논문 20-45-04-19 The Journal of Korean Institute of Communications and Information Sciences '20-04 Vol.45 No.04
https://doi.org/10.7840/kics.2020.45.4.756

PUF-OTP를 활용한 LTE 기반 드론봇 전투체계의 인증 강화방안

윤 상 열◆, 이 수 진°

A Study on the Enhancement of Authentication in LTE-Based Dronebot Combat System Using PUF-OTP

Sangyeol Yun◆, Soojin Lee°

요 약

드론봇 전투체계는 미래 전장에서 핵심 게임 체인저로서의 역할을 담당할 것으로 평가받고 있다. 그러나 무선통신을 기반으로 운용되는 드론의 특성상 다양한 사이버 위협에 노출될 수 있다. 그리고 4G LTE 또는 5G 네트워크 등 전송속도나 서비스 품질에 중점을 두고 개발된 상용 이동통신기술을 드론봇 전투체계의 기반 네트워크로 활용할 경우 안전성과 신뢰성을 보장하기 위한 대책이 반드시 강구되어야 한다. 이에 본 논문에서는 육군이 개발을 추진하고 있는 드론봇 전투체계가 4G LTE 네트워크를 기반으로 운용됨을 가정하고 개선된 인증을 통해 보안성을 강화하는 방안을 제시한다. 제시된 개선방안은 PUF(Physical Unclonable Function)와 OTP(One Time Password)가 결합된 PUF-OTP를 활용하여 4G LTE 네트워크에 적용되고 있는 EPS-AKA 인증절차를 강화한다. 하드웨어의 고유 지문으로서 물리적 복제가 불가능한 PUF 출력값을 OTP의 입력으로 적용함으로써 기존 EPS-AKA가 가지는 다양한 보안취약점을 제거하고 보안성을 강화한다. 그리고 대규모 드론으로 구성되는 군집 드론봇을 운용하는 경우에는 CRP(Challenge Response Table) 테이블에 의한 인증 지연이 발생할 수 있음을 고려하여 CRP 테이블 사용을 배제하고 인증절차를 구성한다. 또한, 4G LTE 네트워크가 기반 네트워크로서의 역할을 수행하지 못할 경우를 대비하여 지상통제소와 드론봇이 PUF-OTP를 활용해 직접 인증을 수행할 수 있는 방안도 포함하고 있다.

Key Words : Dronebot, PUF, OTP. LTE, Authentication, Security

ABSTRACT

Dronebot combat system is considered to be in charge of its role as a key game changer on the future battlefield. However, due to the nature of drones using the wireless communication, they can be exposed to various cyber threats. And when commercial mobile communication technology developed with emphasis on transmission speed or quality of service, such as 4G LTE or 5G network, is utilized as the underlying network of dronebot combat system, measures must be taken to ensure security. This paper assumes that the dronebot combat system, which the ROK Army is currently operating on the basis of the 4G LTE network, and proposes ways to enhance security through improved authentication. Proposed approach enhances the EPS-AKA authentication procedure applied to 4G LTE network by utilizing PUF-OTP, various security vulnerabilities of

◆ First Author : Ajou University, Department of Defense Digital Convergence, rotc323@ajou.ac.kr, 학생(박사), 정회원
° Corresponding Author : Korea National Defense University, Department of Defense Science, Cyberkma@gmail.com, 정교수, 정회원
논문번호 : 201911-312-A-RE, Received November 19, 2019; Revised January 21, 2020; Accepted February 2, 2020

existing EPS-AKA are eliminated and security is enhanced. In addition, the authentication procedure was organized by excluding the use of the CRP table in consideration of possible delay in authentication by the CRP table when operating a large number of dronebots. We also suggest ways to allow ground control stations and dronebot to perform the authentication process using the PUF-OTP in case the 4G LTE network fails.

Ⅰ. 서 론

지난 몇 년 간, 드론은 사람이 도달할 수 없거나 불가피하게 위험에 노출될 수밖에 없는 장소 또는 사람에 의해서는 시기적절하고 효율적인 임무수행이 제한되는 환경에서 다양한 기능을 수행하면서 그 효용성을 입증해왔다. 군사분야에서도 불필요한 인명손실을 줄이고 시간에 민감한 임무를 수행할 수 있다는 높은 편의성 때문에 평시 또는 다양한 분쟁상황 하에서 다수의 군사작전에 활용되었다.

우리 군도 향후 군사작전 수행에 있어 드론의 중요성을 깊이 인식하고 있으며, 육군은 미래 전장의 판도를 뒤바꿀 게임 체인저로서 드론봇 전투체계 구축을 추진하고 있다. '드론봇 전투체계 비전 2030'을 공개하면서, 드론봇 군사연구센터, 드론 교육센터, 드론봇 전투단을 창설하여 운용개념 구체화 및 전투실험 등을 진행하고 있다. 그러나 드론봇 전투체계가 미래 전장을 주도하는 게임 체인저로서의 역할을 확실하게 수행하기 위해서는 다양한 요소들이 검토되고 검증되어야만 한다. 특히 무선통신을 기반으로 운용되는 드론의 특성상 각종 사이버위협에 쉽게 노출될 수 있음을 고려하면 사이버보안 강화를 위한 대책은 반드시 마련되어야 한다.

현재 드론봇 전투체계를 위한 기반 통신체계는 아직 확정되지 않았으며, 군사용 통신체계나 4G LTE 및 5G 등의 상용 통신체계 또는 현재 데이터링크 등이 적용대상으로 검토될 수 있다. 물론 드론봇 전투체계의 기반 네트워크는 운용개념이 다른 무기체계와의 상호운용성 등을 종합적으로 고려하여 선정되겠지만, 현재 수준에서의 기술적 성숙도, 지상통제소(GCS, Ground Control System)에서 가시선(LOS, Line Of Sight) 통신거리 밖까지 드론봇을 제어할 수 있다는 점 등을 고려하면 4G LTE 네트워크가 상당히 유력한 검토대상이 될 수 있을 것이다[1]. 이에 본 연구에서는 드론봇 전투체계의 기반 네트워크를 4G LTE로 가정하고, 드론봇 전투체계의 보안성을 강화할 수 있는 방안을 제안한다.

4G LTE는 EPS-AKA라는 표준 인증절차를 따르고 있기는 하지만, 전송속도와 서비스 품질을 우선 고려하여 개발되고 진화되어 온 기술이기 때문에 다양한 보안취약점을 가지고 있다. 우선 이동통신기기가 네트워크에 접속하는 과정에서 기기인증을 요청하기 위해 전송하는 '사용자 가입정보(IMSI, International Mobile Subscriber Identity)'가 평문으로 전송된다. 이 사용자 가입정보는 노출될 경우 복제를 통해 동일한 가입정보를 가진 기기를 만들 수 있으며, 경쟁조건 공격 등 복잡한 사이버공격의 수행까지 가능해진다. 그리고 인증과정에서 고정된 암호키(LTE K)가 지속적으로 사용되고 있으며 해당 키가 노출될 경우에는 인증과정 전체가 무력화될 수 있다는 문제점을 안고 있다.

