ETRI

2017
Electronics and
Telecommunications
Trends

무인기 제어용 네트워크의 보안기술 동향

Technical Trends on Security of Control and Non-payload Communications Network for Unmanned Aircraft Systems

왕기철 (G.C. Wang) 무인이동체시스템연구그룹 선임연구원
이병선 (B.S. Lee) 무인이동체시스템연구그룹 책임연구원
임광재 (K.J. Lim) 무인이동체시스템연구그룹 책임연구원
안재영 (J.Y. Ahn) 자율무인이동체연구본부 책임연구원

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음[R0126-16-1005, 고신뢰성 다종 무인이동체 통신 및 보안 SW기술 개발].

최근 들어 무인기와 무선통신기술의 비약적인 발전은 무인기들을 국가 공역에 진입시켜 운행할 필요성과 택배, 긴급 통신영역 확장, 재해 감시 및 대처, 위험지역 정찰, 항공촬영과 같은 다양한 분야로의 활용에 대한 요구를 크게 증가시켰다. 다수의 무인기를 안전하게 운행 및 조종하기 위해서는 고신뢰성 및 고보안성을 제공하는 무인기 제어 전용 네트워크가 요구되며, 이러한 네트워크를 무인기 제어용 통합 네트워크라고 한다. 본고는 무인기 제어용 통합 네트워크의 보안 적용 구간을 분류하고, 구간별로 보안 요구사항과 요구사항을 달성할 수 있는 보안기술들을 차례로 제시한다. 또한, 향후에 무인기 제어용 통합 네트워크의 보안성을 강화하기 위해 개선되어야 하는 부분들을 제시한다.

Ⅰ. 서론

일반적으로 무인기는 원격지에서 조종사가 무선으로 비행을 조종 및 제어하거나 자율적으로 비행하는 비행체를 통칭한다. 무인기는 과거에는 거의 군용으로만 만들어져 이용되었으나, 최근에 무인기에 대한 민간의 수요가 커져서 다양한 형태의 민간용 무인기들이 출시되고 있다. 이러한 무인기들은 택배, 긴급 통신영역 확장, 재해 감시 및 긴급 대처, 위험지역 정찰, 항공촬영과 같은 다양한 임무를 인간을 대신하여 수행할 것으로 기대된다.

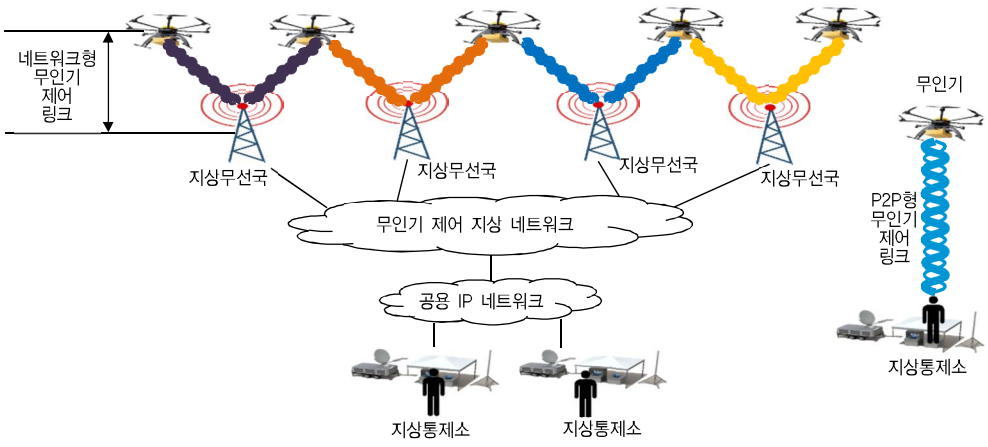
무인기들에 대한 민간의 수요가 증대됨에 따라, 무인기의 국가 공역 운행에 필요한 법과 제도적 노력도 이루어져야 하고, 더불어서 무인기의 안전하고 신뢰성 있는 운행을 위한 기술적 노력도 이루어져야 한다. 이러한 기술적 노력은 유인기와 동일한 수준의 탐지회피 능력 확보, 유무인기 통합 항공 및 교통 관리, 고신뢰성 및 고보안성의 무인기 제어 링크 확보 등을 포함해야 한다[1]. 본고에서는 이들 중 고신뢰성 및 고보안성의 무인기 제어 링크에 집중한다. 특히, 본고는 무인기 제어 링크의 보안 기술에 대해 집중적으로 조명하고자 한다. 무인기 제어 링크는 무인기와 무인기를 조종하고 제어하기 위한 지상통제소(GCS: Ground Control Station)의 조종사가 무선으로 직접 연결된 P2P형의 링크와 지상의 모바일 네트워크를 통해 간접적으로 연결된 네트워크형 링크로 구분된다. 무인기와 GCS를 연결하는 지상의 모바일 네트워크를 무인기 제어 지상 네트워크라 칭한다. 또한, 이후부터 본고에서 언급하는 무인기 제어용 통합 네트워크는 무인기, 무인기 제어 지상 네트워크, 그리고 지상통제소가 연결된 네트워크를 의미한다. (그림 1)은 위에서 설명한 무인기 제어용 통합 네트워크 구성도를 보여준다.

