OcuSync 드론 통신 시스템 분석

정재연, 남해운*

한양대학교 에리카, *한양대학교

jy1019@hanyang.ac.kr, *hnam@hanyang.ac.kr

Analysis of the OcuSync Drone Communication System

Jaeyeon Jung, Haewoon Nam*

Hanyang Univ.

요 약

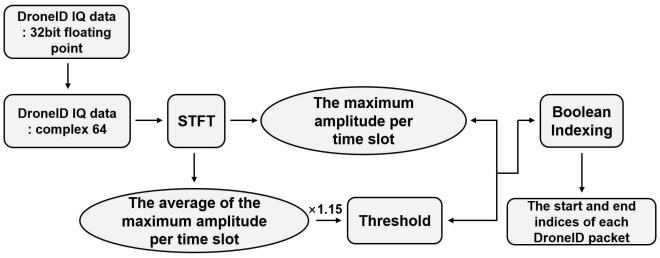
OcuSync 프로토콜을 사용하는 드론 아이디 패킷의 IQ 데이터에서 각 패킷의 시작점과 끝점을 계산하여 패킷을 추출하는 과정은 드론 아이디 패킷을 복조와 디코딩을 하기 이전에 필수적이다. 본 논문은 드론의 다운링크 신호인 드론 아이디 패킷과 업링크 신호인 커맨드 앤 컨드롤 패킷을 포함하는 IQ 데이터에서, Short-Time Fourier Transform (STFT)을 적용하고 타임 슬롯 당 최대 크기 값을 비교함으로써 드론 아이디 패킷 식별 및 식별한 각 드론 아이디 패킷의 시작점과 끝점 인덱스를 추출하는 방법을 제안한다. 시뮬레이션에서는 드론 아이디 패킷과 커맨드 앤 컨트롤 패킷을 가지고 있는 드론 IQ 데이터를 사용하였으며, 이 데이터에 제안한 알고리즘을 적용한 결과 드론 아이디 패킷의 모든 시작점과 끝점 인덱스를 정확하게 추출하였다.

Ⅰ. 서 론

Da-Jiang Innovations (DJI)에서 개발한 OcuSync는 드론과 리모컨 간 원격 제어 및 영상 데이터 전송을 효과적으로 지원하는 전용 통신 프로토콜이다[1]. 드론 아이디 패킷은 드론과 리모컨 간에 교환되는 패킷 중 하나이며, 이는 OcuSync 프로토콜을 사용한다. 드론 아이디 패킷을 복조하고 디코딩함으로써 드론과 원격 조종사의 실시간 위치를 포함한 민감한 정보를 파악할 수 있으며, 이러한 정보를 활용하여 드론을 재밍할 수 있다[2],[3]. 드론 아이디 패킷을 복조하기 위해서는 먼저 Software-Defined Radio (SDR)에서 캡처된 32비트 부동 소수점 드론 IQ 데이터로부터 각 패킷의 시작점과 끝점을 계산하여 패킷을 추출하는 과정이 필요하기에, Short-Time Fourier Transform (STFT)에 기반한 드론 아이디 패킷의 시작점과 끝점 인덱스를 추출하는 알고리즘을 제안한다.

