https://doi.org/10.33778/kcsa.2023.23.2.103

HITL 시뮬레이션 기반 무인비행체 패킷 데이터를 활용한 실시간 이상 탐지 시스템★

박 대 경*, 김 병 진**

요 약

최근 몇 년 동안 무인비행체는 다양한 산업 분야에서 널리 사용되고 있다. 그러나, 무인비행체에 대한 의존도가 급격하게 높아짐에 따라 무인비행체의 보안과 안전에 대한 우려가 커지고 있다. 현재 무인비행체의 제어권을 탈취하거나 웹 애플리케이션에서 무인비행체와 통신할 수 있는 권한을 탈취하는 등 다양한 취약점들이 공개되고 있다. 하지만, 무인비행체의 보안과 관련된 연구가 많이 부족한 실정이다. 따라서 본 논문에서는 실제 환경과 유사한 HITL 시뮬레이션 환경에서 무인비행체의 패킷 데이터를 수집하여 패킷 데이터가 정상 데이터인지 비정상 데이터인지 판단하는 연구를 진행하였다. 또한, 본 논문에서는 모델링 과정에서 Computation Cost를 줄이고 데이터 해석의 용이성을 높이는 방법과 정상 데이터만을 학습하여 비정상 데이터를 탐지하는 기계 학습 기반 이상 탐지 모델 및 최적화된 하이퍼 파라미터값을 제안한다.

Real-time Anomaly Detection System Using HITL Simulation-Based UAV Packet Data

Daekyeong Park*, Byeongjin Kim**

ABSTRACT

In recent years, Unmanned Aerial Vehicles (UAV) have been widely used in various industries. However, as the depend ence on UAV increases rapidly, concerns about the security and safety of UAV are growing. Currently, various vulnerabili ties such as stealing the control right of the UAV or the right to communicate with the UAV in the web application are being disclosed. However, there is a lack of research related to the security of UAV. Therefore, in this paper, a study was conducted to determine whether the packet data was normal or abnormal by collecting packet data of an unmanned aerial vehicle in a HITL(Hardware In The Loop) simulation environment similar to the real environment. In addition, this paper proposes a method for reducing computational cost in the modeling process and increasing the ease of data interpretation, a machine learning-based anomaly detection model that detects abnormal data by learning only normal data, and optimized hyperparameter values.

Key words : Hardware In The Loop, Unmanned Aerial Vehicle, Ground Control Station, Anomaly Detection, Machine Learning

접수일(2023년 04월 13일), 게재확정일(2023년 05월 11일)

★ 본 논문은 2023년 정부(방위사업청)의 재원으로 국방과학연구소의 지원을 받아 수행된 미래도전국방기술 연구개발사업임 (No. 915024201)

* 한화시스템(주) 기반기술연구소(주저자)
** 한화시스템(주) 기반기술연구소(교신저자)

1. 서 론

무인비행체(Unmanned Aerial Vehicle, UAV)라고도 하는 드론은 최근 몇 년 동안 군사 작전, 수색 및 구조, 농업, 배송, 보안 등 다양한 산업 분야에서 널리 사용되고 있다[1, 2]. 특히 무인비행체는 사람이 직접 탑승하지 않고 조종할 수 있어서 인명피해 없이 위험한 임무를 수행할 수 있으며, 현재도 활발하게 연구되고 있다[3, 4]. 또한 무인비행체에 인공지능, 빅데이터 분석 등의 기술들이 적용되면서 자동 운항, 충돌 방지, 임무 수행, 영상 처리 등 다양한 기능을 제공한다. 이에 따라, 무인비행체에 대한 의존도가 높아져 무인비행체의 보안성과 안전성에 대한 우려가 커지고 있다.

현재 무인비행체의 제어권을 탈취하거나 웹 애플리케이션에서 무인비행체의 통신 채널을 탈취하는 등 다양한 취약점들이 공개되고 있다[5, 6]. 이러한 취약점들이 악용될 경우, 무인비행체는 정상적인 행동을 할 수 없으며 더 나아가 인명피해 또는 자산 탈취 등의 피해가 발생할 수 있으므로 지능적으로 다양해지는 취약점들을 방어하는 것은 매우 중요한 문제이다[7].

따라서, 본 논문에서의 목표는 이러한 문제를 해결하기 위해 무인비행체에서 발생하는 패킷 데이터를 활용하여 패킷 데이터가 정상 데이터인지 비정상 데이터인지 판단하는 것이다. 패킷 데이터를 활용하여 비정상 데이터를 탐지하는 기법은 크게 오용탐지(Misuse Detection, MD)와 이상 탐지(Anomaly Detection, AD) 두 가지 유형으로 나눌 수 있다[8, 9].