본 연구에서는 드론봇 전투체계의 기반 네트워크로서 활용이 가능한 4G LTE의 EPS-AKA가 가지는 이러한 보안취약점을 해결하기 위해 물리적 복제방지기술(PUF, Physical Unclonable Function)과 OTP(One Time Password)가 결합된 PUF-OTP를 활용한 개선된 기기 인증방안을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 PUF와 OTP의 개념 및 특징에 대해 간략하게 살펴보고, 4G LTE 네트워크의 EPS-AKA가 가지는 보안취약점을 분석한다. 3장에서는 이러한 보안취약점을 제거하고 보안성을 강화하기 위해 PUF-OTP 기반의 개선된 EPS-AKA를 제안하고, 안전성을 분석한다. 마지막으로 4장에서 연구결과를 정리하고 결론을 맺는다.

Ⅱ. 관련 연구

2.1 PUF(Physical Unclonable Function) Technology

PUF는 IC(Integrated Circuit) 회로의 물리적인 특성으로 동일한 공정으로 생산된 회로라도 같은 입력값에 대해 서로 다른 출력값을 생성하며, 물리적으로 복제할 수 없다는 특징을 가진다[6]. 즉 공격자가 PUF를 복제하더라도 원래의 PUF가 특정 입력에 대해 생성하는 특정 출력값을 동일하게 생성하는 것은 불가능하다.

다양한 PUF 회로 중 그림 1.과 같은 Arbiter PUF는 회로의 입력값에 의해 지연(delay) 경로가 결정되

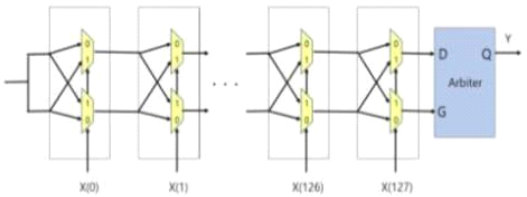

그림 1. Arbiter PUF 회로의 지연 경로
Fig. 1. Delay path of the Arbiter PUF circuit

며 어떤 Path의 값이 먼저 도착하느냐에 따라 출력값이 결정된다. 또한, 같은 지연 경로가 설정되더라도 각 회로 소자가 가지고 있는 하드웨어적 특성으로 인해 각 PUF 회로마다 출력값이 다르게 나타난다.

이러한 특징 때문에 PUF는 Challenge-Response 인증이나 키 생성 알고리즘으로 자주 사용되고 있다. 인증에 활용될 경우에는 PUF가 특정 입력에 대해 출력하는 값의 쌍을 다수 생성하여 CRP(Challenge Response Pairs) 테이블을 구성하고 이를 인증서버에 저장한다. 특정 기기가 인증을 요청하면 인증서버는 특정 입력에 해당하는 Challenge 값을 기기에게 전송하고, 해당 기기에서는 PUF를 통해 전송받은 Challenge에 대한 Response를 생성하여 인증서버로 전송한다. 인증서버는 전송된 Response와 서버 내 저장되어 있는 Response의 일치 여부 확인을 통해 해당 기기를 인증한다. 키 생성 과정에서는 PUF의 출력값을 해쉬함수의 입력으로 사용하여 비밀키를 생성할 수 있다.

2.2 OTP(One Time Password) Technology

OTP는 비밀번호 입력을 수행할 때마다 이전과 다른 새로운 비밀번호를 생성하여 인증하는 인증 수단이다. 매번 변경되는 일회용 패스워드를 사용하므로 정보가 노출되더라도 그 정보는 매우 짧은 시간만 유효하여 재사용 공격은 불가하다. OTP는 OTP 생성 알고리즘에 고정된 랜덤수인 비밀키와 매 세션 변경되는 데이터 값(카운터 등)을 입력받아 6~10자리의 10진수 형태로 나타나는 출력값을 생성한다. 이러한 OTP 생성모듈의 일반적인 형태는 그림 2.에서 보는 바와 같다.

Challenge-Response OTP 방식은 서버에서 임의의 난수를 OTP 토큰으로 보내고 이를 OTP 생성 알고리즘 입력값으로 사용하여 OTP 값을 생성하는 방법이다. OTP값 생성 시 인증서버에서 난수를 생성하여 초기화 시 OTP 토큰과 공유된 비밀키로 암호화하여 OTP 토큰으로 전송한다. OTP 토큰은 이 난수와 비밀

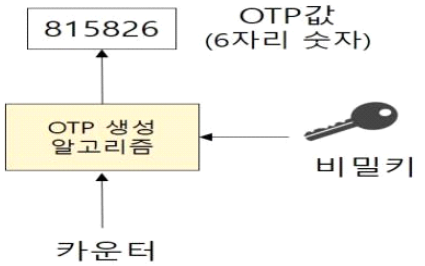

그림 2. OTP 생성 모듈
Fig. 2. OTP Generation Module

키를 OTP 생성 알고리즘의 입력값으로 사용하여 OTP 값을 생성한다. 이후, OTP 토큰은 생성된 OTP 값을 인증서버로 전송한다. 인증서버는 동일 알고리즘과 입력값(비밀키, 난수)을 사용하여 OTP 값을 생성하고 OTP 토큰으로부터 받은 OTP 값과 비교하여 같은 값이면 인증을 수락한다. 이 방식은 매번 다른 난수를 입력값으로 사용하기 때문에 보안성이 강한 장점이 있다[2].

2.3 4G LTE EPS-AKA의 보안취약점

드론봇이 LTE 통신망을 통하여 지상통제소와 통신을 하기 위해서는 먼저 LTE 통신망과 상호인증 및 키 설정(AKA : Authentication and Key Agreement)을 통해 안전한 링크를 구성해야 한다[3, 4].

드론봇의 USIM과 HSS/AUC(Home Subscriber Server/Authentication Center)는 인증 파라미터로 'LTE K'와 'IMSI'를 사용한다. LTE K는 USIM과 HSS/AUC만 소유하는 키를 의미하고 IMSI는 통신망 가입자를 식별하는 ID이다.

LTE 통신망에서 드론봇을 최초 등록 시에는 LTE K와 IMSI가 저장된 USIM이 드론봇에 탑재되고 해당 정보를 HSS/AUC에도 등록한다. 드론봇이 동작하기 위해 LTE 통신망에 접속을 시도하면 통신 링크 설정을 위해 인증절차가 시작된다. 그림 3.은 드론봇과 LTE 통신망간의 상호인증 및 키 설정 절차를 보여주고 있다.

(절차 ①) 드론봇이 MME(Mobility Management Entity)로 Attach Request 메시지를 전달한다. Attach Request에는 IMSI, UE(User Equipment) Network Capability, KSIasme=7를 포함한다. 여기서 7은 최초 접속이므로 키가 없음을 의미한다. 이 단계에서는 드론봇의 IMSI가 무선에서 평문으로 전송되어 도청에 의한 탈취 및 복제가 가능한 취약점이 존재한다.

