JPNT 4(2), 57-65 (2015)
http://dx.doi.org/10.11003/JPNT.2015.4.2.057

JPNT Journal of Positioning, Navigation, and Timing

Effect of Spoofing on Unmanned Aerial Vehicle using Counterfeited GPS Signal

Seong-Hun Seo[1], Byung-Hyun Lee[1], Sung-Hyuck Im[2], Gyu-In Jee[1†]

[1]Department of Electronics Engineering, Konkuk University, Seoul 143-701, Korea
[2]Korea Aerospace Research Institute, Daejeon 305-806, Korea

ABSTRACT

Global Navigation Satellite System (GNSS) including Global Positioning System (GPS) is an important element for navigation of both the military and civil Unmanned Aerial Vehicle (UAV). Contrary to the military UAVs, the civil UAVs use the civil signals which are unencrypted, unauthenticated and predictable. Therefore if the civil signals are counterfeited, the civil UAV's position can be manipulated and the appropriate movement of the civil UAV to the target point is not achieved. In this paper, spoofing on the autonomous navigation UAV is implemented through field experiments. Although the demanded conditions for appropriate spoofing attack exists, satisfying the conditions is restricted in real environments. So, the Way-point of the UAV is assumed to be known for experiments and assessments. Under the circumstances, GPS spoofing signal is generated based on the Software-based GNSS signal generator. The signal is emitted to the target UAV using the antenna of the spoofer and the effect of the signal is analyzed and evaluated. In conclusion, taking the UAV to the target point is hardly feasible. To implement the spoofing as expectation, the position and guidance system of the UAV has to be known. Additionally, the GPS receiver on the UAV could be checked whether it appropriately tracks the spoofing signal or not. However, the effect of the spoofing signal on the autonomous UAV has been verified and assessed through the experimental results. Spoofing signal affects the navigation system of the UAV so that the UAV goes off course or shows an abnormal operation.

Keywords: spoofing, UAV, GPS, signal generator

1. INTRODUCTION

To operate an unmanned aerial vehicle (UAV), the position, velocity and timing information that has been obtained from legitimate navigation data provided by the Global Navigation Satellite System (GNSS) is essential. Most UAVs have a basic inertial measurement unit and vision sensor, RADAR, or LIDAR, which aid in the acquisition of navigation results. However, they only provide information on relative measurements, and thus UAV cannot move to a desired target point without GNSS which provides absolute position information. Therefore, UAV has reliable navigation performance when the GNSS information is accurate. However, normal navigation of UAV could be limited due to natural signal noise or artificial signal interference, jamming, and spoofing (Hu & Wei 2009). In particular, as for the spoofing of GPS, military GPS signals are encrypted and thus cannot be changed (Parkinson & Spilker 1996); but civilian GPS signals are unencrypted and unauthenticated, and thus a user can arbitrarily generate or change signals. In other words, using arbitrarily manipulated signals, it is possible to make target UAV deviate from the existing path and to lead the UAV to a target point designated by the spoofer. In recent years, the Federal Aviation Administration announced a plan that the entrance of civilian UAV into the airspace of the United States would be permitted by September 2015, and Amazon has been trying to implement a delivery system using drones. In this situation, spoofing could be a serious problem for the operation of UAV.

Due to this problem, methods for detecting and dealing with spoofing signals have been actively studied. Warner & Johnston (2002) suggested a basic concept of anti-spoofing.

Received May 11, 2015 **Revised** May 25, 2015 **Accepted** May 26, 2015
†**Corresponding Author**
E-mail: gijee@konkuk.ac.kr
Tel: +82-2-450-3070 Fax: +82-2-3437-5235

Spoofing signals can be detected at the code and carrier tracking level within a receiver (Cavaleri et al. 2010), and spoofing signal detection can also be performed through the horizontal arrangement of receiver antennas (Radin et al. 2015).

Due to the increased interest in spoofing, many studies on the spoofing method have also been performed. Humphreys et al. (2008) analyzed the effect of spoofing signals on a single channel. Tippenhauer et al. (2011) suggested a method in which a number of receivers are spoofed at multiple locations depending on the position of a spoofer, and verified the effect of the spoofer signal generation parameter for the satellite-locking takeover of the receiver. In a recent spoofing experiment on commercial UAV, Shepard et al. (2012) performed spoofing by manipulating the code phase, carrier phase, and Doppler frequency through receiving legitimate GPS signals at a spoofer. In a relevant study (Kerns et al. 2014), time-delayed spoofing signals were generated by decoding legitimate GPS signals, and the effect of the time-delayed spoofing signals on UAV was analyzed. As mentioned above, studies on the spoofing of UAV using actual spoofing signals as well as studies on the spoofing method have continuously been performed.

