A Novel Array Antenna-Based GNSS Spoofing Detection and Mitigation Technique

Young-Seok Lee, Jeong Seon Yeom, and Bang Chul Jung
Department of Electronics Engineering
Chungnam National University
Daejeon, South Korea
Email: yslee@o.cnu.ac.kr, jsyeom@cnu.ac.kr, bcjung@cnu.ac.kr

2023 IEEE 20th Consumer Communications & Networking Conference (CCNC) | 978-1-6654-9734-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/CCNC51644.2023.10060423

***Abstract*—We propose a novel array antenna-based global navigation satellite system (GNSS) anti-spoofing technique. In this paper, we consider a sophisticated spoofing attack scenario where a target single GNSS receiver equipped with an array antenna, a single spoofer with its own GNSS receiver, and multiple GNSS satellites exist. It is assumed that the spoofer knows the accurate location of a target GNSS receiver. The target GNSS receiver can estimate the direction of arrival (DoA) of all pseudo-random noise (PRN) code signals including the spoofing signals in real-time during the signal acquisition process. The target GNSS receiver can obtain a direction of the spoofer by exploiting the spatial characteristics of the spoofing signals in the estimated DoA information. Then, the target GNSS receiver performs the minimum mean squared error (MMSE) beamforming using the estimated authentic and spoofing DoA information. Through computer simulations, we verify that the proposed technique can effectively detect the spoofing attack with a few samples and elaborately mitigate the spoofing signal.**

***Index Terms*—Global navigation satellite system (GNSS), Anti-spoofing, Spoofing detection, Spoofing mitigation.**

I. Introduction

Recently, the use of global navigation satellite system (GNSS) has been rapidly increasing due to the applications in military and civilian industries. In particular, in some application where user location information is important such as autonomous driving, more accurate and reliable positioning should be required [1]. However, the GNSS receiver is vulnerable to intentional interference attacks such as *spoofing* that controls the tracking loop of the receiver by imitating the authentic signal [2]. Specially, it is more challenging for the GNSS receiver to recognize the spoofing attack since spoofing signal has the same signal structure and similar power level as the authentic signal [3]. Hence, GNSS anti-spoofing techniques have been emerging to effectively detect and mitigate spoofing attack. In [4], the authors proposed a signal power monitoring scheme as a simple single antenna-based GNSS spoofing detection technique. On the other hand, array antenna-based anti-spoofing techniques have been attracting significant attention since these can utilize the spatial characteristics of the received signal by exploiting multiple signal classification method [5], [6] or two-dimensional maximum likelihood estimator [7].

In most of previous works, when an abnormal signal is detected in the same direction from multiple pseudo-random noise (PRN) code signals through the DoA estimation, the spoofing signal is mitigated by forming a null in the corresponding direction [5], [8]. However, this process assumes that the power of the spoofing signal is greater than that of the authentic signals and enough samples are needed to estimate the DoA. In a sophisticated GNSS spoofing attack scenario where the spoofer can penetrate the target GNSS receiver more exquisitely and stealthily, the conventional anti-spoofing schemes cannot effectively detect the spoofing signal at the early-stage in which the power of the spoofing signal is small and the samples are not sufficiently collected to estimate DoA of the spoofer.

This work was supported in part by the DS Navcours Co., Ltd. under the array-antenna based anti-spoofing technology design, in part by the National Research Foundation of Korea (NRF) funded by the Korea government (MSIT) under Grant NRF-2021R1A4A1032580, and in part by Institute for Information & communications Technology Planning & evaluation (IITP) funded by the Korea government (MSTI) under Grant 2021-0-00486.

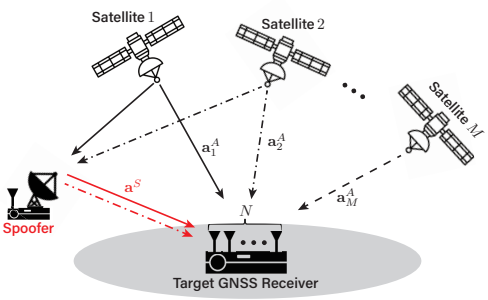

Fig. 1. System model where a single spoofer with a single antenna and a target GNSS receiver with an array antenna exist at a fixed position.

