Global Navigation Satellite System Signal Generation Method for Wide Area Protection against Numerous Unintentional Drones

Minhuck Park¹, Beomju Shin², Jin-Hee Han³, Hak-Du Kim³, and Changdon Kee¹*¹

¹Department of Aerospace Engineering and the Institute of Advanced Machines and Design, Seoul National University, Seoul 08826, South Korea
²Sensor System Research Center, Korea Institute of Science and Technology, Seoul 02972, South Korea
³Danam Systems Inc., Anyang 13930, South Korea
*Corresponding author: Changdon Kee (e-mail: kee@snu.ac.kr).

This research was supported by the “Research for wide area protection method” project funded by Danam Systems Inc. (Anyang, Korea) contracted by the Institute of Advanced Machines and Design at Seoul National University.

ABSTRACT This study proposed a wide area protection method using global navigation satellite system (GNSS) interference signals against numerous unintentional drones. The defensive GNSS signals generated by a single signal generator sweep the authentic GNSS signals so that the signal tracking loop tracks the defensive signals for the drones to be guided to a safe zone. The proposed algorithm performs a sweep in the measurement domain by adjusting the time offset of the signal generator, which makes it possible to sweep a wider area. In this fundamental study to confirm the possibility of wide area protection, we investigated the signal generation method for the transition of signal tracking locks from authentic to defensive signals in situations where a signal generator does not know the drones’ positions. We examined the time discrepancy between the authentic and defensive signals, and the worst-case analysis to determine the minimum sweep range of the time offset. The determined minimum sweep range overcomes the influence of time discrepancy and unconditionally deceives multiple drones regardless of the satellite’s position, drones’ trajectories, and entry timing. To deceive drones approaching a sphere with a radius of 1 km, the minimum sweep range is approximately 6 and 3 km when the signal generator is 0 and 2 km away from the center of the sweep region, respectively. The simulation results verified the theoretical analysis and showed that the defensive signals transmitted by one signal generator can deceive multiple drones to the center of the sweep region, which is the intended location.

INDEX TERMS Global navigation satellite system, Interference, Signal generators, Protection, Unmanned aerial vehicles

I. INTRODUCTION

Drones, which are representative unmanned aerial vehicles, have been used in various fields such as transportation, agriculture, and sports. The development of drones is expected to bring convenience to our daily lives. However, a drone loaded with radioactive sand landed on the roof of the Japanese Prime Minister’s Office in 2015 [1]. In 2018, the president of Venezuela was attacked by a drone carrying explosives while he was making a speech [2]. These cases remind us of the side effects of the development of drones. The advantages of drones that anyone can buy cheaply, learn how to operate, and use easily become disadvantages when they are utilized for terrorism. The worst situation occurs when sinister drone swarms strike a single target, such as a key person or a major facility in the nation. It is very difficult to defend against several drone attacks, and it can be a fatal threat to national security. Therefore, it is necessary to establish defense methods against such multiple drone attacks.

We consider the global navigation satellite system (GNSS) interference signals as a defense method. In general, the GNSS interference signals are usually used in a negative sense, but in this study, they are used to protect key facilities from drone attacks. The GNSS is a key navigation system for unmanned aerial vehicles (UAVs), including drones, and the lower the price of the drones, the more dependent they are on the GNSS. The incorrect position of the drones caused by the GNSS interference makes it difficult to fly to the target point. We
assume that the attack drones use only the GNSS as a navigation system to simplify the problem.

The GNSS interference signals can be divided into jamming, meaconing, and spoofing. Jamming signals broadcast with significantly high power in the same bandwidth as the GNSS signals to prevent the drone from receiving authentic signals [3]. Although the jamming method is very simple to implement, the trajectory of the drone after jamming cannot be predicted. In the worst case, a drone that loses control due to navigation failure can unintentionally crash into a civilian area. Meaconing broadcasts GNSS signals with specific location and time information to the drone, unlike meaningless jamming signals [4]–[6]. The drone that receives the meaconing signals calculates the navigation solution to the intended position of the meaconing signals rather than the authentic signals. However, the meaconing signal strength is very strong, and this causes loss of tracking of the authentic signals and re-acquisition process to the meaconing signals in the drone’s receiver. Tracking lock loss and the re-acquisition process make it easy for the receiver detect the presence of the interference signals.

By contrast, spoofing signals sweep the autocorrelation functions (ACFs) of the authentic signals so that the signal tracking lock is maintained [7]. In other words, the navigation solution of the drone that receives the spoofing signals is changed to the intended position by the spoofer without being detected. There are two conditions for successful spoofing: first, the drone should receive spoofing signals with code delay and Doppler, similar to the authentic signals. This allows the receiver’s tracking lock to change from authentic signals to spoofing signals without lock loss. Second, the drone should receive spoofing signals with proper signal strength up to +12 dB compared to the authentic signal strength [8]. This prevents jamming and meaconing detection based on the signal strength of the receiver. Thus, spoofing is the most effective defense method that leads attack drones to a safe zone away from the major facility without being noticed. However, spoofing requires sophisticated signal generation.

Various studies have been conducted to generate spoofing signals, especially for one target. Successful spoofing field tests on civil UAVs have been reported using spoofing signals aligned with authentic signals [9]. The spoofed UAV moved in the opposite direction of the spoower’s intended trajectory due to the control to maintain its original trajectory. In [10], spoofing signals were generated and field tests targeting a ship were also performed. The ship has other sensors for navigation, but the wrong position was calculated using spoofing signals. In [8], the necessary conditions for UAV spoofing were analyzed through case studies on various factors, such as phase discriminator, integration time, loop filter order, bandwidth, signal strength, and Doppler error between the authentic and spoofing signals. In [11], case studies were conducted based on the signal strength, the clock, and position errors of three commercial GNSS receivers. By developing these case studies, the minimum conditions for spoofing signal strength and sweep velocity in a specific delay-locked loop (DLL) bandwidth for successful spoofing were analyzed [12]. In [13], a signal generation method was proposed in which spoofing signals and inverse signals of authentic signals are broadcast together so that the drone can receive only spoofing signals.

Few studies have been conducted on spoofing methods for multiple targets. In [14], the requirements for spoofing on multiple drones were analyzed while preserving their mutual distances and time offsets. For successful spoofing under the above constraints, a specific spoofer location, multiple transmission antennas, and other satellite constellation-based spoofing signals are required. This reflects the characteristics of formation flight, but can be used in a limited way from a spoofer’s point of view. The authors of [14] also briefly analyzed how to spoof multiple drones to the same location. There was no constraint on the spoofer’s position, and the clock bias of each drone was different. However, it was assumed that drones are close by a few meters, so that one spoofing signal can deceive all the drones even if it is not sweeping authentic signal. Therefore, sufficient analysis of thevalid range of spoofing signals was not performed. In addition, all the studies in [9]–[14] above assumed that the true location of the target drone is known. A spoofing trajectory that sweeps a known true trajectory of the drone was first created, and a spoofing signal was generated based on the trajectory.

