Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.1, Feb. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.1.103

DUML 패킷 분석을 통한 드론 비행기록 포렌식 시스템*

윤 여 훈,[1†] 윤 주 범[2‡]
[1,2]세종대학교 (대학원생, 교수)

Drone Flight Record Forensic System through DUML Packet Analysis*

YeoHoon Yoon,[1†] Joobeom Yun[2‡]
[1,2]Sejong University (Graduate student, Professor)

요 약

드론 범죄가 지속적으로 증가하고 있는 상황에서 드론에 대한 사고 예방 및 대응을 위한 드론 포렌식 연구가 매우 중요해지고 있다. 불법적인 범죄 행위를 수사하기 위해서는 드론 내부 저장소에 생성되는 비행기록 파일에 대한 포렌식 분석이 필수적이다. 하지만 독점 DUML 프로토콜로 생성되는 비행기록 파일을 분석하기 위해서는 프로토콜의 구조와 특징에 대한 개념이 반드시 필요하며 암호화되는 Payload에 대응하고 다양한 드론 모델에 대한 분석이 가능한 포렌식 분석 도구가 필요하다. 따라서 본 연구를 통해 먼저 드론에서 생성되는 비행기록 파일의 획득 방법과 특징을 제시하고 비행기록 파일을 이루고 있는 구조와 DUML 패킷의 특징을 설명한다. 최종적으로 제시한 DUML 패킷의 구조에 따른 포렌식 분석을 수행하고 기존 도구보다 범용적으로 동작하며 확장된 구문 분석을 수행하는 확장 포렌식 분석 시스템을 제안한다.

ABSTRACT

In a situation where drone-related crimes continue to rise, research in drone forensics becomes crucial for preventing and responding to incidents involving drones. Conducting forensic analysis on flight record files stored internally is essential for investigating illegal activities. However, analyzing flight record files generated through the exclusive DUML protocol requires a deep understanding of the protocol's structure and characteristics. Additionally, a forensic analysis tool capable of handling cryptographic payloads and analyzing various drone models is imperative. Therefore, this study presents the methods and characteristics of flight record files generated by drones. It also explains the structure of the flight record file and the features of the DUML packet. Ultimately, we conduct forensic analysis based on the presented structure of the DUML packet and propose an extension forensic analysis system that operates more universally than existing tools, performing expanded syntactic analysis.

Keywords: Drone Forensic, DJI, Drone, Parse Flight Log, Flight Log

I. 서 론

현대 사회에서의 드론 활용도는 농업, 촬영, 군과 같은 다양한 산업에서 급격하게 증가하고 있다. 마찬가지로 드론을 이용한 불법 범죄 또한 증가하고 있는 추세이며 미국 연방 항공처[1]는 2022년 1811건의 불법 사용 통계를 발표하였으며 이에 따라 드론 포렌식의 중요성이 증대되는 상황이다.

한편, DJI(Da-Jiang Innovations)는 세계적으로 80% 이상의 점유율을 가지고 있으며 높은 인기를 끄는 드론 브랜드 중 하나로, 범죄에 매우 많이 사용된다. 따라서 DJI 드론을 사용한 범죄를 예방하

Received(12. 01. 2023), Modified(01. 04. 2024), Accepted(01. 04. 2024)
* 본 연구는 한국연구재단 연구과제(NRF-2021R1F1A1051251) 지원으로 수행됨
† 주저자, yeohoon1991@naver.com
‡ 교신저자, jbyun@sejong.ac.kr(Corresponding author)

고 대응하기 위해서는 각각 드론이 기록하는 비행기록 파일에 대한 포렌식 분석이 매우 중요하다. 하지만 이러한 DJI 드론들은 DUML(DJI Universal Markup Language)이란 독점 프로토콜 구조를 띄는 패킷들로 비행기록 파일을 구성하고 있으며, 자사의 기술을 공개하지 않고 있기 때문에 포렌식 분석에 어려움이 존재한다. 이를 위해 DJI와 협약하여 비행기록 파일을 분석해주는 Phantomhelp[2], AirData[3]와 같은 분석 사이트와 DatCon[4], DROP(DRone Open source Parser)[5]과 같은 비행기록 파일의 구문을 분석하는 도구들이 존재한다. 하지만 충분한 정보가 제공되지 않거나 다양한 드론 모델에 대한 범용적인 구문 분석을 지원하지 않는 등의 한계가 존재한다. 특히, DROP은 DatCon의 역공학을 통해 DUML 프로토콜 구조를 알아내고 이에 맞는 구문 분석 도구를 제시하였지만 현재는 사용되지 않는 DatCon 2.3.1 버전을 통해 분석되었기 때문에 잘못된 구문 분석을 수행하여 포렌식 분석에 큰 문제점으로 야기될 수 있다.

따라서 본 연구를 통해 먼저 드론 모델별 비행기록 파일 저장소에 따른 획득 방법과 그 특징을 제시한 뒤, 23년 3월 출시한 DatCon 4.3.0을 분석하여 얻은 올바른 DUML 패킷 구조와 특징을 제시한다. 아울러 기존 도구들의 한계점들을 개선하여 개발된 드론 비행기록 확장 분석 시스템 (Flight Log Extension Parsing System)을 제안한다.

본 논문은 총 5장으로 구성되며, 2장에서는 DJI 드론 포렌식과 관련된 연구를 서술하고 3장은 FLEPS의 개요 및 비행기록 파일 분석 결과를 제시한다. 이어, 4장을 통해 제안하는 확장 비행기록 분석 시스템의 구현과 실험을 서술 후, 5장의 결론을 통해 본 논문을 정리하고 끝맺는다.

II. 관련연구

과거부터 현재까지 불법적 행위에 대해 DJI 드론이 사용됨에 따라 DJI 드론에 대한 포렌식 연구들이 속속히 등장하고 있다[6]. 이러한 연구에는 드론 아티팩트 획득과 분석에 관한 연구, 드론 포렌식 프레임워크 분석 혹은 포렌식 도구의 제안이나 평가 등의 연구가 존재한다.

