

CL-OTC: UAV 환경에서 LoRa 은닉 채널 기반의 OneTime-Command 프레임워크 구현

허남정*, 최상훈¹, 박기웅[†]

세종대학교 SysCore Lab. (대학원생, 연구교수¹)

**세종대학교 정보보호학과 (교수[†])

CL-OTC: One-Time Command Framework Based on LoRa Covert Channel in UAV environment

Nam-Jung Heo*, Sang-Hoon Choi¹, Ki-Woong Park[†]

*SysCore Lab., Sejong University

**Dept. of Computer and Information Security, Sejong University
(Graduate Student*, Research Professor¹, Professor[†])

요 약

UAV는 해양 경비, 긴급 구조, 환경 모니터링을 아울러 여러 방면으로 다양한 산업 분야에서 사용될 수 있다. 최근 UAV의 취약점을 분석해 UAV의 추락, 제어권 탈취 등과 같은 악의적인 공격을 수행하는 연구가 진행되고 있다. 본 논문이 제안하는 Covert LoRa-One Time Command(CL-OTC) 프레임워크는 LoRa 기술에 OOK 변조 기법을 적용하여 은닉 채널을 형성한다. 형성된 은닉 채널을 통해 짧은 주기로 바뀌는 일회성 명령어를 전송함으로써 리플레이 공격, 중간자 공격, 명령 코드 삽입과 같은 사이버전에 대응할 수 있다. CL-OTC 프레임워크는 UAV 사이버전에서 능동적으로 대응할 수 있는 통신 보안 체계를 제공할 것이다.

I. 서론

UAV(Unmanned Aerial Vehicle)는 해양 경비, 긴급 구조, 환경 모니터링, 적대 국가에서의 임무 수행 등의 다양한 활용 수단으로 사용될 수 있다. 이러한 UAV의 보안은 사이버 보안 원칙에 따라 매우 중요한 요소이며, UAV의 설계 및 개발 단계에서 이를 고려하고 개발해야 한다 [1].

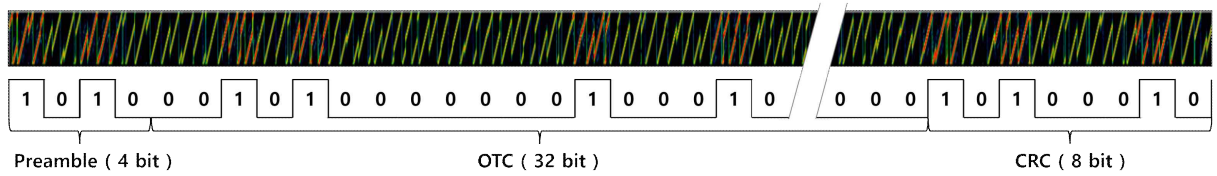
최근에는 UAV가 비허가 지역에서 비행하는 경우, 이를 탐지하고 대상 드론에 리플레이

(replay) 공격, 중간자(MitM) 공격, 명령 코드 삽입(Command and Code Injection)과 같은 사이버전에서 UAV를 무력화시키는 연구가 진행되고 있다 [2, 3]. 이러한 무력화 연구는 UAV의 정상적인 비행을 방해하고 드론의 추락을 유도하거나 제어권 탈취를 목표로 한다.

본 연구에서 UAV의 사이버전에서 무력화 공격 수단을 방어할 수 있는 Covert Lora-OneTime Command Framework (CL-OTC)를 제안한다. 제안된 프레임워크는 일회성 명령 체계를 사용하여, 사이버 무력화 공격으로부터 능동적으로 대응할 수 있게 한다. 일회성 명령어는 LoRa 통신 모듈의 Chirp Spread Spectrum (CSS) 변조 특성을 고려해 추가적인 On-off keying (OOK) 변조 방식의 은닉 채널을 사용함으로써, 공격자는 일회성 명령

[†] 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 논문은 과학기술정보통신부의 재원으로 정보통신기획지원(IITP)의 정보보호핵심원천기술개발(Project No. RS-2024-00438551, 40%), 실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 30%), 국방ICT융합연구(Project No. 2022-11220701, 30%)의 지원을 받아 수행된 연구임.



(그림 2) CSS 변조에 추가 OOK 변조를 적용한 은닉 채널 패킷 구조

체계의 존재를 알아차리기 어렵게 만든다.