In this study, we investigated a GNSS signal generation method for wide area protection. The GNSS signal generator, referred to as the defender in this paper, generates defensive signals based on a specific static point, and sweeps the time offset of the defender by a few µs. The adjustment of the time offset makes it possible to quickly sweep a wide range in the measurement domain compared to the conventional position domain, which provides wide area protection. We analyzed the time discrepancy between the authentic and defensive signals, which must occur because the defender does not know the drone’s position. Next, we conducted a worst-case analysis to determine the minimum sweep range of the defensive signals that overcomes the time discrepancy. As an example of a wide area protection, we designed defensive signals that can unconditionally deceive drones entering a sphere with a radius of 1 km. Regardless of the entry timing, entry angle, and speed, drones change their signal tracking lock to defensive signals if they pass the sphere. The calculated position of all deceived drones is the center of the sphere, and only the clock bias of the navigation solution has a different value depending on the drone. Unlike previous spoofing studies, the proposed method can deceive multiple drones simultaneously without the position and velocity information of the drones. This eliminates the need for equipment, such as the radar, to know the position of the drones. In addition, the proposed method uses a single signal generator and antenna, which can be implemented simply and economically. The proposed defense method can be said to be a type of spoofing technique, but it must be broadcasted with an appropriate signal strength to be a genuine spoofing technique. As the first study to determine
the possibility of a wide area protection using a sweep algorithm, we focused only on the conditions of the defensive signals to pass through the authentic signals.

Various studies have been performed on the detection of spoofing from a receiver’s perspective [15]–[17]. Typical detection methods include signal power monitoring [18]–[20], inertial navigation system (INS)-based detection [10], [21]–[23], automatic gain control (AGC)-based detection [24], receiver autonomous integrity monitoring (RAIM) [25], direction of signal arrival monitoring [26], [27], and clock bias monitoring [28]–[31]. The proposed sweep method can be detected by using the aforementioned detection algorithms. However, from the previously mentioned studies in [8]–[11] and the spoofing cases in Shanghai [32] and the Black Sea [33], commercial GNSS receivers are still vulnerable to sweep algorithms.

The rest of this paper is organized as follows: Section II describes the sweep method in the measurement domain and defines the wide area protection problem. Section III presents the time discrepancy analysis between the authentic and defensive signals in an attack drone, as well as the worst-case analysis to determine the minimum sweep range of the defender to unconditionally deceive drones. Section IV discusses the simulations for all possible cases to verify the analytic minimum sweep range and software-defined radio (SDR)-based simulation as an example of the wide area protection problem. Finally, Section V gives the conclusions of this study.

II. PROBLEM FORMULATION

In this section, a sweep method in the measurement domain is described and compared to the sweep in the conventional position domain. Then, we define the wide area protection problem and present the scope of this paper.

A. SWEEP IN THE MEASUREMENT DOMAIN

Most previous studies generated spoofing signals in the position domain, as shown in Fig. 1(a). First, a signal generator, commonly referred to as a spoofer, generates a spoofing trajectory that sweeps the original trajectory estimated by the radar. Then, based on the spoofing trajectory, the spoofer generates the spoofing signals. In this case, the ACFs of the spoofing signals pass through the ACFs of the authentic signals simultaneously in all satellites, but the sweep speed and direction for each satellite are different. For example, in Fig. 1(b), the sweep speed of satellite #2 is slower than that of the other satellites. This means that it is not an optimal method for fast and wide range sweeps.

However, the sweep method in the measurement domain in this study generates signals in a different way, as shown in Fig. 2. The signal generator, referred to as a defender in this paper, generates and transmits defensive signals based on a specific point expressed as the intended position, but is not identical to the true position of the drone. Instead, the defender generates a sweeping effect by adjusting the time offset, which in turn affects the transmission time of all the satellites’ defensive signals equally. This means that all the pseudoranges of the defensive signals are changed by the same amount. If the time offset is oscillated by 1 μs, it is equivalent to oscillating all pseudoranges by approximately 300 m. The ACFs of the defensive signals pass through the ACFs of the authentic signals at the same sweep speed, but at different timing. Sweep at the same high speed on all the satellites means that the sweep method in the measurement domain can sweep a much wider area in the same time compared to the sweep in the position domain.

The weighted sum of square errors (WSSE) may be large until the tracking locks of all the satellites are changed to defensive signals because the defensive signals and authentic signals meet at different timing. Therefore, the proposed method can be easily detected for WSSE-based RAIM and...
clock bias monitoring. In this work, we assumed that attack drones do not have any detection algorithm.

In practice, the influence of time discrepancy should be considered because the defender does not know the location of the drones. We discuss the time discrepancy in detail in Section III.

**B. DEFINITION OF WIDE AREA PROTECTION PROBLEM**

The wide area protection problem can be divided into two phases. The first phase is the transition process of the signal tracking lock from the authentic to defensive signals by the sweep in the measurement domain described in Section II.A. This process is referred to as deception. In general, deception is mainly used in a bad sense. However, in this study, deception is utilized in a good sense for defensive purpose. After successful deception, the defender can control the calculated position of the drones. The second phase is the transition process of the trajectory to move the drones to a safe zone. If the drones use only the GNSS for navigation and fly in the shortest path toward the target, the trajectory of the defensive signals should be set in the opposite direction of the safe zone to guide the drones to this safe zone. As the first study to examine the possibility of wide area protection using a sweep algorithm, this study deals only with the sweep conditions for the defensive signals corresponding to the first phase.

Fig. 3 shows the first-phase environment of the wide area protection problem. Numerous sinister drones approach the area of major facilities. The defender does not know the information about the drones, such as their number, trajectories, and entry timing. The defender must deceive the drones before they arrive at the major facilities. For this purpose, we designed a protection area (the purple sphere in Fig. 3) that the drones are expected to pass through to attack the area of major facilities. Drones passing through or being tangent to this protection area must unconditionally be deceived. Therefore, the radius of the protection area \( d \) is a requirement for the wide area protection problem.

