JPNT 7(3), 127-138 (2018)
https://doi.org/10.11003/JPNT.2018.7.3.127

JPNT Journal of Positioning, Navigation, and Timing

Development of Anti-Spoofing Equipment Architecture and Performance Evaluation Test System

Junwoo Jung[1†], Sungyeol Park[1], Jongchul Hyun[1], Haengik Kang[1], Kiwon Song[2], Kapjin Kim[2], Youngbum Park[2]

[1]Precision Guided Munitions Research Center, LIG Nex1, Sungnam 13488, Korea
[2]The Third R&D Institute - 4, Agency for Defense Development (ADD), Daejeon 34186, Korea

ABSTRACT

Spoofing attacks including meaconing can provide a bogus position to a victim GPS receiver, and those attacks are notably difficult to detect at the point of view on the receiver. Several countermeasure techniques have been studied to detect, classify, and cancel the spoofing signals. Based on the countermeasure techniques, we have developed an anti-spoofing equipment that detects and mitigates or eliminates the spoofing signal based on raw measurements. Although many anti-spoofing techniques have been studied in the literatures, the evaluation test system is not deeply studied to evaluate the anti-spoofing equipment, which includes detection, mitigation, and elimination of spoofing signals. Each study only has a specific test method to verify its anti-spoofing technique. In this paper, we propose the performance evaluation test system that includes both spoofing signal injection system and its injection scenario with the constraints of stand-alone anti-spoofing techniques. The spoofing signal injection scenario is designed to drive a victim GPS receiver that moves to a designed position, where the mitigation and elimination based anti-spoofing algorithms can be successively evaluated. We evaluate the developed anti-spoofing equipment and a commercial GPS receiver using our proposed performance evaluation test system. Although the commercial one is affected by the test system and moves to the designed position, the anti-spoofing equipment mitigates and eliminates the injected spoofing signals as planned. We evaluate the performance of anti-spoofing equipment on the position error of the circular error probability, while injecting spoofing signals.

Keywords: anti-spoofing equipment, anti-spoofing structure, anti-spoofing evaluation test system, spoofing injection scenario

1. INTRODUCTION

The global positioning system (GPS) was originally developed for the U. S. military in the 1970s (Kaplan & Hegarty 2006). Recently, the GPS has become one of the most popular technologies of navigation. The widespread usage of GPS in terrestrial, marine, and airborne applications has been precipitated by its accuracy, global availability and low cost of user equipment. Additionally, military GPS applications require enhanced robustness against unintentional or intentional interferences such as jamming and spoofing signals (Jung et al. 2014). The jamming and spoofing interferences intentionally mask the weak GPS signals that transmit ranging codes and navigation data using the direct sequence spread spectrum.

Among the intentional interferences, we focus on the spoofing signal attack, which includes the meaconing signal attack. Based on the synchronization to GPS signals, the spoofing attack can provide a bogus position to a victim GPS receiver and the spoofing attack is not easily detectable. At the point of view on a GPS receiver, strong spoofing signals can affect both cross-correlation and multiple access interference (MAI) and increase the noise floor, which adversely affects the tracking performance of the authentic GPS signals. Meanwhile, weak spoofing signals can only affect authentic GPS signals on the same pseudo-range number (PRN) to the spoofing signal.

Several countermeasure techniques for GPS spoofing signals have been studied and classified (Wen et al. 2005,

Received July 19, 2018 **Revised** Aug 17, 2018 **Accepted** Aug 24, 2018
†**Corresponding Author**
E-mail: junu.jung@gmail.com
Tel: +82-31-8026-4598 Fax: +82-31-8026-7088

Humphreys et al. 2008, Jeong et al. 2012). These techniques define and use specific features of the spoofing signals to separate them from authentic signals. A spoofer should know the approximate position of a victim receiver and the propagation channel between the spoofer antenna and the receiver antenna pattern to determine the spoofing power level and generate an approximate code phase of a spoofing signal. The victim receiver information is notably difficult to obtain in real-world spoofing situations and many spoofing countermeasure techniques depend on monitoring the power level of the received GPS signals to detect spoofing signals. In particular, the power level is the most useful detection and classification metric to separate spoofing signals from authentic ones. In Nielsen et al. (2012) and Jafarnia-Jahromi et al. (2014), the presence of spoofing signals is detected based on abnormally high carrier-to-noise ratios (CNRs) and excessive power levels after the pre-despreading method, respectively.

In many practical cases, a spoofer generates multiple fake GPS signals which provide a consistent navigation solution and transmits them using a single antenna. As such, the spoofing power level is sufficiently strong to lose the tracked authentic GPS signals because of cross-correlation and MAI. In order to reduce and eliminate the effectiveness of the strong spoofing signals, several spoofing cancellation and elimination techniques have been studied (Madhani et al. 2003, Broumandan et al. 2012, Kim et al. 2013). In Madhani et al. (2003), the successive interference cancellation technique has been applied to reduce the effect of the structured GPS-like signals, such as spoofing signals, whose power is higher than the ambient noise. In Broumandan et al. (2012), the technique discriminates spoofing signals to detect their presence or occurrence based on the spatial correlation of the spoofed signals using multiple antennas. Then, a spoofing cancellation technique is used to track and remove the spoofed signals and produce a spoof-free signal, which is subsequently tracked by the receiver. In Kim et al. (2013), the technique generates the reciprocal spoof signals with an anti-phase code based on the received spoofed signals. They confirm that the spoofed signals disappear when the code phase of the generated anti-spoofing signal exactly matches the authentic GPS signal.

In this paper, we propose a performance evaluation test system that includes both spoofing signal injection system and its injection scenario with the constraints of stand-alone anti-spoofing techniques. Although many anti-spoofing techniques have been studied in the aforementioned literatures, the evaluation test system has not been deeply studied to evaluate the anti-spoofing equipment with functions to detect, mitigate, and eliminate spoofing signals. The aforementioned studies only have a specific test method to evaluate and verify its anti-spoofing technique. In this paper, we design a spoofing injection scenario to drive a victim GPS receiver that moves to a designed bogus position, where the mitigation and elimination based stand-alone anti-spoofing techniques can provide a reliable position and navigation solution and be successively evaluated. We evaluate the developed anti-spoofing equipment and a commercial GPS receiver using our proposed performance evaluation test system. In the developed anti-spoofing equipment, there are two main techniques to neutralize the effect of spoofing signals: the mitigation technique, which does not use the detected spoofing signals in the navigation solution, and the elimination technique, which successively tracks and removes the detected spoofing signals from the received GPS signals. For the evaluation test system, we assume that all spoofing signals are generated and transmitted from a single source. While injecting spoofing signals, we evaluate the performance of the anti-spoofing equipment in terms of the position error of the circular error probability (CEP).

