정 보 보 호 학 회 지
제 30 권 제2호, 2020. 4

드론 보안에 적용된 암호 기술 현황

조 성 민*, 서 승 현**

요 약

드론은 군용에서부터, 공공 관제 및 모니터링, 촬영 및 취미, 배송 서비스에 이르기까지 다양하게 활용되고 있다. 그러나 드론에 내장된 센서 값 조작이나 수집 데이터 누출, 통신 내용 도감청 및 GPS 신호 조작 등의 보안 취약점을 이용한 공격은 드론을 포획하거나 추락시키고 중요한 데이터를 탈취하는 등 심각한 문제를 야기할 수 있다. 이러한 보안 취약점을 해결하기 위해 드론 전용 난수 생성기와 통신보호를 위한 암호프로토콜, 화이트박스 암호를 통한 정보보호 및 신호 인증을 통한 GPS 스푸핑 탑지 기법 등 안전한 드론 보안 메커니즘이 활발히 연구되고 있다. 이에 본 논문에서는 드론 시스템의 구성 요소별 보안 위협 요소를 살펴보고, 보안 위협 사례를 공격 유형별로 분석한다. 또한 이러한 보안 위협들에 대응하기 위해 드론에 적용된 암호 기술 현황에 대해 살펴본다.

Ⅰ. 서 론

IoT를 비롯한 정보통신 기술과 인공지능 기술, 스마트 기기의 발전으로 드론 관련 산업이 급성장하였으며, 세계 드론 시장의 규모는 2024년까지 약 430억 달러 규모로 커질 것으로 예상하고 있다 [1].

2013년 아마존의 드론 배송 시범 서비스를 시작으로 현재 민간용 드론은 사진 촬영용 소형 드론부터 시설물 인프라 관리, 택배 및 화물수송, 재난방재 및 비료 살포 등과 같은 정밀농업 등으로 활용 범위를 확대하며 다양한 상업 및 공공 서비스들에 이용되고 있다 [2].

그러나 무인시스템으로 무선네트워크 망을 이용하는 드론은 태생적인 특성상 탈취공격과 같은 물리적 보안 취약성과 더불어, 통신도청, GPS 신호조작 및 신호방해 공격, 악성코드 감염 등 각종 사이버 공격에 취약하다 [3]. 드론이 해커의 공격에 의해 수집된 정보가 노출된다면, 드론이 촬영한 영상들은 사용자 프라이버시 침해하는 목적으로 악용될 수 있다. 또한 재난방재 현장에 사용되는 드론이 악성코드 감염으로 인하여 잘못된 알람/경보 정보들을 제공하거나 드론이 전송하는 메시지가 도감청되거나 위변조되어 전달된다면, 시스템에 혼란을 주어 더 큰 위험을 야기할 수 있다.

2011년 12월 이란은 이란 영공을 정찰하던 미 공군 최첨단 드론 'RQ-170 센티널(Sentinal)'을 GPS 조작으로 강제 착륙시키는 GPS 스푸핑(spoofing) 공격을 하였고, 2016년도에는 일본에서 열린 보안 컨퍼런스 ‘2016 PacSec’에서 이카루스라는 시스템이 드론에 적용된 DSMx 통신 프로토콜의 취약점을 이용해 해킹을 하는 기술을 시연해 보였다 [4]. 2019년에는 미국 국토안보부가 중국산 드론에서 민감한 항공 정보나 사용자의 개인 정보가 유출될 가능성을 제기하며, 드론에서의 보안 위협을 규정하였다 [5].

이처럼 드론의 보안 사고가 잇따라 일어나면서, 드론 통신 보호 및 수집정보보호, GPS 스푸핑 대응 등을 위한 드론 보안 메커니즘 개발의 필요성이 대두되었고, 기밀성 및 무결성, 인증 서비스를 제공할 수 있는 암호 기술들을 적용하여 드론보안메커니즘을 설계하는 방안들이 활발히 연구되어왔다.

본 논문에서는 드론의 보안 위협 및 드론에 대한 공격 유형을 분석하고, 보안 위협으로부터 안전한 드론 서비스를 제공하기 위한 보안 메커니즘 기술 동향에

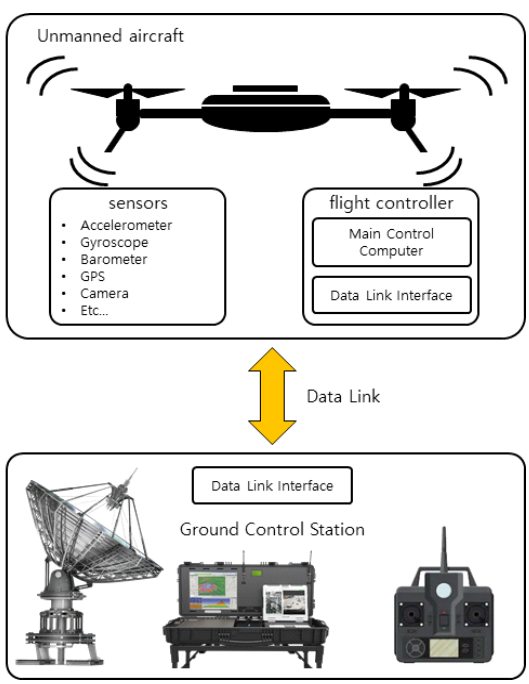
본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었습니다. (IITP-2020-2018-0-01417)
본 연구는 산업통상자원부 ‘산업혁신인재성장지원사업’의 재원으로 한국산업기술진흥원(KIAT)의 지원을 받아 수행되었습니다. (2020년 산업 융합형 웨어러블 스마트 디바이스 전문인력 양성사업, 과제번호 : P0002397)
* 한양대학교 대학원 전자공학과 (대학원생, smcho3315@hanyang.ac.kr)
** 한양대학교 ERICA 캠퍼스 전자공학부 (교수, seosh77@hanyang.ac.kr)