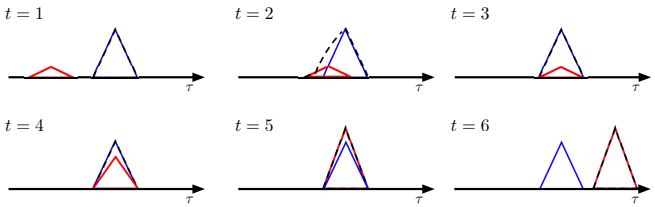

Fig. 2. GNSS Spoofing attack process in sophisticated spoofing scenario [7].

Therefore, we propose a novel array antenna-based GNSS anti-spoofing technique that make it possible to estimate DoA while elaborately detecting spoofing attack in the early stages of the sophisticated spoofing scenario. Specifically, the target GNSS receiver estimates the DoA of all PRN signals by using the simultaneous orthogonal matching pursuit (SOMP) algorithm that enables precise DoA estimation with a few samples. Then, through the estimated DoA information, we perform a spoofing detection by exploiting multi-PRN diversity effect for high detection and low false alarm performance. Finally, the minimum mean squared error (MMSE) beamforming is introduced to mitigate spoofing signal. Through computer simulations, we verify that our proposed anti-spoofing technique shows a superior spoofing detection performance, and it can effectively mitigate the spoofing signal.

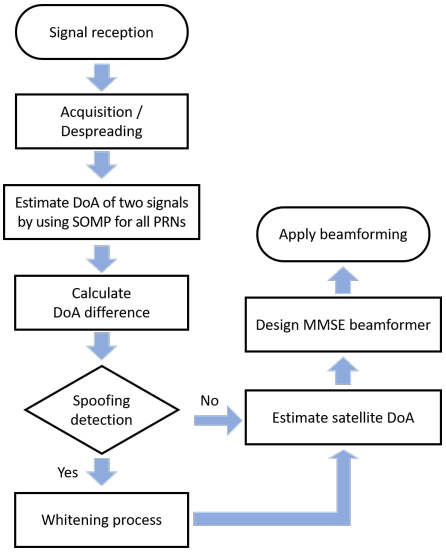

Fig. 3. Overall procedure of proposed array antenna-based GNSS anti-spoofing technique.

II. GNSS Spoofing Scenario and System Model

A. System Model

We consider a single spoofer with a single antenna and a target GNSS receiver with N-element uniform linear array (ULA) antenna at a fixed position as shown in Fig. 1. We assume that the target GNSS receiver has been acquiring and tracking M PRN authentic signals and the spoofer mimics $L(\leq M)$ PRN signals. In this paper, for precisely estimating signal source directions, we deal with post-despreading PRN signals at the target GNSS receiver after PRN code correlation and carrier frequency compensation. Therefore, post-despreading signals $\mathbf{y}$ $(\in \mathbb{C}^N)$ reconstructed from the N_s signal samples can be expressed as

$$\mathbf{y} = x^A\mathbf{a}^A + x^S\mathbf{a}^S + \mathbf{n}, \tag{1}$$

where the superscripts 'A' and 'S' mean for authentic and spoofing, respectively, x denotes the post-despreading signal, i.e., $x^A = \sqrt{N_s E^A}$ and $x^S = \alpha\sqrt{N_s E^S}$ where E denotes a received signal power and $\alpha \in [0.5, 1]$ denotes despreading gain. The vector $\mathbf{a}$ $(\in \mathbb{C}^N) = [a_1, a_2, \cdots, a_N]^T$ represent a steering vector where, for the DoA ϕ of a signal source,

$$a_\nu = e^{-j\frac{2\pi}{\lambda}(\nu-1)d\sin\phi}, \quad \text{for } \nu \ (\in \{1, \cdots, N\}) \tag{2}$$

where λ means a wavelength of GNSS signal and $d = \lambda/2$ denotes antenna spacing. The vector $\mathbf{n}$ $(\in \mathbb{C}^N)$ is an additive white Gaussian noise vector following $\mathcal{CN}(0, \sigma_n^2\mathbf{I}_N)$ after the despreading process. In a sophisticated spoofing scenario, it is assumed that the spoofer can synchronize a code chip delay of the authentic signals within 0.5 chip. The value of α depends on code chip delay difference. Note that since the target GNSS receiver has been tracking the authentic signals, the despreading proceeds according to the delay of authentic signals.

