정 보 보 호 학 회 지
제 30 권 제2호, 2020. 4

드론식별모듈(DIM) 기술 및 표준화 동향

강 유 성*, 김 건 우*, 김 주 한*, 이 상 재*

요 약

널리 알려진 바와 같이 드론산업은 4차 산업혁명을 견인하는 13대 혁신성장 동력 산업 중 하나이다. 드론은 조종사가 탑승하지 않는 무인/원격조종 비행장치로 영상촬영, 감시, 조사, 물품배송 등의 서비스에 활용되고 있다. 드론을 이용한 서비스가 안전하게 상용화되기 위해서는 필수적으로 드론 자체 및 드론 기반 서비스를 보호하는 드론 보안기술이 적용되어야 한다. 드론은 피해자임과 동시에 가해자가 될 수 있는 양면성을 지니고 있기 때문에 이러한 특성을 고려한 보안기술이 필요하다. 최근 드론 보안의 양면성을 고려한 핵심요소로 드론식별모듈(DIM)이 개발되고 있다. 본 논문에서는 드론식별모듈 개념을 정의하고, 주요 기능 소개 및 국제표준화 추진 현황을 설명한다.

Ⅰ. 서 론

구글이 선정한 세계 최고의 미래학자로 꼽히는 토마스 프레이가 2014년 9월에 발표한 “192 Future Uses for Flying Drones”는 드론이 사용되는 비즈니스 영역을 24개 카테고리로 구분하고, 각 카테고리별 8개 예제를 제시하여 총 192개의 활용 가능성을 전망하였다[1]. 24개 카테고리에는 조기경보 시스템, 물품배송, 게임, 마케팅, 엔터테인먼트, 부동산 등 민간 분야에 해당하는 활용이 포함되어 있으며, 이와 더불어 경찰 드론, 군대/스파이 드론과 같이 정부에서 사용하는 특수목적 활용도 고려되고 있다.

최근 드론은 날아다니는 스마트폰이라 할 정도로 디지털화가 진행되어 있고, LTE 또는 5G 통신을 통한 제어 및 정보전달이 가능해지고 있다. 그러나 드론이 다양한 활용 분야에 적용되는 과정에서 보안 취약점이 노출되고 있기 때문에 드론 보안기술 적용은 필수적인 요소가 되고 있다. 드론 자체는 일반적인 디지털 장치와 비슷하지만 활용 분야에 따라서 보호 대상이 되기도 하고, 반대로 공격 대상이 될 수도 있는 양면성을 지니고 있다[2]. 드론이 보호 대상이 되는 경우는 드론을 이용하는 서비스 제공자 또는 사용자 입장에서 안전한 드론 운영 및 드론 데이터 보호와 같은 드론 ICT 보안기술을 적용해야 하고, 드론이 공격 대상이 되는 경우는 건물 관리자나 일반인 입장에서 불법 드론으로부터 내 신체와 재산을 보호하기 위한 안티드론 기술을 개발하여 적용해야 한다[3].

드론 양면성을 고려한 드론 ICT 보안기술 및 안티드론 기술은 서로 다른 보안 관점을 가지고 있다. 예를 들어, 재밍기술은 안티드론 관점에서는 불법 드론을 피할 수 있도록 도와주는 방어기술이지만, 드론 ICT 보안 관점에서는 합법 드론의 정상적인 서비스를 방해하는 공격기술이다. 서로 다른 보안 관점을 가진 드론 ICT 보안기술과 안티드론 기술은 항상 배타적인 상황만 있는 것은 아니다. 앞에서 언급한 재밍기술의 예에서, 비행 중인 드론이 명백하게 불법 또는 비정상 드론이라는 확신이 있어야 재밍신호를 발사해야 하며, 합법 드론은 자신이 합법적 서비스를 수행 중이며 해당 지역에서 비행 허가를 받았음을 증명하여 재밍신호 발사를 막아야 한다.