We assumed that the defender uses a global positioning system (GPS) receiver or network to know the current GPS time and ephemeris information, and can generate and broadcast the defensive signals indicating the arbitrary locations. In this case, the defender generates the defensive signals indicating the center of the protection area and continuously oscillates the time offset to perform the sweep in the measurement domain. Adjusting the time offset changes the pseudoranges of all the satellites by the same amount, which forms a sphere in the position domain (the orange sphere in Fig. 3). The problem is to determine the minimum sweep range to always deceive the drones regardless of the drones’ trajectories, satellite’s position, and entry timing before the drones leave the sweep region.

When the defensive signal passes through the authentic signal, the defensive signal power affects the success of the deception. For this purpose, the defensive signal power should be stronger than the authentic signal power. The receiver’s loop filter bandwidth and sweep speed can also affect the success of this drone deception. We assumed that the defensive signals received are always stronger than the authentic signals in the drones, and the deception succeeds if the defensive signals pass through the authentic signals on the ACF.

The conditions for the transmitted power of the defensive signals, which is an important factor for signal generation, are not covered in this paper. If the defensive signal power is too strong, it can be considered jamming. If it is weaker than the authentic signal power, the signal tracking lock is not transferred to the defensive signal. Therefore, an appropriate transmitted power is required and it depends on the position of the defender. In this study, we assumed that the defender can broadcast the defensive signals with an appropriate transmitted power such that the received signal power in the drones is constant in all the sweep regions and stronger than the authentic signals. This assumption is sufficiently realistic if the defender is sufficiently far away from the sweep region.

The position indicated by the defensive signals can be moved in the process of the sweep, but the sweep region is no longer a sphere; thus, the theoretical analysis becomes difficult. To simplify the problem, the defensive signals indicate a static point and contain only civil GPS signals. Moreover, the user maintains its original trajectory and uniform motion during the deception process.

**III. ANALYSIS OF THE MINIMUM SWEEP RANGE**

First, we conducted an analysis of the time discrepancy between the authentic and defensive signals. Next, we conducted the worst-case analysis to find the minimum sweep range that always deceives the drones in spite of the time discrepancy.

**A. TIME DISCREPANCY ANALYSIS**
A conventional sweep method in the position domain assumes that the spoofer knows the location of the target. The spoofer adjusts the time offset so that the target can receive the spoofing signals at the same time as the authentic signals. However, the defender in the wide area protection problem does not know the information about the trajectory of the drones. Therefore, the best way for the defender is to generate defensive signals based on an arbitrary point where the drones are expected to pass.

Fig. 4 shows the process used to determine the time discrepancy of the drone between the authentic and defensive signal. All error sources, including unintentional clock biases of satellites, the defender, and drones, are ignored. At the center of the sweep region, the propagation delay \( i_{sc} \) of the authentic signal is expressed as follows:

\[
i_{sc} = \left\| \mathbf{R}_i - \mathbf{R}_c \right\|/c,
\]

where \( \mathbf{R}_i \) is the position of the i-th satellite, \( \mathbf{R}_c \) is the center of the sweep region, and \( c \) is the speed of light.

The defender can determine the center of the time delay \( t_{delay,c} \), so that the drone located at \( \mathbf{R}_c \) can receive the defensive signals synchronized with the authentic signals.

\[
t_f = \left\| \mathbf{R}_f - \mathbf{R}_c \right\|/c,
\]

\[
t_{delay,c} = t_{sc} - t_f,
\]

The position of the defender is expressed as \( \mathbf{R}_f \), and the propagation delay of the defensive signals at the center of the sweep region is expressed as \( t_f \). Therefore, the defender broadcasts signals with a delay of \( t_{delay,c} \).

The drone located at \( \mathbf{R}_d \) receives authentic signals with a propagation delay \( t_{su} \) that is different from \( t_{sc} \).

\[
t_{su} = \left\| \mathbf{R}_d - \mathbf{R}_c \right\|/c.
\]

The propagation delay of the defensive signal, defined as \( t_{fu} \) at \( \mathbf{R}_d \), is different from \( t_f \).

\[
t_{fu} = \left\| \mathbf{R}_f - \mathbf{R}_d \right\|/c.
\]

The sum of the center of the time delay and propagation delay is the total defensive signal delay at \( \mathbf{R}_d \). The time discrepancy between the authentic and defensive signals defined as \( \nabla \Delta t \) can be expressed as follows:

\[
\nabla \Delta t = t_{fu} - (t_{su} + t_{fu})
\]

\[
= (t_{su} - t_{sc}) - (t_{fu} - t_f)
\]

\[
= \Delta t_s - \Delta t_f,
\]

where \( \Delta t_s \) and \( \Delta t_f \) are the propagation delay differences of the authentic and defensive signals with respect to the position difference, respectively. Therefore, unless the drone is located at the center of the sweep region, the influence of the time discrepancy is always present.

In general, if the signal power of the defensive signal is sufficiently large and the time discrepancy is within 1 µs (1 chip), the deception can be successful even if the ACF of the defensive signal does not pass through the ACF of the authentic signal. In the theoretical analysis, deception occurs...
only when the defensive signals meet the authentic signal on the ACF.

To meet the authentic signal, the defender additionally adjusts the time offset $t_{\text{sweep}}$. The total delay time of the defender $t'_{\text{delay},i}$ is defined as follows:

$$t'_{\text{delay},i} = t_{\text{delay},i} + t_{\text{sweep}} .$$  \hfill (7)

The term $t'_{\text{delay},i}$ has a different value for each satellite, and $t_{\text{sweep}}$ is the same for all the satellites.

For the defensive signal to meet the authentic signal, the following equation must be satisfied:

$$t'_{\text{su}} - (t_{\text{delay,total}} + t_f) = 0$$

and

$$(t'_{\text{su}} - t_{\text{ic}}) - (t_{\text{ju}} - t_{\text{fc}}) - t_{\text{sweep}} = 0$$

$\therefore \ \Delta t' = t_{\text{sweep}}$ \hfill (8)

Equation (8) represents the deception condition at a specific time. The next subsection details the sweep conditions that satisfy (8) at least once while the drone passes through the sweep region.