오용탐지는 현재까지 알려진 비정상 데이터를 기반으로 데이터가 비정상 데이터와 패턴이 일치하는지 판단하는 기법이다. 이상 탐지는 오용탐지 방법과 달리 정상 데이터를 기반으로 정상 데이터의 패턴과 일치하지 않는 데이터인지 판단하는 기법이다. 오용탐지 방법은 기존에 알려지지 않은 이상 데이터를 판단하기에 적합하지 않지만, 이상 탐지 방법은 기존에 알려지지 않은 이상 데이터를 탐지할 수 있다는 장점이 있다. 하지만, 이상 탐지 방법은 수많은 정상적인 데이터의 패턴을 정의하기가 어렵고 학습하지 못한 정상 데이터의 패턴은 이상 데이터로 간주하기 때문에 잘못 판단할 확률이 증가한다는 문제점이 있다[10].

실험에 사용된 데이터 세트는 HITL 시뮬레이션 환경에서 수집된 무인비행체 패킷 데이터이다. HITL 시뮬레이션 환경에서 패킷을 수집한 이유는 고가의 무인비행체를 파손 및 분실 등 다양한 상황에 노출되어 큰 비용이 발생할 수 있기 때문이다. 이러한 위험과 비효율성을 피하고자 HITL 시뮬레이션 환경에서 무인비행체의 패킷 데이터를 수집했다.

본 논문에서는 HITL 환경에서 발생하는 무인비행체 패킷 데이터를 활용하여 비정상 데이터를 탐지하는 연구를 진행하며, 구성은 다음과 같다. 2장에서는 무인비행체와 지상제어시스템, 통신 프로토콜, HITL 시뮬레이션에 관한 이전 연구를 간단히 소개하고, 3장에서는 HITL 시뮬레이션 환경에서 무인비행체 패킷 데이터를 수집하는 과정과 데이터 전처리, 모델 생성에 관해 설명하였다. 4장에서는 생성된 모델의 평가 방법 및 결과를 확인하고, 5장에서는 본 연구의 최종 결론과 향후 연구에 관해 설명한다.

2. 관련 연구

2.1 PX4 드론 펌웨어

PX4는 무인비행체의 원격조정 및 자율주행을 위해 설계된 소프트웨어로 Dronecode 프로젝트의 일부이다. ROS 기반[11]으로 동작하며 NuttX 운영체제를 사용하며, NuttX는 임베디드 시스템의 플랫폼 중 하나인 RTOS(Real Time Operating System)로 개발되었다. PX4는 크게 4가지 모듈(저장소, 드라이버, 외부 연결, 비행 제어)로 구성되어 있으며, 각 모듈은 uORB(Micro Object Request Broker) 메시지 버스를 사용하여 통신한다. 또한, QGroundControl이라는 지상관제 프로그램과 Drone kit라는 원격조정 애플리케이션의 오픈소스를 제공하고 있다[12].

2.2 지상제어시스템

GCS(Ground Control System)는 지상제어시스템으로 지상에서 사용자가 비행 상태를 확인하는 등 드론을 운용하기 위한 환경을 제공하는 관제 시스템이다[13, 14]. 본 연구에서 GCS로 활용하는 QGC(QGroundControl)는 MAVLink 프로토콜을 지원하는 드론의 GCS 소프트웨어이다. QGC 외에도 다양한 GCS가 있으며, 대부분 MAVLink 프로토콜을 사용한다. QGC는 PX4 펌웨어 업로드, 계획, 비행 임무 등 다양한 기능을 사용자에게 제공한다.

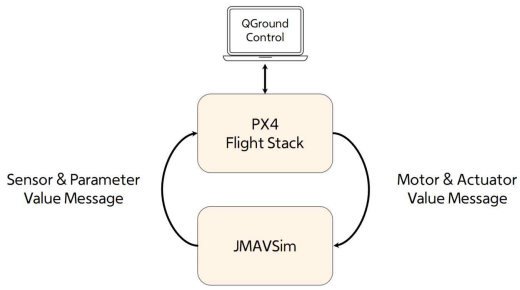
2.3 MAVLink 프로토콜

단일 무인비행체 응용의 예로 대표적인 무인비행체인 드론을 인터넷을 통해 원격 활용하기 위해 지상제어장치와 무인비행체 간에 데이터 송수신을 UDP/IP 기반의 MAVLink(Micro Air Vehicle Link) 응용 프로토콜로 사용하는 방법이 소개되었다[15].

MAVLink 프로토콜은 경량화된 메시지 프로토콜로, 메시지 하나의 패킷은 8Byte에서 최대 263Byte를 한 번에 전송할 수 있다. 또한, 대부분의 GCS는 MAVLink 프로토콜을 지원하고 있으므로 별도의 설정 없이도 드론과 연결할 수 있다[16].

2.4 JMAVSim 시뮬레이터

본 논문에서 구축한 시뮬레이션 환경은 크게 PX4, GCS, JMAVSim 시뮬레이터로 구성되어 있다. (Figure 1)은 JMAVSim과 PX4 사이에서 발생하는 메시지들의 흐름을 나타낸 그림이다.



