Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.5, Oct. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.5.891

무선랜 환경에서 양자 엔트로피 칩 기반 암호모듈을 적용한 드론 피아식별과 안전한 정보 제공 기술 제안*

정 서 우,[1†] 윤 승 환,[2] 이 옥 연[2‡]
[1,2]국민대학교 (대학원생, 교수)

A Proposal for Drone Entity Identification and Secure Information Provision Technology Using Quantum Entropy Chip-Based Cryptographic Module in WLAN Environment*

Seowoo Jung,[1†] Seunghwan Yun,[2] Okyeon Yi[2‡]
[1,2]Kookmin University (Graduate student, Professor)

요 약

세계적 관심과 함께 드론은 물품 수송, 산림 보호, 안전 관리 등 활용 분야의 저변을 확대해 나가고 있으며 드론은 활용 분야 확대 및 규모 확장에 따라 군사 작전, 환경 감시 등 다양한 분야에서 군집 비행이 응용되고 있다. 현재 국내에서는 특정 산업 분야의 서비스를 위한 이음 5G와 같은 특화망을 구축해 나가고 있다. 이와 관련하여 드론 시스템 또한 AI와 자율비행 등과 융합된 서비스를 제공하기 위해 특화망을 구축하려는 움직임이 보이고 있다. 드론이 여러 서비스와 융합됨에 따라 다양한 환경에서의 다양한 보안 위협 또한 종속되고 있으며, 이에 대응하여 국내에서는 드론 보안에 대한 요구사항과 가이드라인을 마련하고 있는 추세이다. 본 논문에서는 드론 시스템 중 드론의 군집 비행 시스템과 이를 위한 이음 5G와 같은 이동통신 특화망에서 무선랜과 양자 엔트로피 기반 난수 발생기를 탑재한 암호모듈을 활용하여 군집 비행 드론 간 피아식별 및 안전한 정보 제공 기술 방법을 제안하고, 구현에 참고할 수 있는 테스트 벡터를 제공한다.

ABSTRACT

Along with global interest, drones are expanding the base of utilization such as transportation of goods, forest protection, and safety management, and cluster flights are being applied in various fields such as military operations and environmental monitoring. Currently, specialized networks such as e-UM 5G for services in specific industries are being established in Korea. In this regard, drone systems are also moving to establish specialized networks to provide services that are fused with AI and autonomous flight. As drones converge with various services, various security threats in various environments are also subordinated, and in response, requirements and guidelines for drone security are being prepared in Korea. In this paper, we propose a technology method for peer identification and safe information provision between cluster flight drones by utilizing a cryptographic module equipped with wireless LAN and quantum entropy-based random number generator in a cluster flight system and a mobile communication network such as e-UM 5G.

Keywords: Drone Identification, UAV, Quantum random number generator

Received(07. 05. 2022), Modified(09. 27. 2022), Accepted(09. 27. 2022)

* 본 연구는 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00085, 5G+ 기반 6G 이동통신 정보보안 기술 연구)

* 본 논문은 2021년도 한국정보보호학회 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임

† 주저자, plourve@kookmin.ac.kr

‡ 교신저자, oyyi@kookmin.ac.kr(Corresponding author)

