JPNT 4(4), 173-180 (2015)
http://dx.doi.org/10.11003/JPNT.2015.4.4.173

JPNT Journal of Positioning, Navigation, and Timing

Design and Performance Evaluation of GPS Spoofing Signal Detection Algorithm at RF Spoofing Simulation Environment

Soon Lim[1†], Deok Won Lim[1], Sebum Chun[1], Moon Beom Heo[1], Yun Sub Choi[2], Ju Hyun Lee[2], Sang Jeong Lee[2]

[1]Satellite Navigation Team, Korea Aerospace Research Institute, Daejeon 34133, Korea
[2]Department of Electronics Engineering, Chungnam National University, Daejeon 34134, Korea

ABSTRACT

In this study, an algorithm that detects a spoofing signal for a GPS L1 signal was proposed, and the performance was verified through RF spoofing signal simulation. The proposed algorithm determines the reception of a spoofing signal by detecting a correlation distortion of GPS L1 C/A code caused by the spoofing signal. To detect the correlation distortion, a detection criterion of a spoofing signal was derived from the relationship among the Early, Prompt, and Late tap correlation values of a receiver correlator; and a detection threshold was calculated from the false alarm probability of spoofing signal detection. In this study, an RF spoofing environment was built using the GSS 8000 simulator (Spirent). For the RF spoofing signal generated from the simulator, the RF spoofing environment was verified using the commercial receiver DL-V3 (Novatel Inc.). To verify the performance of the proposed algorithm, the RF signal was stored as IF band data using a USRP signal collector (NI) so that the data could be processed by a CNU software receiver (software defined radio). For the performance of the proposed algorithm, results were obtained using the correlation value of the software receiver, and the performance was verified through the detection of a spoofing signal and the detection time of a spoofing signal.

Keywords: GPS spoofing, Spoofing signal detection, Software defined radio

1. INTRODUCTION

GPS was developed for military purposes in the United States, and is a representative global navigation satellite system (GNSS) that can be used throughout the globe. Currently, a GPS modernization project is in progress. Also, GLONASS from Russia has resumed the service through a modernization project, and it can be used throughout the globe. In addition, Galileo from EU and Beidou from China have been developed for service, and thus it is expected that various GNSS signals would be available in the future. As for the GPS L1 C/A signal which is one of the civilian signals provided by GPS, the structure is open to the public, and it has been used in the major industrial fields (e.g., aviation and shipping) and the civilian fields (e.g., personal mobile phone) as well as for military purposes. However, a signal that is open to the public (e.g., GPS L1 C/A signal) could be affected by artificial interference signals such as jamming and spoofing. In particular, unlike jamming which transmits a signal having a large signal power in the frequency band identical to that of a GPS signal, the structure of a spoofing signal is the same as that of a satellite signal, and thus a receiver cannot detect the reception of a spoofing signal. A receiver that has received a spoofing signal obtains wrong positioning information and navigation information by the spoofing signal. Due to this characteristic, a spoofing signal can induce a lot of property damage and casualties in the aviation and shipping fields. Therefore, a receiver needs a function that can determine the reception of a spoofing signal. As for an actual case of damage, there was an incident where an unmanned aerial vehicle from the U.S. Army is thought to have been captured by a GPS spoofing signal in Iran in December 2011 (Inside GNSS 2012). Also,

Received Oct 06, 2015 **Revised** Oct 30, 2015 **Accepted** Oct 30, 2015
†**Corresponding Author**
E-mail: dlatns78@kari.re.kr
Tel: +82-42-870-3971 Fax: +82-42-860-2789

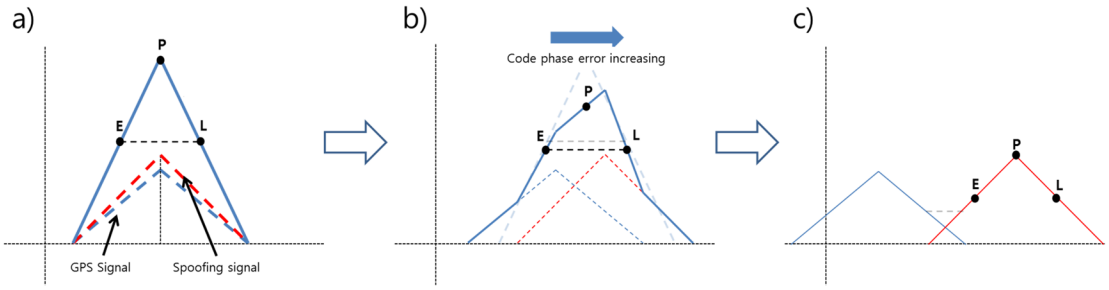

Fig. 1. Effect on a correlation function of a spoofing signal.

in June 2012, the University of Texas in the United States demonstrated a successful capture of an unmanned aerial vehicle with a GPS receiver using a spoofing signal (Inside GNSS 2012).

In this study, the structure and characteristics of a spoofing signal for a GPS L1 C/A signal were introduced along with its effect on a GPS receiver, and an algorithm for detecting a spoofing signal was proposed. Also, the performance of the proposed algorithm was verified through a simulation using an RF signal.