The remainder of this paper is organized as follows. Section 2 provides an overview of the structure of an anti-spoofing equipment we developed. In Section 3, we propose the performance evaluation test system, which includes a spoofing injection scenario to evaluate the anti-spoofing equipment. Section 4 shows the test results and discusses the developed anti-spoofing equipment in the anechoic chamber using our proposed evaluation test system. The summarized conclusions and future works are provided in Section 5.

2. ANTI-SPOOFING EQUIPMENT STRUCTURE

We present the model of received GPS signals in the presence of spoofing signals from an intentional spoofer. The received signals with N authentic signals and K spoofing signals from a spoofer can be modeled as

$$\begin{aligned} r(t) &= \sum_{n=1}^{N} S_n(t) + \sum_{k=1}^{K} S_{SP\_k}(t) + \eta(t) \\ &= \sum_{n=1}^{N} \sqrt{\rho_n^s}\, d_n^s\left(t-\tau_n^s\right) c_n^s\left(t-\tau_n^s\right) e^{j\phi_n^s + j2\pi f_n^s t} \\ &\quad + \sum_{k=1}^{K} \sqrt{\rho_k^{SP}}\, d_k^{SP}\left(t-\tau_k^{SP}\right) c_k^{SP}\left(t-\tau_k^{SP}\right) e^{j\phi_k^{SP} + j2\pi f_k^{SP} t} + \eta(t) \end{aligned} \quad (1)$$

where p_n^s, ϕ_n^s, f_n^s, and τ_n^s are the signal power, carrier phase, Doppler frequency, and time delay of the n-th authentic signal, respectively. $d_n^s(t)$ and $c_n^s(t)$ are the

https://doi.org/10.11003/JPNT.2018.7.3.127

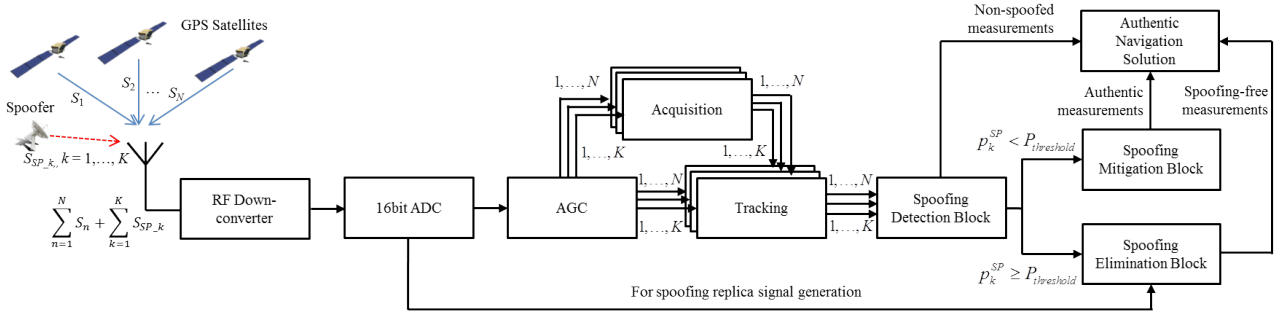


Fig. 1. Structure design of the anti-spoofing equipment.

transmitted data bit and PRN code sequence of the n-th authentic signal at time t. $p_k^{SP}, \phi_k^{SP}, f_k^{SP}$, and τ_k^{SP} are the signal power, carrier phase, Doppler frequency, and time delay of the k-th spoofing signal, respectively. $d_k^{SP}(t)$ and $c_k^{SP}(t)$ are the data bit and PRN code sequence of the k-th spoofing signal, which is synchronized to a specific authentic signal at time t. $\eta(t)$ is the complex additive white Gaussian noise with variance σ^2.

Fig. 1 shows the receiver structure block diagram of the developed anti-spoofing equipment. The anti-spoofing equipment is based on a GPS receiver using a 16-bit analog-to-digital converter (ADC) to increase the resolution of the spoofing signal tracking performance. Based on the information from the acquisition and tracking blocks of the authentic and spoofing signals, the spoofing signals are monitored and detected among N authentic signals and K spoofing signals. The detected spoofing signals are mitigated or eliminated with criteria of the spoofing signal power. If the spoofing signal power is higher than the threshold, $P_{threshold}$, the tracked authentic signals are lost because of the MAI induced by the high cross-correlation effect because of strong spoofing signals. Thus, the strong spoofing signals should be eliminated to track the authentic signals after the spoofing elimination in terms of successive cancellation. The threshold can be adaptively determined by the number of spoofing signals in a spoofer source and different signal powers of each spoofing signal.

The detection block is composed of several sequential blocks to detect spoofing signals using raw measurements, which include the absolute and relative signal powers, Doppler frequency, code range, and ephemeris data. The detection block is mainly applied to monitor the absolute power of each carrier, monitor the relative powers, bound and compare the range rates, check the Doppler shift, analyze the residual, and verify the received ephemeris data. In this paper, the detection block does not consider cross-checking techniques based on external observations such as the inertial system, direction-finding algorithm using array antennas, and radio-frequency (RF) broadcasting system, which includes authentic GPS information.

The spoofing mitigation block attempts to exclude the detected spoofing signal on a navigation filter based on the information of the spoofing detection block when a spoofing signal power is lower than the threshold, $P_{threshold}$, *i.e.*, $p_k^{SP} < P_{threshold}$. Thus, the GPS receiver can output the authentic navigation solution based on the authentic measures from the spoofing mitigation block. The navigation filter output can have integrity from the spoofing signals if the spoofing detection block operates well. However, the authentic navigation solution cannot be solved when fewer than four authentic measurements remain or the position dilution of precision (PDOP) is too high, *i.e.*, the GPS navigation solution is not reliable. Since we focus on the performance evaluation system to verify the anti-spoofing equipment, we should consider the injected number of spoofing signals and the PDOP value obtained by the remaining authentic GPS signals as conditions of limitation for the performance evaluation. Since the performance evaluation should cover all mitigation algorithms, we set the threshold as 300 m, which is known as 1-chip range between an original GPS signal and its spoofing one in the spoofing injection scenario. The spoofing mitigation block of the developed anti-spoofing equipment has a lower threshold value than the threshold for the performance evaluation considering the operation environment.

