J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr
Copyright ⓒ 2024 KSII

무선 주파수 신호 특성 데이터를 사용한 비지도 학습 기반의 위협 탐지 시스템☆

Unsupervised Learning-Based Threat Detection System Using Radio Frequency Signal Characteristic Data

박 대 경[1] 이 우 진[1] 김 병 진[1] 이 재 연[1*]
Dae-kyeong Park Woo-jin Lee Byeong-jin Kim Jae-yeon Lee

요 약

현재 4차 산업 혁명은 다른 혁명처럼 인류에게 커다란 변화와 새로운 삶을 가져다주고 있으며, 특히 빅데이터, 인공지능, ICT 등 다양한 기술들을 합쳐 응용할 수 있는 드론에 대한 수요와 활용도가 증가하고 있다. 최근에는 러시아-우크라이나 전쟁, 북한의 대남 정찰 등 위험한 군사 작전 및 임무를 수행하는 데 많이 사용되고 있으며 드론에 대한 수요와 활용도가 높아짐에 따라 드론의 안전성과 보안에 대한 우려가 커지고 있다. 현재 드론에 관련된 무선 통신 이상 탐지, 센서 데이터 이상 탐지 등 다양한 연구가 진행되고 있지만, 무선 주파수 특성 데이터를 사용하여 위협을 실시간으로 탐지하는 연구는 미비하다. 따라서, 본 논문에서는 실제 환경과 유사한 HITL(Hardware In The Loop) 시뮬레이션 환경에서 드론이 미션을 수행하는 동안 지상 제어 시스템과 통신하면서 발생하는 무선 주파수 신호 특성 데이터를 수집하여 특성 데이터가 정상 신호 데이터인지 비정상 신호 데이터인지 판단하는 연구를 진행하였다. 또한, 드론이 미션을 수행하는 중 실시간으로 위협 신호를 탐지할 수 있는 비지도 학습 기반의 위협 탐지 시스템 및 최적의 임계값을 제안한다.

☞ 주제어 : 무인비행체, 무선 주파수, 신호 특성, 위협 탐지, 비지도 학습, 드론

ABSTRACT

Currently, the 4th Industrial Revolution, like other revolutions, is bringing great change and new life to humanity, and in particular, the demand for and use of drones, which can be applied by combining various technologies such as big data, artificial intelligence, and information and communications technology, is increasing. Recently, it has been widely used to carry out dangerous military operations and missions, such as the Russia-Ukraine war and North Korea's reconnaissance against South Korea, and as the demand for and use of drones increases, concerns about the safety and security of drones are growing. Currently, a variety of research is being conducted, such as detection of wireless communication abnormalities and sensor data abnormalities related to drones, but research on real-time detection of threats using radio frequency characteristic data is insufficient. Therefore, in this paper, we conduct a study to determine whether the characteristic data is normal or abnormal signal data by collecting radio frequency signal characteristic data generated while the drone communicates with the ground control system while performing a mission in a HITL(Hardware In The Loop) simulation environment similar to the real environment. proceeded. In addition, we propose an unsupervised learning-based threat detection system and optimal threshold that can detect threat signals in real time while a drone is performing a mission.

☞ keyword : Unmanned Aerial Vehicle, Radio Frequency, Signal Characteristic, Threat Detection, Unsupervised Learning, Drone

1. 서 론

현재 4차 산업 혁명은 다른 혁명처럼 인류에게 커다란 변화와 새로운 삶을 가져다주고 있다. 특히, 인공지능(Artificial Intelligence) 기반의 다양한 디지털 기술들이 일반화되는 초지능(Super-Intelligence)과 모든 게 다 서로 연결된다는 초연결(Hyper-Connectivity)사회가 현실로 다가오고 있다.

또한, 4차 산업의 발달로 인해 빅데이터(Big Data), 인

1 Cyber Battlefield Team, Hanwha Systems., Gyeonggi-Do, 13524, Korea.
* Corresponding author (jaeyeon.lee@hanwha.com)
[Received 05 October 2023, Reviewed 24 October 2023, Accepted 06 November 2023]
☆ 본 논문은 2023년 정부(방위사업청)의 재원으로 국방과학연구소의 지원을 받아 수행된 미래도전국방기술 연구개발사업임 (No. 915024201)

공지능, ICT(Information and Communications Technology) 등 다양한 기술들을 합쳐 응용할 수 있는 드론에 대한 수요와 활용도가 점진적으로 증가하고 있다[1]. 예를 들어, 농업, 무인 배송, 보안, 수색, 구조, 군사 작전 등 다양한 산업에서 활용되고 있다[2, 3].

특히 최근에는 러시아-우크라이나 전쟁, 북한의 대남 정찰 등[4] 위험한 군사 작전 및 임무를 사람이 직접 탑승하지 않고 수행할 수 있어서 인명피해 없이 위험한 작전 및 임무를 수행할 수 있으며, 최근 많은 연구자가 드론을 활용한 연구를 진행하고 있다[5, 6].

