무인이동체 이상행위 탐지를 위한 소프트웨어 정의형 테스트베드 설계 및 구현

Design and Implementation of Software Defined Testbed for UAV Abnormality Detection

김성경, 강기완, 박기웅*[1)]
Sung-Kyung Kim, Ki-Wan Kang, Ki-Woong Park

(05006) 서울특별시 광진구 능동로 209 세종대학교 정보호학과 시스템보안 연구실, 정보보호학과*
{jotun9935, kkwan0226}@gmail.com, woongbak@sejong.ac.kr

요 약

무인이동체 시스템은 운용 과정에서 다양한 하드웨어 및 소프트웨어 구성요소를 복합적으로 사용한다. 이처럼 다양한 구성요소가 결합 되어 동작하는 무인이동체 시스템은 각 구성요소에 대한 다양한 결함 및 보안 위협에 노출되어 있다. 이에 따라 무인이동체의 일부 위험 및 위협 요소를 대상으로 무인이동체의 이상행위를 탐지하기 위한 다양한 연구들이 꾸준히 수행되어왔다. 무인이동체의 다양한 위험 및 위협 요소를 고려했을 때 실질적인 무인이동체 운용환경에서 이상행위 탐지 알고리즘의 신뢰성 있는 도입을 위해, 이상행위를 유발하는 각각의 요소에 대한 탐지 커버리지를 확장하여 무인이동체 시스템 전반의 강건성 및 보안성을 향상할 필요가 있다. 하지만 기존 이상행위 탐지 알고리즘의 통합적 도입과 검증 과정에서, 각 알고리즘이 이상행위 탐지를 위해 사용하는 데이터의 차이로 인한 통합의 어려움이 있다. 따라서 본 논문은 다양한 이상행위의 요인의 다각적인 수집 및 행위 결과에 대한 분석이 가능한 소프트웨어 정의형 무인이동체 테스트베드의 설계 및 구현을 통해 이상행위 탐지 개발과 적용 및 검증에서의 활용성을 높이고자 한다.

Abstract

The UAV(Unmanned Aerial vehicle) system uses a variety of hardware and software components in the process of operation. The UAV system operating in combination with various components is exposed to various defects and security threats for each component. Accordingly, various studies for detecting abnormal behavior of the UAV system have been continuously studied for some risks and threats of the UAV system. Thus, considering the various defeats and threats of the UAV system, it is necessary to reliably introduce the anomaly detection algorithm in a practical unmanned mobile operating environment. In addition, it is necessary to improve the robustness and security of the overall UAV system by extending the detection coverage for each element that causes abnormal

1) 교신저자

논문투고일자 : 2020. 06. 12 심사일자 : 2020. 07. 15 게재확정일자 : 2020. 08. 19

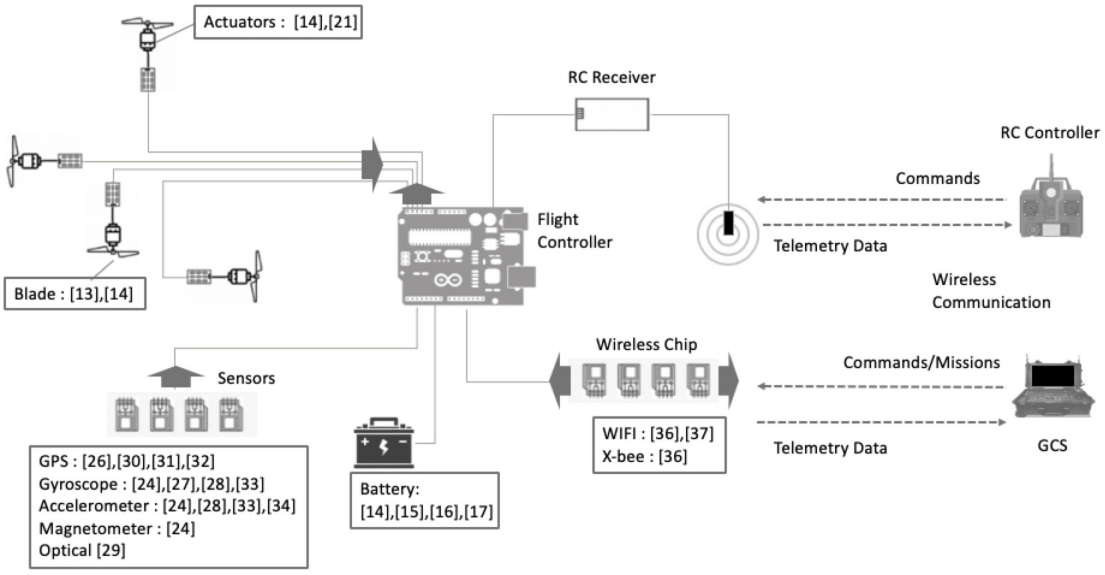
behavior. However, in the process of integrating and verifying the existing anomaly detection algorithm, there is a difficulty in integration due to differences in data used by each algorithm. Therefore, we design and implement a software-defined UAV testbed capable of multi-faceted collection of variables that can be a factor of various abnormal behaviors and analysis of UAV behavior results. Through this, we intend to increase the usability in the development, application and verification of abnormal behavior detection.

키워드: 무인이동체, 무인이동체 보안, 이상행위 탐지, 결함 탐지, 테스트베드 디자인, 소프트웨어 정의형 테스트베드

Keyword: Unmanned Aerial Vehicle(UAV), UAV Security, Abnormal Detection, Fault Detection, Testbed Design, Software Defined Testbed

1. 서론

최근 무인이동체 시스템은 군사 분야에서의 활용을 넘어 미디어, 농업, 레저를 비롯한 다양한 민간분야 등의 산업 분야에서 광범위하게 활용되고 있다[1][2][3]. 이러한 무인이동체 시스템은 물리적 프로세스와 소프트웨어 구성요소의 밀접한 결합으로 이루어진 Cyber Physical System(CPS) 기술을 근간으로 동작한다[4][5]. 이처럼 무인이동체 시스템은 구성요소의 복합적 상호작용을 통해 동작하기 때문에 단일 구성요소에 대한 결함 및 보안 위협의 영향으로 무인이동체 시스템 전체의 오류가 야기될 수 있다. 먼저 무인이동체 시스템은 구성요소의 결함으로 인해 야기될 수 있는 위험 요소를 내포한다. 예를 들어 무인이동체 시스템의 경우 기체 외부 상태 정보(자이로스코프, 가속도계 등) 수집을 위해 다양한 하드웨어 센서가 활용하고, 센싱된 정보는 소프트웨어 제어 로직에서 활용되어 엑추에이터를 동작시킴으로써 무인이동체의 안정적인 운용



