KIPS Tr. Software and Data Eng.
Vol.6, No.9 pp.429~436 pISSN: 2287-5905

https://doi.org/10.3745/KTSDE.2017.6.9.429

Lightweight Authentication Scheme for Secure Data Transmission in Terrestrial CNPC Links

Kim Man Sik† · Jun Moon-Seog†† · Kang Jung Ho†††

ABSTRACT

Unmanned Aerial Vehicles (UAV) that are piloted without human pilots can be commanded remotely via frequencies or perform pre-inputted missions. UAVs have been mainly used for military purposes, but due to the development of ICT technology, they are now widely used in the private sector. Teal Group's 2014 World UAV Forecast predicts that the UAV market will grow by 10% annually over the next decade, reaching $ 12.5 billion by 2023. However, because UAVs are primarily remotely controlled, if a malicious user accesses a remotely controlled UAV, it could seriously infringe privacy and cause financial loss or even loss of life. To solve this problem, a secure channel must be established through mutual authentication between the UAV and the control center. However, existing security techniques require a lot of computing resources and power, and because communication distances, infrastructure, and data flow are different from UAV networks, it is unsuitable for application in UAV environments. To resolve this problem, the study presents a lightweight UAV authentication method based on Physical Unclonable Functions (PUFs) that requires less computing resources in the ground Control and Non-Payload Communication (CNPC) environment, where recently, technology standardization is actively under progress.

Keywords : UA, UAS, CNPC, Data Security, Drone

지상 CNPC 링크에서 안전한 데이터 전송을 위한 경량화된 인증기법

김 만 식† · 전 문 석†† · 강 정 호†††

요 약

무인기는 조종사가 탑승하지 않고 주파수를 통해 컨트롤 센터에서 원격으로 명령을 하달 받거나 미리 입력된 임무를 수행하며, 지금까지는 주로 군용으로 이용되었지만 ICT 기술 발전으로 인해 이제는 민간분야에서도 다양하게 이용되고 있다. Teal Group의 2014년 World UAV Forecast는 향후 10년간 무인기 시장은 매년 10%씩 성장하여 2023년에는 125억 달러에 이른다고 전망하였다. 그러나 무인기는 원격으로 조종되기 때문에 만약 악의적인 사용자가 원격으로 조종되는 무인기에 접근한다면 프라이버시를 크게 침해 하거나 재정적 손실이나 인명피해를 입힐 수 있는 문제점이 있다. 이러한 문제점을 해결 위해서는 반드시 무인기와 조종매체가 상호인증을 통해 보안채널을 구축해야 하지만, 기존 보안기법은 많은 컴퓨팅 자원과 파워를 요구하며, 통신 거리, 인프라, 데이터 흐름 등이 무인기 네트워크와 다르기 때문에 무인기 환경에 적용하기에는 적합하지 않다. 본 논문에서는 이러한 문제를 해결하기 위하여 현재 기술 표준화가 활발히 진행 중인 지상 Control and Non-Payload Communication (CNPC) 환경에서 적은 컴퓨팅 자원을 요구하는 PUF를 기반으로 경량화된 무인기 인증 기법을 제시한다.

키워드 : 무인기, 무인항공시스템, 지상 제어 및 비 임무용 링크, 데이터 보안, 드론

1. 서 론

무인기는 조종사가 비행체에 탑승하지 않고 임무를 수행하는 비행체로 초기에는 주로 군용으로 많이 이용되었으나, 최근 ICT 기술의 발달로 전 세계적으로 민간 분야에서도 널리 이용되고 있다[1, 2]. 무인기 시장은 국내외에서 빠르게 성장하고 있는데, Teal Group의 2014년 World UAV Forecast에 따르면 향후 10년간 무인기 시장은 매년 10%씩 성장하여 2023년에는 125억 달러에 이른다고 전망하였으며, 국내시장은 2014년 100억원에서 2022년까지 매년 5억불씩 22%의 성장이 기대된다고 하였다[3, 4]. 실제로 중국의 DJI는 전 세계 민수 무인기 분야 1위 기업으로 다양한 민간용 무인기를

† 준 회 원 : 숭실대학교 컴퓨터학과 박사과정
†† 종신회원 : 숭실대학교 컴퓨터학과 교수
††† 종신회원 : 숭실대학교 평생교육원 정보보안학과 교수
Manuscript Received : March 8, 2017
First Revision : April 6, 2017
Accepted : April 18, 2017
* Corresponding Author : Kang Jung Ho(kjh7548@naver.com)

출시하여 2014년 매출이 약 5000억원, 2015년 매출이 약 1조 1500억원을 달성하였으며, 미국의 아마존이나 도미노 피자는 무인기를 이용한 배달 사업을 준비 하는 등 새로운 무인기 서비스를 창출하고 있다[5, 6]. 국내 무인기 시장은 주로 군수 시장이 비중을 많이 차지하고 있으나, 취미나 레저용 중심으로 수요가 증가하고 있으며 정부에서도 2016년에 무인기 민간영역 활성화를 위해 '무인이동체 발전 5개년 계획'을 발표하였다. 뿐만 아니라 세계전파통신 2015 World Radiocommunication Conference(WRC-15)에서는 증가하는 무인기 수로 인해 발생하는 주파수 간섭 문제를 해결하기 위하여 무인기 지상 제어용으로 61MHz 대역폭인 5,030~5,091MHz 주파수 대역을 할당하였으며, 고정위성업무 주파수를 이용한 무인기 제어용으로 약 3GHz 대역폭인 10.95~30GHz 주파수 대역을 할당하였다[7].