I. 서 론

4차 산업혁명 시대로 접어들면서 전 세계가 드론 산업에 주목하게 되어 군용으로 개발된 드론은 현재 군뿐만 아니라 농업, 산업, 물류 등 다양한 분야에서 활용되고 있다. 또한, 2019년을 시작으로 초연결, 초저지연, 초고속을 기반으로 하는 5G 시대가 도래하면서 여러 IoT 기기 및 드론 등 다양한 기기가 초연결을 이룰 수 있게 되었다. 이렇게 다양한 기기별로 지역에 다수의 연결을 제공하기 위해 사업자가 직접 5G 망을 구축하여 특정 구역 단위로 5G 주파수를 활용하는 통신망인 이음 5G(5G 특화망)가 등장하였다. 현재 로봇, AI, 자율주행 등의 분야와 융합되어 동작하는 스마트 팩토리, 스마트 팜, 클라우드 시스템들이 많은 양의 데이터를 신속하게 처리하기 위해 이음 5G(e-UM 5G, 5G 특화망, Private 5G)를 사용하고 있다. 드론 시스템 또한 최근 몇 년 사이에 막대한 규모 확장을 경험하였고, 이에 따라 드론을 활용한 서비스의 수와 규모는 점점 증가하는 추세다. 다수의 드론을 활용한 시스템을 운영하고, 해당 시스템에서 수집된 정보를 가공하는 2차 서비스를 생각해 볼 때, 드론 시스템에 대한 이음 5G 설계는 먼 미래가 아니다. 최근 드론의 규모 확장과 더불어 드론의 활용 분야가 확대되고, 많은 수의 기기가 연결됨에 따라 네트워크에 흐르는 트래픽의 양이 대폭 증가하였다. 드론 시스템에서 부유하는 데이터의 양과 질이 증가하면서 보안 위협으로 발생할 수 있는 경제적, 인명적 피해 또한 비례하여 증가할 것이고, 그에 따라 드론 역기능 문제와 함께 드론 보안의 중요성이 대두되고 있다. 특히 2018년 평창 동계 올림픽 개막식에서 보인 군집 비행 같은 경우, 다수의 드론을 안전하게 제어하기 위해서는 각각의 드론 개체에 대한 피아식별이 필수적이다. 군집 비행 시, 수십, 수백 대의 드론을 가시권 내에서 조종하기 어렵기 때문에 드론 간의 충돌 방지를 위해 각 개체 간 위치 정보를 실시간으로 주고받으며 제어 명령 전달 및 임무 수행을 해야 한다. 그러나 이러한 위치 정보는 드론의 중요 데이터기 때문에 평문으로 노출되면 보안 위협이 발생할 수 있다. 그뿐만 아니라, 모선 역할을 하는 리더 드론이 제어를 원활하게 하기 위해서는 수집한 데이터에 대한 보안이 필수적이다. 데이터에 기밀성, 무결성 등 보안을 적용하기 위해서는 사전에 인증 및 키 교환 과정이 요구된다. 따라서 본 논문에서는 드론의 군집 비행 시스템과 이를 위한 이음 5G와 같은 이동통신 특화망에서 무선랜(wireless LAN)과 양자 엔트로피 기반 난수 발생기가 탑재된 암호모듈(이하 양자 암호모듈)을 활용한 인증 및 키 교환 방법을 제안하고, 구현에 참고할 수 있는 테스트 벡터를 제공한다.

II. 관련 연구

2.1 연구의 필요성

무인항공 시스템(Unmanned Aircraft System, UAS)은 무인항공기(UAV, Unmanned Aerial Vehicle) 또는 통칭 드론과 지상조종국(GCS, Ground Control System)으로 구성된다[1]. 일반적인 무인항공 시스템의 구성도는 Fig 1과 같다.

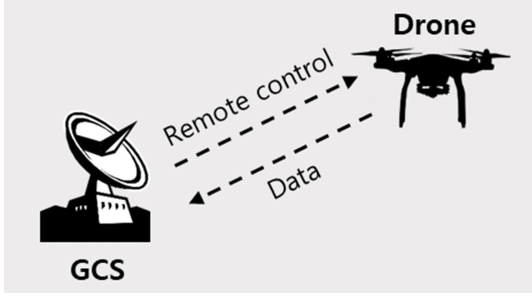

Fig. 1. General UAS system

일반적으로 지상조종국에서 드론을 원격으로 제어하지만, 상공을 비행 중인 드론은 육안으로 식별하기 어렵기 때문에 보안 위협을 사전에 방지하기 위해서는 비행 중 새롭게 출현한 드론 개체에 대한 피아식별이 필수적이다. 그뿐만 아니라 군집 비행 시 위성통신이나 광대역 무선랜을 사용하여 미션을 수행해야 하는 경우에는 다수의 드론을 가시권 내에서 제어하기 어렵다. 따라서 비행 중 드론 간의 충돌을 방지하기 위해서는 각 개체 간 위치 정보를 실시간으로 주고받으며 제어 명령을 내려야 한다. 그러나 이러한 위치 정보와 제어 데이터는 드론의 중요 데이터기 때문에 아군이 아닌 사용자에게 평문으로 노출되면 보안 위협이 발생할 수 있다. 이를 방지하기 위해서는 군집 비행 중 새롭게 출현한 드론에 대해 피아식별이 필요하다. 그뿐만 아니라 모선 역할을 하는 리더 드론이 하위 드론의 제어를 원활하게 하기 위해서는 안전한 데이터의 전달 또한 필요하다. 따라서 각 드론