본고의 구성은 다음과 같다. Ⅱ장에서는 무인기 제어용 통합 네트워크의 구성 및 보안 위협을 살펴본다. Ⅲ장에서는 무인기 제어용 통합 네트워크를 여러 개의 보안 적용 구간으로 분리하고 각 구간에 필요한 보안 서비스들을 설명한다. Ⅳ장에서는 무인기 제어용 통합 네트워크의 각 보안 적용 구간에 이용되는 보안기술들을 자세히 살펴 본다. Ⅴ장에서는 향후에 무인기 제어용 통합 네트워크의 보안성을 강화하기 위한 선결 과제를 제시한다.

Ⅱ. 무인기 제어용 통합 네트워크

1. 무인기 제어용 통합 네트워크의 구성

무인기 제어용 통합 네트워크는 다수의 무인기들과



(그림 1) 무인기 제어용 통합 네트워크[1]

무인기들을 조종 및 제어하는 지상통제소(GCS), 그리고 무인기들과 지상통제소를 결합시켜 주는 무인기 제어 링크로 구성된다. 무인기 제어 링크는 두 가지 형태로 분류된다. 먼저 무인기가 무선링크를 통해 직접 지상 통제소로 연결되고 조종 및 제어되는 P2P형 링크이다. P2P형의 링크는 군 무인기 시스템, 재난구조 수행, 긴급 통신영역 확장과 같은 특수한 통신 환경에서 작은 수의 무인기들을 이용하여 임무를 수행하기 위해 사용한다. 다른 하나는 무인기들이 LTE(Long-Term Evolution)나 IEEE 802.16과 같은 무선 고속 통신 네트워크를 통해 지상통제소와 연결되고 제어 및 조종되는 네트워크형 링크이다. 네트워크형 무인기 제어 링크는 무선 고속 통신 네트워크를 통해 다수의 무인기들을 조종하고 제어할 수 있는 방법으로 향후에 무인기의 대중화 및 이용 증가에 잘 대처할 수 있는 장점이 있다. 미국의 사례를 보면 NASA(National Aeronautics and Space Administration)는 무인기 제어 지상 네트워크로서 IEEE 802.16, LTE, P-34/TETRA Enhanced Data Service(TEDS)를 고려하였다가 결론적으로 IEEE 802.16을 채택하였다[2].