대해 살펴본다. 본 논문의 구성은 다음과 같다. 2장에서 드론 시스템 구조를 설명하고, 3장에서는 현재 드론을 대상으로 하는 보안 위협들을 공격 유형에 따라 분류하여 설명한다. 4장에서는 안전한 드론 서비스를 위해 제안된 드론 암호 기술 동향을 설명하며, 마지막으로 5장에서 본 논문의 결론을 맺는다.

Ⅱ. 드론 시스템 구조

무인 항공기(UAV, Unmanned Aerial Vehicle)라고도 불리는 드론 시스템은 [그림 1]과 같이 기본적으로 무인 비행체(unmanned aircraft)와 지상 관제소(GCS, Ground Control Station), 통신 데이터 링크 등으로 구성되어 있다.

무인 비행체인 드론에는 중앙처리장치인 비행 제어기(flight controller)가 탑재되어 있는데, 이 비행 제어기는 센서로부터 들어오는 값을 읽고 처리하여 드론이 안정적으로 비행할 수 있도록 제어하며, 지상 관제소와의 통신 인터페이스를 구현하여 이러한 정보를 지상 관제소에 전달하는 역할을 한다. 지상 관제소는 무선 링크를 통해 드론과 통신하여 명령을 전송하고 실시간 데이터를 수신하는 가상 조종실로써, 드론 시스템을 운영하는 운영자가 지상에서 드론을 제어 또는 감시할 수 있는 기능을 제공한다. 이처럼 드론과 지상 관제소 사이에 제어 정보를 전달하거나 데이터를 송수신하는 데 사용되는 무선 링크를 데이터 링크라 한다.



〔그림 1〕 드론 시스템 구조

드론 시스템은 구성 요소별로 보안 위협 지점들이 있다. 우선 드론에 내장되어 있는 센서 값들을 조작하게 되면 비행 제어기가 잘못된 센서 값을 받아들여 드론이 추락할 수 있으며, 드론이 추락할 경우, 내부에 저장되어 있던 수집 데이터가 누출될 위험이 존재한다. 또한 드론이 다른 드론이나 지상 관제소와 데이터 링크를 통해 무선 통신할 때 통신 내용이 도청되거나 조작될 수 있으며, 드론을 제어하기 위해 사용되는 GPS 신호가 조작될 수 있다. 3장에서는 이러한 보안 위협으로 인한 드론 공격 유형들을 기술한다.

Ⅲ. 드론의 보안 위협 및 공격 유형

본 장에서는 드론의 보안위협과 이를 이용한 공격 유형들을 분석한다.

3.1. 드론 통신 취약점 공격

드론은 지상 관제소와 데이터 링크를 통해 통신하게 되며, 이때 민간용 드론에서 가장 널리 사용되는 통신 프로토콜 중 하나가 MAVLink(Micro Air Vehicle Link)이다. MAVLink는 경량화에 중점을 두면서 보안 메커니즘이나 암호화 알고리즘을 채택하지 않고 개발되었다. 따라서 MAVLink 프로토콜을 사용하여 통신을 하게 되면 스푸핑, 메시지 위조 및 서비스 거부(DoS, Denial of Service)를 포함한 여러 공격에 취약하며 [6, 7], 기밀성과 무결성, 가용성 등의 보안 서비스를 제공하지 않는다 [8]. 이러한 MAVLink의 보안 문제를 해결하기 위해 2013년도에 STS(Station-to-Station) 키교환 프로토콜과 AES-GCM 대칭키 암호알고리즘을 사용한 sMAVLink(Secure MAVLink)가 제안되었으나 [9], MAVLink 패킷 구조를 완전히 바꿔야 하는 등의 문제와 이식성 문제 때문에 아직까지 상업용 드론에 적용되지 않고 있다.

실제로 2013년에는 이라크에서 작전 중인 미국의 드론 함대에 공격이 가해져 드론이 지상 관제소에 보낸 비디오 피드를 이라크 무장단체가 가로챘으며,

2015년 2월에는 드론의 통신 세션을 하이재킹하여 드론을 자신의 의도대로 조작할 수 있도록 하는 MalDrone 악성코드가 발견되었다. 또한 2016년도에는 일본에서 열린 보안 컨퍼런스 '2016 PacSec'에서 드론 뿐 아니라 원격조정으로 동작하는 어떠한 기기도 해킹이 가능한 이카루스(Icarus) 시스템이 공개되었는데, 이는 드론에 적용된 DSMx 통신 프로토콜의 취약점을 이용해 해킹하였다.

