5G 특화망 내 qSIM 기반 드론 인증 시스템

윤혜진†, 윤승환‡, 이옥연†*
국민대학교 금융정보보안학과†*, 국민대학교‡
{dbswls2265, schneeleopard, oyyi*}@kookmin.ac.kr

Authentication system using qSIM between drones in 5G private network

Hyejin Yoon†, Seunghwan Yun‡, and Okyeon Yi†*
Dept. of Financial information security Kookmin Univ.†, Kookmin Univ.‡

요 약

최근 드론의 수요처가 다양한 분야로 확대됨에 따라 드론이 운용되는 수요처가 공공기관 및 국방에도 적용되고 있으며, 다양한 환경에서 드론이 운용될 수 있도록 5G 기술과 같은 이동통신 환경이 접목되고 있는 추세이다. 드론에 다양한 기술이 접목되고 드론이 공공기관 및 국방에서 운용되기 위해서는 드론의 데이터 보호와 드론의 식별 및 인증을 위해 검증필 암호모듈이 탑재되어야 하는 것이 필수적이다. 본 논문에서는 이러한 드론의 운용 환경에 따른 드론 식별 및 인증을 위해 검증필 하드웨어 암호모듈인 qSIM을 이용한 드론 인증 시스템을 제안한다.

Ⅰ. 서 론

최근 드론의 수요처가 다양한 분야로 확대됨에 따라 드론 운용 및 데이터 관리에 대한 보안이 불가피한 상황이다. 2023년 11월에 정보통신산업진흥원에서 발표한 드론의 시장동향 보고서에 보면, 2022년 10월부터 2023년 9월까지 1년간 조사한 드론 기술과 드론의 수요처를 확인할 수 있다.[1] [그림 1]에 따르면, 드론에 적용되는 다양한 기술 중에서 5G가 3위를 차지하고 있다. 5G 기술을 통해 장거리 비행에서 효율적으로 드론을 운용할 수 있으며, 비행 중 수집한 방대한 양의 데이터를 실시간으로 전송할 수 있다. 특히, 5G 기술이 적용된 드론의 경우, 5G 네트워크를 통해 스마트시티 내에 드론 간 통신을 가능하게 한다. 이러한 5G 기술을 이용하면, 5G 이동통신 기술을 바탕으로 특정 기관 내 주파수로 맞춤형 서비스를 제공하는 5G 특화망 내에서 드론을 운용할 수 있다.

또한, 위 보고서에서 조사한 결과인 [그림 2]를 보면, 드론이 사용되는 수요처로 공공과 국방 등 주요 시설인 수요처가 높은 비율을 차지하고 있다. 공공 안전을 위해 드론을 이용해 데이터 수집 시와 군용 드론 운용시에는 데이터 보호와 인증이 필수적이다. 특히, 국내에서 공공 기관이나 군에서 운용되는 장비는 KCMVP 암호모듈을 통해 데이터 보호 및 인증을 수행해야 한다.

1위	레이더
2위	인공지능
3위	5G
4위	GPS
5위	라이다

[그림 1] 주요 드론 기술 [1]

1위	공공
2위	엔터테인먼트
3위	국방
4위	소매
5위	운송

[그림 2] 주요 드론 수요처[1]

공공기관이나 국방 등의 주요 시설에서 드론이 운용되기 위해서는 드론과 지상국(Ground Control System, GCS)간의 인증 및 송수신 되는 데이터들의 암호화가 필수적이다.

본 논문에서는 5G 특화망 네트워크 상에서 동작하는 드론 운용 환경에서의 인증 및 암호화를 위해 qSIM이라는 양자 엔트로피 칩 기반 하드웨어 암호모듈을 사용하는 인증 시스템을 제안한다.

Ⅱ. qSIM 기반 드론 인증 시스템

본 장에서는 논문에서 제안하는 양자 엔트로피 기반 암호모듈인 qSIM의 소개와 qSIM 기반 드론 인증 시스템을 제안한다.