의 위치 정보를 안전하게 공유하고, 드론의 안전한 비행을 위해서는 드론 개체에 대한 피아식별과 데이터 보안이 필수적이다.

또한, 드론 시장이 확대되면서 충돌, 테러와 같은 공격 행위와 불법적인 사용이 증가하여 많은 인명적, 경제적 피해를 초래하고 있다. 그에 따라 드론을 탐지하고 피아식별한 뒤, 무력화시키기 위한 안티 드론(Anti-Drone) 기술이 주목받고 있다. 프랑스의 내무부는 드론의 전자적 식별에 대해서 비컨은 2.4 GHz Wi-Fi 기술을 이용하고 제조사 코드, 드론 고유번호, 고도, 경도, 위도, 속도 등을 최소 3초에 2번 주기로 전송해야 한다고 제안하였다. 최근 각 나라에서는 드론 식별을 위해 항공기에 사용되는 자동종속감시시설-방송(ADS-B, Automatic Dependent Surveillance -Broadcast)과 같은 전자적 식별 방식을 차용한 드론 식별 체계를 마련하고 있다. 그러나 이는 암호학적 보안 요소가 포함되어 있지 않은 방식이며 이와 같은 방법을 고려하기 위해 국내·외에서 암호학적 보안 요소를 요구하는 표준화된 드론 식별 방법인 드론 식별 모듈(DIM, Drone Identification Module)의 기술 및 표준화 제정에 대한 연구가 진행되고 있다[2]. 이에 따라 본 논문에서는 드론의 군집 비행 시스템과 이를 위한 이음 5G와 같은 이동통신 특화망에서 무선랜과 양자 암호모듈을 활용하여 피아식별을 수행한 뒤, 식별된 드론 간의 안전한 정보 제공 기술을 제안하고, 구현에 참고할 수 있는 테스트 벡터를 제공한다.

2.2 이음 5G

이음 5G란 5G 기술을 이용하여 건물, 공장 등 특정 구역 내에서 도입하고자 하는 특정 서비스에 최적화된 5G 네트워크다. 이음 5G 기술은 지역적으로 주파수를 공동 사용하는 5G 특화망으로, 사업장 내의 합법적인 통신 구역을 보장하고, 인접한 타 특화망으로부터의 간섭을 사전에 차단하는 것을 목적으로 한다[3].

기존의 통신사에서 제공하는 5G 기술을 사용하는 경우에는 통신사에서 제공하는 무선 구간에서의 보안만 적용되며, 사용자 혹은 개체 간의 end-to-end 보안은 적용되지 않는다. 따라서 본 논문에서는 드론의 군집 비행 시스템과 이를 위한 이음 5G와 같은 이동통신 특화망이 구축된 환경 내에서 무선랜과 양자 암호모듈을 이용하여 피아식별을 위한 인증 및 키 교환 방법을 제안한다.

2.3 양자 암호모듈의 필요성

드론 간의 피아식별을 수행할 때, 드론의 식별정보를 이용하여 수행할 수 있다. 드론의 식별정보는 국가 코드, 생산자 번호, 모델 번호, 일련번호의 연접된 형태로 구성될 수 있다[2]. 그러나 이러한 고유 식별정보는 드론 운영자가 아니더라도 예측 가능하기 때문에 본 논문에서는 식별을 위해 고유 식별정보 대신 난수를 이용한다.