2. STRUCTURE AND EFFECT OF A SPOOFING SIGNAL

2.1 Structure of a GPS L1 C/A Spoofing Signal

A GPS spoofing signal is a mimicking signal of an actual GPS satellite signal. In this study, the GPS L1 C/A signal, which is a civilian signal, was examined. Eq. (1) expresses the GPS L1 C/A signal received by a GPS receiver (Kaplan & Hegarty 2006).

$$s_d(t) = A_d \cdot C(t-\tau_d(t)) \cdot D(t-\tau_d(t)) \cdot cos\{2\pi(f_{L1}+f_D(t))t + \phi_0(0)\} + n_d(t) \quad (1)$$

In Eq. (1), $s_d(t)$ is the GPS signal received at an arbitrary time t, where A_d is the power of the satellite signal, C is the C/A code, and D is the navigation data. τ_d is the phase of the code, and f_{L1} is the carrier frequency of the GPS L1 band (1575.42 MHz). f_D is the Doppler frequency, and ϕ_d is the carrier phase (Kaplan & Hegarty 2006).

$$\begin{aligned} s_d(t) = {} & A_d \cdot C(t-\tau_d(t)) \cdot D(t-\tau_d(t)) \cdot \cos\{2\pi(f_{L1}+f_D(t))t + \phi_0(0)\} \\ & + A_S \cdot C(t-\tau_S(t)) \cdot D(t-\tau_S(t)) \cdot \cos\{2\pi(f_{L1}+f_D(t))t + \phi_0(0)\} + n_d(t) \end{aligned} \quad (2)$$

In Eq. (2), A_S is the power of the spoofing signal, and it is larger than A_d in order to make the target receiver track the spoofing signal. $\tau_S(t)$ is the phase error of the code of the spoofing signal. For a general spoofing signal, it is assumed that the position of a spoofing target receiver is accurately known; and in the early stage where a spoofing signal is received, the value of the code phase error is identical to $\tau_d(t)$ which is the code phase of the actual satellite signal. Then, the spoofing signal increases the code phase error $\tau_S(t)$ so that the target receiver can obtain wrong positioning information (Wen et al. 2005, Jafarnia-Jahromi et al. 2012).

2.2 Effect of a GPS L1 C/A Spoofing Signal on a Receiver

Assuming that the correlation function of a GPS signal has an ideal form without thermal noise and band limitation, the effect of a spoofing signal can be expressed as shown in Fig. 1 (Kaplan & Hegarty 2006). In Fig. 1a, the blue dotted line represents the correlation function of the actual satellite signal, and the red dotted line represents the correlation function of the spoofing signal. When the spoofing signal is received by a target receiver, the correlation function is distorted shown in Fig. 1b due to the code phase error induced by the spoofing signal. As the code phase error increases due to the spoofing signal, the target receiver tracks the spoofing signal with a larger signal power as shown in Fig. 1c (Wen et al. 2005, Jafarnia-Jahromi et al. 2012).

3. PROPOSED DETECTION ALGORITHM OF A SPOOFING SIGNAL

3.1 Principle of a Proposed Detection Algorithm

The detection algorithm of a spoofing signal proposed in this study determines the effect of a spoofing signal by detecting the distortion of the correlation function caused by the spoofing signal as shown in Fig. 1. Assuming an ideal correlation function without band limitation and thermal noise, the Early, Prompt, and Late correlation values of the receiver correlator satisfy the relationship shown in Eq. (3) (Kaplan & Hegarty 2006).

$$x_E = x_L = x_P/2 \quad (3)$$

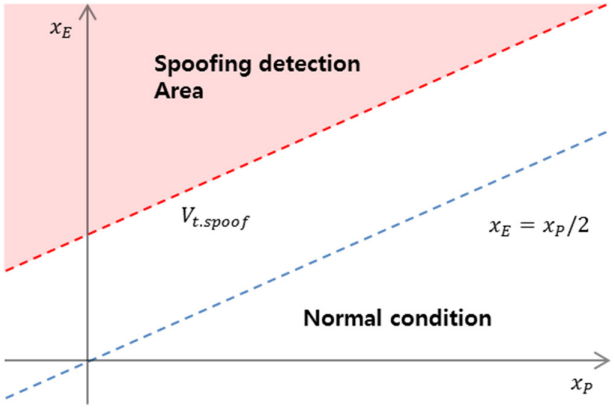

Fig. 2. Detection area of a spoofing signal between early and prompt correlation.

In Eq. (3), x_E, x_P, and x_L are the Early, Prompt, and Late correlation values. When the spoofing signal increases the code phase error as shown in Fig. 1b, the Prompt correlation value decreases further compared to the changes in the Early and Late correlation values. Thus, the relationship in Eq. (3) is no longer satisfied. By detecting this characteristic, the algorithm proposed in this study detects the distortion of correlation function caused by a spoofing signal. Based on the relationship in Eq. (3), the detection criterion of a spoofing signal can be expressed as Eqs. (4) and (5).

$$x_{d.E} = x_E - x_P/2 > V_{t.Spoof} \quad (4)$$

$$x_{d.L} = x_L - x_P/2 > V_{t.Spoof} \quad (5)$$

In Eqs. (4) and (5), $x_{d.E}$ and $x_{d.L}$ are the result values for the Early and Late correlation values. Assuming an ideal correlation function without receiver thermal noise, the values of $x_{d.E}$ and $x_{d.L}$ in Eqs. (4) and (5) become 0.

