JPNT 5(4), 165-172 (2016)
https://doi.org/10.11003/JPNT.2016.5.4.165

JPNT Journal of Positioning, Navigation, and Timing

Implementation of GPS Spoofing Test Environment using Multiple GPS Simulators

Hyoungmin So†

Agency for Defense Development, Daejeon 305-600, Korea

ABSTRACT

A Global Navigation Satellite System (GNSS), which is typically exemplified by the Global Positioning System (GPS), employs a open signal structure so it is vulnerable to spoofing electronic attack using a similar malicious signal with that used in the GPS. It is necessary to require a spoofing test evaluation environment to check the risk of spoofing attack and evaluate the performance of a newly developed anti-spoofing technique against spoofing attacks. The present paper proposed a simulation method of spoofing environment based on simulator that can be implementable in a test room and analyzed the spoofing simulation performance using commercial GPS receivers. The implemented spoofing simulation system ran synchronized two GPS simulator modules in a single scenario to generate both of spoofing and GPS signals simultaneously. Because the signals are generated in radio frequency, a commercial GPS receiver can be tested using this system. Experimental test shows the availability of this system, and anti-spoofing performance of a commercial GPS receiver has been analyzed.

Keywords: GPS spoofing, spoofing environment, GPS simulator, COTS GPS receiver, anti-spoofing

1. INTRODUCTION

A spoofing attack against the Global Navigation Satellite System (GNSS) refers to a situation where a user is induced into incorrect positioning by regenerating similar signals with broadcasting signals of navigation satellite (Dovis 2015). Malicious signal regeneration can be achieved if the same navigation message structure with the open spread-spectrum code such as GPS C/A code, and GPS receivers using such signal source are susceptible to spoofing attack. Much attention has been paid to spoofing threat to the GPS since a drone in the USA was captured in Iran in 2011 (Peterson & Faramarzi 2011). Since then, Professor Todd Humphreys from the University of Texas in the USA performed a spoofing experiment via unmanned helicopter and ship in the outdoor, proving a practical risk of spoofing threat against the GPS (Humphreys 2012). Accordingly, a number of studies on anti-spoofing have been conducted. In the Volpe Report published by the U.S. Department of Transportation, anti-spoofing techniques were classified into six categories according to a level of anti-spoofing performance (John A. Volpe National Transportation Systems Center 2001). According to the Volpe Report, anti-spoofing methods are the detection of receiving signal intensity of navigational signal source, the detection of arrival time, antenna polarization detection, inter-verification of consistence with inertial navigation system, incident angle detection, and cryptographic signal authentication. Among them, it is well known that the cryptographic signal authentication shows the best performance. In recent years, a variety of anti-spoofing techniques have been studied and anti-spoofing characteristics according to strength and weakness of each technique, complexity of implementation, and complexity of spoofing attack have been analyzed (Jafarnia-Jahromi et al. 2012).

In order to analyze the threat of spoofing and develop anti-spoofing techniques, it is necessary to develop spoofing test environment where test and evaluation on the

Received Oct 13, 2016 **Revised** Nov 07, 2016 **Accepted** Nov 11, 2016
†**Corresponding Author**
E-mail: hyoungmin.so@gmail.com
Tel: +82-42-821-4463 Fax: +82-42-823-3400

techniques are performed. It is realistically difficult to let spoofing signals to be synchronized with GPS signals and be regenerated and broadcast because it can be a threat to nearby GPS users. Fundamentally, it is illegal to transmit radio frequency (RF) signals in the GPS signal bandwidth and a considerably a large area of test facility is needed in order to prevent influence on other nearby users. In addition, a risk during the test is also existed during GPS signal spoofing process in dynamic tests to reflect operating environments of real user receivers (Kerns et al. 2014). In order to overcome the above limitation, a mobile spoofing device was combined with a GPS receiver to implement a spoofing environment of in-line type (Humphreys et al. 2008). In addition, a commercial spoofing signal simulator that generates spoofing signals using software that controls commercial GNSS simulator has been introduced in markets (Spirent Communications 2013). However, manufacturing a spoofing signal simulator requires a considerable technical skill and cost and purchasing a commercial product also involves a limitation on operation and considerable cost.

Due to these reasons, most studies employ simulation verification using software receivers and simulators (Jafarnia-Jahromi et al. 2012). It is a method of developing an anti-spoofing algorithm after creating simulation GPS signals and simulation spoofing signals at an intermediate frequency level and analyzing anti-spoofing characteristics at software-based receivers (Shepard & Humphreys 2011). Although various algorithms have been investigated using the above method, it cannot evaluate and test anti-spoofing performance at real commercial GPS receivers. Thus, the need to develop a simulation system of spoofing environment to perform anti-spoofing test evaluations at receivers which are currently used at the time of real spoofing threat.