(그림 1) 무인이동체 주요 구성요소 대상 결함 및 보안 위협

〈표 1〉 무인이동체 주요 구성요소 대상 결함 및 보안 위협과 탐지 및 방어 기법

구성요소		설명	결함	보안 위협	탐지/보호 기법
Battery(Power Source)		무인이동체의 전력 공급의 용도로 사용됨. 대다수의 무인이동체의 경우 주로 LiPo 배터리 등을 사용함.	[14],[15]	[16],[17]	[15],[18]
Rotor	Actuator	무인이동체의 비행 제어 로직 연산의 출력 값을 전달받아 모터의 회전 등의 물리적 변화로 변환하는 장치를 뜻함.	[14],[21]	-	[19],[20],[21],[22],[23]
	Blade	무인이동체의 모터와 접합되어 회전을 통해 비행에 필요한 추력 등을 생성함.	[13],[14]	-	[13]
Sensors	GPS Sensor	GPS 위성 신호를 수신하기 위한 센서로, 위성간 거리 계산을 통한 무인이동체의 현 위치 측정의 용도로 사용.	[26]	[30],[31],[32]	[25],[26]
	Gyroscope	무인이동체의 기울기 계산을 통해 무인이동체의 자세 제어에 활용되는 센서.	[24],[27],[28]	[33]	[24],[25],[27],[28]
	Accelerometer	중력가속도 측정 등을 통해 무인이동체의 이동속도 계산 등에 활용하는 센서.	[24],[28]	[33],[34]	[24],[25],[28].[34]
	Magnetometer	무인이동체 운용에 필요한 방위정보 취득에 필요.	[24]	-	[24]
	Optical Sensor	무인이동체의 미세 움직임 측정을 통해 호버링 등의 운용 목적으로 사용.	[29]	[35]	[29],[35]
Wireless Communication	WIFI	무인이동체와 GCS간 명령/미션 전송과 텔레메트리 데이터 수신 목적으로 사용.	-	[36],[37]	[36][37]
	Zigbee	mesh 네트워크의 특징을 가지고 있어 무인이동체의 군집 비행 등에 활용됨.	-	[36]	[36]

을 제공한다. 이와 같이 무인이동체 시스템은 하드웨어 및 소프트웨어의 다양한 구성요소 간 상호작용을 통해 동작하기 때문에 특정 구성요소에서 발생한 결함이 무인이동체 시스템 전체에 영향을 끼칠 수 있다. 또한 무인이동체 시스템의 경우 구성요소의 결함뿐만 아니라 무인이동체의 소프트웨어 및 하드웨어 구성요소에 대한 다양한 보안 위협 요소들을 내포한다[6]. 이러한 요인으로 인하여 발생하는 무인이동체 시스템의 오동작은 기체 추락으로 인한 인명 및 재산상의 피해로 이어질 수 있으며, 민감 정보를 탑재한 무인이동체의 경우 정보 유출 등의 추가적인 피해로 이어질 수 있기 때문에, 무인이동체 시스템의 안전성에 대한 정밀한 검증이 요구된다[7]. 이에 따라 시스템에 대한 정보의 수학적 모델링을 통해 이상을 탐지하는 방식인 행위 모델 기반 이상 탐지 방식[8], 지도 및 비지도 학습 과정을 통해 생성된 정상 행위에 대한 기계학습 모델을 통해 이상을 탐지하는 방식인 기계학습 기반 이상 탐지 방식[9][10] 등의 무인이동체 시스템의 이상행위를 탐지하기 위한 다양한 연구들이 수행되고 있다. 하지만 우리가 이전에 수행한 연구 결과 이와 같은 이상행위 탐지 연구들은 이상행위 탐지에 있어 서로 상이한 방식의 이상행위 정의 기준을 가지며, 이상행위 탐지 과정에 요구되는 데이터 또한 상이하기 때문에 기존 무인이동체 이상행위 탐지 연구의 종합적인 적용 및 검증에 어려움이 있다[11].

이러한 필요성에 근간하여 본 논문은 (그림 2)와 같이 다양한 이상행위 탐지 기술의 개발 과정과 적용 및 검증 과정에서 활용 가능한 테스트베드를 설계하였다. 본 논문은 테스트베드 설계 과정에서 다음의 2가지 사항을 중점으로 하여 설계를 수행하였다. 첫째로, 무인이동체의 다양한 구성요소에 대한 결함 및 보안 위협 요소들에 대한 이상행위 탐지 기술의 검증 과정에서의 활용성을 높이기 위해, 무인이동체 내부 상태 및 외부 환경 정보들을 고려한 다각적인 데이터 수집을 위한 방법을 고려하였다. 다음으로 안정적으로 무인이동체의 이상행위 데이터를 생성 할 수 있는 방법을 고려하였다. 이는 무인이동체 시스템과 같이 실질적인 하드웨어 기반으로 물리 환경에서 동작하는 시스템의 경우 이상행위 발생으로 인해 하드웨어의 고장으로 이어질 수 있기에, 무인이동체 하드웨어의 손상을 유발하지 않고 이상행위 데이터를 생성하기 위한 방안이 필요하기 때문이다. 따라서 본 논문은 무인이동체 시스

템 운용환경에서의 데이터 수집과 재현 가능한 이상행위 데이터의 생성을 위한 테스트베드 설계를 통해 향후 이상행위 탐지 기술의 개발 과정과 적용 및 검증 과정에서의 테스트베드의 활용성을 높이고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 무인이동체 시스템의 주요 구성요소에 대해 발생 가능한 결함 및 보안 위협과 이에 대한 탐지 기법에 대해 소개한다. 다음으로 3장에서는 무인이동체 테스트베드 설계의 요구사항을 도출한다. 이어서 4장에서는 테스트베드의 설계에 대하여 설명한다. 다음으로 5장에서는 테스트베드의 개념 증명적 구현 결과에 대해 설명한다. 마지막으로 6장에서는 결론에 대하여 기술한다.