본 논문에서 조사한 바에 의하며, LoRa 기술에 은닉 채널을 적용하여, 드론에 일회성 명령을 전달하는 연구는 본 연구가 최초이다.

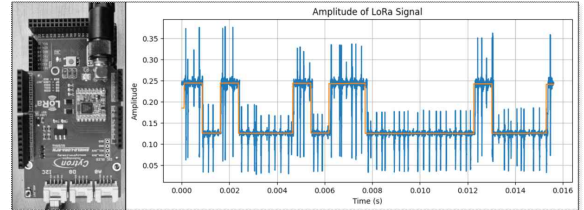
본 논문의 구성은 다음과 같다. 제2장에서는 LoRa 기술에서의 OOK 변조 기법에 대해서 기술한다. 제3장에서는 본 연구에서 제안하는 OneTime-Command(OTC)을 제시한다. 제4장에서 GCS와 UAV 간의 통신에서 CL-OTC 프레임워크의 동작을 설명한다. 제5장에서는 실험 환경에 대해서 설명한다. 제6장에서는 결론과 향후 연구 방향에 대해서 논의한다.

II. LoRa 기술에 OOK 변조를 적용한 은닉 채널 형성 방법

LoRa는 Semtech사에서 개발하고 독점 공급을 하는 저전력 IoT 통신 기술이다. LoRa 기술의 독특한 CSS 변조 방식은 낮은 대역폭으로 높은 효율의 전력 소모와 장거리 전송을 가능하게 하며, IoT, 위성 등 다양한 통신 체계에서 사용된다 [4].

CSS 변조 기술은 주파수 변조를 기반으로 하며, 진폭의 변화를 고려하지 않는다. 이러한 특성 탓에 CSS 변조에 추가적인 진폭 변조를 수행하여도 원본은 바뀌지 않아서, 진폭 변조가 추가적인 은닉 채널의 형성 수단으로 연구되고 있다. B. Liu et al. [5] 연구에서는 CSS 변조에 진폭 변조를 수행하여 LoRa 은닉 채널을 형성하고 최대 900m 거리까지 유효한 통신이 가능함을 평가한다.

본 연구에서는 LoRa 모듈의 TX Power 레지스터를 조작하여, CSS 변조에 진폭을 추가 변조하는 방식으로 On-off keying (OOK)를 적용한다.



(그림 1) LORA 신호의 진폭 변조 수행

실험에 수행된 변조 기법은 신호의 '1'을 표현하고자 할 때는 신호의 TX Power를 높이고, 반대로 '0'을 표현할 때 낮추는 방식이다. (그림 1)은 TX Power 레지스터를 조작하여 OOK 변조를 수행했을 때의 진폭 변화이다.

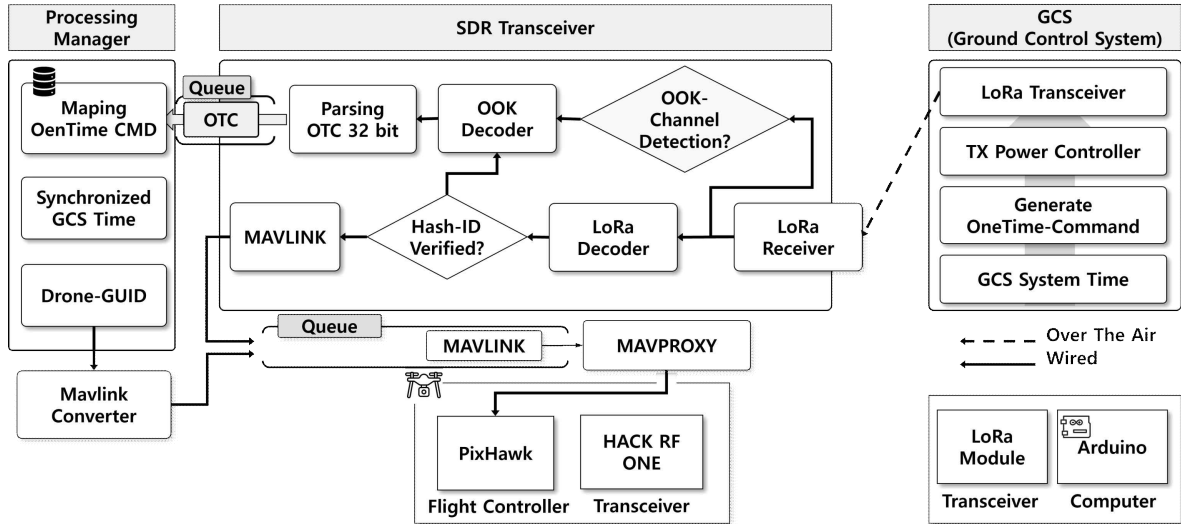
(그림 2)는 OOK 변조가 적용된 LoRa 신호이다. OOK 방식으로 변조된 은닉 채널은 패킷을 검출하기 위한 4개의 비트인 Preamble, 일회성 명령어(OTC)를 의미하는 32비트 그리고 오류를 검출하기 위한 8개의 CRC 비트로 구성된다.