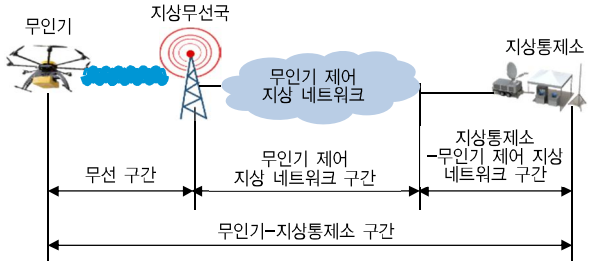
2. 무인기 제어용 통합 네트워크의 보안 위협

무인기 제어용 통합 네트워크에서 전달되는 데이터는 지상통제소의 조종사로부터 무인기에게 전달되는 Telemetry 정보와 무인기로부터 지상통제소의 조종사에게 전달되는 Tele-command 정보로 구성된다. Telemetry 정보는 무인기의 위치, 고도, 속도, 무인기 동작모드 및 상태, 항법보조데이터, 탐지 및 회피관련 추적정보, 영상정보 등을 담고 있다. Tele-command 정보는 비행궤도 제어 정보, 안정된 통신을 위한 제어 정보, 안전운행을 위한 무인기 제어정보 등을 담고 있다. Telemetry 정보와 Tele-command 정보는 무인기의 안전한 운행에 필수적인 데이터이기 때문에 인가되지 않은 사용자의 불법적인 접근, 획득 및 위/변조를 차단하여야 한다. 이를 위해서는 상호인증, 전송정보의 기밀성, 무결성, 최신성, 책임성과 같은 보안서비스들이 무인기 제어 링크에 보장되어야 한다. 일반적으로 P2P형 무인기 제어 링크는 무선링크 양쪽 끝단에 2계층 보안 전용 하드웨어를 설치하여 전달되는 프레임의 기밀성, 무결성, 최신성, 책임성 등을 제공한다. 한편 네트워크형 무인기 제어 링크는 무인기와 지상의 조종사 간에 무인기 제어 지상 네트워크와 공용 IP(Internet Protocol) 네트워크가 결합되어 있는 상황이다. 따라서, 무인기 제어 지상 네트워크에서 가입자들에게 제공하고 있는 상호인증, 기밀성, 무결성과 같은 보안서비스들과 IP기반의 네트워크에서 공통으로 제공할 수 있는 IPSec[3]의 기밀성, 무결성, 최신성, 제한된 트래픽 흐름 기밀성과 같은 보안 서비스들을 결합해서 제공함으로써 상호보완 효과를 기대할 수 있다.

Ⅲ. 무인기 제어용 통합 네트워크의 보안 적용 구간

무인기 제어용 통합 네트워크에서 보안 서비스가 적용되어야 하는 통신구간은 크게 네개로 분리된다. 먼저, 무인기와 지상통제소는 무인기 제어 지상 네트워크를 통하여 상호 연결되어 있으므로, 무인기와 지상통제소 종단 간의 보안이 요구된다. 특히, 무인기와 지상통제소 간에 전달되는 데이터는 무인기의 운행 제어 및 조종에 필수적인 데이터이므로 인증, 무결성, 기밀성이 보장되어야 한다. 현재 대부분의 무인기 제어용 통합 네트워크 구조는 라우터의 필요성, 2계층 스위치를 통한 네트워크 구성 및 관리의 어려움, IP 이동성 지원의 편리성을 고려하여 IP 통신 구조를 채용하고 있다[4]. IP 구조가 무인기 제어용 통합 네트워크에 적용된다면 다양한 보안 요구사항을 만족시키기 위해 IPSec이 바로 이용될 수 있다. 이 구간의 보안기술은 Ⅳ장 1절에서 살펴보기

로 한다. 두번째, 무인기는 무인기 제어 지상 네트워크



(그림 2) 무인기 제어용 통합 네트워크의 보안 적용 구간

를 통하여 자신의 데이터를 전송하게 되므로, 무인기 제어 지상 네트워크를 합법적으로 사용하기 위한 상호인증을 수행해야 하고 핸드오버 및 키 갱신 제어 메시지와 같은 제어 트래픽을 보호하여야 한다. 본고에서는 LTE를 무인기 제어 지상 네트워크로 고려하기에 Ⅳ장 2절에서 무인기와 LTE 간의 무선구간 보호기술을 별도로 기술한다. 세번째, 무인기 제어 지상 네트워크의 내부 구성요소들 간에도 상호인증, 무결성, 그리고 기밀성이 보장되어야 한다. 본고에서는 무인기 제어 지상 네트워크로서 LTE를 고려하기 때문에 LTE 내부 구성요소간 보안기술은 Ⅳ장 3절에서 다룬다. 마지막으로, 지상통제소와 무인기 제어 지상 네트워크간은 임의의 공용 네트워크를 통해 연결될 것이다 따라서, 무인기 제어 지상 네트워크의 게이트웨이 역할을 하는 노드와 지상통제소 사이의 트래픽을 보호하기 위한 보안 기술이 필요하게 된다. 따라서 Ⅳ장 4절에서는 이 구간의 보안 기술을 살펴본다. (그림 2)는 무인기 제어용 통합 네트워크의 보안적용 구간을 보여준다.