하지만, 드론에 대한 수요와 활용도가 점점 많아질수록 의존도가 높아지는데 이에 따라 드론의 안전성과 보안성에 대한 우려가 커지고 있다. 현재 드론의 제어권을 탈취하거나[7] 애플리케이션과 드론이 통신하는 채널을 탈취하는 등[8] 실시간으로 다양한 취약점들이 공개되고 있다. 또한, 공개된 취약점 외에도 악의적인 의도를 가진 공격자는 알려지지 않은 취약점을 악용할 수 있으므로 지능적으로 다양해지는 취약점 중에서도 알려지지 않은 취약점을 악용하는 공격을 방어하는 것은 중요한 문제이다. 이러한 문제를 해결하기 위해 가장 널리 사용되는 방법은 위협 탐지 시스템(Threat Detection System)이다.

따라서, 본 논문에서의 목표는 드론이 임무를 수행하는 동안에 SDR(Software Defined Radio) 플랫폼 중 하나인 SIK Radio를 통해 지상 제어 시스템(Ground Control System, GCS)과 통신하면서 발생하는 무선 주파수(Radio Frequency, RF) 신호 특성 데이터를 활용하여 해당 신호가 아군의 신호인지 아니면 악의적인 의도를 가진 공격자의 신호인지 판단하는 것이다. RF 신호 특성 데이터를 활용하여 아군의 신호인지 아닌지 판단하는 방법은 크게 지식 기반(오용탐지, Misuse Detection)[9] 방법과 행위 기반(이상 탐지, Anomaly Detection)[10] 방법 두 가지로 구분할 수 있다.

지식 기반 방법은 기존에 알고 있는 데이터 또는 미리 정의된 데이터를 기반으로 위협을 판단하는 방식이며, 단순히 패턴을 비교하여 위협인지 아닌지 판단하기 때문에 속도가 빠르고 구현이 쉽지만 알려지지 않은 데이터이거나 정의되지 않은 데이터에 대해 탐지할 수 없다. 반대로, 행위 기반 방법은 정상적인 데이터와 평균적인 데이터를 넘어 데이터의 급격한 변화가 있을 때 위협으로 판단한다. 하지만, 위협인지 아닌지 결정하는 임계값(Threshold)을 설정하는 데 어려움이 있지만 미리 정의되지 않은 데이터에 대해 위협을 탐지할 수 있다는 장점이 있다. 또한, 수많은 정상적인 데이터의 패턴을 미리 정의한다는 것은 매우 어려우며 학습하지 못한 아군의 신호 특성 데이터의 패턴을 위협 데이터로 판단한다는 단점이 있다[11].

실험에 사용된 데이터 세트는 HITL(Hardware In The Loop) 시뮬레이션 환경에서 임무를 수행하는 동안 지상 제어 시스템과 통신하면서 발생하는 RF 신호 특성 데이터이다. 드론에 관련된 연구로 무선 통신 이상 탐지, 센서 데이터 이상 탐지 등[12, 13] 다양한 연구가 진행되고 있지만, RF 특성 데이터를 사용하여 위협을 실시간으로 탐지하는 연구는 미비하다.

이러한 필요성에 근간하여 본 논문에서는 순차 데이터를 학습할 때 우수한 성능을 보이는 알고리즘을 통해 드론이 임무를 수행하면서 실시간으로 위협을 탐지할 수 있는 비지도 학습 기반의 위협 탐지 시스템을 제안하며, 구성은 다음과 같다. 2장에서는 드론 위협 탐지 관련 연구에 관한 이전 연구와 실험에 사용될 딥러닝 모델에 관해 간단히 소개한다. 다음으로 3장에서는 비지도 학습 기반의 위협 탐지 시스템 구현에 대하여 설명한다. 이어서 4장에서는 위협 탐지 시스템의 성능 비교를 진행한다. 마지막으로 5장에서는 본 연구의 최종 결론과 향후 연구에 관해 기술한다.

2. 관련 연구

2.1 드론 위협 탐지 관련 연구

Principi 등[14]은 전기 모터의 고장과 결함을 탐지하는데 비지도 학습 기반의 Deep Autoencoders를 제안했다. 제안된 모델은 정상 데이터만을 사용하여 학습하며, 생성된 모델은 OneClass-Support Vector Machine 알고리즘과 비교하여 성능을 평가하였다.

Ahn 등[15]은 실제 비행 테스트 데이터를 사용하여 군집 드론 비행에 대한 비정상적인 동작을 탐지할 수 있는 기계학습 기반 프레임워크를 제안했다.

Da 등[16]은 무인 항공기의 비행 이상 및 네트워크를 감지할 수 있는 Intrusion Detection System을 제안했다. 무인 항공기가 비행 중에 발생하는 이상은 비지도 학습 기반의 Stacked Autoencoder 알고리즘을 사용하고 지도 학습 기반의 LightGBM 알고리즘을 사용하여 Denial of Service 공격을 탐지한다.

