

보안성 향상을 위한 시나리오 기반 드론 플랫폼 설계 연구

¹김양훈, ^{2*}홍찬기

Designing on Scenario-based Drone Platform to Enhancement Security

¹Yanghoon Kim, ^{2*}Chan-Ki Hong

요약

4차 산업혁명 기술의 융합으로 신산업 드론에 대한 연구가 증가하고 있다. 특히, 정부 정책적으로 4차 산업혁명의 대응책으로 D.N.A 플랫폼으로 지정함에 따라, 해당 플랫폼을 차용한 다양한 시나리오 기반의 연구주제들이 부각되고 있다. 한편, 산업용, 연구용 드론은 관제 운항을 통한 시나리오 기반의 임무를 수행하기 때문에 시분할로 이루어진 공간적 특성을 갖추게 된다. 이에 따라서, 관제 드론 운항 시에는 기존의 보안성을 향상시키기 위한 방법을 다차원적으로 응용할 필요성이 나타났다. 이에 따라 본 연구에서는 보안성을 향상시키기 위한 시나리오 기반의 드론 플랫폼에 대한 연구를 수행하였다. 그 결과 지상 관제시스템, 드론, 드론 데이터 서버의 3분류로 공간을 분류하고 시나리오 기반의 보안기술 적용방안에 대하여 설계하였다.

Abstract

The new industry drone research is increasing through convergence between 4th industrial revolution technology. In particular, the government indicates the D.N.A platform as a countermeasure of 4th industrial revolution. So, the research topics are remarkable which are using D.N.A platform. On the other hand, the drone for industrial and research has spatial factor based on sequential because, they performance scenario-based mission through control operation. When the drone flights as a control operation, they have necessity apply multi-dimensional methods to improve the security level. So, this study researched a scenario based drone platform to improve the security level. As a result, the space classified as a ground control system, drone, drone data server and designed the application method based on scenario security technology.

Keywords: Drone Secure Platform, Monitoring Operation, Drone Operation Scenario, Spatial Characteristics, Drone Security

¹ 신한대학교 사이버드론봇군사학과 조교수(kimyh7902@shinhan.ac.kr)

^{2*} 교신저자 가톨릭관동대학교 의료 IT 학과 정교수(chankih@cku.ac.kr)

Received: Sept. 03, 2021, Revised: Sept. 27, 2021, Accepted: Sept. 27, 2021

I. 서론

4차 산업혁명의 기반기술인 IoT, Cloud, Bigdata, Mobility 를 핵심기술로 하여 기존의 산업을 융합산업으로 변화시키고 있다. 또한, 융합산업 환경에서 기존에 H/W, S/W 의 한계로 인한 문제점이 해결되면서 기존 산업의 강화와 더불어 새로운 산업을 탄생시키고 있다. 특히, 기술의 급격한 발달은 인적자원을 중심으로 진행되는 업무환경에서 무인화된 환경으로 변화시켜가고 있다. 그 예로 자동차 산업에서는 자동화된 조립시스템을 통하여 스마트 팩토리로 발전되어가고 있다[1]. 그중 대표적으로 나타난 신 산업분야에 드론이 있다.

드론은 무인항공기(Unmanned Aerial Vehicles, UAVs)의 세부 분류에 속하며, 고도 150m 이하인 비 관제공역을 비행하는 초경량 비행장치에 대한 다양한 제품과 비즈니스가 개발되고 있다. 그러나 드론은 현재 레저스포츠용을 제외하고는 국방 산업에서 제한적으로 활용하거나 물품수송, 산림 보호 및 감시, 시설물 안전진단, 국토조사 및 순찰, 통신망 활용, 해양 관리, 농업지원, 영상촬영 등 시범사업을 중심으로 진행되고 있는 상황이다[2].