그러나 최근 성장하는 무인기 시장에 비례하여 무인기 안정성에 대한 문제가 이슈가 되고 있는데, 운행 중인 무인기가 장애나 외부적인 요소로 추락한다면 부여된 임무를 완수하지 못할 뿐만이 아니라 재정적인 손실과 인명피해를 입힐 수 있다[8-11]. 이러한 사고를 예방하기 위하여 장애물 감지나 이상상태 모니터링, 비행 범위 설정, 자동 착륙 등 다양한 안전 기능들이 무인기에 탑재되고 있지만, 악의적인 공격자가 무인기를 해킹한다면 안전 기능들이 정상적으로 작동하지 못하고 사용자나 외부에게 치명적인 피해를 입히게 된다[12]. 현재 악의적인 공격자로부터 안전하게 통신할 수 있도록 Mobile ad hoc Network (MANET)나 Vehicular ad hoc Network (VANET) 등의 무선 네트워크 환경에서 여러 보안 기법들이 연구되고 있지만, 무인기 무선 네트워크에 적용하기에는 컴퓨팅 파워나 통신 거리, 인프라, 데이터 흐름 등이 달라 그대로 적용하기에는 어렵다.

본 논문에서는 이러한 문제점을 해결하기 위하여 물리적으로 복제가 불가능하고 저컴퓨팅 자원을 요구하는 하드웨어 기반 보안 기술 Physical Unclonable Functions (PUFs)를 이용하여 무인기 지상 제어용 네트워크에서 안전하게 무인기와 통신할 수 있는 경량화된 인증 기법을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 무인기 제어 시스템에 대하여 소개하고, 3장에서는 무인기 제어 시스템에서 갖추어야하는 보안 요구사항을 정의한다. 4장에서는 보안 요구 사항을 바탕으로 무인기 제어 시스템에서 안전하게 통신할 수 있는 보안 인프라 및 기법을 제안한다. 5장에서는 제안하는 보안 기법을 기존 보안 기법들과 비교하여 보안성 및 성능을 평가한다. 마지막으로 6장에서 결론을 맺는다.

2. 관련 연구

2.1 UAS 개요

무인항공시스템(UAS: Unmanned Aircraft System)은 무인기(UA: Unmanned Aircraft)의 전 비행과정에서 필요한 무인기, 통신 시스템, 항행, 비행 통제 등의 모든 요소 포함한 시스템이다. Fig. 1과 같이 UA는 UAS 시스템을 통해

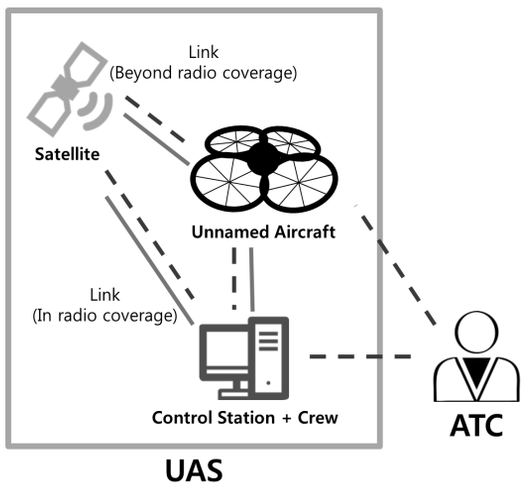


Fig. 1. USA Infrastructure

비가시선통신 기반의 위성이나 가시선통신기반의 지상 제어국(CS: Control Station)으로부터 제어되어 데이터를 교환하며, 데이터를 교환하는 링크에 따라 크게 지상 제어 및 비임무용(CNPC: Control and Non-Payload Communication) 데이터 링크와 UAS 임무용 링크로 구분된다 [13, 14]. 이러한 데이터 링크는 또다시 상향링크와 하향링크로 나누어져, 상향링크는 CS나 위성이 UA에게 제어 명령어나 임무를 전달하고 하향링크는 UA가 수집한 카메라 등의 정보와 임무수행 결과를 CS나 위성에게 전달한다. 만약 위성통신이 아닌데 CS와 UA의 통신거리가 닿지 않을 때에는 네트워크를 통해 지상무선국(GRS, Ground Radio System)을 통해 UA와 통신한다. GRS를 통해 통신 할 때는 UA의 이동경로에 있는 GRS간 핸드오버를 통해 통신을 유지한다. 또한 항공교통관제 센터(ATC: Air Traffic Control)와 주기적으로 통신함으로써 안전하고 효율적으로 운항할 수 있도록 한다.

