무인항공기 시스템의 안전한 제어를 위한 키 관리 프로토콜 설계

방재석
(주)카스아이
e-mail:bangory@cassi.kr

A Design of Key Management Protocol for Secure Control of Unmanned Aerial Vehicle System

Jae-Seok Bang
Cassi Co., Inc

요 약

무인항공기 시스템은 사용자가 무인비행체를 무선으로 제어하고 자율적으로 운행하는 시스템을 통칭한다. 무인항공기는 주로 군용으로 제작되어 감시, 촬영과 간이 군사적인 목적으로 제작되었으나, 민간에 수요가 발생함에 따라 사용자로부터 다양한 서비스를 제공하고 있다. 그러나, 무인항공기는 공격자에 의해서 끊임없이 해킹이 시도되고 있으며, 취약점으로 인한 불법접근이 발생 시 경제적 및 사회적 피해가 발생할 수 있다. 그러므로 본 논문에서는 무인항공기의 안전한 제어를 위한 키 관리 프로토콜을 설계하도록 한다.

1. 서론

군용목적으로 활용되면 무인항공기는 민간 수요가 발생함에 따라서 다양한 종류의 서비스가 제공되고 있으며, 국내외 기업에서 활발히 연구가 진행되고 있다.

사용자로부터 택배, 통신 서비스 영역확대, 재해 재난 방지 대처, 도로교통 시스템 지원 등 다양한 편의성을 제공하여 삶의 질을 높이고 있다.

무인항공기는 무선 네트워크 기반의 통신을 활용함으로써 해커의 공격타깃으로 끊임없이 해킹을 시도하고 있으며, 운행방해, 정보탈취, 기기 탈취 등에 때한 보안위협이 발생되고 있다. 또한 테러리스트의 불법적인 사용을 통해 경제적 피해와 인명피해가 발생할 수 있다.

본 논문에서는 무인항공기 시스템의 안전한 제어를 위해 키 관리 프로토콜을 제안한다.

2. 관련연구

2.1 무인항공기 동향 및 활용 사례

무인항공기는 군용 및 민간기로 구분되고 있으며, 군용은 감시용, 수송용, 감시용, 민간기에서는 촬영, 운송, 농업 등에 활용되어 사용자로부터 편의성을 제공하고 있다. 무인항공기는 형태, 크기, 무게, 고도에 따라서 분류되고 있다.

무인항공기는 교통, 의료, 재난구조 및 지원, 범죄예방 등과 같은 다양한 분야에서 활용되고 있으며, 국내외 기업에서 지속적으로 연구하고 있다.

군용기술에서 민간용 기술로 확대됨에 따라서 활용범위가 지금보다 넓혀지고 있으며, 4차 산업의 핵심기술인 융합기술의 발전을 기대하고 있다.

2.2 무인항공기 시스템의 보안요구사항

무인항공기 시스템 환경에서는 무선신호 침해, 정보변조, 물리적 위협에 따른 유형이 있으며, 대표적으로 무인증 무선 네트워크 접속, Jamming 공격, 물리적 탈취, 비인가 장비 등에 따른 보안위협이 존재한다.

무인항공기에서 촬영한 영상에 따른 정보유출, 중요데이터 탈취가 있으며, 테러리스트를 통한 폭탄테러, 화학물 공격과 같은 사람의 생명을 위협할 수 있는 문제점이 발생할 수 있다.

위의 언급한 보안위협을 방지하기 위해서 무인항공기, 무인항공기에 따른 데이터, 제어용 통합 네트워크의 대한 보안 요구사항이 필수적이다.

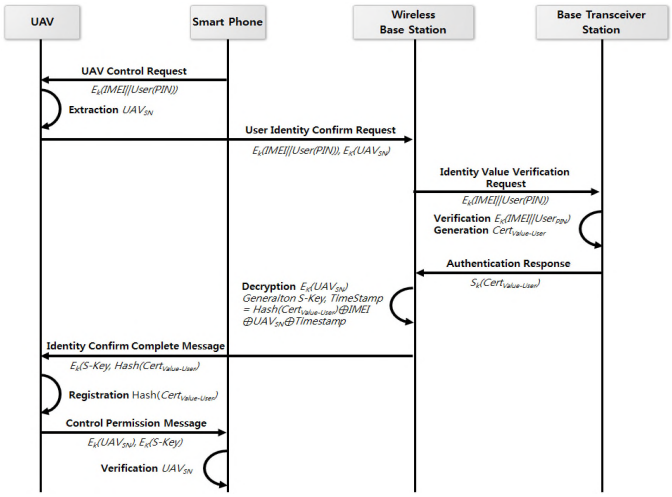
첫 번째, 무인항공기 제어에 따른 인증, 무결성, 기밀성이 보장되어 한다. 두 번째 무인항공기의 데이터에서는 안전한 암호화 기법을 통한 데이터 보안, 상호간의 식별기법 등 요구

된다. 마지막으로 제어용 통합네트워크에서는 사용자 및 무인기 식별을 위한 상호인증 및 키 관리기법이 요구된다.