The spoofing elimination block attempts to successively eliminate the detected spoofing signal when a spoofing signal power is higher than and equal to the threshold, $P_{threshold}$, *i.e.*, $p_k^{SP} \geq P_{threshold}$. In order to eliminate the spoofing signal, the spoofing elimination block should track a spoofing signal and obtain raw measurements, which include the carrier phase, code range, Doppler shift, navigation data, and received power of the tracked spoofing signal. Based on the raw measurements, the spoofing elimination block generates a replica of the tracked spoofing signal and successively cancels the

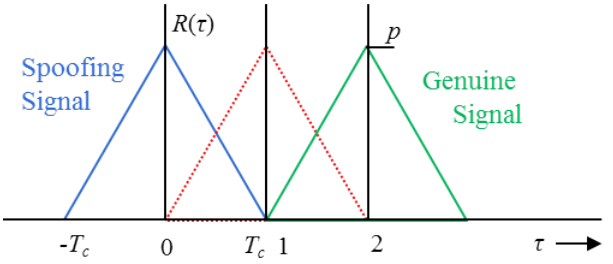


Fig. 2. Limiting condition of the performance evaluation for the spoofing elimination block.

(a) Anti-spoofing antenna (b) Anti-spoofing equipment

Fig. 3. Developed anti-spoofing equipment and antenna.

spoofing signal using the antiphase replica before providing measurements to the authentic navigation solution. The spoofing elimination block can offer the spoofing-free measurements to the authentic navigation solution. Since the success of spoofing signal elimination relies on the precision of the raw measurements of the tracked spoofing signal, the ADC bit resolution holds on the original 16-bit instead of the quantized 2-bit. The 16-bit ADC, 20 MHz frequency sampled input data are connected to the spoofing elimination block. For the spoofing elimination block, there is the basic assumption that an original GPS signal is perfectly recovered after the spoofing elimination when the code range of the spoofing signal is far from that of the original one. Fig. 2 shows the limit condition of the performance evaluation for the spoofing elimination block. In Fig. 2, $R(\tau)$ denotes the auto-correlation function according to time delay τ. T_c and p are the 1-chip duration and signal power, respectively. As shown in Fig. 2, the code range between the spoofing signal and the original one should be further than 600 m, which is known as the 2-chip range. When the code range difference between the original and spoofing signals is less than the 2-chip range, the eliminated antiphase replica signal affects a part of the original GPS signal and the original one cannot be tracked or perfectly recovered. Since we focus on the performance evaluation system to verify the anti-spoofing equipment, we should guarantee that the code range difference between the original GPS signal and its spoofing signal is 600 m by the design of the spoofing injection scenario.

We have developed an anti-spoofing equipment based on the structure design in Fig. 1. The outline of the anti-spoofing antenna and equipment is shown in Fig. 3. We developed the anti-spoofing equipment as a part of the anti-jamming, anti-spoofing, and jammer position finding system in Fig. 3b. The anti-spoofing equipment is composed of a signal processing device, a RF assembly, and a power supply device. We developed the anti-spoofing equipment antenna with the 8-inch size to support the aforementioned anti-spoofing equipment.

3. PERFORMANCE EVALUATION TEST SYSTEM

We consider a spoofing injection simulator that should include a timing synchronization function and a navigation data matching function to the received authentic signals. Based on the received authentic signals, the spoofing injection simulator should control the power and code phase of the generated spoofing signals. In order to automatically control the power and code phase, the spoofing injection simulator should acquire and track the GPS signals in real time. We select the SimSAFE software and hardware of SPIRENT Co. Ltd., which includes those functions as the spoofing injection simulator. The SimSAFE software was developed to generate the simulated spoofing signal and evaluate the performance of an anti-spoofing GPS receiver with a GPS simulator.

Since we evaluate the anti-spoofing equipment including its antenna, we should use a spoofing injection simulator as the spoofing signal emission equipment. Since the spoofing signal emission has a notably dangerous and critical issue when the signal is emitted to the air, the emission is regulated by the government. Thus, we must emit the simulated signal in a restricted environment such as an anechoic chamber and minimize the distance between the anti-spoofing equipment and the spoofing signal transmitting antenna considering the far-field condition. Therefore, the spoofing signal is not emitted in air. The evaluation structure of the anechoic chamber with the spoofing injection simulator to evaluate the performance of the anti-spoofing GPS equipment is shown in Fig. 4.

In this paper, we do not focus on how to successfully inject a spoofing signal to GPS receivers, but we focus on how to successfully evaluate the anti-spoofing GPS equipment in the condition of synchronized spoofing signal injection to GPS signals. Thus, the spoofing signal injection scenarios should be considered to mitigate and eliminate the spoofing signals. In order to evaluate the performance

https://doi.org/10.11003/JPNT.2018.7.3.127

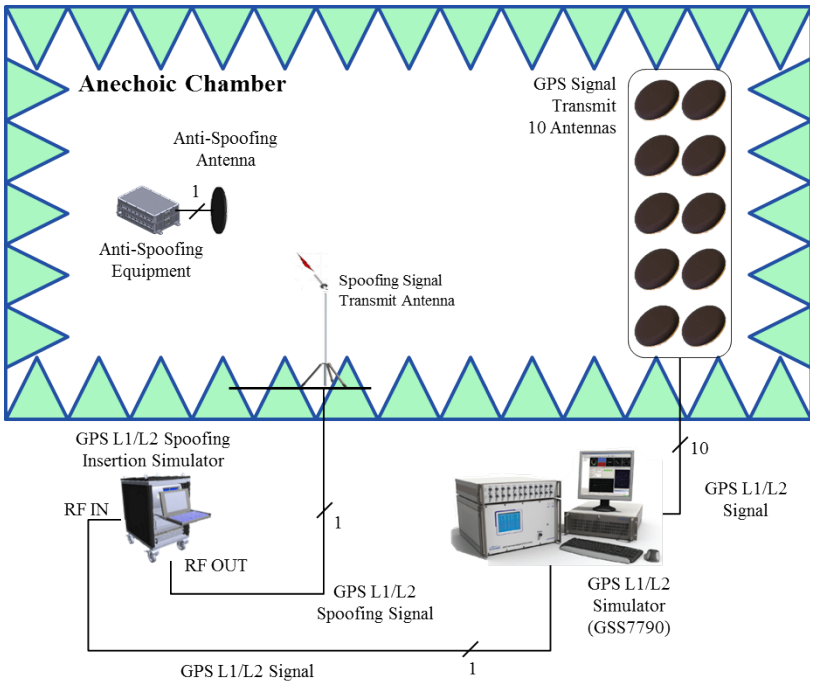


Fig. 4. Evaluation structure of the anechoic chamber using a spoofing injection simulator to evaluate the anti-spoofing equipment.