**B. THE WORST-CASE ANALYSIS**

1) FORMULATION IN TIME DOMAIN

Fig. 5(a) shows the geometric description of the worst-case analysis to find the minimum sweep range. We fixed the trajectory of the drone as a straight line on $y = 0, z = d$. The term $d$ is the radius of the unconditional protection area in Fig. 3, which is an input parameter for the wide area protection problem. The defensive signals vibrate the time offset with an amplitude of $r/c$ (s) around the origin, which forms a spherical sweep region with a radius of $r$ (m). If the drone can be deceived regardless of all the possible satellite’s position, defender’s position, and the drone’s entry time in the sweep region, then any arbitrary drone approaching at a distance $d$ from the origin is always capable of being deceived. The farther the drone trajectory is from the center of sweep region, the less time the drone spends in passing through the sweep region, and the larger the time discrepancy. In other words, deception becomes more difficult. Therefore, if we find a sweep condition in which deception always succeeds for a drone approaching at a distance $d$ away from the origin, we can conclude that any drone approaching the unconditional protection area can always be deceived. The position of the drone is expressed as follows:

$$\mathbf{R}_d(t) = [-V_u t \ 0 \ d]^T, \ (-0.5t_{su} \leq t \leq 0.5t_{su})$$  \hfill (9)

$$t_{su} = 2\sqrt{r^2 - d^2}/V_u ,$$  \hfill (10)

where $V_u$ is the velocity of the drone, and $t_{su}$ is the duration of the drone’s pass through the sweep region. The drone was located at half of the sweep region at $t = 0$. We assumed that $V_u$ is 100 Hz. This value is approximately 19 m/s, which is similar to the maximum speed of a typical drone. If the actual drone speed is slower than 100 Hz, it is easier to be deceived because it stays longer in the sweep region. In this study, the analysis is performed based on the maximum speed of the drone, which is the most difficult case for deception.

The propagation delay difference of the authentic signal $\Delta t'$ is a function of the satellite’s position, the center of the sweep region, and the drone trajectory. The satellite’s position should be expressed in three dimensions, but the worst case $\Delta t'$ occurs when the satellite is on the XZ-plane formed by the center of the sweep region and the drone’s trajectory. Therefore, considering only the elevation angle $\lambda$ of the satellite, $\Delta t'$ is expressed as follows in the measurement domain:
Because the satellite is far away from the ground, we assume that the line-of-sight vector of the satellite is constant.

The propagation delay difference of the defensive signal $\Delta t_j$ can also be analyzed in a similar manner. However, the defender is much closer than the satellite and $\Delta t_j$ is expressed differently. The term $\Delta t_j$ is a function of the defender’s position, the center of sweep region, and the drone’s trajectory. As the worst case of $\Delta t_j$, also occurs when the defender is on the XZ-plane, we consider only the latitude $\theta$ of the defender. In the measurement domain, $\Delta t_j$ is expressed as follows:

$$
\Delta t_j = c \Delta t' = c \left( t_{w} - t_{f} \right) \\
= \rho_{w} - \rho_{f} = \left[ R_{t} - R_{w} \right] - L \\
= \left( L \cos \theta + V_{t} t \right)^2 + \left( L \sin \theta - d \right)^2 - L ,
$$

(12)

where

$$
R_{t} = \left[ L \cos \theta \ 0 \ L \sin \theta \right]^{T} .
$$

The term $L$ is the distance between the center of the sweep region and the defender, which is an input parameter.

Combining (11) and (12), the time discrepancy in (7) can be expressed in the measurement domain as follows:

$$
y_{c,\Delta} (t) = c \sqrt{\Delta t} = c \left( \Delta t' - \Delta t_j \right) \\
= \left( V_{c} \cos \lambda \right) t - d \sin \lambda \\
- \sqrt{\left( L \cos \theta + V_{r} t \right)^2 + \left( L \sin \theta - d \right)^2} + L .
$$

(14)

The time offset $t_{sweep}$ for a sweeping authentic signal is defined as a simple linear function, as follows:

$$
y_{sweep} (t) = c \Delta t_{sweep} \\
= \begin{cases} 
  y_{sweep,1} &= V_{s} (t - t_{d}) + r \left( -t_{a} + t_{d} \leq t < t_{d} \right) \\
  y_{sweep,2} &= -V_{s} (t - t_{d}) + r \left( t_{d} \leq t < t_{d} + t_{a} \right), 
\end{cases}
$$

(15)

where

$$
t_{a} = 2r/V_{s} .
$$

(16)

The term $t_{a}$ is the duration to sweep the diameter of the sweep range, $V_{s}$ is the velocity of the time offset, and $t_{d}$ is the time delay of $y_{sweep}$. Because the entry time of the drone is fixed at $t = -0.5t_{w}$ in (9), the same effect as changing the drone’s entry timing can be obtained by adjusting $t_{d}$ . Equation (15) represents only one period of the time offset and $y_{sweep}$ oscillates at other times, as shown in Fig. 5(b).

In fact, $t_{sweep}$ in (15) is not valid because the frequency-locked loop (FLL) can lose a lock by the Doppler jump at the sharp point. Therefore, $t_{sweep}$ should be designed to always be differentiable when applied in practice. In this section, the $t_{sweep}$ in (15) is used for theoretical analysis. Section IV discusses the simulations we performed considering practical applications $t_{sweep}$.

The sweep velocity $V_{s}$ is also a design parameter for the defender. The faster $V_{s}$ is, the easier it is to find authentic signals. However, if $V_{s}$ is too fast, the FLL can lose a lock during the transition process. Therefore, we set appropriate $V_{s}$ to 245 Hz (= 46.6 m/s) that satisfies all the above conditions.

Fig. 5(b) shows an example of $y_{c,\Delta}$ and $y_{sweep}$. In this case, $y_{c,\Delta}$ and $y_{sweep}$ meet twice, while the drone passes through the sweep region. Therefore, we can conclude that the deception is successful if $y_{c,\Delta}$ and $y_{sweep}$ meet while the drone passes through the sweep region.

(2) WORST-CASE SCENARIOS

The number and position of intersections of $y_{c,\Delta}$ and $y_{sweep}$ change depending on $\lambda$, $\theta$, and $t_{d}$. We find that the worst case is always represented by one of the two cases in Fig. 6. The worst case occurs when two functions manage to have intersections. Depending on the environment, the worst case can be expressed as x-axis symmetry, y-axis symmetry, or translation, as shown in Fig. 6. However, the theoretical minimum sweep ranges are all the same, so we conducted an analysis of the situation shown in Fig. 6.

Fig. 6(a) shows the first worst-case candidate when $\lambda = 90^\circ$, $\theta = 90^\circ$ and $t_{d} = 0$ s . The function $y_{c,\Delta}$ tends to have a relatively gradual slope and meets $y_{sweep}$ at a sharp point $(t = 1.5t_{w})$. If the sweep radius $r$ is slightly smaller, then there will be no intersection point any more.
The functions are symmetric on the y-axis, the equation at \( t = t_m \)
expressed as follows:
\[
y_{\text{sweep}}(t_s; t_a = 0s) - y_{V_{\text{w}}}(t_s; \lambda = 90^\circ, \theta = -90^\circ) = 0. \tag{17}
\]
Equation (17) can be rearranged for sweep radius \( r \) as follows:
\[
r_s = \frac{(L - d) + \sqrt{(L - d)^2 + 4(1 - 4\alpha^2)Ld}}{1 - 4\alpha^2}, \tag{18}
\]
where
\[
\alpha = V_s / V_t. \tag{19}
\]
The subscript 1 in (18) means the first worst-case candidate.