3.2 Setting of The Spoofing Signal Detection Threshold

Fig. 2 shows the detection criterion with Early correlation value of a spoofing signal in Eq. (4) on a two-dimensional plane. In Fig. 2, the blue line represents the relationship between x_E and x_P for an ideal correlation function, the red dotted line represents the detection threshold of a spoofing signal, and the red area represents the detection area of a spoofing signal. In Eqs. (4) and (5), $V_{t.Spoof}$ is the detection threshold of spoofing signal. Thus, if $x_{d.E}$ or $x_{d.L}$ in Eqs. (4) and (5) is larger than $V_{t.Spoof}$, it is determined that the correlation function is distorted by the spoofing signal. To obtain a detection threshold from Eqs. (4) and (5), a probability density function for the result of the Eqs. (4) or (5) is required. x_E, x_P, and x_L, which are the Early, Prompt, and Late correlation values in Eqs. (4) and (5), have the Rician distribution. Eq. (6) expresses the probability density function of each correlation value using the Rician distribution (Kaplan & Hegarty 2006).

$$p_s(x_Y) = \begin{cases} \frac{x_Y}{\sigma_n^2} e^{-\left(\frac{x_Y^2+A^2}{2\sigma_n^2}\right)} I_0\left(\frac{x_Y A}{\sigma_n^2}\right), & x_Y \geq 0 \\ 0, & x_Y < 0 \end{cases}, \text{Y = E or P or L} \quad (6)$$

In Eq. (6), when Y is E, P, and L, it represents the Early, Prompt, and Late correlation values, respectively. If the Rician K factor satisfies the condition in Eq. (7), it can be assumed that the results of Eqs. (4) and (5) have the Gaussian distribution instead of the Rician distribution (Durgin 2003).

$$K(Rician\ K\ factor) \gg 1 \quad (7)$$

For Eq. (8), the condition that satisfies the Rician K factor can be obtained as an equation for C/N as shown in Eq. (9). Eq. (9) expresses Eq. (8) as an equation for C/N_0 (Kaplan & Hegarty 2006, Lim et al. 2014).

$$\text{K} = \frac{A_Y^2}{2\sigma_Y^2} = C/N \text{ , Y = E or P or L} \quad (8)$$

$$C/N_0 = C/N \cdot \frac{1}{T} = \frac{A_Y^2}{2\sigma_Y^2} \cdot \frac{1}{T} \text{ , Y = E or P or L} \quad (9)$$

To assume each correlation value as the Gaussian distribution from Eq. (9), C/N_0 needs to be more than 43 dB-Hz. In this regard, to assume the Early and Late correlation values as well as the Prompt correlation value as the Gaussian distribution, it needs to be two times larger than 43 dB-Hz; and thus the signal strength was set to 46 dB-Hz in the present study (Kaplan & Hegarty 2006, Lim et al. 2014). Therefore, it can be assumed that the Early, Prompt, and Late correlation values have the Gaussian distribution. Eq. (10) expresses the probability density functions of and that have the Gaussian distribution (Ziemer & Tranter 2009).

$$p_s(x_Y) = \frac{1}{\sqrt{2\pi\sigma_Y^2}} e^{\left(\frac{(x_Y+m_Y)^2}{2\sigma_Y^2}\right)}, \quad Y = \text{d.}E \text{ or d.}L \quad (10)$$

In Eq. (10), when Y is d.E and d.L, it represents the results of Eqs. (4) and (5), respectively. Assuming that the thermal noises of the Early, Prompt, and Late correlation values are independent and have the Gaussian distribution with an average of 0 and a variance of 1, the probability distributions of $x_{d.E}$ and $x_{d.L}$ have the Gaussian distribution with an average of 0 and a variance of 1.25 based on the calculation in Eqs. (4) and (5) (Ziemer & Tranter 2009, Lim

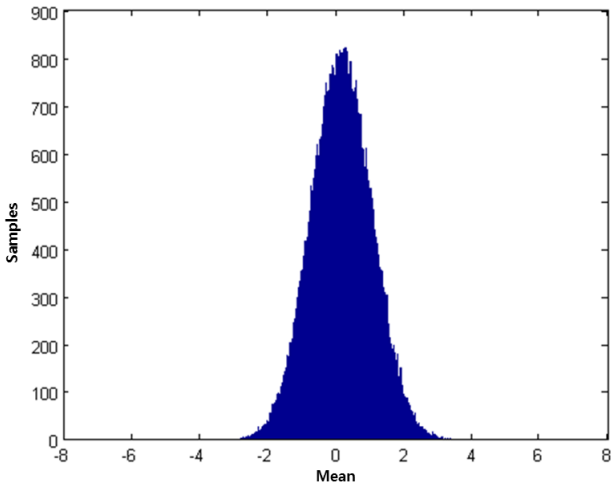

Fig. 3. Histograms of an Eq. (4) result value from RF spoofing signal simulator (Early and Prompt).