III. OTC : OneTime-Command 명령 생성 기법

공격자가 UAV 통신 네트워크에 침입했을 때, GCS(Ground Control System)와 UAV 간의 통신을 엿듣고 통신 프로토콜을 식별하여 명령어 정보를 획득할 수 있다. 공격자는 UAV를 비활성화하는 공격 패킷을 생성하고 통신 과정에서 주입하는 방식으로 공격을 수행한다 [3].

$$OTC = CRC32(GUID, \left\lfloor \frac{T_{now} - T_{sync}}{V} \right\rfloor, CMD)$$

- GUID : 드론을 식별하는 고유 ID
- T_{now} : 현재 시간 (in milliseconds)
- T_{sync} : 동기화 시간 (in milliseconds)
- V : 설정된 유효 시간 (Validity Period)
- CMD : 명령어 제어 ID



(그림 3) 제안된 Covert LoRa - OneTime Command Framework (CL-OTC)

본 연구에서는 제안하는 일회성 명령 체계인 One-Time Command(OTC)는 시간을 기반으로 생성된다. GCS와 UAV 최초의 1회 통신에서 UAV의 GUID와 시스템 시간 정보를 동기화한다.

OTC 생성 기법은 드론의 GUID, 동기화 이후 시간, Command ID 들의 32비트 CRC 해시를 계산한다. V의 크기에 따라서 유효시간은 설정된다. V의 값이 1000인 경우 OTC의 유효값은 1초이고 500인 경우 0.5초이다. 본 연구에서는 CRC 해시 알고리즘을 사용했지만, 다른 해시 알고리즘을 사용해도 무관하다. 일회성 명령어의 유효시간은 GCS에서 송신한 신호가 UAV에 도달하여 처리하는 시간을 고려하여 적절한 시간을 도출해야 한다. 본 연구에서는 최적의 유효시간에 대해서 다루지 않는다.

생성된 일회성 명령어는 짧은 주기로 바뀌는 명령어 테이블을 구성하여 리플레이 공격, 중간자 공격, 악의적인 명령 코드 삽입 등과 같은 사이버 무력화 공격으로부터 방어한다.

IV. Covert LoRa-OTC 프레임워크

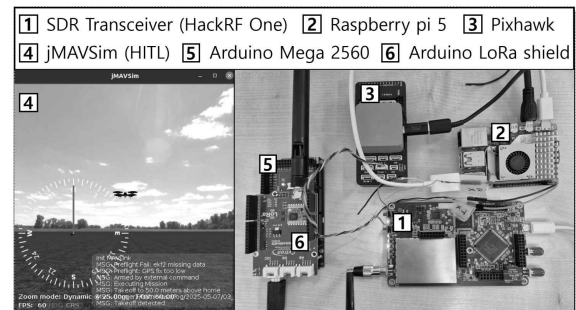
본 논문은 GNU Radio와 gr-lora-sdr [6] 프로젝트를 기반으로 UAV의 장착된 SDR 송수신기(SDR Transceiver)에서 LoRa 패킷을 감지하고 수신한다. 수신된 LoRa 패킷의 샘플링 데이터로 OOK 복조를 수행하여 프리앰블

(Preamble)을 검출한다.

(그림 3)은 논문에서 제안하는 CL-OTC 프레임워크의 전체 구조이다. UAV는 GCS와 동기화된 시간과 고유의 GUID를 가지고 있다.

SDR 송수신기에서 OOK 채널의 프리앰블이 감지되면 OOK 디코딩을 수행하여, 32비트의 OTC를 추출한다. UAV는 내부적으로 관리하는 OTC 테이블을 갱신하고 추출된 OTC에 대응되는 MAVLINK 명령어로 변환하여 픽스호크(PixHawk)에 전달한다. 픽스호크는 드론의 센서 및 모터 제어 등의 UAV의 비행을 담당하는 비행 컨트롤러이다. 만약 내부적으로 맵핑되는 OTC가 존재하지 않는다면, 해당 명령을 오류로 판단하고 패킷을 버리도록 한다.