Yang 등[17]은 무인 항공기의 온보드 로그를 학습하여 발생하는 문제를 해결하기 위해 Software In The Loop 시뮬레이션 환경을 기반으로 하는 Time Line Modeling 방법을 제안했다. 해당 방법을 사용하면 데이터 불균형 문제

를 해결할 수 있으며, Sequential Minimal Optimization, Random Forest, Convolutional Neural Network 알고리즘을 비교하여 성능을 평가한다.

Baskaya 등[18]은 자이로스코프와 가속도계 데이터를 사용하여 Support Vector Machine 모델을 생성하였으며, 해당 모델을 통해 무인 항공기의 결함을 감지하는 방법과 공간 특징 차원을 줄이는 방법으로 주성분 분석 알고리즘을 제안했다.

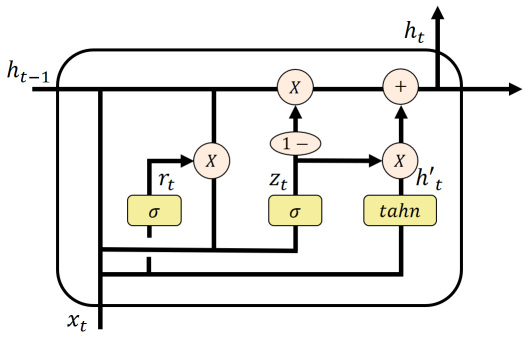
Benini 등[19]은 Linear Discriminant Analysis 알고리즘을 기반으로 무인 항공기의 관성 측정 장치의 가속도 정보 데이터와 주파수 영역 분석을 통해 무인 항공기의 액츄에이터 결함을 탐지한다.

Senigagliesi 등[20]은 무인 항공기와 지상 기지국이 통신하는 동안 발생하는 네트워크 데이터를 사용하여 Autoencoder 기반의 모델을 생성하였으며, 해당 모델을 통해 정상 데이터와 공격자한테서 오는 데이터는 변칙 데이터로 분류하는 방법을 제안했다.

2.2 딥러닝 모델

2.2.1 GRU (Gated Recurrent Unit)

GRU 알고리즘은 2014년 Chung 등[21]이 최초로 제안한 알고리즘이며, LSTM(Long Short-Term Memory) 알고리즘을 간략하게 만든 구조로 RNN(Recurrent Neural Network) 알고리즘 중 하나이다.

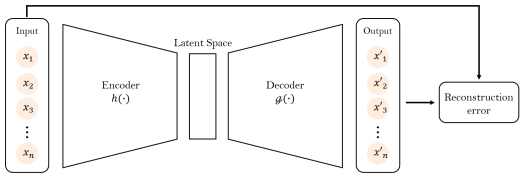


(그림 1) 게이트 순환 유닛 알고리즘 구조
(Figure 1) GRU algorithm structure

GRU 알고리즘은 그림 1과 같은 구조로 구성되어 있으며, LSTM 알고리즘에서 이전 정보를 기억할 것인지 기억하지 않을 것인지 결정하는 셀 상태가 없으며, LSTM 알고리즘에서 셀 상태가 수행하는 역할을 은닉층 값이 대신 수행한다. 또한, 데이터의 양이 적을 때 LSTM 알고리즘을 사용하는 것보다 더 유리하다고 알려져 있으며 LSTM 알고리즘보다 학습 속도가 빠르지만, 비슷한 성능을 보여주기 때문에 많은 연구에서 사용되고 있다.

2.2.2 AE (AutoEncoder)

AE 알고리즘은 인공 신경망 알고리즘 중 하나로, 입력값과 출력값이 같은 값을 가질 수 있도록 학습하는 특징이 있다[22]. AE 알고리즘의 구조는 그림 2와 같이 입력값으로 들어온 학습 데이터의 정보를 저차원의 데이터로 정보를 축약하는 인코더와 축약된 정보를 다시 원래 데이터로 복원하는 디코더로 구성되어 있어서 비지도 학습에 많이 사용된다. 또한, AE 알고리즘은 입력값과 복원된 출력값의 차이를 최소화하는 방식으로 학습하며, 입력값과 복원된 출력값 차이가 임계값을 넘어서면 이상 데이터로 판단한다.



(그림 2) 오토인코더 알고리즘 구조
(Figure 2) AE algorithm structure

본 논문에서는 드론이 임무를 수행하는 동안 실시간으로 위협을 탐지할 수 있는 모델을 생성하기 위해, 순차 데이터를 사용하면 우수한 성능을 보여주면서 경량화되어 있는 GRU 알고리즘을 이용하여 AE 구조로 모델을 구성하였으며, 복원 오차의 크기를 이용해 아군 신호와 위협 신호를 구분하였다.

