하드웨어적 고유 특성 기반 드론 식별 및 인증 기술 연구 동향 분석

박성빈 [1], 지 훈 [2], 이연준 [3]
[1] 한양대학교 컴퓨터공학과 바이오인공지능융합전공 석박사통합과정
[2] 한양대학교 ICT 융합학부 학부생
[3] 한양대학교 컴퓨터공학과 교수

{[1]pbt98, [2]greenpea0819, [3]yeonjoonlee}@hanyang.ac.kr

A Survey on Hardware Characteristic-based Drone Identification and Authentication Technology

Sungbin Park[1], Hoon Ji[2], Yeonjoon Lee[3]
[1]Dept. of Computer Science and Engineering Major in Bio Artificial Intelligence, Hanyang University
[2]Division of Media, Culture and Design Technology, Hanyang University
[3]Dept. of Computer Science and Engineering, Hanyang University

요 약

최근 드론은 군사 작전, 물류 운송, 인명 구조 등 다양한 분야에서 활용되고 있으며 관련 산업의 규모는 증가하는 추세이다. 이에 따라, GPS 스푸핑, 조종사 비익명화 등의 드론을 향한 공격 기법들 또한 발달하고 있다. 이런 공격들은 드론에 대한 인증을 도입함으로써 대비할 수 있는 공격들이다. 이에, 학계에서는 강건한 인증을 위해 드론 하드웨어의 고유 특성을 활용할 수 있는 RF 신호, 소리 신호, 드론 내부 센서 신호 등에 기반한 인증 기술들이 연구되어온 바 있다. 본 논문에서는 지금까지의 드론 인증 기술 연구 동향을 분석하고, 이를 기반으로 향후 연구 방향을 제시한다.

1. 서론

최근 드론 기술은 급속한 발전으로 인해 다양한 분야에서 활용되고 있으며, 이러한 확장은 일상 생활뿐만 아니라 군사 작전과 같은 전략적 영역에도 미치고 있다. 이러한 추세를 뒷받침하기 위해, 전 세계 드론 산업은 2024 년 총 규모 81 억 9 천만 달러를 가지는 거대 산업으로 성장할 것으로 예측된다.[1] 이는 2018 년 대비 약 60%의 증가율을 보이는 수치로, 이러한 경향은 드론 기술이 현대 사회에서 더욱 중요한 역할을 하고 있음을 강조한다.

산업 규모의 지속적인 확장과 함께 드론을 대상으로 하는 공격 사례 및 연구가 증가하고 있다. 예를 들어, GPS (Global Positioning System) 나 자이로스코프와 같은 센서 정보를 스푸핑하는 공격 (이란의 미군 무인 정찰기 GPS 교란 사건[2], He et al.[3], Son et al.[4]) 이나 드론과의 통신에서 사용되는 API 의 보안 취약점을 이용하여 비행 기록을 추적하는 공격 및 드론 조종사의 익명성을 해칠 수 있는 공격 (Nassi et al.[5]) 등이 연구된 바 있다.

위와 같은 공격들은 드론 기체나 사용자에 대한 인증 기술의 미비함으로 인해 가능한 공격들이다. 이에 대응하기 위해 암호 모듈, 정보유출 탐지 시스템 등이 개발되고 있으나, 드론의 제한적인 컴퓨팅 자원으로 인한 개발의 어려움과, 고도화된 공격 기술에는 무력화될 가능성을 가지고 있어, 학계에서는 드론의 하드웨어적인 고유 특성을 활용한 인증 기술 또한 드론 보안의 한 축으로 연구되어온 바 있다.

드론의 하드웨어적인 고유 특성을 활용한 인증은 하드웨어 제조 과정의 불완전성으로 인해 같은 하드웨어여도 작동 시 다른 특성을 보이는 현상을 활용하는 인증 기술이다. 이러한 특성을 보이는 하드웨어는 주로 모터, 회로, 그리고 탑재된 센서들 (자이로스코프, 카메라 등) 로 대표된다. 학계에서는 드론이 작동할 때 이러한 하드웨어로부터 발생하는 음향 신호, RF (Radio Frequency) 신호, 그리고 센서 신호가 드론마다 상이함을 바탕으로 한 다양한 인증 기술이 연구되어왔다.