The purpose of the present study is to develop a GPS spoofing environment that produces RF signals. To do this, spoofing and GPS signals were simulated using two GPS simulators and RF inputs were provided to a commercial receiver through cables. The two GPS simulators were synchronized in time and can be run in a single scenario thereby configuring spoofing and GPS signals with a variety of types. A performance of spoofing simulation was verified using a GPS receiver in order to validate the developed spoofing environment. Characteristics of the autocorrelation function at a spoofing environment and anti-spoofing characteristics of signal tracking loop were analyzed using a software-based receiver, and availability of spoofing test environment was verified using a commercial geodetic-grade receiver.

This paper is organized as follows. In Section 2, an algorithm of how to develop a spoofing environment using two simulators is explained. In Section 3, environments of the implemented spoofing simulation are discussed. In Section 4, the availability of the developed spoofing environment is verified using software-based receiver and geodetic-grade GPS receiver. In Section 5, conclusions are presented.

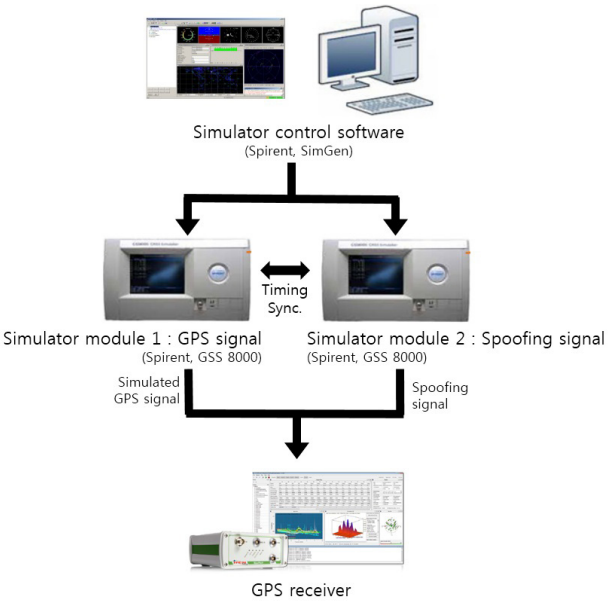

Fig. 1. Conceptual view of spoofing environment using GPS simulators.

2. SIMULATED GPS SPOOFING ENVIRONMENT

GPS spoofing environment refers to an environment that makes a GPS receiver to track spoofing signals instead of GPS signals and thus causes faked positioning results. In order to develop a spoofing environment in outdoor environments, spoofing signals synchronized to real GPS signals should be generated and transmitted to a victim receiver. Although the above method is the closest spoofing environment in reality, it is difficult to be implemented. First, a space shall be controlled not to damage nearby users while generating spoofing signals considering real GPS signals, and it is difficult to broadcast signals in consideration of dynamic characteristics of users.

In the present study, a method of generation of spoofing environment is proposed using two GPS simulators. Since both spoofing and GPS signals can be generated using simulators, user's dynamic characteristics can be simulated and RF signals can be applied to commercial receiver through cables. Hereafter in the present paper, GPS signals

https://doi.org/10.11003/JPNT.2016.5.4.165

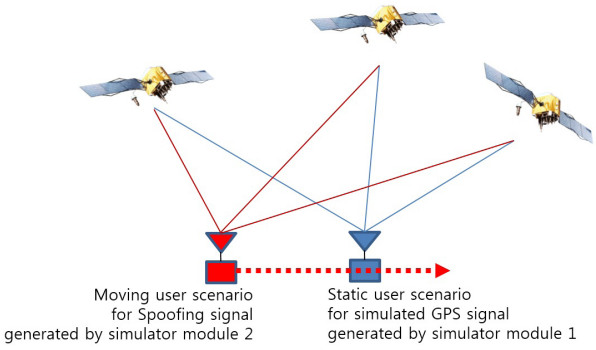

Fig. 2. Conceptual view of simulation scenario for spoofing environment.

simulated in the simulator are called simulated GPS signal and signals simulated as spoofing signal are called spoofing signal. Fig. 1 shows a configuration of the simulator for spoofing environment simulation.