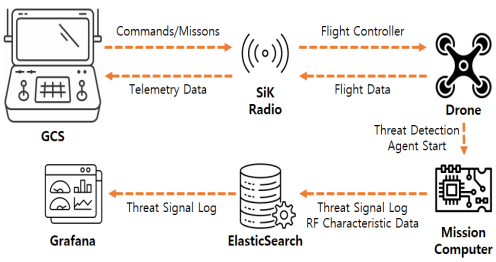
3. 비지도 학습 기반의 위협 탐지 시스템 구현

3.1 위협 탐지 시스템 구조

본 논문에서 제안하는 위협 탐지 시스템 구조는 그림 3과 같다. 지상 제어 시스템이 드론에 임무, 미션 명령 등을 SiK Radio를 통해 전달하면 드론은 임무, 미션 등을 수행하면서 발생하는 Telemetry 데이터를 지상 제어 시스템에 반환한다. 또한, 드론이 임무, 미션 등을 수행하기 시작하면 드론에 탑재된 미션 컴퓨터에서 위협 신호를 탐

지하는 에이전트가 임무, 미션이 종료될 때까지 프로세스로 실행된다.

RF 신호 특성 데이터는 1초에 한 번 발생하기 때문에 위협 신호인지 아닌지 판단은 1초에 한 번씩 진행한다. 위협 신호가 발생하였을 경우 위협 신호 로그와 해당 데이터를 로컬 환경에 저장하고, File Tailer 기능을 통해 실시간으로 Elasticsearch에 저장한다. 저장된 데이터는 사용자가 편리하게 볼 수 있도록 Grafana를 이용하여 시각화하여 대시보드를 제공한다.



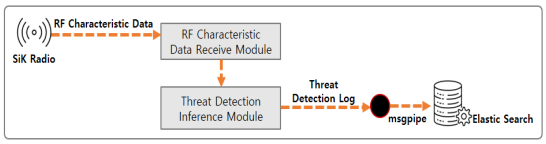
(그림 3) 위협 탐지 시스템 구조
(Figure 3) Threat detection system structure

3.2 미션 컴퓨터(Threat Detection Agent)

그림 3의 Mission Computer는 드론이 임무, 미션 등을 수행할 때 위협 탐지 에이전트를 임무, 미션 등이 끝날 때까지 프로세스로 수행하며, 본 논문에서 제안하는 위협 탐지 에이전트 프로세스는 그림 4와 같다.

위협 탐지 에이전트는 RF 신호 특성 데이터 수신 모듈을 통해 SiK Radio에서 RF 신호 특성 데이터를 받아오며 해당 데이터를 위협 탐지 추론 모듈에 전달한다.

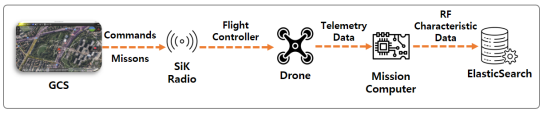
위협 탐지 추론 모듈은 위협 탐지 모델을 통해 해당 RF 신호 특성 데이터가 위협 신호인지 아닌지 판단하며, 위협 신호로 판단되면 File Tailer 기능을 수행하는 msgpipe를 통해 Elasticsearch에 위협 탐지 로그가 실시간으로 저장된다.



(그림 4) 위협 탐지 에이전트 프로세스
(Figure 4) Threat detection agent process

3.3 무선 주파수 신호 특성 데이터

그림 5는 드론이 명령, 임무를 수행하면서 발생하는 RF 신호 특성 데이터를 수집하기 위해 제안하는 구조를 간략하게 그린 그림이다.



(그림 5) 무선 주파수 신호 특성 데이터 수집 구조
(Figure 5) Radio frequency signal characteristic data collection structure

모델을 학습하는 데 사용된 RF 신호 특성 데이터는 2023년 9월 2일 지상 제어 시스템에서 드론에 임무, 미션 등을 명령했을 때 임무를 수행하며 발생하는 RF 신호 특성 데이터를 Elasticsearch에 저장하였다. 또한, 테스트 데이터는 2023년 9월 7일 드론이 임무, 미션 등을 수행하고 있을 때 위협 신호를 실제로 발생시켰으며, 위협 신호는 드론이 임무, 미션 등을 수행하지 못하도록 하는 취약점 공격 등이 해당한다. 기존에 많은 연구는 RF 특성 데이터에서 RSSI(Received Signal Strength Indicator) 값 하나를 이용하여 시계열 분석을 진행하거나 이상 탐지를 진행하였다.

