프라이버시 보호를 위한 PUF 기반의 드론 식별 시스템

박가을 [1], 지찬웅 [1], 김동준 [1], 서승현 [2]
[1] 한양대학교 ERICA 전자공학부 학부생
[2] 한양대학교 ERICA 전자공학부 교수

gaulpark@hanyang.ac.kr, ichanwoong@hanyang.ac.kr, dongjunkim12@hanyang.ac.kr, seosh77@hanyang.ac.kr

Privacy-preserving drone identification system based on PUF

Gaeul Park, Chanwoong Ji, Dongjun Kim, Seung-hyun Seo
Dept. of Electrical Engineering, Hanyang University ERICA

요 약

최근 드론 산업의 성장으로 드론 등록이 증가함에 따라 드론을 효율적으로 관리하기 위해 Remote ID 를 도입하였다. 그러나 현재의 방법은 드론의 개인 정보 보호를 고려하지 않고 있어 드론의 개인 정보 노출과 보안 문제를 초래할 수 있다. 본 논문에서는 하드웨어의 고유 특성을 PUF 를 활용하여 드론의 익명성을 보호하고, 신뢰할 수 있는 대상이 드론을 안전하게 식별할 수 있도록 하는 새로운 프로토콜을 제안한다.

1. 서론

드론은 무인으로 운용할 수 있으며 자유로운 비행을 할 수 있고 휴대성이 편리해 다양한 데이터들을 수집할 수 있다는 장점이 있다. 이러한 장점은 현대 산업에서 큰 활용성을 보이며 전 세계적으로 드론 시장의 연평균 성장률이 2030 년까지 7.8%를 기록할 것으로 예상된다.[1] 이에 따라 미국, 일본 등 여러 국가에서는 드론을 효율적으로 관리하기 위해 드론이 자신의 식별 및 위치 정보를 제공하도록 하는 Remote ID 기능과 관련된 규정이 시행되고 있다.

그러나 Remote ID 를 통해 비행 중인 드론이 제공하는 정보들은 별도의 암호화 없이 누구나 식별할 수 있도록 평문으로 노출된다. 이를 악용하면 공격자는 드론으로부터 제공되는 정보들을 획득하여 90%의 정확도로 비행경로를 추적할 수 있다.[2]

본 논문에서는 PUF 와 같은 하드웨어의 고유특성을 이용하여 Remote ID 의 단점인 프라이버시 노출 문제를 가명정보를 통해 보호하면서, 신뢰할 수 있는 대상이 드론을 정확하게 식별할 수 있도록 하는 프로토콜을 제안한다.

2. 배경 지식

2. 1 PUF (Physically Unclonable Function)

PUF 란 공정 과정에서 반도체에서 임의로 발생하는 미세구조에 의해 고유한 개인 키가 생성되는 기술을 말한다. 이러한 키는 물리적으로 복제될 수 없으며 사람의 지문과 같은 역할을 한다.

PUF 의 종류로는 통신 칩셋(Wi-Fi, SUN 칩)의 여유 SRAM 을 이용한 PHY-PUF, 플래시 메모리를 이용한 Flash PUF 등이 있다. 본 논문에서는 레지스터와 커패시터의 연결을 통해 발생하는 오차를 이용하는 RC(Resister-Capacitor) PUF 를 사용하였다.[3]

2. 2 Remote ID

Remote ID 는 비행 중인 드론이 상대방에게 식별 및 위치 정보를 제공하는 기능이다. 항공 안전과 보안에 대한 드론 사용자의 책임을 강화하기 위한 목적으로 각 국가에서는 이에 대한 규정을 시행하고 있다.

미국 연방 항공청(FAA)에서는 UAS(Unmanned Aircraft Systems) Remote Identification 을 도입하여 비행 중인 드론이 상대방이 수신할 수 있는 식별 및 위치 정보를 제공하도록 규정하고 있다. 이에 따라 2023 년 9 월까지 모든 드론은 Remote ID 를 의무적으로 탑재해야 한다.