B. Sophisticated GNSS Spoofing scenario

For an effective spoofing attack, a sophisticated spoofing scenario is assumed in which the spoofer transmits multiple PRN signals with various power distribution as illustrated in Fig. 2. In addition, it is assumed that the spoofer knows the location information of the target receiver and can precisely synchronize the code chip delay and the Doppler frequency with the authentic signals by exploiting its own GNSS receiver. Specifically, from $t = 1$ to $t = 3$, the spoofer synchronizes the time delay to a lower power level than the authentic signal to prevent the target receiver from recognizing the spoofing attack. Then, from $t = 4$, the power of spoofing signal is gradually increased to steal control of the receiver's tracking loop, and finally succeed the spoofing attack through the relative code chip delay.

Therefore, in this paper, it is assumed that the power of the spoofing signal compared to the authentic signal is similar or smaller so that the target GNSS receiver can detect and respond to the spoofing attack in the early stage of such sophisticated spoofing attack scenario. The overall procedure of the proposed array antenna-based anti-spoofing technique is shown in Fig. 3.

III. Multi-PRN-based GNSS Spoofing Detection

In this section, we design a method to detect a spoofing attack by estimating the DoAs of the received signal through compressed sensing methodology. Specifically, we introduce the SOMP algorithm that can accurately estimate the DoA of signal source with a few of samples, considering the early stage of the sophisticated spoofing scenario. In each PRN signal channel, the number of signals incident to the target GNSS receiver via line-of-sight link would be up to two in which only authentic and spoofing signal are considered while multipath and interference signal are assumed to be negligible. Therefore, when partitioning the angle of incidence that can reach the target GNSS receiver into P, (1) can be represented as follows

$$\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{n}, \tag{3}$$

where $\mathbf{A}(\in \mathbb{C}^{N\times P})$ denotes a sensing matrix including steering vectors for P directions, and each column stands for a steering vector for the $p \in \{1, 2, \cdots, P\}$ direction, i.e., $\mathbf{A} = [\mathbf{a}(\phi_1)\mathbf{a}(\phi_2)\cdots\mathbf{a}(\phi_P)]$. In addition, $\mathbf{x} \in \mathbb{C}^P$ denotes a sparse received signal vector with respect to the incident direction, having up to two non-zero element for (1). Assuming there are I post-despreading signal samples, the received signal for each sample is concatenated into columns of (3), i.e., $\mathbf{Y}_i(\in \mathbb{C}^{N\times I}) = \mathbf{A}\mathbf{X} + \mathbf{N}$ where $\mathbf{X} \in \mathbb{C}^{P\times I}$ and $\mathbf{N} \in \mathbb{C}^{N\times I}$ are matrices in which the received signal and noise for each sample are concatenated as columns, respectively.

The SOMP algorithm for estimating the incident signal source is illustrated in Algorithm 1. Specifically, in the $k \in \{1, \cdots, K\}$-th iteration, each column of $\mathbf{Y}_{(k-1)}$, which is the resultant signal of the previous iteration, is multiplied by each column of $\mathbf{A}$, the steering vector for all directions. Then, the direction p_k in which the sum of the products calculated for each sample is maximum can be included in the signal direction set $\Lambda_{(k)}$. It is noticed that for the sum of the products in a specific direction, the presence or absence of a signal source is determined by setting a threshold $3I\sigma_n$ to prevent false alarms. And, the projection matrix $\mathbf{P}_k \in \mathbb{C}^{N\times N}$ is generated by exploiting the steering vectors for the direction included in the updated $\Lambda_{(k)}$. Then, the currently estimated direction components are removed by null-projection of the current signal $Y_{(k)}$, and the residual is updated. Finally, for a certain PRN channel, an element of the output $\Lambda_{(K)}$ of SOMP represents as the estimated signal source direction index.

Algorithm 1 SOMP algorithm for GNSS Spoofing Detection

Input: $\mathbf{Y} \in \mathbb{C}^{N\times I}$, $\mathbf{A} \in \mathbb{C}^{N\times P}$
Output: $\Lambda_{(K)}$.
Initialization: $\mathbf{Y}_{(0)} = \mathbf{Y}, \Lambda_{(0)} = \varnothing, k = 1$
for $k = 1, \cdots, K$ **do**
  if $\max_{p\in\mathcal{P}} \left(\sum_{i=1}^{I} | < \mathbf{a}_p, \mathbf{y}_{(k-1),i} > |\right) > 3I\sigma_n$ **then**
    $p_k = \arg\max_{p\in\mathcal{P}} \left(\sum_{i=1}^{I} | < \mathbf{a}_p, \mathbf{y}_{(k-1),i} > |\right)$
    Update $\Lambda_{(k)} \leftarrow \Lambda_{(k-1)} \cup \{p_k\}$
    $\mathbf{P}_k = \mathbf{A}\left(\Lambda_{(k)}\right)\left(\mathbf{A}\left(\Lambda_{(k)}\right)^H \mathbf{A}\left(\Lambda_{(k)}\right)\right)^{-1} \mathbf{A}\left(\Lambda_{(k)}\right)^H$
    $\mathbf{Y}_{(k)} = \left(\mathbf{I}_N - \mathbf{P}_k\right)\mathbf{Y}_{(k-1)}$
  end if
  $k = k + 1$
end for