난수의 요구 조건으로는 예측 불가능성, 비편향성, 독립성이 있다. 난수발생기는 유사난수 발생기(PRNG, Pseudo Random Number Generator)와 진난수 발생기(TRNG, True Random Number Generator)로 분류되는데, 진난수 발생기는 열잡음, 전기잡음 등 물리적 잡음을 이용하는 발생기와 양자역학적 성질을 이용하는 양자난수 발생기(QRNG, Quantum Random Number Generator)가 있다[4]. 암호학적으로 안전한 난수발생기 구조는 아래의 그림과 같다.

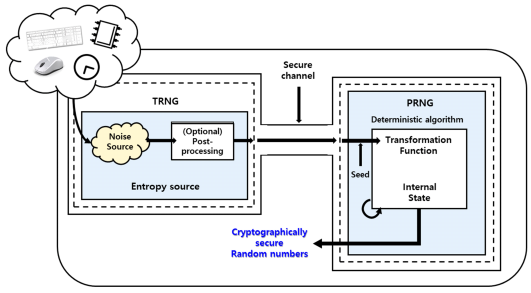

Fig. 2. Cryptographically secure RNG[5]

암호학적으로 안전한 난수발생기 구조는 TRNG와 PRNG를 함께 사용하는 것이다. 즉, TRNG의 출력을 PRNG의 seed(초기값)으로 사용하여 난수를 생성하는 것이다. 여기서 암호학적 난수발생기의 안전성은 TRNG가 생성하는 seed의 안전성에 의해 결정된다.

기존의 드론은 OpenSSL 등 오픈소스 암호 라이브러리를 사용하여 난수를 생성한다. 오픈소스 암호 라이브러리는 키보드 같은 외부 주변 장치, 중단 요청 시간, 디스크 읽기·쓰기 시간 등 PC에서 사용 가능한 사용자 입력 리소스로부터 잡음원을 수집한다.

그러나 드론에는 이러한 주변 기기가 없고, 일부 드론에는 인터럽트 요청 시간과 디스크 읽기·쓰기 시간을 관리하는 운영체제가 없어 충분한 잡음원을 수집할 수 없다[6].

이에 본 논문에서는 이동통신 특화망이 구축된 환경 내에서 양자 암호모듈에서 생성한 안정적인 양자 엔트로피 기반 난수(이하 양자난수)를 이용하여 피아식별을 위한 인증 및 키 교환 방법을 제안하고, 구현에 참고할 수 있는 테스트 벡터를 제공한다.

III. 기술 구현 방법

3.1 기술 구성

본 논문에서 제안하는 기술의 구성도는 Fig 3과 같다. 드론 1은 리더 드론으로, GCS와 하위 드론들 사이에서 MEC(Multi-access Edge Computing)와 유사한 역할을 수행한다. MEC란, 셀룰러 네트워크 edge에서 클라우드 컴퓨팅 기능과 IT 서비스를 가능하게 하는 아키텍처 개념으로, 현재 ETSI에서