3. 무인항공기 시스템의 안전한 제어를 위한 키 관리 프로토콜 설계

본 장에서는 사용자가 스마트폰을 활용하여 무인항공기(드론)의 안전한 제어를 위한 키 관리 프로토콜을 제안한다. 무인항공기 및 사용자 식별 확인 절차, 키 관리 프로토콜에 대해서 서술한다.

3.1 무인항공기 및 사용자 식별 확인 절차



[그림 1] 무인항공기 및 사용자 식별 관련 프로토콜 (키 생성 포함)

1. 사용자는 무인항공기의 제어를 수행하기 위해 제어 요청 메시지를 송신한다.

$$E_K(IMEI||User(IIN))$$

2. 무인항공기의 시리얼 넘버를 추출 후 사용자로부터 받은 메시지와 함께 암호화를 수행하여 기지국으로 메시지를 전송한다.

$$E_k(IMEI||User(IIN)), E_k(UAV_{SN})$$

3. 기지국에서 이통관리국으로 사용자의 IMEI, PIN의 검증을 수행을 위한 검증 요청 메시지를 전송한다.

$$E_k(IMEI||User(IIN)$$

4. 이통관리국에서는 수신 받은 메시지를 확인 후 Cert Value를 생성한다. 이후 이통관리국과 기지국간의 상호 교환한 세션키를 활용하여 Cert Value를 전송한다.

$$S_k(Cert_{Value-user})$$

5. 무선기지국에서는 수신한 UAV에서 수신한 메시지를 복호화 후 이를 기반으로 S-Key를 생성한다.

$$S-Key = Hash(Cert_{Value-User}) \oplus IMEI \oplus UAV_{SN} \oplus Time\ stamp$$

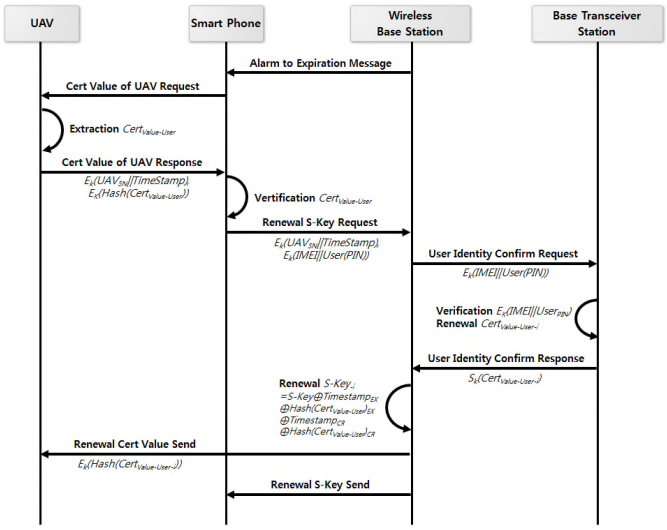
6. 무선기지국에서는 해쉬함수를 통한 증명서와 S-key를 UAV로 식별값 확인 완료메시지를 송신한다.

$$E_k(S-Key, Hash(Cert_{value-User}))$$

7. UAV에서는 수신한 증명서를 등록 후 수신 받은 S-key, 자신의 시리얼 넘버를 사용자로부터 전송한다.

8. 사용자는 시리얼 넘버를 등록 후 생성한 S-Key를 활용하여 UAV를 제어한다.

3.2 키 관리 프로토콜 설계



[그림 2] 키 관리 프로토콜 설계

1. 무선기지국에서는 관리하고 있는 인증서를 확인 후 사용자로부터 만료예정 메시지를 전송한다.

2. 사용자는 UAV로부터 인증서의 만료된 메시지를 확인하기 위해서 Cert Value를 요청한다.

3. UAV는 Cert Value를 추출 후 사용자로부터 Cert Value 응답메시지를 전송한다.

$$E_k(UAV_{SN}||Time\ stamp), E_k(Hash(Cert_{Value-User}))$$

4. 사용자는 Cert Value를 확인 후 무선기지국으로부터 S-Key 갱신 요청 메시지를 송신한다.
$E_k(UAV_{SN} \| Time\,stamp), E_k(IMEI \| User(PIN)$

5. 무선기지국에서는 이통관리국으로 사용자 신원 확인 요청 메시지를 전송한다.
$E_k(IMEI \| User_{PIN})$

6. 이통관리국은 수신한 메시지를 검증 후 Cert Value를 갱신한다. 이후 무선기지국으로 세션키를 활용 후 암호화하여 갱신된 Cert Value를 전송한다.

