JPNT 7(3), 139-146 (2018)
https://doi.org/10.11003/JPNT.2018.7.3.139

JPNT Journal of Positioning, Navigation, and Timing

Technical Issues on Implementation of GPS Signal Authentication System

Hyoungmin So†, Jaegyu Jang, Kihoon Lee, Junpyo Park

Agency for Defense Development, Daejeon 34186, Korea

ABSTRACT

In recent years, a satellite navigation signal authentication technique has been introduced to determine the spoofing of commercial C/A code using the cross-correlation mode of GPS P(Y) code received at two receivers. This paper discusses the technical considerations in the implementation and application of authentication system simulator hardware to achieve the above technique. The configuration of the simulator consists of authentication system and user receiver. The synchronization of GPS signals received at two devices, data transmission and reception, and codeless correlation of P(Y) code were implemented. The simulation test result verified that spoofing detection using P(Y) codeless correlation could be achieved.

Keywords: spoofing, codeless correlation, GPS P(Y) code, authentication, GNSS

1. INTRODUCTION

A satellite navigation system typically represented by Global Positioning System (GPS) is known to be vulnerable to artificial interference due to the characteristics of publicly disclosed signal structure and weak signal reception intensity at the ground. The artificial interference can be divided largely into jamming and spoofing (Kaplan & Hegarty 2006). Jamming is an attack method that prevents user receivers from receiving navigation satellite signals, and spoofing is an attack type that makes user receivers calculate wrong navigation solutions without recognizing it, thereby leading the user to have a wrong position (Dovis 2015). In recent years, as satellite navigation interference attacks have been sophisticated, threats of spoofing attacks have increased and related studies have been actively conducted (Humphreys 2012).

The Volpe Report published in 2001 analyzed the threat of spoofing attacks in satellite navigation and classified a spoofing countermeasure technique into six types based on their performance (John A. Volpe National Transportation Systems Center 2001). Among them, the best spoofing countermeasure technique is a method that uses encrypted signal sources which cannot be maliciously regenerated fundamentally (Jafarnia-Jahromi et al. 2012). However, GPS P(Y) code in the US is the only currently available encryption signal sources in satellite navigation. To use GPS P(Y) code from nations other than the US, the Selective Availability Anti-Spoofing Module (SAASM), which is the decryption module, has to be purchased after the approval of foreign military sales (FMS), and periodical encryption update has to be made for continuous operation, which is regarded as a considerable restriction to the operation. In addition, private sectors cannot get the FMS purchase approval fundamentally. Thus, the use of GPS P(Y) code is not a suitable candidate for general anti-jamming method.

Stanford University proposed a signal authentication technique that was utilized in jamming detection in GPS commercial C/A code using the encryption characteristics of P(Y) code without the SAASM (Lo et al. 2009). The proposed technique cross-compares P(Y) code components contained in GPS signals received at two receivers. This method consists of authentication system that is not vulnerable to spoofing, as it is installed in a secured place, and spoofing verification target receiver. The authentication

Received Nov 17, 2017 **Revised** Jan 04, 2018 **Accepted** Aug 21, 2018
†**Corresponding Author**
E-mail: hyoungmin.so@gmail.com
Tel: +82-42-821-4463 Fax: +82-42-823-3400

system and user receiver stores GPS intermediate frequency (IF) sample data, respectively. When user receiver receive normal GPS signals, IF sample data at the two receivers synchronized with the C/A code will contain the same phase P(Y) code. Thus, if P(Y) code components from the two received signals are extracted and correlation gain is obtained by performing a crossing codeless correlation of the IF sample data, it can give an outcome of normal or spoofing status.

This paper discusses the fabrication of simulator hardware to verify availability and operation performance of the signal authentication system proposed by Stanford University. This paper proposes a method of how to apply the proposed algorithm to real receivers and synchronization technique between user receiver and authentication system. In addition, a gap condition between user receiver and authentication system that affects the correlation gain of codeless correlation is analyzed to propose the gap requirements when applying the system in the Korean Peninsula.

This paper is organized as follows. Section 2 briefly reviews the signal authentication technique proposed in Stanford University. Section 3 describes the configuration of the authentication system simulator consisting of the authentication system and user receiver. Section 4 presents the performance of the authentication system simulator implemented using a GPS simulator. Finally, Section 5 analyzes the codeless correlation loss due to satellite interference according to a gap distance between the user receiver and authentication system.