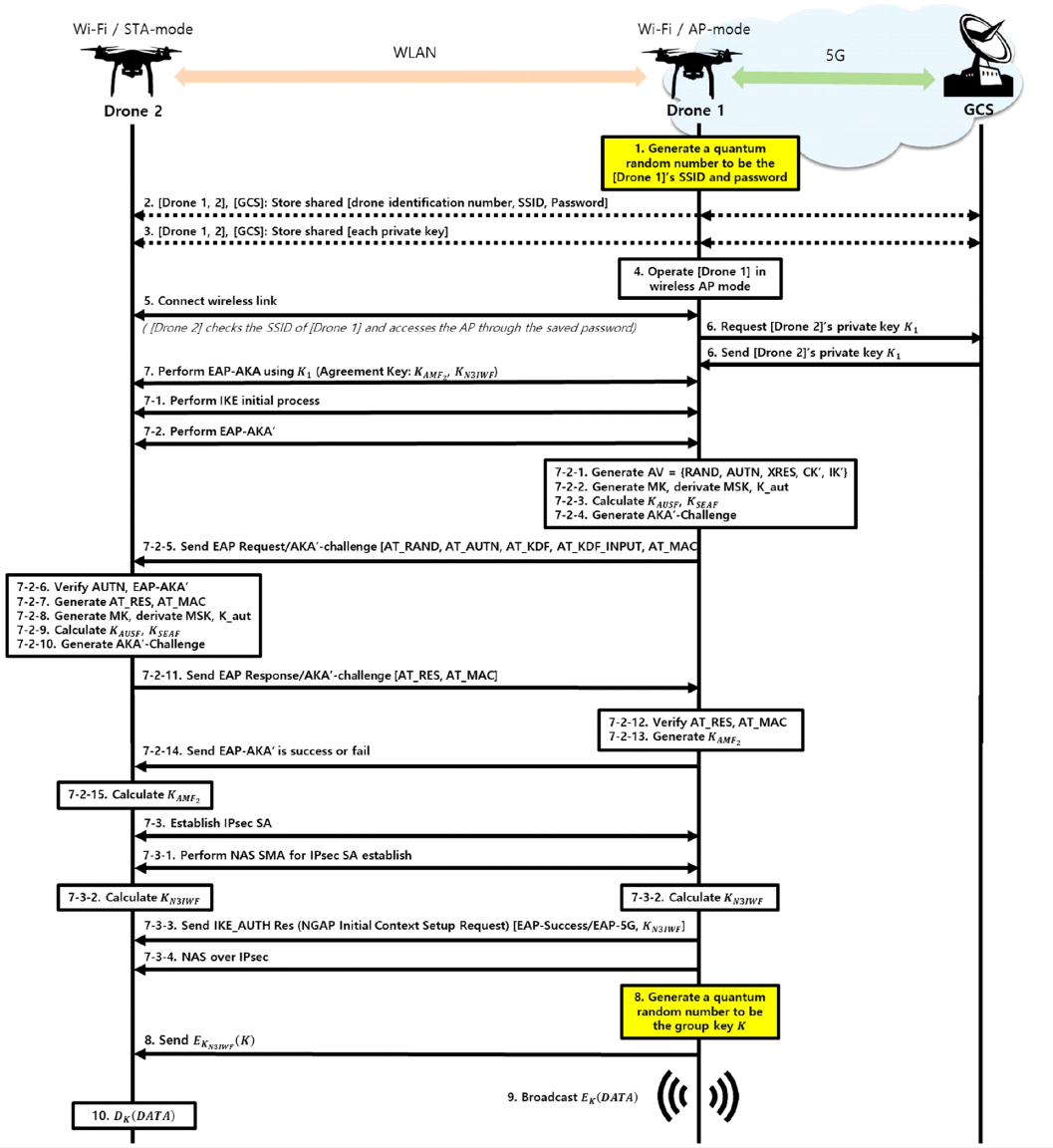

Fig. 3. Process of proposed scheme

표준을 제정 중이다.

드론 1은 군집 비행 중 드론 개체 간의 인증, 혹은 새롭게 출현한 드론의 피아식별을 위한 인증 및 키 교환 과정을 수행한 뒤 위치 정보, 제어 데이터 등의 데이터를 암호화하여 전송한다. 제안하는 기술의 구성도에서 리더 드론인 드론 1과 GCS 사이의 통신은 5G/LTE를 이용하고 이동통신망을 통해 GCS와 연결되어 있다고 가정한다. 또한, 드론 1과 그 외의 하위 드론들은 무선랜으로 통신한다고 가정한다. 데이터 보안을 제공하기 위한 인증 및 키 교환 과정은 Fig 3과 같다.

