International Journal of Control, Automation and Systems 19(X) (2021) 1-15
http://dx.doi.org/10.1007/s12555-019-0745-6
ISSN:1598-6446 eISSN:2005-4092
http://www.springer.com/12555

Spoofing Signal Generation Based on Manipulation of Code Delay and Doppler Frequency of Authentic GPS Signal

Seong-Hun Seo, Gyu-In Jee*, and Byung-Hyun Lee

Abstract: We propose an efficient spoofing signal generation method that uses the processing results of a global positioning system (GPS) receiver for authentic GPS signals. Conventional methods of generating spoofing signals use expensive GPS simulators because the structures of the spoofing signals must be almost identical to those of the GPS signals. Simulators require GPS ephemeris at a specific time and target position. Subsequently, a complicated process is used to generate navigation data using the ephemeris and model error sources such as the satellite clock bias and ionospheric delay. In contrast, the proposed method can generate spoofing signals for the desired target position without requiring GPS simulators; it does so by adjusting the signal processing results of the receiver. Using the navigation results of the receiver, such as position and velocity, the pseudorange delay and spoofing Doppler frequency between the estimated position of the receiver and the target spoofing position are obtained; these are then applied to shift the signal-tracking results of the receiver to create a new signal for the target spoofing position. Our experimental results indicate that the proposed algorithm can effectively generate spoofing signals with characteristics highly similar to those of authentic GPS signals. In addition, we confirmed that the spoofing signals generated by the proposed method are difficult to be detected using conventional spoofing detection techniques.

Keywords: Authentic GPS signal, pseudorange delay, signal processing results, spoofing doppler frequency, spoofing signal generation.

1. INTRODUCTION

The global positioning system (GPS) is an important system used to estimate the absolute position, velocity, and timing information of users worldwide. GPS satellites simultaneously transmit civilian and military signals to the Earth. Military signals are encrypted using restricted codes and are therefore not accessible to the public. In contrast, civilian GPS signals use publicly available pseudo-random noise (PRN) codes that are widely used in multiple fields, such as logistics, transportation, and finance. However, GPS signals are transmitted from GPS satellites that are approximately 20,000 km away from the surface of the Earth. Thus, the intensity of the GPS signals reaching the surface is approximately −130 dBm, rendering these signals highly vulnerable to interference. Among various sources of interference, spoofing signals pose the biggest problem because they can induce a GPS receiver to perform incorrect navigation solutions inadvertently.

Because of the increasing number and variety of GPS applications, the seriousness of the spoofing problem becomes more apparent. Therefore, many studies have been devoted to solving this problem. To study anti-spoofing techniques, it is necessary to generate spoofing signals that can effectively deceive the target receivers. Spoofing signals, whose characteristics differ from those of GPS signals received by the target receiver, can be easily detected. Warner and Johnston [1] proposed low-cost spoofing countermeasures for detecting spoofing attacks using a conventional GPS receiver. Their method involved checking various characteristics of the received signals, such as the number of visible satellites and signal strength. Wen *et al*. [2] improved this method by proposing additional countermeasures, including using characteristics such as the Doppler frequency and performing cross-correlation checks.

Further, many studies generated spoofing signals using high-performance GPS simulators, such as the one illustrated in Fig. 1. Some studies used the simulator for generating spoofing signals to verify various spoofing signal detection methods [3–6] or study anti-spoofing techniques through signal-quality-monitoring functions [7, 8]. Further, Tanıl *et al*. [9] used a simulator to develop a spoofing countermeasure that used an inertial navigation system

Manuscript received September 5, 2019; revised February 17, 2020, April 7, 2020, and May 21, 2020; accepted June 9, 2020. Recommended by Associate Editor Choon Ki Ahn under the direction of Editor Young IL Lee. This work was supported by the Hanwha Systems.

Seong-Hun Seo is with the Postal & Logistics Technology Research Center, Electronics and Telecommunications Research Institution (ETRI), 218 Gajeong-ro, Yuseong-gu, Daejeon 34129, Korea (e-mail: ssh@etri.re.kr). Gyu-In Jee is with the Electronics Engineering, Konkuk University, 120 Neungdong-ro, Gwangjin-gu, Seoul 05029, Korea (e-mail: gijee@konkuk.ac.kr). Byung-Hyun Lee is with the Research & Development Division, Hyundai Motor Group, 417, Yeongdong-daero, Gangnam-gu, Seoul 06182, Korea (e-mail: byunghyun.lee@hyundai.com).
* Corresponding author.

(a) (b)

Fig. 1. GPS signal simulators: (a) Spirent GSS 9000 simulator and (b) Spectracom GPS/GNSS simulator.

(INS). GPS simulators were used to generate spoofing signals because the generated signals feature the same structure as those of the authentic GPS signals. Therefore, the spoofing signals can serve as fake GPS signals that are maliciously generated to deceive the target receiver. The various signal-parameter-setting functions of GPS simulators can be used to generate spoofing signals for the desired target spoofing positions.

However, because GPS simulators are expensive, using them in an experimental environment is not always straightforward. These simulators also generate signals without access to authentic live GPS signals. Thus, they need GPS ephemeris information at specific times to generate spoofing signals. Further, they perform the complex processes of generating navigation data using GPS ephemeris information and by modeling the signal parameters with respect to factors such as the satellite clock error, ionospheric delay, and tropospheric delay. Through these processes, the user can generate intended spoofing signals precisely. However, the characteristics of the generated spoofing signals cannot always be guaranteed to match those of the authentic live GPS signals. Fig. 2 presents the estimated Doppler frequencies of both authentic live GPS signals from GPS satellites and of signals generated using the Satgen v3 software [10]; the time and position were the same in both cases. Both signals were recorded using a Labsat 3 GPS simulator device [11] and processed using a U-blox M8T receiver. Figs. 2(a)-(d) present the Doppler frequencies for PRN 1, PRN 8, PRN 11, and PRN 17, respectively. The results indicate that the Doppler frequencies are different even though the time and position were the same in both cases (i.e., authentic and generated GPS signals). Fig. 3 explains the pseudorange differences between the authentic and generated GPS signals. GPS receivers calculate their positions using the relative differences in pseudorange for each PRN. Thus, if the characteristics of the authentic and generated

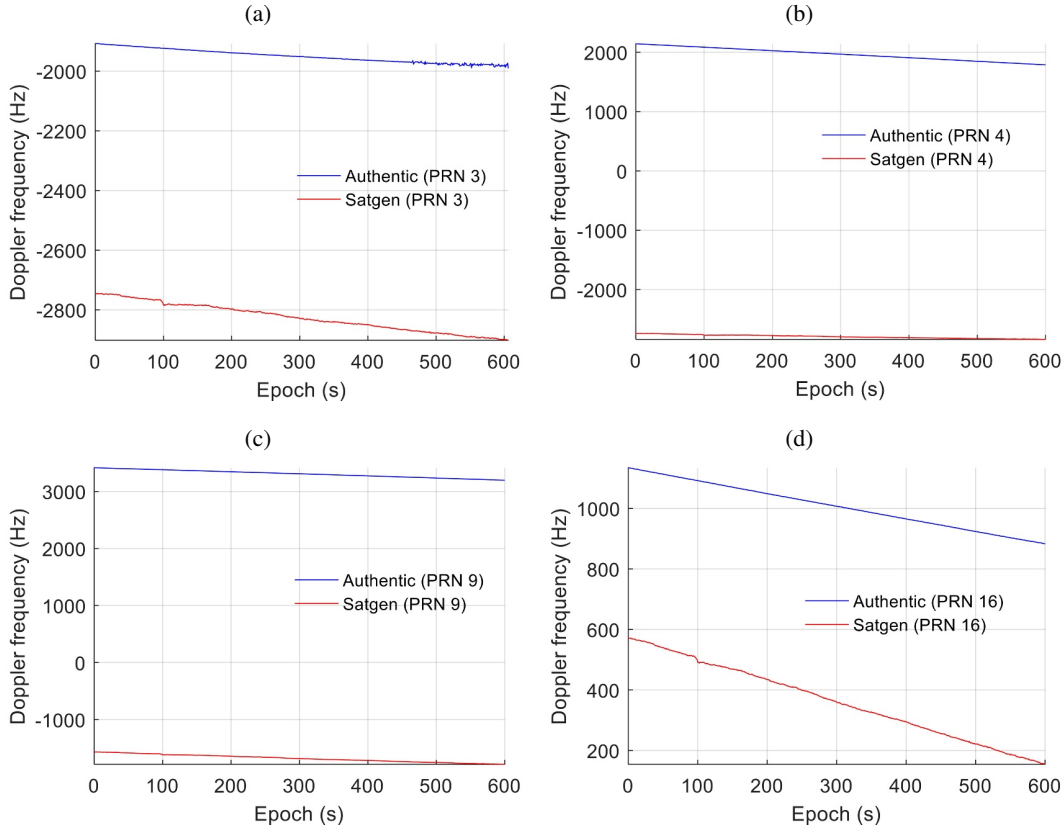


Fig. 2. Doppler frequencies obtained from authentic signals from GPS satellites and signals generated using a GPS signal simulator (Satgen v3 signal generator) for (a) PRN 3, (b) PRN 4, (c) PRN 9, and (d) PRN 16.

