드론 RC 무선조종기 제어 데이터 보호를 위한 경량암호 적용 방법에 관한 연구

윤정일, 윤승용, 김병구, 강유성
한국전자통신연구원 사이버보안연구본부

sigipus@etri.re.kr, syyoon@etri.re.kr, bkkim05@etri.re.kr, youskang@etri.re.kr

A Study on the Application of Lightweight Cryptography for Protecting Drone Remote Control Data

Joungil Yun, Seungyong Yoon, Byoungkoo Kim and Yousung Kang
Cyber Security Research Division, Electronics and Telecommunications Research Institute (ETRI)

요 약

RC 무선조종기를 통해 드론을 원격으로 제어하는 경우, 제어 데이터의 기밀성과 무결성은 드론 제어권 탈취 방지를 위한 핵심 고려 사항이다. 본 논문은 드론 RC 무선조종기 제어 데이터 보호를 위해 경량 암호화 알고리즘 중 하나인 Lightweight Encryption Algorithm (LEA)를 적용하는 방법을 제시한다. LEA 는 32 비트 마이크로 컨트롤러인 ARM Cortex-M4 와 같은 플랫폼에 최적화된 구조로, 저전력으로 데이터 보호를 유지하면서 효율적인 암호화 알고리즘을 적용할 수 있다.

1. 서 론

드론 기술은 군사, 물류, 건설, 농업 등 다양한 산업 분야에서 널리 사용되고 있으며, RC 무선조종기를 통한 원격 제어는 드론 운영의 주요 요소 중 하나이다. 그러나 드론 RC 무선조종기 제어 데이터는 무선 통신을 통해 전송되기 때문에 해킹이나 악용의 위험이 존재한다. 특히 최근 드론의 활용도가 다양화됨에 따라 관련 보안 문제가 점점 중요해지고 있으며, 안전하게 드론을 운영하기 위해서는 드론의 비행 동작 명령 수행을 위한 제어 데이터를 보호하는 것이 필수적으로 요구된다. 하지만 기존 암호화 기술 중 요구되는 컴퓨팅 자원이나 복잡성이 높은 알고리즘들은 배터리 기반의 모바일 기기인 드론 운영 환경에서 조종 딜레이 최소화를 위한 실시간 처리가 중요한 RC 무선조종기의 제어 데이터 보호에는 적합하지 않다.

본 논문은 RC 무선조종기에서 드론으로 전송되는 제어 데이터를 보호하는 효율적인 보안 시스템 설계를 목적으로 경량 암호화 알고리즘인 LEA[1]를 적용하고, 이를 ARM Cortex-M4 마이크로 컨트롤러에 효과적으로 구현하는 방법에 관한 연구이다. LEA 는 충분한 보안성을 유지하면서도 낮은 컴퓨팅 자원만 요구하기 때문에 실시간 시스템인 RC 무선조종기와 같은 장치에서 실행할 수 있는 장점이 있으며, 다양한 운영 모드(modes of operation) 지원으로 제어권 보장을 위한 보안 서비스 제공이 가능하다.

2. 제어 데이터 보호를 위한 LEA 운영 모드

LEA 는 국가보안기술연구소가 개발하여 2019 년말 ISO/IEC 에서 경량암호 표준으로 지정된 128 비트 블록암호 알고리즘으로, 빅데이터, 클라우드 등 고속 환경 및 센서, IoT(Internet of Things) 등 저전력 모바일 환경에서 기밀성을 제공하기 위해 개발되었다. LEA 는 소프트웨어 기반 플랫폼 구현 기준 128 비트 블록암호 알고리즘들 성능 비교 결과 가장 우수한 것으로 평가되었으며[2], 기능 보완이 가능한 소프트웨어 기반 모바일 기기의 경량 암호화 기술 적용에 적합하다.

LEA 는 32 비트 ARX(Addition, Rotation, XOR) 연산을 기반으로 설계되어[3], ARX 연산 고속 처리 명령어가 지원되는 소프트웨어 기반 플랫폼에서 블록암호의 핵심인 라운드 함수(round function) 고속 구현이 가능하며, 아래 <표 1>과 같이 128, 192 또는 256 비트 키 길이를 지원하여 다양한 보안 수준을 제공한다.

또한 LEA 는 ECB(Electronic code book), CBC(Cipher

<표 1> LEA 규격 (길이 단위: bits)

구분	블록 길이	암호 키 길이	라운드 수
LEA-128	128	128	24
LEA-192		192	28
LEA-256		256	32

block chaining), CTR(Counter) 등 다양한 운영 모드를 지원한다[4]. 본 논문은 드론 제어 데이터에 대한 기밀성뿐만 아니라, 정당한 제어권이 있는 조종 장치에서 전송된 데이터임이 인증되고 변조되지 않았는지 판단하여 드론의 제어권 탈취를 방지하는 것이 더욱 중요하다고 보며, 이에 적합한 LEA 기반 인증 암호화 운영 모드 적용을 제안한다.

