JPNT 5(3), 131-136 (2016)
http://dx.doi.org/10.11003/JPNT.2016.5.3.131

JPNT Journal of Positioning, Navigation, and Timing

The Performance Analysis of Beamforming Algorithm for Anti-Spoofing

Yun Sub Choi[1], Sun Yong Lee[1], Chansik Park[2], Byoung Sun Ahn[3], Hyun Hee Won[3], Sang Jeong Lee[1†]

[1]Department of Electronics Engineering, Chungnam National University, Daejeon 34134, Korea
[2]Department of Electronics Engineering, Chungbuk National University, Cheongju 28644, Korea
[3]LIG Nex1 Co., Ltd., Seongnam 13488, Korea

ABSTRACT

The present paper shows that beamforming algorithm such as Minimum Variance Distortionless Response (MVDR) based on array antenna signal processing can have not only anti-jamming but also anti-spoofing characteristics. A beam pattern due to the beamforming algorithm strengthens received signal power as it is formed in the incident direction of desired signal. During the process, the effect of unnecessary signals such as spoofing signals can be reduced because the beam pattern reduces received signal power in the incident directions excluding the beam pattern-directed direction. In order to analyze the anti-spoofing effect due to the beamforming algorithm, a software-based simulation environment was configured. An arbitrary error was applied between incident direction of Global Positioning System (GPS) satellite signal and steering vector direction of the beamforming algorithm to analyze the received signal power and required conditions were provided to see the anti-spoofing effect due to the beamforming algorithm. The used antenna was 7-element planar circular array and beam patterns were formed through the MVDR algorithm.

Keywords: anti-jamming, beamforming, MVDR

1. INTRODUCTION

A Global Navigation Satellite System (GNSS) has been used in various areas more and more. As the GNSS has been applied to not only personal uses but also nation's main infrastructures, concerns about performance degradation and failure of the GNSS have also increased. In order to use the GNSS continuously and safely, a number of studies on techniques to cope with deliberate interference such as jamming signals or spoofers have been conducted. As a typical countermeasure against interference source, adaptive Controlled Radiation Pattern Antennas, spatial nuller or beamformer based on array antenna signal processing has been proposed. They are common in suppressing interference signals which have higher signal power than thermal noise level at the spatial domain using a phase difference of signals which are incident at each element in the array antenna. In contrast, a technique to cope with spoofing signals is various because spoofing signals are transmitted with lower power than thermal noise level, which is similar to that of Global Positioning System (GPS) signal power. A spoofer let a target receiver trace its own signal rather than authentic GPS signal thereby providing disturbed navigation data to the target receiver or degrading quality of pseudo-range measurement values thereby increasing a navigation error.

Largely, there are two categories of countermeasures against spoofing signals: spoofing detection and spoofing mitigation techniques. The spoofing detection technique aims to detect spoofing signals by monitoring a variety of parameters in a GPS receiver constantly and the spoofing mitigation technique aims to remove the effect of spoofing signals directly. The aforementioned array antenna-based

Received Apr 28, 2016 **Revised** Aug 03, 2016 **Accepted** Aug 08, 2016
†**Corresponding Author**
E-mail: eesjl@cnu.ac.kr
Tel: +82-42-825-3991 Fax: +82-42-823-5436