2. 관련 연구

대표적인 무인이동체 시스템인 멀티로터 드론의 경우 일반적으로 Frame, Rotor(Actuator와 Blade로 구성), Electronic Speed Controller(ESC), Power Source, Flight Control Unit(FCU), On-board PC, Sensor, Wireless Communication의 핵심 구성요소로 구성된다[12]. 본 논문에서는 이와 같은 무인이동체의 핵심 구성요소를 기반으로 무인이동체 시스템 결함 및 보안 위협과 밀접한 구성요소를 선별하고, 각 구성요소와 관련된 결함, 보안 위협 및 탐지/보호 연구에 대해 조사 및 분석을 수행한 결과에 대해 <표 1>에 정리하였다.

2.1 무인이동체 주요 구성요소 대상 결함

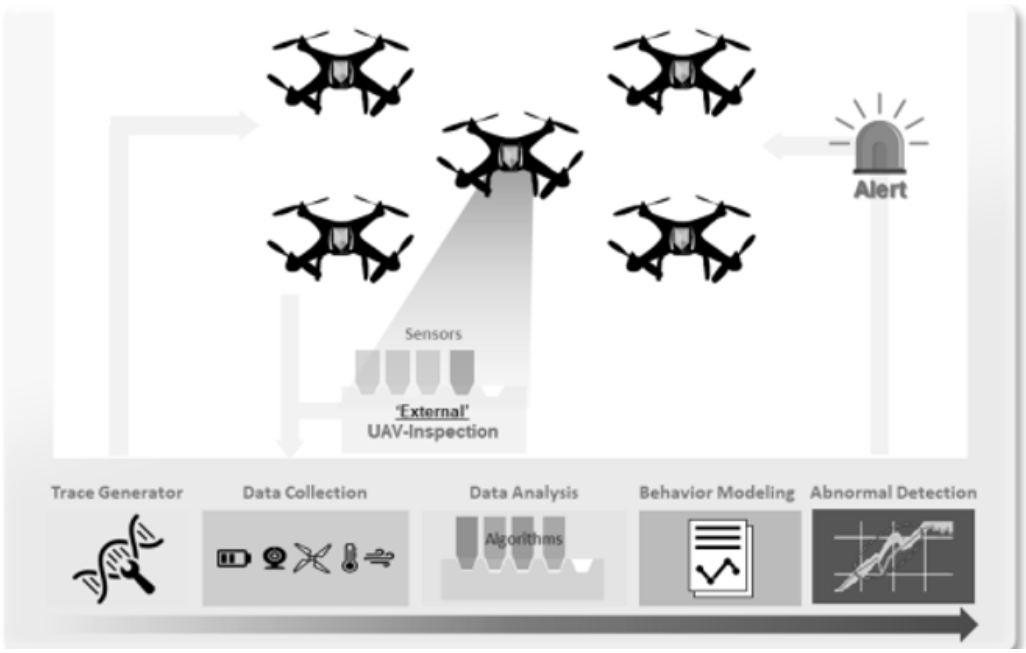
무인이동체 시스템은 동작 과정에서 배터리, 다양한 센서, 엑추에이터 등의 하드웨어 구성요소와 이를 이용하여 비행 상태를 안정적으로 제어하는 소프트웨어 등의 구성요소의 밀접한 상호작용이 이루어진다. 이에 따라 단일 구성요소에 대한 결함이 무인이동체 추락 등의 결과로 이어질 수 있다.

(그림 1)은 무인이동체의 주요 구성요소에서 발생 가능한 대표적인 결함 및 보안위협들에 대해 보여준다. Gino Iannace et al. 연구진[23]은 일반적인 UAV 결함 원인을 배터리, 모터 및 프로펠러 등의 문제라고 말하며, Farhad Pourpanah et al. 연구진[14]은 그 중 모터와 프로펠러에서 고장 발생 가능성이 가장 높다고 말한다. 또한 Anthony Bahadir Lopez et al. 연구진은 모바일 시스템과 CPS에서의 배터리 시스템에 대한 위협 및 잠재적 영향 분석을 수행하였다.

2.2 무인이동체 주요 구성요소 대상 보안 위협

무인이동체의 시스템은 다양한 구성요소의 밀접한 결합으로 이루어져 있기에 공격자의 입장에서 넓은 공격 벡터를 가진 시스템이라고 할 수 있다. 먼저 무인이동체의 전원 공급 용도로 사용되는 배터리 역시 보안 위협의 대상이 될 수 있으며, 많은 연구들을 통해 배터리 시스템에 대한 보안 위협 가능성이 제시었다. Radmilo Racic et al. 연구진[16]은 모바일 기기의 네트워크를 이용한 취약점을 통해 모바일 기기에 탑재된 배터리의 방전을 고의적으로 유발하는 공격을 수행하였다. 무인이동체의 경우 이러한 배터리의 방전은 운용에 직접적인 영향이 될 수 있기에 무인이동체의 결함 탐지에 있어 주요 고려사항이 된다. Miller Charlie는 Lithium-Ion 배터리 제어에 사용되는 주요 컨트롤러의 임의적 제어 가능성에 대해 보여준다[17].

무인이동체 시스템은 외부 GCS(Ground Control System)에서 기체에 탑재된 통신 모듈로의 명령/미션 전송을 통해 운용된다. 이에 따라 무인이동체 또한 범용 컴퓨팅 시스템과 같이 통신 취약점에 노출될 수 있다. Rodday Nils at el. 연구진[36]은 GCS와 무인이동체의 WIFI 칩셋 간의 안전성이 떨어지는 WEP(Wired Equivalent Privacy) 방식의 통신 과정에서 악의적 사용자와 대상 무인이동체간의 WIFI 링크 생성 가능성에 대해 보여준다. 또한 해당 연구에서는 무인이동체의 Xbee 칩셋을 대상으로 사용자와 무인이동체의 Zigbee 통신 채널 변조를 통해 커맨드 인젝션 및 도청 등의 공격 가능성을 보여준다.