① 군집 비행을 수행하기 전, 리더 드론의 SSID(Service Set Identifier)로 사용할 128-bit의 양자난수와 패스워드로 사용할 128-bit의 양자난수를 생성한다.
② ①에서 생성한 SSID와 패스워드를 리더 드론의 고유 식별번호와 매핑시켜 테이블을 생성한 뒤 군집 비행에 참여할 모든 드론의 내부에 저장한다.
③ 각 드론은 서로 다른 비밀키($K_1, K_2, \ldots$)를 GCS와 공유하여 저장한다.
④ 드론 1을 무선 AP(Access Point) 모드로 동작시킨다. 이때 드론 1의 SSID는 ②에서 드론의 고유 식별번호와 매핑시킨 양자난수이다.
⑤ 비행 중, 드론 2는 드론 1의 SSID가 저장한 테이블 내에 있는지 확인한 뒤 패스워드를 입력하여 AP에 접속한다.
⑥ 접속에 성공하면 드론 1은 GCS에게 드론 2의 비밀키 K_2를 요청한 뒤 수신한다.
⑦ 드론 1은 K_2를 이용하여 드론 2와 non-3GPP interworking 방식의 EAP-AKA'(Extensible Authentication Protocol-Authentication and Key Agreement Prime)[7]을 통해 상호 인증 및 키 교환을 수행한다. 이때 상호 인증 및 키 교환을 수행하여 공유된 키는 K_{N3IWF_2}(N3IWF: Non-3GPP InterWorking Function)가 된다.
⑧ 인증 및 키 교환에 성공하면 드론 1은 그룹 키 K가 될 128-bit의 양자난수를 생성하여 K_{N3IWF_2}로 암호화한 뒤, 드론 2에게 전송한다. 이때 K_{N3IWF_2}는 KEK(Key Encryption Key)가 된다.
⑨ 드론 1은 전송한 그룹 키로 암호화한 위치 정보 및 수집한 데이터, 제어 데이터 등을 자신의 무선랜에 접속한 모든 개체에게 브로드캐스트로 전송한다.
⑩ 드론 1의 무선랜에 접속한 모든 개체 중 그룹 키 수신에 성공한 개체는 브로드캐스트로 수신한 메시지를 복호화한다.

위와 같은 과정을 AP 모드로 동작하는 드론 1의 무선랜에 접속한 모든 드론과 동일하게 수행하여 군집 비행용 그룹 키 K를 공유한다. ⑨와 ⑩에서 수행하는 암·복호화 과정은 경량 암호알고리즘인 LEA를 사용한다.

SSID는 2—32개의 문자열로, 출력 가능한 문자와 공백만 가능하기 때문에[8] 먼저 128-bit의 양자난수를 생성한 뒤, 생성한 난수를 string 형태에서 hex 형태로 변환한 256-bit 값을 사용한다. SSID 변환 방법은 Fig 4와 같다.

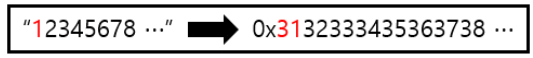

Fig. 4. Changing a string to SSID

본 논문에서는 무선랜 환경뿐만 아니라 다양한 환경에서 동작하는 드론 시스템에 적용할 수 있는 EAP 방식을 이용하여 피아식별을 위한 상호 인증 및 키 교환 방법을 제안한다. 이때 인증에 참여하는 개체인 하위 드론은 non-USIM 환경에서 동작하는 단말로서 non-3GPP interworking 방식을 사용한다. untrusted non-3GPP access를 위한 인증 및 키 교환 과정은 EAP-AKA' 혹은 5G-AKA를 이용하는 IKEv2(Internet Key Exchange version 2)[9] 방식이 있으며[7], 본 논문에서는 EAP-AKA'을 사용한다. EAP-AKA' 과정에서 사용되는 AES 등의 블록암호 알고리즘은 LEA로 대체한다. LEA는 암호화를 위한 모든 라운드 함수가 ARX(Addition, Rotation, XOR) 연산으로만 구성되어 있기 때문에 AES에 비해 연산 과정이 간단하여 훨씬 효율적이다. 리소스가 제한된 소형 장치를 위해 설계된 LEA는 코드 크기가 작고, 전력 소비가 작기 때문에 리소스가 제한된 드론 환경에 적합하다[12]. 따라서 본 논문에서는 국내 환경에 맞춰 경량 암호알고리즘인 LEA로 대체한다.

3.2 테스트 벡터

본 논문에서 제안하는 기술 구현을 위한 테스트 벡터는 Table 1과 같다. 이는 Fig 3에 명시된 단계별 과정에 대해 구현에 참고할 수 있는 테스트 벡터이다.

