single direction. That is, by letting $\boldsymbol{\phi}$ direction of the spoofer, we have

$$a(\boldsymbol{\theta}_i) = a(\boldsymbol{\theta}_j) = a(\boldsymbol{\phi}) \tag{3}$$

for any $N \le i < j \le N+D$. This is because, to deceive a GNSS receiver, anonymous attacker may use a single spoofer that emits lots of spoofing signals at the same time. As a consequence, the total power of signals comes from a spoofer is also much higher than that of any authentic one. Under these two assumptions, we may approximate the covariance of the received signal vector as

$$\boldsymbol{R} = E\{\boldsymbol{r}(t)\boldsymbol{r}^H(t)\} \approx \sum_{i=1}^{N} \sigma_i^2 a(\boldsymbol{\theta}_i)\, a^H(\boldsymbol{\theta}_i) + \sigma_p^2 a(\boldsymbol{\phi}) a^H(\boldsymbol{\phi}) + \sigma_n^2 \boldsymbol{I}_K, \tag{4}$$

where

- $a(\boldsymbol{\phi})$ is the steering vector toward the spoofer. And,
- $\sigma_p^2 = \sum_{j=N+1}^{N+P} \sigma_j^2$ is the total power of spoofing signals emitted by the spoofer;
- $\boldsymbol{\sigma}_i^2$ for i=1,2,...,N is power of the i-th interference signal;
- $\boldsymbol{\sigma}_n^2$ is the noise power.

Herein, we would like to note that a covariance matrix is positive semi-definite. That is, any eigenvalue of a covariance matrix is always greater than or equal to zero.

For the sake of simplicity, in the remaining of this paper, we assume that there is only a single spoofer. Note that, when there are more than one spoofer, all the results of this paper can be easily extended in the similar fashion.

3.2 Eigenspace of the Covariance Matrix and Signal Space

To enhance reception of desired GNSS signals, it is usual to eliminated unwanted signals, e.g., interferences and spoofed signals. Such an elimination is performed by forcing spatial response to the space of unwanted signals be zero.

Before we discuss anti-spoofing technique in detail, we would like to discuss the relationship between eigenspace of the covariance matrix $\boldsymbol{R}$ and signal space of unwanted signals. Let $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_K$ be eigenvectors of $\boldsymbol{R}$ with corresponding eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_K$, respectively. Without loss of generality, we may arrange all the eigenvalues in descending order, i.e.,

$$\lambda_1 \ge \lambda_2 \ge \ldots \ge \lambda_K. \tag{5}$$

Denote by $\boldsymbol{V}$= span$\{a(\boldsymbol{\theta}_1), a(\boldsymbol{\theta}_2), \ldots, a(\boldsymbol{\theta}_N), a(\boldsymbol{\phi})\}$ the space of unwanted signals in spatial domain with dimension $\boldsymbol{D}$=dim$\boldsymbol{V}$. Then, eigenspace of the covariance matrix $\boldsymbol{R}$ and the signal space $\boldsymbol{V}$ have the following relationship:

$$\boldsymbol{V} = \text{span}\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_D\}. \tag{6}$$

This can be directly come from Eq. (4). Denote by $\bar{\boldsymbol{R}}$ the sum of the first two terms in RHS of Eq. (4). Then, we have

$$\boldsymbol{R} = \bar{\boldsymbol{R}} + \sigma_n^2 \boldsymbol{I}_K, \tag{7}$$

which yields that $\boldsymbol{R}$ and $\bar{\boldsymbol{R}}$ have the same eigenvectors. Here, only D eigenvectors in the eigenspace of $\bar{\boldsymbol{R}}$ are corresponding to non-zero eigenvalues. Obviously, those D eigenvectors will be the same to $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_D$ with some proper ordering since $\bar{\boldsymbol{R}}$ is positive semi-definite.

This leads us to an important aspect: instead using exact steering vectors, it is possible to eliminate unwanted signals by suppressing spatial response to $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_D$. This aspect will be used in the next section to eliminate spoofed signals.

