드론 하드웨어 고유특성을 이용한 식별 및 인증 기술 연구 동향

강정훈[1], 서승현[2]
[1] 한양대학교 전자공학과 석사과정
[2] 한양대학교 ERICA 전자공학부 교수

kjh980922@hanyang.ac.kr, seosh77@hanyang.ac.kr

Survey on Identification and Authentication Technology Using the Unique Characteristics of Drone Hardware

Jung-Hun Kang[1], Seung-Hyun Seo[2]
[1]Dept. of Electrical Engineering, Hanyang University
[2] School of Electrical Engineering, Hanyang University ERICA

요 약

최근 성장하고 있는 드론 산업에 맞추어 전세계적으로 드론 운용을 위한 식별 및 인증 규정을 마련하고 있는 추세이다. 대표적으로, 미국 FAA 에서 채택한 Remote ID 기반의 식별방식이 있다. 그러나, ID 기반의 인증 방식은 해당 ID 가 탈취 혹은 위조될 경우 다른 드론으로 위장하여 여러 심각한 사회 문제를 일으킬 위험성이 있다. 따라서 드론에 탑재된 여러 센서나 모터와 같은 하드웨어의 고유한 특성을 이용하여 Remote ID 를 대체하거나 이중 인증에 이용하려는 연구가 이루어지고 있다. 본 논문에서는 드론에 탑재된 하드웨어의 고유특성을 이용한 다양한 식별 및 인증시스템에 대한 연구에 대하여 살펴본다.

1. 서론

드론은 자유로운 이착륙, 소형화, 군집화 등이 가능하고, 무인으로 운용이 가능하며 지상관제센터(Ground Control Station 이하 GCS)에서 적은 인력으로 넓은 지역에 서비스를 제공할 수 있다는 장점이 있다. 이와 같은 드론의 장점은 산업 전반에 있어 큰 활용성을 보이며 국내의 경우도 드론의 신규 등록 건수가 점차 증가하는 추세를 보이고 있다.[1] 따라서 국내도 해외의 사례들을 바탕으로 드론의 원격식별에 대한 규제 마련을 위해 노력하고 있다.

미국 연방항공청(FAA)에서는 허가된 드론에 대하여 원격 식별 번호(Remote ID)를 부여하거나 Remote ID 를 식별할 수 있는 별도의 장치를 부착하고, 일정 시간 혹은 이착륙시에 Remote ID 와, 위치, 기종, 비행경로 등을 브로드 캐스팅하도록 하거나, FAA 가 인지할 수 있는 허가된 지역에서만 비행할 수 있도록 규정하고 있다. 유럽항공안전청(EASA)에서는 미국 FFA 와 유사한 Direct Remote ID 를 통한 브로드 캐스팅 방식과 네트워크를 통한 원격 식별방식인 E-Identification 이 고려되고 있다. 또한, 드론의 운용 위험도와 무게 기준에 따라 7 개의 클래스로 나누어 각 클래스마다 요구되는 항목에 차이가 있다.[2] 앞서 살펴본 두가지 모두 인증기관에서 부여한 ID 기반의 식별방식이다.

하지만, 이러한 ID 기반의 식별 및 인증 방식은 드론의 고유 식별번호(RemoteID)가 공격자에 의해 노출되거나, 드론 자체에 부착된 별도의 식별용 장치가 탈취될 경우, 공격자의 드론이 해당 식별번호 혹은 장치를 이용하여 위장할 위험이 존재한다. 드론에는 카메라, 센서, 통신 시스템이 탑재되어 있기 때문에, 식별 번호 위장에 따른 사생활 침해와 데이터 유출 등의 문제를 일으킬 수 있다.[3]