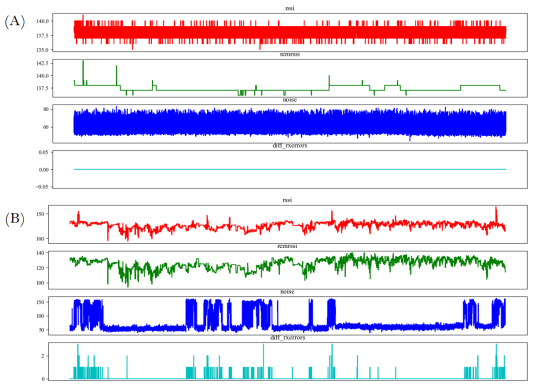
(표 1) 학습에 사용된 무선 주파수 신호 특성 데이터
(Table 1) Radio frequency signal characteristic data used for training

Feature	Description
rssi	The rssi parameter is the RSSI (signal strength) level that the local radio will receive.
remrssi	The remrssi parameter is the RSSI that the remote radio listens for.
noise	The noise parameter is the noise caused by someone else operating a nearby radio that uses the same frequency as the gcs radio.
diff_rxerrors	The diff_rxerrors parameter is the error value and is the difference between the previous accumulated value and the current error value.

하지만, 해당 방법을 드론에 적용하기에는 비행 중에 RSSI 값이 너무 많이 달라지거나 주파수 간섭으로 인해

RSSI 속성 하나만을 이용하여 위협 신호를 탐지하기에는 어려움이 있었다. 따라서, 표 1과 같이 4개의 Feature를 사용하여 위협 탐지 모델을 생성하는 데 사용하였으며, 수집된 데이터는 초당 1회 발생하는 순차 데이터이다.

그림 6은 해당 Feature를 시각화한 그림이다. 그림 6의 (A)는 위협 탐지 모델을 생성하기 위해 사용되는 학습 데이터로 모두 정상 데이터로 구성되어 있으며, (B)는 생성된 모델의 성능을 확인하기 위해 사용되는 위협 신호 데이터가 포함된 테스트 데이터이다.



(그림 6) RF 신호 특성 데이터 세트
(Figure 6) RF signal characteristic data set

3.4 위협 신호 탐지 모델

위협 신호 탐지 모델의 구조는 2.2 딥러닝 모델 파트에서 살펴본 것과 같이 순차 데이터를 분석할 때와 적은 데이터의 양을 학습할 때 우수한 성능을 보여주는 GRU 알고리즘을 사용했다. 또한, 정상 데이터만을 학습하여 위협 신호 데이터를 탐지하기 위해서 AE 구조를 모방하여 GRU 알고리즘을 기반으로 AE-GRU 모델을 생성했다.

(표 2) 위협 탐지 모델 구조
(Table 2) Threat detection model structure

Algorithm	Hyperparameter
AE-GRU	Encoder: GRU(64 - 32) return_sequence: True RepeatVector Decoder: GRU(32 - 64) return_sequence: True TimeDistributed(Dense) optimizer: adam loss: mae

생성된 위협 탐지 모델의 구조는 표 2와 같으며, 생성된 모델은 미션 컴퓨터의 위협 탐지 에이전트 프로세스에서 사용되기 때문에 모델의 깊이가 깊을수록 추론하는 데 많은 리소스가 필요하므로 실시간으로 위협을 탐지하기 위해서 모델을 깊게 설계하지 않았다. 또한, 모델을 최적화하기 위해 사용된 오차 함수는 모든 오차에 동일한 가중치를 부여하여 적은 양의 이상 데이터가 있을 때, 과적합 현상을 방지하기 위하여 MAE(Mean Absolute Error) 함수를 사용하였다.

4. 모델 평가 및 실험 결과

4.1 모델 평가

생성된 위협 탐지 모델의 평가는 Confusion Matrix 값을 기반으로 Precision, Recall, F1-Score, Accuracy, FPR (False Positive Rate), FNR(False Negative Rate)를 계산하여 가장 우수한 성능을 보이는 임계값을 찾는 데 사용하였다[23, 24].

Precision은 위협 탐지 모델이 정상이라고 예측한 것 중에서 정상인 데이터의 비율이며, Recall은 정상 데이터 중에서 위협 탐지 모델이 정상이라고 예측한 비율이다. F1-Score는 Precision과 Recall의 조화평균으로, Precision과 Recall을 통해 위협 탐지 모델이 얼마나 효과적인지 설명할 수 없으므로 F1-Score를 통해 판단한다. Accuracy는 위협 데이터를 위협으로 예측한 때도 올바른 경우로 계산되기 때문에, 불균형 데이터에는 대상이 편향되어 있어 모델의 성능을 파악하는 데 사용하기에는 어렵다는 단점이 있다.

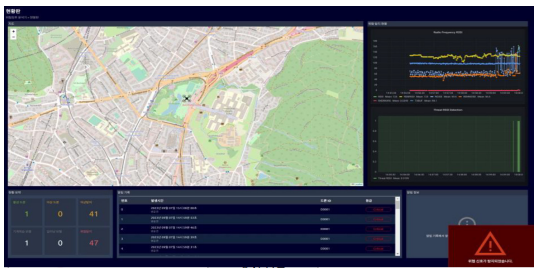
FPR은 위협 데이터 중에서 위협 탐지 모델이 정상 데이터라고 예측한 비율이며, FAR은 정상 데이터 중에서 위협 탐지 모델이 위협 데이터로 예측한 비율이다.

