Trans. Japan Soc. Aero. Space Sci.
Vol. 60, No. 5, pp. 312–319, 2017

Performance Analysis of a COTS GPS Receiver against Spoofing Attack and Spoofing Detection Method using RAIM and a Single Authentic Signal*

Hyoungmin SO,† Jaegyu JANG, Kihoon LEE, and Junpyo PARK

Agency for Defense Development, Daejeon 34186, Republic of Korea

This study investigated the anti-spoofing capability of a Commercial-Off-The-Shelf (COTS) Global Positioning System (GPS) receiver and proposes a spoofing detection method with minimum user complexity. A spoofing test environment with a GPS simulator was developed to test a conventional GPS receiver with an in-line radio frequency (RF) signal. The tests on a geodetic-grade receiver revealed a vulnerability in the COTS GPS receiver against spoofing attacks. Receiver Autonomous Integrity Monitoring (RAIM) was not capable of handling a spoofing attack sufficiently, but could manage a low-level attack. Thus, a spoofing detection method based on the simulation results is proposed as a feasibility check.

Key Words: Spoofing Detection, Anti-spoofing, RAIM, GNSS Interference, GNSS

Nomenclature

y: pseudo-range measurement
$\underline{x}$: user state vector (3-D position and time)
$\underline{w}$: residual between pseudo-range measurement and estimated one
$\underline{\varepsilon}$: measurement error vector
H: matrix whose elements are three columns of direction cosine and value 1 as a fourth column
SSE: square sum of residuals
D: test statistics for spoofing detection
T_D: threshold for spoofing detection

1. Introduction

Recently, global navigation satellite systems (GNSSs) are widely used for various applications. Thus, there is a growing reliance on the location information from GNSSs. As applications become more dependent on GNSSs, the vulnerability of GNSSs against intentional interference, such as jamming and spoofing, is becoming a plausible threat to GNSS users. Intentional interference can be categorized into jamming and spoofing. GNSS jamming is when a high-power signal is transmitted on the same GNSS frequency, blocking GNSS users from receiving the genuine signal from GNSS satellites.[1] GNSS spoofing is when a GNSS-like signal is generated to deceive the user into tracking a fake signal, and consequently, the user is led to the wrong location.[2]

In the jamming situation, the user can recognize abnormal conditions because the GNSS signal is not available, and can therefore handle the situation. However, in a spoofing incident, the user's receiver is not aware that it is tracking a fake signal and being led to the wrong location. This is why spoofing attacks present a greater risk of danger to users.

After the incident of Iran hijacking a US drone in 2011, there has been growing concern about the vulnerability of GPS receivers against spoofing attacks even though it is not clear whether the hijacking incident in 2011 was the result of a spoofing attack.[3] After that incident, Humphreys, of the University of Texas, conducted a field test showing that a drone can be successfully spoofed by causing the drone to lower its altitude from a hovering position.[4] Additionally, in another spoofing experiment on a ship, the course of the ship was altered by a spoofing attack, which Humphreys said was easy to accomplish. These were the first open test results showing that spoofing attacks are a real threat to GNSS users.

According to the Volpe Report, anti-spoofing technologies are categorized into the receiver autonomous integrity monitoring (RAIM), baseband signal processing, checking consistency with an inertial measurement unit (IMU), using an array antenna, and cryptography authentication.[5] RAIM and baseband processing techniques are good in view of their low complexity when being implemented on a user's receiver. However, their spoofing detection capability is not sufficient when it comes to detecting well-designed spoofing attacks. Checking consistency using other sensors is good only when a trustworthy navigation system is available. The drawback of using an IMU is that the IMU uses GPS as a reference to compensate for drift. Since the GPS is being spoofed without detection, the IMU tracks the spoofed position data and does not alarm the user. The victim receiver used in Humphreys' outdoor test was equipped with an IMU and successfully spoofed.[4] It is known that array antenna and cryptography authentication approaches are currently applicable techniques with good performance.

In Jafarnia-Jahromi et al.,[6] spoofing detection techniques are listed by implementation complexity, effectiveness, required receiver capabilities and spoofing scenario generality. Among the available technologies, cryptographic authentication is the most effective. Its user complexity is very low. The

*Received 16 August 2016; final revision received 17 May 2017; accepted for publication 30 May 2017.
†Corresponding author, hyoungmin.so@gmail.com

problem is that the only available encrypted signal at this moment is the GPS P(Y) code. Thus, civilian users cannot take advantage of it. There have been many studies on estimating the direction of the arrival of the signal using an array antenna.[7] This method performs well; however, it requires equipping the user receiver with an array antenna, which causes an increase in the cost, size and weight. Thus, the spoofing detection methods currently available that can be incorporated into GNSS receivers used in a variety of applications are RAIM and other baseband signal processing approaches. However, RAIM is not designed for spoofing detection and other baseband techniques are vulnerable to high-level spoofing attack. Therefore, the aim of this study was to propose and design a high-performance RAIM-based spoofing detection method that utilizes cryptographic authentication. Developing a test and evaluation method that generates RF spoofing signals using a GPS simulator is also addressed.

First, a low user-complexity spoofing detection scheme based on RAIM is proposed. This scheme uses an additional ranging signal from a pseudolite, eLoran or geosynchronous satellite to provide a single authentic signal to a user. This contributes to improving the performance of RAIM by taking advantage of the additional ranging signal to detect spoofing attacks. The scheme proposed requires an additional transmitter but can be used by many user receivers without any hardware modifications on the user side even for currently used GNSS receivers. Lo et al.[8] and Humphreys et al.[9] proposed the idea of RAIM-based spoofing detection similar to ours. They mentioned the feasibility of RAIM-based spoofing detection using signals of opportunity such as eLoran, multiple GNSS, communication signals and Iridium. However, they didn't discuss how to design and implement the algorithm and its performance. Therefore, the contribution of this paper is to address the design of the spoofing detection algorithm with simulated implementation and analysis of the test results.