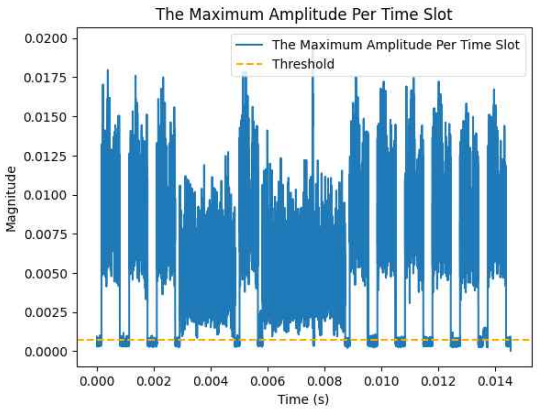
Ⅱ. 드론 아이디 패킷 인덱스 추출 알고리즘

드론 아이디 패킷을 복조와 디코딩하여 정보를 알아내기 이전에 각 패킷의 시작점과 끝점을 계산하여 패킷을 추출하기 위해서는 우선 드론에서 송수신되는 패킷들 사이에서 드론 아이디 패킷을 식별할 필요성이 있다. 패킷은 크게 두 종류로 나뉘며, 리모컨에서 드론으로 송신되는 업링크 신호인 커맨드 앤 컨트롤 패킷과 드론에서 리모컨으로 송신되는 다운링크 신호인 드론 아이디 패킷이 존재한다. 두 패킷은 중심 주파수를 바꿔가며 송신되기 때문에 시간-주파수 관점에서 신호를 관찰하면 드론 아이디 패킷 식별에 용이하다는 이점이 있다. 따라서 본 논문에서는 시간-주파수 슬롯 단위로 주파수 분석이 가능한 STFT에 기반한 드론 아이디 패킷 식별 및 패킷의 시작점과 끝점 인덱스를 추출하는 방법을 제안한다. 전반적인 알고리즘 구성도는 [그림 1]과 같다. 드론 신호의 IQ 데이터에 STFT를 적용하면 신호를 타임 슬롯으로 나누어 각 시간-주파수 슬롯 단위로 주파수 분석이 가능한 행렬을 생성할수 있으며, STFT의 결과 행렬에 절댓값을 취하면 시간-주파수 영역에서의 신호 크기를 관찰할 수 있다. 신

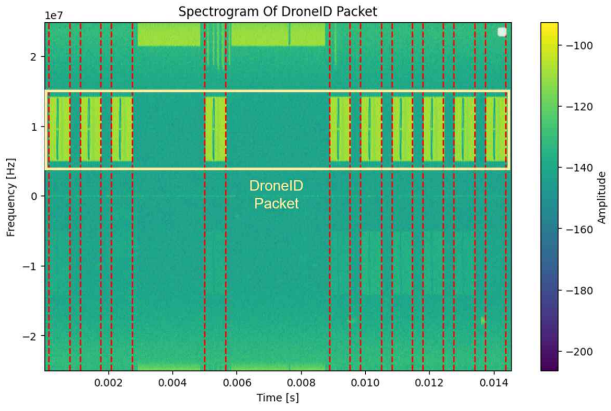


[그림 1] 알고리즘 구성도

호가 없는 시간에서는 상대적으로 낮은 전력을 갖는 반면, 신호가 있는 시간에서는 상대적으로 높은 전력을 갖기 때문에, 이러한 특성을 활용하여 STFT 결과 행렬에서 시간에 따른 신호의 존재 유무를 파악할 수 있다. 신호의 존재 유무를 더 명확하게 확인하기 위해서 절댓값을 취한 행렬의 각 타임 슬롯에서 최대 크기 값을 추출하고, 이 값들을 비교하였다. 각 타임 슬롯에서 추출된 최대 크기 값을 비교하면, 신호가 있는 타임 슬롯과 신호가 없는 타임 슬롯에서의 크기 차이가 더욱 명확하게 드러나기 때문에, 신호의 존재 여부를 잘 파악할 수 있다. 그러나 신호의 정확한 경계를 파악할 수는 없기 때문에, 신호가 있는 타임 슬롯과 없는 타임 슬롯을 판단하기 위한 임계치를 설정하였다. 신호가 없는 타임 슬롯에서는 최대 크기 값들의 평균 값인 노이즈 플로어에 가까운 값을 갖기에 이 값을 임계치로 설정하였다. 그러나 노이즈의 무작위성으로 인해 노이즈 플로어 값이 드론 아이디 패킷의 경계를 정확하게 구분하지 못하는 오류가 발생하여, 임계치를 다른 값으로 수정하였다. 각 타임 슬롯의 최대 크기 값이 추출된 배열에서, 노이즈 플로어에 가까운 값을 가지다가 급격하게 큰 값으로 변환되기 직전의 인덱스에서의 값들을 추출하고, 큰 값을 가지다가 급격하게 노이즈 플로어에 가까운 값으로 변환된 인덱스에서의 값들을 추출하였다. 추출한 값들 사이에서 최대값을 임계치로 설정함으로써 신호와 노이



[그림 2] 각 타임 슬롯에서 추출된 최대 크기 값들과 임계치



[그림 3] 드론 아이디 패킷의 스펙트로그램

즈 플로어 간의 경계를 명확하게 구분하였다. 이에따라. 임계치보다 작은 값을 가지다가 커지는 타임 슬롯이 패킷의 시작점 인덱스, 임계치보다 큰 값을 가지다가 작아지는 타임 슬롯이 패킷의 끝점 인덱스의 후보가 된다. [그림 2]를 통해 각 타임 슬롯에서 추출된 최대 크기 값들과 임계치를 나타낸 그래프를 확인할 수 있다.