4.2 실험 결과

드론이 지상 제어 시스템에서 받은 명령, 임무를 수행하며 발생하는 RF 신호 특성 데이터를 사용한 오토 인코더 구조를 모방한 GRU 알고리즘 기반 위협 탐지 모델을 생성했다. 생성된 위협 탐지 모델을 사용하여 위협 신호를 탐지하는 최적의 임계값을 찾기 위해 표 3과 같이 임계값을 미세하게 조정하여 실험을 진행했다. 표 3에 설정된 임계값은 재구성 손실 값의 평균값과 표준 편차값을 더한 값을 기준으로 ± 0.5 값을 사용하여 실험을 진행했

다. 일반적으로 모델의 성능을 평가할 때 Precision과 Recall 값을 확인하여 좋은 모델인지 아닌지 판단하는데, 본 논문에서는 Precision과 Recall의 조화 평균값인 F1-Score와 FPR, FAR 값을 기준으로 임계값을 선택하였다. F1-Score를 기준으로 사용한 이유는 Precision과 Recall은 반비례 관계이기 때문에 두 개의 성능이 동시에 비교되는 게 좋으므로 위협 신호 탐지 모델이 정상 데이터를 잘 판단하는 모델인지 측정하는데, 해당 수식을 사용했다. 또한, FPR과 FAR을 기준으로 잡은 이유는 보안에서 중요하게 생각하는 오탐율을 측정하여 오탐율을 최소한으로 줄이기 위해서이다.

그 결과, 임계값이 0.8을 사용하여 위협 신호를 탐지할 때 정상 데이터와 비정상 데이터를 잘 판단할 뿐만 아니라 다른 임계값들보다 FPR과 FAR 값이 비교적 우수한 것을 확인하였다. 따라서, 임계값을 0.8로 설정하여 드론이 미션, 임무를 수행하는 동안 위협 탐지 에이전트가 실시간으로 위협을 탐지하였으며, 탐지 결과를 시각화한 대시보드는 그림 7과 같다.



(그림 7) 위협 탐지 시스템 대시보드
(Figure 7) Threat detection system dashboard

그림 7을 보면 위협 신호가 탐지되면 오른쪽 아래에 위협 신호가 발생했다는 알람을 발생하며, 알람뿐만 아니라 그림 7의 우측 그래프는 무선 신호 특성 데이터가 실시간으로 어떻게 들어오는지 확인할 수 있는 그래프와 위협 신호가 탐지된 개수를 카운트하는 그래프도 확인할 수 있다.

5. 결 론

본 논문에서는 드론이 미션, 임무를 수행하는 중 실시간으로 위협 신호를 탐지할 수 있는 위협 탐지 시스템을 제안하고, 실제 미션, 임무를 수행 중인 드론을 추락시킬 수 있는 위협 신호를 발생했을 때 실시간으로 위협 신호를 탐지하는 것을 확인하였다.

또한, 모델을 학습하는 데 사용하기 위해 수집된 RF 신호 특성 데이터는 가상환경이 아닌 실제 환경과 유사한 HITL 시뮬레이션 환경에서 드론이 미션, 임무를 수행하는 동안 지상 제어 시스템과 통신하는 과정에서 수집되었으며, 정상 데이터와 비정상 데이터가 불균형한 데이터이다. 따라서, 딥러닝 기반의 위협 신호 탐지 모델을 생성할 때 정상 데이터만을 학습하여 비정상 데이터를 예측하는 모델을 생성했다.

본 논문에서 제안하는 위협 신호 탐지 모델은 미션 컴퓨터에서 실시간으로 위협을 탐지하며, 순차 데이터에 우수한 성능을 보여주면서 적은 데이터양을 학습할 때 유리한 GRU 알고리즘을 기반으로 오토인코더 알고리즘의 구조를 모방하여 모델을 생성했다.

특히, 비지도 학습에 많이 사용되는 오토인코더 알고리즘은 입력값과 복원된 출력값의 차이를 최소화하는 방

(표 3) 임계값별 위협 신호 탐지 모델 성능
(Table 3) Threat signal detection model performance by threshold

Threshold	Precision (%)	recall (%)	f1-score (%)	accuracy (%)	FPR (%)	FAR (%)
0.5	75.79	72.69	66.25	66.51	0.02	0.54
0.6	76.38	76.03	71.43	71.43	0.05	0.44
0.7	78.01	79.25	76.06	76.14	0.08	0.34
0.8	**80.17**	**81.92**	**80.22**	**80.61**	**0.12**	**0.23**
0.9	74.04	74.52	84.24	75.44	0.29	0.21
1.0	69.61	68.54	68.91	71.41	0.44	0.19
1.1	65.61	63.17	63.45	67.81	0.56	0.17
1.2	63.01	59.82	59.58	65.64	0.64	0.16
1.3	61.21	57.56	56.64	64.31	0.71	0.14
1.4	61.19	56.61	54.94	64.15	0.75	0.12
1.5	59.88	54.82	51.92	63.28	0.81	0.09

식으로 학습하며 입력값과 출력값의 차이가 임계값을 넘어가면 이상 데이터로 판단하기 때문에 임계값을 어떻게 설정하는가에 따라 모델의 성능이 크게 차이 난다는 특징이 있다.

