Laboratory Verification Process for Redirection Algorithm Design using GNSS Deception

Myoung-Ho Chae
Agency for Defense Development
Daejeon, South Korea
mhchae@add.re.kr

Seung-Ho Choi
Agency for Defense Development
Daejeon, South Korea
sh_choi@add.re.kr

Chae-Taek Choi
Agency for Defense Development
Daejeon, South Korea
ctmarine@naver.com

Chang-Hoon Lee
Agency for Defense Development
Daejeon, South Korea
leech@add.re.kr

***Abstract*— Recently, anti-drone technology has been rapidly developed to counter illegal drone intrusion. To counter illegal drone, drone redirection algorithm is used with the global navigation satellite system (GNSS) spoofer and drone detection equipment. In this study, to reduce the performance gap between laboratory and field tests, we proposed a validation process in the laboratory to design and verify the drone redirection algorithm from the initial design stage to the equipment integration state before conducting field tests. The proposed process consists of four steps; tuning drone model based on flight test data, simulation in the loop (SITL) test, hardware in the loop (HITL) test using real flight control computer (FCC), HITL test using FCC, GNSS receiver and GNSS spoofer. In the process, two drone models were used, hence each result was compared and verified using a simple modeled drone and a simulator of Micropilot. In addition, through step-by-step verification, the performance of the drone redirection algorithm and system was verified by considering the performance of RADAR, GNSS spoofer, GNSS receiver, and FCC. Through this verification process, it was possible to identify debugging and redesign factors that may occur during the integration stage for each equipment before field testing. Therefore, it was possible to reduce the time and cost of debugging and redesign that could be required in the field test.**

Keywords—Anti-drone, Drone, Redirection, GNSS deception

I. INTRODUCTION

Recently, the demand for technology to prevent intrusion of illegal drones invading core facilities have significantly increased [1–3]. These technologies, named anti-drone technology, consist of hard-kill, which inflict physical damage, and soft-kill, which can suppress without physical damage. The global navigation satellite system (GNSS) jamming and deception are included in the Soft-kill method. Although, GNSS deception requires a more complex design than GNSS jamming, it can be used with low power. Additionally, because it can manipulate GNSS position and velocity mounted on drones, more effective response is possible. However, GNSS deception is possible only on civilian GNSS signals [4–6]. The effects of GNSS deception have been analyzed. And studies have also been conducted on moving drones to safe areas to prevent them from moving in the wrong direction or to avoid accidents in unintended places during GNSS deception. In [7], the analysis of redirection in various types of multi-rotors was conducted using open-source SITL or experiments. In [8], the author verified that the multi-rotor parrot model of AR Drone 2.0 can be redirected to a target position. In [9], a gun-type GNSS spoofer was presented for moving a multi-rotor in a desired direction. A study presented a result of multi-rotor redirection to a target position using open-source SITL [10]. In [11], a control of multi-rotor in a Hover mode using GNSS deception with human-in-the loop control was demonstrated. Performing flight tests in a real environment and designing a redirection algorithm requires a lot of time owing to considerations of weather, test site, and flight time. Therefore, it is necessary to design and verify the redirection algorithm from the initial design stage to the integration stage in the laboratory, and then perform field tests. Many previous studies have performed many tests through simulations using open-source SITL. At this point, if the simulation is performed without considering the performance of the GNSS spoofer, drone detection device, and GNSS receiver mounted on the drone, a large difference may occur from the result of the field test. Therefore, in this study, to reduce this difference, we present a step-by-step laboratory verification process for the design of the redirection algorithm. In our previous study [12], the redirection algorithm and system were proposed and the fixed-wing redirection result was presented through the proposed laboratory verification process, but this verification process was not described in detail. The proposed process for sequential design and verification aims to reduce the redesign and debugging factors as much as possible and to reduce the difference with field test results through the performance verification of the designed algorithm from the initial design stage to the equipment integration stage.

II. REDIRECTION ALGORITHM

Our previous study [12] presented a configuration of GNSS redirection algorithm and system, as shown in Figure 1. The drone redirection system comprised a radar, which can detect the position and speed of the drone, and a GNSS spoofer, which generates GNSS deception signals to make the drone fly in a desired direction. The drone redirection system generates the GNSS deception position and velocity for drone redirection at every step based on radar measurement data in the drone redirection algorithm to change the direction of the drone and fly it to the target position. If the Kalman filter in GNSS spoofer is used, one can obtain the periodic data and use the estimation result of

the Kalman filter in the case of radar tracking loss. As a result, periodic deception path calculation is made possible using the drone redirection algorithm.

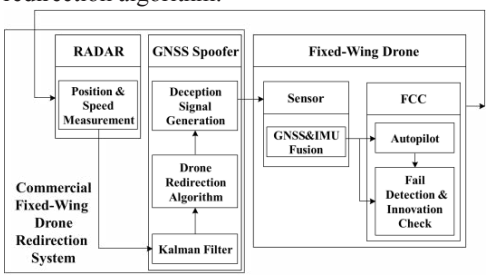

Fig. 1. Configuration of commercial fixed-wing drone redirection system.