DJI 드론에는 팬텀, 매빅, 미니, 에어 시리즈 등이 존재하며 시리즈별로 카메라, 성능, 기능에 따라 Standard, Advanced, Professional 등의 모델이 존재한다[7]. 이영우 등[8]은 팬텀3, 미니1, 미니2 드론에서의 드론 저장소에 따른 획득 가능 아티팩트를 제시하고 각 아티팩트의 포렌식 분석 결과를 제시하였다. 이러한 포렌식 아티팩트에는 사진, 동영상 등과 비행 경로, 드론의 상태 등의 센서 데이터가 기록된 비행기록 파일, 개인을 식별할 수 있는 PII(Personally Identifiable Information) 데이터가 존재한다. 하지만 드론은 제조 업체와 모델마다 상이한 특징을 갖고 있기 때문에 Al-Dhaqm 등[9]은 총 4단계로 구성된 포괄적인 드론 포렌식 조사 프레임워크를 제안하였다. 한편 Roder 등[10]과 Iqbal 등[11] 또한 Phantom3와 4 드론에서의 저장소에 따른 아티팩트 획득과 분석을 제시하였으며, 이와 마찬가지로 [12-16]의 연구들에서 Spark, Matrice210, Mini2, Air1, 2 모델에서의 포렌식을 수행하여 모델별 아티팩트 획득 정보를 제시한다.

포렌식 아티팩트 중 하나인 비행기록 파일은 드론의 행위 추적이 가능한 중요한 아티팩트이지만 DJI 자사만의 독점 프로토콜 구조로 이루어져 있어 분석에 한계가 존재한다. 이러한 비행기록 파일 분석 도구에는 대표적으로 DROP, 확장 DROP, DatCon, Autopsy[17] 등이 존재한다. Kumar 등[18]의 저자는 DatCon과 Autopsy를 사용한 비행기록 추출과 시각적 분석의 중요성을 언급하였으며,[13]의 연구를 통해서도 Cellebrite, Autopsy, DatCon 도구를 사용한 시각적 포렌식 분석 결과와 그 중요성을 제시하였다. 특히 [5]의 연구에서는 DatCon을 역공학하여 DJI 드론이 생성한 비행기록 파일을 구성하는 DUML 패킷의 구조를 분석하고 그 특징을 제시하였고 비행기록 포렌식 분석 도구인 DROP을 제안하였다. 하지만 DROP은 현재는 사용되지 않는 DatCon 2.3.1 버전을 분석하여 개발되었기 때문에 잘못된 DUML 구조로 분석을 수행하고 있으며, 그 특징 또한 변경되었다. 또한 Phantom3 모델에서만 테스트가 진행되었기 때문에 보완이 필요하다. 이를 보완하기 위해 Latzo 등[19]의 연구에서 Inspire2, Phantom4 Adv, Matrice600 Pro 드론을 추가적으로 테스트하여 개발한 DROP Extension을 제안하였다. 하지만 Phantom3의 비행기록 파일에 대해서 잘못된 분석을 수행하는 기존 DROP의 문제점을 그대로 갖고 있으며, 범용적이지 못하다는 한계가 존재한다. 대표적인 DJI 비행기록 분석 도구인 DatCon은 기존 도구보다는 많은 드론 모델에서의 분석을 지원하여

Phantom3, Inspire1, Inspire2, Mavic Pro, Phantom4, Phantom4 Pro, Matrice100, Matrice600으로 총 8종류를 지원한다. 하지만 비행기록 파일 내용 중 분석하지 못하는 정보가 많아 자세한 분석에 한계가 있다.

따라서 먼저 본 연구를 통해서 20종의 드론 모델별 비행기록 파일 저장소에 따른 획득과 특징을 분류한다. 이후, 16종의 드론 모델을 테스트하여 기존의 분석 도구에서는 지원하지 않는 DUML 패킷에 대한 분석과 올바른 DUML 구조가 반영된 확장 비행기록 분석 시스템인 FLEPS를 제안한다.

III. 드론 비행기록 포렌식 시스템(FLEPS)

본 장에서는 비행기록 파일의 분석을 통해 본 연구에서 제안하는 FLEPS의 구성도와 동작 원리를 설명한다. 또한 드론별 비행기록 파일은 미국 국립표준 기술 연구원의 드론 포렌식 프로젝트인 VTOLabs[20]에서 제공하는 드론 포렌식 이미지 데이터 셋과 드론 포렌식 논문을 참조하여 분석되었다.

3.1 시스템 구성도

Fig 1은 FLEPS의 구성도이며 대표적으로 3가지 모듈로 동작한다. 우선 Verification Module을 통해 입력 검사를 수행한다. DJI 비행기록 파일이 아닌 경우 사용자에게 오류를 보고하고, 정상적인 비행기록 파일인 경우 파일 헤더를 통해 파일 버전에 따른 구문 분석 동작 준비를 한다. 이후, DUML 패킷의 탐색을 진행하며 동시에 체크섬 검사를 통해 오류 패킷의 필터링과 사용자에게 보고한다. 정상적으로 추출된 DUML 패킷의 구문 분석을 수행하기 전, 패킷 헤더를 참조하여 전처리 과정을 진행하는데 이를 Preprocessing Module에서 수행한다. 프로토콜에 맞게 바이트 단위로 의미를 초기화한다. 또한 패킷 Payload의 복호화를 진행하면 구문 분석을 위한 전처리 과정이 완료된다. 이후 Payload를 바이트 단위로 구문 분석을 수행하며 분석이 완료되면 해당 데이터를 CSV 파일에 기록한다. 그 후, 다음 DUML 패킷을 추출하기 위해 Extract Packet 단계로 돌아가서 상기 과정을 파일의 끝까지 반복 수행한다. 자세한 DUML 패킷의 분석 방법은 3.4에서 설명한다.