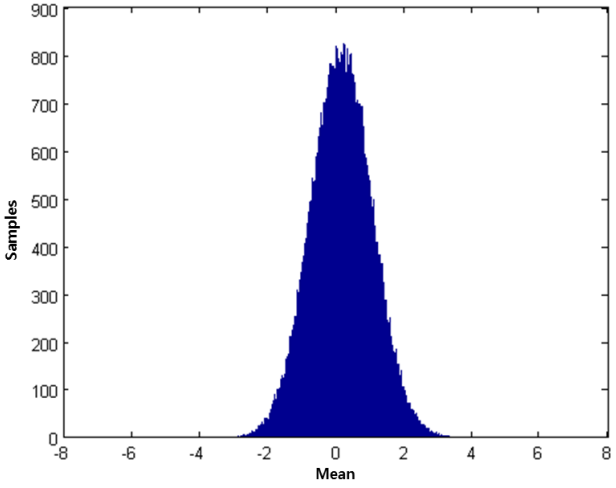

Fig. 4. Histograms of an Eq. (5) result value from RF spoofing signal simulator (Late and Prompt).

Table 1. False alarm probability of spoofing signal detection and a detection threshold.

False alarm probability (%)	Detection threshold
0.1	4.11
0.01	4.85
0.001	5.52
0.0001	6.11

et al. 2014). Figs. 3 and 4 show the histograms of Eqs. (4) and (5) where the signals collected by the GSS 8000 simulator have been processed using the software receiver. As shown in Figs. 3 and 4, the distribution of the data collected by the simulator seems to have the Gaussian distribution, and it demonstrates that the assumption about thermal noise is valid. Table 1 summarizes the detection threshold for the false alarm probability of spoofing signal detection when the average is 0 and the variance is 1.25.

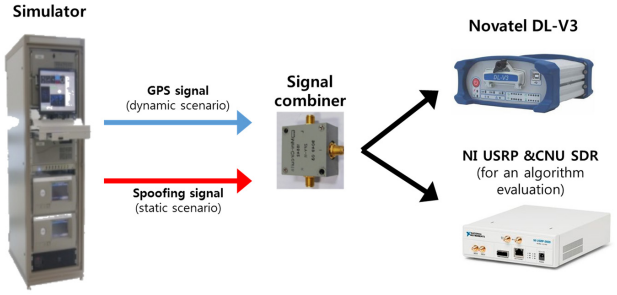

Fig. 5. RF spoofing signal simulation for a proposed algorithm.

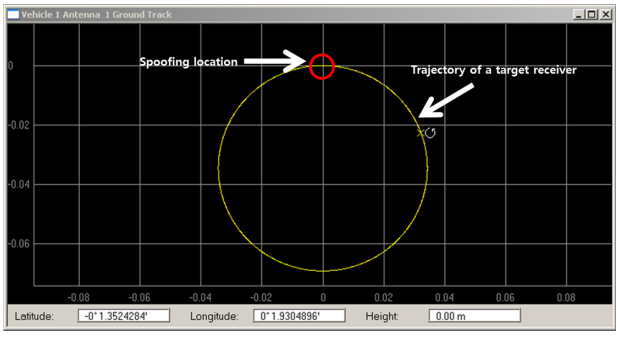

Fig. 6. Dynamic scenario for a target receiver generated by GSS 8000 simulators.

4. SETUP OF RF SPOOFING ENVIRONMENT AND THE PERFORMANCE EVALUATION OF THE SPOOFING SIGNAL DETECTION ALGORITHM

4.1 Setup of RF Spoofing Environment

In this study, an RF spoofing simulation environment was built using two GSS 8000 simulators (Spirent). Fig. 5 shows the RF spoofing simulation environment. As shown in Fig. 5, each GSS 8000 simulator generated signals for a static scenario and a dynamic scenario, respectively. In this study, it was assumed that the spoofing target vehicle moves along a circular trajectory at a uniform speed. Static signals were generated at a latitude of 0, a longitude of 0, and an altitude of 0m, which is the starting point of the circular trajectory, so that they could play the role of spoofing signals. Fig. 6 shows the dynamic scenario of the spoofing target receiver using GSS 8000. The yellow trajectory represents the moving trajectory of the spoofing target receiver, and the red circle represents the spoofing location where the latitude is 0, the longitude is 0, and the altitude is 0m. In Fig. 7, the result was examined using the commercial receiver DL-V3 (Novatel Inc.) to verify the RF spoofing environment. The spoofing signal generated for the verification was 3 dB larger than the satellite signal, and it was received by a target at 1 minute before reaching the location with a latitude of 0, a longitude

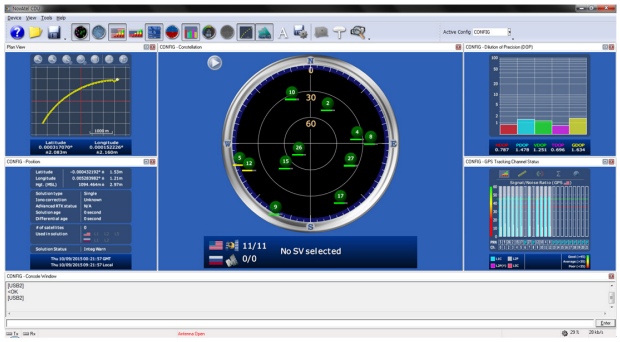

Fig. 7. Verification of RF spoofing signal simulation environment.

Table 2. Evaluation results of a proposed algorithm.