IV. 결 론

본 논문에서는 이음 5G와 같은 이동통신 특화망이 구축된 환경 내에서 무선랜과 양자 암호모듈을 이용하여 피아식별을 위한 인증 및 키 교환 방법과 안전한 정보 제공 기술 구현 방법을 제안하였다. 이처럼 암호학적으로 보안이 적용된 이처럼 암호학적 보안이 적용된 피아식별 및 정보 제공이 이루어진다면, 무선랜 환경 내에서 보다 안전한 드론 운용이 가능할 것으로 기대된다.

향후 연구에서는 드론의 식별 및 안전한 정보 제공을 위하여 국내 환경의 5G+ 기반 이동통신 환경에 적용할 수 있는 기술 연구를 수행할 계획이다.

References

[1] KATS and KSA, "Industry Guide for Global Technical Regulations on Drone (Unmanned Aircraft)," TBT Policy Report 005, Jan. 2018.

[2] "ISO license and drone identity module for drone (Ultra light vehicle or unmanned aircraft system) - Part 1: Physical characteristics and basic data sets for drone licence," ISO/IEC CD 22460-1.2, Oct. 2020.

[3] DaeHong Min, YongHee Shin, and JeeYoung Ahn, "Research on the Trend in Private 5G Introduction in a Foreign Country," Electronics and Telecommunications Trends. Vol. 35, No. 5, pp. 139-150, Oct. 2020.

[4] JungMin Park, SeongJoon Cho, TaeJin Lim, and Mark Tehranipoor, "QEC: A Quantum Entropy Chip and Its Applications," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, pp. 1471-1484, June. 2020.

[5] Elaine Barker, John Kelsey, Kerry McKay, Allen Roginsky, and Meltem Sönmez Turan, "Recommendation for Random Bit Generator (RBG) Constructions," NIST SP(Special Publication) 800-90C, Apr. 2016.

[6] SEONG-MIN CHO, EUNGI HONG, and SEUNG-HYUN SEO, "Random Number Generator Using Sensors for Drone," IEEE Access, vol. 8, pp. 30343-30354, Feb. 2020.

[7] Maurice Pope and Mirko Cano Soveri, "Security architecture and procedures for 5G system (Release 17)," 3GPP TS 33.501, V17.6.0, June. 2022.

[8] C. Kaufman, Ed., "Internet Key Exchange (IKEv2) Protocol," RFC 4306, Dec. 2005.

[9] CISCO, "SSID naming", https://www.cisco.com/assets/sol/sb/WAP321_Emulators/WAP321_Emulator_v1.0.0.3/help/Wireless05.html, Oct. 2021.

[10] Mirko Cano Soveri, "Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5* (Release 17)," 3GPP TS 35.208, V17.0.0, Mar. 2022.

[11] J. Arkko, V. Lehtovirta, V. Torvinen, and P. Eronen, "Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA')," RFC 9048, Oct. 2021.

[12] Donggeon Lee, Dong-Chan Kim, Daesung Kwon, and Howon Kim, "Efficient Hardware Implementation of the Lightweight Block Encryption Algorithm LEA," MDPI, Sensors, vol. 14, pp. 975-994, Jan. 2014.

V. 부 록

Table 1. Test vector for reference[7][10][11]