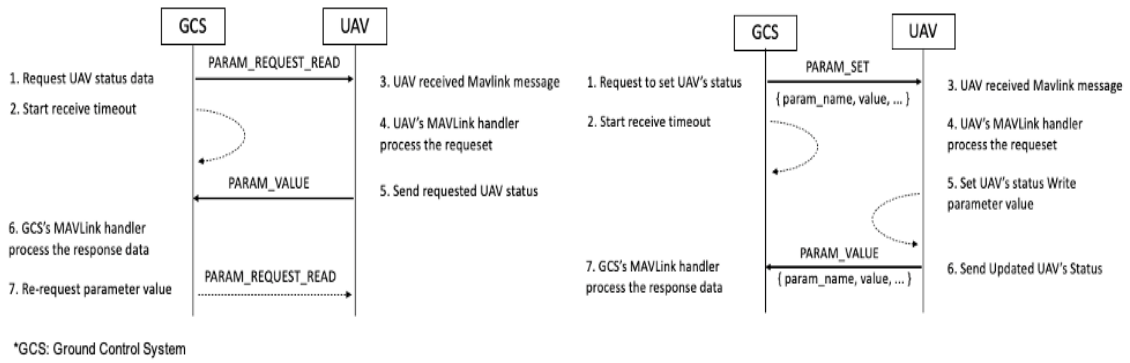


(그림 2) 무인이동체 이상행위 분석 테스트베드 프레임워크의 Blueprint

무인이동체 시스템은 다양한 운용 과정에서 하드웨어 센서를 활용하여 기체 외부 상태를 센싱한다. 최근 하드웨어 센서를 대상 공격 연구가 활발하게 수행되고 있으며, 이에 따라 하드웨어 센서 또한 무인이동체의 보안 위협의 대상으로 급부상하였다. Kexiong Zeng at el. 연구진[30]은 네비게이션 시스템을 대상으로 GPS(Global Positioning System) Spoofing을 은밀히 수행 할 수 있는 실시간 공격에 대한 연구를 수행하였다. Kulp Philip H at el. 연구진[32]는 무인이동체를 대상으로 GPS Spoofing 공격을 통해 은밀한 탈취 공격의 가능성을 보여주었다. 또한 Yunmok Son at el. 연구진[33]은 무인이동체의 자세제어에 활용되는 MEMS(Micro Electro Mechanical Systems) 자이로스코프, 가속도계 센서를 대상으로 잡음 주입을 통한 의도적인 무인이동체의 추락 가능성을 보여준다. Trippel Timothy et al. 연구진[34]은 가속도계 센서를 대상으로 공명 음향 주입 공격을 통해 MEMS 가속도계 센서에 대한 공격 가능성을 보여준다.

2.3 무인이동체 주요 구성요소 대상 이상행위 탐지 및 보호 기법

Khalastchi et al. 연구진[38]은 Robotics System의 결함탐지를 위해 사용되는 방법에 대한 survey연구를 진행하였다. 해당 논문은 무인이동체를 비롯한 robotics system의 결함탐지 관련 연구를 다음과 같이 분류하였다. 첫째로, Knowledge Based 방식은 인간 전문가의 행동을 모방하는 방법으로 인식된 동작을 사전에 정의된 결함 및 진단과 연관지어 판단하는 방식이다. 다음으로 Model Based 방식은 robotics system에서의 각 구성 요소의 올바른 동작을 분석을 통해 모델링하여 예상된 출력과 관찰된 출력을 비교하는 방식이다. 무인이동체의 Model-Based 이상탐지에서 대표적인 예로 Guillaume Ducard의 엑추에이터 결함 탐지 연구가 있다. Guillaume Ducard은 무인이동체의 수학적 모델을 통해 엑추에이터의 결함 및 고장을 효율적으로 감지하기 위한 FDI(Fault Detection and Isolation) 시스템에 대해 소개한다[19]. 셋째



(그림 3) (좌) MAVLink 프로토콜을 활용한 무인이동체 내부 상태 데이터 수집 과정, (우) MAVLink 프로토콜을 활용한 무인이동체 상태 데이터의 임의 변조 과정

로 Data Driven 방식의 결함탐지는 historical하게 관찰된 정상 행동과 잠재적 결함을 통계적으로 구분하여 결함을 탐지하는 방식이다. 대표적으로 Gwino iannace et al. 연구진[13]은 무인이동체의 blade의 불균형을 탐지하기 위하여, 무인이동체 운용 중 방출된 소음 측정 데이터를 활용하여 신경망 기반 blade 불균형 판별 모델을 연구하였다. Farhad Pourpanah et al. 연구진[14]은 무인이동체의 모터에서 발생하는 이상행위 모니터링을 위해 Fuzzy ART(Adaptive Resonance Theory) 신경망을 사용하며, VSA(Vibration Signature Analysis) 기술을 사용하여 무인이동체의 blade에 대한 모니터링을 수행한다. 또한 Adam Bondyra et al. 연구진[21]은 로터 결함 발생의 식별을 위해 IMU (Inertial Measurement Unit) 센서의 가속도 데이터를 활용하여 신호처리 및 머신러닝 기반의 결함 탐지 알고리즘을 제시한다.

3. 소프트웨어 정의형 테스트베드 요구사항 도출

본장에서는 이전 연구 수행 결과[11]를 기반으로, 무인이동체 이상행위 요인의 다각적 수집과 행위 결과 분석이 가능한 무인이동체 테스트베드 구성에 있어 요구되는 사항에 대해 정리하였다.

3.1 데이터 수집 관련 요구사항

일반적으로 무인이동체 이상행위 탐지 알고리즘은 특정 무인이동체의 구성요소에 대한 데이터를 알고리즘의 개발과 적용 과정 전반에서 활용한다. 이에 따라 본 논문은 테스트베드의 무인이동체 관련 데이터 수집 과정에서 요구되는 사항들을 다음과 같이 도출하였다.

- 범용성을 고려한 데이터 수집: 무인이동체 이상행위 탐지 시의 필요 데이터는 탐지 알고리즘에 따라 달라질 수 있다. 이에 따라 기존 탐지 알고리즘의 효과적인 수용을 위해 기존 이상행위 탐지 방식에 따라 상이한 데이터 셋 전반에 대해 범용적인 수집이 가능한 데이터 수집 기술이 필요하다.
- 확장성을 고려한 데이터 수집: 향후 센싱 기술의 발달 및 새로운 이상행위 탐지 기법의 발달에 따른 데이터 셋 추가의 가능성을 고려한 확장성 있는 데이터 수집 기술이 필요하다.
- 신뢰성을 고려한 데이터 수집: 무인이동체 시스템의 이상행위 탐지 알고리즘 개발 시 사용되는 데이터는 높은 신뢰성을 요구한다. 따라서 수집되는 데이터의 신뢰성을 향상하기 위한 데이터 수집 기술이 필요하다.