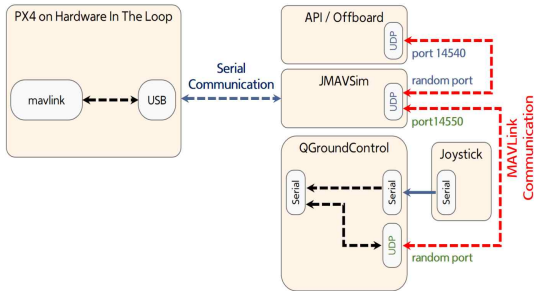
(Figure 1) Interface between JMAVSim simulator and PX4

(Figure 1)에서 사용자가 GCS를 통해 PX4에 조종 신호를 명령하게 된다면, PX4로부터 생성된 motor 값, actuator 값 메시지가 JMAVSim으로 전달된다. 그 후, JMAVSim은 전달받은 메시지를 기반으로 생성된 sensor 값과 parameter 값 메시지를 PX4에 MAVLink API를 사용하여 전달하는 구조로 구성되어 있다[17].

2.5 시뮬레이션

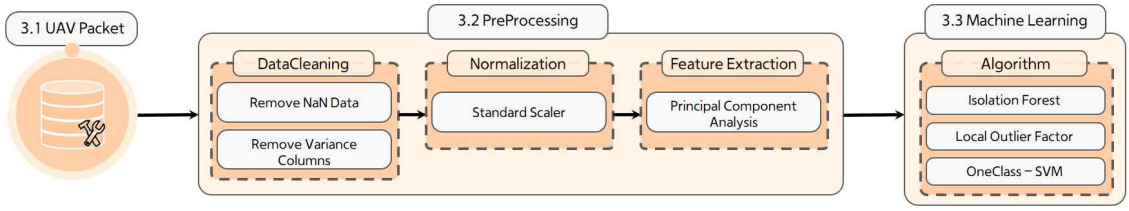
시뮬레이션 환경은 SITL(Software In The Loop), HITL(Hardware In The Loop) 2가지 환경으로 구분할 수 있다[18]. SITL 시뮬레이션 환경은 PX4, GCS, JMAVSim 시뮬레이터 등 단순히 소프트웨어로만 구성되며, HITL 시뮬레이션 환경은 SITL 시뮬레이션 환경과 다르게 드론의 비행 제어 컴퓨터를 모의하는 시뮬레이션 소프트웨어가 아닌 실제 드론을 제어하는 비행 제어 컴퓨터인 Pixhawk 하드웨어가 추가되어 구성된다. 비행 제어 컴퓨터는 컴퓨터 내부에서 센서가 동작하여 센서값을 계산하고 시뮬레이터에 메시지를 전달하기 때문에 가상환경이 아닌 실제 환경과 유사한 실험이 가능하다는 장점이 있다[19].

(Figure 2)는 HITL 시뮬레이션 환경에서 사용한 연결 구조를 그린 그림이다.



(Figure 2) HITL simulation structure

JMAVSim 시뮬레이터는 QGC와 UDP 통신을 하며 QGC에서 전달받은 메시지를 PX4로 전달하고, PX4로부터 전달받은 메시지를 QGC로 전달하는 게이트웨이 역할을 한다. 본 논문에서는 실제로 드론에서 임무를 수행할 때 사용할 모델을 생성하기 위해 실제 환경과 유사한 HITL 시뮬레이션 환



(Figure 3) Proposed HITL packet data based anomaly detection model creation structure

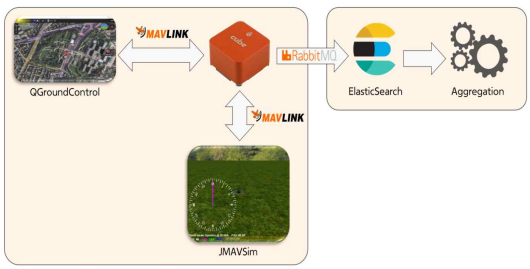
경을 구축하여 비행 제어 컴퓨터 내부에서 생성되는 데이터를 사용하여 실험을 진행한다.

3. 데이터 세트 소개 및 모델 구현

본 논문에서 제안하는 구조는 (Figure 3)과 같다. 무인비행체 패킷 데이터, PreProcessing, 기계 학습 알고리즘으로 구성되어 있으며, 본 절에서 각 파트에 대해 나뉘어 설명한다. 3.1절은 무인비행체 패킷 데이터 수집에 관해 설명한다. 3.2절은 PreProcessing 파트이며, 데이터 형식에 따른 데이터 전처리 과정을 서술한다. 3.3절은 기계 학습 알고리즘이 사용한 Hyper Parameter에 관해 설명한다.

3.1 무인비행체 패킷 데이터 수집

(Figure 4)는 무인비행체 패킷 데이터를 수집 구조를 간략하게 그린 그림이다. (Figure 4)에서 비행 제어 컴퓨터는 MAVLink 프로토콜을 통해 JMAVSim 시뮬레이터 및 QGC와 메시지를 송수신한다. 메시지에는 비행 제어 컴퓨터가 실제 환경에서 발생하는 형태로 데이터가 저장되어 있다.



(Figure 4) UAV packet data generator structure

해당 메시지는 실시간으로 RabbitMQ 메시지 프로토콜을 통해 엘라스틱서치 저장소에 저장되며, 실험에 사용된 데이터는 2023년 3월에 2일 동안 QGC를 통해 비행 임무를 수행하며 무인비행체의 정상적인 행위에 대한 데이터를 엘라스틱서치에 저장했다.