2. BRIEF REVIEW OF GPS P(Y) CODELESS CORRELATION (PSIAKI ET AL. 2011)

Stanford University proposed a signal authentication technique using two receivers in 2009. Since then, Cornell University published a paper on the above algorithm (Psiaki et al. 2011). In this section, the execution process of codeless correlation on GPS P(Y) code at two receivers is briefly reviewed by referring to the paper.

The received signals from arbitrary satellites received at Receivers A and B in the authentication system can be modeled by Eqs. (1) and (2). y_{ai}, y_{bi} refers to the i-th IF sample data received at Receivers A and B, A_{ca}, A_{cb} is the amplitude of C/A code signals, C_f is the C/A code, A_{pa}, A_{pb} is the amplitude of the P(Y) code signal, P_{yf} is the P(Y) code, $\omega_{IF,a}$, $\omega_{IF,b}$ is a carrier wave Doppler in the IF, ϕ_a, ϕ_b is the carrier wave phase, t_{ai}, t_{bi} is a sample time at the i-th sample, and n_{ai}, n_{bi} refers to noise.

$$y_{ai} = A_{ca}C_f(t_{ai})\cos\left[\omega_{IF,a}t_{ai} + \phi_a(t_{ai})\right] + A_{pa}P_{yf}(t_{ai})\sin\left[\omega_{IF,a}t_{ai} + \phi_a(t_{ai})\right] + n_{ai} \quad (1)$$

$$y_{bi} = A_{cb}C_f(t_{bi})\cos\left[\omega_{IF,b}t_{bi} + \phi_b(t_{bi})\right] + A_{pb}P_{yf}(t_{bi})\sin\left[\omega_{IF,b}t_{bi} + \phi_b(t_{bi})\right] + n_{bi} \quad (2)$$

As shown in the above, GPS signals transmit C/A code and P(Y) code simultaneously using the quadrature phase, and their inter-synchronization is maintained. The C/A code tracking information is used to remove only the P(Y) code component from the signals in Eqs. (1) and (2). The C/C code tracking information is utilized to extract IF sample data at the same time from two receivers. Next, the sin component is removed and the cos component containing P(Y) code information is extracted using carrier Doppler estimate $\hat{\omega}_{IF,a}$, $\hat{\omega}_{IF,b}$ which is a carrier wave tracking result, and carrier phase estimate $\hat{\phi}_a$, $\hat{\phi}_b$. The mixing process to extract the cos component from each of the receivers is presented in Eqs. (3) and (4).

$$y_{q,ai} = y_{ai} \cdot \sin\left[\hat{\omega}_{IF,a}t_{ai} + \hat{\phi}_a(t_{ai})\right] \approx \frac{1}{2}A_{pa}P_{yf}(t_{ai}) + n_{qai} \quad (3)$$

$$y_{q,bi} = y_{bi} \cdot \sin\left[\hat{\omega}_{IF,b}t_{bi} + \hat{\phi}_b(t_{bi})\right] \approx \frac{1}{2}A_{pb}P_{yf}(t_{bi}) + n_{qbi} \quad (4)$$

Here, n_{qai}, n_{qai} is the noise included in the P(Y) code component $y_{q,ai}$, $y_{q,ai}$ with regard to arbitrary satellite after quadrature mixing in Eqs. (3) and (4), which includes interference and measurement noise by other satellites.

Finally, normal C/A code is received from two receivers and if they are inter-synchronized, the two receivers receive signals containing the same phase P(Y) code component, and the codeless correlation result γ_{ul} of M samples will have a sufficient correlation gain.

$$\gamma_{ul} = \sum_{i}^{M} y_{q,ai} \cdot y_{q,bi} \quad (5)$$

3. IMPLEMENTATION OF SIGNAL AUTHENTICATION SIMULATOR

3.1 System Architecture

The authentication system simulation was implemented to develop and verify the satellite navigation signal authentication technique to determine whether C/A code was spoofed. The P(Y) codeless correlation system described in Section 2 consists of signal authentication system that receives reference signals, and user receiver as the authentication target. The user receiver acquires IF sample data and transfers the sample data to the authentication system. The authentication system performs GPS P(Y) codeless correlation using its own IF sample data and user