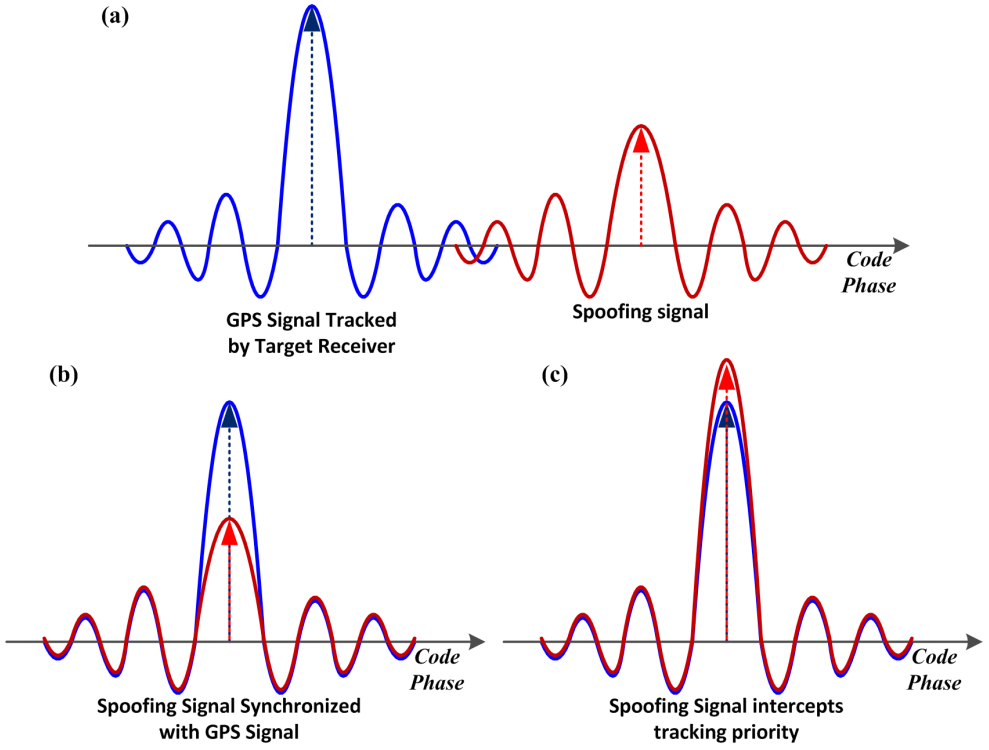

Fig. 1. GPS receiver structure

signal processing techniques, which are made to cope with jamming, are also classified into the spoofing mitigation technique. This is because the array antenna-based signal processing techniques can improve reception power of specific signal in the spatial domain or reduce reception power of unwanted signals. However, even if array antenna-based signal processing methods are capable of mitigation spatially using incident signals to various elements, this capability is not always desirable. This is because an incident direction of spoofing signal can be highly similar to the incident direction of GPS satellite signal although not exactly the same. Although beam pattern or null pattern can be formed in a specific direction using an array antenna-based signal processing technique, their resolution is clearly limited so that array antenna-based signal processing technique cannot guarantee the removal of spoofing signals always. Thus, the present study derives conditions that can remove spoofing signals when array antenna-based signal processing technique, in particular beamforming algorithm, is used against spoofing signals. To achieve this goal, the present study configured simulation environment based on software and 5-Tap applied Minimum Variance Distortionless Response (MVDR) algorithm was applied assuming 7-element planar circular array antenna with 9.5 cm gap between elements.

2. SPOOFING

2.1 Spoofing Attack on GPS

Spoofing attack to the GPS is shown in Fig. 1. In Fig. 1, a peak correlation value of receiver that is targeted by spoofing signal is depicted. A blue-colored correlation value in Fig. 1a refers to authentic GPS signal that is traced normally by the GPS receiver and a red-colored correlation value is a correlation value that can be generated by spoofing signal. Since spoofing signal power (correlation value) is lower than that of the authentic GPS signal in the current condition, the effect of spoofing signal is not revealed in the GPS receiver. In Fig. 1b, spoofing signal is synchronized with the GPS signal to have the same code phase with that of correlation value due to the GPS signal. At this condition, if the spoofing signal power is increased, a GPS receiver traces the spoofing signal rather than the authentic GPS signal. Then, if the spoofing signal adjusts the code phase arbitrarily, quality of a pseudo-range measurement in the targeted GPS receiver is degraded resulting in adverse effect on navigation and timing performance. With precise spoofer, it can make fool of GPS receivers into erroneous positioning information, which is totally different from actual position (Hengqing et al. 2005, Jafarnia-Jahromi et al. 2012).