즉, 드론 양면성을 모두 고려한 드론 보안의 시작은 비행 중인 드론을 식별하고 그 진위여부를 실시간으로 확인하는 것이다. 최근 이러한 목적을 달성하는 핵심적인 기술로 드론식별모듈(DIM: Drone Identity Module) 기술이 개발되고 있다. 본 논문에서는 드론식별모듈 개념을 정의하고, 주요 기능 소개 및 국제표준화 추진 현황과 향후 전망을 설명하고자 한다. 이를 위해 본 논문

본 연구는 과학기술정보통신부의 재원으로 한국연구재단, 무인이동체미래선도핵심기술개발사업단의 지원을 받아 수행되었음. (NRF-2017M1B3A2A01056680, 저고도 무인비행장치 교통관리체계 보안기술 및 불법 행위 억제 기술 개발)
* 한국전자통신연구원 미래암호공학연구실(책임연구원, youskang, wootopian, juhankim, leestrike@etri.re.kr)

은 다음과 같이 구성되어 있다. 제 II장에서는 드론 보안을 두가지 타입으로 정리하여 설명한다. III장에서는 드론식별모듈의 주요 기능과 개발 중인 형상을 요약하고, IV장에서 국제표준화 현황과 전망을 설명한다. 끝으로 V장에서 결론을 맺는다.

Ⅱ. 드론 보안 취약점 및 대응기술

드론 기반 서비스는 기본적으로 드론 비행을 전제로 하고 있다. 따라서 드론 보안은 드론 및 운영 인프라와 더불어 비행이라는 특수한 상황을 고려해야 한다. 일반적인 드론 보안 취약점은 불법탈취 후 키 해킹, 드론 무력화, 정보유출, 악성코드 감염, 불법장치 탑재 등으로 구분할 수 있으며, 이러한 취약점을 극복하기 위한 보안 요구사항은 참고문헌[4]에 잘 정리되어 있다.

이 장에서는 드론 비행을 바라보는 상반된 관점에서 보안 취약점 예시를 보여주고, 이를 극복하기 위한 대응 기술을 소개하고자 한다.

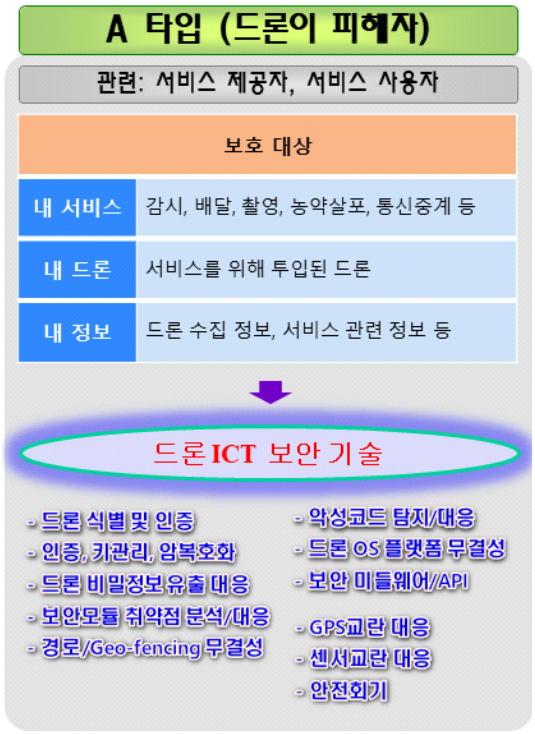
2.1. A 타입: 드론이 피해자인 경우

A 타입은 드론을 이용하여 서비스를 제공하는 서비스 제공자와 서비스를 제공받는 서비스 사용자와 관련된 상황이다. A 타입 관점에서는 드론 비행이 순조롭게 진행되는 것이 목표이다. 즉, 드론 해킹, 재밍, 또는 센서 오동작 공격에 의한 드론 탈취, 무력화, 좀비화 등을 방어해야 한다. 뿐만 아니라, 드론 비행 시 획득한 정보 또는 드론 비행 임무와 관련된 정보가 유출되지 않도록 방어해야 한다.

드론 보안의 양면성 측면에서 보면, A 타입에 해당하는 보안기술은 드론 ICT 보안기술이다. (그림 1)은 A 타입에서의 주요 보호 대상과 보안기술을 보이고 있다. 주요 보호 대상은 내가 제공하거나 제공받는 서비스, 드론 그 자체 및 서비스와 관련된 정보이다. 드론 ICT 보안기술은 드론 식별로부터 시작하며, 식별된 드론과 보안 인프라에 기반하여 드론과 서비스를 보호할 수 있으며, 재밍(RF 신호 교란)을 대비한 항재밍 기술 등이 결합되어 A 타입 상황을 보호할 수 있다.