https://doi.org/10.11003/JPNT.2018.7.3.139

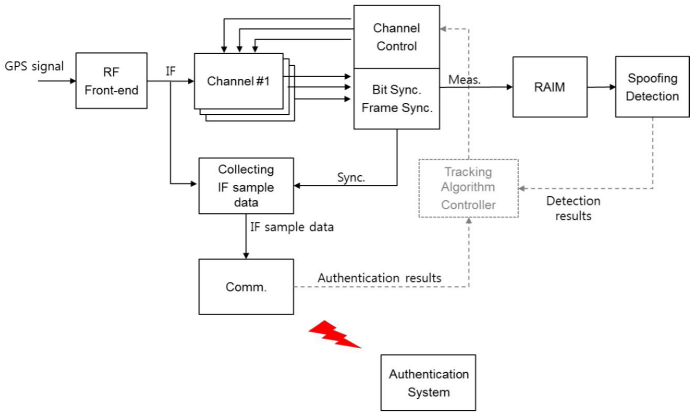

Fig. 1. Flow diagram of user receiver.

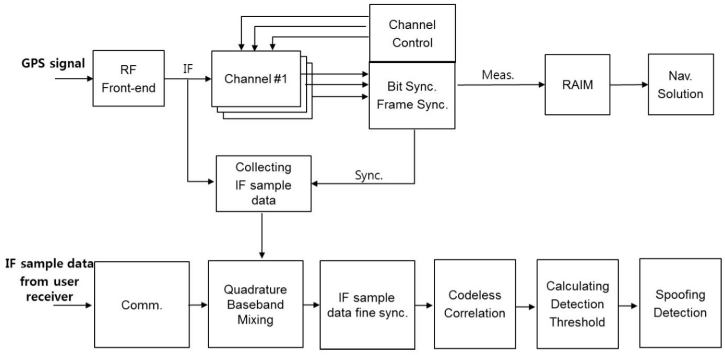

Fig. 2. Flow diagram of authentication system.

receiver's sample data. Here, the authentication system and user receiver have to store sample data synchronized with the satellite time. Thus, frame synchronization information and navigation data bits of signal tracking loop are employed. Fig. 1 shows the configuration diagram of user receiver, which includes synchronization information transmission, sample data collection, and data transmission and receive functions with the authentication system in addition to the signal tracking process.

Fig. 2 shows the configuration diagram of the signal authentication system. As shown in the user receiver in Fig. 1, a function of storing IF sample data was implemented in addition to the generally implemented GPS signal processing process. Furthermore, functions of inputting sample data from the user receiver and performing codeless correlation were implemented additionally.

The synchronization of satellite time between the authentication system and user receiver was based on the sub-frame starting point with six seconds interval. Once the authentication system orders sample data collection to the user receiver, sample data are stored for an arbitrary period of time from the first sub-frame starting point since the order is received. Here, the authentication system sets the reference pseudo-random noise (PRN) and transfers this to the user so that user and authentication system will store sample data based on the same PRN. Since the acquired IF sample data are synchronized with the satellite clock using the common-view method, codeless correlation and signal authentication can be performed after C/A code search within a range of the satellite clock error level even for satellites outside the reference PRN.

3.2 Hardware Implementation

The signal authentication unit consists of GPS receiver for signal authentication data collection, RF-IF data collector, computer for data collection and signal authentication processing, GPS receiver, and computer for signal authentication monitoring. The user receiver consists of GPS receiver for spoofing data collection, RF-IF data collector, and computer for data collection and GPS receiver monitoring. For data transmission between the authentication system and user receiver, wired or Long-Term Evolution Ethernet communication method was used.

To collect synchronized IF sample data between signal authentication unit and user receiver, a high-speed data collection unit is necessary. The fabricated receiver processes

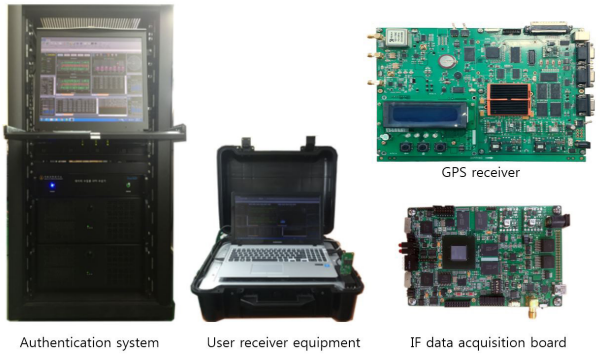

Fig. 3. System implementation.

Table 1. Specification of the implemented system.