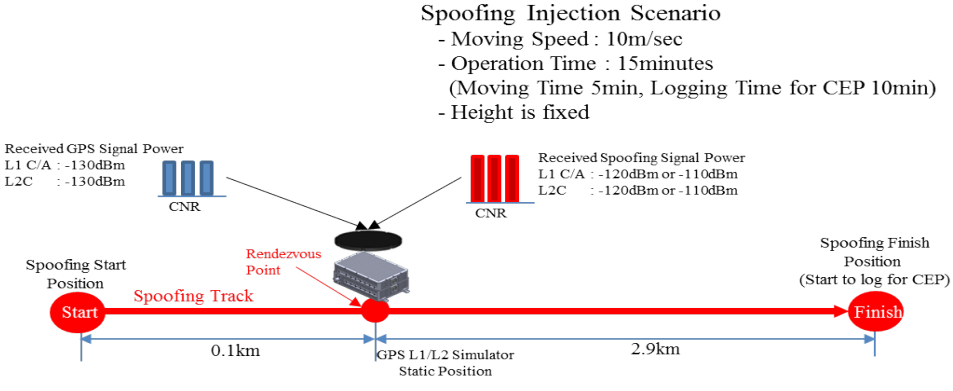


Fig. 5. Scenario of the spoofing injection simulator to evaluate the anti-spoofing equipment.

of the anti-spoofing equipment, we design the spoofing injection scenario as shown in Fig. 5. We assume that all spoofing signals are generated and transmitted from a single source. The scenario should consider both spoofing mitigation and elimination algorithms. In this injection scenario, there is a rendezvous point to cross the position generated by the authentic and spoofing signals and the distance increases from the rendezvous point. In order to evaluate the spoofing detection, mitigation, and elimination blocks, we set different criteria for the range error thresholds as we mentioned in Section 2. For the spoofing mitigation algorithm, we set the threshold as 300 m (1-chip range) between an authentic GPS signal and its spoofing one. For the elimination algorithm, we set the threshold as 600 m (2-chip range). The discrete code range between an authentic signal and its spoofing one can be changed according to the constellation of GPS satellites and spoofing insertion time. To satisfy both requirements, we set the distance of the positions generated by authentic and spoofing signals as 2900 m based on Jung et al. (2016) and the position where spoofing signals stop. At the stop position, the spoofing signals continue injecting for data logging to calculate the horizontal error as the CEP of the anti-spoofing equipment. We do not consider the vertical error, since the spoofing injection scenario is generated to move on the horizontal domain as shown in Fig. 5. As shown in Fig. 5, this spoofing

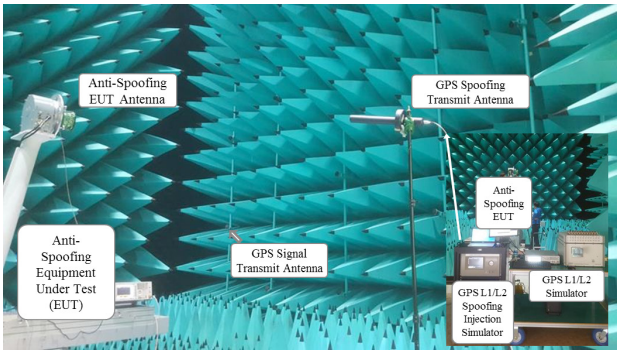


Fig. 6. Test environment for an anti-spoofing equipment in anechoic chamber.

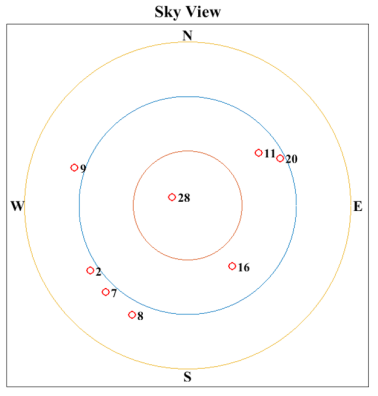


Fig. 7. Satellite constellation example in a spoofing injection scenario to evaluate the anti-spoofing equipment.

Table 1. Performance evaluation test parameters and values.

Parameters	Values
GPS signal type	L1 CA / L2C
Received GPS signal power	-130 dBm
Received spoofing signal power	-120 dBm / -110 dBm
Spoofing jam-to-signal power ratio (J/S)	10 dB / 20 dB
Incidence angle of spoofing signal	30°
Moving speed in spoofing scenario	10 m/sec
Moving distance in spoofing scenario	3000 m
Operation time in spoofing scenario	15 minutes

injection scenario has an advantage that the scenario can start to inject spoofing signals at any time, since the victim anti-spoofing equipment has a fixed position and the scenario has the fixed position as the rendezvous position.

4. EXPERIMENTAL RESULTS

We evaluate the performance of the anti-spoofing equipment in an anechoic chamber as shown in Fig. 6. In order to transmit GPS L1/L2 spoofing signals, we use the GPS L1/L2 spoofing injection simulator based on SimSAFE. The performance evaluation test parameters and values are shown in Table 1. In the spoofing injection simulator, we set the GPS signal types as L1 C/A and L2C. In order to evaluate the anti-spoofing equipment, which includes the spoofing signal mitigation and elimination algorithms, we change the spoofing jam-to-signal power rate (J/S) from 10 dB to 20 dB when the received GPS signal power, which we calibrate, is -130 dBm. Since the anti-spoofing equipment selects between mitigation and elimination algorithms against spoofing signals based on the received signal power, we set all spoofing signal powers as -120 dBm or -110 dBm. We set the GPS spoofing transmit antenna with the incidence angle of 30°. According to the spoofing injection scenario in Section 2, we set the moving speed, moving distance, and operation time as 10 m/sec, 3 km, and 15 minutes, respectively. In this scenario, we set the rendezvous point as 100 m from the start position.

Based on the test parameters and values, we construct the test environment in the anechoic chamber as shown in Fig. 6. We assume that the GPS L1/L2 signal transmitting antennas constructed in the anechoic chamber satisfy the far-field condition for the independence of radio frequency on the magnetic frequency. In the test environment, we should consider satisfying the far-field condition of the distance between the anti-spoofing antenna and the spoofing signal transmitting directional antenna. The GPS and spoofing injection simulators generate signals of GPS L1 and L2 frequencies as 1575.42 MHz and 1227.6 MHz, respectively. Thus, the wave lengths, λ_{L1} of GPS L1 and λ_{L2} of L2 are 0.190 m and 0.244 m, respectively. The sizes of a patch of the anti-spoofing antenna and spoofing signal transmitting antenna are 0.203 m and 0.496 m, respectively. For the GPS L1 and L2 frequencies, the distances that satisfy the far-field condition can be obtained by (Balanis 2015),

$$d_{Lf} = \frac{2D^2}{\lambda_{Lf}}, Lf = L1 \text{ or } L2 \tag{2}$$

where D denotes the size of the antenna, and λ_{Lf} denotes the wave-length of the transmitting signal for frequency Lf. D is determined by the largest antenna size between transmit and receive antennas, D = 0.496 m. Based on Eq. (2), we obtain d_{L1} = 2.589 m and d_{L2} = 2.016 m and we set the distance between the anti-spoofing antenna and the spoofing signal transmitting directional antenna as 3 m.