Ⅳ. 무인기 제어용 통합 네트워크의 보안 기술

1. 무인기와 지상통제소간 보안 기술

일반적으로 IP 통신 구조를 채용하는 네트워크에서 네트워크 계층 보안 서비스를 제공하기 위해서는 IPSec 기술이 사용된다. 무인기 제어용 통합 네트워크에서 무인기와 지상통제소 간에 IP 통신구조가 이용되면 IPSec이 사용 가능하다. 현재 국외의 무인기 개발 프로젝트에서 무인기와 지상통제소 간에 IPSec을 이용하는 예로는 스페인의 SIVA/MILANO[4], 독일의 SANDRA[5], NASA의 CNPC(Control and Non-Payload Communications) 실험실 모델[6] 및 CNPC 비행 모델[7] 등이 있다. 먼저, 모든 기존의 프로젝트에서는 IPSec을 상호인증 방법으로 선택하였다. NASA의 CNPC 비행모델은 패킷의 오버헤드를 줄여 성능을 높이는 IPSec 전송모드를 선택하였고, 다른 프로젝트들은 터널모드를 통해 전송자와 수신자를 숨기는 제한된 트래픽 흐름의 기밀성을 제공하였다. SANDRA 프로젝트를 제외한 모든 프로젝트들은 전송되는 데이터의 기밀성을 보장하기 위해 ESP

〈표 1〉 무인기 프로젝트별 무인기와 지상통제소간 보안 기술

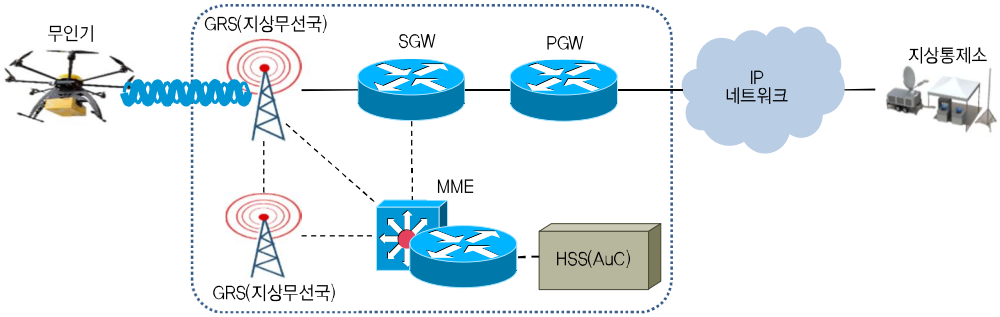
보안기술	SIVA/MILANO[4]	SANDRA[5]	CNPC 실험실 모델[6]	CNPC 비행모델[7]
인증방안	IPSec 인증	IPSec 인증	IPSec 인증	IPSec 인증
모드	터널모드	터널모드	터널모드	전송모드
보안헤더	ESP헤더	알려지지 않음	ESP헤더	ESP헤더
보안 서비스	인증, 기밀성, 무결성, 소스인증, 최신성	인증, 무결성, 소스인증, 최신성	인증, 무결성, 소스인증, 부인방지, 최신성	인증, 기밀성, 무결성, 소스인증, 최신성
보호 데이터 종류	TC, TM, 영상	TC, TM, 영상	ICMP 테스트 트래픽, UDP 테스트 트래픽	UDP 테스트 트래픽
암복호 알고리즘 및 모드	알려지지 않음	알려지지 않음	없음	AES*, GCM* 모드
무결성 알고리즘	알려지지 않음	알려지지 않음	HMAC-SHA 256	CMAC 64
키갱신 방법	비행전 새로운 키 장입	알려지지 않음	테스트전 새로운 키 설정	IKEv2 이용한 키교환
키갱신 주기	없음	알려지지 않음	없음	14분
오버헤드 감소 방안	없음	알려지지 않음	ROHC(RObust Header Compression)	ROHC(RObust Header Compression)