3.2. 드론 수집정보 조작 및 데이터 탈취 공격

드론은 탑재된 여러 센서를 통해 비행 제어를 하며, 기후 정보나 영상 등의 데이터를 수집한다. 이때 센서를 타겟으로 하여 수집정보를 조작하는 공격들이 가해지고 있다. 드론은 비행 제어기에 조작된 값을 주입하여 센서를 손상시키고 드론의 안전한 컨트롤을 저해함으로써 비행을 불안정하게 만드는 거짓 센서 값 주입 공격에 취약하다 [10]. 예를 들어 드론의 비행 자세 제어에 사용되는 자이로스코프 센서의 경우 공진 주파수에서의 잡음으로 인해 공명이 발생되고, 그로 인해 자이로스코프에 성능 저하가 일어난다 [11]. 실제로 2015년에는 상업용 드론에 널리 사용되는 MEMS 자이로스코프의 공명 출력을 분석하고 센서를 조작함으로써 드론을 추락시켰다 [12].

또한 순찰 드론은 외부에 공개되지 않은 지역의 이미지나 영상 파일 등을 가지고 있으며, AI용 빅데이터 수집 드론은 여러 가지 센싱 값들을 데이터화하여 저장함으로써 드론 자체가 매우 중요한 자산이 되는 경우도 있다. 그러나 현재 이처럼 안전하게 보관되어야 하는 중요한 데이터들이 탈취되는 문제가 계속되고 있다. 드론에 암호화되어 저장된 데이터 또한 드론을 탈취하여 암호 알고리즘을 분석하면 드론에 내장되어 있는 암호화 키로 데이터가 복호화될 수 있다. 실제로 2011년에는 '키로거(keylogger)' 악성코드가 미국 네바다 공군기지의 드론 통제시스템을 감염시켜, 조종사가 드론에 입력한 모든 정보가 유출되는 사건이 있었다.

3.3. 드론의 GPS 스푸핑(spoofing) 공격

드론의 항법 제어를 위해 사용되는 브로드캐스트 신호는 불특정 다수를 상대로 브로드캐스트하는 특성상 암호화되지 않거나 인증되지 않기 때문에 쉽게 전파 방해를 받거나 가짜 신호로 대체될 수 있다. 항공기 감시 정보를 일정 주기마다 자동으로 브로드캐스트하여 항공기 간의 충돌을 방지하는 항공기 감시 체계인 ADS-B(Automatic Dependent Surveillance - Broadcast) 또한 이러한 특성 때문에 스푸핑 공격에 취약하다. 따라서 드론에 악의적인 ADS-B 신호를 지속적으로 공급함으로써 드론의 항로를 바꿔 원하는 지역으로 드론을 유도할 수도 있다 [13].

드론 항법 제어를 위한 대표적인 브로드캐스트 신호인 GPS 신호 또한 ADS-B 신호처럼 가짜 신호를 생성하여 공급함으로써 드론의 GPS 수신기가 계산한 지리적 좌표를 변경하는 스푸핑 공격이 가능하다. 따라서 인공위성으로부터 받은 GPS 정보를 수신해 비행하는 드론은 이처럼 교란된 GPS 신호로 인해 엉뚱한 항법 정보가 입력되어 탈취되거나 추락할 수 있다.

2011년 12월에는 실제로 이란이 엉뚱한 착륙지점 신호를 보내 그들이 의도한 곳으로 유인하는 GPS 스푸핑 공격을 가하여 미국의 무인정찰기를 포획하였다. 2014년도에는 텍사스 대학교의 팀이 드론에서 약 0.3 마일 떨어진 곳에 위치한 맞춤형 GPS 스푸핑 장치를 사용하여 GPS 신호의 완벽한 복제본을 만들어 드론에 공급함으로써 드론에 대한 GPS 스푸핑 공격을 입증하였다 [14]. 수신된 신호의 진위를 확인할 수 없는 이 드론은 가짜 신호에 반응하여 추락하였다.

GPS 신호 발생기를 활용하여 원래 위성 신호의 위조된 복제 신호를 만드는 일반적인 GPS 스푸핑 방법 외에도, GPS 수신기에 GPS 악성코드를 내장하여 수

〔표 1〕 드론 보안 공격 유형 별 위협 기술 및 그에 따른 문제점

공격 유형	보안 위협 기술	위협에 따른 문제점
통신 취약점 공격	MalDrone 악성코드	통신 세션 하이재킹
	Icarus 시스템	드론 시스템 해킹, 드론 추락
수집정보 조작 및 데이터 탈취 공격	가짜 센서값 주입	센서 손상, 컨트롤 저해
	Keylogger 악성코드	조종사가 드론에 입력한 정보 유출
GPS 스푸핑 공격	위조된 복제 신호 생성 및 공급	드론 탈취 및 추락
	GPS 악성코드	드론 탈취 및 추락

신된 위성 신호로부터 계산된 위치와 다른 위치를 생성하는 GPS 스푸핑 방법도 존재한다.