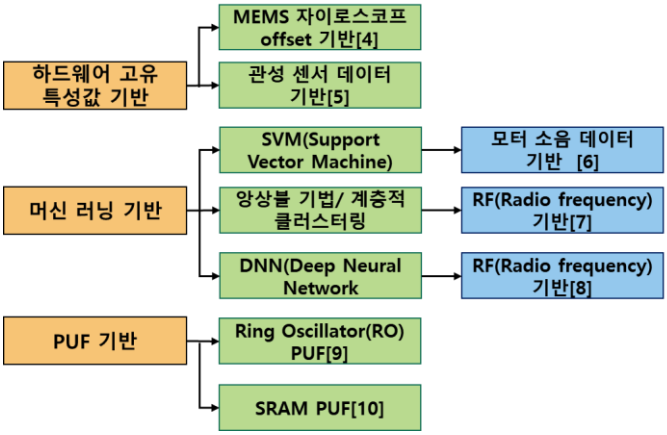
따라서 국, 내외 무인기에 대한 Remote ID 기반의 식별 및 인증방식을 보완하기 위해 여러 방안이 논의되고 있다. 그중, 드론 자체의 하드웨어의 고유 특성을 이용하여 물리적으로 복제가 불가능한 특성 값을 추출하여 인증하는 방식에 대한 연구가 활발히 이루

어지고 있다. 다음 장에서는 드론의 하드웨어 고유특성을 이용한 인증관련 연구 동향에 대하여 기술한다.

2. 드론에 탑재된 하드웨어의 고유특성을 이용한 인증방안 연구 동향

최근 ID 기반 인증방식의 ID 탈취 및 위·변조가능성 문제를 해결하기 위하여 드론에 탑재된 여러 전자장치나 센서들로부터 추출한 고유특성을 이용하여 드론 자체를 인증하려는 연구가 활발히 진행되고 있다. <그림 1>은 드론에 탑재된 하드웨어의 고유 특성을 이용한 주요 연구들을 주요 기법 및 사용 하드웨어 종류에 따라 분류하여 나타내었다.

<그림 1> 하드웨어 특성 기반 드론 식별 및 인증 연구 분류도



2.1 하드웨어의 고유 특성 값을 이용한 드론 식별 및 인증 연구

Son Y et al. [4]은 드론의 자세제어에 필수적인 MEMS 자이로스코프의 공정상의 오차(offset)를 드론 자체의 고유특성으로 활용하여, 비행중에도 실시간으로 항적과 자이로스코프의 오차 값을 확인하여 정당한 드론임을 인증하는 방법을 제시하였다. 두 군데의 제조사에서 제작한 5 가지 모델의 자이로스코프 칩 70 개를 이용하여 실험하였고, 평균 정확도 94.47%를 보였다. 그러나 MEMS 자이로스코프의 특성상 온도 변화에 따라 인증 성공률이 현저하게 낮아지는 점과 측정된 자이로스코프의 오차값은 암호화되지 않은 raw 데이터 형태로 GCS 로 전달되어 탈취될 가능성이 있다.

Ruiz C et al. [5]은 관측용 외부 카메라를 통해 촬영한 드론의 움직임과 드론에서 전송해 주는 관성센서 값을 비교하여 해당 드론이 제어 권 내에 있음을 인증하는 방식을 제안하였다. 실제 운용환경과 비슷하게 구현하기 위해 외부에서 실험하였고, Safety, Uniqueness 두 가지의 동작을 기반으로 하는 motion actuation feedback loop 을 이용하여 기존의 드론의 움직임을 기반으로 하는 인증방식에 비해 빠른 인증 속도를 보이는 점이 특징이다. 그러나, 관측용 외부 카메라가 안정적으로 고정되어 있어야 하고, 드론이 계속 움직이는 상황에서는 인증 실패율이 증가한다는 한계점이 있다.

2.2 머신 러닝을 이용한 드론 식별 및 인증 연구

Ramesh S et al. [6]은 배송에 사용되는 드론에서 고객이 물건을 맡기기 전에 Docker station 에서 드론의 모터소리를 녹음한 데이터를 SVM(Support Vector Machine)을 통해 분류하여 정당한 드론을 인증하는 단계를 추가하는 방법을 제안하였다. 같은 모델 드론 11 대를 대상으로 실험하였을 때 99.48%의 정확성을 보여주었다. 그러나, 소리 신호를 사용하기 위해 특별히 조용한 공간인 Docker station 이 추가로 필요한점과 11 대 이상의 다수의 드론을 운용할 경우에 정확성을 보장할 수 없다는 한계점이 있다.