수집된 데이터는 초당 10회 발생하는 속성들이 있고, 50회 발생하는 속성들이 있으며 초당 발생하는 횟수가 일정하지 않은 것을 확인했다.

이를 해결하기 위해 엘라스틱서치에서 제공하는 Aggregation API를 통해 저장된 패킷 데이터를 1초 간격으로 집계하여 재구성하였다. 재구성된 데이터의 Feature는 총 10개의 Feature 들로 구성되어 있으며, Feature에 관한 설명은 <Table 1>과 같다.

<Table 1> Data set feature description

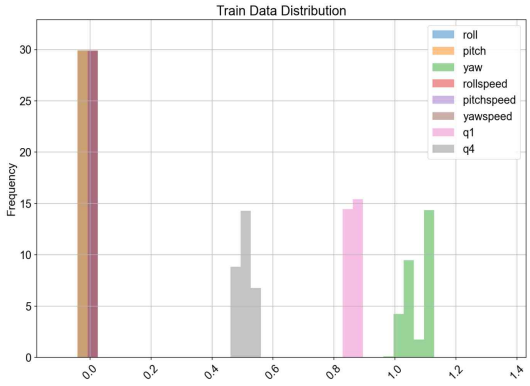
Feature	Description
roll	Roll angle (-pi.. + pi)
pitch	Pitch angle (-pi.. + pi)
yaw	Yaw angle (-pi.. + pi)
rollspeed	Roll angular speed
pitchspeed	Pitch angular speed
yawspeed	Yaw angular speed
q1	Quaternion component1, w(1 in null-rotation)
q2	Quaternion component2, x(0 in null-rotation)
q3	Quaternion component3, y(0 in null-rotation)
q4	Quaternion component4, z(0 in null-rotation)

3.2 데이터 전처리

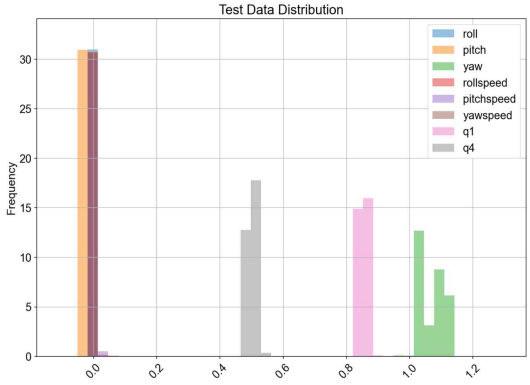
무인비행체 패킷 데이터는 (Figure 3)의 PreProcessing 파트와같이 모든 데이터에 대해 결측

값을 제거했고, 모델링 과정에서 Computation Cost를 줄이고 데이터 해석의 용이성을 높이는 Feature Selection을 수행했다. Feature Selection은 여러 방법이 있지만, 대표적인 Variance Threshold 기법을 사용했다. Variance Threshold 기법을 사용한 이유는 변수의 Variance가 작으면 모델이 예측하는 성능이 낮아지는 현상이 있기 때문이다. 따라서, Variance가 낮은 q2, q3 Feature를 제거했다.

(Figure 5)는 q2, q3 Feature를 삭제한 학습 데이터의 분포이며, (Figure 6)은 q2, q3 Feature를 삭제한 테스트 데이터의 분포이다.



(Figure 5) Train data distribution



(Figure 6) Test data distribution

학습 데이터와 테스트 데이터는 일반적으로 많이 사용하는 80 : 20 비율로 구성되어 있으며, 학습 데이터의 개수는 121,880개로 모두 정상 데이터로 구성되어 있다. 반면에 테스트 데이터의 개수는 30,471개의 정상 데이터와 287개의 비정상 데이터로 구성되어 있다. 그 후, q2, q3 Feature를 제거한 후 남은 8개의 Feature를 기반으로 PCA(Principal Component Analysis) 기법을 사용하기 전에 데이터 표준화를 수행했다. 그 이유는 데이터의 스케일에 따라 PCA의 설명 가능한 Variance가 달라질 수 있으므로 Standard Scaler 기법을 사용하여 표준화하였다.

표준화된 8개의 Feature를 PCA 기법을 통해 새로운 Feature를 생성했다. 기존의 8개의 Feature를 조합하여 새로운 Feature를 생성한 이유는 Variance가 커져야 데이터들 사이에 차이점이 명확해지고, 모델링을 하는 데 있어서 효과적이기 때문이다[20]. PCA 기법을 사용하여 기여율을 구하는 공식은 아래와 같으며, 각 성분의 설명 가능한 분산량과 기여율을 확인한 결과는 <Table 2>와 같다.

$$variance\ ratio = \frac{eigenvalue}{total\ eigenvalues} \quad (1)$$

<Table 2> Eigenvalues and contribution rates of each principal component

	Standard deviation	Proportion of variance	Cumulative proportion
pca1	4.7948	5.9934e-01	0.5993
pca2	2.2169	2.7711e-01	0.8764
pca3	0.4603	5.7538e-02	0.9339
pca4	0.2951	3.6897e-02	0.9708
pca5	0.1912	2.3906e-02	0.9948
pca6	0.0414	5.1751e-03	0.9997
pca7	0.0002	2.1609e-05	0.9999
pca8	0.0001	5.4516e-07	1.0000

누적 기여율(Cumulative proportion) 값이 1에 가까울수록 기존 데이터에 대한 설명력이 높다는 것을 의미한다. 일반적으로 누적 기여율 값이 85% 이상 90% 이하인 지점까지를 주성분 개수로 사용하기 때문에 본 연구에서는 주성분 개수를 2개로 사용하였다.