If precise DoA is estimated for all PRN channels, the number of signals with similar DoA will exist as many as the number of PRNs counterfeited by the spoofer. Specifically, it is possible to calculate the $\binom{M+L}{2}$ DoA differences from the all of PRN signals. Through this information, we consider a vector of DoA differences as $\mathbf{\Phi} = \left[\Delta\phi_{12}\ \Delta\phi_{13}\cdots\Delta\phi_{(M+L-1)(M+L)}\right]$ where a element of $\Delta\phi_{ij}$ denotes the DoA difference of between $i \in \{1, 2\cdots, M + L - 1\}$-th PRN channel and $j \in \{2, \cdots, M + L\}$-th one for $i \neq j$, i.e., $\Delta\phi_{ij} = |\phi_i - \phi_j|$. Then, if $\binom{L}{2}$ elements that have DoA difference less than a certain threshold among $\mathbf{\Phi}$ exist, a spoofing attack can be detected and the spoofing DoA information should be found. However, in practical environment, it is not known how many PRN signals the spoofer mimics and how much difference between the two DoAs must be to be close to each other. Therefore, we first set a threshold which is a criteria for determining that the two DoAs are in the same direction. Considering the angular resolution of the receiver array antenna, array factor is used for the threshold η to determine whether the DoA of two signals is similar. When considering ULA with N elements as an array antenna, the array factor is well-known as Dirichlet sinc function [9] and we exploit the half-power beam width as a threshold η as

$$\eta = \frac{1}{2}\sin^{-1}\frac{2}{N}. \tag{4}$$

In general, the GNSS receiver receives at least 4 PRN signals to estimate its own location [7]. Inversely, that means the spoofer should successfully transmit at least 4 spoofing signals to take full control of the target receiver. Hence, a threatening spoofing attack can be detected when $6 = \binom{4}{2}$ or more elements of DoA difference smaller than η are found in $\mathbf{\Phi}$. In addition, there may be cases where the DoA difference between certain satellites is similar. This events can cause false alarms when no spoofing is present. If the spoofer mimics 4 PRN channels, there are three or more DoA ϕ_i from a specific PRN channel in that elements smaller than η. By adding this conditions, outliers can excluded for superior spoofing detection and precise spoofing mitigation. Then, the suspected DoAs are included in the spoofing candidate set $\mathcal{S}$. Finally, the average DoA of the found spoofing candidate is calculated as the calibrated spoofing DoA as

$$\hat{\phi}_s = \frac{1}{|\mathcal{S}|}\sum_{s\in\mathcal{S}}\phi_s, \tag{5}$$

where $|\cdot|$ means the cardinality of a matrix. With this approach, the more PRNs the spoofer mimics to successfully attack the target GNSS receiver, the more accurately the spoofing DoA information can be estimated due to the multi-PRN diversity.

IV. MMSE Beamforming-based GNSS Spoofing Mitigation

In this section, we propose a spoofing mitigation technique based on MMSE beamforming exploiting the spoofing and authentic DoA information estimated in the spoofing detection procedure. Note that once the spoofing attack is detected, the target GNSS receiver can know that PRNs were counterfeited through our proposed spoofing detection process.

For the spoofed signal of (1), the received signal can be re-expressed as

$$\mathbf{y} = x^A\mathbf{a}^A + \mathbf{z}, \tag{6}$$

where $\mathbf{z}(\in \mathbb{C}^N) = x^S\mathbf{a}^S + \mathbf{n}$ includes the component of both spoofing signal and additive noise, so that it can be seen to a colored noise in the spatial domain. Then, by exploiting the estimated spoofing DoA information, the matrix $\mathbf{K}_z \in \mathbb{C}^{N\times N}$ for whitening the signal in (6) can be calculated as follows

$$\mathbf{K}_z = \sigma_n^2\mathbf{I}_N + \tilde{P}^S\mathbf{a}(\hat{\phi}_s)\mathbf{a}(\hat{\phi}_s)^H, \tag{7}$$