The algorithm and its implementation have been tested. For the test, we developed a spoofing test environment with GPS RF simulators.[10] For comparison, the anti-spoofing performance of GPS receivers currently used with conventional RAIM were examined. Whereas there have been many studies on the response characteristics of the acquisition and tracking functions of GNSS receivers against spoofing attacks in the correlation function domain, this paper concentrates on only the RAIM function against spoofing attack.

The remainder of the paper is organized as follows. Section 2 presents the spoofing test setup for generating a RF spoofing signal using a GPS simulator. In Section 3, the analysis results of using a COTS GPS receiver for a spoofing test are presented. Section 4 briefly reviews the conventional RAIM algorithm used to develop the spoofing detection scheme. Section 5 describes the spoofing detection algorithm proposed by the authors, which is followed by the simulation test results in Section 6. The conclusions of this study are given in Section 7.

2. Spoofing Test Environment using GPS RF Simulators

To test and evaluate a COTS GPS receiver, the spoofing signal should be generated as a radio frequency and fed into the receiver with a genuine GPS signal. However, transmitting the spoofing signal into an open space could cause severe problems for GPS users. For example, GPS receivers near the transmitter could malfunction by being jammed or spoofed by the signal. Thus, instead of transmitting the signal, in-line input to the GPS receiver was carried out using two GPS simulator modules. Each simulator module generated a simulated genuine GPS signal and spoofing signal, respectively. Two Spirent GSS 8000 modules were used. They were synchronized and controlled by the same SimGen software; meaning that they generated signals under the same scenario. Each output was combined and fed into the target GPS receiver. Figure 1 shows the hardware configuration for the test. Additionally, a software GPS receiver was used to check the feasibility of the spoofing test environment generated.

Each GPS simulator module in Fig. 1 generates GPS signals for a certain user. We set the first simulator to generate GPS signals for a static user. Additionally, we chose this as the true GPS signal. We set the second simulator to generate the GPS signals for a moving user passing by the position of the static user of the first simulator. These two simulator outputs are combined to be fed into the GPS receiver. Next, when the second user passes by the position of the first user in the simulations, the combined signal can simulate the sweeping process shown in Fig. 2(b).

The GPS simulator does not provide a spoofing scenario by itself. Using the hardware setup in Fig. 1, we need to control each simulator module to make a spoofing environment that can make the receiver track a spoofing signal instead of a genuine signal without discontinuity. Figure 2(a) is the conceptual view of the scenario for the spoofing test. Using the same SimGen software, two GPS users are simulated. Module 1 is for the genuine GPS signal. The user of module 1 is stationary. Module 2 is for the spoofing signal. The user of the module 2 moves from west to east passing by the position of the stationary user of module 1. Thus, we expect that the spoofing signal sweeps the simulated genuine signal shown in Fig. 2(b). This scenario can simulate the well-known spoofing procedure; namely, matching the real code, capturing the user's reception and taking over directional control, which are described in Shepard and Humphreys.[11]

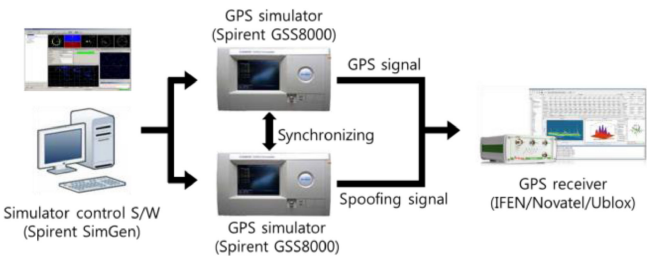
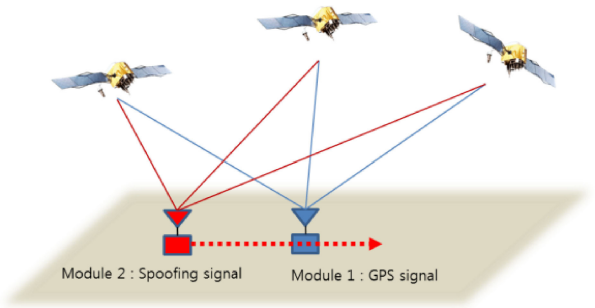
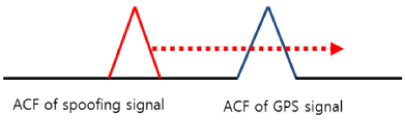


Fig. 1. Conceptual diagram of the GPS spoofing test setup.



(a) Conceptual view of SimGen scenario for 2 modules for spoofing test



(b) Conceptual view of autocorrelation functions for a certain channel

Fig. 2. Conceptual view of the scenarios of each GPS simulator for the spoofing test using two GPS simulator modules: (a) Design of the SimGen scenario to simulate the GPS spoofing environment; module 1 is assumed to be the genuine GPS source generating GPS signals for a static user, and module 2 is assumed to be the spoofing signal source generating GPS signals for the moving user passing by the position of the static user of module 1; (b) Auto-Correlation Function (ACF) characteristics of the user receiver for the spoofing scenario.