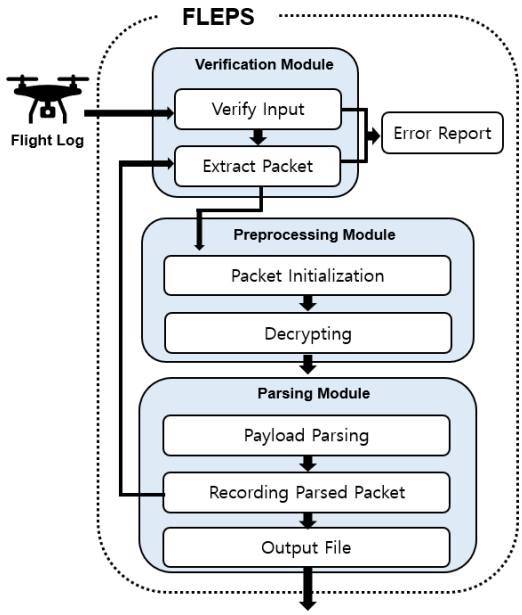


Fig. 1. System Overview

3.2 저장소별 비행기록 특징 분류

일반적으로 비행기록 파일은 드론의 내부 저장소에 존재한다. 내부 저장소는 드론을 분해하면 SD 카드 형태로 존재하거나 드론의 펌웨어를 저장하는 플래시 메모리 칩 형태로 존재한다. 이때 드론 모델에 따라 내부 저장소의 특징과 비행기록 파일 획득 경로가 상이하기 때문에 상황에 맞는 획득 절차를 적용해야 한다. Table 1은 드론 모델별 비행기록 파일의 저장 위치에 따른 유형 분류이다. Type 1, 2는 드론 내부 저장소에 플래시 메모리와 SD 카드가 모두 존재하지만 비행기록 파일 획득 경로의 차이점이 존재한다. Type1은 드론을 분해하여 SD 카드를 추출 후, 디스크 이미징을 수행하여 파일을 획득할 수 있다. 본 연구에선 디스크 이미징 도구로 FTK Imager[21]를 사용하였다. Type3는 드론 내부 저장소에 SD 카드가 따로 존재하지 않고 플래시 메모리만 존재하는 경우이다. 따라서 플래시 메모리를 Chip-off 방법으로 추출하고 메모리 이미지 덤프를 통해 바이너리 파일을 얻은 뒤, 해당 펌웨어 바이너리 파일에서 파일 시스템을 식별하고 비행기록 파일을 추출한다[22]. 바이너리 파일을 획득하기 위해선 하드웨어 전문 지식이 필요하며 [20]의 드론 플래시 메모리의 바이너리 파일을 이용하여 비행기록 파일 추출하였다. 획득한 바이너리 파일로부터의 파일 시

Table 1. Type classification according to storage of Flight log file

Type	Description	Drone Model
Type Ⅰ	Flight Log files exist on MicroSD card	Inspire1 Inspire2 Mavic Pro Matrice210 Agras MG-1S Phantom3 Standard Phantom4 Standard Phantom4 Advanced Phantom4 Professional Phantom4 Professional V2.0 Matrice600 Matrice600 Pro
Type Ⅱ	Media Data exist in MicroSD card and Flight Log files exist on Flash memory	Mavic Air Mavic2 Pro Mavic2 Enterprise Mavic2 Zoom
Type Ⅲ	There is no MicroSD card and Flight log files exist on Flash memory	Spark Mini2 Mavic Air2 Mini3 Pro

스템 식별 및 추출 도구로는 binwalk[23]를 사용하였다. Type2는 Type3와 마찬가지로 플래시 메모리에 비행기록 파일이 존재하여 Type3 절차와 동일하게 비행기록 파일을 획득할 수 있다. 다만 기존의 내부 Micro SD 카드에는 비행기록 파일 대신 사진과 동영상과 같은 미디어 데이터가 존재하였다.

3가지의 Type을 드론의 출시 연월로 미루어 보았을 때, Type 1은 2018년 이전 모델이였으며 Type 2는 2018년~2019년 사이의 모델, Type 3는 Spark를 제외한, 2019년 이후에 출시된 모델이였다. 따라서 DJI의 비행기록 파일 저장 정책이 Type1에서 2로 변경되고 최근에는 3으로 변경되고 있음을 추정할 수 있다.

3.3 비행기록 파일 구조 분석

기존의 Phantom3 드론에서의 비행기록 파일 구조를 분석한 결과를 [5]에서 제시하고 있다. 하지만 드론 모델별로 비행기록 파일 구조는 상이한데, 비행기록 파일의 구문 분석을 위해서라면 파일 구조를 파악해야 한다. 따라서 본 연구를 통해 기존의 구문 분석 도구인 DatCon과 앞서 획득한 비행기록 파일을 분석하여 구조와 특징들을 제시하였다.

DJI 비행기록 파일은 파일 헤더 특징을 기반으로 DatV1과 DatV3로 분류된다. Table 1을 참조하였을 때, 비행기록 파일을 획득하지 못한 Mavic Air1,2와 Mini3 Pro를 제외하고는 DatV1에는 Inspire1, Phantom3 드론이 속하였고 그 외의 드론 모델들은 모두 DatV3에 속하였다. 각각의 비행기록 파일 구조는 Fig 2와 같으며 헤더 길이가 DatV1은 128Bytes, DatV3는 256Bytes를 가진다. 또한 파일 헤더의 첫 바이트는 드론 모델명을 식별하는 값으로써, 예를 들어 첫 바이트가 0x19면 Matrice210 모델, 0x11은 Inspire2 모델을 의미한다. 이후 공통적으로 파일 헤더의 0x10 위치부터 5Bytes 길이의 “BUILD” 문자열이 존재하는 특징이 있다. 하지만 DatV1은 0x80 위치부터 DUML 패킷이 등장하기 시작하며 DatV3는 0xF2 위치부터 “DJI_LOG_V3” 문자열이 있는 특징과 함께 0x100 위치부터 DUML 패킷이 등장한다. 이후 GPS, Motor, 드론 상태 등의 비행기록 정보가