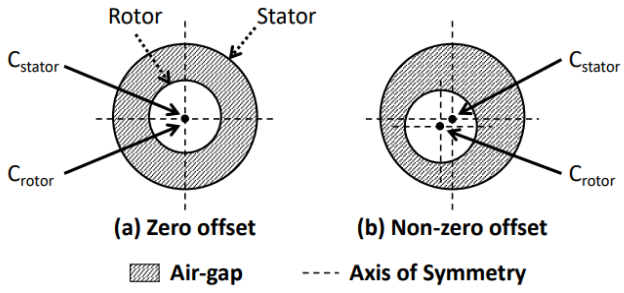
드론의 사용 목적이 다양하므로, 적합한 인증 기술

을 선택하려면 다양한 기술의 장단점과 한계를 정확히 분석해야한다. 이를 위해, 본 논문에서는 그 동안 연구된 드론 인증 기술들을 음향 신호 기반, RF 신호 기반, 그리고 센서 신호 기반의 카테고리로 나누어 연구 동향을 조사하고, 각 인증 기술의 장단점을 비교하여 어떤 사용 사례에 적합하며 어떤 한계점을 가지고 있는지를 도출한다. 이를 토대로 현재 드론 인증 기술의 상황을 고려하여 미래 연구 방향을 제안한다. 이 연구를 통해 드론 인증 기술의 발전과 활용에 기여하고, 드론 관련 분야에서의 보안과 안전성을 향상시키는 데 일조하고자 한다.

2. 음향 신호 기반의 드론 식별 및 인증 기술 동향

음향 신호 기반의 드론 식별은 드론의 모터가 회전하며 발생하는 소리가 드론마다 상이하다는 것을 이용하여 드론을 식별 및 인증하는 기술이다.

Ramesh et al. [6]은 드론의 모터 소리를 이용하여 드론을 인증하는 대표적인 논문 중 하나인데, 드론에 가장 흔하게 사용되는 브러시리스 모터는 영구 자석으로 이루어진 회전자와 권선으로 이루어진 스테이터 폴로 구성되어 있다. 이 부품을 제조하는 공정 과정에서 스테이터와 회전자를 결합 배치할 때, 두 부품의 중심점이 일치하지 않는 일종의 제조 과정에서의 불일치로 인해 드론마다 고유한 모터 회전음을 가진다 (그림 1). 따라서 모터마다, 나아가 같은 타입의 드론이라도 드론마다 고유한 모터 회전음을 가지게 되는 것이다.



(그림 1) 회전자와 스테이터의 영점 불일치.

해당 연구는 개별 모터 회전음 및 4 개의 모터가 탑재된 드론의 비행 소리를 각각 Support Vector Machine (SVM)에 훈련시켰고, 각각 91.83%, 99.48%의 정확도를 산출하였다. 개별 모터 인증의 정확도보다 드론 인증의 정확도가 높게 나온 이유에 대해서 저자들은 드론에는 4 개에 모터가 탑재되기 때문에 각 데이터 간의 음향 핑거프린팅이 유사하게 추출될 가능성이 개별 모터보다 월등히 적다라고 언급하고 있다.

해당 연구는 드론의 모터 소리가 드론마다 상이한 이유에 대해 자세히 설명하고, 개별 모터와 드론의 인증 모두를 실험하여 의미 있는 결과를 도출하였지만, 주변 배경 소음의 영향을 최소화하기 위해 Docking Station 이라는 별도의 인증 공간을 마련해야 한다는 점이 단점이다.

Al-Emadi et al. [7]는 드론 모터 회전음 스펙트로그램 이미지를 입력 데이터로 하여 CNN 모델에 훈련하여 드론을 식별하는 연구이다. 드론 모터 회전음과 일상 생활에서 발생하는 백그라운드 노이즈를 각각 따로 녹음하여 병합하는 방식으로 데이터를 생성하였고, 이를 Recurrent Neural Network(RNN), Convolutional Neural Network(CNN), Convolutional Recurrent Neural Network(CRNN) 각각에 학습시켜 성능을 비교했다. 최종적으로 CNN 에서 최고 성능인 92.94%의 정확도를 보여주었으나, 드론의 타입이 2 개 뿐인 이진 분류 연구였다는 점에서 2 개 이상의 드론을 식별할 경우의 성능을 장담하지 못한다는 단점이 존재한다.

Diao Y et al. [8]은 드론의 모터 회전음으로부터 추출한 Mel-Frequency Cepstral Coefficient(MFCC), Delta MFCC(DMFCC), Delta-Delta MFCC(DDMFCC) 특성들의 결합에 따라 모델의 성능이 어떻게 변화하는지를 정량적으로 분석하고, 해당 특성들을 Quadratic Discriminant Analysis(QDA), Linear Disciminant Analysis(LDA), Latent Support Vector Machine(LSVM), K-Nearest Neighbors(KNN) 등 다양한 모델들에 훈련시켰을 때의 드론 인증 성능을 비교해 보는 정밀한 연구가 시행되었고, QDA 모델에서 최고 성능 96.2%라는 높은 정확도를 보였다.