Channel (Satellite ID)	Status	1 dB Detection time (s)	3 dB Detection time (s)	5 dB Detection time (s)
1 (SV 2)	Spoofing detected	25.68	23.03	19.9
2 (SV 5)	Spoofing detected	53.97	52.54	50.67
3 (SV 8)	Spoofing detected	53.37	51.51	49.94
4 (SV 26)	Spoofing detected	9.06	8.85	8.66
5 (SV 10)	Spoofing detected	9.01	8.82	8.65
6 (SV 4)	Spoofing detected	50.17	47.35	46.05
7 (SV 17)	Spoofing detected	20.2	18.21	11.07
8 (SV 12)	Spoofing detected	54.17	51.13	49.73
9 (SV 15)	Spoofing detected	35.46	32.45	29.66
10 (SV 27)	Spoofing detected	45.25	43.18	41.07

of 0, and an altitude of 0m (Lim et al. 2008). The result of the simulation using the commercial receiver DL-V3 (Novatel Inc.) showed that the position was fixed without a change when the spoofing signal was received, as shown in Fig. 7.

4.2 Performance Evaluation of Proposed Algorithm

For the performance evaluation of the algorithm proposed in this study, the RF signal was stored as IF band data using a USRP signal collector (National Instrument), and the performance of the algorithm was evaluated using a CNU software receiver. For the performance evaluation of the proposed algorithm, the false alarm probability of spoofing signal detection was set to 0.0001%, and the speed of the spoofing target vehicle was set to 20 m/s. Then, the effects of the values increased by 1 dB, 3 dB, and 5 dB on the receiver correlator were analyzed, and the relevant performance and characteristics of the algorithm proposed in this study were analyzed. Table 2 summarizes the spoofing signal detection results using the algorithm proposed in this study when the signal strength of the spoofing signal increased for each channel. Based on Table 2, it was found that the proposed algorithm detected the distortion of correlation function caused by the spoofing signal, and that the detection time of a spoofing signal decreased as the strength of the spoofing signal increased.

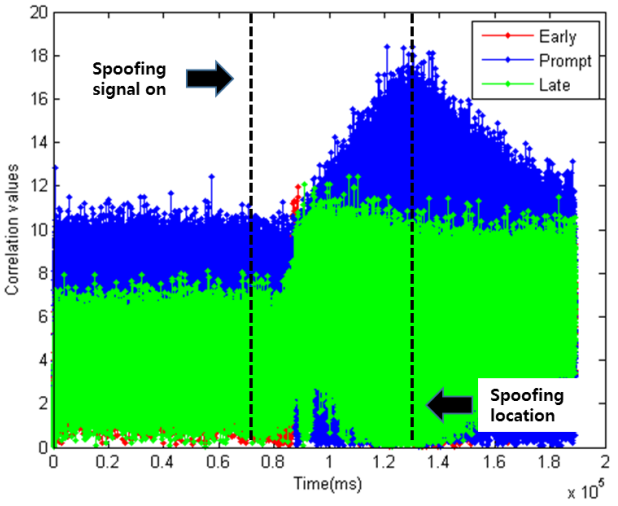

Fig. 8. Correlation values of a target GPS receiver with a spoofing signal (47 dB-Hz).

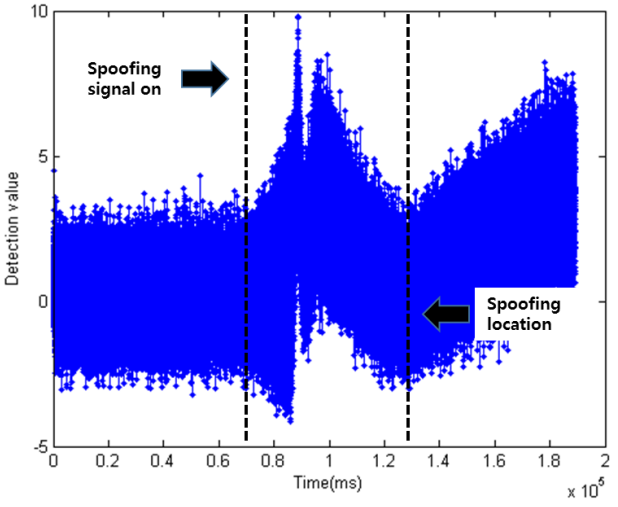

Fig. 9. Result value of Eq. (4) with a spoofing signal (47 dB-Hz).

Fig. 8 shows the effect of the spoofing signal that is 1 dB larger than the satellite signal on the correlation value of the target receiver. The correlation value increased as the spoofing signal was received, and the correlation value showed the highest value when it reached the spoofing location with a latitude of 0, a longitude of 0, and an altitude of 0 m. Figs. 9 and 10 show the results of Eqs. (4) and (5). As shown in Figs. 9 and 10, the value increased as it passed the point where the spoofing signal was received. Based on this, it was found that a correlation function was distorted by the spoofing signal. Fig. 11 shows the spoofing signal detection results using the algorithm proposed in this study. After the point where the spoofing signal was received, the reception of the spoofing signal was determined based on the results of Eqs. (4) and (5). Fig. 12 shows the effect of the spoofing