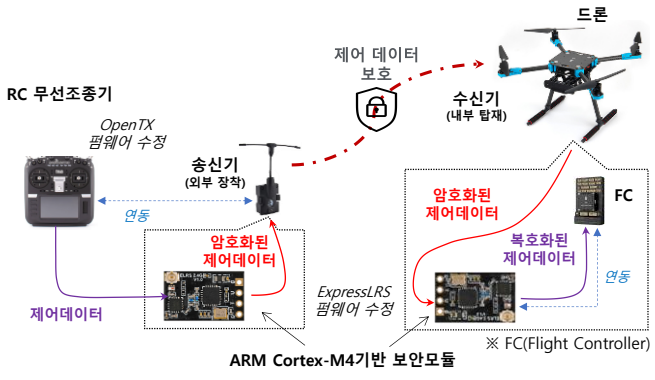
LEA 기반 인증 암호화 운영 모드는 CCM(Counter with CBC-MAC)과 GCM(Galois/Counter Mode)이 표준으로 제정되어 있다. 이들은 공통적으로 기밀성을 제공하는 CTR 운영 모드를 기반으로 CCM 은 CBC-MAC 을, GCM 은 GF(Galois Field) 상에서 정의된 GHASH 함수를 각각 사용하여 메시지를 인증한다. 일반적으로 GCM 이 CCM 보다 더 빠르고 안전하다고 알려져 있으므로, GCM 의 적용이 더 적합하다고 판단된다. LEA 기반의 GCM 운영 모드를 제어 데이터 보호에 적용할 때, 속도(성능)와 보안 강도 사이의 관계와 함께 드론과 RC 무선조종기 연동 시 고려해야 할 여러 요소들이 있다는 것을 <표 2>에서 확인할 수 있다.

<표 2> 제어 데이터 보호를 위한 GCM 파라미터 설정 관련

구 분	보안 vs. 성능	고려 사항
암호 키	암호 키가 길수록 속도 저하, 보안 강도 증가	공유 방법
초기 값 (Nonce)	Nonce 길이가 96 비트가 아니면 카운터 블록 생성 복잡도 증가	재전송 공격 회피를 위한 Nonce 갱신 및 공유 방법
부가 인증 데이터	부가 인증 데이터가 길수록 속도 저하, 보안 강도 증가	필요성 및 공유 방법
인증 값	인증 값(최대 128 비트) 길수록 보안 강도 증가	전송프레임 구조 및 데이터 전송률

3. 시스템 구성

(그림 1)은 드론 RC 무선조종기의 제어 데이터 보호를 위한 시스템 구성을 보여준다. 이 시스템은 지상제어국을 통한 드론 제어가 아닌, 제한된 컴퓨팅 자원을 가진 휴대용 무선조종기 원격 제어 환경에서 오픈소스 프로젝트인 OpenTX 와 ExpressLRS 를 기반으로 한 RC 무선조종기, 외부 장착 송신기, 드론, 그리고 수신기로 구성된다. OpenTX 는 RC 무선조종기를



(그림 1) RC 무선조종기 제어 데이터 보호 시스템 구성도

위한 오픈소스 펌웨어로[5], 제어 데이터 보호 기능의 활성화/비활성화 및 LEA 입력 파라미터 설정 등의 기능 추가를 위해 수정될 수 있다. ExpressLRS 는 고성능의 오픈소스 라디오 컨트롤 링크로, RC 애플리케이션에 사용된다[6]. 이는 900MHz 와 2.4GHz 주파수에서 다양한 통신 기능이 포함된 하드웨어를 지원하며, ARM Cortex-M4 마이크로 컨트롤러가 내장된 ExpressLRS 지원 보안모듈 개발에 활용된다.

Cortex-M4 는 ARM 이 개발한 32 비트 고성능 마이크로 컨트롤러 코어로, 저전력 및 실시간 응용 프로그램에 최적화되어 있다. 이는 단일 코어임에도 불구하고 SIMD(Single Instruction Multiple Data) 확장 기능을 통해 특정 DSP 연산에서 2 개의 16 비트와 4 개의 8 비트 데이터를 병렬 처리할 수 있는 능력을 갖추고 있다. 그러나 본 논문에서는 LEA 의 32 비트 ARX 연산 기반 구조에 대해 Cortex-M4 의 SIMD 기능이 큰 효과를 발휘하지 못할 것으로 예상한다. 대신, GCM 운영 모드의 GHASH 함수를 사전 계산된 32 비트 단위 Lookup Table(LUT) 방식으로 구현하면, 상대적으로 가장 큰 최적화 효과를 얻을 수 있을 것으로 본다.

4. 결 론

드론을 RC 무선조종기를 통해 제어하는 경우, 안정성과 신속성이 중요하다. 본 논문에서는 드론 RC 무선조종기의 제어 데이터 보호를 위한 LEA 기반 인증 암호화 운영모드 적용과 그에 따른 시스템 구성 방법을 제시하였다. LEA 의 경량화된 암호화 구조가 ARM Cortex-M4 마이크로 컨트롤러의 소프트웨어 기반 플랫폼에 최적화되면, 저전력 보안모듈 개발이 가능해진다. 이를 활용하면 드론 제어의 보안성이 강화되어 제어권 보장에 기여할 것으로 기대된다.

사사문구

이 논문은 2023 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.RS-2023-00225201, 국방 무인이동체 역이용 방지 제어권 보호기술 개발)

참고문헌

[1] KS, 128-bit block cipher LEA, KS X 3246, 2016.
[2] 권대성, “ISO/IEC JTC 1 SC 27 암호기술 국제표준화 동향,” 정보보호학회지, 33(4), pp. 103-109, 2023.
[3] D. Hong, et al. “LEA: A 128-bit block cipher for fast encryption on common processors,” WISA 2013, LNCS 8267, pp. 3-27, 2013.
[4] KS, Modes of operation for an n-bit block cipher – Part1: General, KS X 3254, 2016.
[5] OpenTX [Internet], “https://www.open-tx.org/”
[6] ExpressLRS [Internet], “https://www.expresslrs.org/”