음향 신호 기반의 드론 식별 연구는 비교적 직관적인 드론의 고유 특성을 사용하며, 연구 전반적으로 좋은 모델 퍼포먼스를 보여주지만, 드론의 모터 회전음 외의 활용할 수 있는 드론의 고유 음향 특성을 발견하고 활용하기 쉽지 않다는 점, 그리고 음향 신호 특성 상 주변 소음의 간섭에 민감할 수밖에 없어 모델의 성능에 영향을 끼치거나 Docking Station 과 같은 안정적인 인증을 위한 추가적인 제약 사항이 따른다는 점이 단점이다.

3. RF 신호 기반의 드론 식별 및 인증 기술 동향

RF 기반의 드론 식별은 드론에서 만들어내는 무선 주파수의 고유한 특성을 활용하여 드론을 식별 및 인증하는 기술이다.

Nemer et al. [9]는 드론과 비행 컨트롤러가 통신할 때 사용하는 RF 센서에 입력되는 신호값을 특성으로서 활용하여 드론을 감지 및 식별하는 연구로서, XGBoost 과 KNN 두 개의 모델을 앙상블하여 분류기를 생성한다. 최종적으로 드론의 감지 및 식별 단계

를 모두 아우르는 계층적 학습법을 구현하는 연구이며, 이를 통해 약 99%의 정확도로 드론을 감지하고 식별하였다.

Allahham M S et al. [10]는 DroneRF 라는 오픈 데이터셋을 이용하여 세 가지 타입의 드론을 식별하는 연구를 진행하였다. 전체 주파수 스펙트럼을 여러 채널로 쪼개 분류기에 각 채널에 해당하는 입력값을 각각 넣어 주고, 이를 멀티 채널 1-Dimensional Convolutional Neural Network(1DCNN)를 통해 분류하였다. 최종적으로 94.6%의 정확도로 드론을 감지, 식별할 수 있음을 결론으로 내놓았다. 다만, 테스트에 사용한 드론의 종류가 매우 적어 해당 클래스 수 이상의 드론을 식별할 경우의 정확도를 장담할 수 없다는 것이 단점이다.

Li Z et al. [11]는 DroneTrace 라고 하는 RF 신호 송출 및 감지 장치에서 밀리미터파 단위의 신호를 송신하고, 이를 감지한 드론이 Parasitic Response(기생 응답)을 방출하면, DroneTrce 가 이를 수집하여 특성으로 활용하여 드론을 식별하는 연구이다. 이 또한 음향 신호 기반의 식별 연구와 비슷하게 드론을 제조하는 공정 상의 제조 불일치로 인해 드론마다의 기생 응답 수치가 다르게 나타나는 것을 활용한 연구이며, Deep Neural Network(DNN)을 활용하여 드론을 식별하였고, 결과적으로 99% 이상의 정확도를 산출해내는 데 성공하였다.

RF 기반의 드론 식별은 음향 신호 기반 식별 방법론보다 더 많고 다양한 종류의 특성을 사용한 연구들이 존재한다는 것이 장점이지만, 이 역시 경우에 따라 DroneTrace 와 같은 RF 신호를 수집하기 위한 별도의 장비가 필요할 수 있다는 점이 단점이다.

4. 센서 신호 기반의 드론 식별 및 인증 기술 동향

센서 신호 기반 인증 기술은 센서 제조 과정의 불완전성으로 인해 같은 장소에서 같은 제조 과정을 거친 같은 종류의 센서더라도 특정 상황에서 측정값의 차이가 일어나는 현상을 활용하거나 서로 다른 센서들의 측정값의 융합을 활용하는 식별 및 인증 기술이다.