	Specification
RF frequency (MHz)	1575.42
Intermediate frequency (MHz)	14
Sampling frequency (MHz)	56
Signal bandwidth (MHz)	Fc ± 2, Fc ± 4, Fc ± 8, Fc ± 12
IF data interface	High speed USB 3.0
IF data acquisition speed (Gbit/sec)	Max. 1
IF data save time (sec)	Max. 10

the IF with sampling frequency 56 MHz and 8-bit data. Thus, since the data collector had to collect and transmit IF data at a rate of 56 Mbyte per sec, USB 3.0 interface was used to collect data. Fig. 3 shows the implemented authentication system, user receiver, and configuration board, and the specifications are presented in Table 1.

4. EXPERIMENTAL TEST RESULTS USING GPS SIMULATOR

4.1 Test Setup

To verify the performance of the implemented system, GPS simulator and spoofing signal generator were used to simulate the spoofing environment. The spoofing detection technique applied in this study employs two receivers. Thus, two GPS simulators that have the same satellite environment and synchronization information are needed. The configuration of the experimental test devices is shown in Fig. 4. Here, the authentication system and user receiver were set to have 24 MHz and 8 MHz bandwidths. The two GPS simulators simulate signals of the user and authentication systems. The user signal is provided by inputting signals to SimSAFE, which is a spoofing signal generator, and SimSAFE generates spoofing signals synchronized with the current

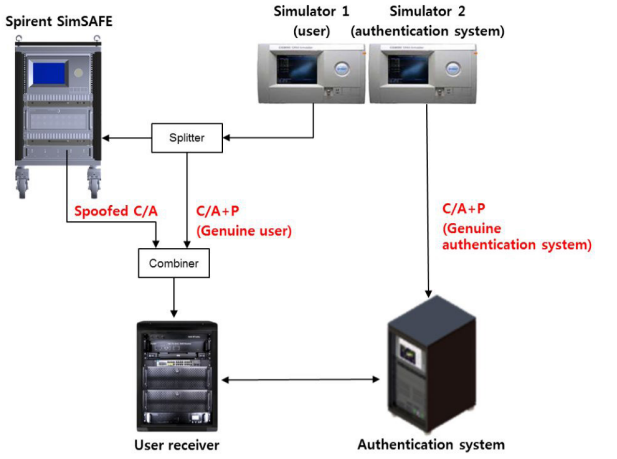

Fig. 4. Test setup for spoofing detection method using two receivers.

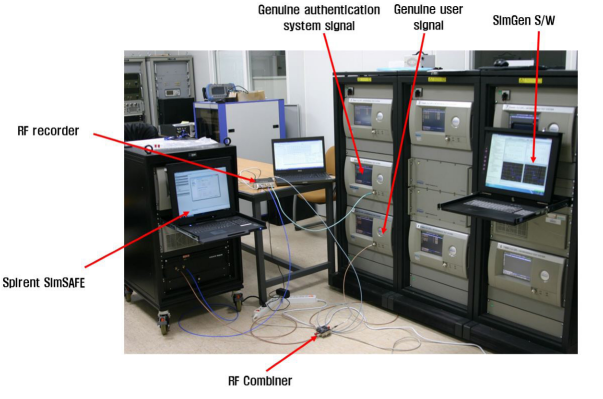

Fig. 5. Picture of test setup.

user signal (Spirent Communications 2013). Fig. 5 shows the photo of the test, in which two modules from multiple RF GPS simulators were used to employ the two synchronized simulators.

4.2 Test Results

The codeless correlation results defined in Eq. (5) were verified when user receiver received normal and spoofing signals using the data collected at the spoofing simulation environment in Figs. 4 and 5. The left side of Fig. 6 shows the correlation integral result of IF data from the two receivers in 1 ms when the user receiver receives normal signals. The right side of Fig. 6 shows the correlation integral accumulation in every 1 ms, which means the result when a correlation integral time of codeless correlation is extended continuously up to 8 sec. The acquisition of correlation gain was verified after passing a sufficient correlation integral time as the user receiver received the same P(Y) code component with that of the authentication system when normal signals