(절차 ②) MME가 HSS/AUC에 인증 데이터를 요청하는 단계이다. MME는 드론봇으로부터 받은 메시

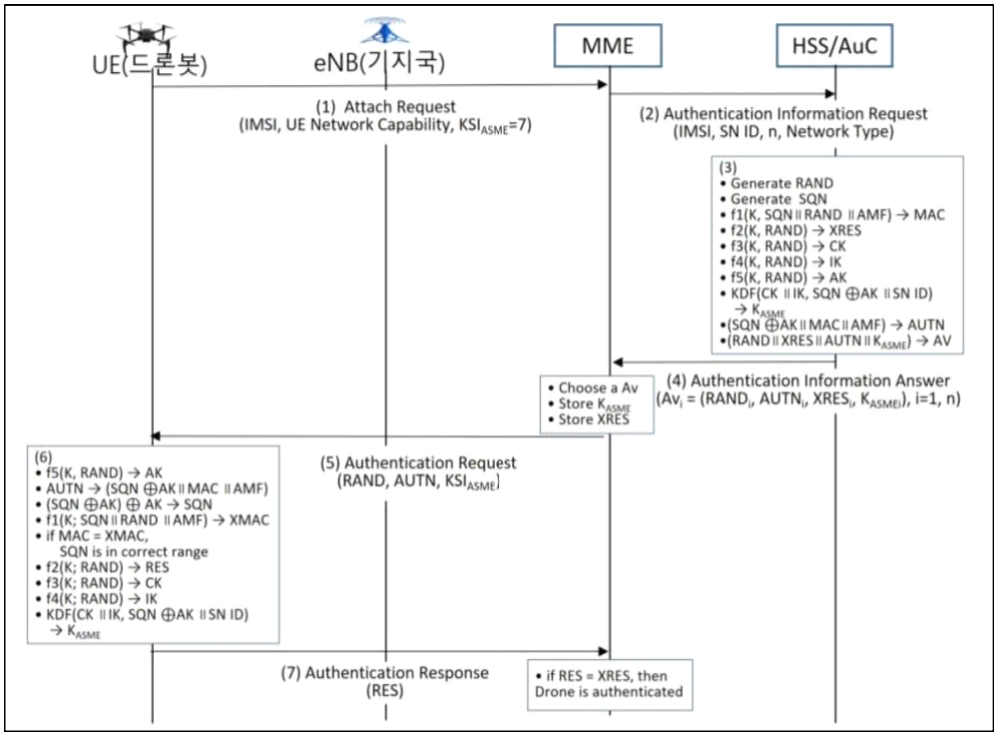

그림 3. EPS-AKA
Fig. 3. EPS-AKA

지의 정보를 바탕으로 HSS/AUC에 Authentication Information Request를 보낸다. 여기에 IMSI, SN(Serving Network) ID, n, Network Type를 포함한다. SN ID와 Network Type은 드론봇이 접속한 Serving Network의 정보와 식별자를 나타낸다. n은 HSS/AUC에게 요청하는 인증 벡터의 수를 의미한다. 이 단계에서는 인증 요청이 동시에 있을 경우, 각 드론봇의 IMSI에 대해 생성되는 보안키를 잘못 연결 지을 수 있다.

(절차 ③) 메시지를 수신한 HSS/AUC는 RAND (Random Number)와 SQN(Sequence Number)을 생성하고 해당 드론봇의 USIM과 HSS/AUC만 가지고 있는 LTE K를 입력값으로 하여 f1~f5 알고리즘 함수를 각각 실행하여 출력값을 통해 MAC(Message Authentication Code), XRES(Expected Response), CK(Ciphering Key), IK(Integrity Key), AK (Anonymity Key)와 AUTN(Authentication Token)를 생성한다. f1~f2는 메시지 인증기능 수행을 위한 무결성 알고리즘이고 f3~f5는 키 생성 기능 수행을 위한 암호화 알고리즘이다. 이후, KDF(Key Derivation Function)를 수행하여 LTE 통신망 접속의 최상위 레벨 키인 Kasme를 생성한다. 이 단계에서는 모든 키를 생성하는 알고리즘의 키로 사용되는 LTE K가 지속적으로 사용되고 있어 보안에 취약하다. USIM이 적에게 탈취될 경우, LTE K가 유출 및 노출 될 수 있어 인증 알고리즘 전체가 무력화될 수 있다.

(절차 ④) HSS/AUC에서 생성한 AV(Authentication Vector)를 MME에서 요청한 n만큼 구성하여 인증 데이터 응답 메시지(Authentication Information Answer)로 MME에 전송한다. 이 단계에서는 Kasme가 IMSI와 바인딩된 메시지로 전달되지 않아 UE에 대한 보안키를 잘못 연결 지을 수 있다.

(절차 ⑤) MME는 인증 벡터 AVn 중 하나를 선택하여 Kasme와 XRES는 기억하고 Authentication Request 메시지를 드론봇에 전송한다. 여기에는 KSI$_{ASME}$(키식별자), RAND, AUTN를 포함한다. 이 단계에서는 RAND와 AUTN이 평문 형태로 무선상으로 전달되기 때문에 제3자가 탈취하여 재전송 가능한 취약점이 존재한다.

(절차 ⑥) 드론봇은 USIM에 최초 저장되어 있는 LTE K와 MME로부터 전달받은 메시지의 RAND와 AUTN 정보를 통해 MAC, AMF, SQN 값을 얻고,

MAC과 XMAC(Expected MAC)이 일치하면 정상적인 네트워크로부터 수신한 메시지임을 확인하고 전달받은 SQN이 정상적인 범위에 있는지 확인한다. 검증 결과 모두 정상이면 (절차 ③)에서 HSS/AUC에서 수행했던 동일한 키 생성 알고리즘을 수행하여 RES, CK, IK를 생성한다. 이들을 활용하여 최상위 레벨키인 K_{ASME}를 자체적으로 생성하고 MME로부터 수신한 KSI_{ASME}를 인덱스로 하여 드론봇에 보관하는 과정을 통해 네트워크의 최상위 레벨키로 활용한다. 이 단계에서는 모든 키 생성 알고리즘의 키로 사용되는 LTE K가 USIM에 저장되어 있어 탈취 및 복제에 취약하다. 또한, 무결성 검증에서 중요한 인자인 SQN이 최초 랜덤하게 생성된 이후 1씩 증가하여 노출될 경우 다음 값 예측이 가능하다.

(절차 ⑦) 드론봇은 RES를 포함한 Authentication Response 메시지를 MME에게 전달한다. 인증 과정에서 자체 생성한 MAC과 전달받은 XMAC이 일치하지 않으면 인증 거절 메시지를 보내면서 이유를 첨부해서 보낸다. 이 단계에서는 인증 실패 메시지에 대한 보안 장치가 없고, 인가된 드론봇이 보냈는지 확인 할 수 있는 검증 장치가 없어 인증과정에서 오류가 야기 가능하다.