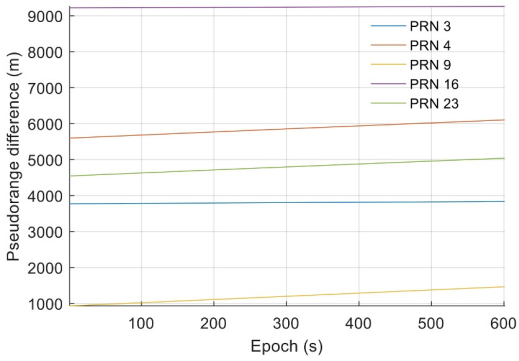


Fig. 3. Pseudorange differences between authentic and simulator-generated GPS signals. The pseudorange differences of all PRNs should be the same if the authentic and simulated GPS signals have identical characteristics.

signals are similar, the difference between the two signals for each PRN must have almost the same value. However, the results presented in Fig. 2 and Fig. 3 indicate that the generated signals fail to accurately reflect the characteristics of the authentic GPS signals. Therefore, there is a high probability that the generated spoofing signals can be easily detected using the aforementioned anti-spoofing methods.

In addition to using such expensive simulators, software-based spoofing signals can be generated by a GPS software signal generator [12]. However, only the signal generation platform changes, while the generated spoofing signals remain vulnerable to anti-spoofing methods. Therefore, prior studies have proposed techniques for generating spoofing signals using signal parameters obtained from a GPS receiver [13, 14]. In these studies, the spoofer has a receiver module and a spoofer module. The receiver module receives a live GPS signal, tracks it, and then provides the signal tracking results to the spoofer module, which uses these results to generate a spoofing signal according to the intended target spoofing position and velocity. Experimental results indicated that the spoofing signal generated using the receiver and spoofer modules could effectively deceive the receiver and take the tracking loop lock from the live GPS signal. However, although these spoofing signal generation techniques were based on a software-defined radio algorithm, a special hardware platform was also required. Further, from the experimental results, it was difficult to analyze how the characteristics of the generated spoofing signals were similar to those of the GPS signals. In other researches, complete software-based spoofing signal generation methods were proposed but these were disadvantageous in that spoofing parameters needed to be manually set for generating spoofing signals [15, 16].

To solve these problems, we propose a simple spoofing signal generation algorithm that uses the information processed by a GPS receiver for authentic live GPS signals. The adopted approach differs from the techniques employed in [13, 14]. The GPS receiver tracks authentic signals and performs navigation. Then, it delivers the tracking and navigation results to the spoofing signal generator. The navigation results are used to calculate the spoofing signal parameters, such as the pseudorange delay and spoofing Doppler frequency, based on a vector-tracking technique. Then, the spoofing signal generator exploits the tracking results to regenerate the authentic signals and applies the spoofing parameters to them, enabling the generation of the final spoofing signals.

The contributions of the present study are summarized below:

- Spoofing signals are generated without high-cost GPS simulators.
- The signal processing procedure is straightforward and does not require navigation message generation using external GPS ephemeris information and modeling of error components, such as satellite clock error, ionospheric delay, and tropospheric delay.
- There is a high level of similarity between the characteristics of authentic GPS and spoofing signals because the latter are generated based on the former.
- Good accessibility and scalability allow the use of open-source software receivers to process the authentic GPS signals, as presented in the experimental results.

Due to these advantages, the proposed method can be flexibly used to study the countermeasures against spoofing attacks when the spoofing signals are similar to the authentic GPS signals on the basis of post-processing.

The rest of this article is organized as follows: Section 2 describes the spoofing environment and the approaches typically utilized. Section 3 introduces the conventional spoofing signal generator. Section 4 presents the proposed spoofing signal algorithm that uses the processing results of a receiver for authentic GPS signals. Section 5 presents the experimental results that demonstrate the performance of the proposed algorithm. Further, the characteristics of the generated signals are analyzed by comparing them with authentic GPS signals. Finally, we conclude the article by summarizing the proposed spoofing signal generation algorithm.

2. SPOOFING ENVIRONMENT

The spoofing environment is divided into two main types based on the method used to generate the spoofing signals. In the first type, commonly referred to as meaconing, a spoofer receives the authentic GPS signals and then strongly propagates them to the antenna of the target receiver after a certain time delay meant to deceive the

receiver. Because meaconing uses authentic GPS signals, it is easy to generate spoofing signals that have characteristics similar to those of the authentic signals received by the target GPS. However, in this case, the same delay is applied to the signals received from each satellite to generate the spoofing signals. This means that the relative pseudoranges between the target receiver and each satellite increase equally so that the spoofing signals can induce the target receiver to calculate the position of the spoofer at a time different from the current time. In other words, there is a limitation to arbitrarily setting the target spoofing position.

The second type of spoofing involves the use of GPS signal generators. GPS simulators are conventionally used as spoofing signal generators because the generated signals are strong counterfeit signals that feature the same structure as those of authentic GPS signals. In this case, it is possible to generate the spoofing signals for the desired target spoofing position at any time. However, as mentioned in Section 1, this method requires expensive equipment and a complicated signal-generation process. In addition, the spoofing signals obtained from the generators have characteristics that differ from those of the authentic GPS signals received by the target receiver.

To effectively deceive the target receiver, spoofing signals with characteristics similar to those of authentic GPS signals received by the target receiver must be generated for a desired target spoofing position at the time when the authentic signals are received.

Therefore, we propose a simple and low-cost spoofing signal generation method that combines the advantages of both spoofing approaches. The proposed method processes authentic GPS signals and applies a satellite-specific delay to generate the spoofing signal for the desired position.

3. CONVENTIONAL SPOOFING SIGNAL GENERATION

In this section, we describe the operating principles of conventional spoofing signal generators and describe the complex steps that must be followed to generate the spoofing signals. Fig. 4 illustrates a conventional generator [17] for GPS L1 C/A (coarse/acquisition) signals. For effective spoofing, the spoofing signals must be tailored to have satellite information that is identical to that of authentic GPS signals. Therefore, once the target spoofing position is determined, the signal generator requires the GPS ephemeris at the same time when the authentic GPS signal is received by the target receiver. The signal generator selects visible satellites from the ephemeris and generates a signal for them.

First, the positions and velocities of the satellites are obtained from the ephemeris [18]. Second, the ranges and range rates between the satellites and spoofing position are calculated. Additionally, error modeling is conducted for satellite clock error, ionospheric delay, and tropospheric delay. The pseudoranges are calculated using the error models and ranges. The pseudoranges $\rho_s^i(t)$ and range-rates $\dot{\rho}_s^i(t)$ are represented as

$$\begin{aligned}\rho_s^i(t) &= \|X^i(t)-X_s(t)\|+\Delta T^i(t)\cdot c+I^i(t)+T^i(t)+\varepsilon^i \\ &= \sqrt{(x^i(t)-x_s(t))^2+(y^i(t)-y_s(t))^2+(z^i(t)-z_s(t))^2} \\ &\quad +\Delta T^i(t)\cdot c+I^i(t)+T^i(t)+\varepsilon^i, \qquad (1)\\ \dot{\rho}_s^i(t) &= v_s^i(t)\cdot a_s^i(t) \\ &= c\left(1-\frac{f_{s,carr}^i(t)}{f_{t,carr}}\right), \qquad (2)\end{aligned}$$

where $X^i(t)=[x^i(t),\, y^i(t),\, z^i(t)]$ is the position of the i-th satellite, $X_s(t)=[x_s(t),\, y_s(t),\, z_s(t)]$ is the target spoof-