그러나 드론이 전송하는 Remote ID 메시지에는 드론의 위치 정보와 식별 정보가 포함되어 있다. 하지만 현재의 규정에서는 드론의 개인 정보 보호를 위한 규정을 제공하지 않는다.

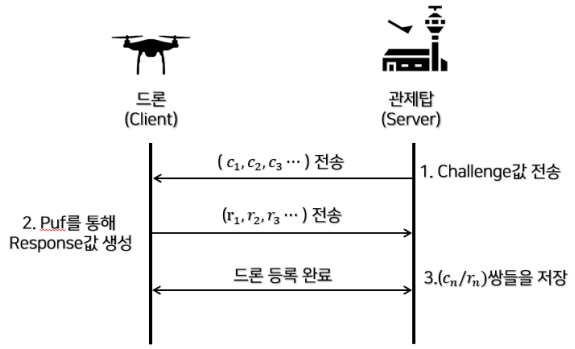
유럽 연합 항공 안전국(EASA)에서는 2024 년 1 월 1 일까지 모든 드론이 Remote ID 기능을 탑재해야 한다고 규정하고 있다. 드론은 무게 및 운용 위험도 등을 기준으로 7 가지 클래스로 분류되며, 일부 클래스를 제외한 드론은 Direct Remote ID 기능을 필수적으로 적용해야 한다. 이를 위해 기존 모바일 장치가 직접 수신할 수 있는 방식으로 개방형 및 문서화된 전송 프로토콜을 사용하여, 비행 전체 기간 동안 주기적인 브로드캐스트 통신을 실시간으로 보장해야 한다.

3. 익명성 보장을 위한 PUF 기반 드론 식별 프로토콜

본 장에서는 하드웨어의 고유특성을 활용하여 익명성이 보장되며 신뢰할 수 있는 대상인 지상관제센터(Ground

Control Station, 이하 GCS) 에서만 식별할 수 있는 드론 식별 방안을 제안한다. 제안하는 프로토콜에는 사전에 드론의 정보들을 GCS 에 저장할 등록 단계와 식별을 위한 식별 단계로 나누어진다.

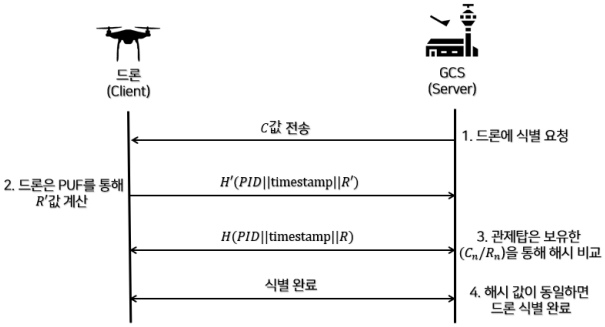
3.1 드론 등록 과정



[그림 1] 드론 등록과정

드론은 비행을 하기 전 GCS 에 등록 과정을 통해 식별을 위한 데이터를 저장한다. 드론은 사전에 안전한 채널을 통해 GCS 으로부터 챌린지 값 C (c_1, c_2, c_3…)를 받아 드론에 장착된 PUF 를 통해 고유의 리스폰스 $R(r_1, r_2, r_3$…) 값을 계산하여 전송한다.[4] GCS 은 (C, R) 값들과 드론 사용자의 정보를 함께 저장하며 식별에 사용된 값들을 삭제되며 일정 기간 뒤 다시 등록 과정을 통해 (C, R)값들을 GCS 에 등록해야 한다.