In this study, the effect of spoofing signals on commercial autonomous UAV was examined. In the spoofing experiment mentioned earlier (Shepard et al. 2012), a spoofer received legitimate GPS signals in real time, and spoofing signals were then generated based on the received information. On the other hand, in the present study, spoofing signals for the corresponding experiment time were predicted and generated through a software-based GNSS signal generator using the ephemeris of GPS satellites in the same time zone (Im & Jee 2014), and the spoofing signals were radiated toward commercial UAV through an antenna. In this regard, for proper spoofing, signals with an appropriate strength need to be radiated based on the position, velocity, guidance, and the action against the malfunction of the navigation device for target UAV; but, in practice, a spoofer cannot have information on target UAV, and the adjustment of signal strength is limited. However, in the present study, for the verification of the spoofing experiment performance, the action against the malfunction of the navigation device that could vary depending on UAV was checked in advance, and it was assumed that the waypoints of UAV are known. Based on the given waypoints, spots for the radiation of the spoofing signals were designated. Through this process, it was examined if the spoofing signals can spoof the receiver installed at UAV in a limited condition, and the effect of the spoofing signals on the navigation solution of the receiver was analyzed and evaluated.

2. GPS SPOOFING SIGNAL GENERATION

To examine the effect of spoofing signals on autonomous UAV in this study, GPS spoofing signals were generated using a software-based GNSS signal generator shown in Fig. 1 (Im & Jee 2014). The process of the GPS signal generation is as follows.

First, the geometric relations between the desired

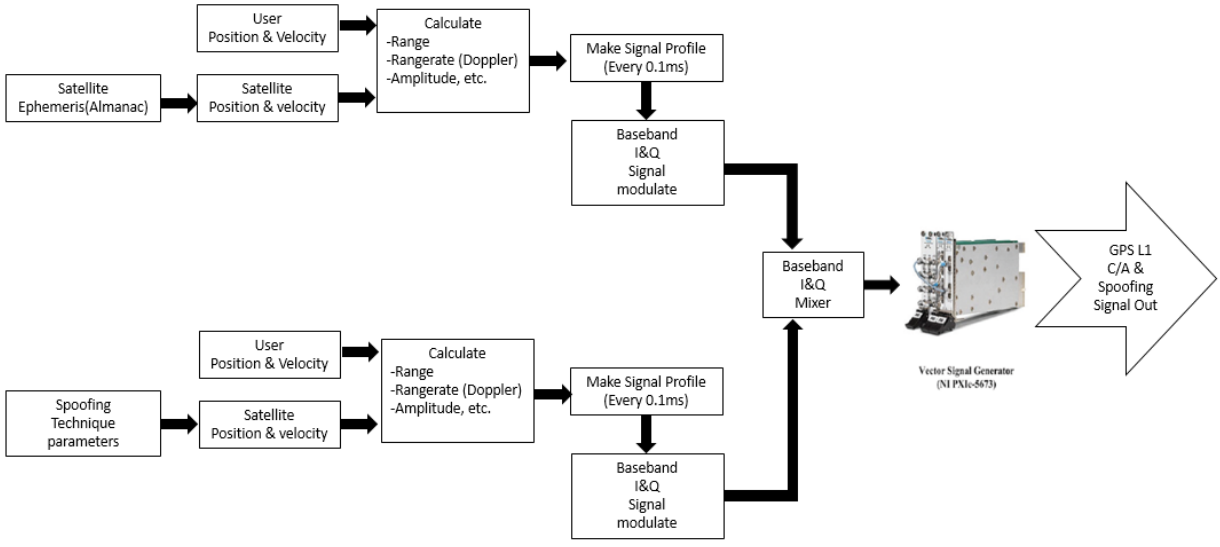

Fig. 1. Structure of a software-based GNSS signal generator.

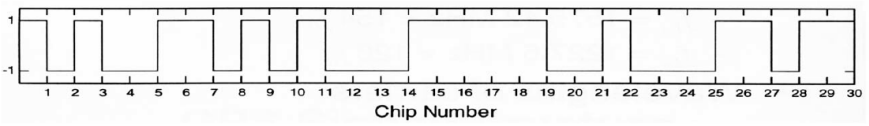

Fig. 2. Pseudo-random noise sequences.

numbers of satellites and receiver are calculated; and for discrete sampling using this, intermediate frequency signals are generated. The generated satellite signals are converted to desirable Radio Frequency signals via Digital to Analog conversion. As GPS signals are generated using discrete samples, the accuracy of the signals is determined by the interval between the samples. For the software-based signal generator used in this study, the code generation accuracy is one over dozens of meters, and the carrier generation accuracy is one over thousands of meters. This corresponds to the levels of a commercial receiver; and to check the accuracy, the generated signals were verified using a commercial GPS receiver.

3. CONDITIONS FOR SPOOFING

For the spoofing of UAV, signals that are the most similar to the GPS signals received by the receiver installed at the UAV need to be generated. A similar signal indicates that it is difficult to distinguish from an existing signal because the code, code delay, and carrier Doppler included in the signal are similar to those of the existing signal. Im et al. (2011) suggested conditions for spoofing depending on the characteristics of the GPS L1 C/A code signal.

The GPS L1 C/A code is a spread spectrum signal using pseudo-random noise. A binary pseudo noise spread sequence that has been designed similar to noise is almost similar to a noise sequence. The generated spread sequence is shown in Fig. 2, and it has an auto-correlation function shown in Fig. 3.