Fig. 6(b) shows the second worst-case candidate. In the second case, the function \( y_{V_{\text{w}}} \) has a relatively steep slope and meets \( y_{\text{sweep}} \) lopsidedly. The intersections are located at the left sharp point \( t = -t_m + t_t \) (\( t_t \)) and the point at which the drone leaves the sweep region \( t = 0.5t_m \) (\( t_t \)). The equations at the intersections are as follows:
\[
F(\tilde{r}_2, \tilde{r}_t) \bigg|_{1,2} = \begin{bmatrix}
y_{\text{sweep}}(t_1; \tilde{t}_s) - y_{V_{\text{w}}}(t_1; \tilde{\lambda}, \tilde{\theta})
y_{\text{sweep}}(t_2; t_t) - y_{V_{\text{w}}}(t_2; \tilde{\lambda}, \tilde{\theta})
\end{bmatrix} = \begin{bmatrix}
0 \\
0
\end{bmatrix}. \tag{20}
\]
Equation (20) represents the two nonlinear equations for the specific elevation angle of the satellite and the latitude of the defender, expressed as \( \tilde{\lambda} \) and \( \tilde{\theta} \), respectively. This equation cannot be simply rearranged like (18). Instead, a numerical nonlinear solver can be used to determine \( \tilde{r}_2 \) and \( t_t \) to satisfy (20). From the values of \( \tilde{r}_2 \) computed from all the possible \( \lambda \) and \( \theta \) combinations, the maximum \( \tilde{r}_2 \) becomes the second worst-case candidate \( r_2 \). Fig. 7 shows the computed \( \tilde{r}_2 \) when \( L = 2000 \) m. Among the various possible \( \tilde{\lambda} \) and \( \tilde{\theta} \) combinations, when \( \tilde{\lambda} = 72 \) deg and \( \tilde{\theta} = -108 \) deg, \( \tilde{r}_2 \) has a maximum value of 3071 m. This value becomes the final minimum sweep range of the second worst-case candidate.
\[
r_2 = \max_{\lambda, \theta \in (-\pi, 0)} \tilde{r}_2 \tag{21}
\]

Next, we compare the two worst-case candidates, \( r_1 \) and \( r_2 \).

The greater candidate is the final worst case, which is the minimum sweep range.

Putting it concisely, the process for determining the sweep range of the defender is as follows:

**Step 1:** Set \( d \) and \( L \).

**Step 2:** Calculate the two worst case candidates \( r_1 \) and \( r_2 \).

**Step 3:** Determine minimum sweep range \( r = \max(r_1, r_2) \).

Fig. 8 shows the two worst-case candidates based on \( L \) when \( d = 1000 \) m. When \( L \) is closer to 700 m, \( r \) is determined by the first worst-case candidates. For example, if \( L \) is zero, the minimum sweep range is 5995 m, computed by the first worst-case candidate. When \( L \) is farther from 700 m, \( r \) is determined by the second-worst-case candidates. For example, if \( L \) is 2000 m, the minimum sweep range is 3071 m, computed by the second worst-case candidate. As the defender is farther away from the center of the sweep region, the sweep radius of the defender for a successful defense decreases. This is because the propagation delay difference of the defensive signals decreases as the defender becomes farther away.

### IV. SIMULATION RESULTS

**A. SIMULATION OF ALL POSSIBLE CASES**

In this simulation, we verified that the minimum sweep range \( r \) obtained from the worst-case analysis in Section III can unconditionally protect the protection area with a radius \( d \). In addition, we confirmed that the first failure case of the defense occurs in the worst-case scenario expected in Section III.

The setting values for the simulation are shown in Table 1. We performed the simulation with the values of \( L \) at zero and 2000 m. These two cases determine the sweep range \( r \) for different worst-case candidates. The drone enters the sweep

![FIGURE. 8. Minimum sweep range (r) of the two worst-case candidates based on L when d=1000 m.](image-url)
region in the $(1,0,0)$ directions, and we adjusted the distance between the drone trajectory and the center of the sweep region, $d_u$. For each $d_u$, we performed simulations at all the possible entry times of the drone, satellite's position, and defender's position, as shown in Table 2. The entry time $t_{dy}$ was the same as the time delay between $y_{\text{sweep}}$ and $y_{\text{VM}}$. We assumed that the elevation and azimuth angle of the satellite are constant while the drone is passing through the sweep region. Moreover, the deception is considered successful if $y_{\text{VM}}$ and $y_{\text{sweep}}$ meet, while the drone is passing through the sweep region.

**TABLE 1. Simulation setting values**

| $V_s$ [Hz] | $V_d$ [Hz] | Direction of drone | $d_u$ [m] | $L$ [m] | $r$ [m] |
|------------|------------|--------------------|-----------|---------|---------|
| 245        | 100        | $(1, 0, 0)$        | 1000      | 0       | 5995    |
|            |            |                    | 2000      |         | 3071    |

Simulation results show that the deception always succeeds until $d_u$ is 1000 m, and failure occurs when $d_u$ is greater than 1000 m. Fig. 9 and 10 show the case in which the deception fails for the first and second worst-case candidates, respectively. At first glance, the two functions seem to meet, but they do not actually meet due to a slight difference.

**FIGURE 9.** First deception failure case when $L = 0$ m and $r = 5995$ m at $d_u = 1001$ m and $\lambda = 90$ deg (the first worst case candidate): (a) geometry description, (b) time discrepancy and time offset of the defender in the time domain. At first glance, the two functions seem to meet, but they do not actually meet due to a slight difference.

**FIGURE 10.** First deception failure case when $L = 2000$ m and $r = 3071$ m at $d_u = 1001$ m, $\lambda = 72$ deg and $\theta = -108$ deg (the second worst-case candidate): (a) geometry description, (b) time discrepancy and time offset of the defender in the time domain. At first glance, the two functions seem to meet, but they do not actually meet due to a slight difference.
II. SDR SIMULATION RESULTS

In this section, we report the simulation of a specific wide area protection scenario. For the simulation, we utilized a MATLAB-based intermediate frequency (IF) signal generator and a MATLAB-based post-processing software GNSS receiver called SDR.