Fig. 7 shows an example of the GPS satellite constellation at the start time of a spoofing injection scenario to evaluate the performance of the anti-spoofing equipment. In the spoofing injection scenario, the spoofing injection simulator can generate at most 8 satellites and maintain the generated spoofing signals at the end of the scenario. The set of spoofing GPS satellites can be changed according to the scenario.

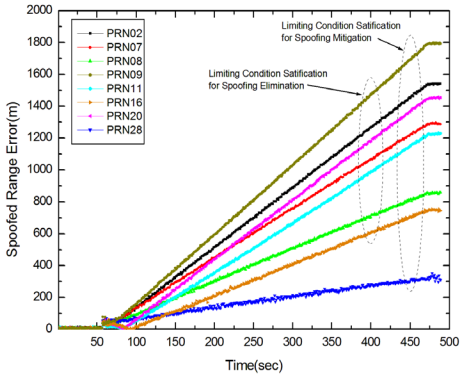


Fig. 8. Range errors increase after spoofing injection without use of spoofing mitigation and elimination blocks.

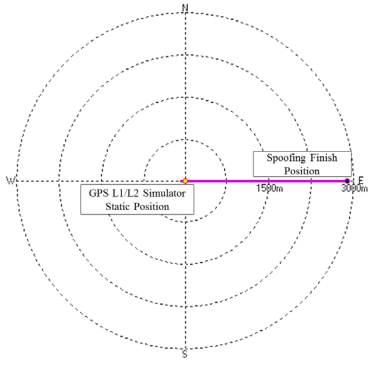


Fig. 9. Moving track of a commercial GPS receiver based on the spoofing injection scenario.

In the case of $p_k^{SP} < P_{threshold}$ and p_k^{SP} = -120 dBm, the spoofing injection simulator generates 4 satellites and k = 1, ..., 4 to evaluate the spoofing mitigation block. After the spoofing detection block, the raw measurements of the detected spoofing satellites are not used in the navigation solution based on the spoofing mitigation block. The raw measurements of the remaining satellites can solve the navigation solution after the exclusion of the detected spoofing satellites. In order to evaluate the spoofing mitigation block of the anti-spoofing equipment, the selection of spoofing satellites should consider that the remaining 4 satellites can solve the navigation solution and make the good PDOP condition.

However, in the case of $p_k^{SP} \geq P_{threshold}$ and p_k^{SP} = -110 dBm, the spoofing injection simulator generates all 8 satellites and k = 1, ..., 8 to evaluate the spoofing elimination block. The spoofing elimination block attempts to eliminate the spoofing signal of the detected spoofing satellite after the detection block. After spoofing signals have been eliminated, the authentic signals can perfectly revive and be re-tracked after the 2-chip correlation between spoofing and authentic signals. In order to evaluate the spoofing elimination block of the anti-spoofing equipment, there should be re-tracked satellites whose code range difference between spoofing and authentic signals exceeds 600 m, and there should be 4 re-tracked satellites to solve the navigation solution in the spoofing injection scenario.

After the spoofing injection according to the scenario, the range error of each signal must increase against the authentic signal because of the spoofing signal if there are not anti-spoofing detection, mitigation, and elimination blocks. Fig. 8 shows that the range errors increase in the time domain after the spoofing signal injection at 57 sec from the beginning of the log. While spoofing signals are injected, the spoofed position passes the rendezvous point and moves toward the spoofing finish position. At the end of the moving distance in the injection scenario, the spoofing detection and mitigation blocks must detect and not use the spoofing signals whose range error is larger than 300 m. When the spoofing detection and elimination blocks perfectly eliminate the spoofing signal whose range error is larger than 600 m, the original GPS signals must revive and can be re-tracked.

In order to verify the spoofing injection simulator and spoofing injection scenario in the anechoic chamber, the generated spoofing signals are injected into a commercial GPS receiver, which does not have anti-spoofing functions. Fig. 9 shows the position of the commercial GPS receiver after running the spoofing injection scenario, where we set spoofing power of p_k^{SP} = -110 dBm, and k = 1, ..., 8. When spoofing signals are injected into the commercial GPS receiver, all tracked GPS signals are started to switch the spoofing signals. After all spoofed signals are tracked in the commercial GPS receiver, its position tracks the spoofing injection scenario. As shown in Fig. 9, the pink line marks the GPS receiver position that moves 2900 m until the end of the scenario.

For the identical spoofing signal injection condition of Fig. 9, we set the spoofing power of p_k^{SP} = –120 dBm, k = 1, ..., 4 for 8 satellites and evaluate the spoofing detection and mitigation blocks in the anti-spoofing equipment. For the test, we select four spoofing PRNs as 6, 18, 21, and 22 and the spoofing signals of the selected PRNs are injected at 57 seconds from the beginning of the log. In Fig. 10, we obtain the position error, CNR, and range error results in the track of a period of the spoofing signal injection scenario. Fig. 10a shows the north and east position errors, which are stabilized after running on the spoofing mitigation block. Fig. 10b shows a CNR plot in the time domain. After spoofing signals are injected, the spoofed position stops at the spoofing start position during 18 seconds, and passes the rendezvous point after 28 seconds from the injection.