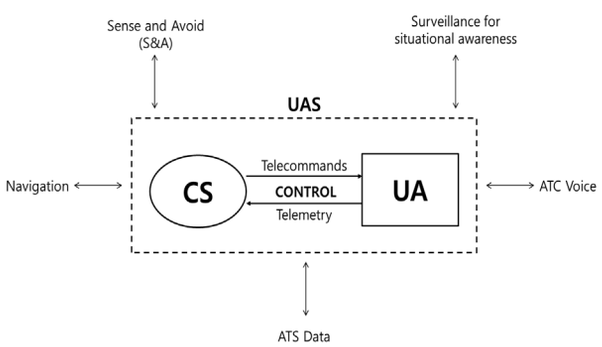


Fig. 2. Internal and External Information Flow of a UAS

UAS에서 교환하는 정보는 Fig. 2와 같다[15]. UAS는 내부적으로 UA와 CS 사이에 고도, 스피드 변경 명령 등과 같은 telecommands와 위도, 기체 상태 정보와 같은 telemetry를 각각 상향링크와 하향링크를 통해 교환하고 UA를 제어한다. 외부적으로는 UA의 Sense and Avoid (S&A) 시스템

을 통해 수집한 목표물 트랙 데이터와, 날씨 레이더 데이터나 비디오 이미지 등의 상황인식 감시 정보, ATC와 UA간에 교환해야하는 음성정보 및 데이터, 항법정보 데이터를 교환한다. UA에게 전달되는 telecommands 데이터들은 주로 적은 용량이지만 UA 동작에 직접적인 영향을 미치며, CS에게 전달되는 telemetry들은 UA가 수집한 대량의 데이터를 CS에게 전달하여 UA 운영에 간접적으로 영향을 미친다. 만약 UAS에서 교환되는 데이터가 간섭되거나 방해를 받아 장애가 생긴다면 UA 운영에 치명적인 피해를 입힐 수 있다. 이러한 문제를 해결하기 위하여 WRC-15에서는 지상 CNPC 링크를 위해 주파수를 61MHz 대역폭인 C 대역(5030~5091 MHz)을 할당하여 전파혼선으로 인한 UA 사고를 최소화 할 수 있도록 하였다[16]. 본 논문에서는 현재 기술 표준화가 활발히 진행 중인 지상 CNPC에서의 보안통신에 대하여 다룬다.

2.2 지상 CNPC 기술

UAS에서 지상 CNPC 링크 인프라는 Fig. 3과 같이 P2P형과 GRS를 통한 네트워크형으로 나누어 진다 [13]. P2P형은 UA가 CS와 중간매개체 없이 바로 통신을 하여 데이터 전송 및 명령을 주고 받는 형태이다. 주로 기존 UAS에서 고려되었던 형태로 UA 조종이 CS의 시야 혹은 통신 범위의 제약을 받지만, 악의적인 사용자로부터 조종권한을 탈취당했거나 제어에 벗어난 행위를 하였을 때 CS가 육안으로 확인할 수 있으며 악의적인 사용자도 공격에 제약을 받는다. 네트워크형은 UA가 CS의 시야나 통신범위에 제약을 받지 않고 지상 네트워크와 GRS를 통해 CS와 통신을 수행하는 형태로 P2P형보다 활용범위가 더 넓다. 그러나 네트워크형은 P2P형과 달리 UA가 활동할 수 있는 범위가 CS에 제약을 받지 않지만, 다수의 UA를 컨트롤 할 수 있는 GRS와 통신 네트워크가 필수적이다. 또한 UA가 기존 통신하고 있는 GRS 네트워크 범위를 벗어나 인접한 GRS 네트워크 영역으로 넘어갔을 때 CS와 끊이지 않고 통신할 수 있는 link handover 기술을 지원해야한다. 네트워크형에서 악의적인 사용자는 CS의 육안에서 벗어나 GRS에 연결되어 있는 UA에 접근하여 권한을 탈취하려 시도 할 수 있으며, 특히 UA가 link handover를 시도할 때 악의적인 사용자는 정상적인 CS로 가장할 수 있으므로 UA와 CS간에 안전한 보안채널을 반드시 구축해야 한다.

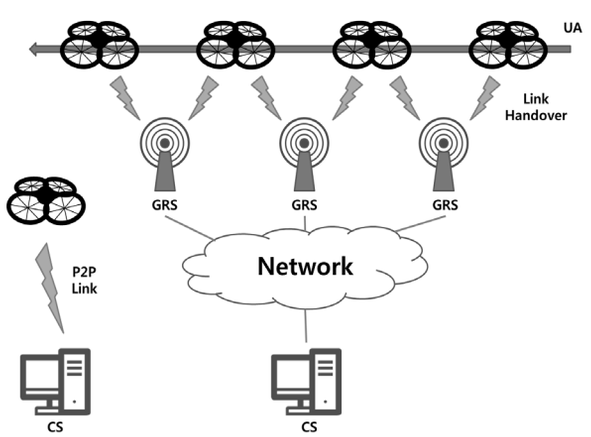


Fig. 3. Infrastructure of Terrestrial based CNPC Link Control

3. UAS 보안 요구사항

UA는 무인 비행체로 미리 입력된 임무를 수행하거나 원격으로 조정할 수 있어 다양한 영역에서 이용될 수 있지만, 악의적인 공격자가 CS와의 통신을 가로채거나 엿들을 수 있는 문제점이 있다[9]. CS와 UA의 안전한 통신 구축하기 위해서는 보안시스템에서 대표적으로 요구하는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 갖추어야 한다[8].