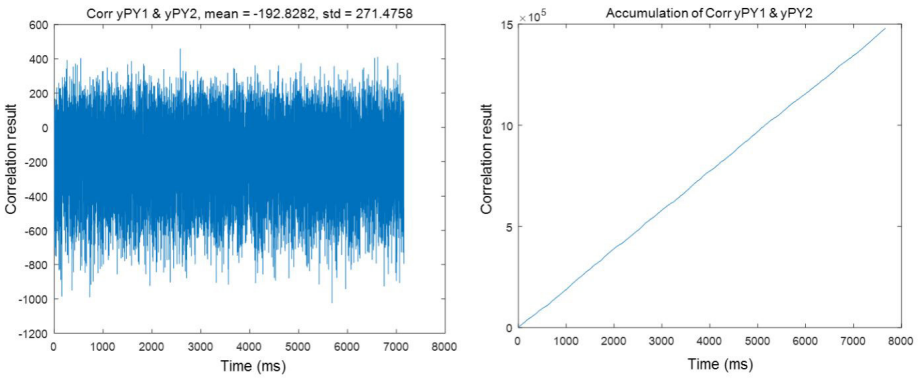

Fig. 6. GPS P(Y) codeless correlation result when a user receiver tracks genuine signal.

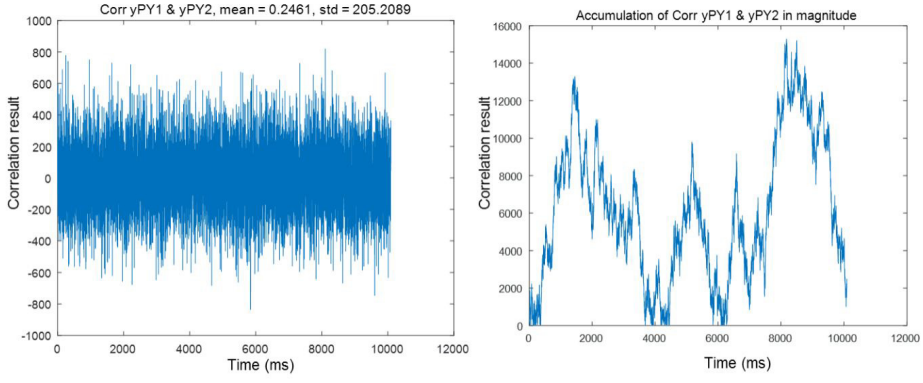

Fig. 7. GPS P(Y) codeless correlation result when a user receiver tracks spoofing signal.

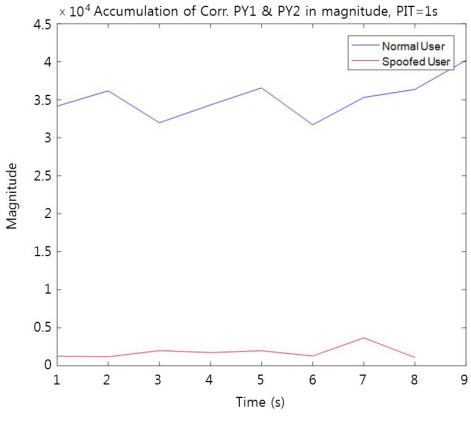

Fig. 8. GPS P(Y) codeless correlation result with 1s integration time.

were received.

Fig. 7 shows the correlation results when the user receiver receives spoofing signals. The left side of the figure shows that a mean value of correlation values every 1 ms is 0.2461, which is close to zero, and the right side figure, in which correlation integral time is extended continuously, also verifies that sufficient correlation gain is not acquired, which is different from that of Fig. 6.

Fig. 8 shows the results when a correlation integral time of GPS P(Y) codeless correlation is set to 1 sec. That is, it shows the correlation values by collecting data every one sec. from the left side figures in Figs. 6 and 7. The figure verifies that the correlation gain can distinguish the users who receive normal and spoofing signals.

5. ANALYSIS OF CODELESS CORRELATION LOSS BY INTER-SATELLITE INTERFERENCE

Fig. 6 shows that the correlation integral result of 1 ms has -192 value on average when normal signals are received. The standard deviation is 271, which shows a considerably low correlation gain in 1 ms and sufficient correlation gain may not be acquired in some cases. This was because the target data where the codeless correlation was performed were IF sample data collected from two receivers. Eqs. (1-5) are simplified equations assuming that signals from only one satellite are received at each receiver. However, in real situations, signals transmitted from multiple satellites are received so that signals from other satellites than correlation target satellite are included in the IF same data of correlation