A GPS spoofing signal can spoof a GPS signal when the code delay with a legitimate GPS signal is less than about 1 μs (C/A code chip length). In Fig. 4, the correlation function of a GPS signal is distorted by a spoofing signal. In Fig. 5, a GPS signal is not affected by a spoofing signal when the code delay between the GPS signal and the spoofing signal is more than 1 μs. Fig. 6 shows the output strength depending on the Doppler error. As shown in the figure, a GPS signal is less affected by a spoofing signal as the Doppler error increases. In particular, when it is close to 1,000 Hz, the output strength becomes 0. Therefore, for the spoofing of the receiver installed at UAV, a spoofer should estimate the position of the vehicle within 300 meters, and the Doppler

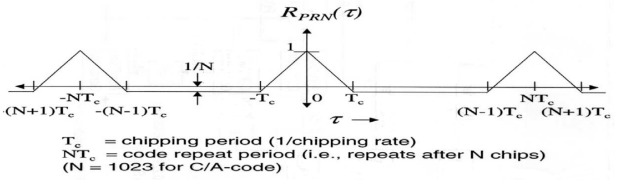

Fig. 3. Auto-correlation function.

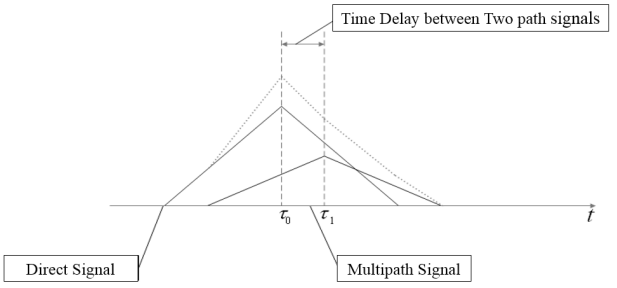

Fig. 4. Cross-correlation with spoofing signal (delay < 1 μs).

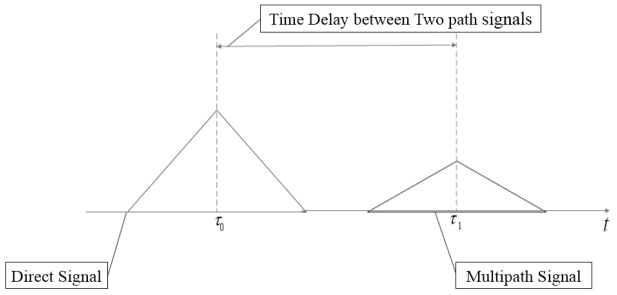

Fig. 5. Cross-correlation with spoofing signal (delay > 1 μs).

within 1,000 Hz. When the signal to noise ratio needs to be considered, a spoofer should have higher estimation accuracies for the position of the vehicle and the Doppler.

Table 1 summarizes the results of the simulation that examined the characteristics of the spoofing signals, and the success of the spoofing was judged based on the Doppler error, the code tracking error, and the strength of the spoofing signal relative to the GPS signal. As shown in the table, spoofing was not successful in most cases. The spoofing was successful when the code sweep rate was 1 cps, which was identical to the code tracking loop bandwidth (=1 Hz), the ratio of the spoofing signal to the GPS signal was larger than 3 dB, and the Doppler offset was smaller than 250 Hz; and when the code sweep rate was 1

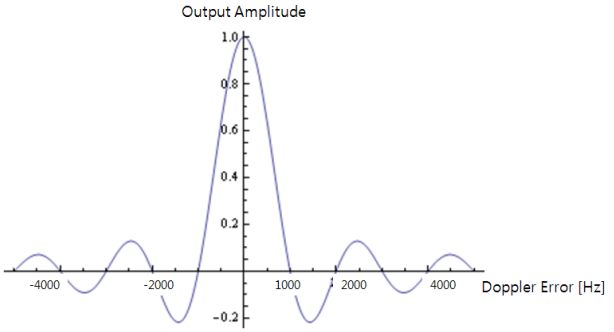

Fig. 6. Relation between Doppler error and correlation power.

Table 1. Spoofing success according to parameters (success: ○, fail: ×).

\ JSR	Sweep rate = 1 cps					Sweep rate = 2 cps					Sweep rate = 3 cps				
	-5	-3	0	3	5	-5	-3	0	3	5	-5	-3	0	3	5
0 Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
25 Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
50 Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
100 Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
200 Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
250 Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
500 Hz	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×
1 kHz	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×

cps, the ratio of the spoofing signal to the GPS signal was 5 dB, and the Doppler offset was smaller than 500 Hz.

When the code sweep rate is 1 cps, the spoofing signal moves 1 chip per second over about two seconds, and thus complete spoofing is possible. However, when the code sweep rate is more than 2 cps, it moves more than 2 chips per second, and thus the code tracking loop with a bandwidth of 1 Hz cannot track the spoofing signal. Accordingly, there is no spoofing.

For complete spoofing, a spoofer should know the guidance and waypoint information of UAV in addition to the aforementioned condition for the similarity between spoofing signal and legitimate GPS signals. If this is not known, the spoofer cannot know which path the UAV would proceed, and thus spoofing signals that lead the UAV to an intended spot cannot be generated.