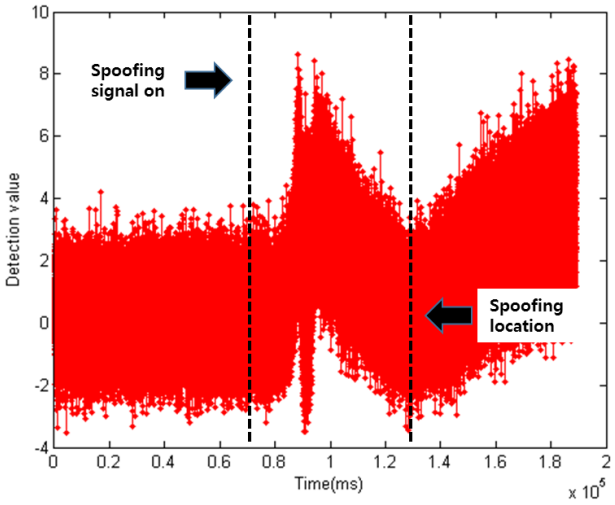

Fig. 10. Result value of Eq. (5) with a spoofing signal (47 dB-Hz).

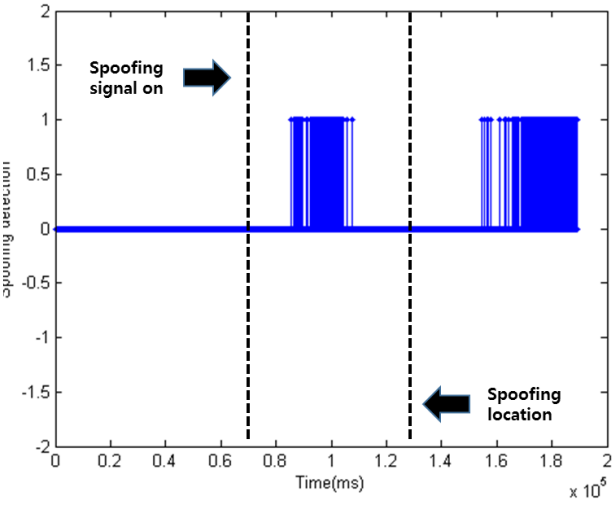

Fig. 11. Spoofing signal detection time of a proposed algorithm with a spoofing signal (47 dB-Hz).

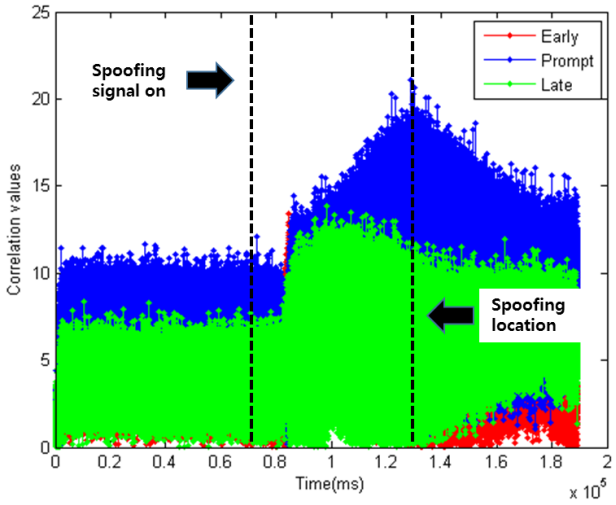

Fig. 12. Correlation values of a target GPS receiver with spoofing signal (49 dB-Hz).

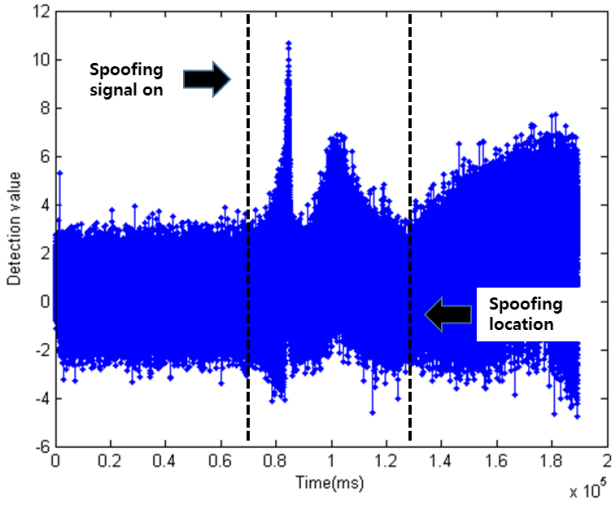

Fig. 13. Result value of Eq. (4) with a spoofing signal (49 dB-Hz).

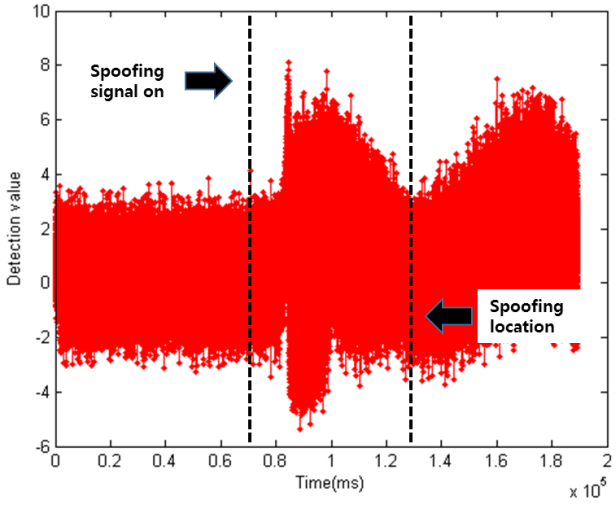

Fig. 14. Result value of Eq. (5) with a spoofing signal (49 dB-Hz).