It is more difficult to cope with jamming or rebroadcasting disturbance if signals with stronger intensity are applied to a victim receiver. On the other hand, it is more difficult to cope with spoofing attack if spoofing signals are closer to real GPS signals that are received by victim receivers. This is because the purpose of spoofing attack is to make user receivers to track spoofing signals instead of GPS signals without differentiating real GPS signal and spoofing signal. In order to generate spoofing environment using a device configuration shown in Fig. 1, a scenario in which simulated GPS signal and spoofing signal should be overlapped. Fig. 2 shows an example of scenario that generates a spoofing condition, in which a static user scenario is configured via simulator 1 that generates GPS signals, and a moving user scenario passing through the static user location made by simulator 1 is configured via simulator 2. Assuming that a spoofing-target receiver receives signals from simulator 1 first, spoofing signals from simulator 2 approach gradually to the receiver so that user's receiver cannot distinguish two signals that which signal is originally tracked one. In the meantime, an intensity of spoofing signal is set to an intensity a little bit larger than that of simulated GPS signal so that user's receiver starts to track spoofing signals instead of simulated GPS signal. Fig. 3 shows a conceptual diagram of autocorrelation function of a certain channel in the receiver when two simulator signals in Fig. 2 are inputted to a spoofing-target receiver using RF combiner. Once a user's position simulated at two simulators in the scenario is overlapped, an overlap of autocorrelation function occurs as shown in Fig. 3 in the channel of the spoofing target receiver. Here, spoofing condition can be generated if an intensity of spoofing signal is a little larger than that of simulated GPS signal.

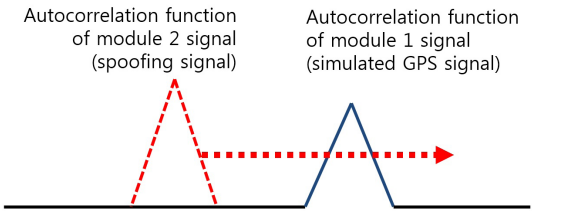

Fig. 3. Conceptual view of autocorrelation function of a certain channel of a victim receiver.

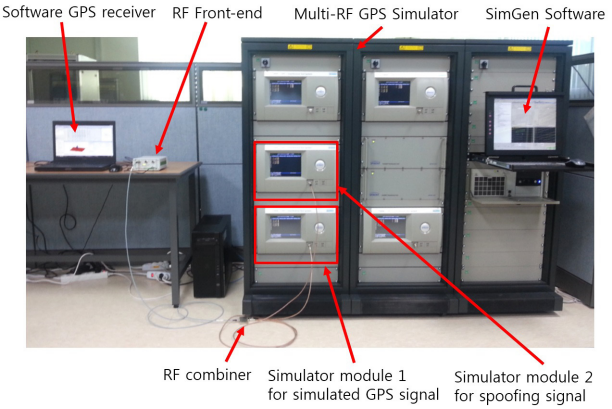

Fig. 4. Implementation of simulated spoofing environment using multiple RF GPS simulators.

3. IMPLEMENTATION OF SPOOFING TEST ENVIRONMENT

Fig. 4 shows an example of implementation of the simulated spoofing environment proposed in the present study. The used multiple RF GPS simulator consists of five modules of GSS 8000 GPS simulator, each of the modules is synchronized with a single clock and controlled by a single scenario operation program (SimGen from Spirent) as shown in Fig. 5 (Spirent Communications 2010). Fig. 5 shows a screen shot of the SimGen software operation from Spirent, in which one shows a control of static user and the other shows a control of moving user in a single scenario simultaneously. This device is a jamming simulation device, which targets an array antenna originally, and it has no spoofing simulation function itself. The device is configured as shown in Fig. 1 and a spoofing environment can be simulated by generating a scenario as shown in Fig. 2. To configure a spoofing environment, two out of five modules were used as a mean to generate GPS and spoofing signals, respectively. Each of the signals generated is applied to the RF input terminal of the receiver using the RF combiner. In order to verify the availability of the implemented spoofing environment, whether a valid spoofing environment is constructed using the software-based receiver is verified as