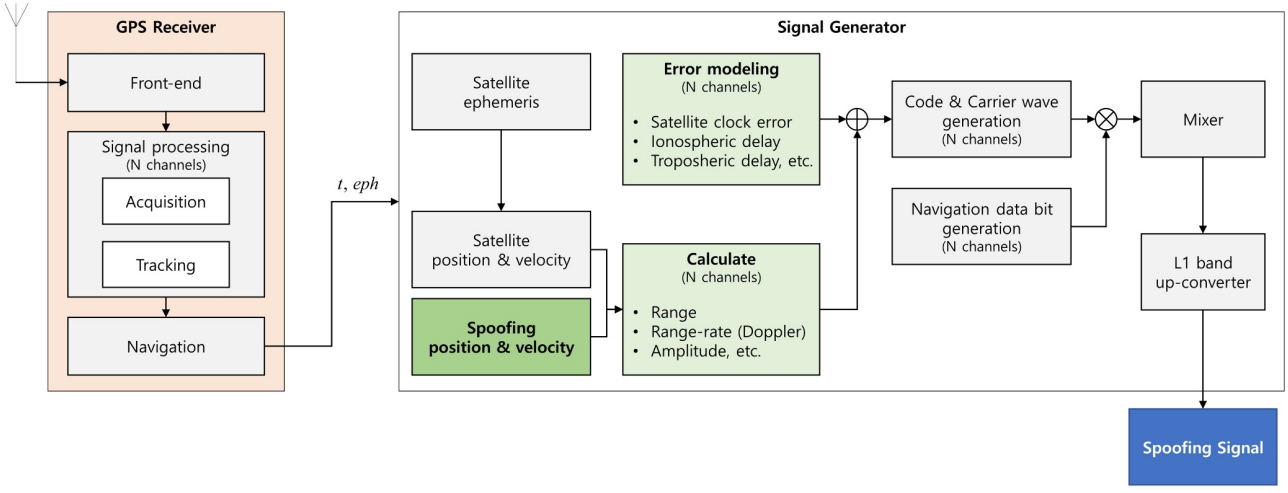


Fig. 4. Conventional spoofing signal generator. This generator requires external information, such as GPS satellites ephemeris, and complicated signal processes, such as range, range-rate calculation, and error source modeling.

ing position, $\Delta T^i(t)$ is the satellite clock error, $I^i(t)$ is the ionospheric delay, $T^i(t)$ is the tropospheric delay, ε^i is the noise term, $v_s^i(t)$ is the satellite-to-spoofing relative velocity vector, $a_s^i(t)$ is the line-of-sight (LOS) vector, c is the speed of light; $f_{s,carr}^i(t)$ is the carrier frequency of the target spoofing position, and $f_{t,carr}$is the carrier frequency used for satellite transmission. The error components (i.e., satellite clock error, ionospheric delay, and tropospheric delay) must be set by using appropriate modeling techniques based on the satellite and weather information at the specific time considered. Moreover, the signal amplitudes $A_s^i(t)$ can be calculated to consider the free-space path loss with respect to the pseudorange of the respective satellites.

The ranges and range rates are used to obtain the PRN code, carrier phase, and Doppler frequency of each satellite. By using the ratio of the carrier frequency $f_{t,carr}$ to the code frequency $f_{t,code}$ of transmission and the Doppler frequency $f_{Dopp}^i(t)$, which can be derived from the range rates, the code phase $\varphi_s^i(t)$ is calculated as follows:

$$f_{s,code}^i(t) = \left(f_{t,code} + \frac{f_{Dopp}^i(t)}{1540}\right), \quad (1540 = f_{t,carr}/f_{t,code}), \tag{3}$$

$$N_{chips}^i(t) = \frac{f_{s,code}^i(t)}{1000}, \tag{4}$$

$$L_{chip}^i(t) = \frac{c}{f_{s,code}^i(t)}, \tag{5}$$

$$\varphi_s^i(t) = rem\left(\frac{\rho_s^i(t)}{L_{chip}^i(t)}, N_{chips}^i(t)\right), \tag{6}$$

where $f_{s,code}^i(t)$ is the code frequency at the target spoofing position, $N_{chips}^i(t)$ is the number of code chips for 1 ms, and $L_{chip}^i(t)$ is the length of one code chip in m. Dividing the pseudorange by the code-chip length yields the total number of code chips for the pseudorange; the remainder obtained when dividing the pseudorange by $N_{chips}^i(t)$ yields the code phase $\varphi_s^i(t)$. The code phase is used to generate the PRN code $C_s^i(t)$ for each satellite, as defined in [18]. Then, the carrier phase $\phi_s^i(t)$ is given by

$$\phi_s^i(t) = rem\left(\frac{\rho_s^i(t)}{L_{cycle}^i(t)}\right) \cdot 2\pi, \tag{7}$$

where $L_{cycle}^i(t)$ is the length of one carrier cycle in m. As with the code-phase calculation, the remainder obtained when dividing the pseudorange by the carrier-cycle length yields the carrier phase $\phi_s^i(t)$. The carrier wave is generated by applying the Doppler frequency and carrier phase to a trigonometric function.

The process of generating the PRN code and the carrier wave is fairly complex; the most complicated aspect of signal generation is the generation of the navigation message, which is generated using the ephemeris provided by external sources, such as the International GNSS Service (IGS) [19] and the Crustal Dynamics Data Information System (CDDIS) [20].

Table 1. Simplified ephemeris data definition (navigation message description of RINEX 3.03).

# of line	Description
1	Satellite system (GPS) / PRN, Epoch: Toc—Time of Clock, Month, day, hour, minute, second, Satellite clock bias, Satellite clock drift, Satellite clock drift rate
2	IODE, C_{rc}, Δn, M_0
3	C_{us}, e, C_{us}, $\sqrt{A}$
4	t_{oe}, C_{ic}, Ω_0, C_{is}
5	i_0, C_{rc}, ω, $\dot{\Omega}$,
6	IDOT, Codes on L2 channel, GPS week, L2 P data flag

Table 1 summarizes the ephemeris parameters listed in each row of the navigation message description of the Receiver Independent Exchange Format (RINEX) 3.03. Further, Appendix A provides a detailed definition of each parameter. The ephemeris includes timing and satellite orbit information. By using this information, the satellite orbit parameters at each time interval can be predicted. Then, the timing and orbit information is transformed into each subframe of the navigation message by reversing the message decoding procedure defined in [18].

Finally, the spoofing signals $S_s^i(t)$ can be represented as the product of the obtained components as follows:

$$S_s^i(t) = A_s^i(t)C_s^i(t)D_s^i(t)\cos(2\pi f_{s,carr}^i(t)\cdot t + \phi_s^i(t)). \tag{8}$$

Here, $A_s^i(t)$ is the amplitude, $C_s^i(t)$ is the PRN code, $D_s^i(t)$ is the navigation data, and $\cos(2\pi f_{s,carr}^i(t)\cdot t + \phi_s^i(t))$ is the carrier wave.

The main advantage of conventional spoofing signal generators is that a signal can be generated for a target spoofing position at the desired time. However, as explained above, conventional generators require additional information, such as the broadcast ephemeris [19, 20] for signal generation. Moreover, further processing is required to generate the navigation message bits using the ephemeris. In addition, if a simulator generates spoofing signals to deceive a target receiver that also receives authentic GPS signals, it cannot be guaranteed that the characteristics of the authentic GPS signals and the spoofing signals will be similar enough to spoof the target receiver effectively. This is because the spoofing signals are generated independently using only the timing and orbit information of the GPS signals that the spoofing signals

are intended to counterfeit. Additionally, although various error-modeling techniques can be applied to signal generation, the simulation of the actual signal-reception environment through modeling has limitations.

4. SPOOFING SIGNAL GENERATION BASED ON SIGNAL PROCESSING OF A GPS RECEIVER

We propose a spoofing signal generation method using the signal processing results of a software-based receiver without using GPS simulators. This method does not require additional navigation message information because it uses the tracking and navigation results of received GPS signals. It also does not require error modeling because the spoofing signals are generated using the received GPS signals. Therefore, this method offers the advantage that the spoofing signal characteristics can be tailored to be similar to those of the authentic GPS signals. Fig. 5 shows a schematic of the proposed spoofing signal generator; it primarily consists of a software GPS receiver, a pseudorange-delay and Doppler-frequency calculator, and a spoofing signal mixer.

4.1. GPS signal processing

In the proposed method, the receiver processes the received authentic GPS signals and provides the processing results to the spoofing signal-generator block. The receiver processes GPS signals through the signal acquisition, tracking, and navigation steps (in that order) [21]. In the acquisition step, the approximate code phases and Doppler frequencies for each visible GPS satellite are estimated using the intermediate frequency (IF) signal input from the front-end component. The signal parameters obtained in this step are used to track signals more precisely in the tracking channels. The tracking channels provide signal parameters to the spoofing signal generation block; these parameters include the signal amplitude, navigation message, PRN code, carrier phase, and Doppler frequency of each satellite. Then, navigation is performed using the navigation message and the receiver's clock. The position, velocity, and LOS vectors between the receiver and the visible satellites are sent to the spoofing signal generation block.

4.2. GPS-to-spoofing pseudorange delay and Doppler frequency calculations

The results obtained from the navigation process are used to calculate the pseudorange delay and Doppler frequency between the GPS and the spoofing signals. The operating principle of the calculator is based on the vector tracking loop technique (VTL) [22]. The VTL is typically used to improve the performance of the signal-tracking loop from the navigation information of the receiver. However, we applied this technique here to generate the spoofing signal parameters.