4. EXPERIMENTAL RESULTS

4.1 Experimental Setup

Fig. 7 shows the configuration for the spoofing experiment. LabSat2 (RACELOGIC limited) is used as a spoofer, and it regenerates signals obtained from the GPS signal generator. Main control PC is connected to LabSat2, and GPS signals are transferred via serial communication,

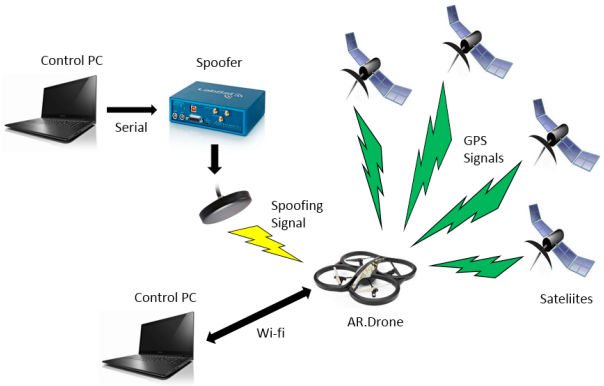

Fig. 7. The experimental setup.

which are then radiated using an antenna connected to LabSat2.

The UAV used in the experiment was the AR.Drone 2.0 quadcopter (GPS chip: SIRF 4) (Parrot SA). As for the navigation of this quadcopter, GPS information is basically used in outdoor environment, and navigation solution is provided using the filtered GPS information that has been generated by combining the GPS information with additional information obtained from an accelerometer, magnetometer, or gyroscope. This filtered navigation solution is the criterion for judging the position of the quadcopter and the arrival at a waypoint. Quadcopter control PC communicates with the quadcopter via Wi-fi. It can perform basic travel commands and waypoint/velocity setting, and can check the navigation information and system status of the quadcopter.

In the normal operation mode, the quadcopter used in this experiment travels along the preset waypoints. If GPS is not normally received or the navigation device malfunctions, it performs hovering at the same spot; and when the emergency status is maintained for 30 seconds, it performs vertical landing at the same spot.

4.2 Experimental Environments

To reduce the error factor (e.g., the multipath of the GPS receiver), the spoofing experiment was conducted in an open sky environment, and the experiment was carried out based on two scenarios. In the first scenario, it was assumed that the spoofer does not know the position of the quadcopter but knows the target point, and it spoofed as if the quadcopter arrived at the target point. As shown in Fig. 8, the waypoints of the quadcopter proceeded in the counter-clockwise direction using the origin of the ENU coordinate system as the starting point. To make the receiver installed at the quadcopter track the spoofing signals at the second

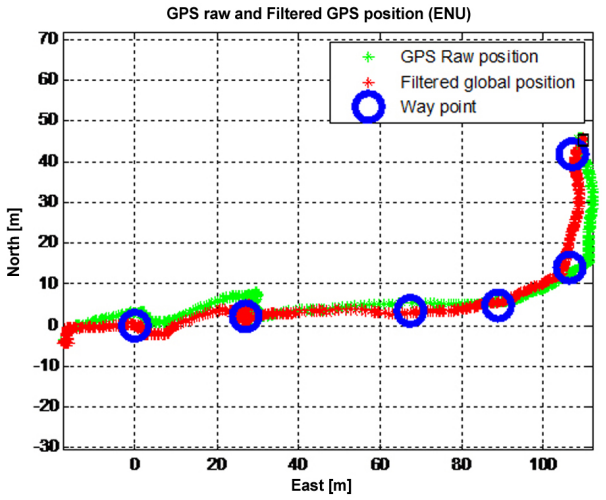

Fig. 8. The UAV trajectory with legitimate GPS signal when spoofer does not know the position of the UAV.

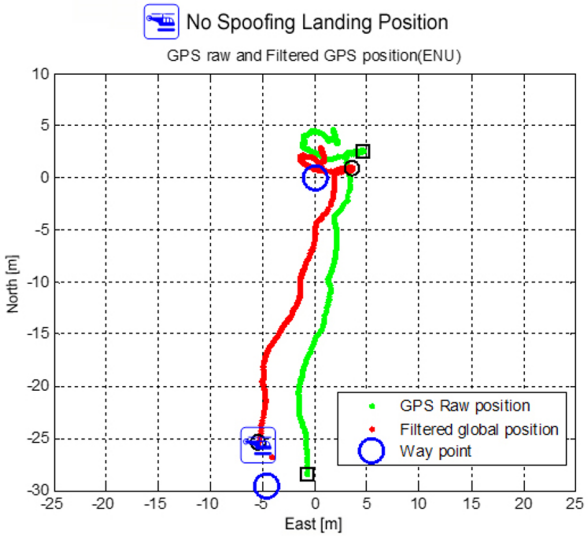

Fig. 9. The UAV trajectory with legitimate GPS signal when spoofer knows the position of the UAV.

waypoint, the quadcopter was set to perform hovering for 60 seconds. To spoof the quadcopter as if it arrived at the target point upon its arrival at the second waypoint, spoofing signals that generate the navigation solution of the last waypoint that is about 100 m apart from the second waypoint were radiated through the spoofer antenna, and the position estimation and maneuver results of the quadcopter were examined.