2.1. qSIM (Quantum-based Subscriber Identity Module)

qSIM은 양자 엔트로피 칩(QEC, Quantum Entropy Chip)을 탑재한 양자 엔트로피 기반 암호모듈로 군이나 공공기관에서의 활용을 위해 KCMVP 암호모듈 보안 요구사항의 보안수준 2를 목표하는 하드웨어 암호모듈이다. 또한, 보안수준 2의 물리적 공격으로부터의 보호를 위해 불투명 경질체로 회로 보드를 보호하여 물리적 공격이 발생했을 시, 변조-증거가 발생한다.

[표 1]은 qSIM이 지원하는 KCMVP 검증대상 암호 알고리즘이며, qSIM은 아래 암호 경계 안에 알고리즘을 통해 암호 키와 응용 서비스의 인증정보 등을 암호화하여 저장할 수 있다.

암호 서비스	암호 알고리즘
블록암호	ARIA, LEA, AES ECB, CBC, CTR, GCM
해시함수	SHA2-256
메시지 인증	HMAC (SHA2-256), GMAC
난수발생기	Hash_DRBG (SHA2-256)
전자서명	ECDSA (P-256/SHA2-256)
키 설정	ECDH (P-256)
키 유도	PBKDF (HMAC-SHA2-256)

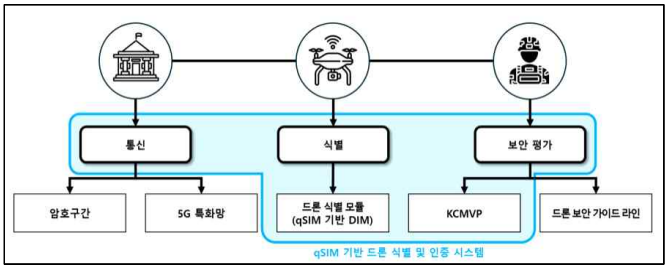
[표 1] 탑재된 검증대상 암호 알고리즘

2.2. qSIM 기반 드론 인증 시스템

아래 [그림 3]은 본 논문에서 제시하는 qSIM 기반 드론 인증 시스템이 공공 기관과 군에서 운용될 시의 충족되어야 하는 요소들의 블록도이다.

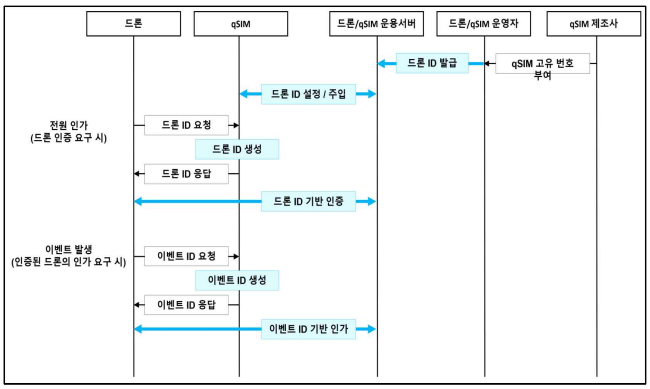
제안하고자 하는 드론 인증 시스템을 통해 드론 운용시에는 통신, 식별, 보안 요소가 필수적으로 필요하며, 각 요소들에 대한 세부사항은 다음과 같다.

- 통신 : 통신 구간은 암호 구간과 5G 특화망 네트워크로 분류할 수 있으며, 암호구간은 암호모듈을 통해 암호화 처리된 구간이고 5G 특화망은 5G 기술이 적용된 특정 주파수 내의 네트워크 통신 환경이다.
- 식별 : 하드웨어 암호모듈인 qSIM을 이용하여, 드론 인증을 수행한다. 드론 인증을 위해 사용되는 드론 ID 또는 식별 값은 qSIM 내부에 저장한다.
- 암호 : 드론의 데이터 보호 및 인증과 같은 보안 요소가 포함되고 이는 드론 보안 가이드 라인의 보안 요구사항에 충족되어야 하며, 공공기관 혹은 군에서 드론을 운용하기 위해서는 KCMVP 검증이 수행된 암호모듈이 탑재되어 암호화 및 인증을 수행해야 한다.