First, the pseudorange delay can be obtained from the relative position between the estimated GPS position and the target spoofing position. Fig. 6 describes the relationship between the GPS position of the receiver and the target spoofing position. If $X(t) = [x(t), y(t), z(t)]$ is the estimated GPS position and $X_s(t) = [x_s(t), y_s(t), z_s(t)]$ is the target spoofing position, the relative position, $\Delta P(t)$, is represented as

$$\Delta P(t) = X_s(t) - X(t). \tag{9}$$

Then, the pseudorange delay, $\Delta\rho^i(t)$, for each satellite signal can be obtained from the LOS vectors, $H^i(t)$, and the

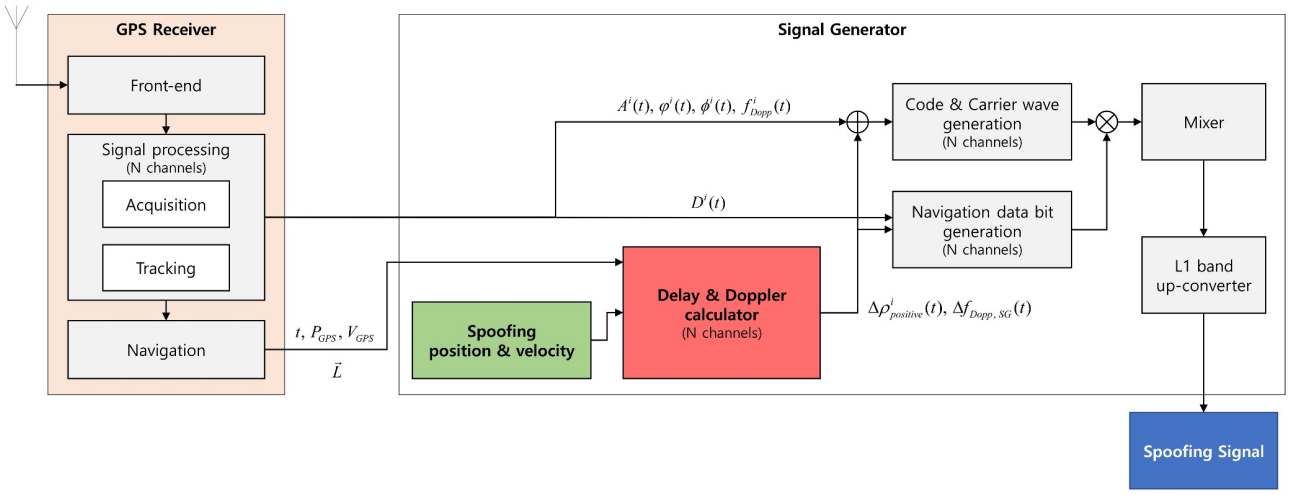


Fig. 5. Proposed spoofing signal generator that uses authentic GPS signals being received by a receiver. The proposed generator uses the GPS signal processing results so that the spoofing signal generation process can be simplified, and the generated spoofing signal has characteristics very similar to those of the authentic GPS signal.

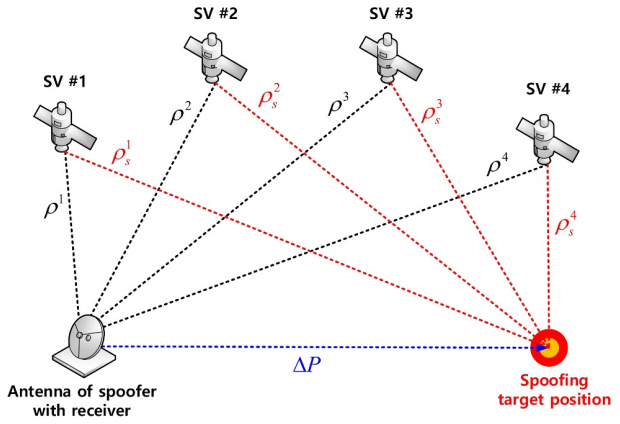


Fig. 6. Relationship between the estimated GPS position and the target spoofing position.

relative position as follows:

$$\Delta\rho^i(t) = H^i(t) \cdot \Delta P(t). \tag{10}$$

At this stage, the pseudorange of the spoofing signals to the visible satellites may sometimes be shorter than the pseudorange of the GPS signals owing to the geometric characteristics between the estimated GPS position and the target spoofing position. Because the pseudorange is determined by the relative difference in the navigation data and the code phase of the signals tracked in each channel, the signal processing results may not be provided by the receiver when the pseudorange delay is negative. To avoid this problem, all delays are converted to positive numbers based on the smallest pseudorange delay. Thus, the final pseudorange delay, $\Delta\rho^i_{positive}(t)$, and time delay, Δt^i, can be calculated as follows:

$$\rho_{positive}(t) = \left|\min(\Delta\rho^i(t) < 0)\right|, \tag{11}$$

$$\Delta\rho^i_{positive}(t) = \Delta\rho^i(t) + \rho_{positive}(t), \tag{12}$$

$$\Delta t^i = \Delta\rho^i_{positive}(t)/c. \tag{13}$$

If the target spoofing position is set to the true position of the antenna of the target receiver, the spoofing signal pseudorange of each satellite can be generated for the position of the target receiver. In this case, if a certain delay is applied to all the spoofing pseudoranges for the satellites, it is possible to generate spoofing signals by causing the target receiver to calculate different times for the actual position of the target receiver. This indicates that it is possible to initiate spoofing of both position and time using the proposed method. However, this study focuses on the position spoofing, which most significantly affects the navigation results of the target receiver.

Second, the spoofing Doppler frequency $f_{Dopp,SG}(t)$ operating between the target spoofing position and the GPS position can be calculated using the relative position and the relative velocity between the two positions as follows:

$$f_{Dopp,SG}(t) = -\left(\frac{V_S(t) - V(t)}{c}\right) \cdot \left(\frac{X_S(t) - X(t)}{\|X_S(t) - X(t)\|}\right) f_{t,carr}, \tag{14}$$

where $V_s(t)$ is the velocity at the spoofing position, and $V(t)$ is the velocity at the estimated GPS position. As explained above, through these delay and Doppler calculations, the spoofing signal parameters can be obtained in a very intuitive and simple manner without the complicated derivation processes adopted by conventional signal simulators.

4.3. Spoofing signal mixer

The spoofing signal mixer generates the final spoofing signal using the tracked-signal parameters delivered by the receiver, as well as the pseudorange delay and spoofing Doppler frequency obtained from the delay and Doppler calculator. At this stage, the mixer has all the information required for regenerating the signal received by the receiver. Therefore, it can restore the received authentic GPS signal with high detail. The regenerated GPS signal $S^i(t)$ can be expressed as follows:

$$S^i(t) = A^i(t)C^i(t)D^i(t)\cos(2\pi f^i_{carr}(t)\cdot t + \phi^i(t)) + \eta(t), \tag{15}$$

where $A^i(t)$ is the amplitude of the signal, $C^i(t)$ is the PRN code, $D^i(t)$ is the navigation bit, $\phi^i(t)$ is the carrier phase, $f^i_{carr}(t)$ is the carrier frequency to which the Doppler frequency is applied, and $\eta(t)$ is the noise component, which includes processing noise and numerical errors.

The spoofing signal is generated by applying the pseudorange delay and the spoofing Doppler frequency to the regenerated GPS signal. Therefore, it is evident that the generated spoofing signal closely reflects the characteristics of the authentic GPS signal. The time delay Δt^i derived from the pseudorange delay is applied to the regenerated signal to shift the signal parameters. The spoofing Doppler frequency is added to the carrier frequency of the regenerated signal. The spoofing signal $S^i_s(t)$ is thus represented as follows:

$$\begin{aligned} S^i_s(t) =& A^i(t+\Delta t^i)C^i(t+\Delta t^i)D^i(t+\Delta t^i) \\ & \times \cos(2\pi\cdot\{f^i_{carr}(t+\Delta t^i) + f^i_{Dopp,SG}\}\cdot t \\ & + \phi^i(t+\Delta t^i)) \\ =& A^i_s(t)C^i_s(t)D^i_s(t)cos(2\pi f^i_{s,carr}(t)\cdot t + \phi^i_s(t)) \\ & + \eta(t), \end{aligned} \tag{16}$$

where $A^i_s(t)$, $C^i_s(t)$, $D^i_s(t)$, $\phi^i_s(t)$, and $f^i_{s,carr}(t)$ are the amplitude, PRN code, navigation bit, carrier phase, and carrier frequency of the spoofing signal, respectively. Table 2 provides a comparison between the conventional and

Table 2. Summary of the process comparison required for signal generation between the conventional and the proposed spoofing signal generator (O=required, X=not required).