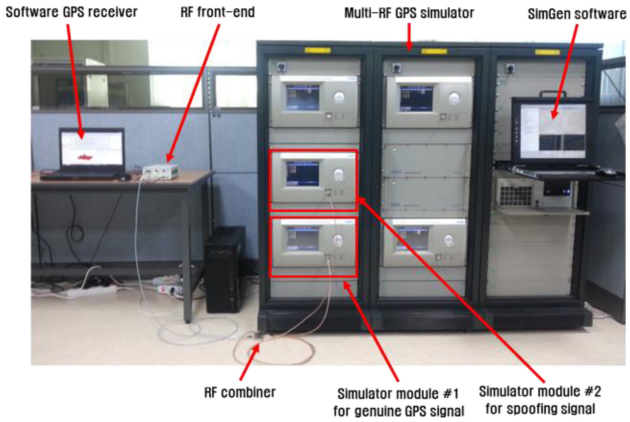


Fig. 3. Test setup for the GPS spoofing test using multiple-RF GPS simulators.

Figure 3 is a picture of the multiple-RF GPS simulators and the test configuration with the IFEN GPS software receiver.[12,13] The multiple RF GPS simulators shown on the right side of Fig. 3 contain five GSS 8000 modules. This equipment can simultaneously control five GPS simulator modules using a single SimGen software application. As explained, we need just two GPS simulator modules to generate genuine GPS signals and spoofing signals. Thus, among the five modules, we used just two of them (i.e., the two boxes indicated by simulator module #1 and simulator module #2, respectively in Fig. 3). Then, using the RF combiner, each RF signal is combined to be fed to the software GPS receiver shown in Figs. 1 and 2.

Figure 4 is the screenshot of IFEN software GPS receiver operation showing the response of the receiver. Using the software receiver, the tracking status can be monitored by displaying the auto-correlation function to see if the spoofing

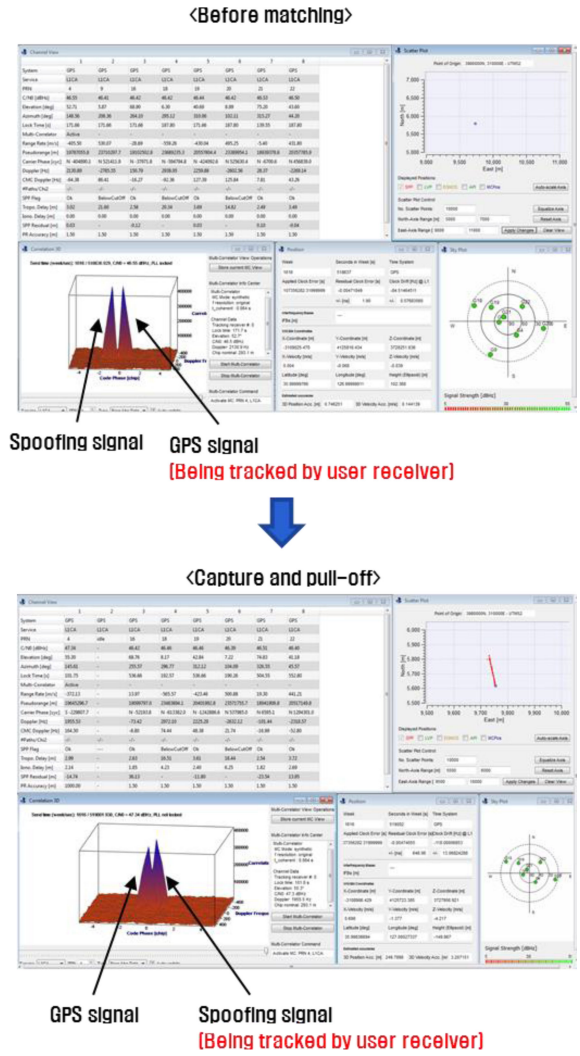
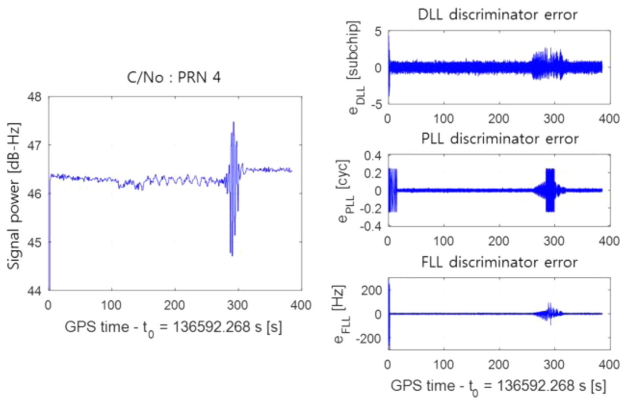


Fig. 4. Monitoring results of the GPS spoofing test using multiple-RF GPS simulators and a software GPS receiver.

procedure—matching, capturing and taking over—is generated, and the user tracking loop is fooled successfully. There are two autocorrelation functions before the matching stage. One is a genuine GPS signal, and the other is a spoofing signal. Because the spoofing signal is far from the genuine signal, there is no influence on the receiver tracking loop and navigation results. When the spoofing signal is getting closer to the genuine signal, the capture process starts. We set the signal power of the spoofing signal to 1 dB higher than that of the genuine signal. Thus, when the spoofing signal passes by the genuine signal, the receiver's tracking function locks onto the fake signal, as shown in Fig. 4 (bottom). As each channel starts to track the fake signal, the positioning solution moves away from the stationary point. This result shows that the spoofing test environment developed works successfully, and it can be used to test COTS GPS receivers.