In the second scenario, it was assumed that the spoofer knows the position of the quadcopter. In this experiment, to make the quadcopter deviate from the normal travel path and move to a spot that is off the final target point, spoofing signal was generated to be gradually changed; and by radiating the signals, the effect of the spoofing signals on the quadcopter was examined. The waypoint for the experiment was established so that the quadcopter would proceed south using the origin of the ENU coordinate system as the starting point, as shown in Fig. 9. At the starting waypoint, the quadcopter received legitimate GPS signals and performed hovering for 30 seconds. At this moment, the spoofer generated signals so that the quadcopter would deviate toward the left side of the waypoint path, and the signals were then radiated toward the quadcopter.

For accurate spoofing to a target position in the above two scenarios, the strength of the radiated signals needs to be adjusted considering the distance between the receiver and the spoofer antenna. However, due to the limitation of the experiment environment, the distance between the spoofer antenna and the receiver was maintained constant as possible, and signals with the same strength were radiated in this experiment.

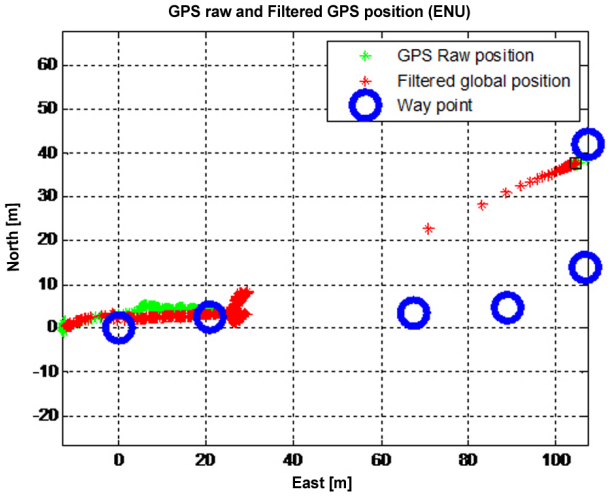

Fig. 10. The navigation system malfunction of the UAV by strong spoofing signal.

4.3 Result-1

Figs. 10, 11, and 12 show the spoofing experiment results for the first scenario. In the case shown as Fig. 10, appropriate strength of the spoofing signals radiated from the spoofer antenna could not be maintained, and the spoofing signals were stronger than the legitimate GPS signals that had been received by the quadcopter. Thus, it functioned similar to a kind of wide-band jammer. At the second waypoint, the receiver installed at the quadcopter entered an emergency status because legitimate GPS signals could not be received due to the malfunction of the navigation device by the strong spoofing signals.

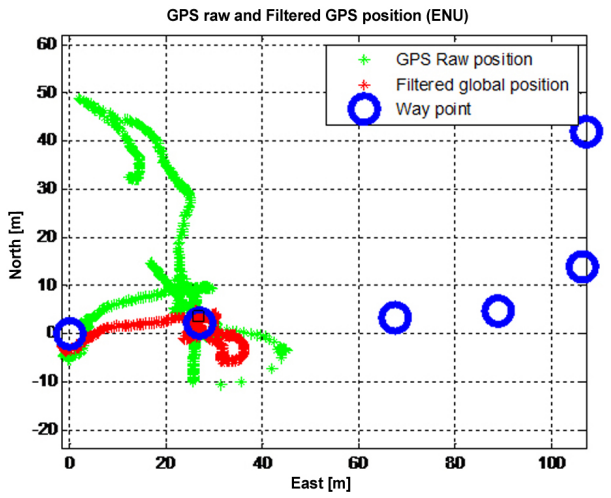

Fig. 11. The navigation system malfunction of the UAV by abnormal navigation solution.

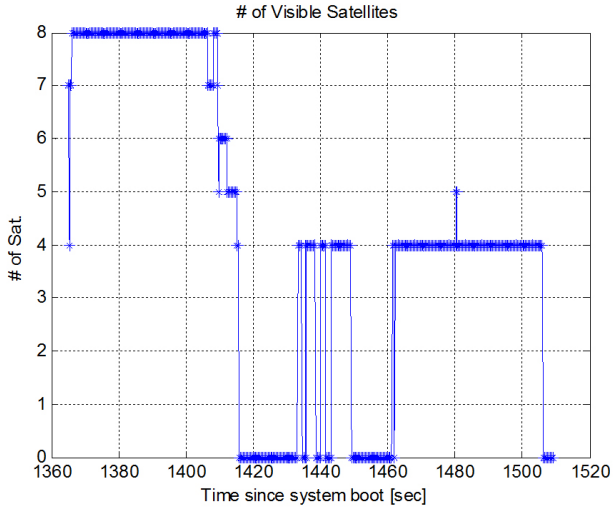

Fig. 12. Number of visible satellites on the receiver of the UAV.