2.2 Anti-Spoofing Techniques

The anti-spoofing technique can largely be divided into two: detection and mitigation techniques. The spoofing detection technique is focusing on how to detect spoofing signal rather than removing the effect of spoofing signal. In contrast, the spoofing mitigation technique copes with spoofing attack proactively, focusing on neutralizing the effect by detecting spoofing signal and recovering navigation capabilities of receivers that are damaged by spoofing signals. There are various techniques in the spoofing detection technique: absolute power monitoring using received signal power, C/N0 monitoring method, and L1/L2 power comparison etc. For spoofing mitigation technique, Receiver Autonomous Integrity Monitoring, Vestigial Signal Detection, and Beamforming algorithm are found. In previous studies, beamforming algorithm was already classified into anti-spoofing technique but no analysis on reception power with regard to GNSS receivers have been done (Hengqing et al. 2005, Jafarnia-Jahromi et al. 2012).

3. BEAMFORMING ALGORITHM

3.1 Signal Modeling and Optimal Weight of MVDR Algorithm

As shown in Fig. 2, 7-element planar circular array antenna was used. Assuming that a gap between elements was constant at λ (≃9.5 cm) and M signals are received, the received signal vector can be expressed as the following equation.

$$\mathbf{x}(t) = \mathbf{A}(\theta,\ \phi)s(t) + \mathbf{n}(t) \tag{1}$$

Here, $\mathbf{A}(\theta, \phi)$ refers to an incident direction of signals which are incident at each element antenna, that is steering vector. θ and ϕ refer to azimuth and elevation angle of the incident signal $s(t)$. $\mathbf{n}(t)$ refers to a noise vector, which is Additive White Gaussian Noise which has zero mean and σ_n^2 variance. The output of the MVDR algorithm is expressed in Eq. (2).

$$y(t) = \sum_{n=0}^{N} w_n^* s_n(t) = \mathbf{w}^{\mathrm{H}}\mathbf{s}(t) \tag{2}$$

The MVDR algorithm minimizes the output power and it is operated as constraint to have unity gain in the beam pattern direction of array antenna. The given constraint is expressed as shown in Eq. (3).

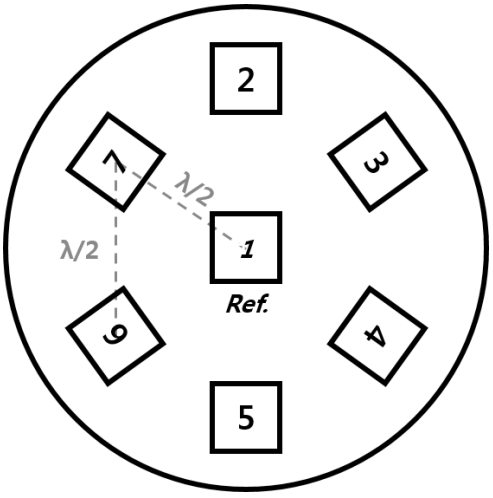

Fig. 2. Geometry of 7-element planar circular array.

$$\min_{\mathbf{w}} \mathbf{w}^H \mathbf{R}\mathbf{w} \quad \text{s.t.} \quad \mathbf{w}^H a(\theta_0, \phi_0) = 1 \tag{3}$$

Here, $a(\theta_0, \phi_0)$ refers to a steering vector of desired signal and optimal weight of the MVDR algorithm can be calculated on the basis of Eq. (3) as shown in Eq. (4) (Godara 2004).

$$\mathbf{w} = \frac{\mathbf{R}^{-1}a(\theta_0, \phi_0)}{a(\theta_0, \phi_0)^H \mathbf{R}^{-1}a(\theta_0, \phi_0)} \tag{4}$$

3.2 Anti-spoofing Process by Beamformer

If a few conditions can be met, spoofing signals can be removed and free from the threat of spoofing using array processing-based beam steering technique. One of the conditions is that all incident directions of GPS satellite signal are known through almanac data or ephemeris aiding or pre-decoding. The incident direction of satellite signal is valid when posture information of vehicle is known. One other condition is that incident directions of authentic GPS signal and spoofing signal are not matched.