3.3 Integrated Anti-spoofing and Anti-jamming Algorithm

The array antenna system generates the final output by multiplying the number of input signals $\boldsymbol{r}$ by a weight vector $\boldsymbol{w}$ and adding them together. The input vector signal $\boldsymbol{r}$ measured at the In-phase and Quadrature-phase channel of an array antenna is defined as a complex number vector. Because the output of the array antenna is $f(\boldsymbol{w})=\boldsymbol{w}^H \boldsymbol{r}$, the expected value of the output power can be expressed as Eq. (8),

$$Output\ Power = E\{|\boldsymbol{w}^H \boldsymbol{r}|^2\} = \boldsymbol{w}^H \boldsymbol{R} \boldsymbol{w} \tag{8}$$

Using Eq. (8), the constrained optimization problem can be expressed as Eq. (9),

$$\min_{\boldsymbol{w}} \boldsymbol{w}^H \boldsymbol{R} \boldsymbol{w} \ \ subject\ to\ \boldsymbol{C}^H \boldsymbol{w} = \boldsymbol{c} \tag{9}$$

where $\boldsymbol{C}$ represents the constraint matrix, and $\boldsymbol{c}$ represents the constraining column vector. In this expression, it is important that $\boldsymbol{C}$ and $\boldsymbol{c}$ can have any value and the interference cancellation performance depends on those values. Also to eliminate the spoofing signal it is need to replace the covariance matrix $\boldsymbol{R}$ as following Eq. (10),

$$\widehat{\boldsymbol{R}} = \boldsymbol{R} + \alpha \cdot \boldsymbol{R}_V \tag{10}$$

where α represents the constant to adjust the nulling depth, and $\boldsymbol{R}_V$ represents the covariance matrix of eigenvectors subject to the spoofing signals. If the value α is 0, then the effect is to turn off the anti-spoofing function and is equal to the just anti-jamming algorithm.

The final weight vector solution to the above constrained optimization problem is one of the stationary points of the Lagrangian and can be obtained using a Lagrangian multiplier. Using this, the optimal weight vector $\boldsymbol{w}_o$ can be calculated as shown in Eq. (11).

$$\boldsymbol{w}_o = \widehat{\boldsymbol{R}}^{-1}\boldsymbol{C}\left(\boldsymbol{C}^H\widehat{\boldsymbol{R}}^{-1}\boldsymbol{C}\right)^{-1}\boldsymbol{c} \tag{11}$$

As mentioned before, the spoofing and jamming signal cancellation performances depend on the constraint conditions of Eq. (9). One of the constraint conditions is the beamforming which is to maintain the gain of satellite directions and to null the direction of spoofing and jamming signals. The beamforming constraint matrix is that the vector of $\boldsymbol{C}$ is equal to the steering vector of the satellite direction.

4. SIMULATION

In this section, simulations are performed to verify the anti-spoofing algorithm designed for the GNSS array antenna system as described in the previous section. A very small array antenna with four elements is modelled and the distance between adjacent elements is 3 cm as shown in Fig. 2. The more detailed simulation conditions are summarized in Table 2. One satellite signal is generated as CN_0 40 dB-Hz power after 1ms integration time. One spoofer generating the spoofing signals which are consisted of 8 faked satellite signals is located in certain directions. The one spoofing signal power is generated as CN_0 45 dB-Hz which is 5 dB stronger than the authentic satellite signal to pull off surely. All signals are generated in baseband of 0 Hz IF frequency and noises are considered as the normal distribution.

The basic performance of the array antenna without the anti-spoofing algorithm is equal to Minimum Variance Distortionless Response (MVDR) algorithm. The MVDR algorithm works to minimize the interference power above the thermal noise. Thus, even the spoofing signal can also be suppressed normally by the MVDR algorithm. Fig. 3 shows the effect of the spoofing signal's self-suppression by the array antenna. Even 0 dB spoofing signal which is equal to the noise power is suppressed by amount of -7 dB. But it is notable that the spoofing signal is increased reversely if the spoofing power is below the -8 dB because the array antenna algorithm cannot detect any meaningful signal power.