V. 실험 환경 및 검증



(그림 4) CL-OTC 프레임워크의 구성 요소

(그림 4)는 본 논문이 제안하는 CL-OTC 프레임워크의 구성 요소를 보여준다. 본 논문

의 실험 환경은 LoRa 신호를 수신하고 샘플링 데이터를 수집하는 SDR 송수신기인 (1) HarkRF One과 SDR로부터 수신된 신호로 OOK 복조를 수행하고, OTC를 추출하는 (2) 라즈베리파이5가 있다. 생성된 OTC는 MAVLINK로 맵핑되어, UART로 연결된 비행 컨트롤러인 (3) 픽스호크에 전달된다. 픽스호크에서는 Hardware in the Loop Simulation(HITL)가 실행되며, 연결된 (4) jMAVSIM 가상 시뮬레이터 환경 안에서 비행한다. (5) Arduino Mega 2560은 OTC를 계산하고 (6) LoRa Shield 통신 모듈이 동작할 때, 모듈 내의 TX_Power 레지스터를 조작하여 은닉 데이터를 송신한다.

VI. 결론

LoRa의 낮은 주파수 대역으로 인해 OOK 변조는 다양한 방해 요소들을 만나 페이딩(fading) 문제가 발생할 수 있다. 더욱 향상된 OOK 변조 기술은 이러한 문제를 일부 보완할 수 있다 [5]. OTC 기술은 사이버 무력화 공격에 능동적으로 대응할 수 있지만, 최적의 유효 시간에 대한 논의는 추가적으로 필요하다. UAV와 SDR 송수신기를 통합하는 것은 무게와 배터리 소모 증가를 고려해야 한다.

Papoči et al. [7] 연구에서는 SDR 송수신기와 UAV의 통합에 관해서 논의한다. 실험에서 SDR 송수신기와 단일 보드 컴퓨터를 픽스호크 기반의 UAV에 탑재하여 실효성을 평가한다. 실험 결과 SDR 장비로 인해 추가 전력 소비는 배터리로부터 22.5V 전압과 5A 전류 부하가 측정되어 112.5W의 전력을 소모한다. 이는 UAV의 비행시간을 10% 감소시킨다. 이를 극복하기 위해 추가 배터리를 구성할 수 있으나 UAV의 무게가 증가할 수 있기 때문에 신중한 고려가 필요하다.

최근 사이버전에서 UAV를 비활성화하고 신호를 분석하는 연구가 진행되고 있기 때문에 [8], 더욱 효과적인 방어 수단인 OTC와 은닉 채널이 필요하다. 본 논문의 실험 결과, UAV 내에서의 CL-OTC 프레임워크의 적용 가능성을 보였으며, 향후 연구로 통신거리 확보, 더

낮은 배터리 소모, 다른 연구와 융합 등의 더 많은 노력이 필요하다. 본 논문의 연구가 더욱 안전한 UAV의 통신 체계 발전에 기여가 되기를 바란다.

[참고문헌]

- [1] F. E. Salamh et al, A comparative uav forensic analysis: Static and live digital evidence traceability challenges, Drones, vol.5, no.2, 2021.
- [2] B. Branco, J. S. S. Silva and M. Correia, Cyber Attacks on Commercial Drones: A Review, IEEE Access, vol.13, pp.9566-9577, 2025.
- [3] Y. M. Kwon et al, Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles, IEEE Access, vol.6, no.43203-43212, Aug, 2018.
- [4] J. Haxhibeqiri et al, A survey of LoRaWAN for IoT: From technology to application, Sensors, vol.18, no.11, 2018.
- [5] L. Boya et al, LoPhy: A resilient and fast covert channel over LoRa PHY, Proceedings of the 22nd International Conference on Information Processing in Sensor Networks, 2023.
- [6] J. Tapparel. gr-lora_sdr. https://github.com/tapparelj/gr-lora_sdr.
- [7] P. Petar, T. Radišić and M. Muštra, Integration of software defined radio on an unmanned aerial vehicle, Transportation Research Procedia, pp.308-315, 2022.
- [8] N. Schiller et al, Drone Security and the Mysterious Case of DJI's DroneID, NDSS, 2023.