(절차 ⑧) MME는 드론봇으로부터 받은 메시지의 RES와 XRES를 비교하여 일치하면 인가된 드론봇으로 최종 인증하고 K_{ASME}를 최상위 레벨 키로 확정한다. 이 단계에서는 IMSI와 각 드론봇에 대한 K_{ASME}가 서로 다른 메시지를 통해 전달되어 잘못 짝 지어 질 수 있다. 이후에 MME는 K_{ASME}를 다음 접속단계부터 활용할 NAS(Non Access Stratum) Signaling의 암복호화키(Knasenc)와 무결성키(Knasint)로 나누어 사용한다. 또한, MME는 Kasme를 기지국(eNB)에 전송하여 기지국이 드론봇과의 RRC(Radio Resource Control) Signaling 통신에 사용할 사용자 데이터 암호화키(Kupenc), 제어 데이터 암호키(Krrcenc), 제어 데이터 무결성키(Krrcint)를 생성한다.

이상과 같은 4G LTE EPS-AKA의 보안취약점을 해결하기 위해 [4]에서는 15자리로 구성된 이동통신 기기의 고유 번호인 '(IMEI, International Mobile Equipment Identity)'를 추가로 인증에 사용하는 방안을 제안하였다. [5]에서는 4G LTE 네트워크 기반으로 운용되는 드론봇에 PUF 회로를 장착한 후 PUF에서 생성되는 고유한 출력값을 인증과정에 추가적으로 활용함으로써 EPS-AKA의 다양한 보안취약점들을 해결하였다. 그러나 제시된 방식은 각 드론봇에서 100,000개의 Challenge-Response 쌍을 생성하여 서버에 등록하는 방식을 취하고 있어 다수의 드론이 운용되어야 하는 환경에서는 CRP 테이블의 크기 증가가 불가피하며, 그만큼 드론봇 전투체계 운용도 복잡해질 수 있다. 특히 군집드론과 같이 수십에서 수백대의 드론이 동시에 운용되면서 인증을 요구할 경우에는 CRP 테이블 조회로 인해 서버에 과도한 부하가 발생하여 인증과정도 지연될 수 있다. 그리고 드론봇 인증을 위해서는 반드시 CRP 테이블의 Challenge와 Response 값을 확인해야 하기 때문에 서버 운용이 불가한 경우에는 즉각적인 드론봇 전투체계 운용이 제한된다. 즉, 전시 적 포탄 공격, 적 특작부대에 의한 서버 피해가 발생할 경우 CRP 테이블에 의한 드론봇 인증이 불가하여 드론봇 전투체계 운용자체가 제한받을 수 있다.

Ⅲ. PUF-OTP를 활용한 드론봇 인증 강화방안

3.1 PUF-OTP 구조

드론봇 인증 시 PUF-OTP를 인증과정에 적용한다. 즉, PUF 회로를 기반으로 OTP를 생성한다는 것이다. PUF-OTP 구조는 그림 4.에서 보는 바와 같으며 OTP 알고리즘의 입력값으로는 PUF 회로의 Response 값 R_i와 R_i의 Shift값인 Dronenbot Key를 사용한다. Dronebot Key는 인증과정에서 Response 값을 전달할 때 암호화하는데 사용한다. 인증센터와 드론봇 모두 PUF의 Response 값을 Shift하여 사용한다. Dronebot Key는 대칭키이며 매 인증 시 마다 새로운 값으로 업데이트되어 사용된다.

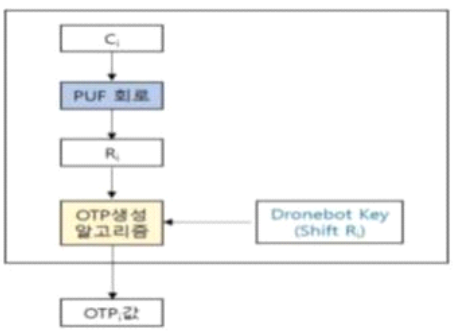

그림 4. PUF-OTP 구조
Fig. 4. PUF-OTP Structure

3.2 PUF-OTP를 활용한 개선된 EPS-AKA

LTE 네트워크 인증센터 기능을 수행하는 HSS/AUC에 드론봇을 등록 시 드론봇 ID인 UE_{ID}와 고유 식별자인 IMSI 및 LTE K, 그리고 최초 드론봇

인증 시에 사용하게 될 PUF의 출력값 R_0 값만 등록한다. 드론봇에는 최초 인증과정에서 사용할 C_0만 주입시킨다.

본 연구에서 CRP 테이블을 사용하지 않고 하나의 Challenge-Response 쌍인 C_0-R_0만을 등록하여 사용하는 이유는 CRP 테이블 사용으로 인한 서버 부하 발생과 인증 지연 등을 원천적으로 제거하기 위함이다. 특히, 향후 드론봇은 다수의 드론이 동시에 작전을 수행하는 군집(Swarming) 체계로 발전해 나갈 것임이 자명한 상황에서 CRP 테이블 사용은 드론봇 전투체계 운용에 심각한 지장을 초래할 수 있다. 이에 본 연구에서는 인증센터인 HSS/AUC에 C_0에 대한 Response 값인 R_0만을 저장하여 사용하고 이후에 진행되는 인증과정에서는 Response 값을 업데이트하여 사용하는 방식을 채택하였다. 그뿐만 아니라, R_0와 R_0를 Shift한 Dronebot Key를 이용하여 OTP 출력값을 생성한 후 비교를 통해 드론봇 인증을 수행한다. 세부 인증과정은 그림 5.에서 보는 바와 같다.

(절차 ①) 드론봇에 장착된 PUF 회로에서 Challenge 값 C_i에 대한 Response 값 R_i을 추출한다. 이후, Attach Request 메시지를 MME에 보낸다. 이 메시지에는 드론봇의 아이디인 UE_{ID}, 드론봇 식별자인 IMSI와 R_i를 XOR 연산을 수행한 후 해시함수를 적용하여 생성된 해시값 등이 포함된다.

- (①-1) $fPuf(C_i) \rightarrow R_i$
- (①-2) UE_{ID}, $h(IMSI \oplus R_i)$, UE Network Capability, KSI_{ASME}=7 전송

(절차 ②) MME는 드론봇으로부터 받은 메시지를 확인하고 Authentication Information Request(UE_{ID}, $h(IMSI \oplus R_i)$, SN ID, n, Network Type) 메시지를 HSS/AUC로 전송한다.