$$S_k(Cert_{Value-User-i})$$

7. 수신 받은 메시지를 확인 후 무선 기지국에서는 키 관리를 수행하기 위해서 S-Key$_i$를 갱신한다.

$$\begin{aligned} & S-Key_i \\ & = S-Key_i \oplus Time\,stamp_{ex} \\ & \oplus Hash(Cert_{Value-user})_{ex} \\ & \oplus Time\,stamp_{CR} \\ & \oplus Hash(Cert_{Value-User})_{CR} \end{aligned}$$

8. 기지국에서는 UAV로부터 갱신된 Cert Value를 전송한다. 그리고 사용자로부터 S-key를 전송한다.
$E_k(Hash(Cert_{Value-User-i})$

4. 안전성 분석 및 비교분석

본 장에서는 무인기 시스템 환경에서 발생하는 보안위협에 따른 안전성 분석 및 비교분석을 수행한다. 무인 시스템에서 발생하는 보안위협에 따른 안전성 분석은 다음과 같다.

비 인가 된 사용자의 접근: 비 인가 된 사용자의 접근위협은 무선 네트워크 환경에서 발생하는 대표적인 공격기법이다. 이를 방지하기 위해서 사용자 식별절차에서 생성한 S-key기반으로 인가된 사용자만 접근이 가능하다. 그리고 안전하게 제어를 하기 위해 키 관리 프로토콜에서 S-key를 갱신하여 비인가 된 상용자의 접근이 불가능하다.

데이터 변조 위협: 공격자가 무선 네트워크상의 데이터를 탈취하여 변조하는 공격이 빈번히 발생하는데 이를 막기 위해서 본 논문에서는 Cert-Value의 값을 사용자와 기지국간에 확인하여 데이터 위변조를 수행하지 못하도록 한다.

물리적 기기에 대한 위협: UAV 장비에 대한 분실 및 도난이 발생하여 이를 제어할 수 있는 위협이 발생할 수 있다. 이에 대한 물리적 위협을 방지하기 위해 기기의 UAV_{SN}과 사용자의 $IMEI$, PIN에 대해서 검증을 수행하여 기기 소유자에 알맞은 권한을 확인하도록 한다.

jamming 신호 및 악성코드 삽입 : 무인항공기 시스템에서 자주 발생하는 공격기법으로 운영 중인 무인항공기에 Jamming 신호를 보내서 신호를 교란시키는 기법이다. 이에 대한 공격을 막기 위해 사용자 접근에 대한 S-key를 활용하여 제어하도록 설계하였으며, Cert-Value를 주기적으로 관리함으로써 안전하게 운용하도록 설계하였다.

5. 결론

본 논문에서 무인항공기 시스템의 안전한 제어를 위한 키 관리 프로토콜을 설계하였다. 무인항공기 및 사용자를 식별 후 생성된 값을 기반으로 제어하도록 하였으며, 추후 안전한 제어를 위해 키 관리 갱신프로토콜을 제안하였다.

무선 항공기 시스템의 발생하는 보안위협 및 공격기법에 대해서 안전성을 분석하였으며, 기존 시스템 환경과 비교분석을 수행하였다.

향후 무인항공기 시스템뿐만 아니라, 전체적인 네트워크 환경에 대한 보안성 연구가 요구된다. 그리고 무인항공기의 효율적인 제어와 신규•변종 공격기법에 따른 대응방안이 필요하다.

참고문헌

[1] 왕기철 외 4명, 무인기 제어용 네트워크의 보안기술 동향, ETRI, No32, Vol1, 2017.2

[2] 김희욱 외, “무인기 제어용 무선통신 기술 및 표준화 동향”,ETRI, 전자통신동향분석, 제 30권, 3호, 2015. 6, pp. 74-83

[3] R.J. Kerczewski and J.H. Griner, “Control and Nonpayload Communications Links for Integrated Unmanned Aircraft Operations,” Proc. Join Conference-18th Ka and Broadband, Sept. 2012, Ottawa, Canada, pp. 24-27.

[4] D.C. Iannicca et al., “Control and Non-payload Communications (CNPC) Prototype Radio - Generation 2 Security Architecture Lab Test Report,” Tech. Report, NASA/TM-2015-218453, May 1st, 2015.

[5] D.C. Iannicca et al., “Control and Non-payload Communications (CNPC) Prototype Radio - Generation 2 Security Flight Lab Test Report,” Tech. Report, NASA/TM-2015-218821, June 1st, 2015.

[6] S.N. Marwat et al., “Congestion-Aware Handover in LTESystems for Load Balancing in Transport Network,” ETRI Journal, vol. 35, no. 5, Oct. 2014, pp. 761-771.