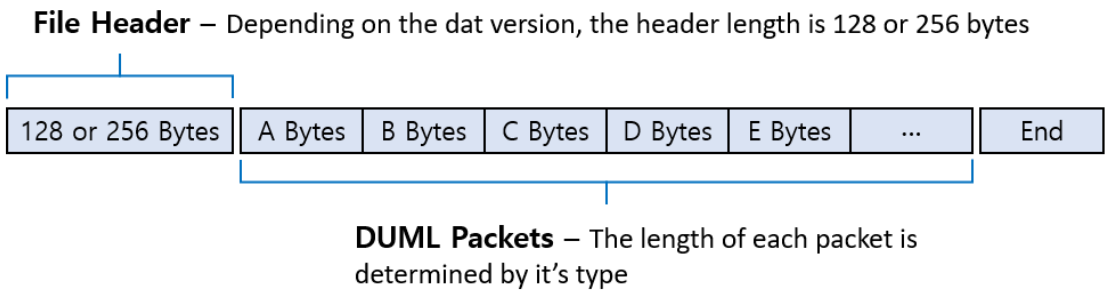


Fig. 2. Basic Structure of Flight Log File

DUML 패킷으로 파일에 기록되어 있으며, 마지막 패킷이 기록된 이후의 파일의 끝에는 3가지 특징을 보이며 비행기록 파일이 끝난다. 3가지 특징의 첫 번째는 파일의 끝이 마지막으로 저장된 DUML 패킷으로 종료되어 끝나는 경우와 두 번째는 다수의 0x00 값으로 종료되는 경우, 마지막 세 번째는 다수의 0xFF 값으로 종료되는 경우이다.

3.4 FLEPS를 활용한 DUML 패킷 분석

DJI 드론은 DUML 프로토콜이란 독점 프로토콜을 사용하여 설정 정보, 조종기, 기체 내부 모듈 간 데이터 송수신 등의 기능에 활용된다[24-26]. 드론 비행기록 파일에 기록된 DUML 패킷들은 비행기록 파일의 헤더와 파일의 끝 부분 사이에 존재하며 그 개수 또한 비행기록 버전과 파일 크기에 따라 차이가 있다. 이러한 DUML 패킷들의 분석을 통해 날짜, 시간, 위도, 경도 등의 GPS 정보나 속도와 모터 등의 센서 정보를 얻을 수 있다.

DUML 패킷의 구조는 Fig 3와 같다. DUML 패킷 헤더는 10Bytes의 길이를 가지고 있으며, 해당 DUML 패킷의 기본적인 정보를 가지고 있다. 따라서 FLEPS는 Header에 기록된 정보를 우선 탐색하여 초기화 과정을 선행함으로써 Payload의 구문 분석 수행 전 전처리 과정을 시작한다. 헤더의 1Byte 길이의 첫 번째 필드는 DUML 패킷의 시작을 알리는 식별자인 0x55 시그니처 값으로 시작하며 고정된 값이다. 이후 2번째 필드는 패킷의 전체 길이를 1Byte로 표현하는 Length 필드이다. 따라서 패킷 시그니처 위치부터 패킷 길이만큼 뒤에는 다음 DUML 패킷의 시그니처 식별자 필드가 나타나게 된다. 이후 3번째 필드는 0x00의 고정 값을 가지는 프로토콜 버전 필드와 4번째로 1~3번째 필드의 체크 값을 의미하는 CRC8 필드가 뒤따른다. 5번째 필드는 2Bytes 길이의 Log entry type으로 해당 패킷이 의미하는 데이터 종류를 식별하는 필드이다. 예시로, Fig 3은 IMU(Inertial Measurement Unit) 센서 데이터에 관한 DUML 패킷을 표현한 것이며, IMU 센서 데이터의 패킷 타입은 0x0800를 가지며 이때의 Payload는 IMU 센서가 측정한 값이 기록되어 있다. 또한 패킷의 전체 길이는 0x84인 132Bytes를 가지며 이때의 Payload는 IMU 센서가 측정한 값이 기록되어 있다. 또한 패킷의 전체 길이는 0x84인 132Bytes를 가지며 이때의