주성분 분석을 2개로 사용하여 PCA 기법을 수행

한 뒤 Test Data를 Class Feature 기준으로 각 Feature 들의 상관관계를 산점도 그림으로 확인한 결과는 (figure 7)과 같다.

(Figure 7) Class feature based test data pairplot

3.3 기계 학습 알고리즘

(Figure 3)의 3.4 파트와같이 실험에 사용된 알고리즘은 Isolation Forest(IF), LocalOutlierFactor(LOF), OneClass-SVM(OC-SVM) 3가지 기계 학습 알고리즘이다.

실험에 사용된 알고리즘의 최종 Hyper Parameter는 <Table 3>과 같다.

<Table 3> Hyper parameter used in the Machine learning algorithm

Algorithm	Hyper Parameter
IF	n_estimators = 60, max_samples = 'auto', contamination = 0.01, max_features = 1, n_jobs = -1
LOF	n_neighbors = 20, contamination = 0.01, novelty = True
OC-SVM	gamma = 'auto', nu = 0.01, kernel = 'rbf'

4. 평가 지표 및 실험 결과

4.1 평가 지표

학습된 모델의 성능 평가는 Precision, Recall, F1-Score, FPR(False Positive Rate), FNR(False Negative Rate)를 사용했으며 성능 평가 및 정확도의 수식은 다음과 같다.

$$Precision = \frac{TP}{TP+FP} \tag{2}$$

$$Recall = \frac{TP}{TP+FN} \tag{3}$$

$$F_1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{4}$$

$$FPR = \frac{FP}{TN+FP} \tag{5}$$

$$FNR = \frac{FN}{TP+FN} \tag{6}$$

(2), (3), (4), (5), (6) 수식에 대한 속성은 <Table 4>, <Table 5>와 같다.

<Table 4> Properties and descriptions used in confusion matrix

Property	True Value	Prediction	Result
True Negative	F	F	Correct
False Positive	F	T	Wrong
False Negative	T	F	Wrong
True Positive	T	T	Correct

<Table 5> Confusion matrix properties

		Predicted Value	
		False	True
Actual Value	False	True Negative (TN)	False Positive (FP)
	True	False Negative (FN)	True Positive (TP)

Precision(정밀도)은 생성한 모델이 True라고 예측한 것 중에서 실제로 True인 것의 비율이며, Recall(재현율)은 실제로 True인 데이터를 생성한 모델이 True라고 예측한 비율이다. F1-Score(조화평균)는 Precision과 Recall의 조화평균이다. 즉, 모델의 성능을 측정하는 데 있어서 Precision과 Recall은 유용하게 사용되지만 실제로 모델이 얼마나 효과적인지 설명할 방법이 없으므로 F1-Score라는 평가 기법을 사용하여 생성한 모델이 효과적인지 아닌지 판단하는 데 사용한다.

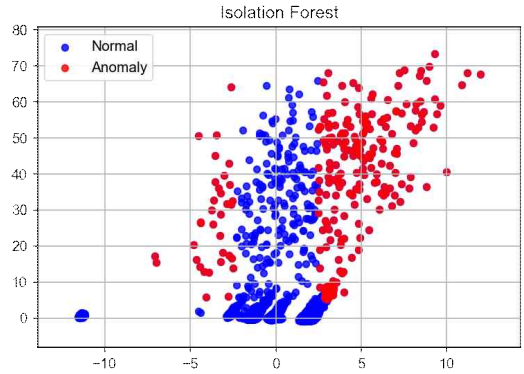
일반적으로 모델 성능 평가에 많이 사용되는 Accuracy(정확성)는 Precision, Recall과 달리 False를 False라고 예측한 예도 옳은 경우로 계산하기 때문에 무인비행체 패킷 데이터와 같이 정상 데이터와 비정상 데이터의 개수가 불균형할 경우 모델의 성능을 측정하는데 유의미한 결과로 사용하기에 적합하지 않다. 따라서, 이상 탐지 모델에서 중요한 문제점인 FPR과 FNR 수치를 통해 모델의 성능을 측정했다.

FPR은 실제로 False인 데이터 중에서 생성한 모델이 True라고 예측한 비율이다. 즉, 모델이 이상 데이터를 정상 데이터로 예측한 비율이다. 반대로 FNR 수치는 실제로 True인 데이터 중에서 생성한 모델이 False라고 예측한 비율이다. 즉, 모델이 정상 데이터를 False라고 예측한 비율이다.