정부에서는 4차 산업혁명의 선도적인 미래 기술개발을 위하여 2017년 11월에 4차 산업혁명 대응계획을 수립하고 데이터(data), 네트워크(network), 인공지능(AI)을 중심으로 D.N.A 정책을 추진해왔다. 이러한 D.N.A 정책을 통하여 개발된 다양한 기술들은 4차 산업혁명 시대 주요산업의 데이터를 인공지능으로 분석하여 최적화된 정보와 서비스를 유·무선 통신망을 통해서 전달하는 형태로 발전되고 있다[3].

이렇듯 정부정책적으로 D.N.A 플랫폼의 한 축으로 데이터, 네트워크, AI의 연계와 활용성에 대하여 제시하고 있지만, 개별 사업과 기술개발 중심의 요소기술에 대한 연구가 이루어지고 있다.

그러나, 초경량 무인 비행장치인 드론은 D.N.A 체계 구조가 일반적인 비즈니스 시스템과 차별성이 있다. 드론의 구조는 프로펠러, 모터, 컨트롤러, GPS(Global Positioning System) 또는 GNSS(global navigation satellite system), 비행제어장치, GCS(Ground Control System), 프레임, 배터리, 각종센서 등으로 구성되어 있다[4]. 드론은 공중에서 임무를 수행하여 데이터를 획득하며, 임무수행을 위한 시간은 주로 배터리의 크기와 비행체의 무게로 결정된다. 드론이 획득하는 데이터는 배터리에 중속된 비행시간과 장소에 따라 변화될 수 있다. 이러한 특성으로 인하여 드론의 데이터 보호에는 공간적 전략 특성을 갖는다 할 수 있다. 근래의 드론 보안성 향상과 관련된 연구들은 드론의 통신, 네트워크 보안을 중심으로 이루어지고 있으며, 공간적 특성을 고려한 드론의 활용 시나리오에 초점을 맞춘 보안성 향상에 대한 연구는 미흡한 상황이다.

본 연구에서는 드론의 특성을 분석하고, 해당 특성에 맞추어 시나리오 기반의 보안성을 향상시킬 수 있는 드론 데이터 연계 플랫폼에 대하여 수행하고자 한다. 구체적으로 선행연구를 통하여 드론에서 활용되는 기존의 네트워크 보안 뿐만 아니라, 드론의 미션 성공과 실질적 안전의 영역까지 확대하여 플랫폼에 대하여 설계하고자 한다. 즉, 기본적인 드론 산업과 드론의 특성, 드론과 데이터 보안의 연계를 고려한 시나리오 기반 플랫폼의 다차원적인 설계를 진행한다.

II. 관련 연구

2.1 드론의 정의와 산업 현황

드론(Drone)은 항공안전법 제 2조 제 3호에서 “ ‘초경량비행장치’란 항공기와 경량 항공기 외에 공기의 반작용으로 뜰 수 있는 장치로서 자체중량, 좌석 수 등 국토교통부령으로 정하는 기준에 해당하는 동력비행장치,행글라이더, 패러글라이더, 기구류 및 무인비행장치 등을 말한다.” 로 규정되어있다. 본 연구에서 드론은 이와같은 정의 중 무인비행장치로 산업용, 연구용을 대상으로 한다.

정부의 드론산업 발전 기본계획에 따르면 드론 기체신고, 사용사업체, 조종자격자 등의 주요지표가 최근 3년간('16~'18) 46~244% 수준으로 증가하고 있는 것으로 나타났다. 또한, Drone Industry Insights 에서는 글로벌 드론 시장에 대해 2025년까지 47.2조 원(약 428억 달러)를 창출할 것으로 예상되며 성장률은 연평균 13.8%로 예상하였다[5].

산업 전반에 걸쳐 드론 채택이 빠르게 진행되어 기업과 조직이 더 짧은 시간에 더 높은 품질과 높은 수준의 안전성으로 많은 양의 데이터를 수집할 수 있게 되고 있다. 드론은 각종 센서와 카메라, 제어 기능을 구비하여, 군용 드론, 상업용 드론, 레크리에이션 드론 등으로 사용된다. 상용 드론은 낮고 느리게 비행할 수 있고 위성이나 항공기보다 더 나은 해상도로 데이터를 수집할 수 있기 때문에 많은 사람들에게 유용한 도구가 되고 있다.