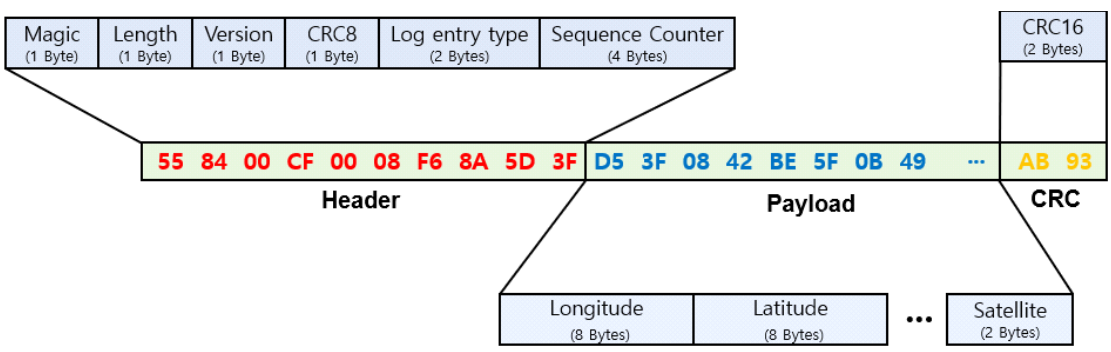


Fig. 3. Structure of DUML Packet

Payload 길이는 132Bytes에서 헤더 10Bytes와 마지막 CRC16 필드 2Bytes 길이를 뺀 120Bytes 길이를 가지게 된다. Payload는 특정 바이트 단위로 데이터 값을 표현하는데, IMU 패킷인 경우 첫 8Bytes는 경도, 다음 8Bytes는 위도를 의미하며 마찬가지로 나머지 Payload 또한 특정 바이트 단위로 그 의미를 갖고 있기 때문에 패킷 분석 시 패킷 타입을 식별하는 것이 중요하다. 아울러 동일한 패킷 타입에 대하여 드론 모델마다 상이한 Payload 길이를 가지고 있다. Fig 4을 보면, 동일한 Battery Info(0x06AE) 타입에 대한 Payload의 길이가 Phantom4 Pro 모델은 44Bytes의 길이를 가지고 있고, Mavic2 Enterprise 모델에선 109Bytes의 길이를 가지고 있다. 이때 Battery Temperature와 같은 동일한 의미를 지닌 각 바이트 위치가 달라지기 때문에 Payload 길이에 따른 구문 분석도 달라져야만 한다. 일반적으로 동일한 패킷 타입에 Payload의 길이가 길수록 자세하고 많은 정보를 담는다. 이처럼 비행기록 파일 내의 DUML 패킷을 분석할 시에는 각 패킷의 타입을 식별하고 Payload의 길이에 따른 상이한 분석을 적용하는 점이 매우 중요하며 Table 2는 DUML 패킷 중 대표적으로 5가지 패킷에 대한 주요 필드 정보와 페이로드 위치를 보인다.

하지만 각각의 DUML 패킷의 Payload 영역은 기본적으로 암호화가 되어 있기 때문에 패킷 타입을 식별한 뒤, Payload의 분석을 수행하기 전 복호화 과정이 선행되어야만 한다. 복호화 방식을 분석해본 결과, 기존 [5]의 연구에서 제시한 DatV1의 복호화 방식이 DatV3에서도 변경되지 않았다. DatV3의 DUML 패킷의 복호화 계산은 기존과 마찬가지로 패킷 헤더의 4바이트 길이를 갖는 6번째 필드인 Sequence Counter 값이 키 계산에 사용된다. 복호화 키는 Sequence Counter 값의 mod 256 연산을 통해 구할 수 있으며 Payload의 각 바이트는 키와 xor 연산하여 복호화가 가능하다. 또한 이때의 Sequence Counter 값은 드론 Internal Bus Clock이며 같은 값을 지니는 다양한 DUML 패킷에 대한 분석의 기준에 사용된다. 이를 활용하여 동일한 Sequence Counter 값을 지닌 DUML 패킷들은 동일한 시점으로 구분하여 구문 분석에 사용된다.

IV. 구현 및 실험

본 장에서는 제시하고자 하는 확장 비행기록 분석 시스템의 Framework 구현을 설명하고, 비행기록 파일의 분석을 위해서 드론별 DUML 패킷 추출 실험을 4.2에서, 범용적인 드론 모델에 대응하기 위한 드론 모델 확장을 4.3에서, 자세한 구문 분석을 위한 분석 도구간 성능 비교를 4.4에서 설명한다.

4.1 프레임워크 구현

FLEPS, Flight Log Extension Parsing System은 다양한 라이브러리를 사용할 수 있는 Python 3.11을 이용하여 개발된 포렌식 시스템이다. 기존의 오픈 소스 포렌식 프로젝트를 FLEPS에

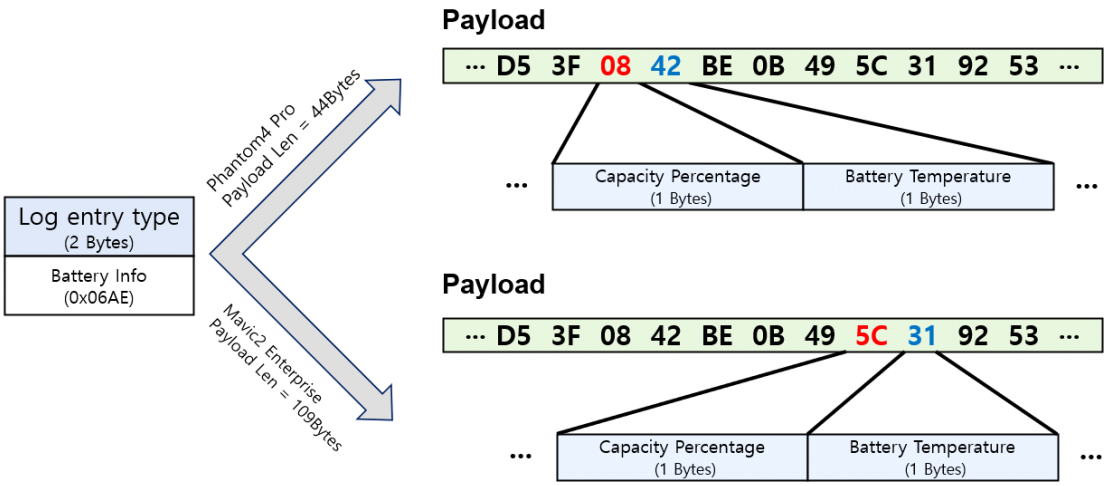


Fig. 4. Parsing Differences by Payload Length

Table 2. Example of Packet Payload Field

Packet Info	Packet Type	Length (Bytes)	Payload Field	
Battery	0x06AE	60	Remaining Time	[2:4]
			Remaining Capacity	[20:22]
			Capacity Percentage	[22:23]
			Battery Temperature	[23:25]
GPS	0x0830	68	Date	[0:4]
			Time	[4:8]
			Longitude	[8:12]
			Latitude	[12:16]
RC GPS	0x276E	30	Hour	[0:1]
			Min	[1:2]
			Sec	[2:3]
			Year	[3:5]
			Month	[5:6]
			Day	[6:7]
			RC Longitude	[7:11]
			RC Latitude	[11:15]
IMU	0x0800	120	Longitude	[0:8]
			Latitude	[8:16]
			Altitude	[44:48]
			IMU Temperature	[106:108]
Motor	0x276A	184	RightFront Speed	[3:5]
			LeftFront Speed	[26:28]
			LeftBack Speed	[49:51]
			RightBack Speed	[72:74]

통합함으로써 Framework를 구성할 수 있었다. 또한, 우리는 비행기록 파일을 분석하기에 앞서, 정확한 분석을 위해 DatCon[4]과 DROP[5]을 사용하여 비행기록 파일 및 패킷 검증 단계를 구현했다. 또한 범용적인 드론 모델에 대응되고 자세한 패킷 타입 분석을 위해서 Dissector[24]를 통합함으로써 확장 비행기록 구문 분석 시스템을 구현하였다.