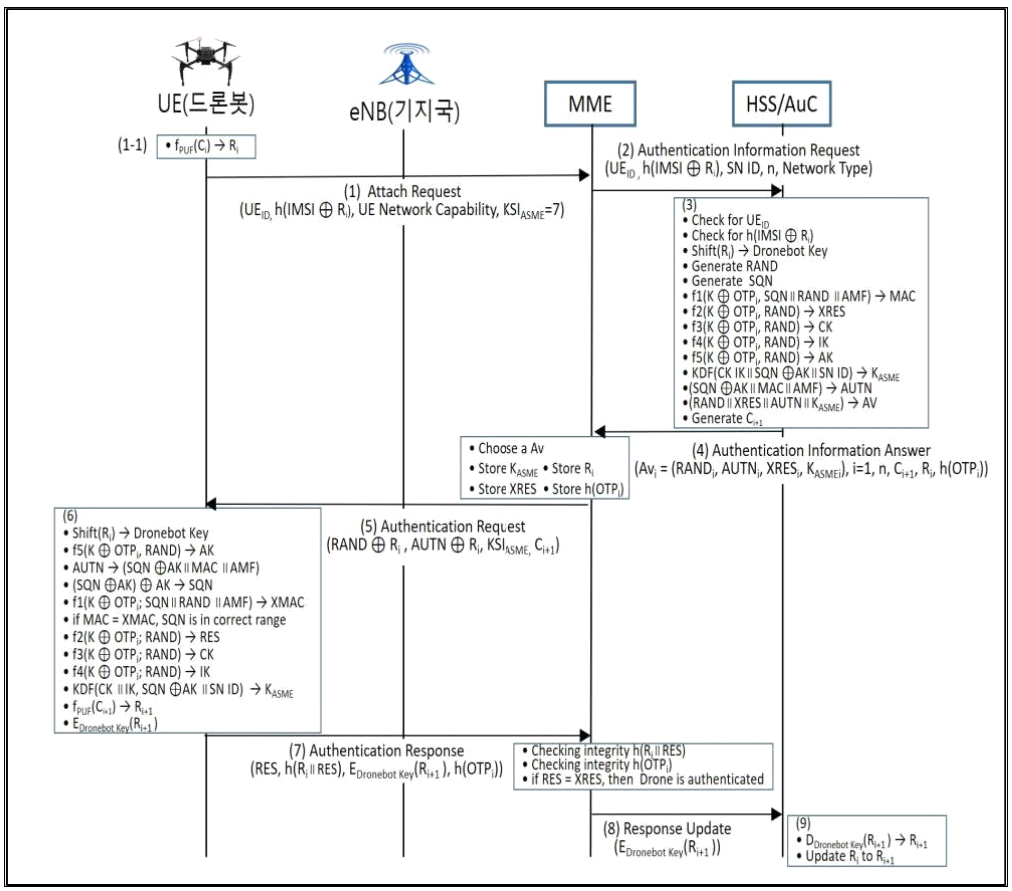

그림 5. PUF-OTP 활용한 EPS-AKA
Fig. 5. EPS-AKA using PUF-OTP

(절차 ③) HSS/AUC는 MME로부터 메시지를 수신하여 드론봇의 UE_{ID}를 확인하고 기 저장된 UE_{ID}와 비교하여 최초로 정상 드론봇임을 확인한다. 이어서, $h(IMSI \oplus R_i)$를 자체적으로 계산하고 MME로부터 받은 $h(IMSI \oplus R_i)$와 비교한다. 그리고 R_i를 Shift하여 드론봇 키를 생성한다. 이어서, PUF-OTP를 활용한 개선된 키 생성 알고리즘을 수행한다. R_i 값과 Dronebot Key를 입력값으로 하여 OTP_i 값을 생성하고 LTE K와 XOR 연산을 통해 키 생성 알고리즘을 수행하여 RAND, SQN, MAC, XRES, CK, IK, AK, K_{ASME}, AUTN, AV를 생성한다. 그리고 다음 인증에 사용될 Challenge 값인 C_{i+1}을 생성한다.

(절차 ④) PUF-OTP를 활용한 키 생성 알고리즘 수행 후, HSS/AUC는 인증벡터 AV_i=((RAND, AUTN, XRES, K_{ASME}), i=1, n, C_{i+1}, R_i, $h(OTP_i)$)를 MME에서 요청한 수 (n개)만큼 구성하고 Authentication Information Answer 메시지를 MME에 전송한다. 이때 드론봇에서 키 생성 알고리즘 수행 및 다음 인증 시도 시 필요한 C_{i+1}과 MME에서 무선으로 전송되는 메시지 보호를 위해 필요한 R_i도 함께 전송한다. 또한, OTP 인증을 위해 OTP_i도 해시함수로 보호하여 보낸다.

(절차 ⑤) MME는 전달받은 메시지 중 하나의 벡터를 선택하여 최상위 레벨 키인 K_{ASME}와 최종 정상적인 드론봇 확인을 위해 필요한 값인 XRES, R_i을 저장한다. 그리고 드론봇의 OTP 확인을 위해 OPT_i도 저장한다.

이후, Authentication Request(RAND$\oplus R_i$, AUTN $\oplus R_i$, KSI_{ASME}, C_{i+1}) 메시지를 구성하여 드론봇에 전송한다.

(절차 ⑥) 드론봇에서는 MME로부터 전달받은 메시지를 통해 필요한 정보를 얻는다. 최초 R_i 값을 Shift하여 Dronebot Key를 생성하고 R_i와 Dronebot Key를 입력으로 하여 OTP_i를 생성한다. 이어서 OTP_i와 LTE K를 XOR하여 HSS/AUC가 수행했던 과정과 동일하게 PUF-OTP를 활용한 키 생성 알고리즘을 수행한다. 이를 통해 AK, SQN$\oplus$AK $\|$ MAC $\|$ AMF, SQN, XMAC, RES, CK, IK, K_{ASME}를 생성한다. 그리고 생성된 K_{ASME}를 USIM에 저장한다. 또한, 다음 인증절차 시도 시 사용할 R_{i+1}를 MME로부터 받은 C_{i+1}을 PUF 회로에 통과시켜 생성하고 대칭키인 Dronebot Key로 암호화한다.

(절차 ⑦) 드론봇은 (RES, $h(R_i \| RES)$, $E_{Dronebot\ Key}(R_{i+1})$, $h(OTP_i)$)로 구성된 Authentication Response 메시지를 MME에 전송한다. LTE 네트워크에서는 무선 상태에서 평문 형태로 전송되는 Authentication Response 메시지 탈취를 통한 중간자 공격이 가능하다. 따라서 해시함수를 이용하여 무결성 검증이 가능한 형태로 메시지를 생성한다.

(절차 ⑧) MME에서는 저장하고 있던 R_i와 RES를 이용하여 무결성을 검증한다. 또한, 저장하고 있던 OTP_i의 해시값과 전달받은 OTP_i의 해시값을 비교하여 무결성을 검증한다. 무결성이 입증되었다면, RES와 XRES가 일치하는지 확인하여 정상 등록된 드론봇 여부를 최종 확인한다. 그리고 Response 업데이트를 위해 $E_{Dronebot\ Key}(R_{i+1})$을 HSS/AUC에 전송한다.

(절차 ⑨) HSS/AUC는 $E_{Dronebot\ Key}(R_{i+1})$을 복호화하여 Response 값을 R_i에서 R_{i+1}로 업데이트한다.

이상과 같은 인증 절차는 드론봇이 본격적으로 작전을 수행하기 이전 단계, 즉 비행을 준비하는 단계에서 운용부대 내에서 실시한다.