3.2 드론 식별



[그림 2] 드론 식별과정

드론은 랜덤으로 생성된 PID (Pseudo ID)를 브로드캐스트 하며 비행을 한다. GCS은 익명의 드론을 발견한 후 비행 중인 해당 드론의 사용자 및 드론의 정보를 파악하기 위해 식별요청을 하며 드론에 챌린지 값 C을 전송한다. 드론은 C값을 수신 받아 PUF를 통해 R'을 계산한다. 그 후 드론은 자신의 PID, timestamp, R'을 SHA-256 방식으로 해시를 적용한 값인 $H'(PID||timestamp||R')$를 GCS에 송신한다. GCS은 공개되어 있던 PID와 자신이 보낸 C값을 통해 등록 과정에서 저장한 (C, R)값들을 사용하여 $H(PID||timestamp||R)$들을 계산한다. 이후 GCS은 드론으로부터 수신받은 해시 값 $H'(PID||timestamp||R')$과 GCS에서 계산했던 해시 값 $H(PID||timestamp||R)$들을 비교하여, 드론을 식별한다. 식별에 사용되었던 (C, R)쌍은 폐기되며 다음 식별 시 저장 되어있던 새로운 (C, R)쌍을 사용한다.

4. 결론 및 토의

[표 1] PUF 를 사용한 드론 식별방법의 장단점

	D2D-MAP (SRAM PUF)[5]	Ring Oscillator PUF[6]	본 논문 (RC PUF)[7]
장점	CRP쌍을 메모리에 저장하여 데이터의 무결성을 보장	드론에 부착된 센서와 RO PUF 를 통해 생성된 값의 해시를 통한 하드웨어 및 소프트웨어의 무결성 보장	GCS에 여러 CRP쌍을 등록 후 인증에 사용된 쌍은 삭제 인증의 고유성 제공
단점	한 개의 CRP쌍을 사용하므로 보안 위협에 취약 및 오버플로우 발생가능	전압 변화에 취약 (8%의 전압차이로부터 7.2%의 오차 발생)	

[표 1]은 다양한 PUF 를 사용하여 드론 식별을 하였을 때 발생할 수 있는 장단점을 비교한 것이다. 본 논문에서 제안하는 프로토콜은 여러 쌍의 CRP 를 사용하여 식별 과정에서의 고유성 및 안정성을 강화하였다. 본 논문에서 사용한 RC PUF 는 10%의 전압 변화에도 1%의 오차를 보이며 다른 PUF 에서 발생할 수 있는 하드웨어의 결함을 개선하여 안정적이고 정확한 드론 식별이 가능하다.

본 논문에서는 Remote ID 규정으로 인해 노출되는 드론의 프라이버시를 보호하기 위해 PUF 기반의 드론 식별 프로토콜을 제안하였고, RC PUF 를 사용하여 기존 연구의 하드웨어 및 보안 취약점을 개선하였다.

PUF 기반의 드론 식별 프로토콜은 하드웨어의 고유 특성을 활용하여 드론의 익명성을 보호하면서도 안전한 식별이 가능하다. 또한 해시를 사용하여 GCS 을 제외한 다른 참여자들은 드론의 실제 식별정보가 아닌 PID 만을 확인할 수 있어 드론의 프라이버시를 보호할 수 있다. 이를 통해 드론 운용의 안전성과 개인 정보 보호를 동시에 보장할 수 있다.

Acknowledgement

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.RS-2023-00225201, 국방 무인이동체 역이용 방지 제어권 보호기술 개발)

참고문헌

[1] 국토교통부, 항공안전기술원, (2022), 드론 산업실태조사 보고서, 2022.12.30

[2] SVAIGEN, Alisson R., et al. Is the Remote ID a Threat to the Drone's Location Privacy on the Internet of Drones? In: *Proceedings of the 20th ACM International Symposium on Mobility Management and Wireless Access*. 2022. p. 81-88.

[3] 김주한, et al. 센서 기반의 디바이스 DNA 기술 동향. 전자통신동향분석, 2020, 35.1: 25-33.

[4] Alladi, Tejasvi, et al. "SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication." *IEEE Transactions Vehicular Technology* 69.12 (2020): 15068-15077

[5] PAL, Vishal, et al. Puf based secure framework for hardware and software security of drones. In: *2020 asian hardware oriented security and trust symposium (AsianHOST)*. IEEE, 2020. p. 01-06.

[6] LOUNIS, Karim; DING, Steven HH; ZULKERNINE, Mohammad. D2D-MAP: A drone to drone authentication protocol using physical unclonable functions. *IEEE Transactions on Vehicular Technology*, 2022, 72.4: 5079-5093.