The IF signal generator generates the authentic and defensive signals to be received by the drone. First, the IF signal generator loads the broadcast ephemeris information corresponding to the input coordinate universal time (UTC). Second, using the satellite’s position and the entered trajectory of the drone, an authentic analog signal is generated without considering other error sources. Similarly, the analog defensive signal received by the drone can be generated by considering the propagation delay to the drone in (5) and the total time delay of the defender in (7). The defensive signal strength was set to +2 dB greater than the authentic signal. Third, analog signals from each satellite and defender were added, and digitization was performed to generate the IF data.

The SDR is equivalent to the GPS receiver of the drone, and it employs the IF data as the input. The signal acquisition, tracking, and navigation calculations were performed sequentially. It was assumed that the pre-integration time of the drone is 1 ms. The signal tracking loop was based on a conventional loop filter, and the least square-based navigation filter was adopted.

Additionally, we considered the conditions for maintaining the FLL lock. The Doppler jump inevitably occurs when the tracking lock changes from the authentic to defensive signals. Therefore, it is necessary to set the appropriate sweep speed not too fast so that the FLL can maintain the lock. Moreover, the time offset design as in (15) can cause a Doppler jump at the sharp point. This problem can be prevented by modeling the vicinity of the sharp point as a quadratic function. Considering the above two factors, the average \( V_s \) was set to 245 Hz. This change in the time offset design affects the theoretical minimum sweep range in Section III, but it is a more conservative design. Therefore, there is no problem in using the average \( V_s \) to determine the minimum sweep range.

The deception is considered successful when the signal tracking lock changes from the authentic to the defensive signals in all the visible satellites. The estimated position should also be shifted from the original trajectory to the center of the sweep region into the defensive signals. During this process, the DLL and FLL should be retained.

We performed simulations for various distances from the center of the sweep region to the trajectory \( d_s \), entry time \( t_d \), and entry angle \( \alpha \), and the settings and results are summarized in Table 3. The drone enters the sweep region at \( t = t_d \) and passes through the sweep region during \( t_m \).

![Image](Image3)

**TABLE 2. Variables and search range of simulation**

| Variables                          | Range          |
|------------------------------------|----------------|
| \( d_s \), the distance between the center of sweep region and the trajectory of drone | 990 : 1 : 1010 m |
| \( t_d \), entry time when the drone enters the sweep region | 0 : 0.1 : \( t_m \) s |
| \( \lambda \) and \( \phi \), the elevation and azimuth angle of satellite | 0 : 3 : 90 deg |
| \( \theta \) and \( \psi \), the latitude and longitude of the defender | 0 : 3 : 360 deg |

**TABLE 3. Simulation settings and results depending on the scenarios.**

| Scenario | \( d_s \) [m] | \( t_d \) [s] | \( \alpha \) [deg] | \( t_m \) [s] | Results     |
|----------|--------------|--------------|-----------------|--------------|-------------|
| 1        | 0            | 4            | -22.6           | 283.8        | Success     |
| 2        | 1000         | 4            | -22.6           | 263.6        | Success     |
| 3        | 1250         | 4            | -22.6           | 251.5        | Success     |
| 4        | 1250         | 4            | 40              | 251.5        | Success     |
| 5        | 1250         | 90           | 40              | 251.5        | Success     |
| 6        | 1250         | 118          | 40              | 251.5        | Failure     |

We discussed scenario 4 in more detail below.
Fig. 13 and 14 show the navigation solutions in scenario 4. We can confirm that the estimated position and velocity are converted from the original position to the intended position and velocity by the defender. In Fig. 13(d) and 14(d), the clock bias and drift are estimated differently from the intended clock bias and drift by the defender. This is because the delay of the
defensive signals is adjusted based on the center of the sweep region, but the actual drone’s position is located at a different point. The drone receives the delayed or advanced defensive signals by the position difference, and the position difference is also reflected in the pseudorange and Doppler estimation results. The authentic pseudorange of the $i$-th satellite $\rho^i_s$, the intended pseudorange by the defender $\rho^i_f$, and the theoretically estimated pseudorange $\hat{\rho}^i_{\text{theo}}$ are expressed as follows:

$$\rho^i_s = \| R^i_s - R_u \| + B = d^i_{s} + B,$$

$$\rho^i_f = \| R^i_f - R_u \| + B + B_{\text{sweep}} = d^i_{s} + B + B_{\text{sweep}},$$

$$\hat{\rho}^i_{\text{theo}} = \begin{cases} \rho^i_f, & \text{before deception} \\ \rho^i_f + (d_{fu} - d_{fc}), & \text{after deception} \end{cases} \quad (23)$$

An additional clock bias term $d_{fu} - d_{fc}$, which is not intended by the defender, occurs in common to all the visible satellites, and the additional clock drift occurs in the same manner. However, because the same magnitude of clock bias and drift is added to all the satellites, the position and velocity estimation results are not affected.

Fig. 15(a) shows the time discrepancy of all the satellites $\gamma_{vy}$ and the time offset of the defender $y_{\text{sweep}}$ in scenario 4. It is shown only from 4 s to 257 s in which the drone passes through the sweep region. If the two functions intersect during this period, deception is considered successful. In the pseudorandom noise (PRN) 9, the earliest case, $\gamma_{vy}$ and $y_{\text{sweep}}$ meet at $t = 7$ s. In PRN 8, the latest case, $\gamma_{vy}$ and $y_{\text{sweep}}$ meet at $t = 166$ s. During the transition of approximately 160 s, the receiver tracks the authentic signals in some satellites.
and the defensive signals in the other satellites. Therefore, it can deviate significantly from an unintended point when calculating the navigation solution. In particular, the point where the velocity jumps in Fig. 14 is because one satellite is deceived additionally, and the navigation solution is calculated at different points.

The difference in the deception timing can also be seen in Fig. 15(b), which shows the pseudorange difference between the estimated pseudorange in the drone and the theoretical pseudorange after the deception in (24). When the difference becomes zero, the deception has been successfully performed. All the satellite signals succeed in deception, and the timing at which the tracking lock is changed to a defensive signal is widely distributed.

As shown in Fig. 12(a), the position error during the transition process in scenario 3 is not as large as that in scenario 4, because all the tracking channels have similar deception timing. In essence, depending on the conditions of the scenario, the position error during the transition process has different levels. This is a limitation of the proposed deception algorithm, which should deceive the drone in situations where the position of the drone is unknown.

In addition, we can see that the authentic and defensive signals intersect again from 180 s to 220 s in Fig. 15(a). At this time, the drone is already tracking the defensive signals, so the authentic signals have an effect similar to a multipath error. However, because the defensive signal power is stronger, the tracking lock does not change back to the authentic signals. Only the signal tracking performance is affected, and large position and velocity errors due to re-intersections can be seen between 180 s and 220 s in Fig. 13 and 14.