Ⅳ. 드론에 적용된 암호 기술 현황

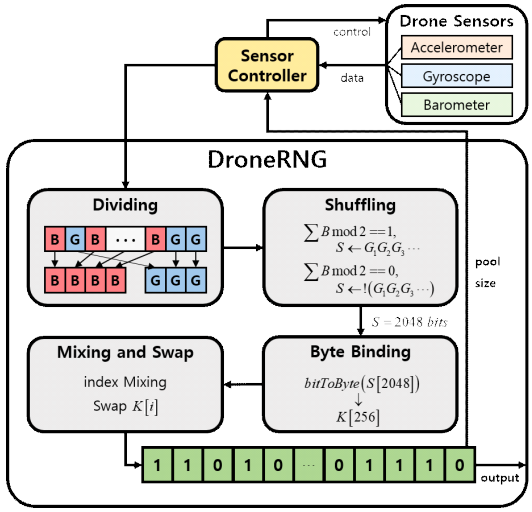
3장에서 서술한 것처럼 드론에는 다양한 보안 위협들이 존재한다. 본 장에서는 이러한 보안 위협들에 대응하기 위해 드론에 적용된 암호 기술을 살펴본다.

4.1. 드론 전용 난수 생성기

드론에 보안 프로토콜을 탑재하여 안전한 드론 시스템을 구축하기 위해서 기본적으로 수반되어야 하는 것이 난수를 사용하여 안전한 암호 키를 생성하고 보호하는 것이다. 따라서 안전한 난수 생성기의 설계는 보안 프로토콜의 안전성과 직결된다. 그러나 기존에 드론에 사용되던 난수 생성기들은 데스크톱 PC의 마우스나 키보드와 같은 사용자/외부 주변장치, 인터럽트 요청 시간, 디스크를 읽고 쓰는 시간 등 PC에서 얻을 수 있는 자원을 seed로 이용하여 난수를 생성하였다. 따라서 이를 드론에 적용하였을 때 생성된 난수의 난수성이 떨어지는 문제가 존재한다. 이러한 문제를 해결하기 위해 2020년에 드론의 센서를 활용한 드론 전용의 난수 생성기인 DroneRNG가 제안되었다 [15].

드론은 정지하고 있을 때와 비행하고 있을 때 출력하는 센서값이 매우 다르기 때문에 센서값을 활용하여 난수를 생성할 때는 두가지 상황 모두를 고려하여야 한다. DroneRNG는 드론이 정지 상태일 때와 비행 중일 때 각각의 센서값의 특성을 분석하고 그 특징을 활용하여 각각의 상황에 따라 다르게 센서값을 후처리하는 과정을 거친다. 이로 인해 정지 상태와 비행 상태일 때 모두에서 사용이 가능한 난수 생성기를 설계하였다. DroneRNG의 구조는 [그림 2]와 같다.

먼저 센서 컨트롤러에 의해 드론의 비행을 위해 탑재된 가속도계, 자이로스코프, 기압계 등의 센서로부터 센서값을 받아서 Dividing 단계에서 센서값 중 난수성이 좋은 비트와 난수성이 안 좋은 비트로 나눈다. Shuffling 단계에서는 난수성이 안 좋은 비트들을 활용하여 난수성이 좋은 비트들을 후처리하여 준 뒤, Byte Binding 단계와 Mixing and Swap 단계를 통해 바이트 단위의 믹싱 과정을 거쳐 난수를 생성하게 된다. 생



〔그림 2〕 DroneRNG의 구조 〔15〕

성된 난수열은 난수열 버퍼에 저장되어 필요시 사용되게 된다. 이때 난수를 생성하여 난수열 버퍼를 채우는 과정과 버퍼에서 난수열을 읽어와 사용하는 과정이 각각 독립된 쓰레드에서 진행되어 난수를 생성하는데 걸리는 시간을 기다릴 필요 없이 바로 버퍼에서 난수를 불러와 사용할 수 있게 구현하였다. 또한 DroneRNG는 난수를 생성하는데 필요한 시간과 메모리가 기존 난수 생성 기법과 비교하여 크게 차이가 나지 않으면서, 생성된 난수가 더 좋은 통계적 특성과 예측불가능성을 지니는 동시에 전력소모율도 적은 장점을 가지고 있다. 따라서 프로펠러를 돌리는 모터가 배터리의 대부분의 전력을 소모하며, 제한된 계산 능력과 메모리 크기를 가진 드론에 적용이 적합하다.

4.2. 드론 통신보호를 위한 암호프로토콜

드론과 지상 관제소 혹은 다른 사물과의 안전한 통신을 위해서는 인증된 사용자와의 사전 키 공유가 수반되는 암호화 통신 프로토콜을 탑재하여야 한다.