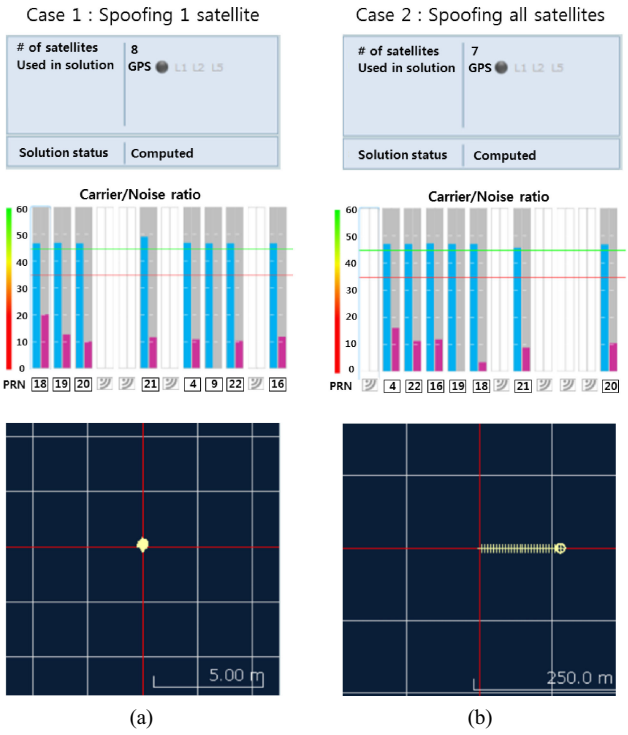
3. Response Characteristics of a COTS GPS Receiver Subjected to a Spoofing Attack

In this section, the analyzation of the anti-spoofing performance of a COTS GPS receiver by monitoring the track-



(a) (b)

Fig. 5. Response characteristics of the tracking channel against a spoofing attack: (a) C/No variation during the spoofing procedure, and (b) variation of the tracking loop errors for the DLL (top), PLL (middle) and FLL (bottom).



(a) (b)

Fig. 6. Response characteristics of a geodetic-grade COTS GPS receiver against a spoofing attack for two cases, including navigation status (top), the C/No of the signal received for the GPS C/A code on the left and GPS P(Y) code on the right of each PRN column (middle), and the horizontal positioning result marked by '+,' indicating the positions of each epoch (bottom): (a) one of the visible satellites was fooled; (b) all of the visible satellites were fooled.

ing channel, navigation results and RAIM is discussed. As mentioned, we tested a current COTS GPS receiver using RF input without a baseband signal model but equipped with a software receiver. These results show how a COTS GPS receiver is vulnerable to a spoofing attack.

3.1. Response characteristics of the tracking channel

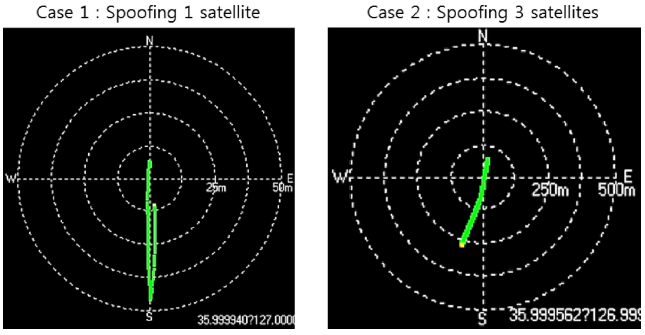
Figure 5 shows the C/No, delay lock loop (DLL) error, frequency lock loop (FLL) error, and phase lock loop (PLL) error for a tracking channel. The spoofing signal gets close to the genuine signal near 250 s and then fades near 310 s. In Fig. 5(a), the estimated carrier/noise ratio (C/No) after 310 s is higher than before. This means that the receiver is now tracking the fake signal from the spoofing attack after 310 s. Between 250 s and 310 s, there is a fluctuation in the C/No estimation result. This is due to constructive and destructive interference caused by the spoofing signal. During the same time span, tracking loop errors are observed for the DLL, FLL and PLL, as shown in Fig. 5(b).

As shown in Fig. 5, the response of the receiver tracking loop against a spoofing attack can be characterized by the C/No fluctuation, tracking loop errors, fluctuation in the code measurements, Doppler jump, and carrier phase lock loss. The spoofing detection method based on baseband signal monitoring identifies these phenomena.[6] This approach has an advantage in that it is very easy to implement in conventional GNSS receivers without any additional hardware modifications. However, its shortcoming is that it cannot detect anomalies after successful spoofing if it missed the moment when the receiver was affected during the capture procedure.

3.2. Response characteristics of a COTS GPS receiver based on RAIM during a spoofing attack

As shown in Fig. 2, the spoofing test scenario deceives the stationary receiver into moving from west to east. A geodetic-grade Novatel OEMV receiver was used as the victim receiver. The test was done by changing the number of spoofed channels to test the performance of the RAIM.