	Conventional	Proposed
Cost	High	Low
Tracking result	X	O
Navigation result	X	O
Spoofing position & velocity	O	O
External ephemeris	O	X
Satellite position calculation	O	X
Satellite clock error modeling	O	X
Ionospheric delay modeling	O	X
Tropospheric delay modeling	O	X
Spoofing pseudorange delay calculation	X	O
Spoofing Doppler frequency calculation	X	O

proposed spoofing signal generators. It can be seen that, with the exception of the signal processing operations required to ensure similarity with the authentic GPS signals, the signal-generation process of the proposed generator is simpler than that of the conventional signal generator. This is because the complicated process of generating spoofing signals in the conventional signal generator is simplified by calculating the spoofing pseudorange delay and Doppler frequencies using the proposed method.

5. EXPERIMENTAL RESULTS AND ANALYSIS

To test the performance of the proposed method, we conducted an experiment using authentic GPS signal data and the software receiver presented in [23]. The GPS signal data used were open-source data recorded using the SiGe GN3S sampler presented in [24]. Table 3 details the specifications of the authentic signal data. GPS signal data were used as input to the software receiver. Then, the software receiver tracked the authentic GPS signals and obtained navigation solutions. As explained in the subsections below, the software receiver also tracked the generated spoofing signals and calculated the navigation solutions to explain how similar the generated spoofing signals are to the authentic GPS signals. In the experiments, all the authentic and spoofing signal streams were stored in units of 8 bytes per sample based on the bit for which the first TOW of each signal was calculated. Then, through the sample index, all the signal streams were synchronized to analyze the experimental results.

Table 3. Specifications of GPS signal data used.

Data name	SiGe_Bands-L1.dat
Signal type	GPS L1 C/A
Antenna motion	Static
Intermediate frequency	4.092 MHz
Sampling frequency	16.368 MHz
Sample type	8 bit
Recording date	2013-05-23
PRN	1, 7, 8, 9, 11, 17, 28

5.1. Static spoofing scenario

The spoofing signals were generated using the signal-tracking results and the navigation solution obtained from the software receiver, as explained in Section 3. The target spoofing position was set to have an offset of 1,500 m east, 1,000 m north, and 500 m above the initial position of the authentic GPS in the earth-centered earth-fixed coordinate system.

Fig. 7 presents the spoofing signal parameters obtained from the delay and Doppler calculator. Fig. 7(a) presents the spoofing Doppler frequency and indicates that it had

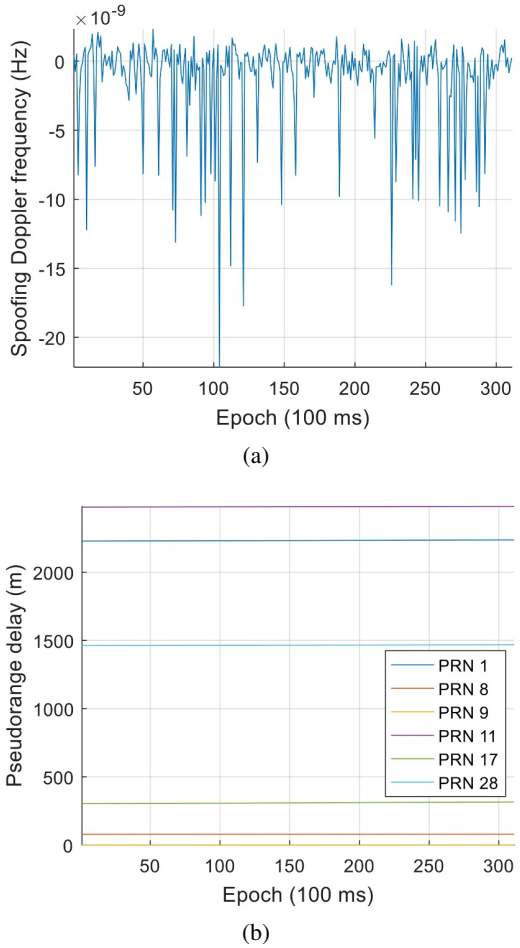


Fig. 7. Spoofing signal parameters calculated by the delay and Doppler calculator: (a) spoofing Doppler frequency and (b) pseudorange delay.

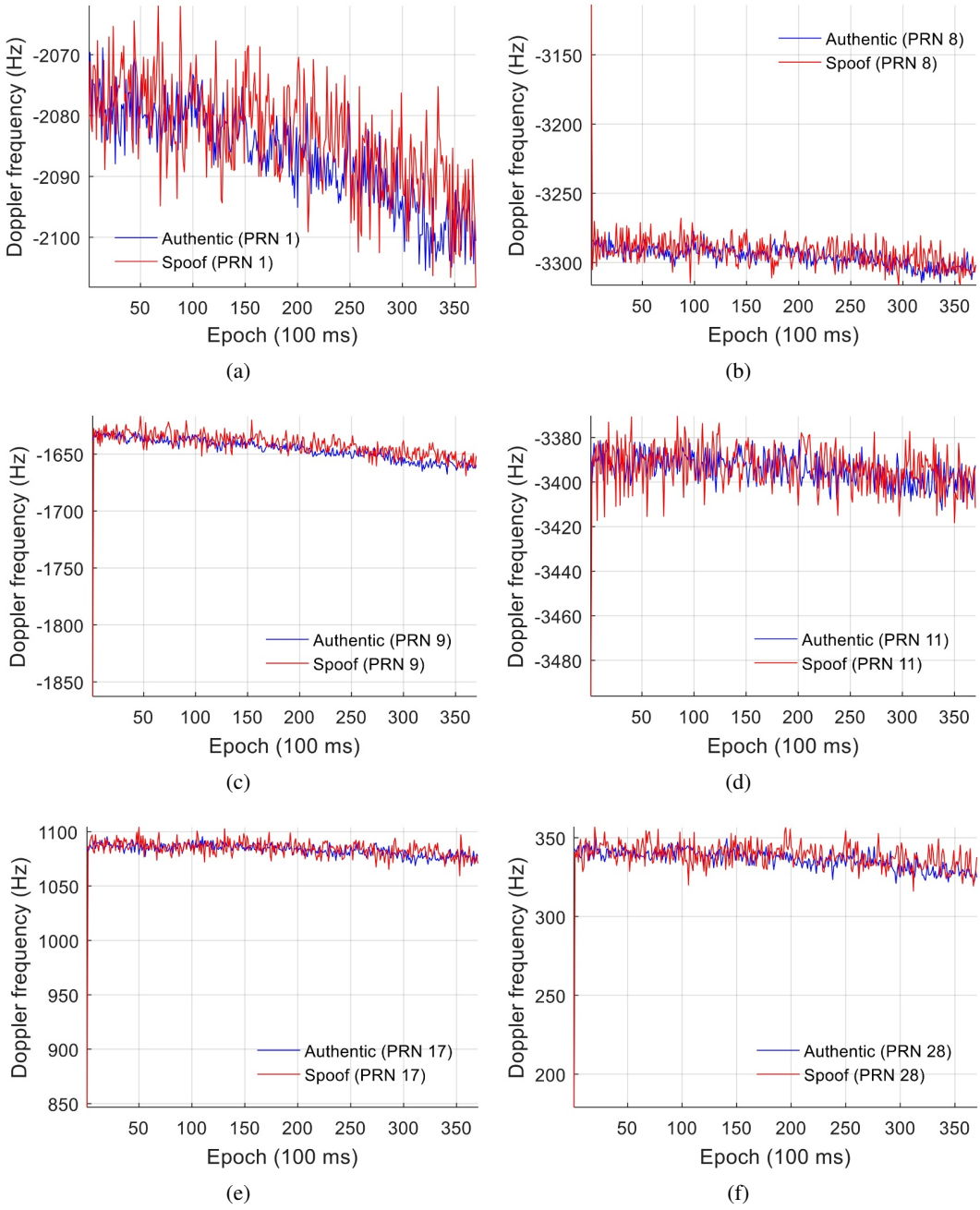


Fig. 8. Estimated Doppler frequencies obtained from the authentic GPS signals and the generated spoofing signals for (a) PRN 1, (b) PRN 8, (c) PRN 9, (d) PRN 11, (e) PRN 17, and (f) PRN 28.

a value close to 0 Hz because the authentic-GPS position and the target spoofing position were static. Fig. 7(b) presents the pseudorange delay for each PRN signal. The pseudorange delays were calculated according to the geometric arrangement between the position of the visible satellites, authentic GPS position, and target spoofing position. These delays were then used to shift the authentic GPS-signal-tracking results.