4.2 비행기록 파일 내 DUML 패킷 추출

비행기록 파일의 구문 분석을 수행하기 위하여 앞서 획득에 성공한 16종의 드론 모델이 기록하는 비행기록 파일에서 DUML 패킷을 추출하고 발견된 패킷 타입 유형을 분석하였다. Table 3는 각 드론이 생성하는 비행기록 파일 중 하나를 임의로 선택하여 분석하였으며 파일을 구성하는 DUML 패킷의 총 개수와 발견된 패킷 타입 유형의 총 개수를 파일 크기 별로 분류하였다. 비행기록 파일의 크기는 드론의 비행 시간에 따라 상이하기 때문에 최저 19MB의 크기부터 최고 268MB의 크기를 갖는 비행기록 파일을 분석에 사용하였다.

우선 Phantom3에서의 66.5MB 크기의 비행기록 파일에서 발견된 총 패킷 타입 유형은 37가지 종류가 발견되었다. 이때의 비행기록 파일을 구성하는 총 DUML 패킷은 약 117만 개였다. 같은 DatV1인 Inspire1의 비행기록 파일은 153MB 크기에서 40가지 종류의 패킷 타입이 발견되었고 약 260만 개의 패킷으로 구성되었다. 이로써 DatV1은 평균적으로 약 39가지의 종류로 구성된 DUML 패킷이 1MB 당 약 17,000개의 패킷으로 이루어진 것을 알 수 있다. 이외의 비행기록 파일은 모두 DatV3이며 모델별로 결과가 다양하기 때문에 시리즈별로 분석할

Table 3. Analysis of DUML Packets by Model

Drone Model	File Size (MB)	Number of Found Packet Types	Total Number of Packets
Phantom3 Std	66.5	37	1,175,964
Phantom4 Std	257	87	10,137,149
Phantom4 Adv	22.9	83	431,519
Phantom4 Pro	87.8	83	1,684,312
Phantom4 Pro+	140	116	2,875,814
Inspire1	153	40	2,613,418
Inspire2	234	100	7,963,585
Spark	219	70	2,509,357
Mavic Pro	64.6	100	1,708,145
Agras MG-1S	268	67	5,942,842
Matrice210	252	112	7,615,049
Matrice600 Pro	81.3	116	1,442,474
Mavic2 Pro	67.4	86	1,093,323
Mavic2 Zoom	36.7	85	607,292
Mavic2 Enterprise	49.1	73	928,629
Mini2	19	41	271,254

필요가 있다. 우선 Phantom4 시리즈는 83~116가지의 패킷 타입이 발견되었으며 그 중 Standard 모델은 다른 모델에 비해 매우 많은 DUML 패킷이 발견되었고 평균적으로 1MB 당 약 3만개의 패킷으로 이루어졌다. Mavic2 시리즈는 73~86가지 종류의 패킷 타입으로 이루어졌고 1MB 당 약 17,000개의 패킷으로 이루어졌다. 그 외의 드론 모델들은 최소 41가지의 패킷 타입부터 최대 116가지까지 발견되었으며 1MB 당 약 22,000개의 패킷으로 이루어졌다. 이렇듯 드론 모델마다 발견되는 패킷 타입과 평균적으로 기록되는 패킷 개수가 다르다. 이때 자세한 분석을 위해서라면 발견된 DUML 패킷 타입에 대해 충분한 분석을 지원할 필요가 있다.

4.3 드론 분석 모델 확장

현재 알려진 DJI 비행기록 분석 도구는 DROP, 확장 DROP, DatCon 등이 있다. 하지만 각 도구는 2장. 관련 연구에서 언급한 일부 드론 모델에서만 테스트가 되었기 때문에 범용적이지 못하다는 한계가 있다. 따라서 본 장에서 기존 도구에서 지원하는 드론 모델외의 비행기록 파일에서 DUML 패킷을 추출하고 동일한 복호화 방식을 적용하여 분석한 결과가 올바른 결과를 출력하는지 검증을 통해 드론 모델의 확장을 꾀하였다. 예를 들어 기존 분석 방식을 적용한 결과가 이상하거나 불일치하는 정보가 출력된다면 이는 기존의 복호화 방식이 적용되지 않음을 추정할 수 있다. 따라서 본 실험은 추가적인 8가지 모델에 대한 출력된 분석 결과 중 GPS 좌표 정보나 시간 정보가 일치하는지 확인을 통해 검증하였다.

Table 4는 추가적인 8가지 모델에 대한 분석, 검증을 시도한 결과이다. 분석에 사용된 드론은 Spark, Matrice210, MG-1S, Phantom4 Pro+(2.0), Mavic2 시리즈, Mini2이다. 결과적으로 Mini2 드론을 제외한 7가지 드론 모델의 비행기록 분석 결과는 Fig 5, 6과 같이 정상적으로

Table 4. Verification of Flight Log

Drone Model	Verification
Spark	○
Matrice210	○
Agras MG-1S	○
Phantom4 Professional+	○
Mavic2 Zoom	○
Mavic2 Pro	○
Mavic2 Enterprise	○
Mini2	×

Fig. 5. Phantom4 Pro+ Flight Trajectory

GPS 좌표와 시간 정보가 출력되었다. 하지만 Mini2 드론만은 Fig 7과 같이 이상한 좌표 정보와 시간 정보가 기록되어 있는 것을 확인할 수 있다. 그럼에도 Mini2 비행기록 파일에서도 기존 DUML 패킷이 발견되는 것을 미루어보아, Payload의 암호화 방식이 기존 드론과 다르다고 추정하고 있으며, Mini2 이후에 출시되는 드론 모델들 또한 이와 마찬가지로 기존과 다른 복호화 방식이 적용되어야 비행기록 파일 분석이 가능하다고 판단된다.