3.2 이상행위 데이터 생성 관련 요구사항

상당수의 무인이동체 이상행위 탐지 관련 연구는 무인이동체 및 하위 시스템의 구성 요소에 대한 정상행위를 정의 및 모델링을 통해 이상행위 발생 여부를 판단한다. 해당 과정에서 정상 행위 데이터 셋뿐만 아니라 이상행위 데이터를 활용하여 알고리즘의 성능 검증을 수행한다. 하지만 일반적인 무인이동체의 운용을 통해 간편한 수집이 가능한 정상 행위 데이터와 달리, 이상행위 데이터는 일반적인 무인이동체의 운용과정에서 낮은 빈도로 발생하기에 수집에 어려움이 있다. 이에 따라 본 논문은 테스트베드를 통한 무인이동체의 행위 결과의 분석 시 요구되는 이상행위 데이터 생성 기술의 요구사항을 다음과 같이 도출하였다.

- 지속적인 이상행위 데이터 생성 : 무인이동체 시스템은 실질적인 하드웨어를 기반으로 물리 환경에서 동작한다. 이러한 환경에서 이상행위의 발생은 무인이동체의 직접적인 고장으로 이어질 수 있기에 하드웨어의 파손을 유발하지 않는 이상행위 데이터 생성 기술이 요구된다.

- 재현 가능한 이상행위 데이터 생성 : 일반적으로 무인이동체 시스템은 물리 환경에서 운용되기 때문에 특정 시점에서 무인이동체의 이상행위가 발생하더라도 이를 향후 분석 과정에 활용하기에 어려움이 있다. 이에 따라 이상행위 데이터 생성 시 향후의 무인이동체 행위 결과 분석을 고려하여 이상행위 데이터 생성에 재현의 용이성을 향상하기 위한 기술이 요구된다.

4. 소프트웨어 정의형 테스트베드 설계

본 장에서는 무인이동체 시스템을 대상으로 하는 이상행위 탐지 관련 다양한 연구들을 적용 및 검증할 수 있는 테스트베드의 설계에 요구되는 기반 기술과 테스트베드의 설계와 구현 결과에 대해 설명한다.

4.1 무인이동체 내/외부 데이터 수집 기술

무인이동체는 다양한 센서를 활용하여 수집한 외부 환경 정보와 엑추에이터 출력에 대한 피드백 값을 기반으로 자세 제어를 수행한다. 이에 따라 대부분의 연구에서 무인이동체 시스템의 자세 제어의 원인이 되는 센싱 데이터와 출력 피드백 데이터를 활용하여 이상행위를 탐지한다. 따라서 해당 데이터와 같이 이상행위 탐지 연구에서 실질적으로 활용되는 범용적인 데이터 셋은 수집 과정에서 필수적인 대상이 된다. 이와 같은 무인이동체 운용 중 발생하는 내부 상태 데이터의 경우, GCS와 무인이동체 간 통신에 활용하는 프로토콜을 활용한 대부분 수집이 가능하다. 한편, 무인이동체 데이터 수집 과정에서 프로토콜이 지원하는 모든 데이터에 대한 수집을 진행하는 것은 상대적으로 낮은 하드웨어 리소스를 사용하는 소형 무인이동체의 경우, 데이터 수집에서 발생한 오버헤드로 인해 시스템 장애로 야기될 수 있다. 따라서 우리는 무인이동체 내부 상태 데이터 수집 과정에 있어서 소프트웨어 형태로 수집 대상 데이터의 선택적 지정 가능 여부를 고려하여 테스트베드를 디자인하였다. 본 논문은 테스트베드 설계에서 무인이동체 내부 상태 데이터의 지속적 수집을 위해 대부분의 오픈소스 기반 무인이동체 관련 프로젝트에서 지원[39][40]하는 MAVLink 프로토콜[41]을 활용한다.

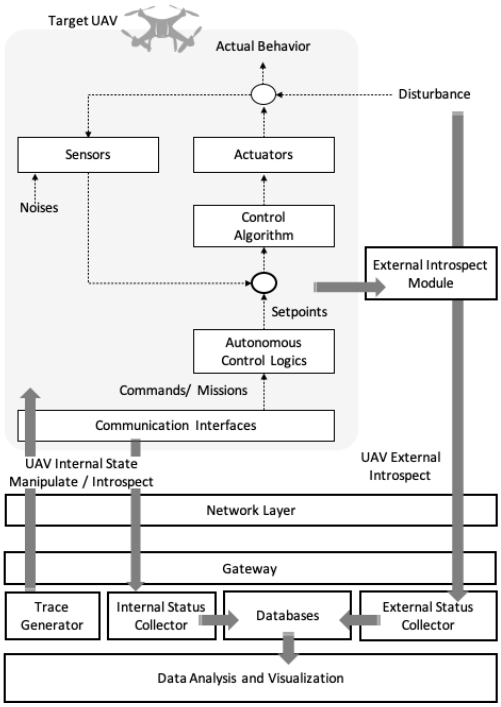
4.2 무인이동체 이상행위 데이터 생성 기술

무인이동체 이상행위 알고리즘의 개발과 검증 과정에서 알고리즘의 성능 측정을 위해 무인이동체 시스템에서 발생한 이상행위 데이터가 사용된다. 하지만 해당 과정에서 무인이동체 이상행위 탐지 알고리즘이 탐지에 활용하는 이상행위는 일반적인 운용 과정에서 발생 빈도가 낮다. 이에 따라 운용중인 무인이동체를 대상으로 이상행위를 임의적 방법으로 발생하기 위한 기술이 필요하다. 본 논문은 (그림 3) 우측과 같이 MAVLink 프로토콜의 PARAM_SET 기능을 활용하여 운용중인 무인이

동체의 내부 데이터를 임의로 변조하는 방식을 사용한다. 이 때 PARAM_SET 명령을 통해 무인이동체의 기체 설정 등에 대한 정보를 원격에서 변경이 가능하다.

4.3 소프트웨어 정의형 무인이동체 이상행위 분석 테스트베드 설계

설계된 무인이동체 이상행위 분석을 위한 테스트베드 프레임워크의 구조는 (그림 4)와 같다.