3.1 기밀성(Confidentiality)

기밀성은 기본적으로 시스템의 자원이나 정보에 정당한 권한을 부여받은 사용자만 접근하고 열람할 수 있는 것을 의미하며, 주로 악의적인 사용자가 정보를 가로채는 방법으로 기밀성을 해칠 수 있다. 만약 UAS에서 악의적인 사용자가 통신링크를 통해 정보를 가로챈다면, CS의 의도와 상관없이 UA가 수행하는 임무가 유출될 수 있으며 UA가 임무수행 중에 수집한 민감한 정보들도 노출될 수 있다. 정보를 가로채기 위한 공격 기법으로는 대표적으로 가장 공격, 도청 등이 있다.

3.2 무결성(Integrity)

무결성은 정당한 권한을 부여받은 사용자만이 시스템의 자원이나 정보를 조작하거나 변경할 수 있는 것을 의미하며, 주로 악의적인 사용자는 기존 정보를 변경하거나 새로운 정보로 변조함으로써 무결성을 해칠 수 있다. 만약 UAS가 교환되는 정보들의 무결성을 보장하지 못한다면 CS나 UA는 상대방으로부터 수신한 데이터를 신뢰할 수 없어 의도된 동작을 수행하지 못할 수 있다. 또한 최종적으로 UA가 성공적으로 임무를 수행하였더라도 CS가 제대로 확인할 수 없다. 정보의 무결성을 해치는 공격은 재전송 공격, 데이터 변조, 물리적 공격 등이 있다.

3.3 가용성(Availability)

가용성은 시스템 내외부가 장애 없이 의도된 서비스를 정상적으로 운영하는 것을 의미한다. 악의적인 사용자는 시스템의 가용자원을 의도적으로 고갈시켜 가용성을 해칠 수 있다. 일반적으로 UA는 공중에서 무선으로 임무를 수행하기 때문에 무게에 민감하고 제한적인 파워를 가지고 있으며, 연산을 수행할 수 있는 메모리나 IC도 기존 컴퓨팅 환경보다 적은 자원을 가지고 있다. 만약 UA가 CS와 안전한 통신을 구축하기 위하여 기존 컴퓨팅 환경을 기반으로 한 보안기법을 이용한다면, 악의적인 사용자는 UA에 보안 인증을 시도하는 것만으로 UA의 시스템 자원을 크게 소모시킬 수 있다.

현재 많은 보안모델들이 다양한 무선환경의 통신 링크를 위해 연구되고 있지만, UAS에서 이용되는 무선 통신 네트워크는 컴퓨팅 파워나, 통신 거리, 인프라, 데이터 흐름 등이 센서 네트워크나 ad-hoc 네트워크와 같은 기존 무선환경과 다르기 때문에 적용하기 어렵다. 본 논문에서는 지상 CNPC 환경에서 UA와 CS가 안전하게 통신할 수 있도록 PUFs 기반의 경량화된 보안 기법을 제안한다.

4. 제안하는 기법

본 논문에서는 제안하는 기법은 제안하는 지상 CNPC 인프라에서 UA-CS 등록 프로토콜, UA-CS 인증 프로토콜로 이루어져 있다. 제안하는 프로토콜에서 이용하는 파라미터는 Table 1과 같다.

Table 1. Proposed Protocol Parameters

Notation	Meaning
ID	Identity
CV	Challenge vector
RV	Response vector
C	Challenge value
R	Response value
Ni	Nonce
Ti	Time stamp
SK	Session key
M	Encrypted message
PUF()	Physically Unclonable Function
h()	Hash function
E()	Encryption function
D()	Decryption function
f()	Session key generator

4.1 제안하는 지상 CNPC 인프라

제안하는 지상 CNPC 인프라는 Fig. 4와 같다. UA의 적은 컴퓨팅 자원으로 안전하게 CS와 상호인증을 하기 위하여 각각의 UA에 물리적으로 복제가 불가능한 PUF를 설치한다. PUF는 물리적으로 복제가 불가능한 칩으로 각 PUF마다 유니크한 challenge-response 값을 가지며 키 생성에도 이용될 수 있다[17, 18]. PUF기반의 인증은 PUF의 challenge-response record를 사전에 서버의 DB에 저장하며, 인증을 수행할 때마다 이용한 각 record를 제거함으로써 재사용이 불가능하고 challenge에 대응하는 response 값을 예측할 수 없도록 한다. UA는 사전에 CS와 challenge-response record를 교환하며 차후에 PUF를 기반으로 상호인증 및 키 생성을 수행한다.

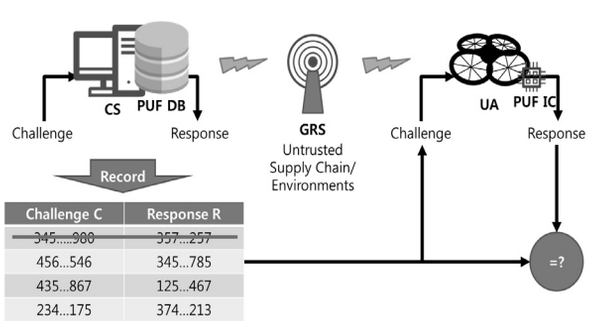


Fig. 4. Proposed CNPC Infrastructure

4.2 UA-CS 등록 과정

Fig. 5는 UA가 CS에 등록하는 과정을 보여준다. 제안하는 프로토콜은 CS와 GRS가 사전에 세션키 SK_{GRS-CS}를 공유하고 있다고 가정한다.