where $\mathbf{a}(\hat{\phi}_s)$ means the steering vector for the estimated spoofing DoA as defined in (2) and $\tilde{P}^S$ means the power of spoofing signal after despreading approximated by the average received power of satellite signal.[1] Then, (6) can be whitened by exploiting (7). Thereby, the direction of the remaining authentic signal can be estimated with reduced error. Finally, using the estimated satellite and spoofing DoA information, the MMSE beamformer of a specific spoofed PRN can be designed as follows

$$\mathbf{w}_{\mathrm{MMSE}}(\in \mathbb{C}^N) = \mathbf{K}_z^{-1}\mathbf{a}(\hat{\phi}_A), \tag{8}$$

where $\mathbf{a}(\hat{\phi}_A) \in \mathbb{C}^N$ denotes the authentic steering vector calculated by exploiting re-estimated DoA information of satellite. Then, by applying (8) to (1), MMSE beamforming can be performed. Here, (8) consists of the signal whitening process and matched filtering in the spatial domain for the whitened signal. Thus, MMSE beamforming can maximize signal to interference plus noise ratio (SINR) by attenuating the spoofing signal considered interference to the noise level and maximizing the signal power in the direction of the satellite [10].

V. Simulation Results

In simulation setup, the target GNSS receiver equipped with 7-elements ULA antenna would receive GPS L1 C/A signals from 9 visible satellites and a single spoofer. The DoA information of each signal source is illustrated in Table I for $[-90°, 90°]$ where the partition of azimuth angle P for DoA estimation is set to $1°$ resolution. Here, the spoofer mimics the satellite PRN signals received on channels 1 to 4 of the target receiver. We set the sampling frequency to 2 MHz, the received authentic signal power to -158 dBW, and the received

[1]Since there is no assumption in this paper that the power of the spoofing signal is greater than that of the authentic signal, the exact power of the spoofing signal cannot be known. However the altitude and transmit power of satellites are well-known, and the despreading gain can be calculated from the number of samples used in despreading process, allowing the GNSS receiver to easily calculate the average received power of satellite signal.

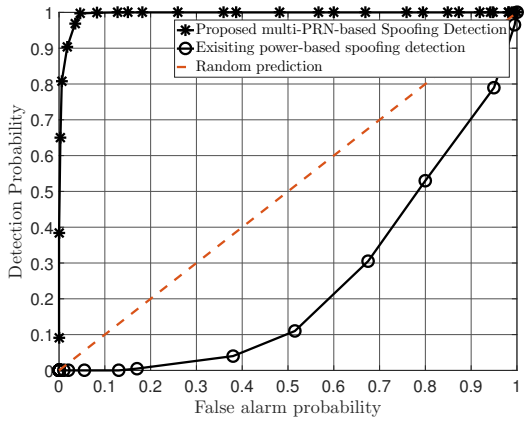

Fig. 4. Receiver operating characteristic curves of the proposed multi-PRN-based GNSS spoofing detection technique

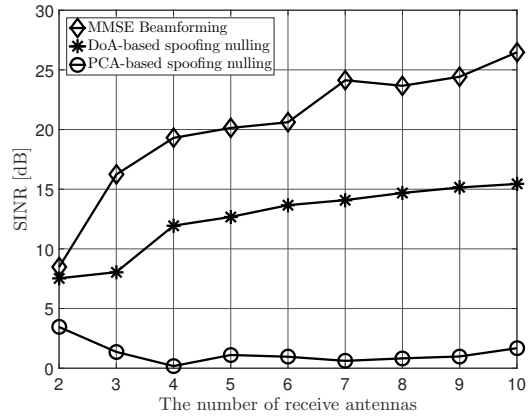

Fig. 5. SINR performance of the proposed MMSE beamforming-based spoofing mitigation technique

noise power to -140 dBW. It is also assumed that the spoofer is perfectly synchronized with the Doppler frequency of the authentic signal and the code delay difference is 0.5 chips. Also, the received power of spoofing signal is the same as that of the authentic signal. The time at which the anti-spoofing algorithm starts to operate is set to 10 ms after signal reception.

Fig. 4 shows the receiver operating characteristic (ROC) curves of proposed multi-PRN diversity-based spoofing detection technique. In this paper, 1,000 Monte-Carlo experiments were performed, and the spoofing detection and false alarm probability mean the ratio of the number of spoofing detection to the total number of simulations when spoofing signal is present and absent, respectively. The existing power-based spoofing detection operates by monitoring the power of the received signal when multiple signals are received in the same direction. Hence, this method works only when the power of the spoofing signal is 3 dB or more higher than that of the authentic signals. On the other hand, even considering the early stages of a sophisticated spoofing scenario, our proposed multi-PRN-based spoofing detection technique has high spoofing detection and low false alarm performance.