If the above conditions are all met, a receiver forms a beam pattern in the incident direction of the authentic GPS signal, which is originally traced, thereby increasing the received signal power of the authentic GPS signal and reducing the received signal power of the spoofing signal. Accordingly, intensities of the received signal powers of authentic GPS signal and spoofing signal are reversed as shown in Fig. 3 thereby removing the effect of spoofing signal and tracing only GPS signal. However, since a beam-width and a beam-depth of the beam pattern formed by the MVDR algorithm are limited, it is not necessarily true that spoofing signal is removed via the same process as shown

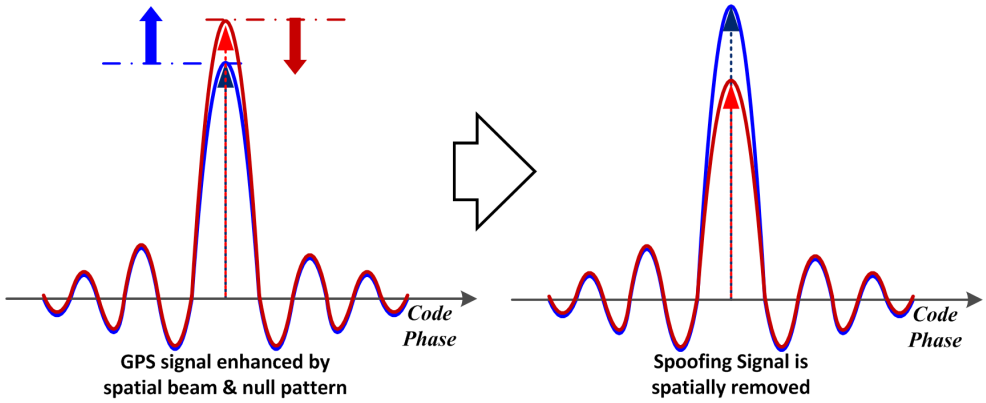

Fig. 3. Spoofing signal mitigation by STAP structure.

Table 1. GPS receiver parameters.

Parameters	Value
Radio frequency (MHz)	1575.42
Intermediate frequency (MHz)	2.5
Sampling frequency (MHz)	40
Array type	Circular
Array elements (#)	7
Array spacing (cm)	9.5 ($\simeq\lambda/2$)

in Fig. 3 in all cases. Depending on the characteristics of formed beam patterns, areas where spoofing signal is removed or not can be distinguished. This was verified through simulations.

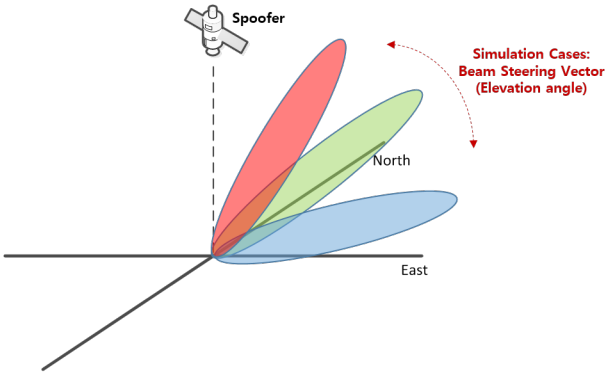

Fig. 4. Simulation setup - steering vectors.

4. SIMULATION SETUP AND RESULTS

4.1 Simulation Setup

As mentioned in the above, a 7-element Planar Circular Array Antenna whose gap between elements was approximately 9.5 cm was used and a receiver with GPS L1 band was assumed. The down-conversion medium frequency was set to 2.5 MHz and sampling frequency was set to 40 MHz. Table 1 summarizes the parameters related to antennas and receivers.