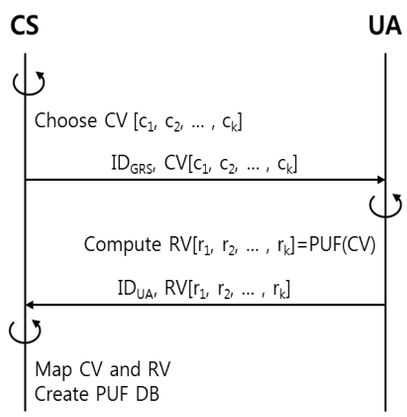


Fig. 5. UA-CS Registration Phase

Step 1. CS는 PUF DB를 만들기 위해 challenge C를 선택하여 challenge 벡터인 CV를 만들어 자신의 ID인 ID_{CS}와 함께 UA에게 전달한다.

Step 2. CS로부터 CV를 전달받은 UA는 자신이 가지고 있는 PUF IC로부터 challenge C에 대응하는 response R을 추출하여 벡터 RV를 만들고 CS에게 자신의 ID인 ID_{UA}와 함께 CS에게 전달한다.

Step 3. UA로부터 RV와 ID_{UA}를 전달 받은 CS는 자신이 만든 CV와 UA로부터 전달 받은 RV를 맵핑하여 PUF DB를 만들어 저장한다.

4.3 UA-CS 상호 인증 과정

Fig. 6은 UA가 CS에 등록한 이후에 CS와 상호인증하는 과정을 보여준다.

Step 1. CS는 UA와 challenge-response를 하기 위한 challenge C값을 선택한다.

Step 2. CS 인증 요청 메시지와 자신의 ID인 ID_{CS},중간 통신 매개체인 GRS의 ID인 ID_{GRS}, 조종하기 원하는 UA의 ID인 ID_{UA}를 C와 함께 GRS을 통해 UA에게 전송한다.

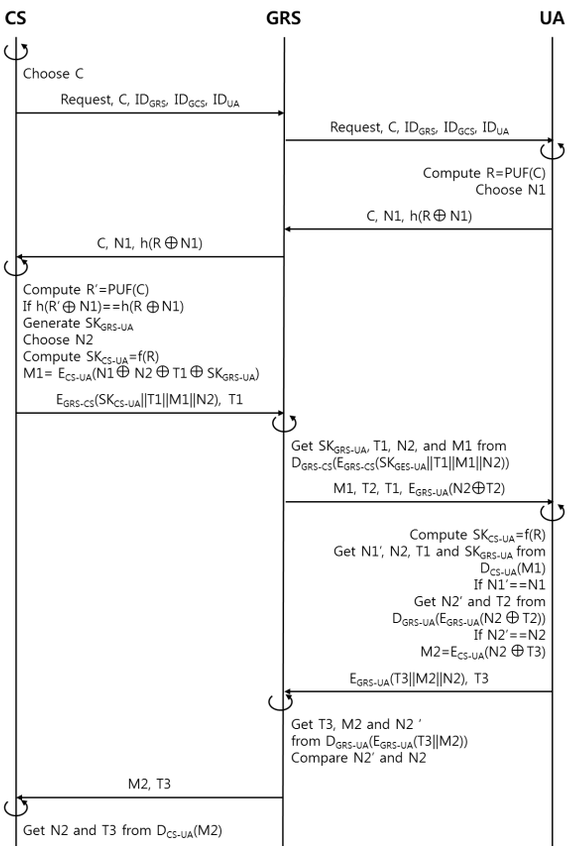


Fig. 6. Authentication Phase Between CS and UA

Step 3. GRS를 통해 CS로부터 값을 받은 UA는 자신에게 내장되어 있는 PUF IC를 통해 challenge C에 대응하는 response R을 추출하고 랜덤값 N1을 선택한다.

Step 4. UA는 R값과 N1값을 XOR하고 해쉬하여 h(R⊕N1)를 계산한다. 그리고 C값과 랜덤값 N1과 함께 GRS을 통해 CS에게 전송한다.

Step 5. GRS를 통해 UA로부터 값을 전달받은 CS는 PUF DB에서 C에 대응하는 R′를 추출하고 h(R′⊕N1)를 계산한다. 만약 h(R′⊕N1)이 h(R⊕N1)와 같으면 UA를 인증하고, GRS와 UA가 사용할 세션키 SK_{GRS-UA}를 생성한다. 그리고 GRS와 UA가 서로 인증하기 위한 랜덤값 N2를 생성하고, CS와 UA의 세션키 SK_{CS-UA}=f(R)를 생성한다. 마지막으로 UA에게 전달할 N1, N2, T1, SK_{GRS-UA}를 모두 XOR하고 세션키 SK_{CS-UA}로 암호화하여 $M1=E_{CS-UA}(N1⊕N2⊕T1⊕SK_{GRS-UA})$을 만든다.

Step 6. M1를 생성한 CS는 SK_{CS-UA}, T1, M1, N2를 서로 연접하여 GRS와 사전에 공유하고 있는 세션키 SK_{CS-UA}로 암호화한 $E_{GRS-CS}(SK_{CS}-UA||T1||M1||N2)$를 T1과 함께 GRS에게 전달한다.