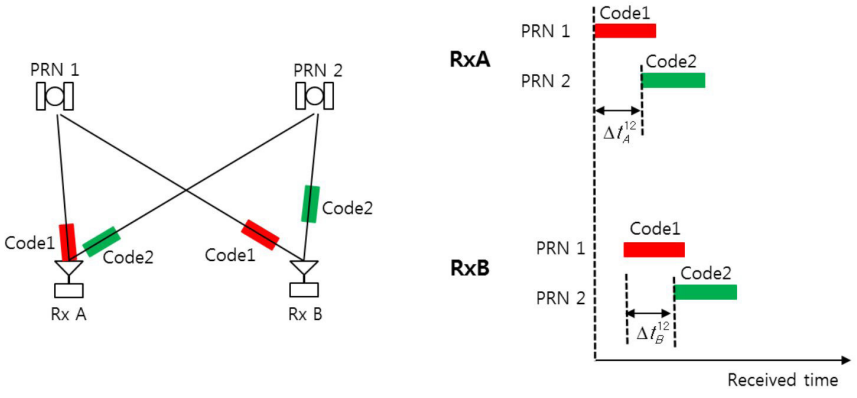

Fig. 9. Simulation case of 2 satellites in view (left), conceptual timing graph of received time of code 1 and code 2 from receiver A and B (right).

target, thereby causing the interference. The codeless correlation process with regard to received sample data at Receivers A and B is described as follows as shown in Fig. 9 with two satellites.

The signal models received at Receivers A and B in Fig. 9 are presented in Eqs. (6) and (7). The superscripts 1 and 2 in the equations refer to satellite numbers.

$$y_{ai} = A_{ca}^{1} C_{f,a}^{1}(t_{ai})\cos\left[\omega_{IF}^{1} t_{ai} + \varphi_{a}^{1}(t_{ai})\right] + A_{pa}^{1} P_{yf}^{1}(t_{ai})\sin\left[\omega_{IF}^{1} t_{ai} + \varphi_{a}^{1}(t_{ai})\right] + A_{ca}^{2} C_{f,a}^{2}(t_{ai})\cos\left[\omega_{IF}^{2} t_{ai} + \varphi_{a}^{2}(t_{ai})\right] + A_{pa}^{2} P_{yf}^{2}(t_{ai})\sin\left[\omega_{IF}^{2} t_{ai} + \varphi_{a}^{2}(t_{ai})\right] + n_{ai} \quad (6)$$

$$y_{bi} = A_{cb}^{1} C_{f,b}^{1}(t_{bi})\cos\left[\omega_{IF}^{1} t_{bi} + \varphi_{b}^{1}(t_{bi})\right] + A_{pb}^{1} P_{yf}^{1}(t_{bi})\sin\left[\omega_{IF}^{1} t_{bi} + \varphi_{b}^{1}(t_{bi})\right] + A_{cb}^{2} C_{f,b}^{2}(t_{bi})\cos\left[\omega_{IF}^{2} t_{bi} + \varphi_{b}^{2}(t_{bi})\right] + A_{pb}^{2} P_{yf}^{2}(t_{bi})\sin\left[\omega_{IF}^{2} t_{bi} + \varphi_{b}^{2}(t_{bi})\right] + n_{bi} \quad (7)$$

Assuming that signal authentication is performed on No. 1 satellite, Eqs. (6) and (7) perform synchronization with regard to No. 1 satellite time, followed by a quadrature mixing process in Eqs. (3) and (4) that removes the C/A code component using the carrier wave Doppler and phase tracking value of No. 1 satellite. After this, the correlation result using the same mode in Eq. (5) can be arranged into the result of Eq. (8). Here, it satisfies ${}_{a}\Delta_{b}(\cdot)=(\cdot)_{a}-(\cdot)_{b}$ and ${}^{1}\nabla^{2}(\cdot)=(\cdot)^{1}-(\cdot)^{2}$.

$$\begin{aligned}\gamma_{ul} &= \sum_{i}^{M} y_{q,ai} \cdot y_{q,bi} \\ &= \sum_{i}^{M} A_{pa}^{1} A_{pb}^{1} P_{yf,a}^{1}(t_{ai}) P_{yf,b}^{1}(t_{bi}) \\ &\quad + \frac{1}{2} A_{pa}^{2} A_{pb}^{2} P_{yf,a}^{2}(t_{ai}) P_{yf,b}^{2}(t_{bi}) \cdot \left\{\cos\left({}^{1}\nabla^{2}{}_{a}\Delta_{b}\omega_{IF} t_{i} + {}^{1}\nabla^{2}{}_{a}\Delta_{b}\varphi\right)\right. \\ &\quad \left. + \cos\left({}^{1}\nabla^{2}\omega_{IF,a} t_{i} + {}^{1}\nabla^{2}\omega_{IF,b} t_{i} + {}^{1}\nabla^{2}\varphi_{a} + {}^{1}\nabla^{2}\varphi_{b}\right)\right\}\end{aligned} \quad (8)$$