signal on the correlation value of the target receiver when the spoofing signal was 3 dB larger than the satellite signal. The change of the correlation value were larger than those when the spoofing signal was 1 dB larger than the satellite signal. Figs. 13 and 14 show the results of Eqs. (4) and (5), and Fig. 15 shows the result of the spoofing signal detection algorithm. Fig. 16 shows the effect of the spoofing signal on the correlation value of the target receiver when the spoofing signal was 5 dB larger than the satellite signal. Figs. 17 and 18 show the results of Eqs. (4) and (5), and Fig. 19 shows the result of the spoofing signal detection algorithm. The simulation of this study showed that a correlation function was distorted by the spoofing signal, and that the effect of the spoofing signal could be detected through the proposed algorithm.

http://dx.doi.org/10.11003/JPNT.2015.4.4.173

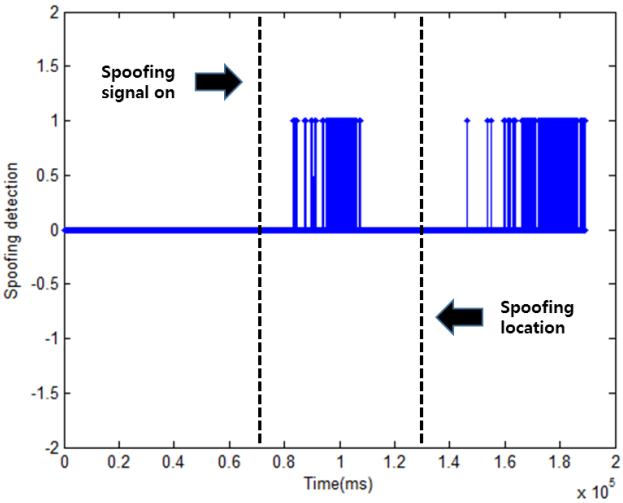

Fig. 15. Spoofing signal detection time of a proposed algorithm with a spoofing signal (49 dB-Hz).

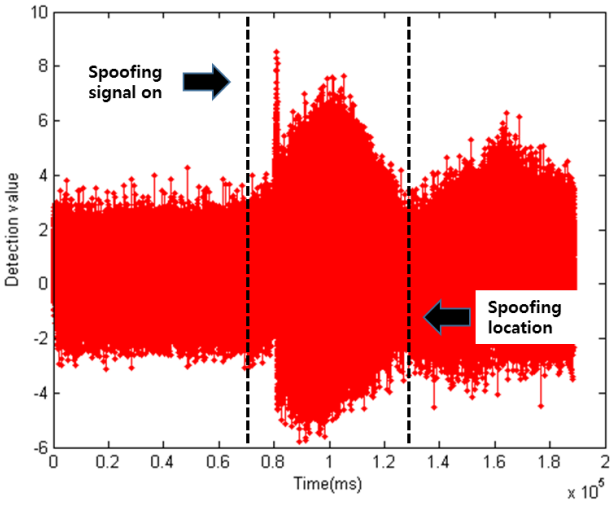

Fig. 18. Result value of Eq. (5) with a spoofing signal (51 dB-Hz).

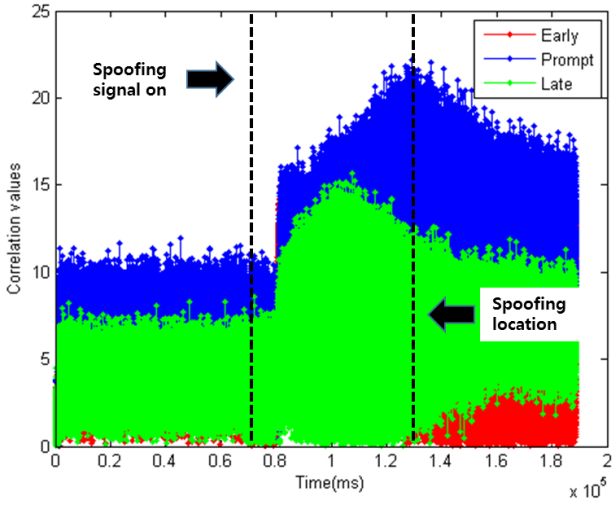

Fig. 16. Correlation values of a target GPS receiver with a spoofing signal (51 dB-Hz).

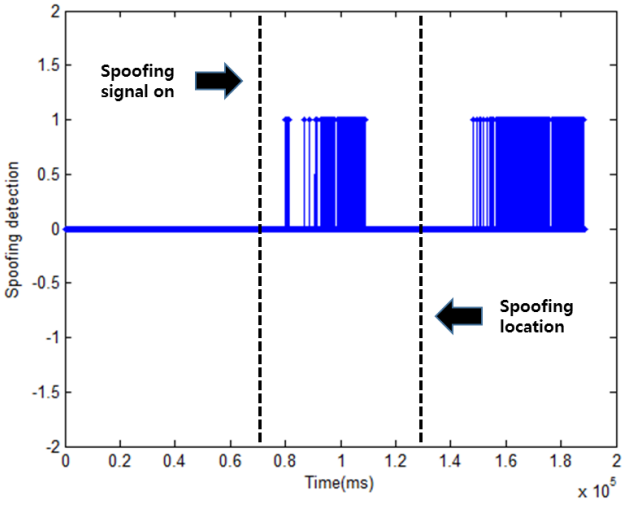

Fig. 19. Spoofing signal detection time of a proposed algorithm with a spoofing signal (51 dB-Hz).