Figure 6 shows the results for cases in which one and all satellites were fooled, respectively. Figure 6(a) shows the case in which only one of the visible satellites was fooled. In the middle of Fig. 6(a), the C/No of PRN 21 is higher than that of the others. This means that the channel is tracking the fake signal, not the true one, because the spoofing signal is set to be transmitted at a higher power. However, the solution status of the receiver is computed normally and the positioning result remains in a stationary location, as shown at the top and bottom of Fig. 6(a). Thus, RAIM successfully detected the fault in PRN 21 and then excluded it to calculate the position. When some of the seven visible satellites were fooled, the solution status shows an integrity warning. There were positioning errors at the beginning of the spoofing attack; however, it stopped providing a solution after the takeover stage. The receiver could not remove the fake channel, but did raise an alarm. In short, when one or some of visible satellites are fooled, the RAIM function can successfully detect a spoofing attack by checking inconsistencies between the measurements and the solution. Figure 6(b) shows a case where all visible satellites were fooled. In this case, the RAIM function failed to raise an alarm and kept providing false positioning results from the spoofing attack. This is because all fake measurements and false solutions were consistent even though they were not genuine. The bottom of Fig. 6(b) shows that the solution started to move to the east, like the spoofing scenario was designed to do induce. As mentioned, the purpose of RAIM is not to handle a spoofing



(a) (b)

Fig. 7. Horizontal positioning results of a low-cost COTS GPS receiver against a spoofing attack for two cases: (a) one visible satellite was fooled, and (b) three visible satellites were fooled.

attack. Nevertheless, it can detect an incomplete spoofing attack. However, it is not a perfect countermeasure against spoofing attacks, as can be seen from the results in Fig. 6(b).

Figure 7 shows the spoofing test results for a low-cost Ublox GPS receiver. Figure 6(a) shows that RAIM could detect an incomplete spoofing attack. Figure 7(a) and 7(b) shows a similar test as in Fig. 6(a). However, the response of the low-cost receiver is different. Figure 7(a) shows, when one visible satellite is fooled, while RAIM successfully detects an anomaly in the spoofed tracking channel and then excludes the measurement for calculating the position. However, compared to Fig. 6(a), it took more time to make a decision, and subsequently an error of approximately 50 m south of the actual position was caused before detecting the anomaly. Figure 7(b) shows when three satellites were fooled, but the geodetic-grade receiver detected the anomaly and raised an alarm because not all satellites were fooled. However, the RAIM implemented in the Ublox receiver could not detect the anomaly, and therefore kept providing the wrong position results caused by the spoofing signals. Figures 6 and 7 show the different levels of spoofing detection capability depending on the RAIM algorithm utilized. High-quality RAIM could handle an incomplete spoofing attack. However, both kinds of RAIM failed to raise an alarm when all channels were fooled.

4. Brief Review of RAIM

In this section, the conventional RAIM algorithm is briefly reviewed. The spoofing detection method proposed is based on this algorithm. The formulas described here are used to explain the spoofing detection method in the next section.

First, the linearized measurement equation is defined as Eq. (1):

$$\underline{y} = H\underline{x} + \underline{\varepsilon} \tag{1}$$

where, $\underline{x}$ is the 4×1 linearized user state vector, $\underline{y}$ is the $n \times 1$ linearized pseudo-range measurement vector of n visible satellites, $\underline{\varepsilon}$ is the $n \times 1$ measurement error vector, and H is the $n \times 4$ matrix whose elements are three columns of direction cosines from user to each satellite with a value of 1 as the fourth column.

The RAIM algorithm cannot use the user position error itself as a test statistic because calculating the user positioning solution and verifying the integrity must be performed simultaneously. Instead, the range residual vector $\underline{w}$, which is the difference between the pseudo-range measurement $\underline{y}$ and estimated measurement $\underline{\hat{y}}_{LS}$ from the least-square positioning solution is used to derive the test statistic in Eq. (2).

$$\begin{aligned} \underline{\hat{x}}_{LS} &= \left(H^T H\right)^{-1} H^T \underline{y} \\ \underline{\hat{y}}_{LS} &= H \cdot \underline{\hat{x}}_{LS} \\ \underline{w} &= \underline{y} - \underline{\hat{y}}_{LS} \end{aligned} \tag{2}$$

The scalar test statistic D is calculated from the square sum of error (SSE) shown in Eq. (3). When the statistic is larger than the predefined threshold, RAIM detects a fault.

$$\begin{aligned} SSE &= \underline{w}^T \cdot \underline{w} \\ D &= \sqrt{SSE} \end{aligned} \tag{3}$$

This is a brief derivation of the RAIM algorithm. More details are explained in Hofmann-Wellenhof[14] and Brown.[15]

Equations (2) and (3) explain the results shown in Fig. 7. When some parts of the measurement in $\underline{y}$ are fake, an inconsistency exists between $\underline{y}$ and $\underline{\hat{x}}_{LS}$. This causes the square sum of the error to become a large value and raise an alarm. However, when all components of $\underline{y}$ are fake, there is no inconsistency and no alarm. This is why RAIM itself cannot be a perfect solution against a spoofing attack.

5. A Spoofing Detection Scheme using an Additional Ranging Source

The RAIM algorithm detects an inconsistency between the measurements and the estimated solution to raise an alarm. The reason RAIM cannot be a perfect countermeasure for detecting spoofing is that spoofing signals can maintain consistency for a misleading position. We propose a spoofing detection scheme that supplements the shortcomings of RAIM for spoofing detection using one additional encrypted ranging source. In order for a receiver to navigate with an encrypted signal, access to the whole encrypted navigation system, such as the Selective Availability and Anti-Spoofing Module (SAASM) for GPS P(Y) code, is required. However, the algorithm proposed requires just one encrypted signal for spoofing detection. Additionally, there is no additional hardware required for user receivers. The concept of the algorithm is shown in Fig. 8.