Fig. 8 presents the estimated Doppler frequency of the authentic GPS signals and the spoofing signals generated using the software receiver. Figs. 8(a)-(b) present the estimated Doppler frequencies for PRN 1 and 8, respectively. The figures indicate that the estimated Doppler frequencies of the spoofing signals have values similar to those of the authentic GPS signals. Figs. 8(c)-(f) present the estimated Doppler frequencies for PRN 9, 11, 17, and 28, respectively. Although there is an initial estimation error, the figures indicate that the estimated Doppler frequencies of the spoofing signals converge to values similar to those of the authentic GPS signals. However, the covariance of

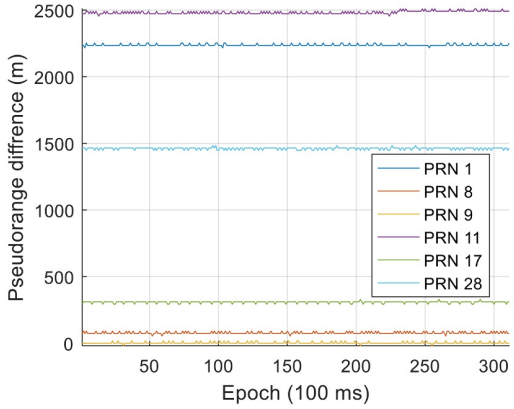


Fig. 9. Pseudorange difference between the authentic GPS signals and the generated spoofing signals.

the Doppler frequencies of the spoofing signals is larger because it includes the numerical errors and processing noise from digitally reprocessing the tracking results of the receiver.

Fig. 9 presents the difference in pseudorange between the authentic GPS signals and the generated spoofing signals. The figure indicates that the pseudorange difference is almost the same as the pseudorange delay presented in Fig. 7(b). Therefore, the results presented in Fig. 9 indicate that the pseudorange delay values given in Fig. 7(b) were appropriately applied to the authentic GPS signal tracking results because the relative differences between the PRNs were highly similar. This pseudorange difference directly affects the estimated target spoofing position.

Fig. 10 presents the positioning error for each reference position for both the GPS and the generated spoofing signals. Fig. 10(a) shows that the horizontal positioning errors for the spoofing signals had variance values similar to those of the authentic GPS signals in each direction. Similarly, Fig. 10(b) shows that the vertical positioning errors had similar characteristics to those of the authentic GPS signals. These results demonstrate that the proposed spoofing signal generation algorithm can appropriately mimic the characteristics of authentic GPS signals.

Fig. 11 presents the navigation solutions obtained from both the authentic GPS signals and the generated spoofing signals. Fig. 11(a) presents the local east position differences and indicates that the approximate differences were 1500 m, as intended. Figs. 11(b)-(c) present the local north and up position differences and confirm that the approximate differences in these directions were 1000 m and 500 m, respectively, as intended. Fig. 11(d) presents the receiver clock bias. Because both the authentic GPS signals and the spoofing signals had fairly similar characteristics in terms of pseudorange, the variances in both cases were almost the same.

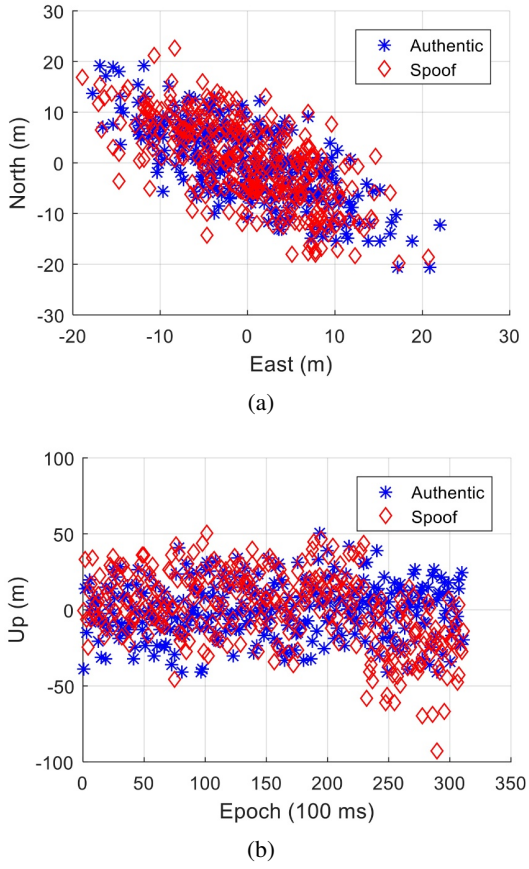


Fig. 10. Positioning error for each reference position for both the authentic GPS signals and the generated spoofing signals: (a) horizontal positioning error and (b) vertical positioning error.

5.2. Dynamic spoofing scenario

For the second experiment, we set a dynamic target spoofing position for the spoofing signals, as shown in Fig. 12. The GPS signal data provided in Table 3 were again used for this experiment. The target spoofing position was set to perform a counterclockwise circular motion with a 1,000 m radius, starting from the east of the initial GPS position. As in the static case, the spoofing signals were generated using the proposed algorithm described in Section 4.

Fig. 13 presents the navigation solutions obtained from both the authentic GPS signals and the generated spoofing signals. Figs. 13(a)-(b) present the local east and north position differences, respectively. The figures indicate that the spoofing signals were generated along the desired target position and were processed normally by the software receiver, as intended. Fig. 13(c) presents the local up position difference. Because we set the target spoofing position only in the horizontal plane, the up difference values were almost insignificant, with a small offset caused by the processing noise and the estimation error. Fig. 13(d)

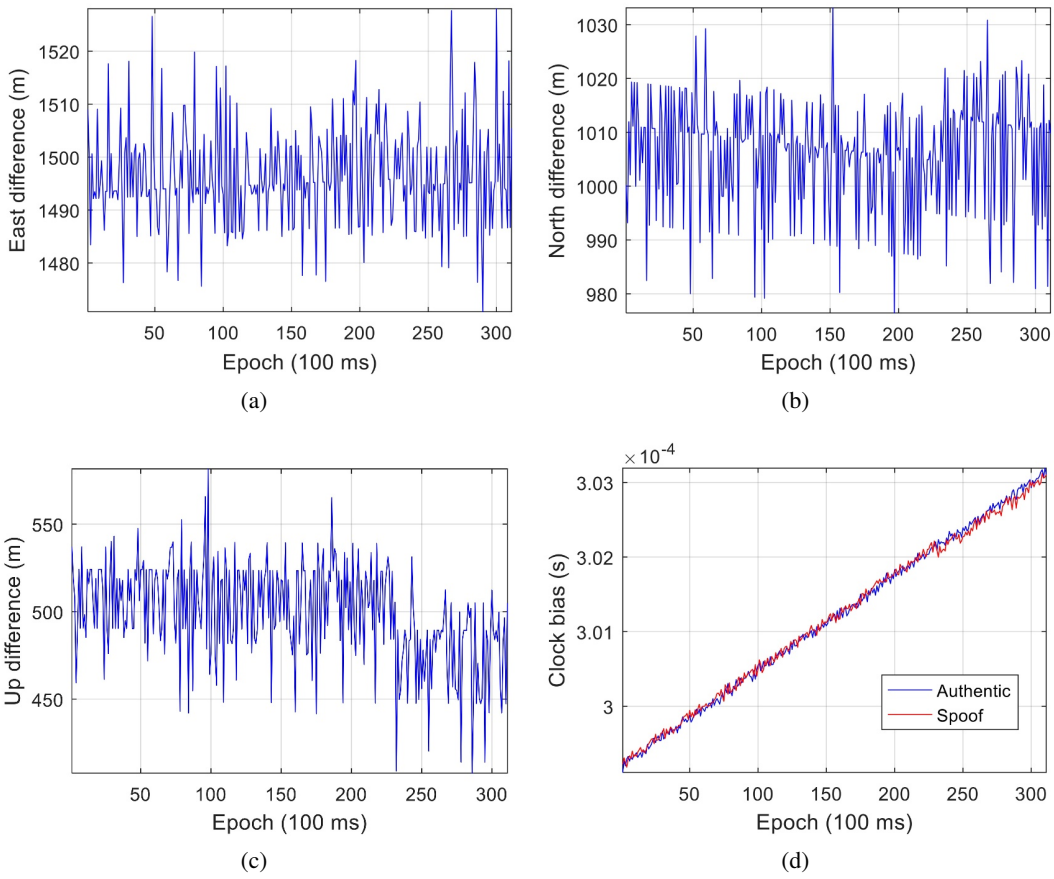


Fig. 11. Comparisons of navigation solutions obtained from authentic GPS signals and generated spoofing signals: (a) local east position difference, (b) local north position difference, (c) local up position difference, and (d) receiver clock bias.