3.3 드론봇과 지상통제소와의 직접 인증절차

4G LTE 네트워크 기반의 드론봇 전투체계는 전시적 포탄 공격, 특작부대에 의한 테러 등으로 인해 기지국 및 인증서버가 파괴되어 드론봇 인증이 제한되는 상황에 직면할 수도 있다. 이런 상황에서는 드론봇을 조종기에 직접 1:1 방식으로 연결하여 운용해야 하며, 보다 신속하고 안전하게 정상 드론봇을 인증할 수 있어야만 한다.

본 절에서는 PUF-OTP를 활용하여 드론봇과 지상통제소가 직접 1:1로 인증하는 절차에 대해 설명한다. 세부적인 인증진행 절차는 그림 6.에서 보는 바와 같다.

(절차 ①) 드론봇에서 최초 PUF 회로를 통해 Challenge C_i에 대한 R_i를 추출하고 해당 R_i를 Shift하여 Dronebot Key를 생성한다. 이어서 R_i값과 Dronebot Key를 입력으로 하여 $OTP_{Dronebot}$ 값을 생성한다.

(절차 ②) 드론봇에서는 지상통제소에 Authentication Request를 전달한다. 이때 대칭키인 Dronebot Key를 이용하여 $OTP_{Dronebot}$ 값을 암호화하여 전송한다.

(절차 ③) 지상통제소에서는 Authentication Request 메시지를 받고 최초 저장하고 있던 R_i 값을 Shift하여 Dronebot Key를 생성한다.(드론봇에서의 절차와 동일) 그리고 R_i 값과 Dronebot Key를 이용하여 지상통제소의 OTP 값인 OTP_{GCS}를 생성한다. 여기서 $OTP_{Dronebot}$ 값과 OTP_{GCS}를 비교하여 동일하면 다음

인증을 위한 C_{i+1}을 생성한다.

(절차 ④) 지상통제소는 Authentication Information를 드론봇에 전송하는데 이때 C_{i+1}을 Dronebot Key로 암호화하여 전송한다.

(절차 ⑤) 드론봇에서는 지상통제소에서 받은 C_{i+1}을 PUF 회로에 통과시켜 R_{i+1}을 생성한다. 그리고 이미 생성되어 있는 Dronebot Key를 사용하여 R_{i+1}을 암호화한다

(절차 ⑥) 드론봇에서는 다음 인증에 사용될 Response 값의 업데이트를 수행하기 위해 R_{i+1}을 Dronebot Key로 암호화하여 지상통제소에 전송한다.

(절차 ⑦) 지상통제소에서는 이미 생성되어 있는 Dronebot Key를 이용하여 암호화된 R_{i+1}을 복호화하고 Response 값을 R_i에서 R_{i+1}으로 업데이트한다.

이러한 방식은 서버 사용이 제한되는 전장상황에서도 드론봇과 지상통제소 간 직접 인증을 통해 드론봇 운용이 지속적으로 가능하도록 보장해준다. 서버에 PUF 회로의 CRP 테이블을 유지하여 인증하는 기존 방식은 서버 운용이 제한될 경우 드론봇 운용까지도 불가해진다는 단점을 가진다. 그러나 제안하는 방식은 서버 운용이 제한되는 상황에서도 지상통제소에 저장되어 있는 PUF 회로의 R_0 값을 사용하여 드론봇을 인증할 수 있다.

CRP 테이블과 관련하여 고려해야 할 또 다른 요소는 지상통제소의 형태이다. 일반적으로 지상통제소는 차량형에서부터 휴대용까지 다양하게 운용되며, 제대별로 운용되는 드론봇의 형태와 크기에 따라 지상통제소의 형태와 규모 등도 달라진다. 하위제대로 내려갈수록 지상통제소는 소형화·경량화 된다. 이러한 특징 때문에 하위제대에서 운용하는 소규모 또는 휴대용 지상통제소에 CRP 테이블을 운용하는 것은 결코 쉬운 문제가 아니다.

3.4 제안 프로토콜 분석

기존 EPS-AKA 인증절차와 PUF-OTP를 활용한 개선된 EPS-AKA를 비교하면 표 1.과 같다. 본 연구에서 제안하는 프로토콜은 유일하고 복제불가능한 PUF 회로의 출력값과 그 출력값을 Shift하여 생성한 대칭키를 OTP 알고리즘의 입력값으로 사용하여 OTP 값을 생성하여 인증에 활용함으로써 다음과 같은 강점들을 가진다.

첫째, USIM만을 탈취 또는 복제한 후 재사용하는 공격이 불가능하다. 공격자는 공격하고자 하는 드론봇의 USIM을 복제하거나 탈취하여 아군의 드론봇과 동일한 형태의 다른 드론봇에 장착할 수 있겠지만 복제불가능한 PUF에 의해 생성되는 Response를 만들어 낼 수는 없다. 따라서 공격자는 정상적인 Attach Request 메시지 자체를 생성할 수 없다. 만약, 인증을 시도하더라도 키 생성 알고리즘의 입력값인 LTE K⊕ OTP_i 값을 알아 낼 수 없으며, RAND 및 AUTN도 생성할 수 없기 때문에 사실상 정상적인 인증절차 수행은 불가능하다.

둘째, Replay 공격이 불가하다. 개선된 인증과정에서는 키 생성시 동일한 LTE K를 사용하지 않고 C_i와 R_i를 업데이트하여 적용하고, 이를 통해 OTP 값을 매 인증 시 마다 변경한다. 따라서 무선으로 전송되는 메

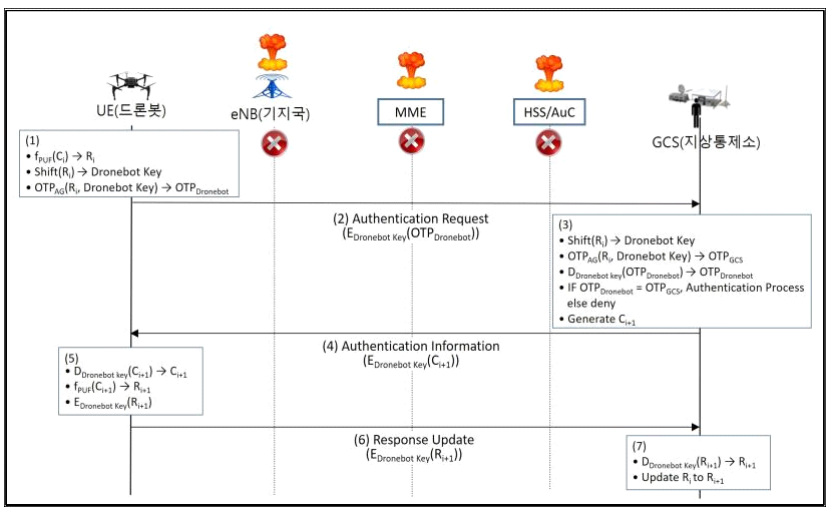

그림 6. 드론봇과 GCS간 직접 인증절차
Fig. 6. Direct authentication procedure between Dronebot and GCS