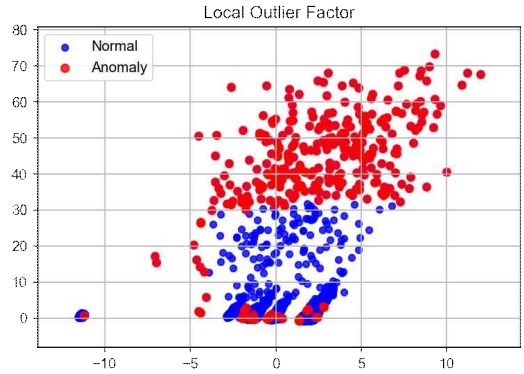
4.2 실험 결과

HITL 시뮬레이션 환경에서 수집한 무인비행체 패킷 데이터와 최적의 파라미터값을 사용하여 3개의 기계 학습 기반 이상 탐지 모델을 생성했다.

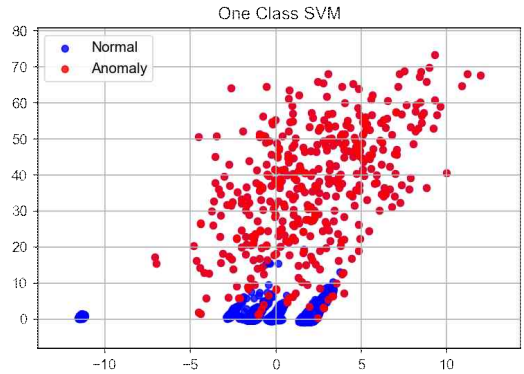
(Figure 8), (Figure 9), (Figure 10)은 생성한 이상 탐지 모델이 정상 데이터와 비정상 데이터를 예측한 결과이다.



(Figure 8) IF model based predict result



(Figure 9) LOF model based predict result



(Figure 10) OC-SVM model based predict result

<Table 6> Machine learning model evaluation result

Algorithm	Hyper Parameter	Precision	Recall	F1-Score	FPR	FNR
IF	contamination (0.1)	56%	95%	58%	0.01%	9.76%
LOF	contamination (0.1)	54%	89%	53%	9.04%	13.82%
OC-SVM	nu (0.1)	56%	95%	57%	0.01%	10.1%
IF	**contamination (0.01)**	**93%**	**76%**	**83%**	**4.65%**	**0.18%**
LOF	**contamination (0.01)**	**94%**	**85%**	**89%**	**9.81%**	**0.12%**
OC-SVM	**nu (0.01)**	**95%**	**99%**	**97%**	**0.26%**	**0.14%**
IF	contamination (0.001)	99%	51%	52%	97.67%	0.01%
LOF	contamination (0.001)	69%	50%	50%	99.48%	0.01%
OC-SVM	nu (0.001)	94%	97%	96%	5.68%	0.16%
IF	contamination (0.005)	78%	74%	76%	50.91%	0.47%
LOF	contamination (0.005)	83%	91%	87%	16.79%	0.51%
OC-SVM	nu (0.005)	85%	98%	91%	0.24%	0.53%

또한, 본 연구에서는 최적의 파라미터값을 찾기 위해서 <Table 6>과 같이 contamination parameter와 nu parameter를 미세하게 조정하여 실험을 진행했다. 많은 연구에서 모델의 성능을 평가할 때 Precision과 Recall 두 개의 성능이 높으면 좋은 모델이라고 판단한다. 하지만, 일반적으로 Precision과 Recall은 반비례 관계이기 때문에 두 개의 성능이 함께 고려되어야 한다.

<Table 6>의 결과를 보면 모델의 Recall이 Precision보다 낮게 측정된 모델이 있는데 이는 정상 데이터만 학습하였고, 하이퍼 파라미터값이 최적화되지 않았기 때문에 모델의 Recall이 낮게 나온 것으로 판단할 수 있다.

또한, 하이퍼 파라미터값이 0.1로 구성된 모델들은 전체적으로 정상 데이터를 제대로 예측하지 못하고 모두 비정상 데이터로 예측하는 문제점을 확인하였다. 반면에, 하이퍼 파라미터값이 0.005로 구성된 모델들은 SVM 모델을 제외하고 정상 데이터는 제대로 예측했지만, 비정상 데이터를 제대로 예측하지 못하는 문제점을 확인할 수 있다.

하이퍼 파라미터값이 0.01로 구성된 IF 모델과 LOF 모델, SVM 모델은 다른 파라미터값으로 구성된 것보다 우수한 성능을 보여주었기 때문에 해당 파라미터값을 사용하여 학습을 진행하였다.