Scenario 5 adjusts only the entry time of the drone compared to scenario 4. Fig. 16(a) shows $y_{\text{cn}}$ and $y_{\text{sweep}}$ in scenario 5. The functions $y_{\text{cn}}$ of PRNs 16 and 26 no longer intersect $y_{\text{sweep}}$ at approximately t = 170 s. Nevertheless, Fig. 16(b) shows that the signal tracking of PRNs 16 and 26 is changed to defensive signals at approximately t = 170 s. This is because the minimum difference between $y_{\text{cn}}$ and $y_{\text{sweep}}$ is 150 m in PRN 26, which is within one chip. If the ACF of the defensive signal exists within one chip of the ACF of the authentic signal, the tracking lock moves to the defensive signal with a stronger signal power. Therefore, the deception can be successful even if the two functions do not meet; the theoretical analysis in Section 3 is a conservative deception condition.

Fig. 17 shows the results of scenario 6 when the difference between the two functions becomes more than one chip (385 m in PRN 16) at approximately t = 170 s by delaying the entry time of the drone. In this case, the deception fails at approximately t = 170 s for PRNs 16 and 26. Eventually, PRN 16 is not deceived to the end because the two functions do not meet until the drone is out of the sweep region.

Scenarios 1 to 5 take 127, 136, 138, 162, and 170 s to deceive the drone after the drone enters the sweep region, respectively. The duration required for deception significantly depends on the entry timing of the drone. It is clear that the deception succeeds unconditionally before the drone leaves the sweep region.

Through the wide area protection simulations, it has been confirmed that it is possible to deceive multiple drones using the fixed defensive signals generated by a single signal generator. With the currently designed sweep range of 2700 m, the deception is successful even in some scenarios approaching $d_s=1250m$. The success or failure of the deception depends on the satellite's position, defender's position, entry timing, and entry angle of the drone. The deception is possible in a broader region than in the theoretical analysis in Section 3. This is a conservative design, so there is no problem in defending major facilities.

V. CONCLUSION

This study proposed a wide area protection algorithm using a GNSS signal generator against numerous unintentional drones. The signal generator, referred to as the defender, generates defensive signals to sweep authentic signals on the ACFs. This defense method using signal sweeping is the most effective way to lead drones to a safe zone without being noticed. We proposed a sweep algorithm in the measurement domain that adjusts the time offset of the defender. The sweep in the measurement domain can sweep a wider area than the traditional sweep method in the position domain. In addition, the proposed protection method can deceive multiple drones simultaneously without the drones' trajectory information. As a fundamental study to determine the possibility of wide area protection based on the sweep algorithm, the minimum sweep range of the defender was examined to unconditionally deceive the drone approaching a sphere with a radius of 1 km.

To calculate the minimum sweep range, we first analyzed the time discrepancy between the authentic and defensive signals. Next, we examined two worst-case candidates and determined the larger of the two as the minimum sweep range. When the defender is located at 0 and 2000 m away from the center of the deception, the minimum sweep ranges of the defender are 5995 and 3071 m, respectively.

The simulation results showed that the theoretical analysis is valid, and the first failure case occurred in the expected worst-case candidate. Simulation using SDR was also conducted as an example of a wide area protection problem. When the defender was 7800 m away from the center of the sweep region, various scenarios were tested for fixed defensive signals. We confirmed that wide area deception is possible with the analyzed sweep range, and the defender can deceive multiple drones simultaneously.

However, further studies on the signal power requirements of the defender are required. If the defensive signal power is too large in the sweep region, it may be influenced by jamming. Conversely, if the defensive signal power is smaller than the authentic signal, the deception will fail. Therefore, the defender should broadcast the defensive signals with an appropriate transmission power considering the distance to the center of the sweep region. In addition, studies on how to guide the deceived drones to a safe zone

VOLUME XX, 2017 9
should be conducted in the future for a complete wide area protection. The trajectory indicated by the defender should be designed to guide the drones to the safe zone.

ACKNOWLEDGMENT

This research was supported in part by the Institute of Advanced Aerospace Technology at Seoul National University. The Institute of Engineering Research at Seoul National University provided research facilities for this work.

REFERENCES

[1] “Japan radioactive drone: Tokyo police arrest man,” BBC News, Apr. 25, 2015. [Online] Available: https://www.bbc.com/news/world-asia-32465624

[2] “Venezuela President Maduro survives ‘drone assassination attempt’,” BBC News, Aug. 5, 2018. [Online] Available: https://www.bbc.com/news/world-latin-america-45073385

[3] H. Hu and N. Wei, “A study of GPS jamming and anti-jamming,” in Proc. 2nd Int. Conf. Power Electron. Intell. Transp. Syst. (PEITS), vol. 1, Dec. 2009, pp. 388–391.

[4] D. Marnach, S. Mauw, M. Martins, and C. Harpes, “Detecting meaconing attacks by analysing the clock bias of GNSS receivers,” Artif. Satell., vol. 48, no. 2, pp. 63–83, Jan. 2013.

[5] Ng Yuting, Gao, and G. Xingxin, “Mitigating jamming and meaconing attacks using direct GPS positioning,” Proc. IEEE/JON PLANs 2016, Savannah, GA, April 2016, pp. 1021–1026.

[6] F. Wang, H. Li, and M. Lu, “GNSS spoofing countermeasure with a single rotating antenna,” IEEE Access, vol. 5, pp. 8039–8047, 2017.

[7] M. L. Psiaki and T. E. Humphreys, “GNSS spoofing and detection,” Proc. IEEE, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[8] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, “Unmanned aircraft capture and control via GPS spoofing,” J. Field Robot., vol. 31, no. 4, pp. 617–636, 2014.

[9] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, “Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks”, Proc. ION GNSS Meeting, pp. 1–15, 2012.

[10] J. Bhatti and T. E. Humphreys, “Hostile control of ships via counterfeited GPS signals: Demonstration and detection,” Navigation, J. Inst. Navig., vol. 64, no. 1, pp. 51–66, Mar. 2017.

[11] L. Perdue, H. Sasaki, and J. Fischer, “Testing GNSS receivers to harden against spoofing attacks,” in Proc. Int. Symp. GNSS 2015, Kyoto, Japan, 16–19, Nov. 2015.

[12] B. Shin, M. Park, S. Jeon, H. So, G. Kim, and C. Kee, “Spoofing attack results determination in code domain using a spoofing process equation,” Sensors, vol. 19, no. 2, pp. 293, Jan. 2019.

[13] Q. Meng, L.-T. Hsu, B. Xu, X. Luo, and A. El-Mowafy, “A GPS spoofing generator using an open sourced vector tracking-based receiver,” Sensors, vol. 19, no. 18, p. 3993, Sep. 2019.