표 1. 기존 EPS-AKA와 개선된 EPS-AKA 비교
Table 1. Existing EPS-AKA vs. Enhanced EPS-AKA

기존 EPS-AKA		개선된 EPS-AKA(PUF-OTP 적용)	
①	**Attach Request** - IMSI 전송	①	**Attach Request** - 드론봇의 ID(UE_{ID}) 추가 전송 - IMSI 대신 h(IMSI⊕R_i) 전송
②	**Authentication Information Request** - IMSI 전송	②	**Authentication Information Request** - 드론봇의 ID(UE_{ID}) 추가 전송 - IMSI 대신 h(IMSI⊕R_i) 전송
③	**HSS/AUC 키 설정** - K(LTE K)를 입력값으로 f1~f5 알고리즘 함수를 각각 실행	③	**HSS/AUC 키 설정** - 드론봇의 ID(UE_{ID}) 확인 - h(IMSI⊕R_i) 확인 - K(LTE K) 대신 K⊕OTP_i 입력값으로 f1~f5 알고리즘 함수를 각각 실행
④	**Authentication Information Answer** - 인증벡터(AV_i) 전송	④	**Authentication Information Answer** - 인증벡터(AV_i)에 C_{i+1}, R_i, h(OTP_i) 추가 전송
⑤	**Authentication Request** - RAND, AUTN 전송	⑤	**Authentication Request** - RAND, AUTN 대신 RAND⊕R_i와 AUTN⊕R_i 전송 - C_{i+1} 추가 전송
⑥	**드론봇 키 설정** - K(LTE K)를 입력값으로 f1~f5 알고리즘 함수를 각각 실행	⑥	**드론봇 키 설정** - R_i를 Shift하여 Dronebot Key 생성 - K(LTE K) 대신 K⊕OTP_i 입력값으로 f1~f5 알고리즘 함수를 각각 실행 - PUF를 통해 R_{i+1} 생성 - Dronebot Key통해 R_{i+1} 암호화
⑦	**Authentication Response** - RES 전송	⑦	**Authentication Response** - h(R_i ‖ RES), $E_{Dronebot\ Key}(R_{i+1})$, h($OTP_i$) 추가 전송
·	·	⑧	**Response 업데이트** (MME) - $E_{Dronebot\ Key}(R_{i+1})$
·	·	⑨	**Response 업데이트** (HSS/AuC) - $D_{Dronebot\ Key}(R_{i+1}) \rightarrow R_{i+1}$

시지를 도청하여 탈취한 후 재전송 공격을 수행하는 것 자체가 불가능하다. 한편, Replay 공격을 수행하는 공격자도 식별할 수 있다. 정상적이지 않거나 이미 유효기간이 지난 C_i와 R_i를 포함하는 메시지를 송신하는 장비를 공격자로 판단할 수 있다. 이렇게 식별된 비정상적인 드론봇은 HSS/AUC에 등록하여 원천적으로 접속을 차단할 수 있다.

셋째, IMSI 탈취가 불가능하여 경쟁조건 공격도 불가하다. 경쟁조건 공격은 IMSI가 노출되어야만 가능한데 개선된 인증과정에서는 평문으로 전송되던 IMSI에 Response 값을 XOR 연산한 다음 해시함수를 적용하여 보호함으로써 IMSI 탈취에 대한 공격 가능성을 원천적으로 차단한다. 그리고 이를 통해 드론봇의 중요정보나 위치 프라이버시 노출까지도 방지할 수 있다.

넷째, 대칭키 암호 알고리즘 적용으로 중요정보 보호가 가능하다. PUF의 Response 값 R_i를 매 인증 시마다 Shift하여 대칭키인 Dronebot Key를 생성하여 OTP_i 값 생성 시 비밀키로 사용하고, R_i 값 업데이트를 위한 무선 전송 시 노출 방지를 위해 암호화키로 활용한다. 때문에 공격자가 차후 인증에 사용되는 R_{i+1} 값을 획득하는 것은 불가능하다. 공격자가 R_{i+1} 값을 알기 위해서는 R_i 값을 Shift하여 생성한 Dronebot Key를 알아야 하며, Dronebot Key를 알기 위해서는 R_i 값을 알아야 하기 때문이다.

다섯째, UE_{ID} 사용으로 다수의 드론봇이 동시 인증을 시도할 때 해당 드론봇에 대한 키를 잘못 연결 지을 수 없고, 공격자는 IMSI를 획득할 수도 없다. 따라서 UE_{ID}를 획득할 수 있다 하더라도 IMSI를 알 수 없어 경쟁조건 공격의 수행 자체가 불가능해진다.

여섯째, 군집드론 및 다수의 드론봇 운용환경에서 유리하다. 제안방식은 PUF 회로를 적용함에도 CRP 테이블을 서버에 저장하지 않기 때문에 서버 자원의 효율적 사용이 가능하다. 최초 인증 시에 필요한 R_0만

을 저장하고 매 인증 시 마다 업데이트하여 사용하기 때문에 CRP 테이블에 대한 관리 부담이 없다. 또한, 서버에서 인증에 필요한 연산을 수행 시 서버부하 감소효과도 기대할 수 있다.

일곱째, PUF를 사용하는 기존 연구에서는 CRP 테이블을 서버에 저장하기 때문에 적 포탄 공격 등 서버 운용이 제한되는 상황에서는 드론봇 운용이 불가하였다. 하지만 제안 방식의 경우, 드론봇 생산 시부터 해당 드론봇의 PUF 회로의 최초 출력값 R_0를 지상통제소에 저장하고 있어 드론봇과 지상통제소와의 직접 인증도 가능해져 인증서버 사용 제한 시에도 드론봇의 정상 운용이 가능하다. 또한, PUF-OTP를 통해 인증과정의 보안을 강화함으로써 악의적인 의도로 드론봇 전투체계에 접속을 시도하는 비정상 드론봇의 인증시도를 효율적으로 차단할 수 있다.

3.5 군 적용 방안

PUF-OTP를 적용하여 드론봇을 관리하는 방안에 대한 개념은 그림 7.에서 보는 바와 같다. PUF-OTP를 적용한 드론봇을 운용하기 위해서는 PUF-OTP를 장착하여 드론봇을 생산하는 방산업체와 PUF 회로의 Response 값을 측정하여 관리하는 군 PUF 관리기관, 그리고 드론봇 인증센터(HSS/AUC)가 필요하다.

방산업체에서는 PUF-OTP 회로를 적용한 드론봇을 생산하고 군 PUF 관리기관으로 드론봇과 지상통제장비를 함께 이송한다. 군 PUF-OTP 관리기관에서는 드론봇에 탑재된 PUF 회로에서 C_0의 입력에 대한 Response 값인 R_0를 추출한다. 이후, 인증센터인 HSS/ AUC 측에 R_0를 신뢰할 수 있는 통신채널을 통해 전달한다. HSS/AUC는 R_0를 저장하고 드론봇 인증 간 사용한다. 또한, 인증센터 및 기지국 등 파괴로 인해 드론봇 인증이 제한될 경우에 드론봇과 지상통제소 간 직접 인증을 위해 지상통제소에도 R_0를 주입한다.