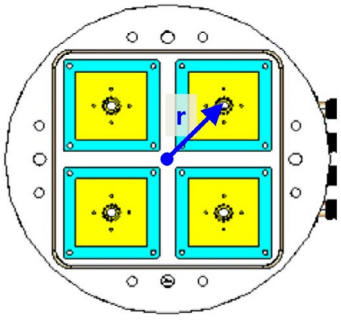

Fig. 2. Small circular array antenna diagram.

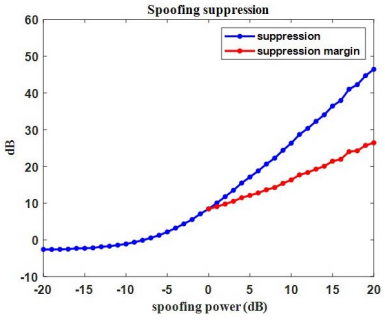

Fig. 3. Basic performance of spoofing signal suppression with array antenna.

Table 2. Simulation conditions.

Conditions	Description
Satellite signal CN_0	40 dB
Spoofer: CN_0 (per 1 satellite)	45 dB
Spoofer: satellite number	8
Antenna element number	4
Array type	Circular
Array radius	4.24 cm
IF frequency	0 Hz (baseband)
Sampling frequency	20 MHz

Another simulation is performed to confirm the benefit of anti-spoofing algorithm. The authentic satellite direction is at the azimuth 270 degree and the elevation 45 degree. The spoofing direction is at the azimuth 90 degree and the elevation 5 degree. Fig. 4 shows the result of conventional MVDR beamforming algorithm. The left of Fig. 4 shows the power spectrum of input and output signals. Very little difference can be seen because the input spoofing signal's power is almost same to noise power and cannot be detected significantly by the MVDR algorithm. The right of Fig. 4 shows the gain pattern. The nulling depth by the MVDR algorithm is about -7 dB as expected.

As contrast, Fig. 5 shows the effect of anti-spoofing algorithm. The left of Fig. 5 is the power spectrum of the input and output signals, which show the significant difference below 1 MHz where the spoofing signal exists. The right of Fig. 5 is the gain pattern which shows the deep nulling in

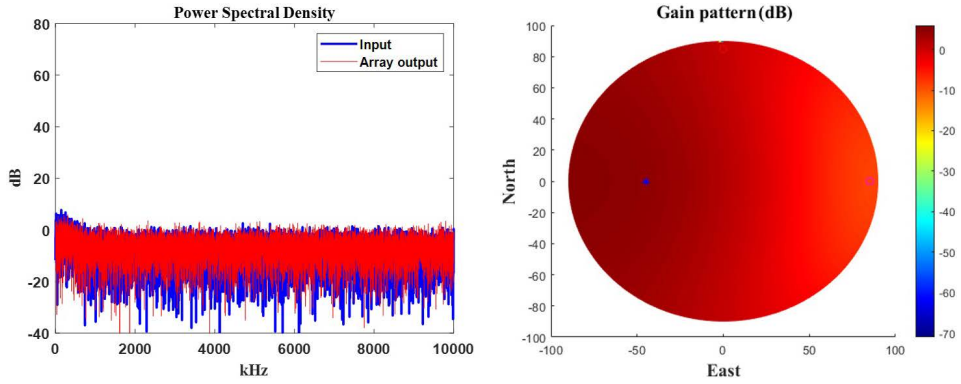

Fig. 4. Power spectrum and gain pattern using the general beamforming algorithm.