또한, 학습에 사용된 RF 신호 특성 데이터는 비행 중에 RSSI 값이 너무 많이 달라지거나 주파수 간섭으로 인해 RSSI 속성 하나만을 사용하여 위협 신호를 탐지하기에는 어려움이 있다고 판단하여 기존 연구와는 다르게 표 1과 같이 4개의 Feature를 학습하는 데 사용하였다.

4개의 Feature를 학습하여 생성된 비지도 학습 기반의 위협 탐지 모델을 통해 위협 신호를 탐지하는 최적의 임계값을 찾기 위해서 임계값을 미세하게 조정하여 실험을 진행하였으며, 임계값은 재구성 손실 값의 평균과 표준편차값을 더한 기준으로 ± 0.5 값을 사용하여 실험을 진행했다.

그 결과, 생성된 모델은 임계값을 0.8로 설정하여 사용하는 것이 전체적으로 가장 우수한 성능을 보여주었고, 다른 임계값들보다 FPR과 FAR 값이 비교적 우수한 것을 확인하였다. 이후, 드론이 미션, 임무를 수행하는 동안 미션 컴퓨터에서 위협 신호를 실시간으로 탐지하였으며 실제로 드론에 위협 신호를 보냈을 때 위협 신호가 1초 이내에 탐지되면서 알람을 발생하며, 대시보드를 통해 실시간으로 위협 신호가 발생한 것을 확인할 수 있었다.

향후 연구로 본 논문에서 제안된 위협 탐지 시스템을 기반으로 위협 신호가 발생하였을 때 적의 공격 복잡도를 높이고 임무, 미션을 성공적으로 완수하기 위해 드론의 정보를 의도적으로 변이하는 이동 표적 방어(Moving Target Defense, MTD)에 관한 연구를 진행할 것이다. 또한 드론 및 무선 통신에 관련된 연구에 대해서 실험을 확장시킬 수 있다.

참고문헌(Reference)

[1] Lee, Yang-Kyoo, et al. “A Study on the Anomaly Prediction System of Drone Using Big Data.” Journal of Internet Computing and Services, vol. 21, no. 2, pp. 27-37, Apr. 2020. https://doi.org/10.7472/jksii.2020.21.2.27.

[2] Vashisht, Sahil, Sushma Jain, and Gagangeet Singh Aujla, “MAC protocols for unmanned aerial vehicle ecosystems: Review and challenges,” Computer Communications, vol. 160, pp. 443-463, 2020. https://doi.org/10.1016/j.comcom.2020.06.011

[3] Restas, Agoston. “Drone applications for supporting disaster management,” World Journal of Engineering and Technology, vol. 3, No. 3C, pp. 316-321, 2015. http://doi.org/10.4236/wjet.2015.33C047

[4] Lee, Woojin, et al. “A Study on the Generation and Transmission of Drone Jamming Signals Based on the MAVLink Protocol,” Jouranl of Information and Security, vol. 23, no. 2, Korea Convergence Security Association, pp. 75 - 84, 30 June 2023. https://doi.org/10.33778/kcsa.2023.23.2.075

[5] Alwateer, Majed, Seng W. Loke, and Niroshinie Fernando, “Enabling drone services: drone crowdsourcing and drone scripting,” IEEE access, Vol. 7, pp. 110035-110049, 2019. https://doi.org/10.1109/ACCESS.2019.2933234

[6] Culver, Kathleen Bartzen, “From battlefield to newsroom: Ethical implications of drone technology in journalism,” Journal of mass media ethics, vol. 29, Issue 1, pp. 52-64, 2014. https://doi.org/10.1080/08900523.2013.829679

[7] Lee, Woojin, Kyungdeok Seo, and 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. https://doi.org/10.33778/kcsa.2020.20.4.103

[8] 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. https://doi.org/10.1109/NOMS.2016.7502939

[9] Bhushan, Bharat, “Intrusion detection system (IDS) for security enhancement in wireless sensing applications,” Innovations in Electronics and Communication Engineering: Proceedings of the 9th ICIECE 2021. Singapore: Springer Singapore, 39-49, 2022. https://doi.org/10.1007/978-981-16-8512-5_5

[10] Yeruva, Ajay Reddy, et al., “Anomaly Detection System using ML Classification Algorithm for Network Security,” 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), IEEE, 2022.