설정한 임계치를 기준으로, 각 타임 슬롯의 최대 크기 값을 추출한 배열을 True와 False만으로 이루어진 Boolean 인덱싱 배열로 변환한다. 임계치보다 큰 요소는 True, 작은 요소는 False로 표현하면 신호에 해당하는 인덱스에서는 모두 True로 표시되기 때문에, 신호에 해당하는 인덱스를 식별하기 용이해진다. 그러나 Boolean 인덱싱 배열에서 모든 연속적인 True 집합이 드론 아이디 패킷에 해당하는 것은 아니다. [그림 3]에서 확인할 수 있듯이 드론 아이디 패킷보다 긴 길이를 가지는 커맨드 앤 컨트롤 패킷 또는 임계치를 넘어서는 값을 가진 노이즈에 해당될 수 있기 때문에, 이 세 가지의 경우 중에서 드론 아이디 패킷을 식별할 수 있는 알고리즘이 요구된다. 따라서 배열 내의 연속적인 True 집합 중에서 두 가지 조건을 동시에 만족하는 집합을 드론 아이디 패킷으로 식별하였다. 첫 번째 조건은 연속적인 True 개수가 드론 아이디 패킷의 샘플 개수와 정확히 일치해야 하는 것이며, 이는 드론 아이디 패킷의 길이와 일치하는 신호 집합을 찾기 위한 조건이다. 두 번째 조건은 연속적인 True 집합의 첫 번째 True 직전과 마지막 True 직후의 인덱스에서 모두 False를 가져야 하는 것이며, 이는 첫 번째 조건을 만족하는 신호 집합 중에서 드론 아이디 패킷에 해당하는 인덱스를 식별하기 위한 조건이다. 첫 번째 조건에서 사용되는 드론 아이디 패킷의 샘플 개수는 [1]에서 언급한 드론 아이디 패킷의 최소 및 최대 시간 길이인 630μs와 650μs를 STFT를 통해 얻은 타임 슬롯의 간격으로 나누어, 최소 및 최대 샘플 개수를 구하였다.

Ⅲ. 시뮬레이션

시뮬레이션에서 사용된 드론 데이터는 mini2 기종의 신호가 SDR을 통해 50MHz의 샘플링 레이트로 캡처된 32비트 부동 소수점 드론 IQ 데이터이며, 이 데이터에는 9개의 드론 아이디 패킷과 시간 주파수가 겹치지 않는 2개의 커맨드 앤 컨트롤 패킷 정보가 포함되어 있다 [4]. 시뮬레이션에서는 해당 IQ 데이터를 64비트 부동 소수점 형식의 복소수로 변환한 후, STFT를 포함한 드론 아이디 패킷 인덱스 추출 알고리즘을 적용하였다. 시뮬레이션한 결과, 9개의 드론 아이디 패킷의 시작점과 끝점 인덱스를 모두 추출하였다. 정확한 인덱스를 추출한 것인지 검증하기 위해 각 타임 슬롯의 최대 크기 값을 추출한 배열에서 해당 인덱스에서의 크기 값을 확인해보았다. 그 결과, 시작점 인덱스부터 끝점 인덱스까지는 임계치를 넘는 크기 값을 가지고, 시작점 인덱스 전과 끝점 인덱스 이후에서는 임계치보다 작은 크기 값을 가지는 것을 확인함으로써, 추출된 9개의 드론 아이디 패킷의 시작점과 끝점 인덱스가 100% 정확한 것을 검증할 수 있었다. [그림 3]은 드론 IQ 데이터를 스펙트로그램으로 나타내고, 추출한 시작점과 끝점의 인덱스를 스펙트로그램 상에서 빨간 줄로 나타낸 것이다.

Ⅳ. 결론

본 논문에서는 드론의 IQ 데이터에 STFT를 적용하고 타임 슬롯에 따른 신호 크기를 비교함으로써 각 드론 아이디 패킷의 시작점과 끝점 인덱스를 추출하는 알고리즘을 제안하였다. 신호가 있는 타임 슬롯과 없는 타임 슬롯을 판단하기 위해 설정한 임계치를 기준으로 STFT 결과 행렬을 Boolean 인덱싱 배열로 변환하고, 배열 내에서 드론 아이디 패킷의 시작점과 끝점의 인덱스를 찾는 두 가지 조건을 제시하였다. 시뮬레이션 결과, 9개의 드론 아이디 패킷 정보를 가지고 있는 드론의 IQ 데이터로부터 각 패킷의 시작점과 끝점 인덱스를 정확하게 추출하였다. 향후 연구에서는 추출된 각 드론 아이디 패킷을 복조와 디코딩하여 패킷에 담긴 정보를 파악할 수 있을 것이다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2022R1A2C1011862)

참 고 문 헌

[1] Schiller, Nico, et al. "Drone Security and the Mysterious Case of DJI's DroneID." Network and Distributed System Security Symposium (NDSS). 2023.

[2] Bender, Conner. "DJI drone IDs are not encrypted." arXiv preprint arXiv:2207.10795 (2022).

[3] D.Protzman DJI DroneID RF Analysis, GitHub (www.github.com/proto17/dji_droneid), 2022.

[4] Merlin Chlosta, DroneSecurity. Github (https://github.com/RUB-SysSec/DroneSecurity), 2023.