2015년에는 드론과 스마트 객체 간의 안전한 통신을 위해서 단방향 키 합의와 전자서명을 결합한 효율적인 일대일(one-to-one) 통신 보안 프로토콜(eCLSC-TKEM, efficient Certificate-less Signcryption Tag Key Encapsulation Mechanism)이 제안되었다 [16]. eCLSC-TKEM은 무인증서 공개키 암호(CL-PKC, Certificateless Public Key

Cryptography)를 이용하여 대칭키를 공유하는 키 캡슐화(key encapsulation) 프로토콜이다. 이 기법은 CL-PKC를 기반으로 설계되어 인증서 기반 공개키 암호(ID-PKC, Identity-based PKC)의 키 에스크로 문제와 전통적인 PKC 기반 암호의 인증서 관리로 인한 오버헤드 문제를 해결하였다 [17]. 또한 발급된 개인키에 유효 기간을 부여하고 기간이 만료되면 새 개인키가 생성되게 함으로써 드론이 탈취되어도 개인정보 등의 데이터가 유출되는 것을 방지하였다. 이로 인해 인증된 키 합의와 부인방지, 사용자 해지 등의 모든 보안 요구사항들을 만족한다.

일대일 통신 보안을 제공하는 eCLSC-TKEM 외에도 2017년에는 일대다(one-to-many) 통신 보안 프로토콜인 CL-MRES(Certificateless Multi-Recipient Encryption Scheme)와 다대일(many-to-one) 통신 보안 프로토콜인 CLDA(Certificateless Data Aggregation)가 제안되었다 [18]. CL-MRES는 드론이 다수의 스마트 객체에 효율적이고 안전하게 데이터를 전송할 수 있도록 설계된 하이브리드 암호화 방식이다. 하이브리드 암호화를 위한 대칭키 공유에는 eCLSC-TKEM이 활용되며, 다중 수신자에게 데이터를 전송하기 위해 random re-use 기법이 적용된다. 이때 드론이 다수의 스마트 객체와 통신해야 하기 때문에 드론에서의 연산 오버헤드가 최소화되어야 한다. 이를 위해 전자 서명 기능을 제외함으로써 부인방지를 지원하지는 않지만 드론에 대한 연산 및 통신 오버헤드를 크게 줄였다. CLDA는 EC-ElGamal 동형 암호화와 최적화된 batch 검증 기술을 활용하여 다중 스마트 객체로부터 데이터를 효율적으로 수집할 수 있도록 한다. 이로 인해 수집된 모든 값들은 data pollution 공격으로부터 보호되며, 데이터의 기밀성과 프라이버시를 보장한다.

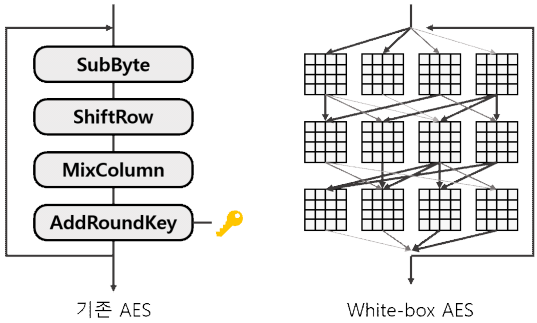
이외에도 2017년에는 드론과 지상 관제소 간의 안전한 데이터 전송을 위해 일회성 패드(One-Time Pad) 기반 암호 통신 방법이 제안되었다 [19]. 이 기법은 높은 암호화 속도와 단순한 구현이 가능한 일회성 패드 암호화를 이용하여 통신 데이터를 암호화함으로써 제한된 계산 능력을 갖는 드론에 기밀성을 제공한다. 2019년에는 MAVLink의 보안 취약점을 보완하기 위해 MAVLink에 ChaCha20 암호화 알고리즘 [20]을 통합하여 메모리와 CPU와 같은 성능에 영향을 주지 않고 메시지의 기밀성을 보장하는 MAVSec이 제안되었다 [21].

4.3. 드론내 저장된 정보보호를 위한 화이트박스암호

드론에 저장된 데이터는 항상 안전하게 보관되어야 하며, 드론이 스푸핑 공격 등에 의해 탈취되더라도 드론에 저장되어 있는 데이터는 악의적인 사용자에게 노출되지 않아야 한다. 그러나 데이터가 암호화되어 저장되어 있더라도 암호화 키가 드론에 내장되어 있다면, 탈취된 드론에서 암호화 키를 획득함으로써 저장된 데이터를 확인할 수 있다. 그러나 탈취된 드론의 경우 공격자가 드론의 암호 알고리즘을 분석하여 암호 연산 과정을 들여다 볼 수 있는 화이트박스 공격에 취약하다. 이러한 화이트박스 공격으로부터 배달용 드론의 중요한 데이터와 암호화 키를 보호하기 위해 2016년 화이트박스 암호(WBC, White-Box Cryptography)를 사용하는 보안 프레임워크가 제안되었다 [22].

[그림 3]은 화이트박스 암호 기법인 화이트박스 AES의 구조를 보여준다. 화이트박스 암호는 룩업테이블로 만들어진 암호 알고리즘에 암호 키를 숨겨둠으로써 내부의 동작을 분석할 수 있는 공격자라 하더라도 암호 키를 쉽게 유추하지 못하도록 한다.