Fig. 5 shows the SINR performance for varying the number of receive antennas. In this paper, the SINR of the PRN signal for channel 1 is analyzed. Spoofing mitigation techniques in Fig. 5 refer to a principal component analysis (PCA)-based spoofing nulling where the steering vector of spoofing signal is approximated as an eigenvector corresponding to the maximum eigenvalue of the auto-correlation function, DoA-based spoofing nulling where a null is formed by exploiting

TABLE I
DoA INFORMATION OF AUTHENTIC AND SPOOFING SIGNAL

PRN number	Azimuth angle(°)	PRN number	Azimuth angle(°)
PRN2(ch.1)	-20	PRN8(ch.2)	54
PRN14(ch.3)	-5	PRN18(ch.4)	60
PRN20(ch.5)	-30	PRN22(ch.6)	-90
PRN24(ch.7)	40	PRN25(ch.8)	80
PRN26(ch.9)	-70	Spoofer	20

estimated spoofing DoA information, and the proposed MMSE beamforming. The PCA-based technique is the simplest way, but works only when the power of spoofing signal is greater than that of authentic signal. DoA-based spoofing nulling can form a null in the direction of the spoofer, but the noise component in the spatial domain would be boosted in all directions except the direction of spoofing signal. On the other hand, the MMSE beamforming for spoofing mitigation outperforms the other spoofing mitigation techniques in terms of the SINR performance by performing matched filtering on the direction of the satellite while mitigating the spoofing signal. It is worth noting that the ultimate goal of satellite signal processing is about how well the GNSS receiver can receive the authentic signals. This superiority is rather emphasized as the number of receive antennas increases since the beam in the direction of the satellite becomes sharper.

VI. Conclusion

In this paper, we proposed an array antenna-based GNSS anti-spoofing technique in early stages of sophisticated spoofing scenario. We exploited spatial characteristics of spoofing signals, multi-PRN diversity, and the MMSE beamforming in order to spoofing detection and mitigation. Through computer simulations, we verified that the proposed technique can effectively detect a spoofing attack due to the precise DoA estimation using SOMP algorithm even with a few samples and the DoA calibration procedure with multi-PRN diversity. Therefore, the target GNSS receiver can elaborately mitigate the spoofing signals while forming a precise beam in the direction of the satellite.

References

[1] J. Neil, L. Cosart, and G. Zampetti, "Precise timing for vehicle navigation in the smart city: An overview," *IEEE Commun. Mag.*, vol. 58, no. 4, pp. 54–59, Apr. 2020.
[2] T. E. Humphreys *et. al.*, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Techn. Meet. Satellite Division ION GNSS*, Savannah, GA, Sep. 2008, pp. 2314–2325.
[3] A. Broumandan, R. Siddakatte, and G. Lachapelle, "An approach to detect GNSS spoofing," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 8, pp. 64–75, Aug. 2017.
[4] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 739–754, Apr. 2018.
[5] J. Zhang, X. Cui, H. Xu, and M. Lu, "A two-stage interference suppression scheme based on antenna array for GNSS jamming and spoofing," *Sensors*, vol. 19, no. 18, pp. 3870, Sep. 2019.
[6] Y. Hu, S. Bian, B. Li, and L. Zhou, "A novel array-based spoofing and jamming suppression method for GNSS receiver," *IEEE Sensors J.*, vol. 18, no. 7, pp. 2952–2958, Apr. 2018.
[7] J. Magiera, "A multi-antenna scheme for early detection and mitigation of intermediate GNSS spoofing," *Sensors*, vol. 19, no. 10, pp. 2411, May 2019.
[8] J. H. Noh, B. H. Gong, Y. -S. Lee, B. C. Jung, and S. J. Lee, "Performance analysis of GNSS spoofing mitigation techniques based on array antennas in various spoofing scenario," in *Proc. of the 2021 ITM ION GNSS*, Jan. 2021, pp. 282–294.
[9] D. Reed and A. Rodriguez-Herrera, "Array factor derived from a correlation matrix," in *Proc. 13th Eur. Conf. Antennas Propag.*, Krakow, Poland, Mar. 2019, pp. 1–5.
[10] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication.* Cambridge, U.K,: Cambridge Univ. Press, 2005.