드론 구성은 다양한 애플리케이션과 임무에 맞게 조정된다. 다양한 센서를 운반 할 수 있을 뿐만 아니라 상업용 드론은 로봇 팔, 분무기 또는 디스펜서, 화물(예: 물품 또는 사람)을 운반할 수도 있다. 드론 산업이 확장됨에 따라 최근 몇 년 동안 상업적 사용의 다양성이 크게 증가하고 있다. 국내 드론 제조 산업은 해외 선진국들에 주도권을 빼앗긴 상태에서, 이를 추격하기보다는 다양한 형태의 특수용 드론 제작 및 드론 활용 장치 개발에 주력하고 있다. 향후 드론을 활용한 데이터 및 AI 서비스 시장이 전 세계적으로 크게 성장할 전망이지만, 국내 드론 산업은 이러한 시장에 진입할 기술이 부족하고 투자 또한 미미한 상황이다. 따라서, 드론을 활용한 데이터 및 AI 서비스 시장을 빠르게 선점할 기술 개발 및 투자가 절실히 필요한 시점이다[6].

2.2. 드론 관련 연구 현황

드론에 대한 학술적 연구로는 드론 활용과, 서비스, 안전 등과 관련된 연구들이 있다. 또한, 기술과 비즈니스에 대한 연구도 활발히 진행 중이다.

드론에 대한 기술은 Bigdata 와 A.I.를 활용한 자율운항을 목표로 다양한 요소기술들과 안전한 활용을 위한 보안기술이 주를 이루고 있다. 자율운항에는 기본적인 소재 연구와 항공역학을 중심으로 한 운항 S/W 및 H/W 기술들이 있다. 그리고 보안기술에는 네트워크보안, 드론보안(안전) 등이 주를 이루고 있다[1, 7, 8].

또한 드론 기술에 대한 연구 외에 활용하는 비즈니스에 대한 연구도 활발히 진행중에 있다. 스마트 물류에 보안 및 안전과 관련된 연구, 군 보안과 관련된 국방 산업의 활용과 안전에 관한 연구 등이 진행 중이다[9, 10]. 특히, 드론에 대한 활용은 국방산업에서 오래전부터 진행되어왔기 때문에 항공산업 관련된 다양한 연구들이 진행중에 있다.

III. 보안성 향상을 위한 드론 플랫폼 설계

3.1 산업 및 연구용 드론 활용 시나리오 설계

드론 활용 시나리오는 국내 드론 운항 10년 이상 전문가 5인을 대상으로 공간적 특성을 기반으로 조사하였다. 공간적 특성을 적용하기 위하여 임무중심의 관제 비행을 수행하는 전문가들을 대상으로 하였다. 그리고 시야 내 비행으로 스포츠, 놀이 등을 위한 드론 운항을 제외하였다. 조사한 공간에 대하여 임무계획, 관제비행, 드론운항, 데이터 저장/분석, 데이터 활용으로 구성된 5개로 구분하였으며, 각 공간의 연계와 주요 기능을 그림 1과 같이 설계하였다.

첫 번째 공간으로 임무 중심의 산업 및 연구용 드론의 운항은 임무 계획에서부터 시나리오가 시작된다. 풍향, 풍속, 온·습도 등 당일의 기상상태부터 드론의 정비와 배터리의 상태를 고려한 임무 수행범위까지 계획을 수행한다.

두 번째 공간으로 임무 중심의 관제 비행을 수행할 수 있는 최적의 지점에서 지상 관제 시스템 등을 활용하여 드론을 운항한다. 지상 관제 시스템은 드론 운항에서 수집되는 데이터들의 저장과 원격지의 드론 데이터 저장/분석 서버에 데이터를 전송하는 역할을 수행한다.