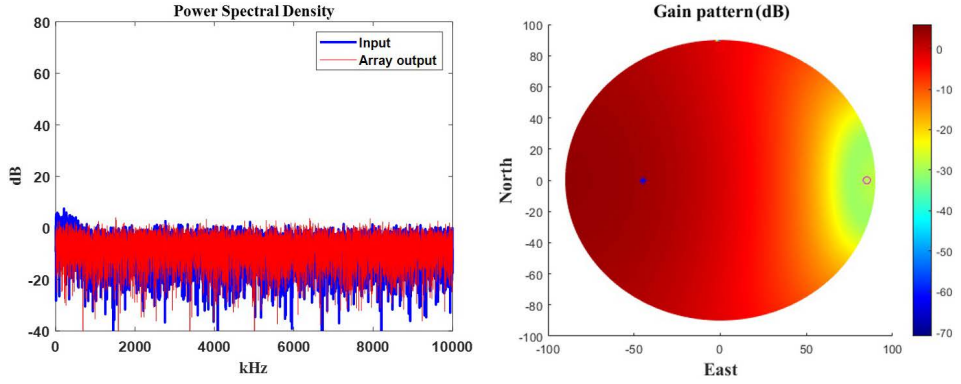

Fig. 5. Power spectrum and gain pattern using the eigenvector beamforming algorithm.

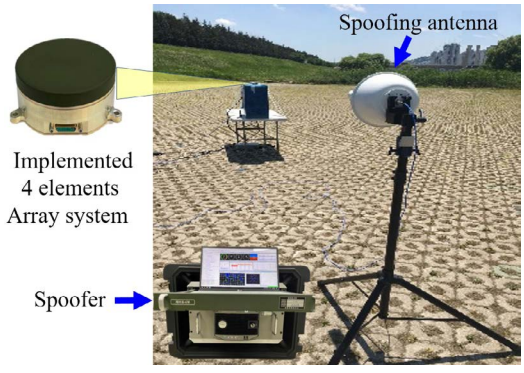

Fig. 6. Experimental environment setup of the anti-spoofing algorithm.

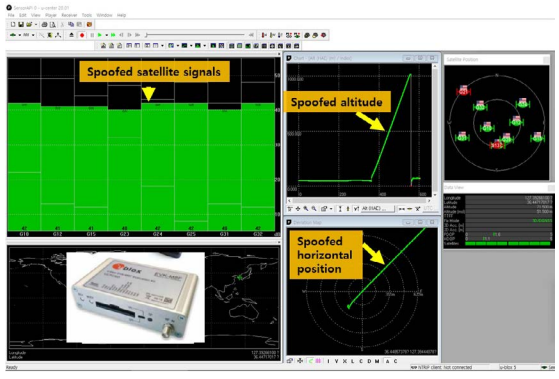

Fig. 7. The result of Ublox receiver spoofing experiment.

the direction of the spoofing signal about 30 dB. This effect means the possibility of the elimination of the spoofing signal and anti-spoofing performance.

5. EXPERIMENT

5.1 Spoofing System Setup

To test the performance of anti-spoofing algorithm it is needed to setup the spoofing system. Therefore, we have developed the spoofing system based on the Spirent's Simsafe device. Fig. 6 shows the spoofing system and our implemented 4 elements array antenna system. The spoofing system has the capability of GPS, Galileo, Glonass spoofing with about 50 ns time synchronization accuracy. For the safety, we used the directional antenna and the very weak signal with a few meter distance between the antenna and the array antenna system.

Fig. 7 shows the spoofing test result of Ublox receiver by

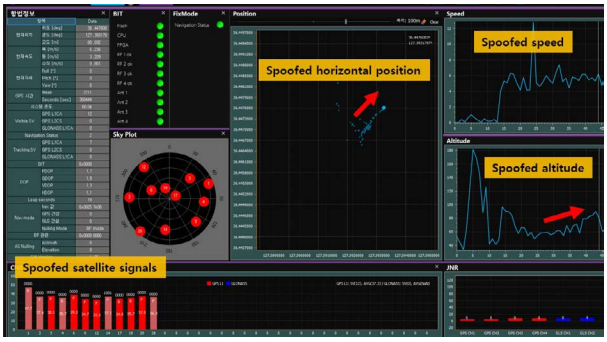

Fig. 8. Test result of the array antenna with no anti-spoofing algorithm: Spoofed at J/S 30 dB.