Drone redirection algorithm was designed based on two main redirection strategies; Cases 1&2 and Cases 1&3. In the case of Cases 1&2, when compared to Cases 1&3, the probability of drone fail-detection and innovation check detection is lower, and the probability of radar tracking loss is reduced through relatively slow drone flight direction change, but the redirection range depends on the position of the drone's way-point. At this point, in this study, the direction of the drone's path line can be estimated, but the way-point of the drone is unknown; therefore, there is a limitation in that the redirection range cannot be unknown. By contrast, *Cases 1&3* does not depend on the position of drone's way-point. However, *Cases 1&3* may need modification depending on the algorithm of the drone.

III. VERIFICATION PROCESS OF REDIRECTION ALGORITHM

Verification process of designed redirection algorithm in a laboratory was shown in Figure 2.

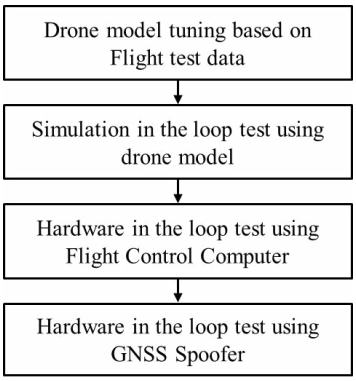

Fig. 2. Verification process of designed redirection algorithm

The proposed process consists of four steps. Drone model tuning is first step in the process. For drone model, several simulators are available from open-source SITL and autopilot companies [12]. To design and verify the drone redirection algorithm using these simulators, it is necessary to tune the drone model of the simulators similarly to the actual flight result of the drone. To tune the drone model for the simulation, the aircraft size, aerodynamic, and thrust coefficient, which are the aircraft information of the drone, are input; the type of the path-following algorithm is selected; the controller structure is tuned, and the control variables and other variables are set in detail. However, except for drones that apply autopilot using open-source code, the information for drone tuning, reference sensor setting for flight control, sensor fusion conditions, and fail-detection conditions are not disclosed. Furthermore, to determine the detailed drone information for drone tuning, it is necessary to use a reverse engineering approach for the target drone. Another approach is to model and use a simple drone model. Using a simple drone model reduces the time required to tune the model based on flight test data as fewer variables are required to tune the drone model. Accordingly, various types of drone models can be created. In this study, a simple drone model and Micropilot's simulator were used as drone models, respectively, and they were tuned based on the flight test results.

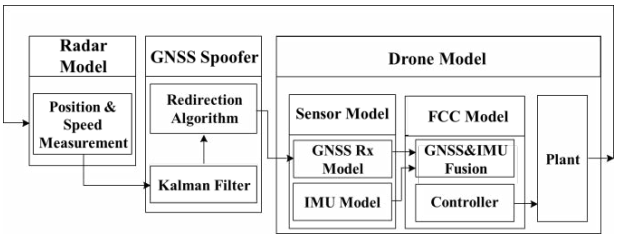

Fig. 3. Test configuration for SITL

The second step is for the software in the loop (SITL) test using the drone model, as shown in Figure 3. The test configuration is based on the configuration of the drone redirection system in Figure 1. In this step, a simple drone model tuned in the first step was used as the drone model. In addition, a radar noise model that models the radar error was used. At this point, to operate only with software, the radio frequency (RF) signal generation, deception signal generation part in the GNSS spoofer, has been omitted. Since this configuration is composed of a closed-loop structure using Radar, it can be used to verify the basic operation of the redirection algorithm according to the presence or absence of Radar error. The accuracy and latency of the GNSS spoofer, the GNSS receiver mounted on the drone, and the flight control computer are not taken into account in this configuration. In the third step, Micropilot's FCC hardware was used for the SITL. If you used an open-source drone model at this stage, you can use an FCC that is compatible with that open-source. Simulation results reflect control delay and characteristics caused by FCC. As shown in Figure 4, the fourth step is to check the integration between the GNSS signal generator and the redirection algorithm, which can be simulated taking into account the accuracy and delay of the GNSS Rx mounted on drones and GNSS spoofer. In this case, a GNSS simulator was used for a simulation of authentic GNSS signals. Therefore, the authentic GNSS signals were generated according to the trajectory of the drone model in real-time.

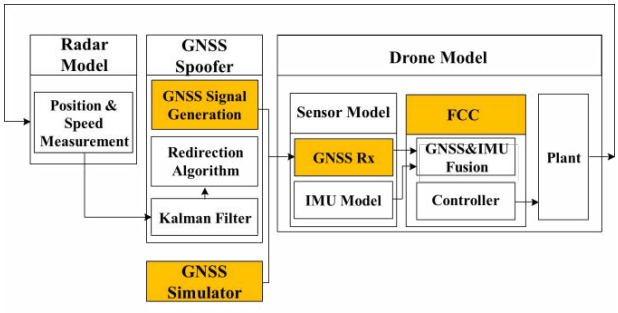

Fig. 4. Test configuration for HITL using GNSS Spoofer and GNSS Rx.