세 번째 공간으로 드론 운항시에 사전에 설계한 임무를 중심으로 다양한 데이터를 수집하고, 관제 비행 공간의 지상 관제 시스템에 데이터를 전송한다.

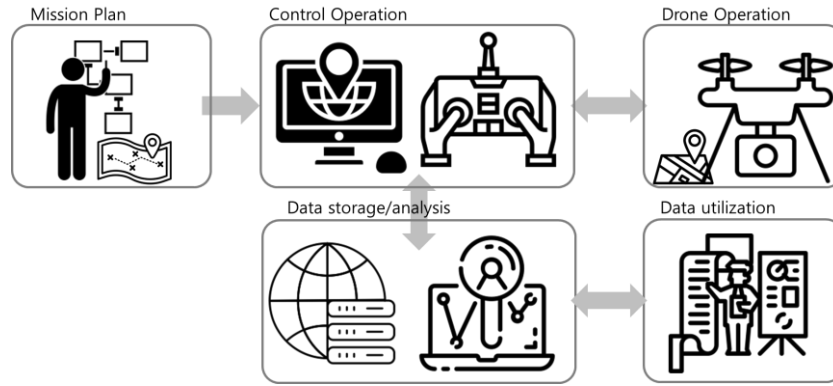


Figure 1. Drone Utilization Scenario Design
 그림 1. 드론 활용 시나리오 설계

네 번째 공간으로 수집된 다양한 데이터에 대하여 데이터의 저장, 정제, 가공, 분석을 수행하고 다섯 번째 공간인 데이터 활용을 수행한다.

3.2 드론 플랫폼 설계

드론활용 시나리오와 선행 연구를 기반으로 보안성 향상을 위한 드론 플랫폼은 그림 2 와 같이 3 개의 분류로 축약, 설계하였다. 분류에 대한 기능을 살펴보면, 비시야 거리에서 관제 드론 운항에 중심이 되는 지상관제시스템, 미션 계획에 따라 임무를 수행하며 다양한 데이터를 취득하는 드론, 모든 데이터에 대하여 저장, 가공하고 분석 및 활용하는 드론 데이터 서버로 구분된다.

지상 관제 시스템은 플랫폼을 기반으로 한 드론 운항에 핵심이 되는 부분으로써 임무중심 운항을 위한 미션 계획 기능, 드론으로부터 수집되는 데이터 수집 및 실시간 조합기능, 수집 데이터와 조합 데이터를 통해 관제를 수행하는 모니터링 기능, 드론수집 데이터에 대한 상황분석과 이에 대한 운항의 변화를 위한 물 기반 이벤트 처리 기능, GNSS 기반의 지도 기능이 있다.

드론은 IoT, 센터 등으로 이루어진 외장장치로 구성된 페이로드 기능과 드론의 모터, 프로펠러 등과 연관된 구동부, Flight Controller 등 드론 전체 시스템을 제어하는 제어부, 지상 관제 시스템 또는 멀티 드론들과 통신을 수행하는 통신부로 구성된다.

드론 데이터 서버는 드론으로부터 수집된 데이터가 지상 관제 시스템을 거쳐서 동기, 비동기 형태로 전용 서버에 저장/가공된다. 그리고 Bigdata 를 형성하여 다양한 데이터 분석/활용을 위한 사용 기능으로 구성된다.