화이트박스 암호화는 암호화 키가 암호화 알고리즘 내부에 숨겨져 있는데, 이때 공격자가 비밀키가 내장되어 있는 화이트박스 복호화(WBD, White-Box Decryption) 코드를 분리하여 키로 직접 사용할 수 있는 코드 리프팅(code lifting) 공격에 취약하다. 코드 리프팅 공격으로부터 보호하기 위해 배달용 드론에는 WBD 모듈 없이 WBE(White-Box Encryption) 모듈만 탑재하고 배송 받는 고객 혹은 배송 관리자가 WBD 모듈과 WBE 모듈을 모두 가지고 있도록 한다. 따라서



〔그림 3〕 White-Box AES의 구조

고객 주소나 전자 영수증 등의 배송 정보와 비행 정보 데이터는 드론에 탑재된 WBE 모듈을 통해 암호화되며, 드론이 탈취되어 코드 리프팅 공격이 가해져도 드론에 저장된 데이터나 비밀키를 유추하는 것이 불가능하다. 암호화된 전자 영수증은 고객의 WBD 모듈로 복호화가 가능하며, 타원곡선 전자서명 알고리즘(ECDSA, Elliptic Curve Digital Signature Algorithm)을 통해 전자 영수증에 서명을 함으로써 부인방지가 제공된다. 이외에 드론에 저장된 고객 주소나 비행 정보 등은 배송 관리자만이 WBD 모듈을 통해 복호화를 하여 확인할 수 있다.

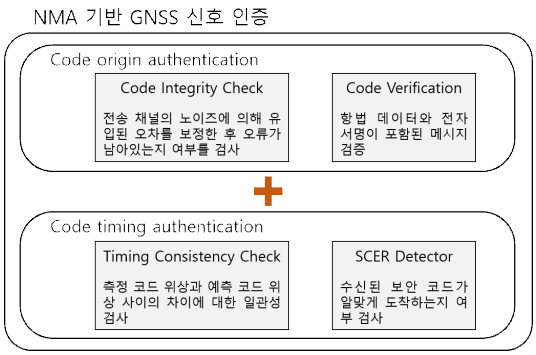
4.4. 드론 GPS 신호인증

실제 GPS 신호를 모방하여 잘못된 항법해(navigation solution)로 이끄는 스푸핑 공격은 GPS 신호를 기반으로 비행하는 드론에 심각한 위협이다. 최근에는 SDR (Software-Defined Radio) 기술의 급격한 발전으로 스푸핑 공격도 더욱 정교해지고 있다 [23]. GPS 수신기가 위협을 인식하지 못하고 잘못된 항법해에 의존하게 되면 추락이나 탈취 등 심각한 결과를 초래할 수 있다. 따라서 신뢰할 수 있는 GPS 스푸핑 탐지 기법을 적용해야 할 필요성이 있다. GPS 스푸핑 공격을 탐지하기 위해 물리적 방법을 통한 여러 스푸핑 탐지 메커니즘들이 제안되어왔다. 2005년도에는 민간용 GPS를 대상으로 하는 스푸핑 공격이 1575.42 MHz 주파수 대역의 L1 신호만 조작한다는 점을 감안하여 L1 신호와 1227.60 MHz 주파수 대역의 L2 신호의 세기 차이를 활용하여 스푸핑 공격을 탐지하는 기법이 제안되었다 [24]. 2012년도에는 스푸핑 신호의 세기가 일반적으로 진짜 신호의 세기보다 크고 심한 변동을 가지는 특성을 이용하여 수신되는 신호 세기의 통계적 분석에 기반한 스푸핑 탐지 기법이 제안되었다 [25]. 2014년도에는 수신된 GPS 신호의 비정상적인 도플러 주파수(Doppler frequency)로 스푸핑 공격을 탐지하는 기법이 제안되었다 [26]. 그러나 개별 위성에서 수신된 GPS 신호의 물리적 특성에 의존하는 기존의 기법들은 신호 처리(signal processing)를 통해 이러한 물리적 특성을 위조하여 스푸핑 탐지를 무력화시킬 수 있다.

물리적 특성을 활용한 스푸핑 탐지 기법의 한계를 해결하기 위해 브로드캐스트 신호를 암호화하거나 전자서명하는 암호학적 스푸핑 탐지 기법이 제안되었으며, 그 중 대표적인 것이 GNSS(위성측위시스템, Global Navigation Satellite System) 위성이 생성하는 내비게이션 메시지에 메시지 인증 개념을 적용한 NMA(Navigation Message Authentication)이다. 그러나 NMA에 기반한 신호 인증은 리플레이 스푸핑 공격에 취약하며 [25, 27], 통계적 가설 테스트를 활용하여

〔표 2〕 드론에 적용된 암호기술과 해당 기법들이 제공하는 기능 및 정보보호 서비스

암호 기술	기법	제공 기능	제공된 정보보호 서비스
드론 전용 난수 생성기	DroneRNG [15]	안전한 암호 키 생성	-
드론 통신 보호를 위한 암호프로토콜	eCLSC-TKEM [16]	효율적이면서 안전한 일대일 통신	기밀성, 무결성, 인증, 사용자 해지, 인증된 키 합의, 부인방지
	CL-MRES [18]	다수의 스마트 객체에 대한 안전한 데이터 전송	기밀성, 무결성, 인증, 사용자 해지, 인증된 키 합의
	CLDA [18]	다중 스마트 객체로부터의 안전한 데이터 수집	기밀성, 무결성, 인증, 사용자 해지, 프라이버시 보호
	One-Time Pad 기반 암호 통신 [19]	지상 관제소와의 안전한 데이터 전송	기밀성, 무결성
	MavSec [21]	MAVLink의 보안 취약점 보완을 통한 안전한 통신	기밀성, 무결성
드론내 저장된 정보보호를 위한 화이트박스암호	화이트박스 암호 [22]	드론에 저장된 데이터와 암호화 키 보호 및 사용자 인증	기밀성 무결성, 인증, 부인방지
드론 GPS 신호인증	NMA 기반 GNSS 신호 인증 [28]	GPS 신호 인증을 통한 스푸핑 공격 신호 탐지	인증