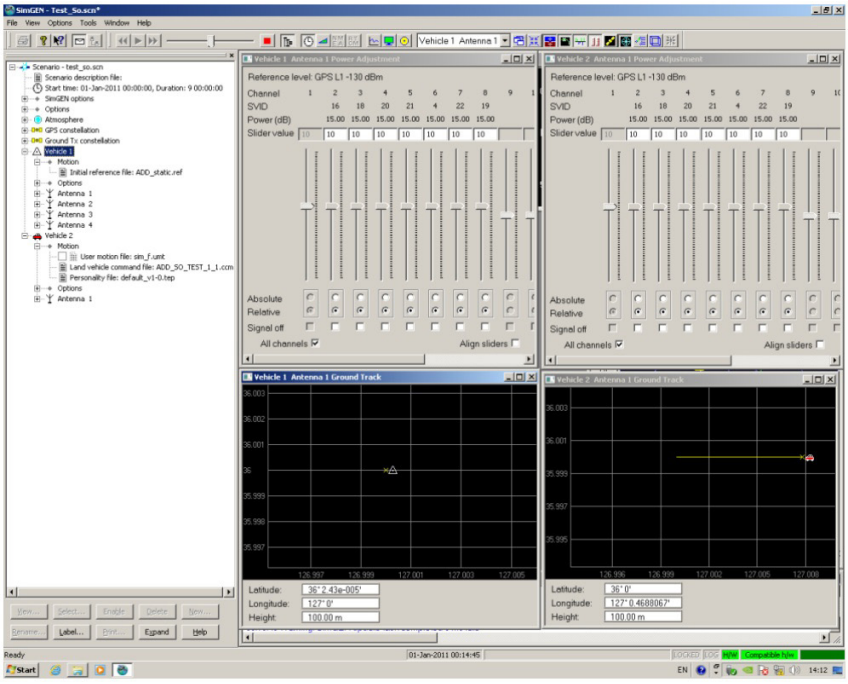

Fig. 5. Screen shot of Spirent SimGen software display which controls two simulator modules in a single scenario.

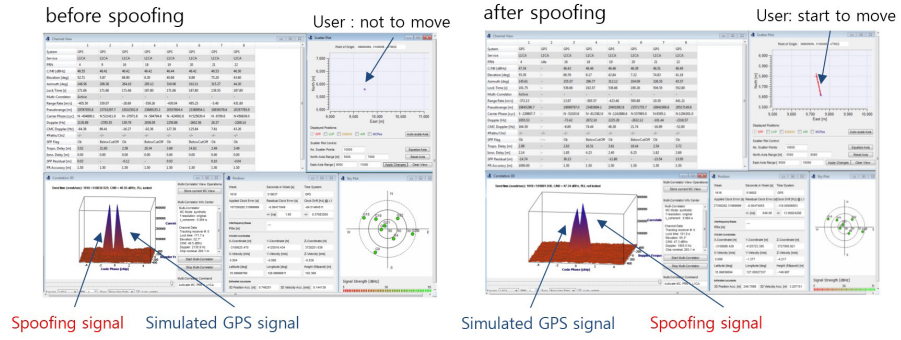

Fig. 6. Verification of simulated spoofing environment using software GPS receiver (left: before spoofing, right: after spoofing).

shown in Fig. 4.

Fig. 6 shows the result of receiving generated signals from the spoofing simulation device at the GPS software receiver. Fig. 6 shows the autocorrelation function and positioning calculation result at a specific channel before and after spoofing. Since the spoofing signal is not overlapped with the simulated GPS signal at the time prior to spoofing in the left side of the figure, the user receiver receives simulated GPS signals normally and shows fixed positioning. At the time after spoofing as shown in the right side of the figure, the signal tracking loop shows a result of tracking spoofing signals instead of simulated GPS signals Here, the positioning result verified the successful spoofing according to the scenario of spoofing signals. The proposed spoofing simulation environment showed valid result as shown in the above.

4. VERIFICATION OF THE SPOOFING TEST ENVIRONMENT

4.1 Configuration of spoofing tests

In order to verify the validation of the spoofing environment implemented in Section 3, a spoofing-target user receiver was linked to test the anti-spoofing performance of the receiver. A scenario used in the test was based on Fig. 2, in which user receiver received simulated GPS signals that simulated static user, and then let spoofing signals that simulated moving