2.2. B 타입: 드론이 공격자인 경우

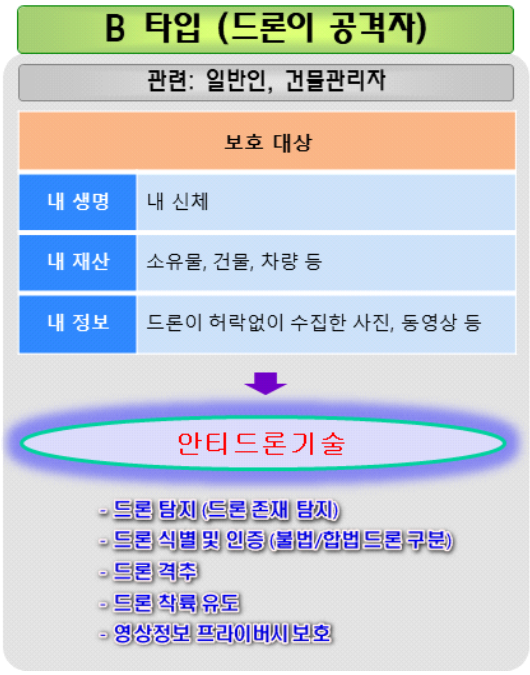
B 타입은 드론이 비행 중인 상황을 바라보고 있는



〔그림 1〕 A 타입(드론이 피해자) 보호 대상 및 보안기술

드론 서비스와 상관없는 일반인과 관련된 경우이다. B 타입 관점에서는 드론 비행이 자신을 위협하지 않는 것이 목표이다. 즉, 비행 중인 드론이 자기 신체에 위협을 가하거나 차량 또는 건물 등 자신의 재산에 충돌하여 손해를 입히는 것을 방어해야 한다. 뿐만 아니라, 비행 중인 드론이 자신의 허락없이 촬영하는 사진과 동영상으로부터 야기될 수 있는 프라이버시 침해 문제도 방어해야 한다.

드론 보안의 양면성 측면에서 보면, B 타입에 해당하는 보안기술은 안티드론 기술이다. (그림 2)는 B 타입에서의 주요 보호 대상과 보안기술을 보이고 있다. 주요 보호 대상은 개인의 신체, 차량, 건물 등이며 또한 드론이 취득하게 되는 사진이나 동영상으로부터 야기될 수 있는 개인의 프라이버시와 관련된 정보이다. 안티드론 기술에서도 비행 중인 드론에 대한 정확한 식별이 필요하다. 비행 중인 드론이 합법 드론인지 불법 드론인지 파악한 이후에 위협적인 존재라고 판단하게 되면 신고, 격추, 착륙 등의 안티드론 기술을 활용하여 B 타입 상황을 보호할 수 있다.



〔그림 2〕 B 타입(드론이 공격자) 보호 대상 및 보안기술

Ⅲ. 드론식별모듈(DIM) 기술

드론 식별의 핵심요소인 드론식별모듈 기술을 표준화하고 있는 ISO/IEC JTC1 SC17 WG12 표준그룹에서는 드론식별모듈을 “functional module with the capability of storing data, at least drone identification information and drone registration information and cryptographic functions”로 정의하고 있다[5]. 즉, 드론식별모듈은 드론 식별정보 또는 드론 등록정보 등 최소 1개 이상의 드론 관련 정보를 저장하고 있으며 보안 기능을 수행할 수 있는 기능 모듈이다. 이 장에서는 드론식별모듈의 기술적 특징을 설명한다.

3.1. 주요 저장 정보 및 보안 기능

국제표준화가 진행 중인 드론식별모듈 표준문서인 ISO/IEC 22460-2 작업초안에서 정의하고 있는 드론식별모듈의 주요 저장 정보는 드론 식별정보, 드론 운영자 정보, 그리고 암호 연산에 사용되는 보안 파라미터이다.