The algorithm proposed has two parts. One is an additional encrypted ranging source. Pseudolite or geosynchronous satellites can be used as the signal source. Because this signal is encrypted, the spoofer cannot generate the signal. This means that the user receiver can always trust the encrypted signal. The second part is the RAIM for spoofing detection implemented in a user receiver. Because there is always one authentic signal from the encrypted source, this results in an inconsistency with other signals. Accordingly, RAIM can detect the inconsistency and raise an alarm. This is very simple, but can provide a spoofing detection capabil-

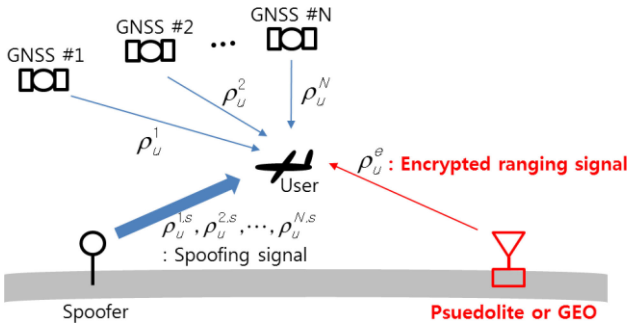


Fig. 8. Conceptual view of the GNSS spoofing detection scheme using an additional encrypted ranging source.

ity to users without any hardware modifications.

In Fig. 8, in a spoofing environment, the user receiver can receive signals from both the GNSS satellites and the spoofer. The pseudo-range measurements could be ρ_u^1, ρ_u^2, $\cdots$, ρ_u^N when the receiver is tracking the GNSS satellites or $\rho_u^{1,s}$, $\rho_u^{2,s}$, $\cdots$, $\rho_u^{N,s}$ when tracking the signals from the spoofer. Because the spoofer transmits GNSS-like signals for each satellite, the user receiver cannot discriminate if the signal received comes from the GNSS or the spoofer by itself. However, the measurement, ρ_u^e, from the additional encrypted ranging source can be treated as trustworthy because the spoofer cannot transmit the signal. It could be retransmitted like a meaconing attack; however, in that case, there is always a time delay compared to the true signal. Assuming that the receiver is fooled, the received measurements are $\rho_u^{1,s}$, $\rho_u^{2,s}$, $\cdots$, $\rho_u^{N,s}$ from the spoofer and ρ_u^e from the additional transmitter. The method proposed uses measurements consisting of two steps.

5.1. Step 1: Conventional RAIM without an encrypted signal

The first step is to apply conventional RAIM without an additional signal. The purpose of this step is to eliminate the cases when not all visible satellites are fooled. In an environment where a real signal is received, the body effect of the user vehicle, geographical conditions and an imperfect spoofing attack could result in not all of the tracking channels of the user receiver to be fooled. In this situation, conventional RAIM can detect an anomaly, as discussed in Section 3. If there is an alarm in the first step, there is no need for the next step.

However, there could be a case when a majority of the visible satellites are fooled. For example, assuming that all but one satellite are fooled, the conventional RAIM might eliminate the genuine signal and keep calculating the fake position. This is the function of the Fault Detection and Elimination (FDE) of RAIM. In this case, the purpose of the first step is to deliver only the fake measurement to Step 2.

5.2. Step 2: Spoofing detection with RAIM using an encrypted signal

The second step is to use the measurements delivered from the first step and the additional ranging measurement. Assuming that the user receiver has been fooled, the measurements from Step 1 are all fake. Then, the measurement vector $\underline{y}^*$ can be defined by Eq. (4). The measurements $\rho_u^{1,s}$, $\rho_u^{2,s}$, $\cdots$, $\rho_u^{N,s}$ are the faked satellite measurements, and ρ_u^e is the additional encrypted measurement.

$$\underline{y}^* = \begin{bmatrix} \rho_u^{1,s} & \rho_u^{2,s} & \cdots & \rho_u^{N,s} & \rho_u^e \end{bmatrix}^T \tag{4}$$

The geometry matrix H^* in Eq. (5) is constructed by appending the line of sight vector of the additional transmitter to the end of Eq. (1). The appended three elements of Eq. (5), $e_{u,x}^e$, $e_{u,y}^e$, $e_{u,z}^e$ are the line-of-sight vector from the user receiver to the additional transmitter, which is transmitting the encrypted signal. The position of the transmitter can then be acquired through the navigation message.

$$H^* = \begin{bmatrix} & H & \\ e_{u,x}^e & e_{u,y}^e & e_{u,z}^e & 1 \end{bmatrix} \tag{5}$$

Next, following the conventional RAIM described in Eqs. (2) and (3) using the new measurement vector $\underline{y}^*$ and geometry matrix H^*, the residual vector and final test statistic for spoofing detection can be calculated as described in Eqs. (6) and (7).

$$\begin{aligned} \underline{\hat{x}}_{LS}^* &= \left(H^{*T} H^*\right)^{-1} H^{*T} \underline{y}^* \\ \underline{\hat{y}}_{LS}^* &= H^* \cdot \underline{\hat{x}}_{LS}^* \\ \underline{w}^* &= \underline{y}^* - \underline{\hat{y}}_{LS}^* \end{aligned} \tag{6}$$

$$\begin{aligned} SSE^* &= \underline{w}^{*T} \cdot \underline{w}^* \\ D^* &= \sqrt{SSE^*} \end{aligned} \tag{7}$$

The residual vector $\underline{w}^*$ is calculated using both spoofed satellite measurements and the genuine additional transmitter's measurement. The additional signal causes an inconsistency when the others are faked. Thus, the test statistic D^* can be used to detect the spoofing attack.