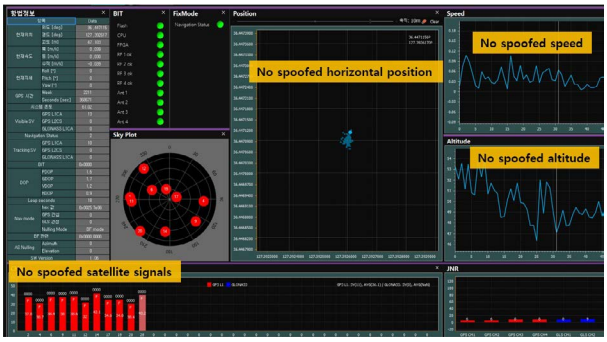

Fig. 9 Test result of the array antenna with anti-spoofing algorithm: Not spoofed at J/S 30 ~ 40 dB.

the spoofing system. The spoofing signal power was J/S 30 dB which S is assumed as the nominal satellite power of -160 dBW. At the spoofing power level, the measured signal power was around 40 dB-Hz. It can be seen that the altitude and horizontal position data were moving even though the receiver was stationary. From this experiment we can confirm the normal operation of the spoofing system.

5.2 Anti-spoofing Experiment Results

The anti-spoofing algorithm test was implemented with above spoofing system and 4 elements array antenna system. Fig. 8 shows the captured control and display program of the 4 elements array antenna system without anti-spoofing algorithm. Without the anti-spoofing algorithm, the array antenna system executes the MVDR beamforming algorithm only. When the spoofing signal power was J/S 30 dB, the array antenna system in static position was spoofed, which meant the position and speed data was manipulated by the spoofing system as shown in Fig. 8. At some time, the array antenna's navigation data shows the spike as the mixed usage of the spoofing and authentic satellite signals.

On the other hand, the array antenna system with the anti-spoofing algorithm could output the correct position and speed data as shown in Fig. 9. The spoofing signal power has varied from J/S 30 ~ 40 dB. Even under the stronger power, the anti-spoofing algorithm has worked as designed. One satellite of PRN 28 was unhealthy in the satellite navigation data. The others satellites were tracked properly and used in the PVT solution.

6. CONCULUSION

To counter the spoofing threats, we have researched the anti-spoofing algorithm of the array antenna to overcome the jamming and spoofing issues simultaneously. We presented the theoretical analysis results of the spoofing signal response of MVDR algorithm in array antenna. Then the eigenvector algorithm using the covariance matrix is suggested and verified to work with the modified anti-jamming method. The modeling and simulation are used to confirm the effectiveness of the anti-spoofing algorithm. Also, the field test results show that the array antenna system with the proposed algorithms can perform the anti-spoofing function. Even at the stronger spoofing signal, the anti-spoofing algorithm of the array antenna can output the correct position and speed data. This anti-spoofing method using array antenna is very effective in the point of solving both the jamming and spoofing problems using the same array antenna hardware. To apply this algorithm for the real products, it is needed to make the faster digital signal processor to calculate the complex eigenvector information in the future.