(그림 4) 무인이동체 이상행위 분석 테스트베드 프레임워크 구조

• Data Collector

데이터 수집 측면에서 테스트베드 프레임워크는 크게 무인이동체 내부 상태와 외부 상태 수집의 2가지 모듈로 구성되어 있다. 먼저 무인이동체의 내부 상태에 대한 수집 모듈인 Internal Status Collector 모듈은 무인이동체가 GCS로부터 전달받은 명령이나 미션을 기준으로 무인이동체의 폐루프 제어 과정에 따라 끊임없이 변화하는 외부 환경에 대한 센싱, 제어 로직의 출력, 엑추에이터의 출력 데이터 등을 비롯한 무인이동체의 현재 내부 상태에 대한 다각적 정보의 수집 지속적으로 수행한다. 다음으로 External Status Collector 모듈은 무인이동체 운행에 영향을 미치는 풍속, 습도, 온도 등의 외부 환경 데이터들에 대한 수집을 지속적으로 수행한다. 또한 해당 모듈은 수집 데이터의 신뢰성을 위해 무인이동체의 내부 상태 데이터 중 배터리 온도나 모터 온도 등의 데이터를 교차 수집한다. 추가적으로 External Status Collector 모듈의 경우 특정 이상행위 탐지 알고리즘에서 Internal Status Collector로 수집에 어려움이 있는 데이터에 대한 요구가 있는 경우에 대비하여 확장성을 고려한 pluggable 방식으로 센서의 추가 적재가 용이하도록 설계되었다. 이와 같이 Internal/External Status Collector 모듈로부터 지속적으로 수집되는 데이터는 분석자의 요구사항에 맞는 데이터베이스에 저장되어 향후 데이터 분석 과정에 사용된다.

• Trace Generator

테스트베드를 무인이동체 이상행위 알고리즘 개발에 사용하기 위해서는 무인이동체의 상태 변화에 대한 변인 통제가 가능해야한다. 이를 위해 본 논문은 지정된 미션을 통해 무인이동체를 운용하고, 동작중인 무인이동체의 외부에서 무인이동체의 내부 상태에 대한 임의적 변화를 가할 수 있는 모듈을 설계하였다.

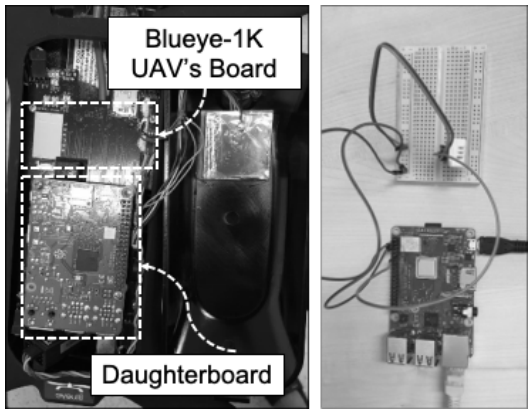
5. 소프트웨어 정의형 테스트베드 구현을 통한 Proof of Concept

본 장에서는 무인이동체 이상행위 분석을 위한 테스트베드의 Proof of Concept 형태의 구현에 사용된 환경과 구현 결과에 대해 설명한다.

5.1 소프트웨어 정의형 테스트베드 구현 환경

본 논문의 테스트베드 Proof of Concept 개발환경은 다음과 같다. 먼저 테스트베드 개발 과정에서 Ardupilot 무인이동체를 대상으로 테스트베드를

구현하였다. 이를 위해 Blueye-1K 드론(그림 5)과 무인이동체 시뮬레이션 환경인 SITL(Software in the Loop)를 사용하였다. 이 외에도 내부 상태의 교차 모니터링을 위한 도터보드를 탑재하여 사용하였으며, (그림 5)의 우측 그림과 같이 외부 환경 데이터 수집을 위한 모듈로 Raspberry Pi3를 사용하였다.



(그림 5) 〔좌〕 무인이동체 내부 상태 모니터링을 위한 Blueye-1K 드론과 Raspberry Pi3 도터보드, 〔우〕 외부 환경 데이터 수집을 위한 모듈

5.2 소프트웨어 정의형테스트베드 구현

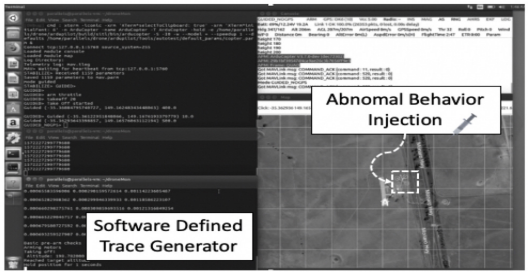
본 논문은 (그림 4)의 설계를 기반으로 다음과 같이 각 구성요소에 대한 개념증명적 구현을 진행하였다.

• Data Collector

무인이동체의 내부 상태 정보 데이터의 경우 일반적으로 GCS와 무인이동체의 통신 프로토콜의 기능을 활용하면 수집이 가능하다. 본 논문은 (그림 3)의 좌측에 해당하는 MAVLink 프로토콜의 파라미터 리퀘스트 기능을 활용하여 Internal Status Collector 모듈을 구현하였다. 이때 해당 기능은 MAVLink 프로토콜을 통해 GCS에서 무인이동체의 행위 데이터 모니터링을 위해 사용하는 기능이다. 다음으로 External Status Collector 모듈의 경우 (그림 5)의 좌측에 위치한 그림과 같이 무인이동체에 도터보드를 탑재하는 방식으로 데이터를 수집한다. 해당 모듈은 Internal Status Collector가 무인이동체에 장착된 센서를 사용해 외부 환경에 대한 데이터 수집을 수행하는 것과 달리, 무인이동체 내부에 탑재되지 않는 센서를 사용한 데이터 수집을 수행한다. 대표적으로 actuator에서 발생한 noise나 모터 온도 등의 데이터 수집에 활용 가능하다. 하지만 해당 모듈은 무인이동체에 탑재되는 형태로 운용되기 때문에 다각적 데이터 수집을 위한 많은 양의 센서 장착에 어려움이 있다. 따라서 본 논문은 마지막으로 외부 환경에 대한 다각적 정보 수집을 위해 무인이동체 운용 테스트 환경과 연관된 풍향, 풍속 등의 추가적인 수집 요구사항을 반영할 수 있도록 (그림 5)와 같이 외부 보드 형태로 외부 환경 관측 모듈을 구현하였다.

• Trace Generator

본 논문의 테스트베드는 하드웨어의 제약 없이 원격에서 무인이동체 내부 상태에 대한 변화의 가능성 제시를 위해 (그림 3)의 우측에 위치한 MAVLink 프로토콜의 파라미터 설정 기능을 Trace Generator 구현에 활용하였다. (그림 6)은 Trace Generator를 활용하여 무인이동체가 일련의 미션을 통해 운용되는 도중, 이상행위를 주입하여 무인이동체의 오동작을 유발하는 동작을 SITL 상에서 실험한 결과를 나타낸다.