The first term $A_{pa}^{1}A_{pb}^{1}\mathrm{P}_{yf,a}^{1}(t_{ai})\mathrm{P}_{yf,b}^{1}(t_{bi})$ among the correlation results is the codeless correlation result value of No. 1 satellite, the target satellite. The correlation gain can be obtained by P(Y) code when two receivers are synchronized with No. 1 Satellite. The remaining part after the first term in the equation refers to the interference component generated by No. 2 Satellite. The $A_{pa}^{2}A_{pb}^{2}\mathrm{P}_{yf,a}^{2}(t_{ai})\mathrm{P}_{yf,b}^{2}(t_{bi})$ component in the second term refers to the codeless correlation result by P(Y) code component of No. 2 Satellite at each receiver. In the satellite arrangement environment where a pseudorange difference between Receivers A and B with regard to No. 1 Satellite is similar to that with regard to No. 2 Satellite, or Receivers A and B are located nearby, No. 2 satellite is also synchronized by the clock synchronization with regard to No. 1 satellite, thereby acquiring a correlation gain as well, which acts as the interference with regard to the correlation of No. 1 Satellite.

The codeless correlation gain loss due to the interference between satellites analyzed in Eq. (8) is calculated with regard to the two visible satellites. However, if it is involved with more than two visible satellites, interpretive analysis is difficult. Thus, this paper analyzed the gap condition between user receiver and authentication system to exclude the inter-satellite interference at the satellite arrangement environment in the Korean Peninsula. To eliminate the interference term $A_{pa}^{2}A_{pb}^{2}\mathrm{P}_{yf,a}^{2}(t_{ai})\mathrm{P}_{yf,b}^{2}(t_{bi})$ in Eq. (8) during the integral process, a difference in distance observed between user receiver and authentication system should be larger than 30 m, which is a single chip length of P(Y) code with regard to a combination of any two satellites in the visible satellites.

Fig. 10 shows the analysis result of inter-satellite interference effect according to the position of user receiver when authentication system is located in Daejeon region for 24 hours using the BRDC RINEX navigation data of DOY266 in 2014. The left side of Fig. 10 shows a distribution of the minimum values of difference in double difference pseudoranges between authentication system and user receiver obtained in all combinations of two satellites in the

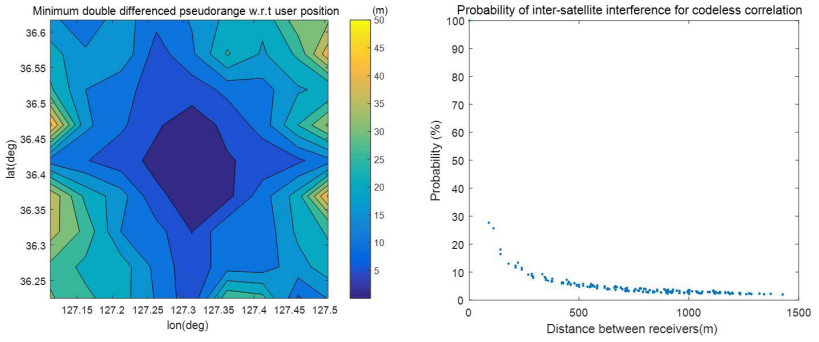

Fig. 10. Minimum double differenced pseudorange distribution with respect to the location of user receiver (left) and probability of inter-satellites interference for codeless correlation with respect to the distance between user receiver and authentication system.

visible satellites. Assuming that the authentication system is located in latitude 36° 25.130' and longitude 127° 18.732', which is the center in the figure, a user is escaped from the 30m condition, which is a double difference pseudorange that generates the interference, as the user is farther away from the location of the authentication system. The right figure of Fig. 10 shows the results of the left figure in terms of the distance, and probabilities of codeless correlation interference occurrence between visible satellites according to the distance between user receiver and authentication system. The probability in the figure was defined as the number of satellites where interference occurs out of all visible satellites. The processing results verified around 5% and 2% of interference occurrence probability at a gap of 500 m and 1,500 m, respectively.