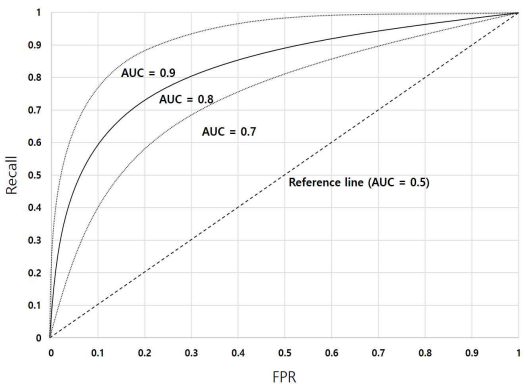
본 연구에서는 무인비행체 패킷 데이터가 비정상 데이터보다 정상 데이터가 많은 불균형한 데이터 세트기 때문에 앞서 설명한 평가 지표의 수치가 높게 측정되는 것으로 판단된다. 따라서, 앞서 측정한 지표는 모델이 정상 데이터를 잘 판단하는 모델인지 확인하는 데 사용하였고, 모델이 이상 데이터를 잘 판단하는지 확인하는 방법으로 FPR과 FNR를 측정하여 판단했다.

<Table 6>의 FPR과 FNR의 성능을 확인했을 때 정상 데이터를 제대로 예측하지 못한 모델의 성능이 더 높은 예도 있는데 이는 데이터 대부분을 이상 데이터로 예측했기 때문에 정상 데이터를 예측하지 못했다고 판단된다. 따라서 모델이 정상 데이터를 제대로 예측하는 모델이면서 FPR과 FNR 성능이 높게 나온

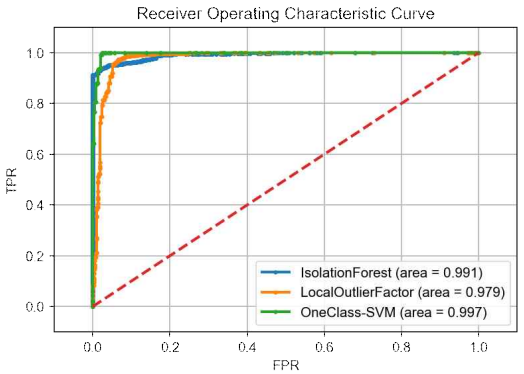
하이퍼 파라미터값은 확인했다.

그 결과, contamination과 nu 값이 0.01로 구성된 모델이 우수한 성능을 보여주었고, 그중에서도 SVM 모델이 전체 모델 중 가장 우수한 성능을 보여주었다. 추가로, 생성한 모델들이 정상적으로 생성되었는지 확인하기 위해서 ROC Curve를 통해 AUC 값을 확인하여 생성한 모델이 높은 정확도를 갖는지 확인했다.

AUC는 (Figure. 11)과 같은 ROC Curve에서 ROC 분석을 통해 그려지는 곡선 밑의 면적을 의미한다. 일반적으로 AUC 값이 0.7 보다 작은 경우 낮은 정도의 정확도, 0.7 이상 0.8 미만이면 보통 정도의 정확도, 0.8 이상 0.9 이하이면 높은 정확도를 갖는 것으로 해석할 수 있다[21].



(Figure 11) AUC Curve



(Figure 12) Machine learning model roc curve

(Figure 12)는 최적의 파라미터값을 사용하여 생성한 모델의 ROC Curve를 그린 그림이다. (Figure 12)에서 AUC 값을 보면 3개의 모델 모두 높은 정확도를 갖는 것을 확인할 수 있다.

5. 결 론

본 논문에서 수집된 무인비행체 패킷 데이터는 가상환경이 아닌 실제 환경과 유사한 환경에서 QGC를 통해 임무를 수행하며 수집되었으며, 정상 데이터와 비정상 데이터가 불균형한 데이터이다. 따라서, 기계학습 기반 이상 탐지 모델을 생성할 때 정상 데이터만을 학습하여 비정상 데이터를 예측하는 모델을 생성했다. 또한, 수집된 패킷 데이터는 Computation Cost를 줄이고 데이터 해석의 용이성을 높이기 위해 Feature Selection을 진행하였고, Feature Selection은 대표적인 Variance Threshold 기법을 사용했다.

Variance Threshold 기법을 사용한 이유는 Variance가 작으면 모델이 예측하는 성능이 낮아지는 현상이 있기 때문이다. 이를 해결하기 위해 Variance가 낮은 q2, q3 Feature를 제거하였다. 그 후, 남은 8개의 Feature를 기반으로 PCA 기법을 사용하여 새로운 Feature 들을 생성하여 데이터를 재구성하였다.

기존의 8개의 Feature를 조합하여 새로운 Feature를 생성한 이유는 Variance가 커져야 데이터들 사이에 차이점이 명확해지고, 모델링을 하는 데 있어서 효과적이기 때문이다. 재구성한 데이터를 pairplot을 통해 확인한 결과 데이터의 분산이 올바르게 구분되는 것을 확인할 수 있었다.

또한, 정상 데이터만을 학습하기 때문에 모델의 성능을 최적화하기 위해서 contamination parameter와 nu parameter 값을 미세하게 조정하여 기계 학습 기반 모델을 생성하는 데 최적화를 진행했다. 그 결과, IF 모델과 LOF 모델은 contamination 0.01 값을 사용하는 것이 가장 우수한 성능을 보여주었고, OC-SVM 모델은 nu 0.01 값을 사용한 모델이 가장 우수한 성능을 보여주었다. contamination과 nu parameter는 전체 데이터에서 이상 데이터의 비율을 의미하는 데 parameter 값이 0.01이 가장 우수한 성능을 보여

준 것을 보면 데이터가 불균형 데이터일 경우 정상 데이터와 비정상 데이터의 비율을 계산하여 parameter 값을 적절하게 사용하였을 때 모델이 가장 우수한 것을 알 수 있다.