AUTHOR CONTRIBUTIONS

Conceptualization, K. Lee. and M. Song.; methodology, K. Lee, M. Song, and J. Lee.; validation, K. Lee. and M. Song.; writing-original draft preparation, K. Lee.; writing-review and editing, M. Song, and J. Lee.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Akos, D.M. 2012, Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC), NAVIGATION, 59, 281-290. https://doi.org/10.1002/navi.19

Appel, M., Konovaltsev, A., & Meurer, M. 2015, Robust Spoofing Detection and Mitigation based on Direction of Arrival Estimation, Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015), Tampa, Florida, September 2015, pp.3335-3344

Berefelt, F., Boberg, B., Eklöf, F., Malmström, J., Pääjärvi, L., et al. 2003, INS/GPS Integration with Adaptive Beamforming, Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation, Portland, OR, September 2003, pp.1096-1106

Bhatti, J. & Humphreys, T. E. 2017, Hostile Control of Ships via False GPS Signals: Demonstration and Detection, NAVIGATION: Journal of The Institute of Navigation, 64, 51-66. https://doi.org/10.1002/navi.183

Broumandan, A. & Curran, J. T. 2017, GNSS spoofing detection in covered spoofing attack using antenna array, Proc. International Technical Symposium on Navigation and Timing (ITSNT), ENAC, Toulouse, France, 14-17 Nov 2017, pp.1-9

Broumandan, A., Jafarnia-Jahromi, A., Daneshmand, S., & Lachapelle, G. 2016, Overview of Spatial Processing Approaches for GNSS Structural Interference Detection and Mitigation, Proceedings of the IEEE, 104, 1246-1257. https://doi.org/10.1109/JPROC.2016.2529600

Broumandan, A. & Lachapelle, G. 2018, Spoofing Detection Using GNSS/INS/Odometer Coupling for Vehicular Navigation, Sensors, 18, 1305-1322. https://doi.org/10.3390/s18051305

De Lorenzo, D. S., Gautier, J., Rife, J., Enge, P., & Akos, D. 2005, Adaptive Array Processing for GPS Interference Rejection, ION GNSS 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005), Long Beach, CA, September 2005, pp.618-627. https://www.ion.org/publications/abstract.cfm?articleID=6256

Dempster, A. G. & Cetin, E. 2016, Interference Localization for Satellite Navigation Systems, Proceedings of the IEEE, 104, 1318-1326. https://doi.org/10.1109/JPROC.2016.2530814

Di, A. & Tian, L. 1984, Matrix Decomposition and Multiple Source Location, in ICASSP '84. IEEE International Conference on Acoustics, Speech, and Signal Processing, San Diego, CA, USA, 19-21 Mar 1984. https://doi.org/10.1109/ICASSP.1984.1172651

Fante, R. L. & Vaccaro, J. J. 2000, Wideband Cancellation of Interference in a GPS Receive Array, IEEE Transactions on Aerospace and Electronic systems, 36, 549-564. https://doi.org/10.1109/7.845241

Haefner, B., Naylor, J., & Sorber, S. 2003, G-STAR, Lockheed Martin's Advanced GPS Anti-Jam Technology, Proceedings of the 59th Annual Meeting of The Institute of Navigation and CIGTF 22nd Guidance Test Symposium, Albuquerque, NM, June 2003, pp.301-307

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, Jr., P. M. 2008, Assessing the spoofing threat: Development of a portable GPS civilian spoofer, Proc. Of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation, Savannah, GA, September 2008, pp.2314-2325

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. 2012, GPS vulnerability to spoofing threats and a review of antispoofing techniques, International Journal of Navigation and Observation, 2012, Article ID 127072, 1-16. https://doi.org/10.1155/2012/127072

Kaplan, E. D. & Hegarty, C. J. 2006, Understanding GPS: Principles and Applications, 2nd ed. (Boston: Artech House Inc.)

Konovaltsev, A., Caizzone, S., Cuntz, M., & Meurer, M. 2014, Autonomous spoofing detection and mitigation with a miniaturized adaptive antenna array, Proc. Of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation, Tampa, FL, September 2014, pp.2853-2861.