Step 7. GRS는 CS로부터 전달 받은 $E_{GRS-CS}(SK_{CS}-UA||T1||M1||N2)$를 복호화하여 UA와의 세션키 SK_{GRS-UA}와 T1, N2, M1을 추출하고 타임스탬프 T1을 확인한다. 그리고 N2와 T2 XOR하여 UA와의 세션키 SK_{GRS-UA}로 암호화한 $E_{GRS-UA}(N2⊕T2)$를 M1, T2값과 함께 UA에게 전달한다.

Step 8. UA는 R값을 통해 CS와의 세션키 SK_{CS-UA}=f(R)를 생성하여, M1으로부터 N1′와 N2, T1, SK_{GRS-UA}를 추출하고 타임스탬프 T1을 확인한다. 만약 추출한 N1′가 처음 CS에게 전달받은 N1과 일치하면 CS를 인증한다. 그리고 SK_{GRS-UA}로 $E_{GRS-UA}(N2⊕T2)$를 복호화하여 N2′와 T2를 추출하고 타임스탬프 T2를 확인한다. 만약 N2′와 N2가 일치하면 GRS를 인증하고, N2와 T3을 XOR하고 CS와의 세션키 SK_{CS-UA}로 암호화하여 CS에게 전달한 M2를 만든다.

Step 9. UA는 T3과 M2, N2를 연접하고 GRS와의 세션키 SK_{GRS-UA}로 암호한 $E_{GRS-UA}(T3||M2||N2)$를 T3와 함께 GRS 에게 전달한다.

Step 10. UA로부터 값을 전달받은 GRS는 $E_{GRS-UA}(T3||M2||N2)$를 UA와의 세션키 SK_{GRS-UA}로 복호화하여 T3과 M2, N2′를 추출하고 T3을 확인한다. 만약 N2'가 CS로부터 전달받은 N2와 일치하면 UA를 인증한다.

Step 11. UA를 인증한 GRS는 M2와 T3을 CS에게 전달한다.

Step 12. GRS로부터 값을 전달 받은 CS는 UA와의 세션키 SK_{CS-UA}로 M2를 복호화하여 N2와 타임스탬프 T3을 확인하고 GRS와 UA가 정상적으로 세션키를 교환했음을 확인한다.

5. 성능 평가

본 논문에서 제안하는 기법은 물리적으로 복제가 불가능한 PUF를 기반으로 UA와 CS사이에서 안전하고 적은 컴퓨팅 자원을 효율적으로 이용하는 상호 인증 기법이다. 제안하는 기법을 평가하기 위해 기밀성, 무결성, 가용성 측면에서 다양한 공격들에 대해 분석하고 기존 보안 기법과 비교·분석하였다. Table 2는 제안하는 보안 기법과 MANET, VANET, 드론 환경에서 제안된 기존 보안 기법을 비교 분석한 결과를 보여준다[20, 21].

Table 2. Comparative Security Analysis

	Verma et al.	Studer et al.	Wang et al.	Proposed scheme
Eavesdropping	O	O	O	O
Masquerade attack	O	O	O	O
Physical attack	X	X	X	O
Replay attack	X	O	O	O
Data modification	O	O	O	O
Row resource	X	X	Δ	O

O: Support, Δ: Not fully support, X: Not support

5.1 기밀성(Confidentiality)

제안하는 인증 기법은 UA와 CS 간에 교환하는 데이터가 허가받지 않은 개체로부터 노출되지 않도록, 매 세션마다 세션 키를 교환하여 보안채널을 구축한다. 또한 기밀성을 해칠 수 있는 악의적인 사용자의 도청이나 가장 공격으로부터 안전하게 설계되었다.

• 도청(Eavesdropping)

CS와 GRS, UA 사이에서 악의적인 공격자는 교환되는 데이터를 도청하여 기밀성을 해칠 수 있다. 그러나 CS가 UA와 상호인증하기 위해 교환하는 데이터들 중에 PUF()의 challenge C값과 랜덤 N값은 비밀값이 아니고 재사용되지 않으며, 타임스탬프 T도 공개된 값이다. 그리고 세션키를 생성하거나 인증을 하기 위한 비밀값은 랜덤값과 함께 해시 h()되거나 세션키로 암호화 E() 되어 전달되므로 악의적인 공격자에게 노출되지 않는다.

• 가장 공격(Masquerade attack)

악의적인 공격자는 CS나 GRS, UA로 가장하고 CS와 UA 사이에 전달되는 정보들을 가로채어 기밀성을 해칠 수 있다. 그러나 만약 악의적인 공격자가 UA로 가장하려면 물리적으로 유니크한 UA의 PUF를 복제하거나 UA가 사전에 CS에 등록한 PUF의 challenge-response 값을 예측할 수 있어야 한다. 그러나 PUF는 물리적으로 복제가 불가능하고 모든 PUF마다 유니크한 challenge-response 값을 산출하므로 예측하기가 매우 어렵다. 또한 CS로 가장하여 UA에 인증을 시도하여도 재사용 되지 않는 PUF의 response 값으로 생성한 세션키 $SK_{CS-UA}=f(R)$가 필요하므로 불가능하다. GRS는 UA와 CS에 사이에 교환되는 인증값이 평문으로 전달되지 않아 볼수 없으며, GRS로 가장을 시도하려고 해도 CS와 사전에 공유하고 있는 세션키 SK_{GRS-CS}가 필요하다.