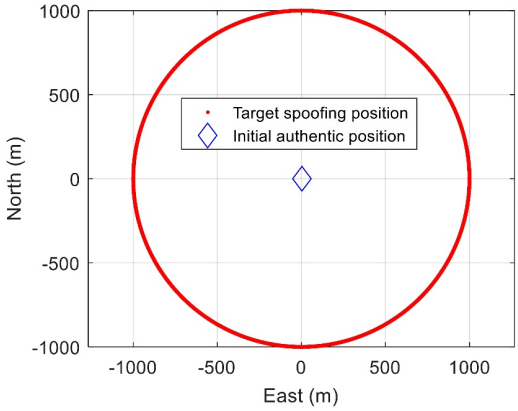


Fig. 12. Target spoofing position for generated spoofing signals in a dynamic scenario.

presents the receiver clock bias; although the bias leads to oscillations of the spoofing signals owing to the dynamic characteristics of the target spoofing position, the overall tendency of the receiver clock bias for the spoofing signals is similar to that for authentic GPS signals.

The navigation solutions in both the static and dynamic scenarios were directly affected by the measurements. Therefore, the similarity in characteristics between the navigation solutions means that the measurement characteristics were similar. In other words, we verified that the characteristics of the authentic GPS signals and the generated spoofing signals were nearly identical. In conclusion, as mentioned in Section 1, we have demonstrated that the proposed algorithm is effective enough to deceive a target GPS receiver.

5.3. Signal performance and anti-spoofing techniques

To analyze the performances of the signals generated by the proposed method and those generated by the conventional signal generator, we use an anti-spoofing technique based on the signal-characteristic analysis [2]. Fig. 14 presents the Doppler frequencies of the authentic GPS signals and spoofing signals generated by the proposed and conventional signal generators. As shown in the figure, the proposed method successfully incorporates the Doppler

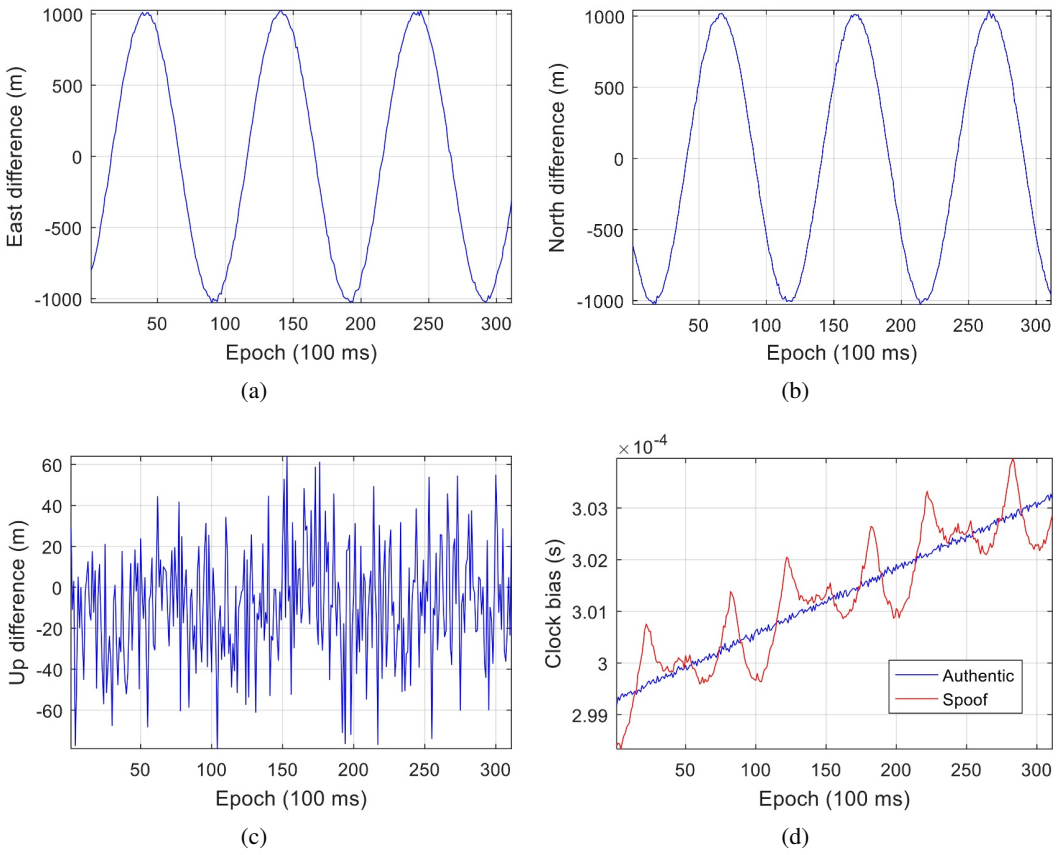


Fig. 13. Navigation solutions obtained from both the authentic GPS signals and the generated spoofing signals in a dynamic scenario: (a) local east position difference, (b) local north position difference, (c) local up position difference, and (d) receiver clock bias.

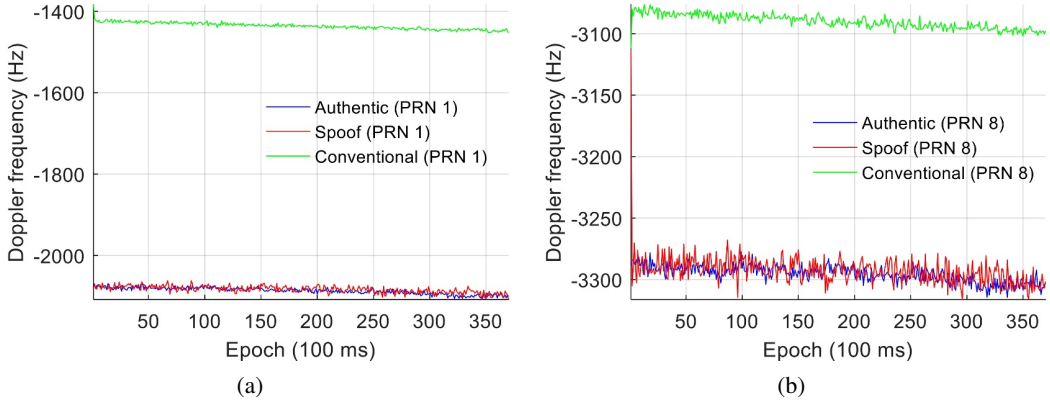
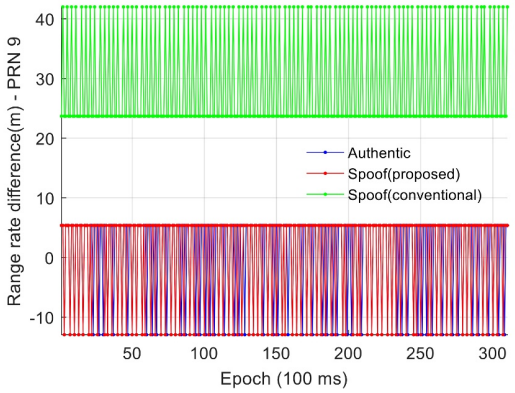
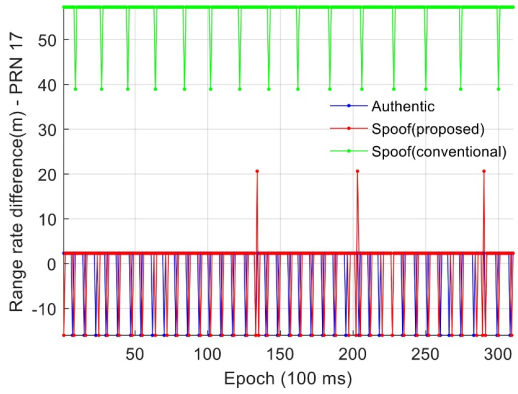


Fig. 14. Doppler frequencies of the authentic GPS signals and spoofing signals generated by the proposed and conventional signal generators: (a) PRN 1, (b) PRN 8.

frequencies in the spoofing signals, whereas the conventional signal generator does not. As a result, the spoofing signals generated by the conventional signal generator can easily be detected using the anti-spoofing technique. Fig. 15 presents the test statistics obtained by subtracting the average change in the authentic GPS pseudorange rate from the change in the spoofing pseudorange rates from both signal generators. In the proposed method, because the pseudorange is generated using the same code, carrier, and navigation data of the authentic GPS signals, the



(a)



(b)

Fig. 15. Range rate difference of the authentic GPS signals and spoofing signals generated by the proposed and conventional signal generators: (a) PRN 9, (b) PRN 17.

change in the pseudorange rate is highly similar to that of the authentic signals. However, because the signal from the conventional signal generator is produced using mathematical calculations based on external ephemeris information and error modeling, its corresponding test statistics have very large values. In addition, when selecting a reference channel for generating pseudoranges, conventional generators set a channel that tracks signals with the earliest or latest TOW as a reference channel. If the method of selecting the TOW of the reference channel between a target receiver and the conventional signal generator is different, the distinction in the range rate would be larger. This confirms that it is considerably more difficult to detect the spoofing signals generated by the proposed method than it is to detect those generated by the conventional method.