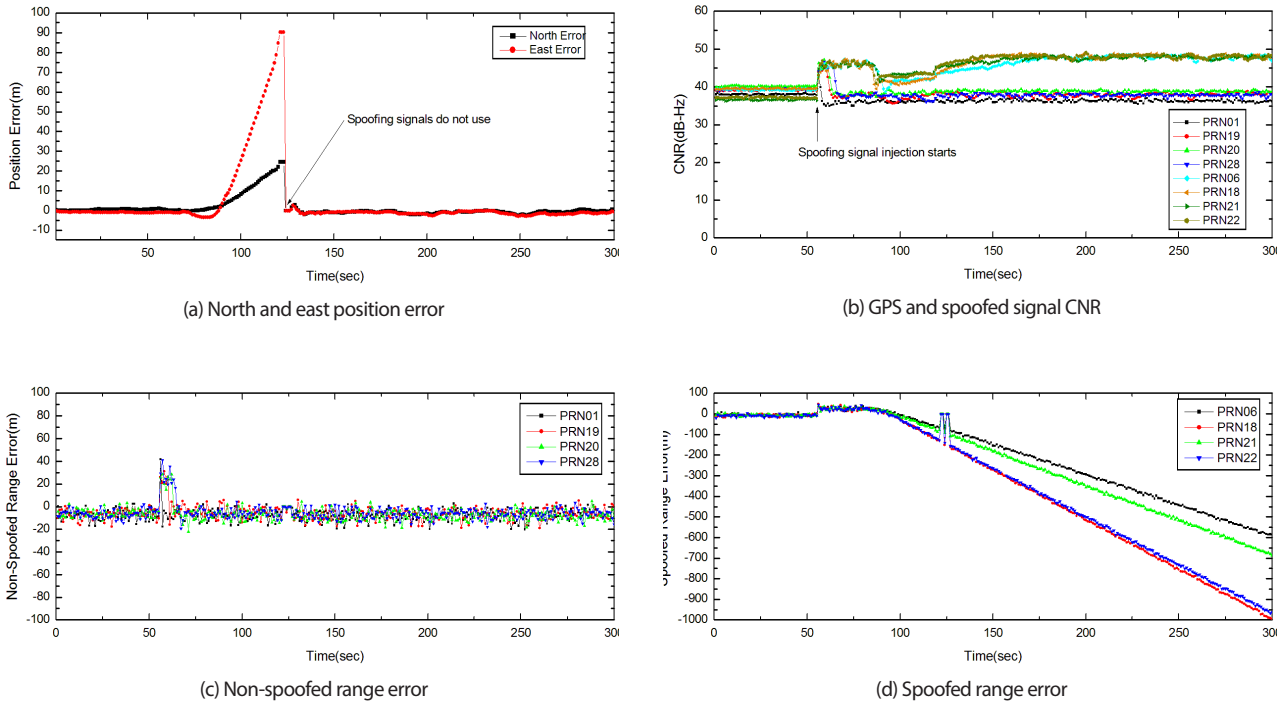
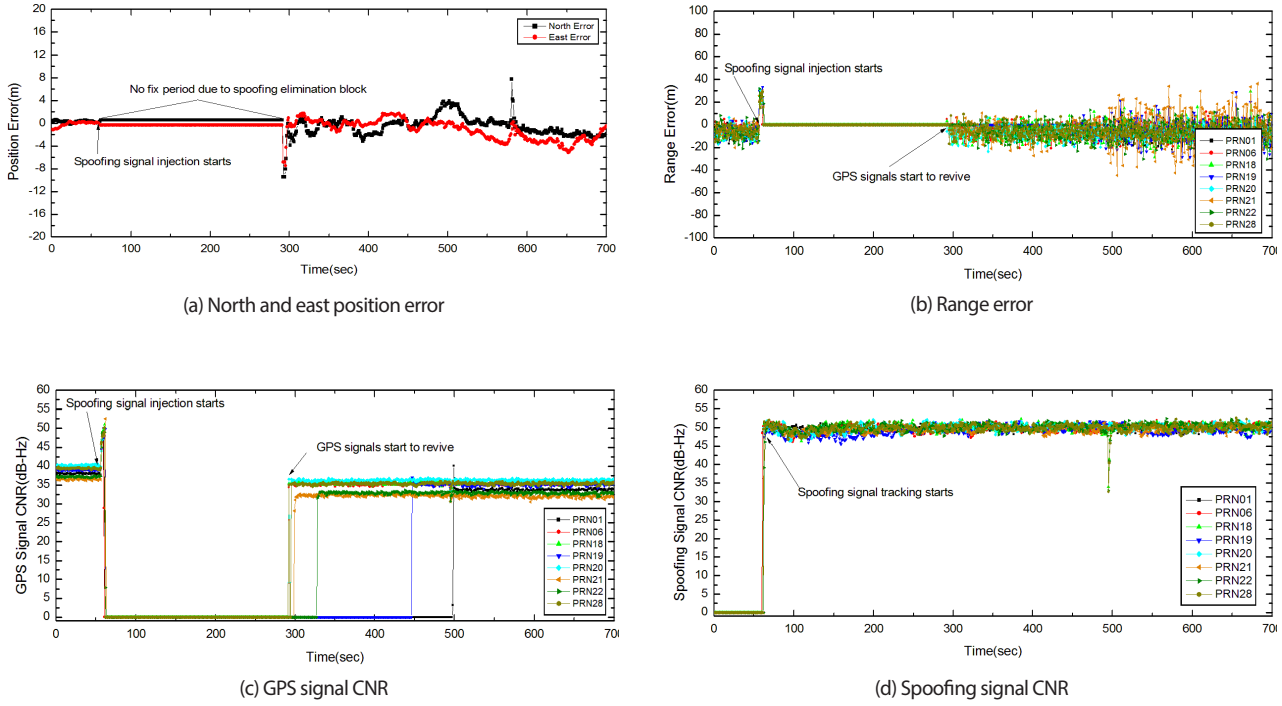


Fig. 10. Position error, CNR, and range error after spoofing injection to evaluate the spoofing detection and mitigation block.

Thus, the position errors of Fig. 10a dynamically increase after 28 seconds from the spoofed CNRs are increasing. After the signal injection, the CNRs of generated spoofing signals immediately increase since the original GPS signals and spoofing signals are well synchronized. As the position difference between the positions generated by original GPS and spoofing signals increases, the range difference also increases. At that time, the correlation peak ambiguities of the original GPS and spoofing signals increase and the CNRs of spoofing signals decrease in the tracking module of the anti-spoofing equipment. The decreased CNRs of spoofing signals are recovered after the original GPS and spoofing signals are totally discrete. In Fig. 10b, the CNRs of spoofing signals are comparatively lower than the injected spoofing power at 10dB. Since the received powers of the original GPS and spoofing signals exceed the threshold of the automatic gain control module in front of tracking module after the spoofing signal injection, the output powers of the original GPS and spoofing signals are automatically quantized and the CNRs of spoofing signals decrease. Figs. 10c,d show the non-spoofed and spoofed range errors, which are the differences between the estimated range and the true value of a simulation logging file. According to the increment of spoofed range errors because of the spoofing signal injection scenario, the position errors also increase until 123 seconds from the beginning of the log. At that time, the spoofing signals are detected and not included in the authentic navigation block by the spoofing mitigation block. After the spoofing signals are blocked, the navigation solution is obtained by the non-spoofed PRNs of 1, 19, 20, and 28, which are selected based on the PDOP. In this test, the PDOP is 3.1 when the spoofing signals are blocked.