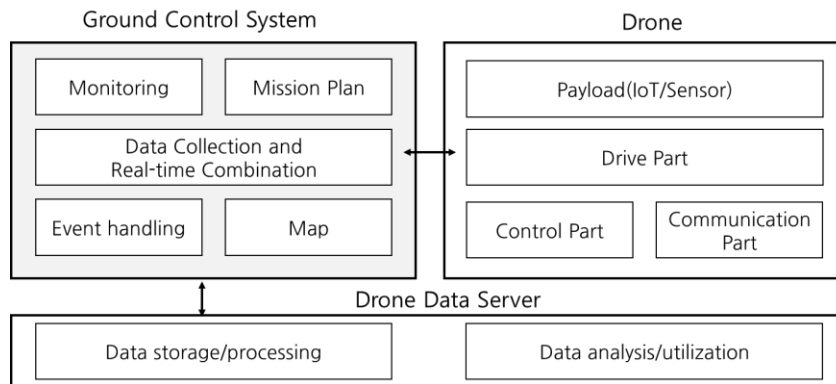


Figure 2. Drone Platform Design
 그림 2. 드론 플랫폼 설계

3.3 보안성 향상 방안 설계

드론 플랫폼에서 보안성을 갖추기 위한 기본적인 기능은 사용자 인증, 암호화의 기반기술을 토대로 드론에 대한 식별 기술, 드론 인증, 드론 데이터 암호화 기술, 수집정보 무결성 기술, 수집정보 프라이버시 보호기술 등이 필요하다. 이를 구분에 따라 재배치하고 보안성 향상을 위한 전략을 시퀀스 다이어그램을 기반으로 설계하면 그림 3 과 같다.

첫 번째, 사전 계획에서 드론과 드론 외부 환경안전에 대한 정보를 기반으로 지상 관제 시스템에 계획을 입력한다. 두 번째, 입력된 정보의 무결성을 유지하며 드론에게 운항 정보를 입력한다. 세 번째, 드론은 계획에 따른 운항과 함께 외부로부터 필요한 정보를 수집하고, 정보에 대한 무결성, 가용성을 유지한다. 또한, 수집된 정보에 대하여 최적의 드론 운항 현황을 도출하여 안전한 운항을 할 수 있게 한다. 네 번째, 수집된 정보를 지상 관제 시스템으로 보내고, 필요시에 데이터 서버로 전송하여 저장, 가공, 활용하는데 활용한다.

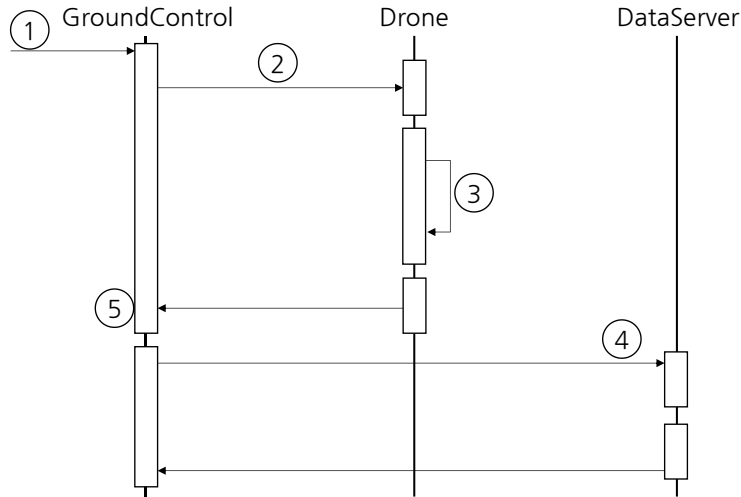


Figure 3. Sequence diagram of drone platform utilization to enhance security
 그림 3. 보안성 향상을 위한 드론 플랫폼 시퀀스 다이어그램

IV. 결론 및 향후 연구

4차 산업혁명의 기반기술인 IoT, Cloud, Bigdata, Mobility 를 핵심기술로 하여 기존의 산업을 융합산업으로 변화시키고 있으며, 드론을 중심으로 한 신산업이 대두되고 있다.

드론은 공중에서 임무를 수행하여 데이터를 획득하며, 임무수행을 위한 시간은 주로 배터리의 크기와 비행체의 무게로 결정된다. 드론이 획득하는 데이터는 배터리에 종속된 비행시간과 장소에 따라 변화될 수 있다. 이러한 특성으로 인하여 드론의 데이터 보호에는 공간적 전략 특성을 갖게 된다.

이에 따라 본 연구에서는 시나리오 기반의 보안성을 향상시킬 수 있는 드론 데이터 연계 플랫폼에 대하여 수행하였다. 연구결과는 다음과 같이 세 가지 의미를 갖을 수 있다.