〔그림 4〕 NMA 기반 GNSS 신호 인증 구성 요소

리플레이 스푸핑 공격에 안전한 GPS 신호 인증이 제안되었다 [28]. 이 기법은 암호학적 코드 원본(code origin) 인증과 코드 타이밍(code timing) 인증을 결합하여 GNSS 스푸핑 신호를 탐지한다. [그림 4]는 개략화된 NMA 기반 GNSS 신호 인증의 구성을 보여준다.

코드 원본 인증에서는 전송 채널의 노이즈에 의해 유입된 오차를 보정한 후 오류가 남아있는지 여부를 검사하는 Code Integrity Check와 항법 데이터와 전자서명이 포함된 메시지를 암호 키로 검증하는 Code Verification 알고리즘을 통해 메시지를 인증하게 된다. 코드 타이밍 인증에서는 측정 코드 위상과 예측 코드 위상 사이의 차이에 대한 일관성을 검사하는 Timing Consistency Check와 수신된 보안 코드가 알맞게 도착하는지 여부를 검사하는 SCER Detector를 통해 메시지를 인증하게 된다. 이러한 통계적 가설 검사를 통해 채널당 매 5분마다 인증이 이루어지면서 0.97 이상의 확률로 리플레이 스푸핑 공격을 탐지한다.

Ⅴ. 결 론

드론이 단순 취미용 뿐만이 아니라 여러 산업에서 활용되면서 드론 산업은 급격한 성장을 이루었다. 그러나 군용으로 사용되던 시절부터 민간 서비스에 활용되는 현재까지 드론에 대한 보안 위협은 계속해서 존재해 왔으며, 드론의 보안 취약점을 이용하여 드론을 공격하는 보안사고가 잇따라 발생하고 있다. 이러한 드론의 보안 공격의 유형으로는 드론이 수신하는 통제 명령 혹은 통신하는 데이터를 탈취하거나 조작하는 통신 보안 공격, 드론이 저장하고 있는 데이터나 센싱 값들을 탈취하고 조작하는 수집정보 탈취 및 조작 공격, 그리고 드론의 항법에 이용되는 GPS 신호를 조작하여 드론을 탈취하는 GPS 스푸핑 공격 등이 있다. 본 논문에서는 이러한 공격 유형들을 분석하고 그에 따른 드론 보안 위협 사례들을 살펴보았다. 또한 드론 보안을 위해 제안된 드론 암호 기술들을 대응되는 보안 위협별로 정리하여 서술하였다. 드론에서의 암호 키 생성을 위해 제안된 드론 전용 난수 생성기를 살펴보았으며, 드론에서의 안전한 통신을 위한 암호프로토콜을 통해 드론의 통신보안 공격에 대응하는 방안을 살펴보았다. 또한 암호 키를 암호 알고리즘 내부에 숨김으로써 화이트박스 공격으로부터 드론의 데이터를 보호하는 방법과 메시지 인증을 통한 GPS 스푸핑 탐지 기법을 살펴보았다.

참 고 문 헌

[1] 국토교통부, “아프리카 하늘로 한국 드론 뜬다”, 보도자료, 2020.

[2] 김대종, 임륭혁, “국토관리를 위한 무인항공기 활용 사례,” 국토정책 Brief, 578, 1-8, 2016.

[3] TTA 표준, “드론 기반 서비스를 위한 보안 요구사항,” TTAK.KO-12.0317, 2016.

[4] 신동연, “해킹 쉬운 드론, GPS 교란시켜 빼돌릴 수 있을까,” 중앙일보, https://news.joins.com/article/23177968, 2018.

[5] 이세원, “美정부, 중국산 드론에도 경계령...“보안 정보 탈취 우려,”” 연합뉴스, https://www.yna.co.kr/view/AKR20190521064300009?section=search, 2019.

[6] A. Koubaa, B. Qureshi, M. F. Sriti, A. Allouch, Y. Javed, M. Alajlan, O. Cheikhrouhou, M. Khalgui, and E. Tovar, “Dronemap planner: A service-oriented cloud-based management system for the internet-of-drones,” *Ad Hoc Networks*, vol. 86, pp. 46-62, 2019.

[7] Y. M. Kwon, J. Yu, B. M. Cho, Y. Eun, and K. J. Park, “Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles,” *IEEE Access*, vol. 6, pp. 43203-43212, 2018.

[8] J. A. Marty, “Vulnerability analysis of the mavlink protocol for command and control of

unmanned aircraft," *Tech. Rep.*, 2013.