If simple drone modeling was used in second stage, simulation can be operated in non-real time much faster than real time simulator such as open-source SITL. Therefore, if the trend of the results is similar to others, the test can be repeated several times to obtain statistical results or to train a deep learning model. By considering each factor sequentially through the proposed process, it was possible to reduce the time required for debugging or redesign of the algorithm in the field test. Additionally, in the third and fourth steps, it was confirmed that the indirectly designed redirection algorithm can be applied to various drones by implementing and comparing both Micropilot's simulator and simple drone model.

IV. Experiments

As shown in Fig. 5, a simulation result in the fourth step was presented. Micropilot's FCC hardware, Ublox GNSS receiver, GNSS spoofer and GNSS simulator were used for HITL. The minimum goal distance in fourth step was measured at 8.16 m.

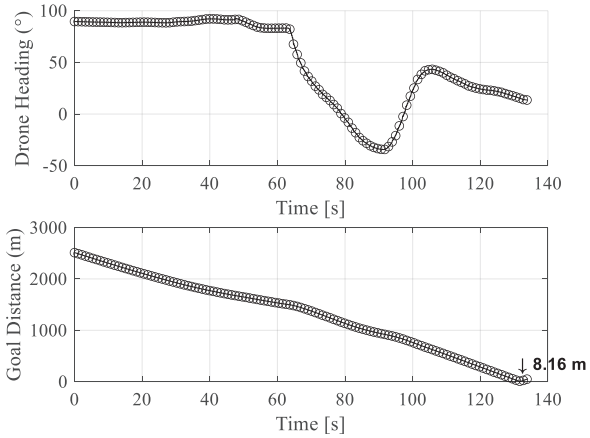

Fig. 5. Simulation Result of HITL using GNSS Spoofer and GNSS Rx.

V. Conclusion

In this study, we presented four methods for verifying the drone redirection algorithm and system via laboratory tests. By sequentially applying each factor to be considered according to each procedure, the factors required for debugging and redesign occurring in each verification process, was identified before the field test.

Acknowledgment

This work was supported by the Agency for Defense Development – Grant funded by Defense Acquisition Program Administration (DAPA) (311JJ5-912967201)

References

[1] C. Lyu and R. Zhan, "Global analysis of active defense technologies for unmanned aerial vehicle," IEEE Aerosp. Electron. Syst. Mag., vol. 37, no. 1, pp. 6–31, 1 Jan. 2022, doi: 10.1109/MAES.2021.3115205

[2] H. Kang, J. Joung, J. Kim, J. Kang, and Y. S. Cho, "Protect your sky: A survey of counter unmanned aerial vehicle systems," IEEE Access, vol. 8, pp. 168671–168710, 2020

[3] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS deception threat and countermeasures," ACM Comput. Surv., vol. 48, no. 4, pp. 1–31, May 2016

[4] Z. Renyu, S. C. Kiat, W. Kai and Z. Heng, "Deception attack of drone," Proc. IEEE Int. Conf. Comput. Commun., pp. 1239–1246, Dec. 2018

[5] D. Shepard, J. Bhatti, and T. Humphreys, "Drone hack: Deception attack demonstration on a civilian unmanned aerial vehicle," GPS World, vol. 23, pp. 30–33, Aug. 2012

[6] S. P. Arteaga, L. A. M. Hernández, G. S. Pérez, A. L. S. Orozco, and L. J. G. Villalba, "Analysis of the GPS deception vulnerability in the drone 3DR solo," IEEE Access, vol. 7, pp. 51782–51789, Apr. 2019, doi: 10.1109/ACCESS.2019.2911526

[7] J. Noh, Y. Kwon, Y. Son, H. Shin, D. Kim, J. Choi, and Y. Kim, "Tractor beam: Safe-hijacking of consumer drones with adaptive GPS deception," *ACM Trans. Privacy Secur.*, vol. 22, no. 2, pp. 1–26, 2019, doi: 10.1145/3309735

[8] D. He, Y. Qiao, S. Chen, X. Du, W. Chen, S. Zhu, and M. Guizan, "A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles," *IEEE Netw.*, vol. 33, no. 2, pp. 146–151, Mar./Apr. 2019, doi: 10.1109/MNET.2018.1800065

[9] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, "A software defined radio based anti-UAV mobile system with jamming and deception capabilities," *Sensors*, vol. 22, no. 4, 2022, doi: 10.3390/s22041487

[10] W. Chen, Y. Dong, and Z. Duan, "Accurately redirecting a malicious drone," *IEEE CCNC*, 2022, pp. 827–834, doi: 10.1109/CCNC49033.2022.9700664

[11] H. Sathaye, M. Strohmeier, V. Lenders, and A. Ranganathan, "An experimental study of GPS spoofing and takeover attacks on UAVs," in *31st USENIX Security Symposium*, 2022, pp. 3503–3520.

[12] M. Chae, S. Park, S. Choi, and C. Choi, "Commercial Fixed-Wing Drone Redirection System using GNSS Deception", *IEEE Trans. Aerosp. Electron. Syst.*, 2023, DOI. 10.1109/TAES.2023.3264193