5.3. Determination of the detection threshold

Determination of the spoofing detection threshold for the test statistic D^* is similar to the threshold for conventional RAIM, which is described in Brown and Chin.[16] The SSE in Eq. (7) is assumed to have a chi-square probability density function with respect to the number of visible satellites. Additionally, the false alarm rate is set to $3.33 \cdot 10^{-7}$ following the Minimal Operational Performance Standards (MOPS) of the Radio Technical Commission for Aeronautics (RTCA). The only difference is the consideration of an additional transmitter to set the degree-of-freedom of the chi-square probability density function. If we have N GPS or spoofing signals and 1 additional signal, the degree-of-freedom is $N + 1 - 4$. Moreover, to get a reasonable threshold, we set the standard deviation of the pseudo-range measurement to 5 m. Table 1 presents the spoofing detection threshold that we used for the experimental test, which will be explained in Section 6. This has been recalculated from the RAIM detection threshold table in Brown and Chin.[16]

6. Experimental Test Results

The algorithm proposed was tested by post-processing the measurements from a Novatel geodetic-grade receiver. To simulate a spoofing environment, the test setup explained

Table 1. Spoofing detection threshold.

Number of satellites in view with an additional transmitter	Chi-square degree-of-freedom (DOF)	Normalized Chi-square threshold (T_D^2/σ^2)	Threshold T_D in meters ($\sigma = 5$ m)
5	(Gaussian, $n = 5$)		
6	2	29.828	27.308
7	3	32.929	28.692
8	4	35.701	29.875
9	5	38.268	30.931
10	6	40.690	31.894
11	7	43.002	32.788
12	8	45.227	33.626

in Section 2 was used. Figure 9 is the sky plot of the satellites used in the test environment. As described in Section 5, the algorithm proposed requires an additional encrypted ranging source. To simulate the additional signal, PRN 4 in Fig. 9 was treated as the encrypted ranging signal by not letting the simulator generate a spoofing signal for PRN 4. This means that the authentic measurement ρ_u^e for spoofing detection in Eq. (4) can be acquired from PRN 4.

Two spoofing scenarios were used to test the algorithm. The first case was when four of the six visible satellites were fooled; in other words, most of the visible satellites were fooled. The other case was when all visible satellites were fooled. For both cases, PRN 4 was used as an additional authentic signal for the algorithm proposed. However, the conventional algorithm could not use the signal. Figures 10 and 11 show the results of the two cases, respectively.

Figure 10 shows that both the conventional and proposed RAIM can detect the spoofing attack. The red line is the threshold, and the blue line is the test statistic described in Eqs. (3) and (7). When the value of the blue line is larger than the red line, an alarm is raised. The spoofing signal started to affect the tracking loop at an epoch time of approximately 250 s. Before 250 s, for both RAIMs, the test statistic is below the threshold. The spoofing was completed at an epoch time of approximately 380 s. After that, the test statistics for both RAIMs exceeded the threshold. This means that they can successfully detect spoofing and raise an alarm. As shown for Case 1 in Fig. 6, the conventional RAIM can handle an imperfect spoofing attack.

Figure 11 shows the results when all visible satellites were fooled. In this test, the spoofing started at approximately 300 s and was completed at approximately 490 s. As can be seen on the left side of Fig. 11, after completion of the spoofing attack, the test statistic is still below the threshold. This means that the conventional RAIM missed detecting the spoofing attack. This is why the Novatel receiver could not raise an alarm against the spoofing shown for Case 2 in Fig. 6. However, the test statistic of the algorithm proposed exceeds the threshold after approximately 490 s. This means that it can detect the attack and raise an alarm, even when all the satellites have been fooled.

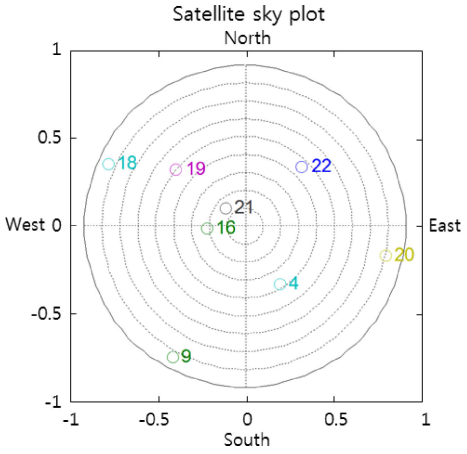


Fig. 9. Sky plot of the satellites for the spoofing test setup.

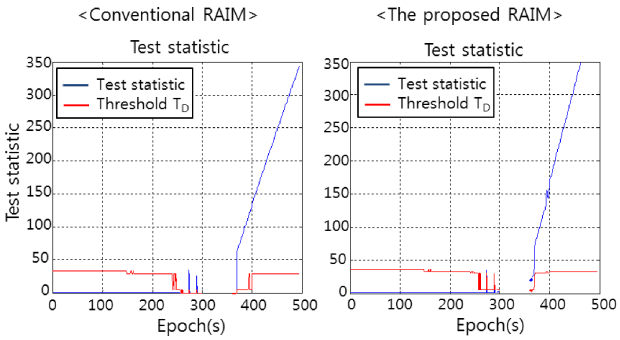


Fig. 10. Test statistics of the conventional RAIM (left) and the proposed RAIM (right) when most of the visible satellites are fooled.

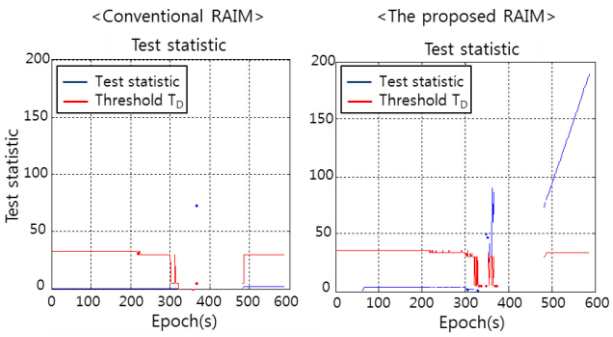


Fig. 11. Test statistics of the conventional RAIM (left) and proposed RAIM (right) when all visible satellites are fooled.