https://doi.org/10.11003/JPNT.2016.5.4.165

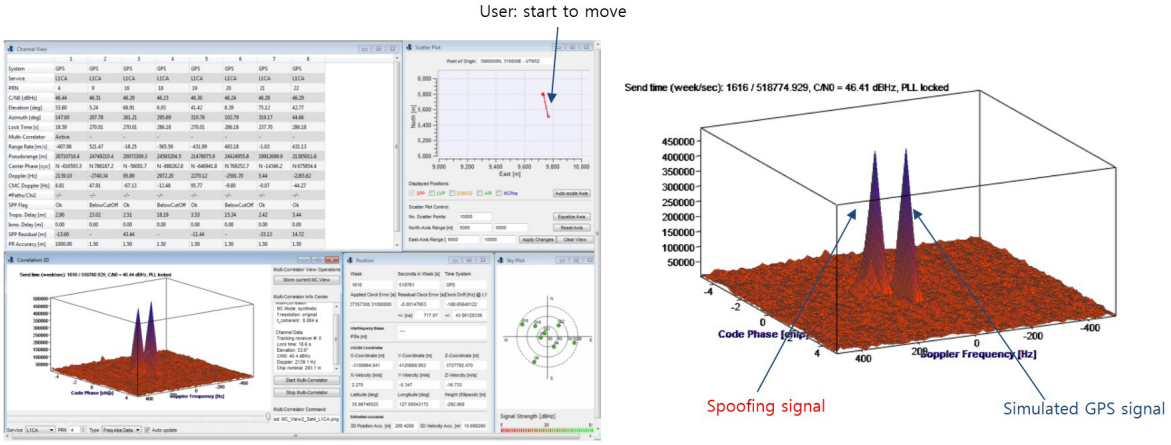

Fig. 7. Results of test 2 (left: screen shot of receiver display, right: enlarged view of autocorrelation function).

Table 1. Test configuration.

	User motion of simulated GPS signal	User motion of spoofing signal	
		Sweeping speed (m/s)	Line of sight Doppler difference for PRN 4 with elevation angle 52° (Hz)
Test 1	stationary	5	8
Test 2	stationary	30	48
Test 3	stationary	200	323

user to pass the position of the static user. About 1 dB higher signal intensity of spoofing signal than that of simulated GPS signal was applied and whether a user receiver was spoofed or not according to a speed that passed through the static user was verified. The test was performed with three cases of a user moving speed: 5 m/s, 30 m/s, and 200 m/s simulated by spoofing signals. It induced a Doppler difference of 8Hz, 48 Hz, and 323Hz in the line of sight direction with regard to PRN 4 satellite at an angle of altitude 52°. The test configuration is summarized in Table 1. For a victim receiver, SX-NSR software receiver from IFEN was employed (IFEN 2014).

4.2 Test results using software receiver

The configurations at Tests 1 and 2 were cases where spoofing signal source was passed through the simulated GPS signal source at a rate of 5m/s and 30m/s, respectively. Since a static state user position simulated by simulated GPS and a moving user position simulated by spoofing signals were overlapped, a code phase at the user receiver was the same at the time where the position of two users is equivalent but a Doppler difference of 8 Hz and 48 Hz occurs for PRN 4 due to the moving speed of spoofing signals.

First, in the configuration of Test 1, a user receiver started tracking spoofing signals instead of simulated GPS signals which were tracked previously thereby being moved to the spoofed position. In the case of Test 2, a user receiver started tracking spoofing signal instead of existing signals despite of about 50 Hz Doppler difference thereby being moved to the spoofed position. Fig. 7 shows a screen shot of operation in the IFEN software receiver, which was used as a spoofing target receiver in Test 2. In the left side of Fig. 7, signal tracking state, autocorrelation function of PRN 4, and positioning result are depicted, in which it showed tracking of spoofing signals as it was started to move from a static condition as shown in the positioning result in the upper right side of the figure. The right side of Fig. 7 shows an enlarged figure of autocorrelation function, in which simulated GPS and spoofing signals that reveal a Doppler difference is verified.

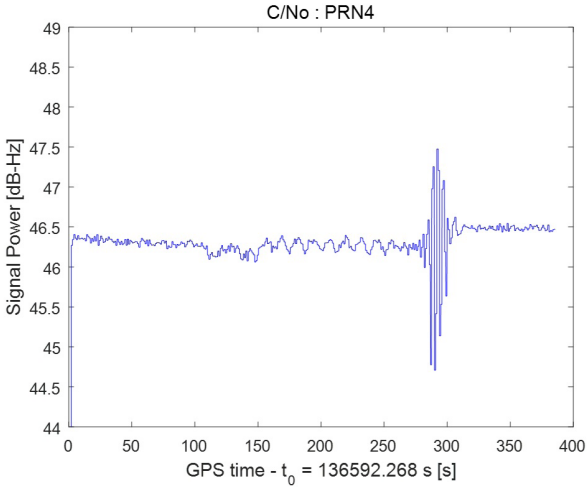

Fig. 8. Measured C/No of PRN 4 signal.

Fig. 8 shows C/No of PRN 4 measured by the spoofing-target receiver during the spoofing process. A large movement of C/No was verified at about 280 sec to 300 sec and since then, signal intensity was increased by about 0.5 dB compared to that prior to 280 sec. This result was

obtained because the spoofing target receiver tracked spoofing signals instead of existing simulated GPS signals after 300 sec. Furthermore, a large movement of C/No at 280 sec to 300 sec was due to effects of reinforcement or offset interference according to phase difference in carrier waves of spoofing signal.