Nemer I et al. [7]은 드론과 조종장치 및 GCS 간의 통신에 사용하는 RF(Radio Frequency)센서로부터 RF 신호를 추출하여, 앙상블 학습 기법을 이용한 머신러닝과 계층적 클러스터링 기법을 활용하여 정확성 99%이상으로 드론의 기종과 비행모드를 구별해 내는 방법을 제안하였다. 이 연구는 기존의 다른 센서를 사용한 연구들에 비하여 비교적 환경요소에 의한 영향을 덜 받는 다는 장점이 있다. 그러나, 사전에 수집한 데이터를 이용한 전처리 과정이 필요하고 같은 주파수 대역을 사용하는 다수의 드론을 동시에 구별해 내지 못하는 한계점이 있다.

Li Z et al.[8]은 드론을 감지할 수 있는 DroneTrace 라는 감지장치로부터 밀리미터 파를 방출하고, 그 Parasitic Response(기생 응답 성분)이 전자 장치의 공정상의 오차로 인하여 같은 공정과 모델의 드론이어도, 각각의 개체마다 다른 특성을 보이는 점에서 착안하여, 감지장치가 수집한 기생 응답 성분을 DNN(Deep Neural Network)기반의 머신 러닝 알고리즘을 통하여 구별하는 디지털 포렌식 방법을 제안하였다. 그러나, DroneTrace 라는 별도의 감지 장치의 설치가 필요하고, 드론이 손상되어 일부 부품을 교체하거나, 알루미늄 포일등으로 차폐막을 형성하게 되면 인증에 사용할 수 없다는 한계점이 있다.

2.3 PUF(Physically Unclonable Function)을 이용한 드론 식별 및 인증 연구

Pal V et al[9]은 PUF 중에서 Ring Oscillator PUF 를 이용하여 드론에 내장된 여러 센서들(자이로스코프, 카메라, 마이크, 가속도계 등)로부터 물리적으로 복제가 불가능한 유일한 고유특성을 추출하여 인증에 사용하는 프레임워크를 제안하였다. 이 방식의 경우 기존의 PKI(Public Key Infrastructure)방식과는 달리 고유특성값을 드론의 저장공간에 저장해 둘 필요가 없다는 특징이 있다. 그러나 Ring Oscillator PUF 의 특성상 반도체 자체의 defection 으로부터 기반하는 Arbiter PUF 에 비해 안정성이 떨어지는 한계점이 있다.

Lounis K et al.[10]은 드론 내부에 탑재한 SRAM-PUF 를 이용하여 드론과 드론간의 상호 인증을 통해

안전한 대칭키 교환이 가능하도록 프토토콜을 제시하였다. 기존의 인증 프로토콜 보다 빠르고 가볍다는 특징이 있다. 그러나 드론에 저장된 CRP(Challenge-Response Pairs)가 하나밖에 없기 때문에, 반드시 CRP 를 업데이트 해 주어야 또 다른 드론과의 인증에 사용할 수 있다. 또한, SRAM-PUF 또한, 온도, 노이즈, 전압 변화등에 의해 특성이 바뀔 수 있어 다른 PUF 에 비해 안정성이 떨어진다는 한계점이 있다.

Alladi T et al[11]은 드론 내부에 특정 챌린지 값을 입력하면 고유한 아웃풋 값으로 반환시켜 주는 Challenge-Response PUF 를 장착하고, GCS 와 서로 CRP 쌍 (C, R)을 사전에 안전한 채널을 통해 공유한 상태에서 인증을 요구할 때 마다 미리 공유해 둔 CRP 쌍을 사용하여 인증하고, 생성한 세션키를 나누어 가짐으로 써 안전한 통신을 가능하게 하고, 이 채널을 통해 다시 다음 인증에 사용할 CRP 쌍을 공유하는 형태의 인증방식을 제안하였다. 이 방법 역시, PUF 라는 물리적인 장치를 사용하기 때문에, 직접적으로 드론 내부에 비밀 정보를 저장하지 않아도 되는 장점과 매 인증 마다 CRP 쌍이 새로 설정되므로, 여러 전형적인 공격방식(재전송 공격, 위장 공격 등)에 대해 안전하다고 주장하고 있다.