* AES(Advanced Encryption Standard) * GCM(Galois Counter Mode)

(Encapsulating Security Payload) 헤더를 사용하였으나, CNPC 실험실 모델은 구현시 암복호화를 수행하지 않아서 실제로는 기밀성이 제공되지 않는 문제점을 가진다. SIVA/MILANO와 SANDRA 프로젝트는 Tele-command와 Telemetry 정보, 그리고 영상을 IPSec을 이용하여 보호하였으나 CNPC 모델들은 UDP 테스트 트래픽을 이용하여 테스트를 진행하였다. 암복호 및 무결성 알고리즘의 경우에는 CNPC 모델들만 각각의 알고리즘 및 모드를 공개하였다. 키의 경우에는 CNPC 비행 모델만이 IKEv2를 이용한 동적인 키갱신을 실제 비행 중에 14분마다 한번씩 수행하였다. 그 외에 SIVA/MILANO나 CNPC 실험실 모델은 키 갱신 없이 비행 전에 새로운 키를 설정하는 정적인 방법을 채택하였다. 특이한 점은 CNPC 비행 모델은 IPSec 오버헤드를 감소시키기 위해서 ROHC (RObust Header Compression)를 이용한다는 것이다. 〈표 1〉은 각 프로젝트별로 무인기와 지상통제소간에 적용된 보안 기술을 보여준다.

2. 무선 구간 보안 기술

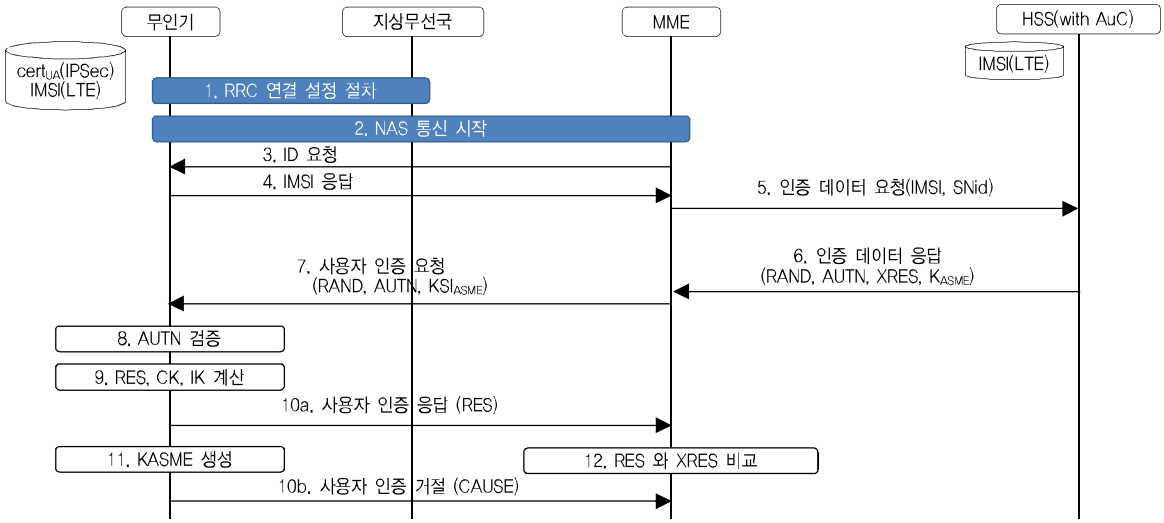
무인기 제어용 통합 네트워크에서 무선 구간은 실제로는 무인기 제어 지상 네트워크에 포함되는 통신구간이기 때문에 지상 네트워크의 보안기술에 크게 의존하게 된다. 본고에서는 무인기 제어 지상 네트워크로서 LTE 기술을 고려하기에 먼저 어떠한 LTE 구성요소들이 무인기 제어를 위해 필요한지 밝힌다. 먼저, 다른 IP 기반의 네트워크에서 지상무선국(GRS)을 통해 무인기로 IP 트래픽을 전달하기 위해서는 SGW(Serving Gateway)와 PGW(Packet Gateway)가 필요하다. 다음