[14] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, “On the requirements for successful GPS spoofing attacks,” in Proc. 18th ACM Conf. Comput. Commun. Security (CCS’11), New York, pp.75–86. Oct. 2011.

[15] L. Junzhi, L. Wanqing, F. Qixiang, and L. Beidian, “Research progress of GNSS spoofing and spoofing detection technology,” Proc. IEEE Int. Conf. Commun. Technol., pp. 1360–1369, Oct. 2019.

[16] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapel, “GPS vulnerability to spoofing threats and a review of antispooﬁng techniques,” Int. J. Navig. Observ., vol. 2012, May 2012, Art. no. 127072.

[17] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, “A survey and analysis of the GNSS spoofing threat and countermeasures,” ACM Comput. Surveys, vol. 48, no. 4, pp. 1–31, May 2016.

[18] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapel, “GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables,” Int. J. Satell. Commun. Netw., vol. 30, no. 4, pp. 181–191, Jul. 2012.

[19] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, “GNSS signal authentication via power and distortion monitoring,” IEEE Trans. Aerosp. Electron. Syst., no. 99, pp. 1–1.

[20] J. N. Gross, C. Kilic, and T. E. Humphreys, “Maximum-likelihood power-distortion monitoring for GNSS-signal authentication,” IEEE Trans. Aerosp. Electron. Syst., vol. 55, no. 1, pp. 469–475, Feb. 2019.

[21] C. Tanil, S. Khanafsh, M. Joerger, and B. Pervan, “An INS monitor to detect GNSS spoofers capable of tracking vehicle position,” IEEE Trans. Aerosp. Electron. Syst., vol. 54, no. 1, pp. 131–143, Feb. 2018.

[22] C. Tanil, S. Khanafsh, and B. Pervan, “GNSS spoofing attack detection using aircraft autopilot response to deceptive trajectory,” in Proc. IONGNSS+, Tampa, FL, USA, 2015, pp. 3345–3357.

[23] J.-H. Lee, K.-C. Kwon, D.-S. An, and D.-S. Shim, “GPS spoofing detection using accelerometers and performance analysis with probability of detection,” Int. J. Control Auton. Syst., vol. 13, no. 4, pp. 951–959, 2015.

[24] D.M.Akos, “Who’s afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC),” Navigation, vol. 59, no. 4, pp. 281–290, Winter 2012.

[25] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller “An in-line anti-spoofing module for legacy civil GPS receivers,” in Proc. 2010 Int. Tech. Meeting Inst. Navig., San Diego, CA, Jan. 2010.

[26] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, “Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer,” in Proc. ION Int. Tech. Meeting, Anaheim, CA, Jan. 2009, pp. 124–130.

[27] M. L. Psiaki, B. W. O’Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, and T. E. Humphreys, “GNSS spoofing detection using two-antenna differential carrier phase,” in Proc. 27th Meeting Satell. Div. Inst. Navig., 2014, pp. 2776–2800.

[28] D. Marnach, S. Mauw, M. Martins, and C. Harpes, “Detecting meaconing attacks by analysing the clock bias of GNSS receivers,” Artif. Satell., vol. 48, no. 2, pp. 63–83, Jan. 2013.

[29] A. Jafarnia-Jahromi, S. Daneshmand, A. Broumandan, J. Nielsen, and G. Lachapel, “PVT solution authentication based on monitoring the clock state for a moving GNSS receiver”, Proc. Eur. Navigat. Conf. (ENC), pp. 1–11, 2013.

[30] K. Zhang, M. Spanghero, and P. Papadimitratos, “Protecting GNSS-based services using time offset validation.” 2020 IEEE/JON Position, Location and Navigation Symposium (PLANS), IEEE, 2020.

[31] Z. Chen, H. Li, J. Wen, and M. Lu, “Moving receiver PVT solution authentication based on monitoring the combination of clock bias and drift.” in Proc. 2020 Int. Tech. Meeting Inst. Navi. San Diego, CA, Jan. 2020.

[32] “Sinister spoofing in Shanghai”, InsideGNSS, Dec. 10, 2019. [Online]. Available: https://insidegnss.com/sinister

[33] M. Jones, “Spoofing in the Black Sea: What really happened?,” GPS World, Oct. 11, 2017. [Online]. Available: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/
MINHUCK PARK received the B.S and M.S. degrees in the School of Mechanical and Aerospace Engineering from Seoul National University, Seoul, South Korea, in 2015 and 2017, respectively, where he is currently pursuing the Ph.D. degree in the School of Mechanical and Aerospace Engineering. His research interests include GNSS receivers, spoofing and GPS/INS integrated navigation systems.

BEOMJU SHIN received the B.S. and M.S. degrees in Information and Communication Engineering from Sejong University, Seoul, South Korea, in 2010 and 2012, respectively, and the Ph.D. degree in the School of Mechanical and Aerospace Engineering from the School of Mechanical and Aerospace Engineering, Seoul National University, Seoul, South Korea, in 2020. Since 2020, he has been working with the Korea Institute of Science and Technology as a Post-Doctoral Researcher. His current research interests include pattern recognition, machine learning, and indoor navigation systems.

JIN-HEE Han received the B.S., M.S., and Ph.D. degree in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejon, South Korea, in 1991, 1993, and 1999, respectively. He is working at Danam Systems Corp. Ltd. as Head of GNSS R&D center. His company develops and produces GNSS chips/receivers and GNSS-related products for commercial and military uses.

HAK-DU Kim received the B.S. and M.S. degree in Computer Science and Statistics from University of Seoul, Seoul, South Korea, in 2001 and 2003, respectively. He is currently a senior researcher at Danam System Inc. He has been developing GNSS receivers for commercial and military use since 2008. His research interests include the development of high-precision receivers for use in high-speed environments.

CHANGDON KEE is a Professor in the School of Mechanical and Aerospace Engineering at Seoul National University (SNU), South Korea and supervises SNU GNSS Lab (SNUGL, http://gnss.snu.ac.kr). He received the B.S. and M.S. degrees in Aeronautics Engineering from Seoul National University, Seoul, South Korea, in 1984 and 1986, respectively, and a Ph.D. degree in Aeronautics and Astronautics from Stanford University, CA, USA, in 1994. He served as a Technical Advisor to the Federal Aviation Administration (FAA) on the Wide Area Augmentation System (WAAS) in 1994. Prof. Kee currently serves as a Technical Advisor for Korea Civil Aviation Safety Authority (KCASA) and Ministry of Public Administration and Security (MOPAS). He also served as a President of Korean Institute of Navigation. He has more than 20 years of GNSS and flight control research experiences.