5.2 무결성(Integrity)

제안하는 기법은 지상 CNPC 인프라에서 교환되는 데이터의 무결성을 보장하기 위해서 매번 교환하는 데이터 마다 무결성을 확인 한다. 또한 악의적인 사용자의 물리적 공격이나, 재사용 공격, 데이터 변조 공격 등으로부터 무결성을 보장한다.

• 물리적 공격(Physical attack)

만약 제안하고 있는 프로토콜이 상호인증에 기반하고 있는 PUF가 물리적으로 복제되거나 변조 된다면, 악의적인 공격자가 정상적인 사용자로 가장하여 데이터를 가로채어 기밀성을 해칠 수 있다. 그러나 PUF는 IC가 제조될 때 랜덤적으로 생성되는 유니크한 물리적인 특성을 이용하여 물리적인 복제가 불가능하다. 또한 PUF가 물리적으로 변조된다면 UA가 등록과정에서 CS에 등록한 PUF의 challenge-response mapping 값과 달라지므로 악의적인 공격자는 변조된 PUF를 더 이상 이용할 수가 없다.

• 재사용 공격(Replay attack)

악의적인 공격자는 CS와 UA가 상호 인증과정 중에 교환하는 데이터를 도청하여 재사용 공격을 시도하여 무결성을 해칠 수 있다. 그러나 악의적인 공격자가 challenge-response 값에 대하여 재사용 공격을 시도하여도 CS는 UA와 인증을 하고서 PUF DB로부터 사용한 challenge-response 값을 제거하므로 재사용할 수 없다. 그리고 UA가 CS에게 인증하기 위하여 전달하는 N값은 매번 랜덤으로 생성되므로 재사용될 수 없다.

• 데이터 변조(Data modification)

악의적인 공격자는 GRS를 거쳐 교환되는 CS와 UA 사이의 데이터를 변조 및 가짜 데이터 전송을 하여 무결성을 해칠 수 있다. 그러나 제안하는 프로토콜에서는 상호인증을 통해 UA와 CS가 서로 인증하고 세션키를 생성하여 보안통신을 하므로 악의적인 공격자가 암호화된 데이터를 변조하거나 가짜 데이터를 전송하는 것이 어렵다.

5.3 가용성(Availability)

Fig. 7은 제안하는 인증 기법에서 키를 생성할 때 시간과 RSA 기법에서 키를 생성할 때의 시간을 비교하여 그래프로 보여준다. 제안하는 기법에서 f()는 SHA-256을 이용하였다. 제안하는 인증 기법에서는 세션키를 CPU를 거치지 않고 PUF에서 R값을 추출하여 f(R)를 통해 생성한다. UA와 CS가 안전한 채널을 구축하기 위하여 PUF 기반으로 기존의 키 생성 기법보다 적은 컴퓨팅 자원과 시간으로 세션키를 생성하기 때문에, CS가 한번에 여러 UA와 인증을 시도하거나 악의적인 사용자가 여러번의 인증을 시도하여 UA와 CS의 자원을 소모시키려고 할 때 기존 기법보다 안정적으로 서비스를 제공할 수 있다.

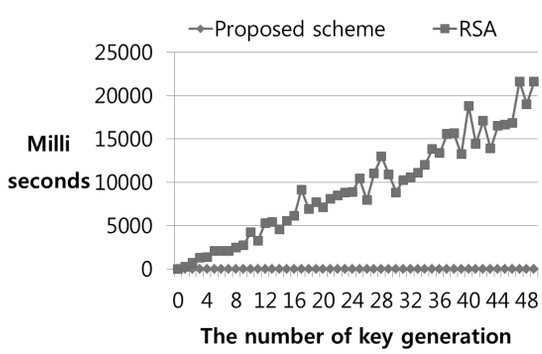


Fig. 7. Comparison of Time for Key Generation

6. 결 론

무인기는 조종사가 탑승하지 않고 무선 혹은 미리 입력된 임무에 따라 컨트롤되는 비행체로 초기에는 군용으로 대부분 이용되었으나 최근 민간 영역에서도 많이 이용되고 있다. 중국의 DJI는 전 세계 민수 무인기 분야 1위 기업으로

이미 다양한 민간용 무인기를 출시하고 있으며, Teal Group의 2014년 World UAV Forecast에 따르면 향후 10년간 무인기 시장은 매년 10%씩 성장하여 2023년에는 125억 달러에 이른다고 전망하였다. 그러나 성장하는 무인기 사장에 비례하여 다양한 문제들이 이슈가 되고 있는데, 만약 운행중인 무인기가 악의적인 공격자로부터 권한을 탈취당한다면 추락을 하거나 다른 사람의 프라이버시를 크게 침해할 수 있다[19]. 이러한 문제점을 예방하기 위하여 UA와 CS 간에 안전한 보안채널을 구축해야 하지만 기존 보안 기법은 제한적인 컴퓨팅 자원을 가지고 있는 UAS환경에 적합하지 않다. 본 논문에서는 이러한 문제점을 해결하기 위하여 현재 기술 표준화가 활발하게 진행 중인 지상 CNPC에서의 인증기법을 제시하였고, 보안 기법이 갖추어야 하는 기밀성, 무결성, 가용성을 기준으로 제안하는 기법의 안정성과 효율성을 평가하였다.