드론 식별정보는 국가 코드, 생산자 번호, 모델 번호, 일련 번호의 연접된 형태로 구성될 수 있다. 드론 운영자 정보는 운영자 이름, 주소, 이메일 주소, 전화 번호, 면허 번호 등을 포함할 수 있다. 드론식별모듈에 저장되는 보안 파라미터는 주로 키 관련 정보로 비대칭키 연산에 사용되는 개인키, 인증서 및 대칭키 연산에 사용되는 비밀키 등이며, 이러한 정보는 드론식별모듈의 안전한 영역에 저장되어야 한다.

드론식별모듈은 드론 ICT 보안과 안티드론 기술에서 활용할 수 있는 기본적인 보안 기능을 제공해야 한다. 예를 들면, 엔티티 인증, 세션키 합의, 데이터 암복호화, MAC 코드 생성, 전자서명, 해시 등의 보안 기능을 수행할 수 있어야 한다.

이 외에도 ISO/IEC 22460-2 국제표준 작업초안에는 드론과 드론 관리 시스템 사이의 드론식별모듈 기반 상호 인증 절차 및 비행경로 정보에 대한 데이터 무결성을 보장하는 기법 등을 정의하고 있다.

3.2. 주요 형상

ISO/IEC 22460-2 국제표준 작업초안에서는 드론식별모듈의 물리적 형상에 대해 제약사항을 정의하지는 않는다. 특정 하드웨어 폼팩터로 제한하지는 않지만, USIM 타입, micro SD 타입, eSIM 타입, SoC 내의 모듈 형태 등을 구현 예로 들고 있다.

(그림 3)은 ETRI에서 구현한 드론식별모듈의 3가지 타입(USIM 타입, micro SD 타입, USB 타입)을 보이고 있다.

〔그림 3〕 드론식별모듈 구현 예 (USIM, uSD, USB)

Ⅳ. 드론식별모듈(DIM) 표준화 동향

드론식별모듈에 대한 기술 표준화를 담당하고 있는 국제표준화 그룹은 ISO/IEC JTC1 SC17 WG12(이하 WG12)이다. ISO/IEC JTC1 SC17(이하 SC17) 표준위원회의 공식 명칭은 “Cards and security devices for personal identification”으로 표준화 대상은 IC 카드 물리적 규격, IC 카드 보안기술 규격, IC 카드 형태의 ISO 운전면허증(운전자 라이선스), 그리고 드론 조종자 면

허증 및 드론식별모듈 등이다[6]. SC17 산하 표준 작업 그룹 중 하나인 WG12의 공식 명칭은 “Drone license and drone identity module”로 드론 면허증(라이선스)과 드론식별모듈을 표준화하고 있다.

4.1. 국제표준화 현황

(표 1)은 현재 작업초안 상태인 드론식별모듈 표준에 대한 현황을 요약한 것이다.

WG12는 2018년 4월에 서울에서 제1차 회의를 시작하여 현재(2020년 3월)까지 총 8차례 회의를 진행했다. 2018년 10월 일본에서 개최된 제3차 회의에서는 드론식별모듈 표준인 ISO/IEC 22460-2 표준의 첫 번째 WD가 발표되어 논의되었다. 그 이후 현재까지 WG12에서는 드론식별모듈이 가지는 데이터 셋(드론 식별정보, 드론 등록정보, 드론 비행정보, 그리고 키, 인증서, 난수와 같은 암호 연산용 데이터 등)과 드론식별모듈이 처리하는 보안 프로토콜(비대칭키 기반의 인증 및 키 설립, 대칭키 기반의 인증 및 키 설립, 그리고 드론 비행정보 무결성 보장을 위한 전자서명 등)에 대한 표준화를 진행 중이다[3].