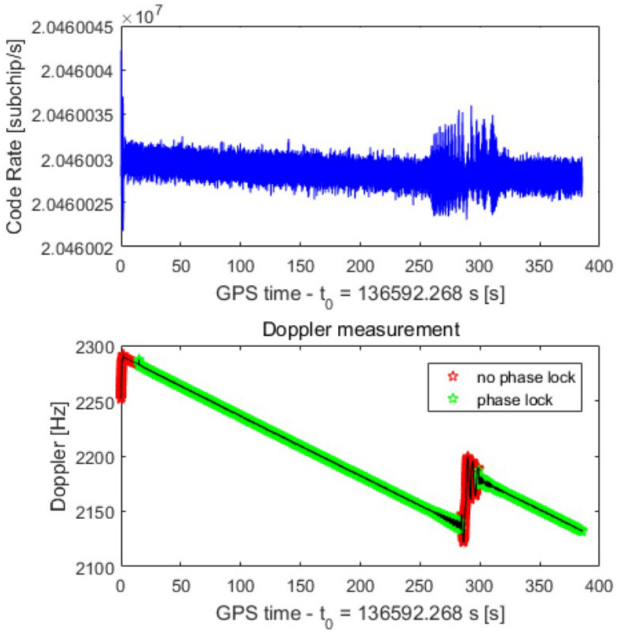

Fig. 9. Code rate measurement (top) and Doppler measurement (bottom) of PRN 4.

Fig. 9 shows code rate measurements and Doppler measurements at the same time with that shown in Fig. 8. In the code rate, an error was induced at the time when spoofing occurred but verified providing continuous pseudo-range measurements. In the Doppler measurement, phase lock loop (PLL) of carrier wave was failed to track a phase temporarily during the spoofing process. In addition, 50 Hz of Doppler shift was verified as it tracked spoofing signals instead of previous simulated GPS signals. An I-Q plot depicted at the right side in Fig. 10, and an frequency lock loop (FLL) discriminator in the lower side and a code delay lock loop (DLL) discriminator in the upper side of Fig. 10 showed that code DLL and FLL in the spoofing process performed signal tracking continuously.

In Test 3, a gap between simulated GPS signal and spoofing signal was shown in the autocorrelation function figure in the left lower side in Fig. 11. As a result, the positioning result at the right upper side in Fig. 11 showed that static condition was maintained continuously as a result of stable receive of simulated GPS signals.

4.3 Test results using geodetic-grade GPS receiver

The test result using the software receiver in Section 4.2 verified that the spoofing simulation environment proposed in the present paper worked successfully. The validity of the spoofing simulation environment implemented using a