References

[1] C. Drubin, "The Global UAV Market 2015 - 2025," *Microw. J.*, Vol.58, No.3, pp.53-54, Mar., 2015.

[2] Y. I. Bae and H. R. Shin, "Prerequisites for Drones Industry Development," *Issue & Analysis*, No.237, pp.1-25, 2016.

[3] S. J. Song and B. O. Kil, "A Study on the Glo UAV Market," *KADIS*, Vol.22, No.4, pp.49-76, 2015.

[4] B. Canis, "Unmanned aircraft systems (UAS): Commercial outlook for a new industry," Congressional Research Service, Washington, 2015.

[5] J. H. Jin and G. B. Lee, "Understanding and Trend of UAV / Dron," *KICS*, Vol.33, No.2, pp.80-85, 2016.

[6] A. R. Lee, "Weekly Tip - Industry," *CRPC*, Vol.53, 2017.

[7] J. H Lee, Y. T. Kim, J. Y. Seo, and S. J. Hwang, "2015 World Radiocommunication Conference (WRC-15)," *TTP. J.*, Vol.163, pp.105-109, 2016.

[8] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," *Homeland Security (HST), 2012 IEEE Conference on Technologies for. IEEE*, pp.585-590, 2012.

[9] N. M. Rodday, R. D. O. Schmidt, and A. Pras, "Exploring security vulnerabilities of unmanned aerial vehicles," *Network Operations and Management Symposium (NOMS),* 2016 IEEE/IFIP. IEEE, pp.993-994, 2016.

[10] J. H. Kim, B. K. Kim, and Y. T Shin, "A Study on the Improvement of security vulnerabilities in Civilian Drone," *KIISE*, pp.1069-1071, 2016.

[11] C. A. Gomez, "Cybersecurity of unmanned aircraft systems (UAS)," Diss. UTICA COLLEGE, 2015.

[12] F. Schenkelberg, "How reliable does a delivery drone have to be?" *Reliability and Maintainability Symposium (RAMS), 2016 Annual,* IEEE, 2016.

[13] H. W. Kim, K. S. Kang, D. I. Chang, J. Y. Ahn, "Technical and Standardization Trends on Control and Non-Payload Communications for Unmanned Aircraft Systems," ETRI, Vol.30, No.3, pp.74-83, 2015.

[14] R. J. Kerczewski, and J. H. Griner, "Control and Non-Payload Communications Links for Integrated Unmanned Aircraft Operations," 2012.

[15] J A. Kakar, "UAV communications: Spectral requirements, MAV and SUAV channel modeling, OFDM waveform parameters, performance and spectrum management," Diss. Virginia Tech, 2015.

[16] Y. H. Kang, "An Efficient Frequency Utilization Policy for UAS in Hyper-Connectivity Era," *The Journal of Korean Institute of Electromagnetic Engineering and Science*, Vol.26, No.10, pp.914-923, 2015.

[17] R. Maes, "Physically Unclonable Functions," Springer, Berlin, 2013.

[18] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," *Proceedings of the 44th annual Design Automation Conference*, ACM, 2007.

[19] B. Jenkins, "Watching the Watchmen: Drone Privacy and the Need for Oversight," *Ky. LJ*, Vol.102, pp.161-182, 2013.

[20] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *Journal of Communications and Networks*, Vol.11, No.6, pp.574-588, 2009.

[21] G., Wang, B. S. Lee, and J. Y. Ahn, "Authentication and Key Management in an LTE-Based Unmanned Aerial System Control and Non-payload Communication Network," *In Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on*, IEEE, pp.355-360, Aug., 2016.

[22] U. K. Verma, S. Kumar, and D. Sinha, "A secure and efficient certificate based authentication protocol for MANET," *In Circuit, Power and Computing Technologies (ICCPCT), 2016 International Conference on,* IEEE, pp.1-7, Mar., 2016.

김 만 식

e-mail : mansik@ssu.ac.kr

2010년 안양대학교 컴퓨터공학과(학사)

2012년 Towson University Computer Science(석사)

2014년~현 재 숭실대학교 컴퓨터학과 박사과정

관심분야 : 네트워크 보안, 드론, IoT, 스마트 디바이스

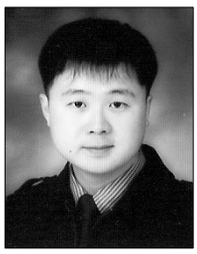
전 문 석

e-mail : mjun@ssu.ac.kr

1989년 Univ. of Maryland Computer Science(박사)

1991년~현 재 숭실대학교 컴퓨터학과 교수

관심분야 : RFID, PKI 컴퓨터통신



강 정 호

e-mail : kjh@naver.com

2000년 서울과학기술대학교 컴퓨터공학과 (학사)

2002년 서울과학기술대학교 컴퓨터공학과 (석사)

2013년~현 재 숭실대학교 평생교육원 정보보안학과 교수

관심분야 : 네트워크 보안, NFC, IoT