Therefore, it performed hovering for 30 seconds at the same position using the last GPS position information and the inertial sensor, and then performed vertical landing. After the completion of the maneuver by the landing of the quadcopter, the receiver installed at the quadcopter did not judge the malfunction of the navigation device, and thus, the GPS position (GPS Raw Position, GRP) and filtered position (Filtered Global Position, FGP) of the quadcopter moved to the last waypoint intended by the spoofing signals.

Fig. 11 shows the result in which the quadcopter failed normal path travel due to a GPS solution problem after the radiation of the spoofing signals. Fig. 12 shows the number of visible satellites for the receiver installed at the quadcopter in the experiment shown in Fig. 11. During

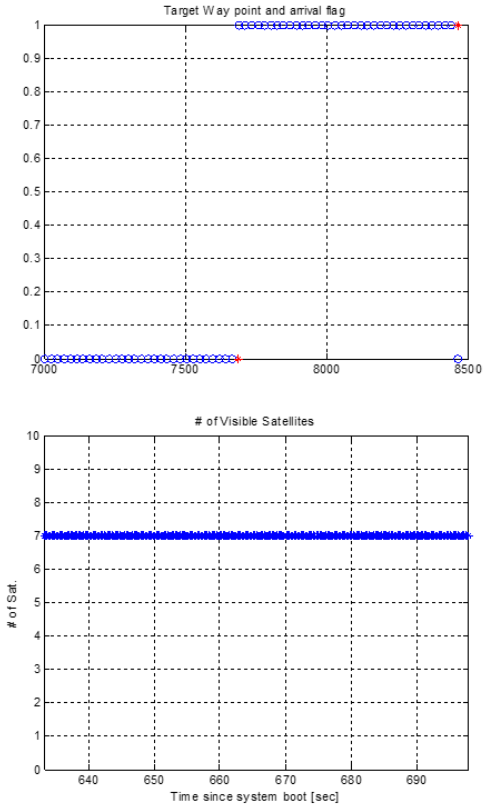

Fig. 13. Way point information of the UAV and number of visible satellites on the receiver (GPS signal).

the normal path travel, the number of visible satellites for the receiver was 8, which was stable; but when the spoofing signals were radiated, the number of satellites was not normally maintained. However, unlike the previous experiment result, the receiver installed at the quadcopter calculated GRP, but the quadcopter judged that the navigation device had not operated normally because the GRP of the receiver was different from the previously calculated legitimate GRP. Thus, it performed hovering in an emergency status using only the inertial sensor, and then performed vertical landing after 30 seconds.

The cause of the GRP miscalculation for the quadcopter cannot be accurately examined because the channel status of the GPS receiver installed at the quadcopter cannot be known. However, considering that the GPS solution of the quadcopter was abnormal but continuously generated, it is thought that normal navigation solution could not be obtained because the spoofing signals could not completely solve the tracking loops of all the channels and thus part of the channels of the receiver installed at the quadcopter tracked the legitimate GPS signals while the remaining channels tracked the spoofing signals.

http://dx.doi.org/10.11003/JPNT.2015.4.2.057

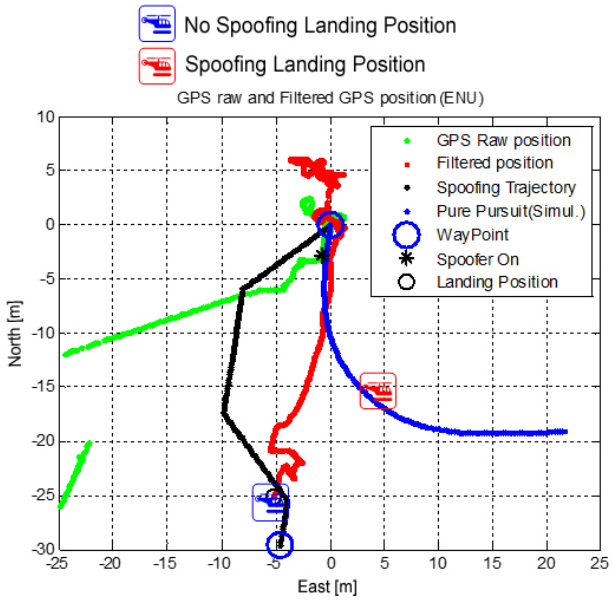

Fig. 14. The UAV trajectory with spoofing signal.