3. 결론

현재 드론 개체의 탐지 및 ID 기반의 식별에 대한 보조적인 수단으로 하드웨어의 특성을 수집하여 머신러닝을 통해 기종을 구별하는 등의 연구는 활발히 이루어지고 있는 반면, 드론의 하드웨어 고유특성을 활용한 연구는 상대적으로 미비한 실정이다. ID 기반의인증방식은 비행경로상에서 주기적으로 개체의 ID 와 비행 경로 등을 broadcasting 하는 방식으로 언제든 공격자에 의해 ID 를 탈취당해 다른 드론으로 위장할 수 있는 위험성이 있다. 따라서 드론에 탑재된 여러 전자부품 혹은 센서들로부터 추출한 고유한 특성을 인증의 한 요소로 사용하는 연구가 필요하다. 또한, 여러가지 PUF 를 통한 복제 불가능한 키 생성방식은 강력한 키 은닉 기법 역할을 수행할 수도 있다. 따라서 앞으로의 연구는 크게 머신러닝을 활용한 하드웨어 고유특성 추출 및 인증과 PUF 를 이용한 키 은닉 기술을 바탕으로 한 인증방안으로 발전할 것이다.

그러나, 드론의 하드웨어에 전적으로 의존한 인증방식은 드론자체가 탈취당하였을 경우, 내부 정보에 대한 보호가 어렵다는 단점이 존재한다. 따라서 드론의 소유자 혹은 조종사를 상호 인증하는 방식이나 특정한 장소나 환경에서만 내부 정보에 접근이 가능하도록 하는 형태의 내부정보보호에 대한 연구도 필요하다.

Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음" (IITP-2023-2018-0-01417)

참고문헌

[1] 국토교통부, 항공안전기술원. 2021 년 국내외 드론 산업 동향 분석 보고서. 2022.01.18.

[2] 김희욱, 강군석, 김대호. 드론 원격 식별 규정 및 표준화 동향 분석. [ETRI] 전자통신동향분석. 2021 Dec;36(6).

[3] Gang YS, Kim JH, Kim GU. 표준 소개-드론 기반 서비스를 위한 보안 요구사항. TTA Journal. 2018:74-9.

[4] Son Y, Noh J, Choi J, Kim Y. Gyrosfinger: Fingerprinting drones for location tracking based on the outputs of mems gyroscopes. ACM Transactions on Privacy and Security (TOPS). 2018 Feb 5;21(2):1-25.

[5] Ruiz C, Pan S, Bannis A, Chen X, Joe-Wong C, Noh HY, Zhang P. Idrone: Robust drone identification through motion actuation feedback. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous 2018 Jul 5;2(2):1-22.

[6] Ramesh S, Pathier T, Han J. Sounduav: Towards delivery drone authentication via acoustic noise fingerprinting. InProceedings of the 5th Workshop on Micro Aerial Vehicle Networks, Systems, and Applications 2019 Jun 12 (pp. 27-32).

[7] Nemer I, Sheltami T, Ahmad I, Yasar AU, Abdeen MA. RF-based UAV detection and identification using hierarchical learning approach. Sensors. 2021 Mar 10;21(6):1947.

[8] Li Z, Chen B, Chen X, Xu C, Chen Y, Lin F, Li C, Dantu K, Ren K, Xu W. Reliable Digital Forensics in the Air: Exploring an RF-based Drone Identification System. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2022 Jul 7;6(2):1-25.

[9] Pal V, Acharya BS, Shrivastav S, Saha S, Joglekar A, Amrutur B. PUF based secure framework for hardware and software security of drones. In2020 Asian Hardware Oriented Security and Trust Symposium (AsianHOST) 2020 Dec 15 (pp. 01-06). IEEE. Technologies.

[10] Lounis K, Ding SH, Zulkernine M. D2D-MAP: A Drone to Drone Authentication Protocol Using Physical Unclonable Functions. IEEE Transactions on Vehicular Technology. 2022 Nov 24.

[11] Alladi T, Bansal G, Chamola V, Guizani M. SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication. IEEE Transactions on Vehicular Technology. 2020 Oct 22;69(12):15068-77.

[12] Gang YS, Kim JH, Kim GU. 표준 소개-드론 기반 서비스를 위한 보안 요구사항. TTA Journal. 2018:74-9.

[13] Shoufan A, Al-Angari HM, Sheikh MF, Damiani E. Drone pilot identification by classifying radio-control signals. IEEE Transactions on Information Forensics and Security. 2018 Mar 23;13(10):2439-47.