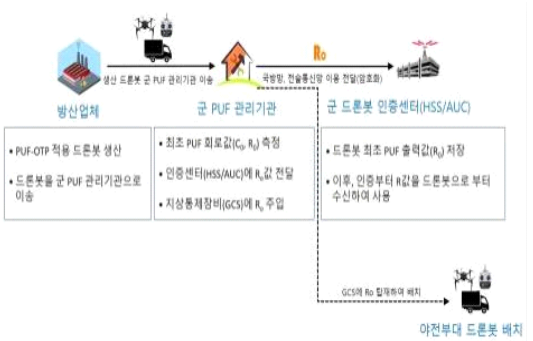

그림 7. PUF-OTP 적용 드론봇 관리방안
Fig. 7. Management of Dronebot with PUF-OTP

드론봇 인증센터인 HSS/AUC는 최초 R_0를 저장하고 이후 인증부터는 R값(R_{i+1})을 드론봇으로부터 전달받아 인증에 사용한다. 드론봇 대 지상통제소 간 직접 인증방식에서도 최초 인증 이후부터는 드론봇으로부터 R값(R_{i+1})을 전달받아 업데이트하여 사용한다.

Ⅳ. 결 론

본 연구는 미래 전장에서 게임 체인저로서의 역할을 담당할 드론봇 전투체계에 4G LTE 네트워크가 적용될 것임을 가정하고, 발생 가능한 보안취약점을 제거하여 보안성을 강화할 수 있는 방안을 제안하였다.

4G LTE의 EPS-AKA 인증은 사용자 식별자인 IMSI가 노출될 수 있어 USIM 복제 및 탈취를 통한 재사용공격이 가능하며 경쟁조건 공격을 통해 위치정보나 기기정보가 노출될 가능성도 존재하였다. 또한 키 생성에 사용되는 Long Term Key인 LTE K가 지속 사용됨에 따라 노출 시 인증과정 전체가 무력화될 가능성이 상존하였다. 이러한 문제점을 해결하기 위해 첫째, PUF 회로의 출력값을 IMSI와 XOR한 후 그 해시값을 인증요청 메시지에 포함시킴으로써 IMSI의 노출을 방지하고, 탈취 및 복제에 의한 재사용 공격과 경쟁조건 공격 가능성을 원천 제거하였다. 둘째, PUF의 출력값을 OTP의 입력으로 적용하고, 이렇게 생성된 OTP 출력값을 LTE K와 XOR 연산하여 LTE 최상위 키인 K_{ASME}를 생성하였다. 즉 드론봇에 대한 인증이 수행될 때마다 업데이트된 PUF 회로의 Response 값과 그 Reponse 값을 Shift한 값을 OTP 알고리즘의 입력으로 적용하여 OTP를 생성함으로써 보안성이 더욱 강화되었다. 셋째, 해시함수와 대칭키(Dronebot Key)를 이용하여 무선 상태에서 평문으로 전송되던 인증 파라미터의 노출을 방지하고, 무결성까지 검증할 수 있도록 개선하였다. 넷째, PUF를 이용함에도 CRP 테이블을 저장하지 않아 서버의 관리 부담을 경감시키는 효과와 자원의 효율적 사용 효과도 달성하였다. 이는, 군집 드론봇 및 다수의 드론봇 운용환경에서 인증시간 단축 등의 효과를 줄 것으로 기대된다. 또한, 인증서버에 문제가 발생할 경우 지상통제소와의 1:1 인증을 통해 드론봇을 인증할 수 있도록 함으로써 운용상의 제한사항을 최소화하였다. 마지막으로 제안된 접근방법은 경제적 측면이나 드론봇 운용 측면에서도 상당한 긍정적 효과를 거둘 것으로 기대된다. 암호장비 개발에는 많은 시간과 예산이 투자

되는 반면, 제안하는 PUF-OTP는 기존 USIM과 연동하여 간단한 회로 개선만으로 적용이 가능해짐으로써 적은 비용으로 드론봇 전투체계 보안을 획기적으로 강화할 수 있게 될 것이다. 암호장비를 드론봇에 장착할 경우 페이로드 증가로 인해 운용시간이 단축되거나 작전반경이 축소될 가능성도 있으나, PUF-OTP는 페이로드 증가 부담이 없기 때문에 작전적 측면에서도 많은 긍정적 효과가 기대된다.

향후에는 5G에 적용되고 있는 AKA에 PUF-OTP를 접목하는 방안과 군집드론에 의한 동시다발적 인증 요구를 효율적으로 처리할 수 있는 방안에 대해 연구를 진행할 계획이다.

References

[1] K. C. Wang, B. S. Lee, K. J. Lim, and J. Y. Ahn, "Technical trends on security of control and non-payload communications network for unmanned aircraft systems," *Electron. and Telecommun. Trend Anal.*, vol. 32, no. 1, 2017.

[2] D. K. Kim, "PUF-based OTP token for mobile pages," *J. Korea Multimedia Assoc.*, vol. 19, no. 1, pp. 2-4, Mar. 2015.

[3] K. Hamandi, J. B. Abdo, I. H. Elhajj, A. Kayssi, and A. Chehab, "A Privacy-enhanced computationally efficient and comprehensive LTE-AKA," *Comput. Communi.*, vol. 98, pp. 20-30, 2017.

[4] H. Y. Lee and S. J. Lee, "Enhanced EPS-AKA for adapting LTE technology in military tactical communication network," *J. Secur. Eng.*, vol. 12, no. 5, pp. 455-468, Oct. 2015.

[5] J. W. Jung and S. J. Lee, "A security enhanced EPS-AKA using PUF technology for LTE-based DroneBot combat system," *Korea Inst. Military Sci. and Technol. Conf.*, pp. 887-888, Nov. 2018.

[6] Y. S. Kang, M. K. Oh, S. J. Lee, and D. H. Choi, "International trend in standardization of physical copy protection (PUF) security requirements and testing methods," *J. Soc. for Inf. Protection*, vol. 28, no. 4, pp. 1-3, Aug. 2018.

윤 상 열 (Sangyeol Yun)

2002년 2월 : 국립순천대학교 정보통신공학 학사

2019년 8월 : 국방대학교 국방정보관리학 석사

2019년 9월~현재 : 아주대학교 국방디지털융합학과 박사과정

<관심분야> 사이버전, 무선네트워크, 국방전술통신

[ORCID:0000-0003-4679-3707]

이 수 진 (Soojin Lee)

1992년 2월 : 육군사관학교 이학사

1996년 2월 : 연세대학교 컴퓨터과학 석사

2006년 2월 : 한국과학기술원 전산학 박사

2006년 3월~현재 : 국방대학교 국방과학학과 교수

<관심분야> 사이버전, 사이버안보, 암호이론 및 응용, 침입탐지시스템

[ORCID:0000-0002-4117-407X]