[그림 3] 제안하는 qSIM 기반 드론 인증 시스템 구성도

위 구성요소 중 [그림 3]과 같이 표시된 부분은 qSIM을 이용한 드론 인증 시스템 영역을 나타낸다.



[그림 4] qSIM 기반 드론 인증 시스템 구성도

[그림 4]에 따르면, 위에서 설명된 인증 시스템에 대한 절차는 다음과 같다.

1) qSIM은 제조사로부터 고유번호가 부여되어 제작된다.
2) 드론을 운용하는 기관의 운영자는 고유번호가 부여된 qSIM에 대해 드론 ID 또는 식별 값을 발급하고 이를 드론에 탑재하여 운용한다.
3) 드론의 ID 또는 식별 값은 qSIM 및 운용 서버에 설정되고 관리된다.
4) qSIM을 탑재한 드론은 첫 부팅시에 qSIM 기반 인증을 처리한다.
5) qSIM 내부에 저장되어 있는 드론 ID를 요청한다.
6) 드론은 qSIM으로 부터 드론 ID를 발급받는다.
7) 드론은 qSIM의 암호 알고리즘 처리와 드론 ID를 통해 운용 서버와 인증을 수행한다.

이러한 인증 절차를 통하여 유도된 키를 이용하여 드론과 운용 서버 간 인증을 요구하는 이벤트가 발생할 때 안전하고 빠른 인증을 수행할 수 있다. 아래 [표 2]는 위 인증 절차에 처리를 위해 사용되는 암호 알고리즘을 정리한 표이다.

qSIM 용도 구분	qSIM 내 암호 알고리즘
qSIM 고유 번호	-
드론 ID	Hash_DRBG(SHA2-256)
드론 인증	LEA (키 길이: 256-bit, GCM) HMAC (SHA2-256) Hash_DRBG (SHA2-256) ECDSA (P-256/SHA2-256)
이벤트 식별 정보	HMAC (SHA2-256)
키 관리	Hash_DRBG (SHA2-256) ECDH (P-256) PBKDF (HMAC-SHA2-256) LEA (키 길이: 256-bit, GCM)

[표 2] qSIM 기반 인증 시스템 처리 암호 알고리즘

인증 시스템의 절차가 구체화되기 위해서는 드론 운영환경에 적합한 보안 정책과 암호모듈이 요구되며, ID 기반의 인증뿐만 아니라 기기 인증서, qSIM 기반 암호 알고리즘 처리를 통해 인증을 수행하는 다양한 방식을 고려해야 한다.

Ⅲ. 결론

본 논문에서는 공공기관이나 군에서 운용되는 드론에 대한 데이터 보호 및 인증을 수행하기 위해 KCVMP 하드웨어 암호모듈인 qSIM을 이용한 드론 인증 시스템을 제안하였다. qSIM 기반 드론 인증 시스템을 적용함으로써, 공공기관 및 군에서 드론이 운용될 때에 드론 운용 기관에서는 정당한 드론을 인증하고 관리할 수 있을 것으로 기대된다.

향후에는 다양한 방식으로 처리되는 qSIM 기반 인증 시스템을 구현 및 구축함으로써, 인증 시스템의 가용성 및 추가 보안 요구사항에 대해 분석할 예정이다.

ACKNOWLEDGMENT

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(RS-2022-00207416, 안전한 차세대 IoT 통신 환경 구축을 위한 양자내성암호 최적화 및 보안 프로토콜 적용 연구)

참 고 문 헌

[1] 정보통신산업진흥원, “ICT Global Market Analysis, 품목별 ICT 시장동향 - 드론”, 2023년 11월 3일, pp. 3.