드론 서비스를 위한 PQC 기반 보안채널 통신기술 구현

윤승용, 윤정일, 김병구, 김건우, 강유성
한국전자통신연구원 사이버보안연구본부 책임연구원

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

Implementation of PQC-based Secure Channel for Drone Services

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

요 약

드론은 초기에 주로 군사적 목적으로 사용되었으나, ICT 기술이 발전함에 따라 다양한 산업 서비스에 활용되고 있다. 그러나 드론이 네트워크에 연결됨으로써 많은 보안위협과 취약점에 노출되었으며, 이는 드론 탈취, 정보유출, 서비스 장애 등의 심각한 피해를 야기할 수 있다. 따라서, 본 논문에서는 기존 드론의 보안위협 뿐만 아니라 다가올 양자시대의 보안위협에 대비하여 안전한 드론 서비스를 제공할 수 있는 PQC 기반 보안채널 통신기술을 제안하고 구현한다.

1. 서론

드론은 조종사가 직접 탑승하지 않고 원거리에서 무선으로 원격조정을 하거나 입력된 프로그램에 따라 비행이 가능한 비행체로 정의하고 있다. 초기에는 주로 군사적 목적으로 개발 및 활용되었으나, ICT(Information & Communications Technology) 기술이 발전함에 따라 배송, 안전관리, 환경관리, 재난 상황 감시 등의 다양한 산업 서비스에 활용되고 있다[1].

드론은 공격이나 보안위협이 발생하면 정보유출, 서비스 마비뿐만 아니라 인명피해와 같은 치명적인 피해를 입을 수 있다. 따라서, 드론 서비스를 활성화하기 위해서는 다양한 보안 기술이 드론 시스템에 적용되어야 하며, 향후 도래할 양자시대의 보안위협도 극복할 수 있는 최신 보안 기술이 적용되어야 한다. 그러나 아직까지는 미흡한 실정이며, 본 논문에서는 안전한 드론 서비스를 제공하기 위한 PQC(Post-Quantum Cryptography) 기반 보안채널 통신기술을 제안한다.

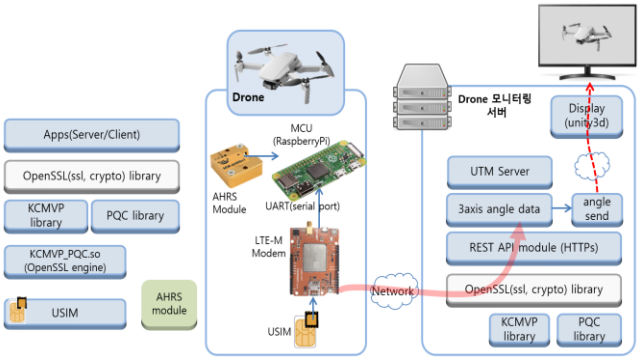
2. 드론 보안위협 및 보안통신기술 구현

드론 시스템의 보안위협에 대한 많은 연구가 진행되고 있으며, 중간자 공격, 가용성 방해, 데이터 손실, 부적절한 암호사용, 악의적인 프로그램 실행, 잘못된 설계 및 구현 등의 위협이 존재한다[2][3][4]. 대부분의 네트워크 통신 관점에서의 보안위협은 암호화된 통신채널을 통해 데이터를 전송함으로써 대응 가능하다. 그러나, 국방 및 민간 드론에 적용된 기존 암호기술은 양자컴퓨팅 시대 도래에 따라 심각한 보안위협에 직면하게 될 것이며, 원격제어권 탈취를 위한 다양한 사이버 공격에 효과적으로 대응하기에는 한계가 있다. 즉, Shor 알고리즘의 등장[5]과, 양자 알고리즘을 구동하는 양자컴퓨터의 성능이 발전하면서 기존 RSA 및 ECDSA(Elliptic Curve Digital Signature Algorithm) 서명 기반의 드론 인증 프로토콜은 심각한 보안위협에 직면하게 될 것이다.

KCMVP(Korea Cryptographic Module Validation Program)은 국가・공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도로써[6], 드론의 안전성 보장을 위해 국방 분야뿐만 아니라 민간 분야의 드론 서비스에도 점차 확대되어 사용될 전망이다. KCMVP 검증 암호의 사용은 관리 부주의로 인한 암호키 노출이나 취약한 암호사용으로 인한 정보유출을 근본적으로 차단할 수 있는 대응책이 될 수 있다.