Parameter	Value (Hex string)	Length (Bits)	Step
K	5122250214C33E723A5DD523FC145FC0	128	Prerequisites
RAND	81E92B6C0EE0E12EBCEBA8D92A99DFA5	128	
SQN	16F3B3F70FC2	48	
AMF	C3AB	16	
OP	746F7279746F7279746F746F72797279	128	
OP_C	9BD18D07D3D8CD86D3094B640B9D8D77	128	
f1	EC49AD04ED395130	64	
f1*	6CDC87615DD5102A	64	
f2	47A4E939FDE1954E	64	
f5	2FECB7D270EE	48	
f3	8A8FDCF34AB2699817ADBA11D8A283C7	128	
f4	76D5E0EDF739B6CE1CBD7893BC99AEAA	128	
f5*	D1E1086E618E	48	
Identity	30353535343434333333323232313131	128	
Network name	574C414E	32	
RAND	81E92B6C0EE0E12EBCEBA8D92A99DFA5	128	Figure 2, 7-2-1
AUTN	391F04257F2CC3ABEC49AD04ED395130	128	
CK	8A8FDCF34AB2699817ADBA11D8A283C7	128	
IK	76D5E0EDF739B6CE1CBD7893BC99AEAA	128	
RES, XRES	47A4E939FDE1954E	64	
CK'	57BC5E6F37679518D1497A09513B7fE5	128	
IK'	ABCAE830AB3470BBBF1285FE930E9585	128	
MK	E6C5E4C00510B426F29528695FF6F725909ED915FAE71C806F30DD9D287A78171BAB1B005D8DD37F83B636DEF30897ADFB3A0A90080599F00B3F3084AED607108513FFEEA7F664024E3B02A1059F6BD6CE732CB8B404C2F27B3260B31EFF864F618EE5D99E9C573EA9A9532BE17824CC488C064BAB79C734310DDC0A56FE270298C4085400B228201979DE2B8BEEF11443997A6AE9C8422101D9758FED834D6F41D93AD123438DB78E7722D2FAC5AEDE078DBDCDA660A45A33E1FE4DD62A9901FBB0714FA220D9CDE63798B3CA4125DD	1,664	Figure 2, 7-2-8
K_{encr}	E6C5E4C00510B426F29528695FF6F725	128	
K_{aut}	909ED915FAE71C806F30DD9D287A78171BAB1B005D8DD37F83B636DEF30897AD	256	

Parameter	Value (Hex string)	Length (Bits)	Step
K_{re}	FB3A0A90080599F00B3F3084AED607108513FFEEA7F664024E3B02A1059F6BD6	256	Figure 2, 7-2-8
MSK	CE732CB8B404C2F27B3260B31EFF864F618EE5D99E9C573EA9A9532BE17824CC488C064BAB79C734310DDC0A56FE270298C4085400B228201979DE2B8BEEF114	512	
EMSK	43997A6AE9C8422101D9758FED834D6F41D93AD123438DB78E7722D2FAC5AEDE078DBDCDA660A45A33E1FE4DD62A9901FBB0714FA220D9CDE63798B3CA4125DD	512	Figure 2, 7-2-8
K_{AUSF}	CE732CB8B404C2F27B3260B31EFF864F618EE5D99E9C573EA9A9532BE17824CC	256	Figure 2, 7-2-3, 7-2-9
K_{SEAF}	4A035895A2AC0C059880FD762BE71357DE0AF0B97F0D18BC43B42097461B3921	256	Figure 2, 7-2-3, 7-2-9
K_{AMF}	98A5D883ACD8DB6E09B4AA39FBC7DE859B87112175CCFCFDE78E71057FC8D6BB	256	Figure 2, 7-2-13, 7-2-15
K_{N3IWF}	2B754BE1674F43F03C86F0EA54116FC88EF180E1914DD629B2D9F9A80BC5C5B5	256	Figure 2, 7-3-2

〈저자소개〉

정 서 우 (Seowoo Jung) 학생회원
2021년 2월: 국민대학교 정보보안암호수학과 졸업
2021년 2월~현재: 국민대학교 금융정보보안학과 석사과정
〈관심분야〉 드론 보안, IoT 보안, 5G/6G 보안, KCMVP

윤 승 환 (Seunghwan Yun) 종신회원
2005년 2월: 국민대학교 수학과 졸업
2007년 2월: 국민대학교 수학과 석사
2019년 2월: 국민대학교 금융정보보안학과 박사
2019년 3월~현재: 국민대학교 전임연구교수
〈관심분야〉 암호모듈, 양자난수, 5G+ 보안, CMVP

이 옥 연 (Okyeon Yi) 종신회원
1988년 2월: 고려대학교 수학과 졸업
1990년 2월: 고려대학교 수학과 석사
1996년 8월: Univ. of Kentucky 박사
〈관심분야〉 5G/6G 보안, 위성통신 보안, KCMVP