향후 연구로 수집된 무인비행체 패킷 데이터를 활용하여 자세 제어뿐만 아닌 GPS 스푸핑, RF 신호 전파방해 등 다양한 공격에 대한 이상 탐지 연구를 진행할 것이다. 또한 무인비행체에 관련된 연구에 대해서 실험을 확장 시킬 수 있다.

참고문헌

[1] Restas, Agoston. "Drone applications for supporting disaster management." World Journal of Engineering and Technology 3.03 (2015): 316.

[2] Vashisht, Sahil, Sushma Jain, and Gagangeet Singh Aujla. "MAC protocols for unmanned aerial vehicle ecosystems: Review and challenges." Computer Communications 160 (2020): 443-463.

[3] Culver, Kathleen Bartzen. "From battlefield to newsroom: Ethical implications of drone technology in journalism." Journal of mass media ethics 29.1 (2014): 52-64.

[4] Alwateer, Majed, Seng W. Loke, and Niroshinie Fernando. "Enabling drone services: drone crowd sourcing and drone scripting." IEEE access 7 (2019): 110035-110049.

[5] 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.

[6] 이우진, 서경덕, and 채병민. "오픈소스 활용 드론에 대한 보안 위협과 Telemetry Hijacking 을 이용한 군용 드론 공격 시나리오 연구." 융합보안논문지 20.4 (2020): 103-112.

[7] Alladi, Tejasvi, et al. "Consumer IoT: Security vulnerability case studies and solutions." IEEE Consumer Electronics Magazine 9.2 (2020): 17-25.

[8] Choi, Yun-Jeong, and Seung-Soo Park. "Reinforcement mining method for anomaly detection and misuse detection using post-processing and training method." Proceedings of the Korean Information Science Society Conference. Korean Institute of Information Scientists and Engineers, 2006.

[9] 김태희, 강승호. "실시간 탐지를 위한 인공신경망 기반의 네트워크 침입탐지 시스템." 융합보안논문지 17.1 (2017): 31-38.

[10] Choi, S. O., and W. N. Kim. "Control system intrusion detection system technology research trend." Rev. KIISC 24.5 (2014): 7-14.

[11] Meier, Lorenz, Dominik Honegger, and Marc Pollefeys. "PX4: A node-based multithreaded open source robotics framework for deeply embedded platforms." 2015 IEEE international conference on robotics and automation (ICRA). IEEE, 2015.

[12] Lin, Tzu-Chiao, et al. "Realization of Intelligent-Inspection Functions of UAV in Transmission Grids Using Machine Learning." 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, 2023.

[13] Dardoize, Tristan, et al. "Implementation of ground control system for autonomous multi-agents using qgroundcontrol." 2019 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED UAS). IEEE, 2019.

[14] Khan, Navid Ali, Sarfraz Nawaz Brohi, and N. Z. Jhanjhi. "UAV's applications, architecture, security issues and attack scenarios: A survey." Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2019. Springer Singapore, 2020.

[15] Marty, Joseph A. Vulnerability analysis of the mavlink protocol for command and control of unmanned aircraft. AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT, 2013.

[16] Bae, Myeong-Jin, and Seong-Il Kim. "항공 드론 지상 제어 시스템 기술 동향." Korea Multimedia Society 20.1_2 (2016): 22-28.

[17] Wandarosanza, Rendy, Bambang Riyanto Trilaksono, and Egi Hidayat. "Hardware-In-the-Loop Simulation of UAV hexacopter for Chemical Hazard monitoring mission." 2016 6th International Conference on System Engineering and Technology (ICSET). IEEE, 2016.

[18] Hentati, Aicha Idriss, et al. "Simulation tools, environments and frameworks for UAV systems performance analysis." 2018 14th international wireless communications & mobile computing conference (iwcmc). IEEE, 2018.

[19] Bacic, Marko. "On hardware-in-the-loop simulation." Proceedings of the 44th IEEE Conference on Decision and Control. IEEE, 2005.

[20] 김한석, and 이수진. "기계학습 기반 랜섬웨어 공격 탐지를 위한 효과적인 특성 추출기법 비교분석." 융합보안논문지 23.1 (2023): 117-123.

[21] Muller, Matthew P., et al. "Can routine laboratory tests discriminate between severe acute respiratory syndrome and other causes of community-acquired pneumonia?." Clinical infectious diseases 40.8 (2005): 1079-1086.

〔저자소개〕

박 대 경 (Daekyeong Park)
2020년 2월 숭실대학교 학사
2022년 2월 세종대학교 석사
現, 한화시스템(주) 기반기술연구소
email :
daekyeong.park@hanwha.com

김 병 진 (Byeongjin Kim)
2008년 2월 경희대학교 학사
現, 한화시스템(주) 기반기술연구소
email :
bj001.kim@hanwha.com