For the identical spoofing signal injection condition of Fig. 9, we set the spoofing power of p_k^{SP} = -110 dBm, k = 1, ..., 8, and evaluate the spoofing detection and elimination blocks in the anti-spoofing equipment. For the test, we select all eight PRNs to inject spoofing signals at 57 seconds from the beginning of the log. In Fig. 11, we obtain the position error, range error, and CNR results in the track of a period of the spoofing signal injection scenario. Fig. 11a shows the north and east position errors and there is no fix period because of the spoofing elimination of all PRNs. Fig. 11b shows the range errors which are differences between the estimated range and the true value of a simulation logging file. Since Fig. 11b shows the range errors of the original GPS signals, the range errors cannot be shown before the injected spoofing signals are eliminated. As shown in Fig. 11b, the range error appears similar to the position error of Fig. 11a. Figs. 11c,d show the CNR of GPS signals and spoofing signals. After the spoofing signal injection begins, the spoofing elimination blocks cut off all PRNs with higher CNRs than the threshold value as shown in Fig. 11c. Since all PRNs are cut off, there is no fix period in Figs. 11a,b. The spoofing elimination block keeps track of and eliminates the



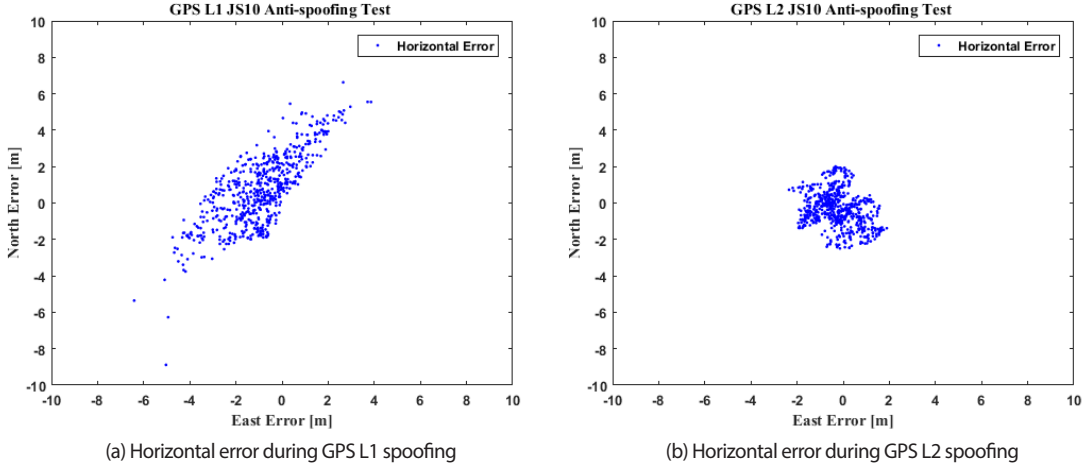
(a) North and east position error

(b) Range error

(c) GPS signal CNR

(d) Spoofing signal CNR

Fig. 11. Position, range error, and CNR after spoofing injection to evaluate the spoofing detection and elimination block.



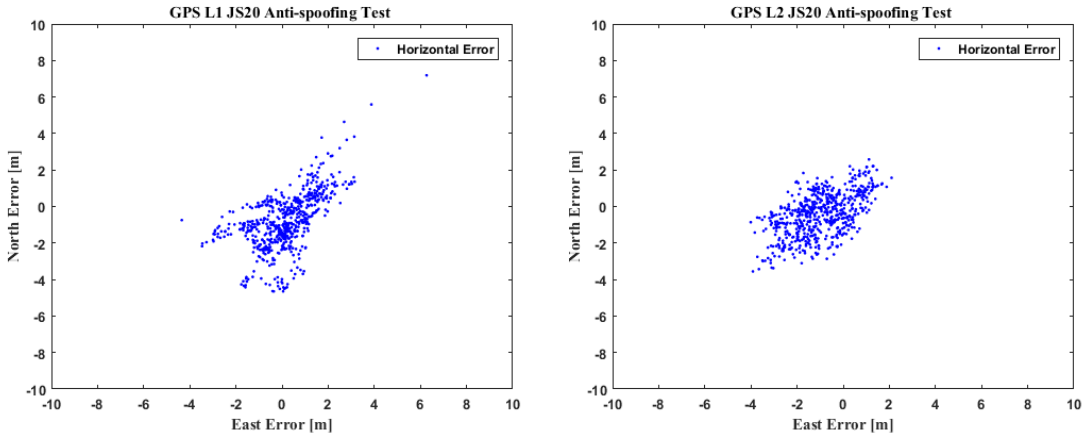
(a) Horizontal error during GPS L1 spoofing

(b) Horizontal error during GPS L2 spoofing

Fig. 12. Horizontal error plots of the anti-spoofing equipment for the GPS L1/L2 spoofing signal injection of J/S 10 dB.

detected spoofing signals. Since the code range difference between the original GPS signal and its spoofing signal increases as time passes, the original GPS signals are re-tracked and the navigation solution is obtained at 292 seconds from the beginning of the log. However, the signal re-track time differs among all PRNs as shown in Fig. 11c. Because it depends on the code range difference between the original GPS signal and its spoofing signal, and the difference depends on the spoofing injection scenario. The anti-spoofing equipment must be not perfect to eliminate the spoofing signal in real-time because of the time and hardware limitations. Therefore, since the spoofing signals continue being injected during the test, the north and east position errors and range errors after the signal injection are higher than those before signal injection.

Based on the spoofing injection scenario, the position generated by the spoofing signals is stopped at 2900 m from the rendezvous point. At the stop position, we begin the



(a) Horizontal error during GPS L1 spoofing (b) Horizontal error during GPS L2 spoofing

Fig. 13. Horizontal error plots of the anti-spoofing equipment for GPS L1/L2 spoofing signal injection of J/S 20 dB.

data logging for 10 minutes to calculate the horizontal error of the CEP, while GPS L1 or L2 spoofing signals are injected. In order to evaluate the anti-spoofing equipment, we define the CEP as the radius of a circle that contains 50 % of the error distributions when centered at the correct location. For a two-dimensional Gaussian random variable, the CEP is defined as (Williams 1997),

$$CEP = 0.563 \times \sigma_L + 0.614 \times \sigma_S \tag{3}$$

where σ_S and σ_L represent the standard deviations of the short (north) and long (east) errors, respectively. Figs. 12 and 13 show the horizontal error plots of the anti-spoofing equipment tested by the proposed performance evaluation system in the anechoic chamber. When GPS L1 or L2 spoofing signals are injected, the horizontal error distributions of positions of Figs. 12 and 13 are obtained by the GPS L1 and L2 solutions, respectively. The plots are shown in the logged data at the stop position in the spoofing injection scenario. The CEP results of the same logged data are shown in Table 2. In Table 2, we verify that the anti-spoofing equipment can detect, mitigate, and eliminate spoofing signals and track the original GPS signals at the stop position.

Table 2. CEP results of the anti-spoofing equipment.