6. CONCLUSION

We have proposed a simple spoofing signal-generation algorithm that uses the processing results for authentic live GPS signals obtained from a GPS receiver. Since the proposed method is based on post-processing, it has the advantage of accurately analyzing the difference in signal characteristics between authentic and generated spoofing signals on a sample basis.

First, we briefly introduced conventional spoofing signal generators. These are typically expensive GPS simulators, with which it is difficult to configure and set up experimental environments. Further, such simulators require external GPS ephemeris information for a specific time in order to generate spoofing signals. GPS simulators also use navigation data from the GPS ephemeris and model signal parameters, such as satellite clock error, ionospheric delay, and tropospheric delay, to follow a complicated generation process. Because the signals generated by the simulators are generated arbitrarily by the user, their characteristics may differ from those of the authentic GPS signals received by the receiver. Therefore, we proposed the aforementioned spoofing signal generation algorithm that uses the processing results of the receiver for authentic live GPS signals. A key advantage of this method is that the spoofing signals are generated based on the authentic GPS signals currently arriving at the receiver. Therefore, effective spoofing signals with characteristics similar to those of authentic GPS signals can be generated without the requirement of expensive GPS simulators. We performed experiments using a software receiver to compare the results obtained after processing authentic live GPS signals and the corresponding spoofing signals generated via the proposed method. These results indicate that the characteristics of the generated spoofing signals are highly similar to those of authentic GPS signals, and that the receiver calculated its intended navigation solution using the spoofing signals. In addition, the experiment described in Section 5.3 shows that the spoofing signals generated by the proposed method, unlike those generated by the conventional signal generator, are difficult to detect using previously studied anti-spoofing techniques based on signal characteristics analysis.

In conclusion, because the proposed method can be implemented through a post-processing open-source software GPS receiver at the PC-level, it can be effectively used to study spoofing or anti-spoofing techniques in algorithm verification stages.

APPENDIX A

Table A.1. Description of ephemeris parameters [18].

Parameter	Definition
M_0	Mean anomaly at reference time
Δn	Mean motion difference from computed value
e	Eccentricity
$\sqrt{A}$	Square root of the semi-major axis

Ω_0	Longitude of ascending node of orbit plane at weekly epoch
i_0	Inclination angle at reference time
ω	Argument of perigee
$\dot{\Omega}$	Rate of right ascension
IDOT	Rate of inclination angle
C_{uc}	Amplitude of the cosine harmonic correction term to the argument of latitude
C_{us}	Amplitude of the sine harmonic correction term to the argument of latitude
C_{rc}	Amplitude of the cosine harmonic correction term to the orbit radius
C_{rs}	Amplitude of the sine harmonic correction term to the orbit radius
C_{ic}	Amplitude of the cosine harmonic correction term to the angle of inclination
C_{is}	Amplitude of the sine harmonic correction term to the angle of inclination
t_{oe}	Reference time ephemeris (reference paragraph 20.3.4.5)
IODE	Issue of data (ephemeris)

REFERENCES

[1] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homel Secur J*, vol. 25, no. 2, pp. 19-27, December 2003.

[2] H. Wen, P. Y.-H. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," *Proc. ION GNSS*, pp. 1285-1290, 2005.

[3] A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," *Proc. IEEE/ION PLANS*, pp. 479-487, 2012.

[4] A. Jafarnia-Jahromi, A. Broumandan, S. Daneshmand, N. Sokhandan, and G. Lachapelle, "A double antenna approach toward deteection, classification and mitigation of GNSS structural interference," *Proc. NAVITEC*, pp. 1-8, 2014.

[5] D. S. Radin, *GPS Spoofing Detection Using Multiple Antennas and Individual Space Vehicle Pseudoranges*, M.S. thesis, Dept. Elect. Eng., Univ. of Rhode Island, 2015.

[6] H. So, J. Jang, K. Lee, and J. Park, "Performance analysis of a COTS GPS receiver against spoofing attack and spoofing detection method using RAIM and a single authentic signal," *JSASS*, vol. 60, no. 5, pp. 312-319, May 2017.

[7] H. Kuusniemi, M. Z. H. Bhuiyan, and T. Kroger, "Signal quality indicators and reliability testing for spoof-resistant GNSS receveir," *EJN*, vol. 11, no. 2, pp. 12-19, August 2013.

[8] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, L. Demicheli, and W. Feng, "A new signal quality monitoring method for anti-spoofing," *Proc. CSNC*, pp. 221-231, 2018.

[9] C. Tanıl, P. M. Jimenez, M. Raveloharison, B. Kujur, S. Khanafseh, and B. Pervan, "Experimental validation of INS monitor against GNSS spoofing," *Proc. ITM. Satellite Division. ION GNSS+*, pp. 2923-2937, 2018.

[10] Satgen GNSS Simulation Software. [Online]. Available: https://www.labsat.co.uk/index.php/en/products/satgen-simulator-software, Accessed on Aug. 21, 2019.

[11] Labsat 3 GPS Simulator. [Online]. Available: https://www.labsat.co.uk/index.php/en/products/labsat-3, Accessed on Aug. 20, 2019.

[12] G. A. Elango, and G. F. Sudha, "Design of complete software GSP signal simulator with low complexity and precise multipath channel model," *JESIT*, vol. 3, no. 2, pp. 161-180, September 2016.

[13] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: development of a portable GPS civilian spoofer," *Proc. 21st ITM. Satellite Division. ION GNSS*, pp. 2314-2325, 2008.

[14] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *JFR*, vol. 31, no. 4, pp. 617-636, July 2014.

[15] A. M. Khan, N. Iqbal, and M. F. Khan, "Synthetic GNSS spoofing data generation using field recorded signals," *MethodsX*, vol. 5, pp. 1272-1280, January 2018.

[16] E. Horton and P. Ranganathan, "Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter," *J. Glob. Position. Syst.*, vol. 16, no. 1, pp. 1-11, December 2018.

[17] S. H. Im, and G. I. Jee, "Software-based real-time GNSS signal generation and processing using a graphic processing unit (GPU)," *JPNT*, vol. 3, no. 3, pp. 99-105, September 2014.

[18] GPS Directorate. Systems Engineering & Integration Interface Specification IS-GPS-200, Revision J. 2018. [Online]. Available: https://www.gps.gov/technical/icwg/IS-GPS-200J.pdf, Accessed on: Aug. 20, 2019.

[19] INTERNATIONAL GNSS SERVICE. [Online]. Available: http://www.igs.org/products/data, Accessed on Aug. 20, 2019.

[20] Crustal Dynamics Data Information System. [Online]. Available: https://cddis.nasa.gov/index.html, Accessed on Aug. 20, 2019.

[21] J. B. Tsui, *Fundamental of Global Positioning System Receivers: A Software Approach*, 2nd ed., John Wiley & Sons, Hoboken, Ltd, 2005.

[22] S. Zhao and D. Akos, "An open source GPS/GNSS vector tracking loop – Implementation, filter tuning, and results," *Proc. ITM. ION*, pp. 1293-1305, 2011.

[23] K. Borre and D. Akos, "A software-defined GPS and Galileo receiver: single-frequency approach," *Proc. ION GNSS*, pp. 1632-1637, 2005.

[24] ION GNSS Software Defined Receiver Metadata Standard. [Online]. Available: http://sdr.ion.org/api-sample-data.html, Accessed on: Aug. 21, 2019.

Seong-Hun Seo received his B.S. and Ph.D. degrees in electronics engineering from Konkuk University, Seoul, Korea, in 2014 and 2020, respectively. His research interests include precise GPS positioning, GPS/INS integration, software GNSS receivers, anti-jamming and anti-spoofing techniques, multiple sensor fusion systems, and integrated navigation system for UGV and UAV.

Gyu-In Jee received his B.S. and M.S. degrees in control and measurement engineering from Seoul National University, Korea, in 1982 and 1984, respectively, and a Ph.D. degree in control engineering from Case Western Reserve University, Cleveland, Ohio, USA in 1989. His research interests include indoor positioning, software GNSS receiver, precise GNSS positioning, anti-jamming and anti-spoofing techniques, autonomous vehicles, SLAM, navigation through sensor fusion using GNSS, Lidar, Vision.

Byung-Hyun Lee received his B.S., M.S., and Ph.D. degrees in electronics engineering from Konkuk University, Seoul, Korea, in 2007, 2009, and 2016, respectively. His research interests include software GNSS receivers, GNSS modernization, precise positioning, GNSS anti-jamming and anti-spoofing techniques, and navigation for autonomous vehicles through sensor fusion using GNSS, Lidar, Vision.