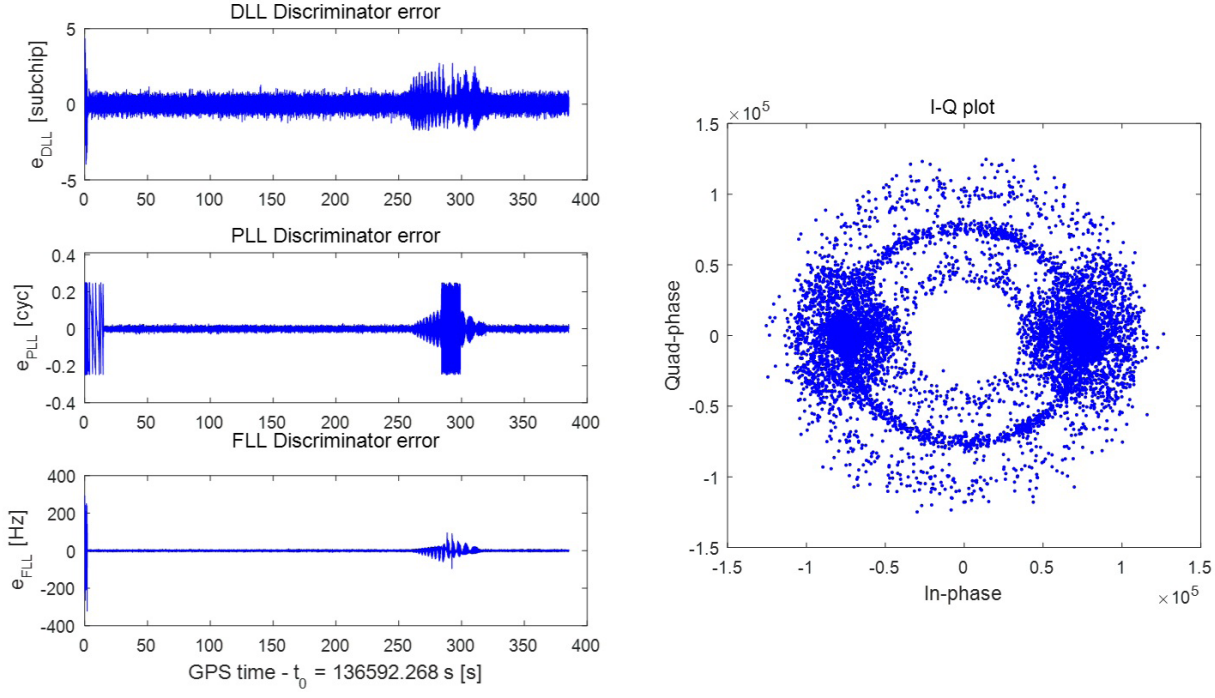

Fig. 10. Discriminator output of code and carrier track loop (left - top: DLL, middle: PLL, bottom: FLL) and I-Q plot (right).

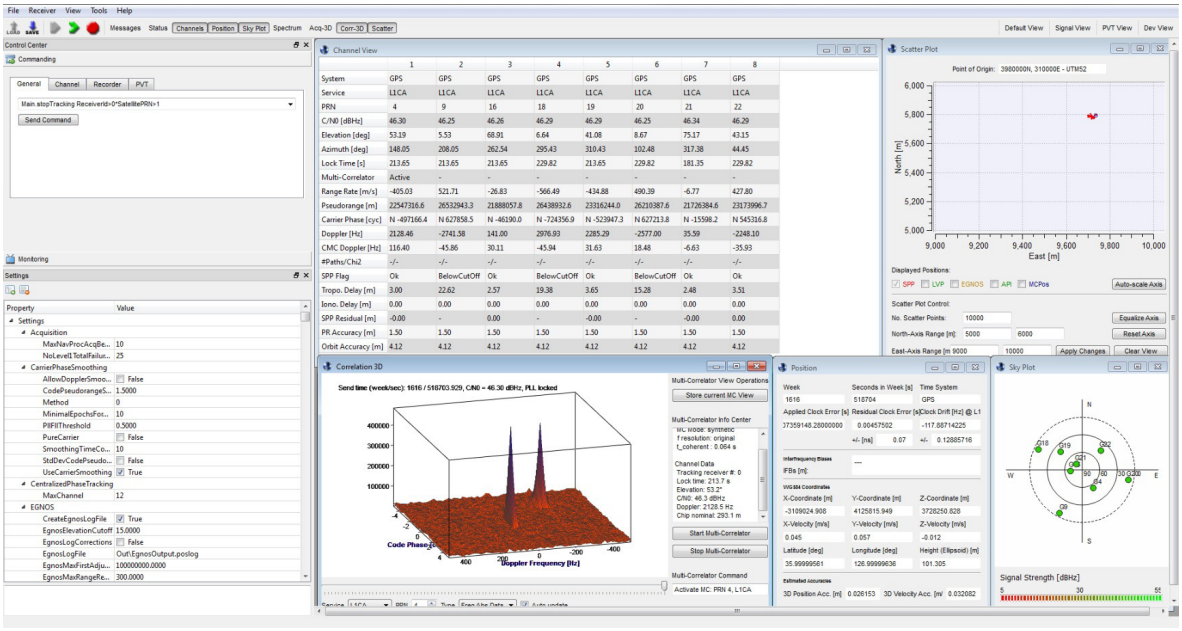

Fig. 11. Results of test 3 screen shot of receiver display.