Son et al.[12]는 자이로스코프 측정값을 활용한 인증 방법을 제안하였다. 자이로스코프의 불완정성의 알려진 원인으로는 제조 기계의 단차로 인해 센서 간의 미세한 정전 용량의 차이가 있는 것을 밝히며, 이것 때문에 x, y, z 축 방향 각각 가속이 있지 않은 상황에서의 센서 출력값 (오프셋) 에 차이가 생기는 것을 인증에 활용하였다. 각 축마다 128 개의 출력 샘플의 평균을 드론의 지문으로 활용하였으며, 이때 세 개의 축 모두 사용했을 때와 두 개의 축만 사용했을 때 (평균) 의 F1-score 는 각각 98.78%, 94.47%를 달성하였다. 그러나, 실제 드론을 운용하여 실험한 것이 아닌 각 축으로의 가속을 인위적으로 만들 수 있는 실험 기구에 자이로스코프를 장착하여 만든 기구로 실험하였기에 실제 상황에서의 동작을 보장하지 못한다는 단점이 있다.

Wu et al.[13]은 릴레이 공격으로부터 드론과 사용자 모두를 보호하기 위하여 둘을 상호 인증하는 기술을 제안하였다. 릴레이 공격은 드론을 통한 물건 배달 시나리오 내에서 일어난다. 우선, 공격자의 드론이 배달 드론을 가장하여 피해자 앞에 나타난 후, 이를 모르는 피해자가 물건을 받기 위해 판매자로부터 발급받은 QR 코드를 공격자 드론에 보여주면 공격자는 공격 드론으로부터 QR 코드를 전송 받을 수 있다. 마지막으로 공격자는 QR 코드를 통해 실제 배달 드론으로부터 피해자의 물건을 탈취한다.

이를 방지하기 위해, 사용자가 드론으로부터 물건을 전달받을 때 사용자가 드론을 향해 스마트폰을 들고 손을 좌우로 흔드는 행위를 통해 드론과 사용자를 상호 인증한다. 손을 흔들 때, 스마트폰의 자이로스코프 신호 기록으로부터 도출된 손의 가속도 정보와 드론의 카메라로부터 도출된 손의 가속도 정보의 상관계수와 두 기기가 통신하기 시작한 timestamp 정보를 활용해 실제 배달 드론과 사용자가 함께 있는지 상호 인증한다. 이때, 전반적인 인증 성능은 1.58%의 평균 EER 을 달성하였다. 그러나, 카메라를 활용하는 점에서 프라이버시 침해 문제가 있고, 좋지 않은 기상 상황 (바람, 안개, 비) 에서는 성능이 평가된 바가 없어 사용성이 제한적인 단점이 있다.

Ruiz et al. [14]은 여러 개의 똑같이 생긴 드론 중 특정 드론을 식별하는 기술을 제안하였다. 이 기술 또한 하드웨어 제조 과정의 불완전성 때문에 드론의 진동이 달라진다는 점을 활용한다. 이 기술의 경우, 관성 센서에 의해 감지된 드론의 모션과 카메라에 포착된 드론의 모션을 매칭 시켜서 같은 종류의 드론이 모여있을 때 어떤 드론이 해당 모션을 보이는지 감지한다. 3 대의 드론을 가지고 2x2x1m 방에서 실험 시, 호버링 (그대로 떠 있는 상태) 에서는 진동이 다르기 때문에 7 초 후 100%의 평균 식별 정확도를 보였고, 드론마다 방 안에서 무작위로 날아다니게 만들었을 때는 4 초 후 100%의 평균 식별 정확도를 보였다. 그러나, 공격자가 식별을 피하기 위해 주변의 드론이 보이는 비행 형태를 모방할 수 있는 위험이 있고, 시스템을 사용할 수 있는 범위가 좁고, 실내에서만 실험을 진행했기 때문에 악조건의 기상에서 작동 가능 여부를 알 수 없다는 것이 단점이다.

센서 신호 기반의 인증 및 식별은 인증에 필요할

수 있는 하드웨어 추가 설치가 필요 없고, 특정 사용례를 고려하여 설계된 경우가 많아 기술 자체의 사용성을 뛰어난 장점이 있지만, 실제 환경에서 테스트된 경우가 적어 기술의 강건함에 대한 입증이 부족한 것이 단점이다.

5. 결론

지금까지 드론 식별 및 인증 기술을 음향 신호 기반, RF 신호 기반, 그리고 센서 신호 기반의 기술들로 나누어 각 연구 동향을 살펴봤다.

음향 신호 기반 기술의 경우, 드론에 탑재된 모터의 소음이 드론마다 차이가 있는 것을 활용하여 식별 및 인증을 진행하였다. 인증에 필요한 추가 하드웨어를 탑재할 필요가 없고, 온도 변화에는 강건한 장점이 있지만, 주변 소음에 취약한 단점이 있어, 차고나 격납고 등 주변 소음에서 차단되는 별도의 인증 공간이 있는 경우 사용성이 극대화된다.