In order to analyze how long the separation shall be taken by the direction of the beam pattern formed by the MVDR algorithm from the incident direction of the spoofing signal to remove the effect of spoofing signal, a spoofer was positioned at the zenith axis, which was perpendicular to the ground at the receiver location and azimuth was fixed while elevation angle was changed from 90° to 76° by an increment of 2° in the steering vector direction in the MVDR algorithm as shown in Fig. 4 to conduct simulations. Here, changes in posture of vehicle were not considered and only incident direction of satellite signal was taken into consideration. For spoofing power, four cases were analyzed with regard to general GPS transmitted power: +0 dB, + 1.5 dB, + 3 dB, and +4.5 dB. Since spoofing can be easily detected via C/N0 monitoring only with high spoofing power, spoofing power that was less than +6 dB was considered (Hengqing et al. 2005, Jafarnia-Jahromi et al. 2012). The anti-spoofing effect analysis due to beamforming algorithm was conducted with power that can make disturbance to the spoofing detection process. When spoofer power was +0 dB, it can provide criteria how much received power shall be reduced with beam pattern or null pattern in order for GPS receivers not to trace spoofing signal. A mean of 10 simulations was indicated.

4.2 Results

Figs. 5 and 6 show the simulation results. Fig. 5 shows the radiation pattern, which is depicted using a weight derived from the MVDR algorithm. Only 90° and 78° were depicted among simulation cases. The x-axis in Fig. 6 refers to a change in elevation angle of the steering vector and the y-axis refers to received signal power of spoofing signal derived by the peak correlation value. The graph can reveal how many degrees (°) shall be separated from the incident direction

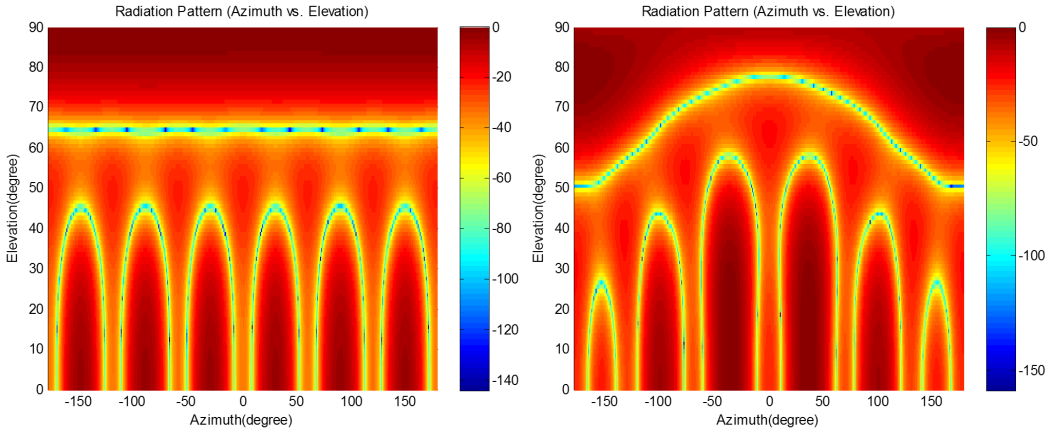

Fig. 5. Simulation results – radiation pattern (left: 90°, right: 78°).

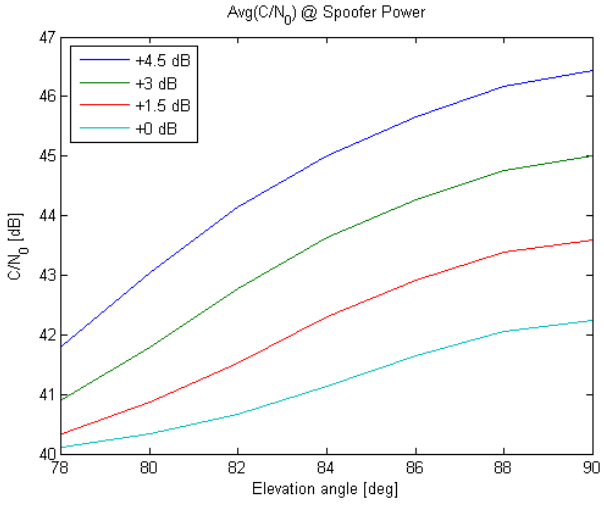

Fig. 6. Simulation results – received signal power.

Table 2. Requirement of spoofer mitigation.