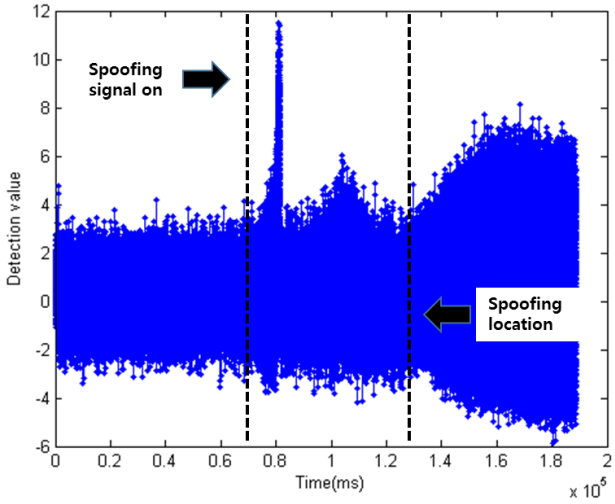

Fig. 17. Result value of Eq. (4) with a spoofing signal (51 dB-Hz).

5. CONCLUSIONS

In this study, an algorithm that detects a spoofing signal for a GPS L1 C/A signal was proposed, and the performance of the proposed algorithm was verified based on GNSS simulation in an RF signal environment. The results of the simulation showed that the proposed algorithm normally detected spoofing signals that are 1 dB, 3 dB, and 5 dB larger than the satellite signal, in an RF signal environment. Also, the detection time of a spoofing signal decreased as the signal strength of the spoofing signal increased. The simulation environment built in this study can be used for the test of existing spoofing signal detection algorithms

as well as the proposed algorithm. In the future, the performance of the algorithm proposed in this study will be compared with those of existing algorithms. In addition, by adding an assumption that the trajectory of a spoofing target vehicle is not accurately known, the effect of a spoofing signal and the characteristics and performance of the proposed algorithm will be analyzed in a more realistic spoofing environment.

REFERENCES

Durgin, G. D. 2003, Space-Time Wireless Channels (New Jersey: Prentice Hall).

Inside GNSS 2012, UAVs Vulnerable to Civil GPS Spoofing [Internet], cited 2012 July 16, Available: http://insidegnss.com/node/3131

Jafarnia-Jahromi, A., Lin, T., Broumandan, A., Nielsen, J., & Lachapelle, G. 2012, Detection and Mitigation of Spoofing Attacks on a Vector-Based Tracking GPS Receiver, in Proceedings of ION ITM, pp.790-800

Kaplan, E. D. & Hegarty, C. J. 2006, Understanding GPS: Principles and Applications (Boston, London: Artech House), pp.221-222.

Lim, S., Lim, D., Heo, M., & Nam, G. 2014, Design of GPS L1 C/A Spoofing Signal Detection Algorithm, Journal of Advanced Navigation Technology, 18, 7-13

Lim, S., Shin, M., Cho, S., Park, C., & Lee, S. 2008, Design of Software-based GPS Spoofing Signal Generator, in Proceedings for ICS08, Seoul, pp.63-64

Wen, H., Huang, P., Dyer, J., Archinal, A., & Fagan, J. 2005, Countermeasures for GPS signal spoofing, in Proceeding of 2005 ION GNSS, pp.1285-1290

Ziemer, R. E. & Tranter, H. W. 2009, Principles of Communications (Hoboken: Wiley)

Soon Lim received the Master's degree in Electronics from Chungnam National University in 2009. He is now working in Korea Aerospace Research Institute. His research interests include GNSS software simulator and anti-spoofing techniques.

Deok Won Lim received the B.S and Ph.D degrees in the Department of Electronics Engineering from Chungnam National University, Korea in 2004 and 2011, respectively. He is now working in Korea Aerospace Research Institute. His research interests include GNSS receiver design and anti-jamming technologies.

Sebum Chun received a Ph.D degree in aerospace engineering at Konkuk university in 2008. His research interests include GNSS, non-linear filter and indoor navigation.

Moon Beom Heo received a M.S. and Ph.D. degrees in mechanical and aerospace engineering from the Illinois Institute of Technology. He is currently a Head of KARI in Daejeon, Korea. His work is focused on Global Navigation Satellite Systems (GNSS).

Yun Sub Choi received the Bachelor of degree in Electronics from Chungnam National University in 2010. His research interests include GNSS receivers and anti-jamming techniques.

Ju Hyun Lee received the Bachelor of degree in Electronics from Chungnam National University in 2011. His research interests include GNSS, anti-jamming techniques and indoor navigation.

Sang Jeong Lee is a professor in the Department of Electronics Engineering, Chungnam National University, Korea. He received B.S., M.S. and Ph.D. degrees from Seoul National University, Korea in 1979, 1981, and 1987, respectively. His research interests include GNSS receiver design and robust control.

http://dx.doi.org/10.11003/JPNT.2015.4.4.173