(그림 6) Ardupilot SITL 환경에서의 Trace Generator 동작

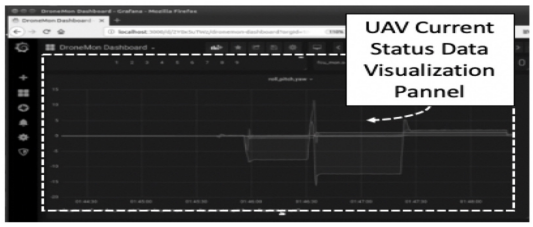
• Database

Data Collector 모듈을 통해 지속적으로 수집되

는 데이터는 테스트베드 내의 Database에 저장된다. 본 논문의 프로토타입 테스트베드의 경우 분석 요구사항에 적합한 데이터 활용이 가능하도록 시계열(e.g. InfluxDB) 및 관계형 데이터베이스(e.g. MySQL)에 대한 연동을 지원한다.

• Data Analysis and Visualization

본 논문의 테스트베드의 경우 (그림 7)과 같이 무인이동체 관련 데이터를 활용한 이상행위 탐지 알고리즘 개발과정에서 분석자의 데이터 분석의 편의를 위해 수집된 데이터에 대한 시각화 기능을 지원한다. 본 논문은 수집된 데이터에 대한 우선적인 분석을 용이하게 하기 위해 무인이동체의 행위 정보가 저장된 데이터베이스를 대상으로 쿼리를 수행할 수 있는 기능을 지원한다. 이를 위해 본 논문은 웹을 통해 다양한 데이터 분석 쿼리에 대한 플러그인을 제공하는 Grafana를 통해 데이터 분석과 시각화 기능을 고려하였다.



(그림 7) Grafana를 활용한 수집 데이터 종합 시각화 기능

6. 결론

현재 무인이동체 시스템은 다양한 분야에서 광범위하게 활용되고 있다. 무인이동체 시스템은 하드웨어 및 소프트웨어 간의 상호작용을 통해 운용되기 때문에 특정 구성요소에서 발생한 장애가 무인이동체 시스템 전체에 영향을 미칠 수 있는 특징을 가지고 있다. 특정 구성요소의 장애 발생 시 무인이동체 시스템 전체의 장애로 이어져 인명 및 재산상의 피해가 야기될 수 있으며, 민감 정보를 탑재한 무인이동체의 경우 정보 유출 등의 추가적인 피해로 이어질 수 있다. 이런 피해를 방지하고자 무인이동체 시스템의 이상행위 탐지를 위해 다양한 연구들이 진행되고 있다. 그러나 다양한 이상행위 탐지 연구들에 있어 서로 상이한 이상행위 기준을 정의하고 있으며, 이상행위 탐지 과정에서 요구되는 데이터 또한 상이하기 때문에 기존 무인이동체 시스템의 이상행위 탐지 연구의 종합적인 적용 및 검증에 어려움이 존재하는 상황이다. 따라서 본 논문에서는 무인이동체의 다양한 구성요소에 대한 결함 및 보안 위협 요소들에 대한 이상행위 탐지 기술의 검증 과정에서의 활용성을 높이기 위해, 무인이동체 내부 상태 및 외부 환경 정보들을 고려한 다각적인 데이터 수집과 안정적으로 무인이동체의 이상행위 데이터를 유발할 수 있는 테스트베드를 설계하였다. 본 논문에서 설계한 테스트베드를 통해 향후 이상행위 탐지 기술의 개발 과정과 적용 및 검증 과정에서의 신뢰성을 제공할 수 있을 것으로 기대된다.

Acknowledgments

본 연구는 ETRI부설연구소 위탁과제(2020-114)의 지원, 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 지원(No.2019-0-00426) 및 한국연구재단 연구과제(NRF-2020R1A2C4002737)의 지원을 받아 수행된 연구임.

참고문헌

[1] Adams, Stuart M., and Carol J. Friedland. "A survey of unmanned aerial vehicle (UAV) usage for imagery collection in disaster research and management." 9th International Workshop on Remote Sensing for Disaster Response. Vol. 8. 2011.

[2] 박찬정,김기용. "안티드론 기술의 특허동향 분석 : 무력화 수단 및 방법을 중심으로." 한국차세대컴퓨팅학

회 논문지, 16.2 (2020):7-17.
〔3〕 이택희. "가상 드론 시뮬레이터 구축을 위한 시스템 구성." 한국차세대컴퓨팅학회 논문지, 13.6 (2017): 124-131.
〔4〕 R. H. Rawung and A. G. Putrada, "Cyber physical system: Paper survey," 2014 International Conference on ICT For Smart Society (ICISS), Bandung, 2014, pp. 273-278, doi: 10.1109/ICTSS.2014.7013187.
〔5〕 H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li and J. Wei, "Survey on Unmanned Aerial Vehicle Networks: A Cyber Physical System Perspective," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1027-1070, Secondquarter 2020, doi: 10.1109/COMST.2019.2962207.
〔6〕 Son, Yunmok, et al. "Rocking drones with intentional sound noise on gyroscopic sensors." 24th {USENIX} Security Symposium ({USENIX} Security 15). 2015.
〔7〕 Hartmann, Kim, and Christoph Steup. "The vulnerability of UAVs to cyber attacksAn approach to the risk assessment." 2013 5th international conference on cyber conflict (CYCON 2013). IEEE, 2013.
〔8〕 Choi, Hongjun, et al. "Detecting attacks against robotic vehicles: A control invariant approach." Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018.
〔9〕 Lu, Huimin, et al. "Motor anomaly detection for unmanned aerial vehicles using reinforcement learning." IEEE internet of things journal 5.4 (2017): 2315-2322.
〔10〕 I. Al-Dein Al-Zyoud and K. Khorasani, "Neural Network-based Actuator Fault Diagnosis for Attitude Control Subsystem of an Unmanned Space Vehicle," The 2006 IEEE International Joint Conference on Neural Network Proceedings, Vancouver, BC, 2006, pp. 3686-3693, doi: 10.1109/IJCNN.2006.247383.
〔11〕 Ki-Wan Kang, SungKyung Kim, Ki-Woong Park, "Requirements Derivation of Testbed of UAV Anomaly Detection", The 5th International Conference on Next Generation Computing 2019. Korean Institute of Next Generation Computing. 2019.
〔12〕 Yang, Hyunsoo, et al, "Multi-rotor drone tutorial: sy stems, mechanics, control and state estimation." Intellige nt Service Robotics 10.2, 79-93, 2017.
〔13〕 Iannace, Gino, Giuseppe Ciaburro, and Amelia Trematerra. "Fault Diagnosis for UAV Blades Using Artificial Neural Network." Robotics 8.3 (2019): 59.
〔14〕 Pourpanah, Farhad, et al. "Anomaly Detection and Condition Monitoring of UAV Motors and Propellers." 2018 IEEE SENSORS. IEEE, 2018.
〔15〕 Lopez, Anthony Bahadir, et al. "A security perspective on battery systems of the internet of things." Journal of Hardware and Systems Security 1.2 (2017): 188-199.
〔16〕 Racic, Radmilo, Denys Ma, and Hao Chen. "Exploiting MMS vulnerabilities to stealthily exhaust mobile phone's battery." 2006 Securecomm and Workshops. IEEE, 2006.
〔17〕 Miller, Charlie. "Battery firmware hacking." Black Hat USA (2011): 3-4.
〔18〕 Hu, Chao, Byeng D. Youn, and Jaesik Chung. "A multiscale framework with extended Kalman filter for lithium-ion battery SOC and capacity estimation." Applied Energy 92 (2012): 694-704.
〔19〕 Ducard, Guillaume. "Actuator fault detection