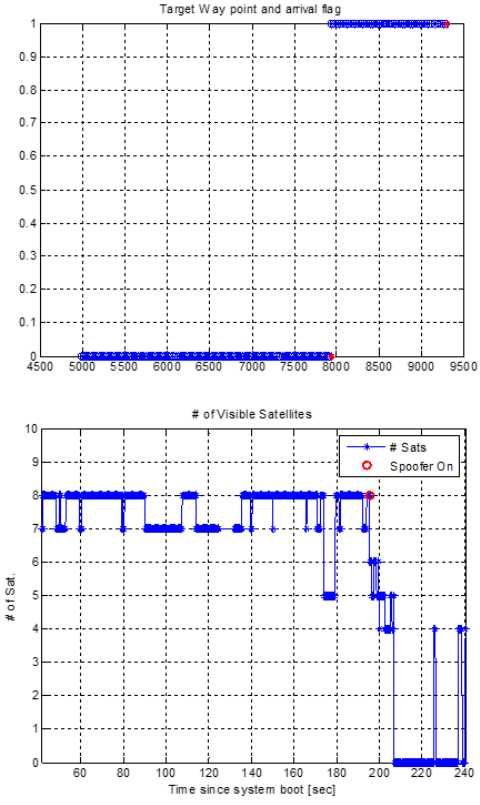

Fig. 15. Way point information of the UAV and number of visible satellites on the receiver (spoofing signal).

4.4 Result-2

Figs. 9, 13, 14, and 15 show the waypoint navigation results of the quadcopter for the legitimate GPS signals and the spoofing signals based on the second scenario. Fig. 9 shows the position estimation with the legitimate GPS signals. For the navigation of the quadcopter, the GRP and FGP had similar trajectories, and the error between the two positions was due to the inertial sensor within the quadcopter. In this case, the number of visible satellites for the receiver was stably maintained as shown in Fig. 13; and through the arrival confirmation flag, the quadcopter perceived that it normally arrived at the target position. Actually, the quadcopter performed vertical landing near the last waypoint. On the other hand, for the navigation result of the quadcopter in the experiment with the radiation of the spoofing signals as shown in Fig. 14, the FGP had a trajectory similar to that of the FGP with the legitimate GPS signals, but the GRP showed a trajectory where it tracked the spoofing signals after the radiation of the spoofing signals, lost the spoofing signals, and then moved in one direction. In this case, the number of visible satellites for the receiver was not maintained constant due to the effect of the spoofing signals as shown in Fig. 15; but through the arrival confirmation flag, the quadcopter perceived that it arrived at the target position. However, in practice, the quadcopter deviated from the set travel path and performed vertical landing in the southeast direction of the target waypoint with a position offset of about 14 m, as shown in the satellite map in Fig. 16.

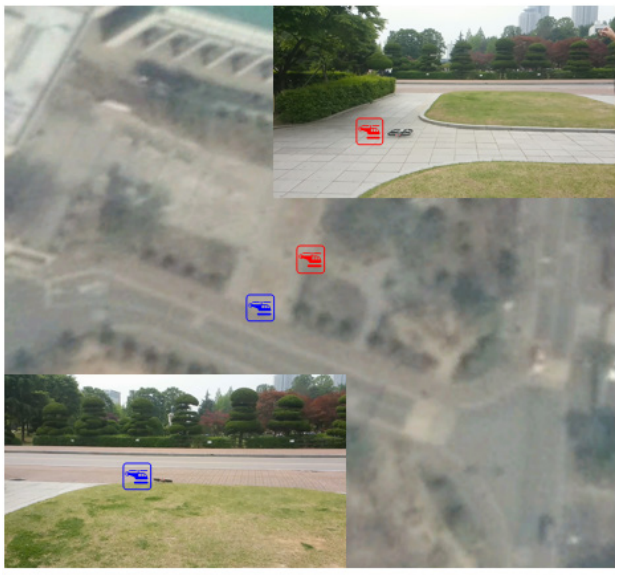

Fig. 16. The true landing position of the UAV.

For accurate analysis of the experiment results, the true position information of the quadcopter is required, but the data obtained from the quadcopter do not provide true position. Therefore, for the analysis of the results, a predicted travel path was generated by applying the Pure

pursuit (Snider 2009) Guidance method to the spoofing signals. As shown in Fig. 14, the predicted travel path of the quadcopter deviated toward the left side of the actual travel path; and if the receiver installed at the quadcopter had not lost the spoofing signals and had tracked all the paths, the quadcopter would have landed more to the left, similar to the simulation result.

5. CONCLUSIONS

In this study, GPS spoofing signals were generated and radiated toward commercial UAV, and the effect of the spoofing signals on the navigation of the UAV was examined.

In the experiment for the first scenario, it was assumed that the spoofer does not know the position of the target UAV, and spoofing was performed so that the UAV would judge that it arrived at the target point. As shown in Result-1, it was found that spoofing could not be normally performed when the strength of the spoofing signals applied to the UAV was not appropriate or when the spoofing signals with an appropriate strength were applied but the navigation device was in a malfunction status due to the internal condition of the receiver and the internal logic of the navigation system. However, normal autonomous travel of the UAV could be hindered as the UAV could not arrive at the target point and judged a malfunction due to the spoofing signals.

In Result-2, it was demonstrated that it is possible to make the UAV deviate from the normal travel path if the position of the UAV and the intended travel path are known, even though the guidance system of the UAV and the spoofing of the receiver are not known. In this regard, the UAV judged that it arrived at the target point by performing normal autonomous travel; but in practice, it landed on an incorrect position. If the travel distance of the quadcopter is longer and the spoofing signals are radiated and tracked for a longer time, the travel path and landing position offsets of the quadcopter would be larger.