4.4 비행기록 분석 도구 간 성능 비교

앞서 실험에서 드론 모델별로 DUML 패킷의 추출과 분석을 통해 비행기록 파일에 기록된 패킷의 평균 개수와 해당 파일을 구성하고 있는 패킷 타입의 총 개수를 파악하였다. 본 장에서는 발견된 패킷 타입에 대하여 기존 분석 도구들과 본 연구에서 제시하는 확장 비행기록 분석 시스템(FLEPS) 간의 성능을 비교한다. 따라서 도구 간에 비행기록 파일에서 발견된 패킷 타입의 분석 수행 정도를 비교하였다.

Table 5는 비행기록 분석 도구 간의 성능 비교 결과이다. 우선 Number of Packet Types는 비행기록 파일을 구성하고 있는 DUML 패킷 타입의 총 개수이다. 하지만 이렇게 발견된 패킷 타입에 대하여 도구별로 분석을 지원하는 패킷 타입 유형이 다르기 때문에 자세하고 정확한 포렌식 분석을 위해서라면 더 많은 패킷 타입 유형에 대한 분석이 필요하다. 이를 Parsed Packet Types에서 제시한다. 분석 결과 중 ×는 해당 도구에서 지원하지 않는 드론 모델을 의미하고 비행기록 파일을 구성하는 패킷 타입 중 분석을 지원하는 패킷 타입의 총 개수를 도구별로 보여준다. 예를 들어, Phantom4 Adv 드론에서 발견된 패킷 타입 유형의 총 개수는 83개이며 그 중 DatCon과 Drop Extension은 32개의 패킷 타입에 대하여 분석을 수행한다. 하지만 본 연구에서 제시하는 도구는 45개의 유형에 대하여 분석을 지원하기 때문에 기존 도구보다 13개 유형에 대한

latitude	longitude	altitude	date	time	imuTemp	roll	pitch	yaw
39.9612	-106.216	2487.549	20180621	21:25:29	64.97	0.889686	-0.86523	-118.352
39.9612	-106.216	2487.549	20180621	21:25:29	64.97	0.889604	-0.86473	-118.352
39.9612	-106.216	2487.549	20180621	21:25:29	64.95	0.889685	-0.8643	-118.352
39.9612	-106.216	2487.549	20180621	21:25:29	64.98	0.888222	-0.86562	-118.354
39.9612	-106.216	2487.549	20180621	21:25:29	64.99	0.888957	-0.86549	-118.354

Fig. 6. Phantom4 Pro+ Flight Log Analysis Result

latitude	longitude	altitude	date	time	imuTemp	roll	pitch	yaw
145.97	-207.987	1803803	3.7E+09	275896:-2	-105.9	1.07E-41	-180	180
145.97	-207.987	1803803	3.7E+09	275896:-2	103.81	-6.28E-43	180	180
145.97	-207.987	1803803	3.7E+09	275896:-2	-291.58	-6.40E-43	180	0.00098
145.97	-207.987	1803803	3.7E+09	275896:-2	54.58	-9.82E-19	-6.30E-10	-1.85E-05
-64.4888	17.6771	-452110	1.4E+09	72121:27:5	54.58	-9.82E-19	-6.30E-10	-1.85E-05
-64.4888	17.6771	-452110	1.4E+09	72121:27:5	-24.46	7.75E-19	180	-180

Fig. 7. Mini2 Flight Log Analysis Result

Table 5. Comparison of Performance between Flight Log Analysis Tools

Drone Model	Number of Packet Types	Parsed Packet Types			
		FLEPS	DatCon	DROP Extension	DROP
Phantom3 Std	35	**11**	11	9	9
Phantom4 Adv	83	**45**	32	32	
Matrice600 Pro	116	**47**	33	28	
Inspire2	100	**44**	30	30	
Inspire1	40	**11**	11		
Phantom4 Std	87	**45**	32		
Phantom4 Pro	83	**45**	32		
Mavic Pro	100	**43**	30		×
Matrice210	112	**45**			
Phantom4 Pro+	116	**45**		×	
MG-1S	67	**25**			
Spark	70	**38**	×		
Mavic2 Pro	86	**37**			
Mavic2 Enterprise	73	**33**			
Mavic2 Zoom	85	**37**			

분석 확장이 가능하다. 이처럼 전체적으로 최대 14개 패킷 타입에 대해 구문 분석을 지원하기 때문에 포렌식 분석에 있어 더 자세한 구문 분석이 가능하다. 이처럼 FLEPS는 분석 확장을 통해 비행기록에 기록되었지만 분석되지 못했던 드론의 에러 정보나 입력 신호, 기타 센서 정보, Barometer와 같은 드론의 FMU(Flight Management Unit) 센서 정보, Fig 8, 9와 같은 조종자의 GPS 좌표와 날짜 및 시간 정보 등을 분석할 수 있다.

Fig. 8. Matrice600 Pro RC GPS

Fig. 9. Inspire2 RC GPS

V. 결 론

본 연구를 통해서 먼저, 드론 모델별로 비행기록 파일 저장소에 따른 3가지 분류를 제시하였다. 각 3가지 분류에 따라 비행기록 파일의 획득 방법과 차이점을 설명하였고 비행기록 파일 저장 정책이 변경되고 있음을 보였다.

이후, DJI의 독점 프로토콜인 DUML 프로토콜에 따라 비행기록 파일이 구성되어지고 있음을 보여주고 동시에 비행기록 파일의 구조와 DUML 패킷의 구조 및 특징을 제시하였다. 또한 DUML 패킷의 Payload 길이에 따른 분석의 차이점을 언급하며 포렌식 분석 시, 이 점을 고려해야 함을 보여준다.