in uavs." Handbook of Unmanned Aerial Vehicles. Springer Netherlands, 2015. 1071-1172.

〔20〕 Marichal, Graciliano Nicolás, et al. "An artificial intelligence approach for gears diagnostics in AUVs." Sensors 16.4 (2016): 529.

〔21〕 Bondyra, Adam, et al. "Fault diagnosis and condition monitoring of uav rotor using signal processing." 2017 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA). IEEE, 2017.

〔22〕 Xie, Xi-hua, et al. "GRNN Model for Fault Diagnosis of Unmanned Helicopter Rotor's Unbalance." Proceedings of the 5th International Conference on Electrical Engineering and Automatic Control. Springer, Berlin, Heidelberg, 2016.

〔23〕 Lu, Huimin, et al. "Motor anomaly detection for unmanned aerial vehicles using reinforcement learning." IEEE internet of things journal 5.4 (2017): 2315-2322.

〔24〕 Heredia, Guillermo, and Anibal Ollero. "Detection of sensor faults in small helicopter UAVs using observer/Kalman filter identification." Mathematical Problems in Engineering 2011 (2011).

〔25〕 Heredia, Guillermo, et al. "Multi-unmanned aerial vehicle (UAV) cooperative fault detection employing differential global positioning (DGPS), inertial and vision sensors." Sensors 9.9 (2009): 7566-7579.

〔26〕 Guo, Dingfei, et al. "A hybrid feature model and deep learning based fault diagnosis for unmanned aerial vehicle sensors." Neurocomputing 319 (2018): 155-163.

〔27〕 Guo, Kai, et al. "UAV sensor fault detection using a classifier without negative samples: A local density regulated optimization algorithm." Sensors 19.4 (2019): 771.

〔28〕 Avram, Remus C., et al. "IMU sensor fault diagnosis and estimation for quadrotor UAVs." IFAC-PapersOnLine 48.21 (2015): 380-385.

〔29〕 Chen, Zhongyuan, et al. "Fault-tolerant optical flow sensor/SINS integrated navigation scheme for MAV in a GPS-denied environment." Journal of Sensors 2018 (2018).

〔30〕 Zeng, Kexiong Curtis, et al. "All your {GPS} are belong to us: Towards stealthy manipulation of road navigation systems." 27th {USENIX} Security Symposium ({USENIX} Security 18). 2018.

〔31〕 Su, Jie, et al. "A stealthy gps spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle." IFAC-PapersOnLine 49.22 (2016): 291-296.

〔32〕 Gaspar, João, et al. "Capture of uavs through gps spoofing." 2018 Global Wireless Summit (GWS). IEEE, 2018.

〔33〕 Son, Yunmok, et al. "Rocking drones with intentional sound noise on gyroscopic sensors." 24th {USENIX} Security Symposium ({USENIX} Security 15). 2015.

〔34〕 Trippel, Timothy, et al. "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks." 2017 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2017.

〔35〕 Davidson, Drew, et al. "Controlling UAVs with sensor input spoofing attacks." 10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16). 2016.

〔36〕 Rodday, Nils Miro, Ricardo de O. Schmidt, and Aiko Pras. "Exploring security vulnerabilities

of unmanned aerial vehicles." NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2016.

〔37〕 Pleban, Johann-Sebastian, Ricardo Band, and Reiner Creutzburg. "Hacking and securing the AR. Drone 2.0 quadcopter: investigations for improving the security of a toy." Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2014. Vol. 9030. International Society for Optics and Photonics, 2014.

〔38〕 Khalastchi, Eliahu, and Meir Kalech. "On fault detection and diagnosis in robotic systems." ACM Computing Surveys (CSUR) 51.1 (2018): 1-24.

〔39〕 ardupilot, https://ardupilot.org/

〔40〕 px4, https://px4.io/

저자소개

◆ **김성경**

- 2019년 세종대학교 정보보호학과 학사
- 2018년 세종대학교 정보보호학과 석사 과정
- 관심분야: CTF, Exploit, 시스템 보안, 클라우드 컴퓨팅

◆ **강기완**

- 2019년 순천향대학교 정보보호학과 학사
- 2018년 세종대학교 정보보호학과 석사 과정
- 관심분야: 클라우드 컴퓨팅, 임베디드 시스템, 시스템 보안 등

◆ **박기웅**

- 2005년 연세대학교 Computer Science 학사
- 2007년 KAIST Electrical Engineering 석사
- 2012년 KAIST Electrical Engineering 박사
- 2008년 Microsoft Research Asia, Wireless and Networking Grourp, Research Intern
- 2009년 Microsoft Research, Network-Research Group, Graduate Research-Fellow
- 2012년 국가보안기술연구소 연구원
- 2012년~2016년 대전대학교 정보보안학과 교수
- 2016년~현재 세종대학교 정보보호학과 교수
- 관심분야: 시스템 보안, 모바일-클라우드 컴퓨팅, 보안 프로토콜, 디지털 포렌식 등