[9] L. Meier, "smavlink-secure mavlink, request for comments," Available: http://www.diydrones.com/profiles/blogs/smavlink-secure-mavlinkrequest-for-comments, 2013.

[10] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," *in Proceedings of the 1st Workshop on Secure Control Systems*, 2010.

[11] R. N. Dean, G. T. Flowers, A. S. Hodel, G. Roth, S. Castro, R. Zhou, A. Moreira, A. Ahmed, R. Rifki, B. E. Grantham, D. Bittle, and J. Brunsch, "On the degradation of MEMS gyroscope performance in the presence of high power acoustic noise," in *IEEE Intl. Symp. on Industrial Electronics*, 2007.

[12] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," *In Proceedings of the 24th USENIX Conference on Security Symposium*, USENIX Association, pp. 881-896, 2015.

[13] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, 4(2), pp. 78-87, 2022.

[14] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617-636, 2014.

[15] S. M. Cho, E. Hong, and S. H. Seo, "Random Number Gererator Using Sensors for Drone," *IEEE Access*, Vol.8, pp.30343-30354, 2020.

[16] J. Won, S. H. Seo, and Bertino, "A Secure Communication Protocol for Drones and Smart Objects," *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '15, Singapore, April 14-17, 2015.

[17] K. G. Paterson, "A comparison between traditional public key infrastructures and Identity-based Cryptography," *Information Security Technical Report*, vol. 8, no. 3, pp. 57-72, 2003.

[18] J. Won, S. H. Seo, and E. Bertino, "Certificateless Cryptographic Protocols for Efficient Drone-Based Smart City Applications," *IEEE Access*, vol. 5, pp. 3721-3749, 2017.

[19] I. Avdonin, M. Budko, M. Budko, V. Grozov, and A. Guirik, "A method of creating perfectly secure data transmission channel between unmanned aerial vehicle and ground control station based on One-Time pads," in *Proc. 9th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, pp. 410-413, 2017.

[20] D. J. Bernstein, "Chacha, a variant of salsa20," *in Workshop Record of SASC*, vol. 8, pp. 3-5, 2008..

[21] A. Allouch, O. Cheikhrouhou, A. Koubaa, M. Khalgui, and T. Abbes, "MAVSec: Securing the MAVLink protocol for ardupilot/PX4 unmanned aerial systems," *arXiv:1905.00265*. [Online]. Available: http://arxiv.org/abs/1905.00265, 2019.

[22] S. H. Seo, J. Won, E. Bertino, Y. Kang, and D. Choi, "A Security Framework for a Drone Delivery Service," *in Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*, ser. DroNet '16. ACM, pp. 29-34, 2016.

[23] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. OHanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development portable GPS civilian spoofer," *Proceedings of the ION GNSS Meeting*. Institute of Navigation, Savannah, GA, pp. 2314-2325, 2008.

[24] H. Wen, P. T. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation*, pp. 1285-1290, 2005.

[25] V. Dehghanian, J. Nielsen, and G. Lachapelle, “GNSS spoofing detection based on signal power measurements: statistical analysis,” *Hindawi International Journal of Navigation and Observation*, pp. 1-8. 2012.

[26] A. Jovanovic, C. Botteron, and P.-A. Farine, “Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers,” *in Proc. IEEE/ION Position, Location and Navigation Symposium*, pp. 1258-1271, 2014.

[27] X. Chen, F. Dovis, M. Pini, and P. Mulassano, “Turbo architecture for multipath mitigation in global navigation satellite system receivers,” *IET Radar, Sonar and Navigation*, vol. 5, no. 5, pp. 517-527, 2011.

[28] K. Wesson, M. Rothlisberger, and T. Humphreys, “Practical Cryptographic Civil GPS Signal Authentication,” *journal of the Institute of Navigation*, 59(3), 177-193, 2012.

〈저 자 소 개〉

조 성 민 (Seong-Min Cho)

학생회원

2019년 : 한양대학교 ERICA 캠퍼스 전자공학부 졸업

2019년 3월 ~ 현재 : 한양대학교 전자공학과 석박통합과정

<관심분야> IoT 보안, 임베디드 시스템 보안, 양자내성암호

서 승 현 (Seung-Hyun Seo)

정회원

2000년 : 이화여자대학교 수학과 졸업

2002년 : 이화여자대학교 컴퓨터학과 공학석사

2006년 : 이화여자대학교 컴퓨터학과 공학박사

2006년 12월~2010년 1월 : 금융보안연구원 주임연구원

2010년 2월~2012년 2월 : 한국인터넷진흥원 선임연구원

2012년 2월~2014년 5월 : 미국 퍼듀대학교 컴퓨터학과 박사후연구원

2014년 6월~2015년 2월 : 고려대학교 정보보호대학원 BK21+ 사업단 연구교수

2015년 3월~2017년 2월 : 고려대학교 세종캠퍼스 수학과 조교수

2017년 3월~현재 : 한양대학교 ERICA 캠퍼스 전자공학부 교수

<관심분야> 암호프로토콜, 암호이론, IoT 보안, 블록체인 보안, 악성 코드 분석