Konovaltsev, A., Marcos, E. P., Cuntz, M., Meurer, M., Wong, R., et al. 2019, Development of Array Receivers with Anti-Jamming and Anti-Spoofing Capabilities with Help of Multi-Antenna GNSS Signal Simulators, ION GNSS+ 2019, Miami, Florida, 16-20 Sept 2019, pp.953-966. https://doi.org/10.33012/2019.16988

Lee, K., So, H., Song, M., Choi, J., & Lee, J. 2021, Performance analysis of Spoofing Signal Cancellation Using Array Antenna, 2021 IPNT Conference, Gangneung, Korea, 3-5 Nov 2021, pp.341-343. http://ipnt.or.kr/2021proc/79

Li, J., Li, W., Fu, Q., & Liu, B. 2019, Research Progress of GNSS Spoofing and Spoofing Detection Technology, 2019 IEEE 19th International Conference on Communication Technology, Xi'an, China, 16-19 October 2019, pp.1360-1369. https://doi.org/10.1109/ICCT46805.2019.8947107

Monzingo, R. A. & Miller, T. W. 2004, Introduction to Adaptive Arrays (Raleigh, NC: SciTech Publishing)

Moore, T. D. 2002, Analytic study of space-time and space-frequency adaptive processing for radio frequency interference suppression, PhD Dissertation, The Ohio State University.

Park, K. & Seo, J. 2020, Performance Analysis of MUSIC-Based Jammer DOA Estimation Technique for a Misaligned Antenna Array, Journal of Positioning, Navigation, and Timing, 9, 7-13. https://doi.org/10.11003/JPNT.2020.9.1.7

Psiaki, M. L. & Humphreys, T. E. 2016, GNSS spoofing and

detection, Proc. Of the IEEE, 104, 1258-1270. https://doi.org/10.1109/JPROC.2016.2526658

Pullen, S., Gao, G., Tedeschi, C., & Warburton, J. 2012, The Impact of Uninformed RF Interference on GBAS and Potential Mitigations, International Technical Meeting of the Institute of Navigation, Newport Beach, CA, USA, Jan 2012, pp.780-789

Schmidt, R. 1986, Multiple Emitter Location and Signal Parameter Estimation, IEEE Transactions on Antennas and Propagation, 34, 276-280. https://doi.org/10.1109/TAP.1986.1143830

Seo, S., Park, Y., & Song, K. 2020, An Iterative MUSIC-Based DOA Estimation System Using Antenna Direction Control for GNSS Interference, Journal of Positioning, Navigation, and Timing, 9, 367-378. https://doi.org/10.11003/JPNT.2020.9.4.367

Spilker Jr., J. J., Axelrad, P., Parkinson, B. W., & Enge, P. 1996, The Global Positioning System: Theory and Applications, Volume1 (Washington: AIAA)

Vo, A., Falchetti, C. R., & Morrison, A. W. 2007, ADAP: Enhancing GPS Protection for Navwar, Proceedings of the 2007 National Technical Meeting of The Institute of Navigation, San Diego, CA, January 2007, pp. 990-997. https://www.ion.org/publications/abstract.cfm?articleID=7193

Kihoon Lee is a principal researcher at Agency for Defense Development. He received his B.S. from the Mechanical Engineering Department of POSTECH in 1999. He received his M.S. from the Mechanical Engineering Department of KAIST in 2001. He received his Ph.D. from the Aerospace Engineering Department of KAIST in 2018. He has served as a researcher at Agency for Defense Development since 2001. His research focuses on the development of GNSS system, Anti-Jamming and Anti-Spoofing technologies.

Min Kyu Song received the B.S. degree in electronic engineering from Konkuk University in 2011, and the M.S. and Ph.D. degrees from Yonsei University in 2013 and 2019, respectively. He is currently working at Agency for Defense Development as a senior researcher. His research interest includes coding theory, GNSS systems, and robust GNSS receiver architecture.

Jang Yong Lee is a principal researcher at Agency for Defense Development, Daejeon, Korea since 1997. He received his B.S, M.S degrees from Electronic Engineering at Chonnam National University in Korea. in 1995 and 1997. His research interests include digital communications and channel coding, satellite navigation system, anti-Jamming system.