https://doi.org/10.1109/IC3I56241.2022.10072303

[11] Urbina, David I., et al., “Survey and new directions for physics-based attack detection in control systems,” Gaithersburg: US Department of Commerce, National Institute of Standards and Technology, 2016. https://doi.org/10.6028/NIST.GCR.16-010

[12] 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. https://doi.org/10.1109/NOMS.2016.7502939

[13] Lu, Huimin, et al., “Motor anomaly detection for unmanned aerial vehicles using reinforcement learning,” IEEE internet of things journal, Vol. 5, Issue 4, pp. 2315-2322, 2017. https://doi.org/10.1109/JIOT.2017.2737479

[14] Principi, Emanuele, et al., “Unsupervised electric motor fault detection by using deep autoencoders,” IEEE/CAA Journal of Automatica Sinica, Vol. 6, Issue 2, pp. 441-451, 2019. https://doi.org/10.1109/JAS.2019.1911393

[15] Ahn, Hyojung, et al. ″Learning-based anomaly detection and monitoring for swarm drone flights.″ Applied Sciences 9.24 (2019): 5477. https://doi.org/10.3390/app9245477

[16] Da Silva, Leandro Marcos, et al., “Anomaly-Based Intrusion Detection System for In-Flight and Network Security in UAV Swarm,” 2023 International Conference on Unmanned Aircraft Systems (ICUAS), IEEE, 2023. https://doi.org/10.1109/ICUAS57906.2023.10155873

[17] Yang, Tao, et al., “Acquisition and Processing of UAV Fault Data Based on Time Line Modeling Method,” Applied Sciences, 13(7), 4301, 2023. https://doi.org/10.3390/app13074301

[18] Baskaya, Elgiz, Murat Bronz, and Daniel Delahaye. ″Fault detection & diagnosis for small UAVs via machine learning.″ 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC). IEEE, 2017. https://doi.org/10.1109/DASC.2017.8102037

[19] Benini, Alessandro, et al., “Fault detection of a VTOL UAV using acceleration measurements,” 2019 18th European Control Conference (ECC), IEEE, 2019. https://doi.org/10.23919/ECC.2019.8796198

[20] Senigagliesi, Linda, Gianluca Ciattaglia, and Ennio Gambi. “Autoencoder based Physical Layer Authentication for UAV Communications,” 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), IEEE, 2023. https://doi.org/10.1109/VTC2023-Spring57618.2023.10200623

[21] Chung, Junyoung, et al., “Empirical evaluation of gated recurrent neural networks on sequence modeling,” arXiv preprint arXiv:1412.3555, 2014. https://doi.org/10.48550/arXiv.1412.3555

[22] Aygun, R. Can, and A. Gokhan Yavuz, “Network anomaly detection with stochastically improved autoencoder based models,” 2017 IEEE 4th international conference on cyber security and cloud computing (CSCloud), IEEE, 2017. https://doi.org/10.1109/CSCloud.2017.39

[23] Vujović, Ž., “Classification model evaluation metrics,” International Journal of Advanced Computer Science and Applications, Vol. 12, Issue 6, pp. 599-606, 2021. https://doi.org/10.14569/IJACSA.2021.0120670

[24] Catal, Cagatay, “Performance evaluation metrics for software fault prediction studies,” Acta Polytechnica Hungarica, 9(4), 193-206, 2012. http://hdl.handle.net/11413/1662

◐ 저 자 소 개 ◑

박 대 경(Dae-kyeong Park)
2020년 2월 숭실대학교 컴퓨터공학(공학사)
2022년 2월 세종대학교 일반대학원 컴퓨터공학(공학석사)
2022년~현재 한화시스템(주) 기반기술연구소 연구원
관심분야 : 사이버 상황인식, 이상탐지, 정보보호, 시스템 침입분석 etc.
E-mail : daekyeong.park@hanwha.com

이 우 진(Woo-jin Lee)
2018년 7월 부산대학교 정보컴퓨터공학부(공학사)
2018년~현재 한화시스템(주) 기반기술연구소 선임연구원
관심분야 : SW 역공학, 취약점 분석, 컴퓨터공학, 정보보안 etc.
E-mail : holinder4s@hanwha.com

김 병 진(Byeong-jin Kim)
2008년 2월 경희대학교 컴퓨터공학과(공학사)
2007년~현재 한화시스템(주) 기반기술연구소 전문연구원
관심분야 : 사이버 상황인식, 정보보호, 컴퓨터공학 etc.
E-mail : bj001.kim@hanwha.com

이 재 연(Jae-yeon Lee)
2002년 2월 가톨릭대학교 정보통신공학(공학사)
2004년 2월 광주과학기술원 대학원 정보통신공학(공학석사)
2004년~현재 한화시스템(주) 기반기술연구소 수석연구원
관심분야 : 사이버 상황인식, 정보보호, 시스템 침입분석 etc.
E-mail : jaeyeon46.lee@hanwha.com