RF 신호 기반 기술의 경우, 드론이 방출하는 전자기파의 특성을 활용하여 식별 및 인증을 진행하였다. 소음과 환경적 요인에 강건한 장점이 있지만, 신호를 수집하기 위한 별도의 장비가 필요한 단점이 존재하여, 일상 생활보다는 비즈니스, 군사 작전의 목적으로 사용하기 적합하다.

마지막으로 센서 신호 기반 기술의 경우, 하드웨어 제조 과정의 불완전성으로 인해 생기는 센서의 측정값 차이나 여러 센서들의 정보를 융합하여 드론 식별 및 인증을 진행하였다. 드론에 탑재된 센서들을 활용하기 때문에 인증에 필요한 추가 하드웨어를 탑재할 필요가 없고, 사용자 경험을 고려하여 설계되어 사용성이 뛰어난 장점이 있으나, 실제 환경에서 테스트된 경우가 드물어 기술의 강건함이 입증된 바가 없다는 단점이 있어, 기상 조건이 양호한 일상 환경에서 사용하기 적합하다.

이러한 점을 고려하면, 미래 연구는 보다 범용적인 사용 시나리오를 고려하고, 환경적 조건에 강건한 기술을 개발하며, 인증 비용을 절감하기 위한 노력이 필요하다. 현재까지의 연구는 특정 공격에 집중하거나 한정된 사용 사례에 중점을 두어 전반적으로 적용 범위가 한정적인 경우가 많았다. 또한, 별도의 장비가 필요한 경우가 있어 드론의 제한된 리소스를 고려할 때 높은 인증 비용을 요구하는 경우도 많아 이를 최소화하기 위한 노력이 필요하다. 마지막으로, 다양한 환경 조건에 강건한 기술을 개발하는 데 중요한 연구 노력이 필요하다.

ACKNOWLEDGEMENTS

이 논문은 2023 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.RS-2023-00225201, 국방 무인이동체 역이용 방지 제어권 보호기술 개발)

이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(NRF-2022R1F1A1074999)을 받아 수행된 연구임.

참고문헌

[1] Statasia, Volume of the global drone market from 2018 to 2028, https://www.statista.com/forecasts/1399076/drone-market-volume-worldwide, 2023.03

[2] 보안뉴스, 좋은 드론, 나쁜 드론, 이상한 드론, https://www.boannews.com/media/view.asp?idx=54409&skind=O, 2017.04

[3] He, Daojing, et al. "A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles." IEEE Network, 33.2, 146-151, 2018

[4] Son, Yunmok, et al. "Rocking drones with intentional sound noise on gyroscopic sensors." 24th USENIX Security Symposium (USENIX Security 15), Washington. D.C., 2015, 17p

[5] Nassi, Ben, et al. "SoK: Security and privacy in the age of commercial drones." 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, 2021, 18p

[6] Rasmesh S, “SoundUAV, Towards Delivery Drone Authentication via Acoustic Noise Fingerprinting”, Dronet’19: Proceedings of the 5th Workshop on Micro Aerial Vehicle Networks, Systems, and Applications, Seoul, 2019, 27-32

[7] Al-Emadi S, “Audio Based Drone Detection and Identification using Deep Learning”, International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, 2019, 459-464

[8] Diao Y, “Drone Authentication via Acoustic Fingerprinting”, ACSAC: Annual Computer Security Applications Conference, Austin, 2022, 658-668

[9] Nemer I, “RF-based UAV detection and identification using hierarchical learning approach”, Sensors, 2021, 21(6), 1947

[10] Allahham M S, “Deep Learning for RF-Based Drone Detection and Identification: A Multi-Channel 1-D Convolutional Neural Networks Approach”, IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, 2020, 112-117

[11] Li Z, “Reliable Digital Forensics in the Air: Exploring an RF-based Drone Identification System”, ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies,Atlanta and Cambridge, 2022, 1-25

[12] Son, Yunmok, et al. "Gyrosfinger: Fingerprinting drones for location tracking based on the outputs of mems gyroscopes." ACM Transactions on Privacy and Security (TOPS) 21.2 (2018): 1-25.

[13] Wu, Chuxiong, et al. "G2Auth: secure mutual authentication for drone delivery without special user-side hardware." Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services, Oregon, Poland, 2022, 84-98

[14] Ruiz, Carlos, et al. "Idrone: Robust drone identification through motion actuation feedback." Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 2.2, Singapore, 2018, 1-22.