(그림 3) LTE 기반의 무인기 제어 지상 네트워크 구성

으로 무인기의 식별자(ID)를 저장하고 무인기와 LTE 네트워크 간의 상호인증이 요구될 때 인증에 필요한 정보를 제공하기 위한 HSS/AuC(Home Subscriber Server/Authentication Center)가 필요하다. 마지막으로 무인기의 이동에 따른 핸드오버 처리 및 무인기와 지상무선국 사이에 설정된 통신키를 갱신하기 위해 MME(Mobility Management Entities)가 필요하다. (그림 3)은 LTE 기반의 무인기 제어 지상 네트워크의 구성을 보여준다.

가□무선 구간의 상호인증 및 키설정 기술



(그림 4) LTE 기반 무인기 제어 지상 네트워크의 상호인증 및 키설정

무인기가 LTE 네트워크를 통하여 지상통제소와 통신하기 위해서는 먼저 LTE 네트워크와 상호인증 및 키 설정(AKA: Authentication and Key Agreement)을 통해 무인기와 LTE간의 안전한 링크 설정을 수행해야 한다. 또한, 지상통제소는 무인기 조종에 앞서 먼저 LTE의 PGW와 IPSec과 같은 보안기술을 이용하여 상호인증 및 키 설정 절차를 수행해야 한다. (그림 4)는 무인기와 LTE 네트워크 간의 상호인증 및 키 설정 절차를 보여준다. 먼저, 무인기와 MME가 지상무선국을 통하여 상호 연결되기 때문에 무인기와 지상무선국간 연결설정(절차 1) 및 무인기와 MME간의 연결설정(절차 2)을 수행한다, 이후에 MME는 무인기에 인증에 필요한 ID를 요청하고(절차 3), 무인기는 응답으로 IMSI(International Mobile Subscriber Identity)를 MME에 제공한다(절차 4). 이후에 MME는 수신한 IMSI와 인증에 필요한 자신의 ID (Serving Network ID)를 HSS에 제공한다(절차 5). HSS는 이들을 이용하여 인증에 필요한 정보인 RAND, AUTN, XRES와 MME와 무인기간 통신키인 K_{ASME}를 생성하여 MME에 반환한다(절차 6). MME는 HSS의 응답을 검증하고 성공하면, 무인기가 LTE 네트워크를 인증하는 데 필요한 정보인 RAND, AUTN, 키식별자 (KSI_{ASME})를 무인기에게 전송한다(절차 7). 무인기는 HSS와 같은 방법으로 AUTN을 계산하고(절차 8) 일치하면 무인기와의 통신에 사용될 키들인 Cipher Key(CK), Integrity Key(IK). 그리고 RES를 생성한다(절차 9). 무인기는 AUTN이 일치하면 생성된 RES를 MME에게 전송하고 (절차 10a) 그렇지 않으면 사용자 인증 거절 메시지를 보내면서 이유(CAUSE)를 첨부해서 보낸다(절차 10b). 무인기는 AUTN이 일치하면 미리 생성한 CK와 IK를 연접하여 MME와의 통신키인 K_{ASME}를 생성한다(절차 11). MME는 수신된 RES와 자신이 HSS로부터 수신한 XRES를 비교하여 동일하면 수신한 K_{ASME}를 무인기와의 통신키로 설정한다(절차 12). 이후에 MME는 설정된 K_{ASME}를 암복호화키(K_{NASenc})와 무결성키(K_{NASint})로 나누어 사용한다. 또한, MME는 K_{ASME}를 지상무선국(GRS)에 전송하여 지상무선국이 무인기와의 통신에 사용할 사용자 데이터 암호화 키(K_{Uenc}), 제어 데이터 암호화 키(K_{RRCenc}), 제어 데이터 무결성 키(K_{RRCint})를 생성하도록 한다.