실험을 통해 먼저, 16가지의 드론 모델의 비행기록 파일에서 DUML 패킷을 추출하고 패킷 타입의 개수와 그 특징을 제시하였으며, 자세하고 충분한 포렌식 분석을 위해서라면 더 많은 패킷 타입에 대한 구문 분석이 중요하다. 또한 제시한 포렌식 시스템을 통해 기존 도구들과의 성능 비교를 하여 기존 도구들과 다르게 더 자세한 포렌식 분석이 수행됨을 보였다.

References

[1] FAA, "UAS Sightings Report" https://www.faa.gov/uas/resources/public_records/uas_sightings_report accessed Jan. 2023.

[2] Phantom Help, "Phantom help" https://www.phantomhelp.com/getting-started/, accessed Nov. 2023.

[3] Airdata UAV. "Airdata" https://app.airdata.com/, accessed Sep. 2023.

[4] DatCon Tool. "Datcon/CsvView" https://datfile.net/DatCon/intro.html, accessed Sep. 2023.

[5] Clark, D. R., Meffert, C., Baggili, I., and Breitinger, F. "DROP (DRone Opensource Parser) your drone: Forensic analysis of the DJI Phantom III" Digital Investigation, 22, S3-S14. 2017.

[6] NPR, "drone Russia-Ukraine war" https://www.npr.org/2023/03/21/1164977056/a-chinese-drone-for-hobbyists-plays-a-crucial-role-in-the-russia-ukraine-war accessed Mar. 2023.

[7] DJI, "DJI" https://www.dji.com/kr, accessed Nov. 2023.

[8] Y. Lee, J. Kim, J. Yu and Yun, J.,"Classification of DJI Drones Based on Flight Log Decryption Method",Journal of The Korea Institute of Information Security & Cryptology,32(1), Feb 2022

[9] Al-Dhaqm, Arafat, et al. "Research challenges and opportunities in drone forensics models." Electronics, vol. 10, no. 13, June 2021

[10] Roder, A, et al. "Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study." arXiv preprint arXiv:1804.08649 Apr 2018

[11] Iqbal, F. et al. "Drone forensics: A case study on DJI phantom 4" In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1 - 6 Nov 2019

[12] Kao, Da-Yu, et al. "Drone forensic investigation: DJI spark drone as a case study." Procedia Computer Science Vol.159,pp.1890-1899,Sep 2019

[13] Salamh, F. et al. "UAV forensic analysis and software tools assessment: DJI Phantom 4 and Matrice 210 as case studies." Electronics, Vol 10, no. 6, March 2021

[14] Stanković, M. et al. "UAV forensics: DJI mini 2 case study" Drones, Vol 5, no.2, June 2021

[15] Yousef, M. et al. "Drone forensics: A case study on a DJI Mavic Air." 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). IEEE, pp.1-3, Nov 2021

[16] Lan, James Kin Wah, and Frankie Kin Wah Lee. "Drone Forensics: A Case Study on DJI Mavic Air 2." 2022 24th International Conference on Advanced Communication Technology (ICACT). IEEE, pp. 291-296. Feb 2022.

[17] Autopsy. "Autopsy forensic Tool" https://www.basistech.com/autopsy/, accessed Sep. 2023.

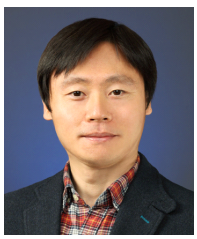
[18] Kumar. R, et al. "Drone GPS data analysis for flight path reconstruction: A study on DJI, Parrot & Yuneec make drones." Forensic Science International: Digital Investigation 38: 301182. Sep 2021

[19] Latzo. T, et al. "Maraudrone's Map: An Interactive Web Application for Forensic Analysis and Visualization of DJI Drone Log Data." Nordic Conference on Secure IT Systems. Cham: Springer International

Publishing, pp. 329-345 Jan 2023
〔20〕 VTO Labs, "VTO Labs Drone" https://www.vtolabs.com/drone-forensics accessed Nov. 2023.
〔21〕 FTK Imager. "FTK Imager forensic" https://www.exterro.com/ftk-imager accessed Jun. 2023.
〔22〕 J. Jeong, et al.,"A Digital Forensic Process for Ext4 File System in the Flash Memory of IoT Devices", Journal of KIISE, 48(8), Aug 2021
〔23〕 github, "binwalk for extract file" https://github.com/ReFirmLabs/binwalk accessed Sep. 2023.
〔24〕 github, "dji-firmware-tools" https://github.com/o-gs/dji-firmware-tools/tree/master/comm_dissector accessd Nov 2023
〔25〕 Schiller, Nico, et al. "Drone Security and the Mysterious Case of DJI's DroneID." Network and Distributed System Security Symposium (NDSS). 2023.
〔26〕 S. Lee, et al. "A Study on Acquiring Data from DJI Drone using DUML Protocols", Journal of Digital Forensics , 17(2), 89-103. Jun 2023

〈저자소개〉

윤 여 훈 (YeoHoon Yoon) 학생회원
2022년 2월: 대전대학교 컴퓨터공학과 졸업
2022년 3월~현재: 세종대학교 일반대학원 정보보호학과, 지능형 드론 융합전공 석사과정
〈관심분야〉 정보보호, 드론 포렌식



윤 주 범 (Joobeom Yun) 종신회원
1999년 2월: 고려대학교 컴퓨터학과 학사
2001년 2월: 서울대학교 컴퓨터공학과 석사
2012년 2월: KAIST 전산학과 박사
2001년 3월~2015년 2월: ETRI부설연구소 선임연구원
2015년 3월~현재: 세종대학교 정보보호학과, 지능형 드론 융합전공 부교수
〈관심분야〉 네트워크 보안, 시스템 보안, 인공지능 보안