Spoofer power (dB)	Elevation angle (°)	Separation angle (°)
+0	88	2
+1.5	83	7
+3.0	81	9
+4.5	79	11

of actual spoofing signal in order to remove spoofing signal effectively. For +0 dB, which corresponds to GPS nominal transmitted power, the highest received signal power at 90° elevation angle, in which steering vector direction and signal incident direction are matched, is approximately 42 dB/Hz. If the received signal power of spoofing signal is less than 42 dB/Hz, the GPS receiver will not be disturbed by the spoofing signal. Table 2 summarizes elevation angles where the received signal power becomes smaller than 42 dB/Hz in experimental cases other than +0 dB. If reception power of spoofing signal is less than 42 dB/Hz, GPS receiver will trace the authentic GPS signal. On the basis of 90° where beam pattern and satellite signal incident directions are matched based on the elevation angles indicated in Table 2, separation angle that is required between satellite signal and spoofing signal incident directions can be calculated. This is also presented in Table 2.

Now, a region where spoofing signal whose power is slightly higher than the GPS nominal transmit power is not removed can be predicted. For example, if spoofing signal whose power is +1.5 dB with regard to satellite signals that are incident in the zenith-axis direction is incident at a range of azimuth 0 to 360° and elevation angle 83-90°, it cannot be removed.

5. CONCLUSIONS

The present paper analyzed the required conditions when the effect of spoofing signal is removed through beamforming technique such as MVDR algorithm. It was analyzed via software-based simulations and 7-element Planar Circular Array whose gap between elements was 9.5 cm was employed. The MVDR algorithm of STAP structure using 5-Tap was applied. A region where spoofing signal was not removed due to each resolution of beam pattern formed by the beamforming algorithm was derived and the region was increased as spoofer power was increased. A separation angle required when spoofer power was +4.5 dB was approximately 11° and approximately 24% of total range, which corresponded to azimuth 0-360° and elevation angle 0-90°, was found as a region where spoofing signal cannot be removed.

In recent years, the beamforming algorithm has been closely related to GPS receivers more than ever so a number of studies on methods of applying constraints to

maximize SNR or C/N0 have been conducted using signals after correlator. Methods using signals of front part of RF such as MVDR algorithm require pre-information about GPS satellite locations whereas beamforming algorithms after correlator do not require pre-information as well as jamming removal performance is comparable. Despite the above advantages, the beamforming algorithms after correlator may derive a weight that can maximize received signal power always thereby being vulnerable to spoofing signals. The effect of spoofing signals on beamforming algorithms after correlator will be the future research subject.

REFERENCES

Godara, L. C. 2004, Smart Antennas (New York: CRC Press)

Hengqing, W., Huang, P. Y., Dyer, J., Archinal, A., & Fagan, J. 2005, Countermeasures for GPS Signal Spoofing, Proceedings of the 18th International Technical Meeting of the Satellite Division of the ION GNSS 2005, pp.1285-1290.

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. http://dx.doi.org/10.1155/2012/127072

Yun Sub Choi received the B.S. degrees from in Electronics Engineering at Chungnam National University in 2010. His research interests include GNSS receivers and anti-jamming techniques.

Sun Yong Lee received the B.S. degrees from in Electronics Engineering at Chungnam National University in 2013. His research interests include GNSS receivers and signal processing techniques

Chansik Park is currently a Professor in the Department of Electronics Engineering at Chungbuk National University, Chungju, Korea. His research interests are in the general area of signal processing and precise positioning using carrier phase measurement.

Byoung Sun Ahn received B.S., M.S., degrees from in electrical and electronics engineering from Chung-Ang University, Seoul, Korea. He is currently a research engineer in communication R&D laboratory, LIG Nex1 Co,.Ltd. His research interests are in the area of digital beamforming and adaptive processing.

Hyun Hee Won received B.S. degree from in computer science and electical engineernig from Handong Global University, Phohang, Korea. He is currently a research engineer in commnuication R&D laboratory, LIG Nex1 Co,.Ltd. His research interests are in the area of array signal processing and adaptive processing.

Sang Jeong Lee is currently a Professor in the Department of Electronics Engineering at Chungnam National University, Daejeon, Korea. He received the Doctor's degree in Control and Measurement in Seoul National University in 1987. His research interests include GNSS and Robust Control.