In conclusion, for spoofing that accurately leads UAV to a target point, a spoofer should know the position, guidance, and waypoint of the target UAV and the status and internal signal processing method of the receiver installed at the UAV. Based on this, spoofing signals need to be generated so that they can have characteristics similar to those of legitimate GPS signals, and the generated spoofing signals need to be radiated toward the UAV at an appropriate signal strength. However, in an actual spoofing environment, a spoofer cannot know the aforementioned characteristics of target UAV. Based on an experiment, it was found that spoofing is not easy in such a situation, and the causes were analyzed. The results of this study indicated that it is possible to hinder autonomous travel and to make UAV deviate from the target point if the position and waypoint of the target UAV are known, although accurate spoofing of the UAV to an intended spot is not possible.

However, in this study, spoofing of UAV using a low-priced GPS receiver was investigated. For the spoofing of a more precise receiver, studies on more accurate spoofing signal generation and radiation methods are additionally required.

ACKNOWLEDGMENTS

This work was supported by National GNSS Research Center program of Defense Acquisition Program Administration and Agency for Defense Development.

REFERENCES

Cavaleri, A., Motella, B., Pini, M., & Fantino, M. 2010, Detection of spoofed GPS signals at code and carrier tracking level, Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, Noordwijk, 2010, pp.1-6. http://dx.doi.org/10.1109/NAVITEC.2010.5708016

Hu, H. & Wei, N. 2009, A Study of GPS Jamming and Anti-jamming, in 2009 International Conference on Power Electronics and Intelligent Transportation System, Shenzhen, 19-20 Dec 2009. http://dx.doi.org/10.1109/PEITS.2009.5406988

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'hanlon, B. W., & Kintner, P. M. 2008, Assessing the spoofing threat: Development of a portable GPS civilian spoofer, Proceedings of the ION 21st International Technical Meeting of the Satellite Division of The Institute of Navigation, Savannah, GA, 16-19 September 2008.

Im, S. -H., Im, J. -H., Song, J. -H., Baek, S. -W., Lee, I. -W., et al. 2011, Susceptibility of Spoofing On A GPS L1 C/A Signal Tracking Loop, The Journal of Korea Navigation Institute, 15, 32-38.

Im, S. -H. & Jee, G. -I. 2014, Software-based Real-time GNSS Signal Generation and Processing Using a Graphic Processing Unit (GPU), Journal of Positioning, Navigation, and Timing, 3, 99-105. http://dx.doi.org/10.11003/JPNT.2014.3.3.099

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

Parkinson, B. W. & Spilker, J. J. 1996, Global Positioning system: Theory and Applications, Volume 1 (Washington, D.C: AIAA), pp.57-119.

Radin, D. S., Swaszek, P. F., Seals, K. C., & Hartnett, R. J. 2015, GNSS Spoof Detection Based on Pseudoranges from Multiple Receivers, Proceedings of the 2015 International Technical Meeting of The Institute of Navigation, Dana Point, CA, 26-28 January 2015

Shepard, D. P., Bhatti, J. A., Humphreys, T. E., & Fansler, A. A. 2012, Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks, Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation, Nashville, TN, 17-21 September 2012

Snider, J. M. 2009, Automatic Steering Methods for Autonomous Automobile Path Tracking, Tech. report of Robotics Institute, CMU-RI-TR-09-08

Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., & Capkun, S. 2011, On the requirements for successful GPS spoofing attacks, in 18th Proceedings of the ACM Conference on Computer and Communications Security, Chicago, IL, USA 2011, pp.75-86. http://dx.doi.org/10.1145/2046707.2046719

Warner, J. S. & Johnston, R. G. 2002, A Simple demonstration that the global positioning system (GPS) is vulnerable to spoofing, Journal of Security Administration, 25, 19-28.

Seong-Hun Seo received Bachelor's degree from Konkuk University in 2014. He is working for Master's degree on electronic engineering at the same university. He is interested in GNSS receiver signal processing, Software-based GNSS receiver, Anti-spoofing, GNSS precise positioning, etc.

Byung-Hyun Lee received Master's degree from Konkuk University in 2009. He is working for Ph.D. degree on electronic engineering at the same university. He is interested in GNSS receiver signal processing, Software-based GNSS receiver, Anti-jamming techniques, GNSS precise positioning, etc.

Sung-Hyuck Im is a senior researcher in the Korea aerospace research institute. He received Ph.D. degree from Konkuk University in 2011. He is interested in (Real-time) Software GNSS receiver, Generation and processing of navigation signals, Vector-based signal processing, Anti-Jamming/Spoofing, Indoor positioning, Navigation sensor integration, etc.

Gyu-In Jee is a professor in the department of Electronics Engineering at Konkuk University in Seoul, Korea, since 1992. He received his Ph.D. in Systems Engineering from Case Western Reserve University in 1989. His research has been focused on GNSS, autonomous vehicle, and navigation system. He has worked on several research and development project: Autonomous ground vehicle system implementation, Indoor positioning, Software GNSS receiver, IEEE 802.16e based wireless location system, precise GNSS system, etc.