〔표 1〕 드론식별모듈 표준 (2020년 3월)

표준번호	표준명	현단계	에디터
ISO/IEC 22460-2	ISO License and Drone Identity Module for Drone(Ultra Light Vehicle or Unmanned aircraft system) – Part 2: Drone Identity Module	3rd WD*	강유성 (한국 ETRI), 김건우 (한국 ETRI), Haiying Lu (중국 CESI)

* WD(Working Draft, 작업초안): 위원회 승인받기 전, 작업그룹이 작성 중인 문서

4.2. 국제표준화 전망

드론식별모듈의 보안 기능에 대한 표준화는 2021년 하반기 제정을 목표로 논의가 활발하게 진행될 것으로 예상되며, 이와 함께 드론식별모듈에 저장될 글로벌 식별코드 체계에 대한 협력도 필요할 것으로 보인다. 글로벌 식별코드 체계와 드론식별모듈이 표준화된 방식으로 전 세계의 드론과 운영시스템에 적용되면 보다 안전하고 편리하게 합법 드론과 불법 드론을 식별할 수 있을 것으로 보인다.

Ⅴ. 결 론

4차 산업혁명을 견인하는 13대 혁신성장 동력 중 하나인 드론산업은 그 발전 가능성이 상상을 초월할 수 있다. 지금은 주로 영상촬영과 개인 엔터테인먼트용의 소형 드론이 대세이지만 가까운 미래에는 물품배송, 감시, 조사를 비롯해 인류를 위한 교통수단으로 확대될 수 있기 때문에 그 활용처는 사람의 삶 전반에 영향을 주게 될 것이다. 따라서 드론이 비행하는 상황에서는 반드시 드론 ICT 보안기술과 안티드론 기술이 구현되어 있어서 서비스 제공자, 서비스 사용자, 서비스와 무관한 일반인 모두의 보안과 안전을 보장해야 한다.

본 논문에서 기술 및 표준화 현황을 소개한 드론식별모듈은 드론 기반 서비스 확대를 위한 핵심적인 보안 기능을 제공할 수 있을 것으로 기대된다.

참 고 문 헌

[1] Thomas Frey, “192 Future Uses for Flying Drones”, https://futuristspeaker.com/business-trends/192-future-uses-for-flying-drones/, 2014.

[2] 강유성, “드론 활용 양면성을 고려한 드론 보안 기술”, 제25회 정보통신망 정보보호 컨퍼런스 (NetSec-KR 2019), April 2019.

[3] 강유성, 김건우, 김주한, 이상재, “드론 ICT 보안기술 표준화 동향”, TTA 저널, Vol. 182, pp. 66-71, April 2019.

[4] 강유성, 김건우, 김주한, “드론 기반 서비스를 위한 보안 요구사항”, TTA 저널, Vol. 177, pp. 74-79, June 2018.

[5] ISO/IEC WD2 22460-2, “Cards and security devices for personal identification – ISO License and Drone Identity Module for Drone(Ultra Light Vehicle or Unmanned aircraft system) – Part 2: Drone Identity Module”, ISO/IEC JTC1 SC17 WG12, May 2019.

[6] ISO/IEC JTC 1/SC 17, https://www.iso.org/committee/45144.html

〈저 자 소 개〉

강 유 성 (Yousung Kang)

종신회원

1997년 2월 : 전남대학교 전자공학과 졸업
1999년 8월 : 전남대학교 전자공학과 석사
2015년 8월 : KAIST 전기및전자공학부 박사
2011년 1월~2012년 4월 : 영국 북아일랜드 QUB 방문연구원
1999년 11월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원/기술총괄
<관심분야> 암호엔지니어링, IoT보안, 드론보안, 키 보호 및 분석, 부채널 분석 등

김 건 우 (Keonwoo Kim)

1999년 2월 : 경북대학교 전자공학과 졸업
2001년 2월 : 경북대학교 전자공학과 석사
2013년 2월 : 충남대학교 컴퓨터공학과 박사
2000년 12월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
<관심분야> 암호프로토콜, 이동통신보안, 드론보안, IoT보안 등

김 주 한 (Juhan Kim)

1997년 2월 : 충남대학교 컴퓨터과학과 졸업
1999년 2월 : 충남대학교 컴퓨터과학과 석사
2000년 8월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
<관심분야> IoT보안, 드론보안, 키관리, 부채널 분석 등

이 상 재 (Sangjae Lee)

1999년 2월 : 전북대학교 전자공학과 졸업
2001년 2월 : 전북대학교 전자공학과 석사
2013년 8월 : 충북대학교 정보통신공학부 박사
2000년 12월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
<관심분야> 전자공학, 무선통신 칩, PUF 설계, IoT보안 등