- 드론 운항과 관련된 현업의 전문가들과 함께 드론 활용 시나리오에 대하여 설계하였다.
- 기존의 연구들을 기반으로 드론 플랫폼에 대하여 설계 및 정리하였다.
- 시나리오와 플랫폼을 기반으로 보안성을 향상시키기 위한 주요 지점에 대하여 개발하였다.

향후 연구로는 본 연구를 기반으로 드론 플랫폼 상에서 드론의 안전성을 향상시킬 수 있는 지상관제 시스템에 대한 연구를 수행하고자 한다.

V. 참고문헌

- [1] Yeong-Woo Yang, Ju-Lak Lee, "Utilization of Drone Technology in Physical Security and Its Limitations," The Journal of Police Policies, Vol. 32, No. 3, pp. 255-284. 2018.
- [2] Sung-Jun Kang, Eun-jeong Song. "A Study on the Application and Analysis of FPV Drones Using Virtual Reality," Proceedings of the Korean Institute of Information and Communication Sciences Conference, pp. 312-314. 2021.
- [3] JoonHwa Jung, SoYoung Park, "Current status and tasks of D.N.A. (data, network, AI) policies for the digital age," National Assembly Research Service, Issue and Arguments, No. 1828. 2021.
- [4] Chan-Seok Yu, Seok-Gu Kim, "Drone basics and technology," Magazine of the Korean Society of Agricultural Engineers, Vol. 57, No. 3, pp. 11-19. 2015.
- [5] Korea Institute of Aviation Safety Technology, 2020 Domestic and International Drone Industry Trend Analysis Report, 2020.
- [6] Kichul Wang, Byung-sun Lee, Jae-young Ahn, "Drone-based D.N.A. service technology and application development trend," Institute for Information & communication Technology Planning & evaluation , Weekly technology trend, No. 1946, pp. 16-27. 2020.
- [7] Tae-Wan Kim, Se-Yoon Lee, Seo-Woo Jung, Han-saem Wi, Ok-yeon Yi, "A Research on the Security of Drone Control Data Using Quantum Entropy-Based Random Number Generator," Journal of The Korea Institute of Information Security and Cryptology, Vol. 31, No. 2, pp. 133-144. 2021.
- [8] Woojin Lee, Kyungdeok Seo, Byeongmin Chae, "A study on security threats to drones using open source and military drone attack scenarios using telemetry hijacking," Convergence Security Journal, Vol. 20, No. 4, pp. 103-112. 2020.
- [9] Keun-Seog Park, Sang-pil Cheon, Seong-Pyo Kim, Jung-ho Eom, "Security Threats and Scenarios using Drones on the Battlefield," Convergence Security Journal, Vol. 18, No. 4, pp. 73-79. 2018.
- [10] Sun-Woo Yun, Il-Gu Lee, So-Hyun Park, Na-Eun Park, So-Eun Jeon, Ye-Sol Oh, Ji-Eun Lee, "Industrial Security Technologies and Policies for Smart Logistics Utilizing Drones," Korean Journal of Industry Security, Vol. 11, No. 1, pp. 137-161. 2021.

저자소개



김양훈(Yanghoon Kim)

- . 2007 년 : 대전대학교 컴퓨터공학과(공학석사)
- . 2011 년 : 대전대학교 컴퓨터공학과 소프트웨어공학 전공(공학박사)
- . 현재: 신한대학교 사이버드론봇군사학과 조교수
- . 관심분야: 산업보안, 융합보안, 드론, 스마트팩토리



홍찬기(Chan-Ki Hong)

- . 1988 년 : 중앙대학교 대학원 전자계산학과 (공학석사)
- . 1992 년 : 중앙대학교 대학원 전자계산학과 (공학박사)
- . 1992 년 3 월~현재 : 가톨릭관동대학교 의료 IT 학과 정교수
- . 관심분야: 정보보안, PKI, 블록체인