6. CONCLUSIONS

This paper implemented a spoofing detection system of codeless correlation method that utilized synchronization system of GPS P(Y) code using two receivers, and verified the signal authentication performance. The implemented system consisted of signal authentication system for normal signal reception, which was the authentication reference, and user receiver that was a target of spoofing detection. In each receiver, the following functions were implemented: acquiring IF sample data, acquiring synchronization information with navigation data bits, data transmission and reception, and codeless correlation in addition to GPS signal reception processing. To verify the performance of the implemented system, two GPS simulators and SimSAFE spoofing signal generator from Spirent were used to configure the spoofing environment.

In the experiment, correlation gain results with regard to normal and spoofing signals for 1 ms correlation integral time were checked, and correlation gain between the two receivers could be acquired according to the codeless correlation while increasing the correlation integral time. The experiment result verified that when normal signals were received, sufficient correlation gains were secured in the authentication system and user receiver as the correlation between the same P(Y) code components was achieved according to the synchronization due to the C/A code. In contrast, when spoofing signals were received, correlation gains were not increased even if the correlation integral time was increased. Since correlation target in this system was not the code itself but IF sample data, inter-satellites interference occurred due to a number of satellites existed inside the collected data. This paper analyzed the cause of the interference, and verified that a sufficient distance gap between the authentication system and user receiver is necessary while long-term correlation integral time is required to minimize the interference.

REFERENCES

Dovis, F. 2015, GNSS Interference threats and countermeasures (Norwood, MA: Artech House)

Humphreys, T. E. 2012, Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing. https://radionavlab.ae.utexas.edu/images/stories/files/papers/Testimony-Humphreys.pdf

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. 2012, GPS vulnerability to spoofing threats and a review of antispoofing techniques, International Journal of Navigation and Observation, Article ID127072, 1-16. http://dx.doi.org/10.1155/2012/127072

John, A. Volpe National Transportation Systems Center 2001, Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System,

Technology Report
Kaplan, E. D. & Hegarty, C. J. 2006, Understanding GPS: Principles and Applications, 2nd ed. (Boston: Artech House Inc.)
Lo, S., Lorenzo, D. D., Enge, P., Akos, D., & Bradley, P. 2009, Signal authentication: A secure civil GNSS for today, Inside GNSS, Sept/Oct 2009
Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P., & Humphreys, T. E. 2011, Civilian GPS spoofing detection based on dual-receiver correlation of military signals, in Proceedings of the 24th ITM of The Institute of Navigation, Sept. 2011, Portland, OR.
Spirent Communications 2013, SIMSAFE user manual (Devon, UK: Spirent Communications)

Hyoungmin So is a senior researcher of Agency for Defense Development (ADD) in Korea, Republic of. He received B.S. degree in mechanical engineering at Korea Univ. and M.S. and Ph.D. degree in aerospace engineering at Seoul National University (SNU). He worked in the field of GNSS and pseudolite receiver development including SDR and vector tracking loop algorithm in SNU GNSS laboratory. Since 2011, he's been working for ADD. His research interests are GNSS receiver, anti-jamming/spoofing algorithm, and WADGPS technologies.

Jaegyu Jang is a senior researcher of Agency for Defense Development (ADD) in Republic of Korea. He received B.S. degree in mechanical & aerospace engineering at Seoul National University and M.S. and Ph.D. degree in aerospace engineering at Seoul National University. He worked in the field of mobile communication and GNSS research for more than 10 years. His research interests include anti-jamming, radio navigation and GNSS signal processing.

Kihoon Lee is a senior researcher at Agency for Defense Development. He received his B.S. from the Mechanical Engineering Department of POSTECH in 1999. He re-ceived his M.S. from the Mechanical Engin-eering Department of Korean Advanced Institute of Science and Technology in 2001. He has served as a researcher at Agency for Defense Devel-opment since 2001. His research focuses on the development of GNSS receiver, Anti-Jamming and Space Based Augmen-tation System.

Junpyo Park received B.S. and M.S. degree in mechanical engineering at Pusan National Univ. and Ph.D. degree in aerospace engineering at Chung-nam National Univ. He is a principal researcher in the Agency for Defense Development, Korea. His research interests include integrity monitoring of GNSS signal, pseudolites, and GNSS-related engineering problems.

https://doi.org/10.11003/JPNT.2018.7.3.139