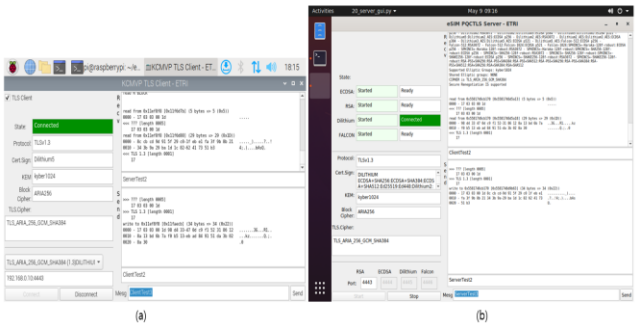
본 논문에서는 드론 서비스를 위한 PQC 기반 보안채널 통신기술을 구현하기 위해 OQS-OpenSSL[7]를 활용한다. OQS-OpenSSL 은 TLS v1.3 을 기반으로 PQC 암호모듈을 연동하여 네트워크를 통한 데이터 통신에 사용되는 TLS 를 구현한 오프소스 프로젝트이다. C 언

어로 작성되어 있는 중심 라이브러리 안에는, 기본적인 PQC 를 포함한 기존 암호화 기능 및 여러 유틸리티 함수들이 구현되어 있다. 그러나 KCMVP 검증대상인 블록암호 ARIA, LEA 등의 알고리즘이 구현되어 있지 않아, 해당 알고리즘 지원하도록 추가 구현이 필요하다. 또한 다양한 기존 응용들의 호환성 보장을 위해 TLS v1.2 지원도 필요하다.



(그림 1) PQC 기반 보안채널 통신 드론 시스템

(그림 1)은 이러한 요구사항을 반영하여 구현한 PQC 기반 보안채널 통신 드론 시스템 구조도이다. 개발환경으로 서버는 Linux UbntuOS 20.04 LTS, 드론은 Raspberry PI OS 11, OpenSSLdms 1.1.1f 버전을 사용하였다. 드론의 AHRS(Attitude Heading Reference System) 모듈에서 측정한 센싱 정보는 PQC 기반 TLS 보안채널을 통해 암호화되어 GCS(Ground Control Station)의 모니터링 서버로 안전하게 전송된다. 이때 보안채널을 생성하기 위해 Crystals-Kyber, Crystals-Dilithium, Falcon 등의 PQC 암호 알고리즘이 활용되고, 데이터 암/복호화를 위해 KCMVP 블록암호 ARIA, LEA, SEED 등이 활용된다.



(그림 2) 시스템 화면: (a)드론, (b)GCS 서버

(그림 2)는 PQC 기반 보안채널 생성 및 데이터 통신을 위한 드론과, GCS 모니터링 서버의 암/복호화 시스템 화면이다. TLS 버전, 서명 알고리즘, 키교환 알고리즘, 블록암호 알고리즘 등을 설정하여 데이터를 암호화하여 전송하고, 수신된 데이터를 복호화하여 확인할 수 있는 기능을 제공한다. 우리는 시험을 통해 TLS v1.2 와 v1.3 을 모두 지원하며, 키 설정 알고리즘인 Crystals-Kyber, 인증 알고리즘인 Crystals-Dilithium/Falcon, 블록암호 알고리즘인 ARIA/SEED/LEA 등의 조합으로 생성할 수 있는 TLS Cipher Suites 를 보안레벨 5 수준으로 모두 확인하였다. (예, TLS v1.2 기준 Cipher Suites: KYBER1024-DILITHIUM5-ARIA256-GCM-SHA384)

3. 결론

본 논문에서는 기존 드론 시스템의 보안위협 뿐만 아니라 다가올 양자시대의 공개키 암호 붕괴 위협에 대비하여 안전한 드론 서비스를 제공할 수 있는 PQC 기반 보안채널 통신기술을 구현하고, 기능을 확인하였다. 향후, 드론에 적용가능한 하드웨어 기반의 암호기술, 드론의 특성을 고려한 경량/저전력의 보안 기술 등에 대한 연구가 필요하여, 이를 활용한 보안채널 생성 및 통신 기술 개발도 필요하다.

사사문구

이 논문은 2023 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No.RS-2023-00225201, 국방 무인이동체 역이용 방지 제어권 보호 기술 개발, 50%)과 2023 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2022-0-01019, eSIM 생태계 조성을 위한 엣지 디바이스 전용 eSIM 보안 플랫폼 기술 개발, 50%)

참고문헌

[1] 한국인터넷진흥원, “드론 사이버보안 가이드”, 2020
[2] Westerlund, O., and Asif, R., “Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things”, 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS), IEEE, Muscat, Oman, 2019, pp. 1-10
[3] Rodday, N. M., Schmidt, R. D. O., and Pras, A. “Exploring security vulnerabilities of unmanned aerial vehicles” NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium, IEEE, Istanbul, Turkey, 2016, pp. 993-994
[4] Kwon, Y. M., Yu, J., Cho, B. M., Eun, Y., and Park, K. J., “Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles”, IEEE Access, Vol 6, pp. 43203-43212, 2018
[5] Shor, P. W., “Algorithms for quantum computation: discrete logarithms and factoring”, 35th annual symposium on foundations of computer science, IEEE, Santa Fe, USA, 1994, pp. 124-134
[6] KCMVP, https://www.nis.go.kr:4016/AF/1_7_3_1.do
[7] OQS-OpenSSL, https://openquantumsafe.org/