Spoofing power level (dB)	Spoofing injection frequency band (m)	
	GPS L1	GPS L2
J/S 10	2.42	1.14
J/S 20	1.76	1.67

5. CONCLUSIONS AND DISCUSSIONS

In this paper, we have introduced the developed anti-spoofing equipment and proposed the performance evaluation system of the equipment with spoofing injection scenarios. The anti-spoofing equipment has been developed to simultaneously detect, mitigate, and eliminate spoofing signals. Therefore, we also construct the performance evaluation system and generate the scenarios to verify those anti-spoofing functions. In the anechoic chamber test, we have verified both anti-spoofing equipment and evaluation system in comparison with the commercial GPS receiver. Based on the received spoofing signal power, we have analyzed the anti-spoofing test results obtained by the spoofing mitigation and elimination blocks. We have guided the anti-spoofing evaluation criteria based on the horizontal position errors as CEP after the spoofing signal detection, mitigation, and elimination.

In fact, all anti-spoofing techniques are not perfect and are counter-measured solutions with constraints of the number of spoofing signals or threshold of the range and range rate. As we mentioned, since all types of stand-alone anti-spoofing equipment have constraints, we recommend the simultaneous use of an anti-jamming solution as a controlled radiation pattern array system (Kaplan & Hegarty 2006). When the anti-jamming solution is used in front of the anti-spoofing equipment, most of the injected spoofing signals are eliminated or decreased. Then, the remained spoofing signals are easily mitigated and eliminated by the anti-spoofing solution. For the combination of anti-jamming and anti-spoofing equipment, the performance evaluation system should be considered and developed from another view point.

https://doi.org/10.11003/JPNT.2018.7.3.127

ACKNOWLEDGMENTS

This research was supported by Active response technology on GPS complex anti-jamming environment funded by the Defense Acquisition Program Administration (912430201).

REFERENCES

Balanis, C. A. 2016, Antenna Theory: Analysis and Design, 4th ed. (Hoboken, NJ: John Wiley & Sons, Inc.).

Broumandan, A., Jafarnia-Jahromi, A., & Lachapelle, G. 2012, Spoofing detection, classification and cancellation (SDCC) receiver architecture for a moving GNSS receiver, GPS Solutions, 19, 475-487. https://link.springer.com/article/10.1007/s10291-014-0407-3

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, in Proc. of ION GNSS 2008, Sep. 16-19, 2008, pp.2314-2325.

Jafarnia-Jahromi, A. Broumandan, A., Nielsen, J., & Lachapelle, G. 2014, Pre-despreading authenticity verification for GPS L1 C/A signals, Navigation, 61, 1-11. https://doi.org/10.1002/navi.50

Jeong, S. K., Kim, T. H., Sin, C. S., & Lee, S. U. 2012, Technical trends of smart jamming for GPS signal, Electronics and Telecommunications Trends, 27, 75-82. https://doi.org/10.22648/ETRI.2012.J.270609

Jung, J., Jo, S.-W., Yang, G., Park, S., Lee, C.-H., et al. 2014, Testing and Simulation of Inertial Navigation System (INS) Simulation Software for Verification of INS-aided GNSS Systems, in Proc. ISGNSS 2014, Oct. 21-24, 2014, pp.885-895.

Jung, J., Lee, C.-H., Yang, G.-J., Kang, H., Jeong, T., et al. 2016, Test evaluation of GPS L1/L2 spoofing signal insertion for anti-spoofing algorithm verification, in Proc. KGS 2016, Nov. 11-13, 2016, pp.9-12.

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

Kim, T., Lee, S., & Kim, J. 2013, The anti-spoofing methods using code antiphase of spoofing signal, Journal of KICS, 38C, 1044-1050. https://doi.org/10.7840/kics.2013.38C.11.1044

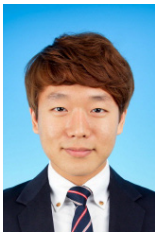
Madhani, P. H., Axelrad, P., Krumvieda, K., & Thomas, J. 2003, Application of successive interference cancellation to the GPS pseudolite near-far problem, IEEE Transaction on Aerospace and Electronic Systems, 39, 481-488. https://doi.org/10.1109/TAES.2003.1207260

Nielsen, J., Dehghanian, V., & Lachapelle, G. 2012, Effectiveness of GNSS spoofing countermeasure based on receiver CNR measurements, Intl. Journal of Navigation and Observations, Article ID 501679, 1-9. http://dx.doi.org/10.1155/2012/501679

Wen, H., Huang, P.Y., Dyer, J., Archinal, A., & Fagan, J. 2005, Countermeasures for GPS signal spoofing, in Proc. ION GNSS 2005, Sep. 13-16, 2005, Long Beach, CA, pp.1285-1290.

Williams, C. E. 1997, A comparison of circular error probable estimators for small samples, U.S. Air Force Institute of Technology Technical Report, AFIT/GOA/ENS/97M-14. http://handle.dtic.mil/100.2/ADA324337

Junwoo Jung received the Ph.D degree in information and communication engineering from Ajou University, Korea in 2012. Since January 2012, he has been employed in the LIG NEX1 and engaged in the development of anti-jamming GNSS systems and tactical communications. He received a President award of NIPA from ITRC Forum 2012. His interests are in the MAC protocol design, multiple access, and resource management for WiMax, WLAN, and WPAN systems. He currently works on anti-spoofing and anti-jamming GNSS systems and military SBAS systems.



Sungyeol Park received the B.S. degree in electrical engineering from Hanyang University, Korea, in 2012. Since 2012, he has been employed in the R&D Lab of the LIG NEX1 and engaged in the research and development of anti-jamming GNSS systems.

Jongchul Hyun received the B.S. degree in electrical engineering from Hongik University, Korea, in 2004. He received the M.S. degrees in electrical engineering from Hongik University, Korea, in 2006. Since 2006, he has been employed in the R&D Lab of the LIG NEX1 and engaged in the research and development of anti-jamming GNSS systems.

Haengik Kang received the B.S. degree in electrical engineering from Yonsei University, Korea, in 1996. He received the M.S. degrees in electrical engineering from Yonsei University, Korea, in 1998. In 1998, he started as a researcher at LG Innotek and engaged in the development of military satellite

terminal. In April 2004, he joined Pantech and engaged in the development of the CDMA cellular phone. Since 2008, he has been employed in the R&D Lab of the LIG NEX1 and engaged in the research and development of anti-jamming GNSS systems and tactical communications.

Kiwon Song received the Doctor's degree in Electronicsfrom Chung-nam National University in 2002. His research interests include design of satellite navigation system architecture, GNSS signal generation processing, and integration optimal filter of INS/GPS.

Kapjin Kim received the B.S degree in control and instrumentation engineering from Hanyang University, Korea, in 1997. He has employed in the 3rd R&D Institute-4th Directorate of Agency for defense development (ADD) and engaged in research and development of GNSS and NAVWAR technology.

Youngbum Park received the Ph.D. degree in Aerospace engineering from Seoul National University in 2017. Since 2001, he has been working for Agency for defense development (ADD). His research interests include estimation, localization, and integrated navigation system.

https://doi.org/10.11003/JPNT.2018.7.3.127