7. Conclusions

In this paper, the anti-spoofing performance of a COTS GPS receiver was analyzed. GPS spoofing attacks are now a real threat. Of course, there have been many studies on anti-spoofing methods. However, the problem is that many GPS receivers are being used in the field without having an anti-spoofing function. Thus, the current status of the COTS GPS receiver needs to be determined first. This paper has shown how vulnerable the COTS GPS receiver is against spoofing. To test COTS receivers, a spoofing signal should be injected into the receiver using a RF input. In outdoor testing, transmitting a spoofing signal with a live GPS signal

could cause problems for other users. Thus, we developed an in-line spoofing test environment using two GPS simulator modules. With this test environment, we were able to test a COTS receiver indoors.

The test results show that the tracking loop of each channel could not cope with an attack by itself. When a spoofing signal with slightly higher power sweeps the genuine signal, the tracking loop readily changes its lock to the fake signal. During the transition phase, some characteristics such as fluctuation in the estimated signal power, PLL lock loss, and Doppler jump can be observed. We also analyzed the navigation function against spoofing. It is well known that RAIM is designed to detect inconsistencies between measurements. Our results show that RAIM could detect an imperfect spoofing attack when not all visible satellites were fooled. This situation could occur in a real environment because of the body effect of the user vehicle, geographical obstacles or an inaccurate spoofing attack. However, when all visible satellites are fooled, it fails to detect the attack. Since RAIM is not designed to detect spoofing, it is not a perfect solution by itself.

This study proposed a spoofing detection method based on RAIM using an additional ranging source. When considering that COTS GPS receivers are being used in the field, a spoofing detection method requiring additional hardware is not practical. It is well known that the best solution is to use encrypted signals for navigation. However, at this moment, the GPS P(Y) code is the only source, and civilians are not able to use it. What we propose is to add just one additional transmitter, not an entire encrypted navigation system. This could be useful to protect some areas from spoofing attacks by adopting a pseudolite. Otherwise, some countries that do not have their own satellite navigation system could use one satellite to transmit an encrypted signal to support a spoofing detection capability for their users.

References

1) Kaplan, E. D.: *Understanding GPS: Principles and Applications,* 2nd Ed., Artech House, Norwood, MA, USA, 2005.
2) Dovis, F.: *GNSS Interference Threats and Countermeasures*, Artech House, Norwood, MA, USA, 2015.
3) Peterson, S. and Faramarzi, P.: Exclusive: Iran Hijacked US Drone, Says Iranian Engineer, csmonitor.com (retrieved 15 December 2011).
4) Humphreys, T. E.: Statement on the Vulnerability of Civil Ummanned Aerial Vehicles and Other Systems to Civil GPS Spoofing, July 2012, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf
5) Anon.: Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System Technology Report, John A. Volpe National Transportation Systems Center, 2001.
6) Jafarnia-Jahromi, A., Brounmandan, A., Nielsen, J., and Lachapelle, G.: GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques, *Int. J. Navigation Observation*, **2012** (2012), 127072.
7) Danesshmand, S., Jafarnia-Jahromi, A., Brounmandan, A., and Lachapelle, G.: A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array, Proceedings of the Institute of Navigation (ION GNSS 2012), Nashville, TN, USA, September 2012.
8) Lo, S. C., Peterson, B. B., and Enge, P. K.: Assessing the Security of a Navigation System: A Case Study using Enhanced Loran, Proceedings of European Navigation Conference, Naples, Italy, May 2009.
9) Humphreys, T. E., Bhatti, J. A., and Ledvina, B. M.: The GPS Assimilator: a Method for Upgrading Existing GPS User Equipment to Improve Accuracy, Robustness and Resistance to Spoofing, Proceedings of the Institute of Navigation (ION GNSS 2010), Portland, OR, USA, September 2010.
10) So, H., Jang, J., Lee, K., Song, K., and Park, J.: GNSS Spoofing Detection Scheme Based on the Combined Use of a Single Authentic Ranging Signal and RAIM, Proceedings of 2015 International Association of Institutes of Navigation World Congress (2015 IAIN World Congress), Prague, Czech, October 2015.
11) Shepard, D. P. and Humphreys, T. E.: Characterization of Receiver Response to Spoofing Attacks, Proceedings of the Institute of Navigation (ION GNSS 2011), Portland, OR, USA, September 2011.
12) Anon.: GSS8000 GNSS Constellation Simulator Datasheet, Spirent Communications, 2010.
13) Anon.: SX-NSR Navigation Software Receiver User Manual, IFEN, 2014.
14) Hofmann-Wellenhof, B., Lichtenegger, H., and Wasle, E.: *GNSS–Global Navigation Satellite Systems: GPS, GLONASS, Galileo, and More*, Springer-Verlag Wien, 2007.
15) Brown, R. G.: A Baseline GPS RAIM Scheme and a Note on the Equivalence of Three RAIM Methods, *Navigation*, **39**, 3 (1992), pp. 301–316.
16) Brown, R. G. and Chin, G. Y.: GPS RAIM: Calculation of Threshold and Protection Radius Using Chi-Square Methods–A Geometric Approach, *Global Positioning System: Institute of Navigation*, Vol. V, 1997, pp. 155–179.

S. Matunaga
Associate Editor