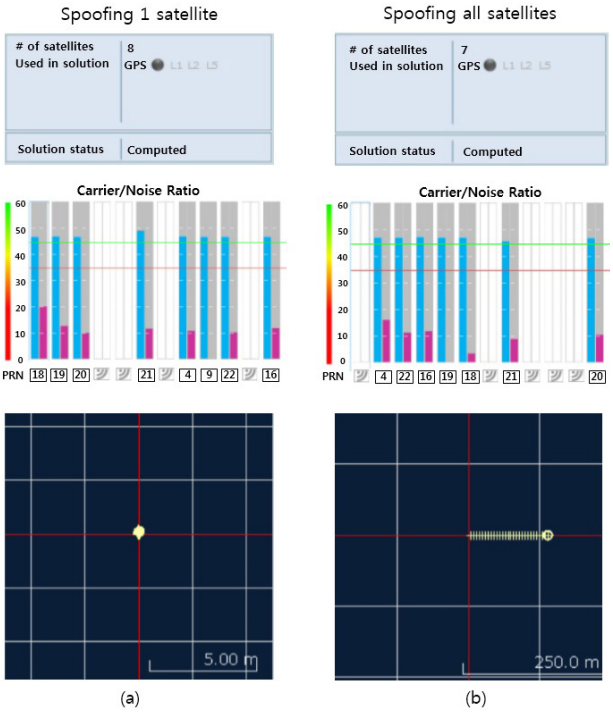

Fig. 12. Spoofing test results of Novatel GPS receiver where (a) is when only one satellite is spoofed and (b) is when all the visible satellites are spoofed (top: navigation status, middle: C/No of each channel, bottom: horizontal positioning results).

geodetic-grade GPS receiver used in real fields was tested. The receiver used was a GPS OEMV receiver from Novatel. The setups in Tests 1 and 2 verified in Section 4.2 were applied without modification. Fig. 12 shows positioning results using the Novatel receiver after applying the setup in Test 2. Fig. 12a shows only PRN 21 is spoofed. In the middle figure of Fig. 12a, PRN 21 has a large C/No value compared to that of other satellite signals. This indicates that the corresponding channel tracked only spoofing signals instead of simulated GPS signal. However, the result of the top positioning state and the bottom horizontal positioning showed normal positioning results with regard to simulated GPS signals. This meant that the abnormality of the corresponding channel was found through receiver autonomous integrity monitoring (RAIM) of the receiver so it was eliminated from the positioning calculation. Fig. 12b shows all visible satellites are spoofed. Given that the bottom positioning results are moved to the right-side direction, it verified that all channels were spoofed. As such, it was verified the implemented spoofing simulation environment can be applicable to a commercial receiver as well.

5. CONCLUSIONS

The present study proposed a method that implemented a spoofing simulation environment in which RF signals were produced using two GPS simulators and verified the method using a receiver. The proposed spoofing simulation method synchronized two GPS simulators and it was run under a single scenario. A spoofing condition can be provided to user receiver by making a scenario, in which

a user position produced by spoofing signals was passed through a user position produced via simulated GPS signals.

The validity of the spoofing simulation environment implemented using software receiver was verified. A spoofing phenomenon, in which a signal source that had a larger signal intensity was tracked once code phase and Doppler of signal in the two simulators were matched, was verified by a method that visualized an autocorrelation function. Furthermore, phenomena such as a large movement of C/No and measurements, Doppler shift, and signal tracking loss of PLL that occurred during the spoofing process were witnessed. The baseband signal processing, which was a basic anti-spoofing method, can detect such phenomena and determine whether spoofing occurred or not. Finally, the validity of the spoofing environment was verified using a geodetic-grade commercial receiver. A geodetic receiver could also not avoid spoofing in the track loop in individual channels. However, anti-spoofing can be achieved through RAIM in the positioning process with regard to incomplete spoofing attack where some parts of all visible satellites were spoofed.

In the implemented spoofing simulation environment, since both of simulated GPS signal and spoofing signal are implemented in a simulator, various dynamic user environments can be simulated and spoofing environment can be provided via RF output, which can be applicable to a performance evaluation tool of arbitrary commercial receivers. In the future, an anti-spoofing level of commercial receivers at more various dynamic environments than the present study will be verified and performances of various anti-spoofing techniques will be tested.

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, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf

Humphreys, T. E., Ledvina B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, Jr., P. M. 2008, Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer, In Proceedings of the Institute of Navigation (ION GNSS 2008), pp.2314-2325, Savanna, GA, USA

IFEN 2014, SX-NSR Navigation Software Receiver User manual (Poing, Germany: IFEN)

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, 2012, 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

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. 2014, Unmanned aircraft capture and control via GPS spoofing, Journal of Field Robotics, 31, 617-636. http://dx.doi.org/10.1002/rob.21513

Peterson, S. & Faramarzi, P. 2011, Exclusive: Iran hijacked US drone, says Iranian engineer [Internet], cited 2011 Dec 15, available from: http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer

Shepard, D. P. & Humphreys, T. E. 2011, Characterization of receiver response to spoofing attacks, in Proceedings of the Institute of Navigation (ION GNSS 2011), Portland, OR, USA

Spirent Communications 2010, GNSS Constellation Simulator Datasheet (Devon, UK: Spirent Communications)

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.