나□무선 구간의 지상무선국간 이동성 지원 보안 기술

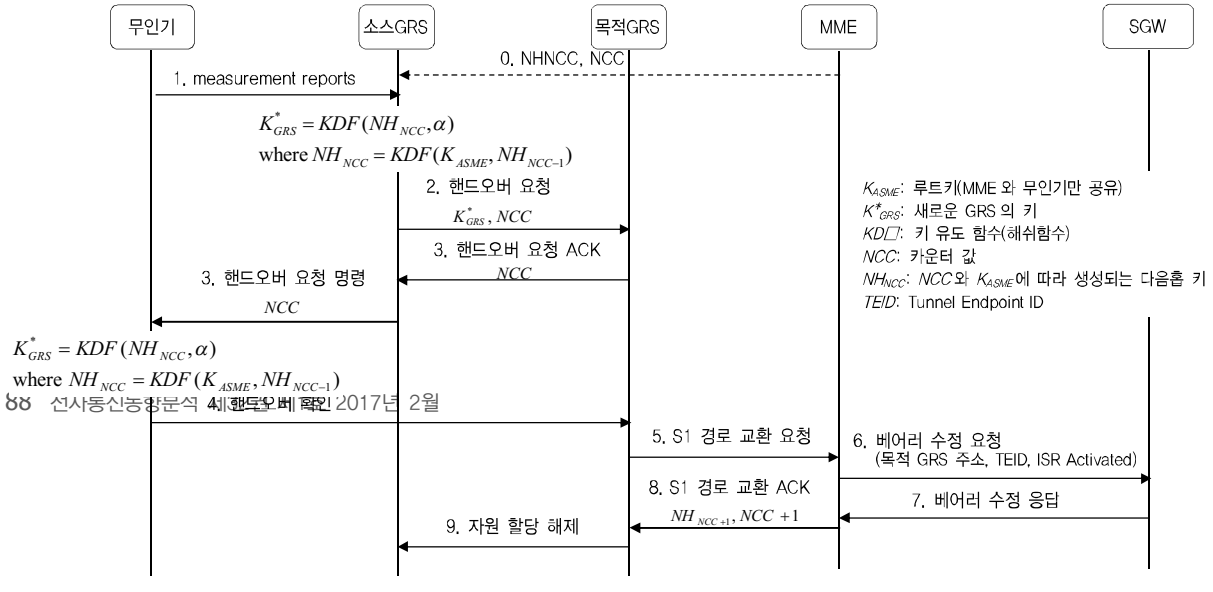
일반적인 LTE 네트워크는 서비스하는 단말의 이동성을 지원하기 위한 이동단말의 핸드오버 지원 및 이에 따른 키 갱신 절차를 명시하고 있다. 즉, 단말이 지상무선국 간을 이동하는 경우, 단말이 MME간을 이동하는 경우, 단말이 다른 네트워크에서 LTE로 이동하거나 반대의 경우를 각각 기술하고 있으나 무인기 지원 LTE의 경우에는 그 특성상 다른 경우는 발생하지 않고 오로지 지상무선국간을 이동하는 경우와 MME간을 이동하는 경우만 발생한다. 먼저, 무인기가 지상무선국간을 이동하는 경우에 핸드오버가 발생하면 기존 지상무선국과 목적 지상무선국만 핸드오버 키 갱신 절차에 참여하는 X2 핸드오버와 MME가 참여하는 S1 핸드오버로 나뉜다. 이때 X2는 LTE 네트워크 구조에서 지상무선국 간에 연결되는 인터페이스를 의미하고 S1은 MME와 지상무선국간의 인터페이스를 의미한다.

(그림 5)는 LTE 기반의 무인기 제어 지상 네트워크에서 X2 핸드오버 절차를 보여준다. 핸드오버는 무인기가 자신에게 서비스를 제공하고 있던 소스 GRS로부터 수신된 신호세기를 해당 GRS에게 전송하면서 핸드오버 절차가 시작된다[8](절차 1). 소스 GRS는 다음의 식 (1)을 사용하여 목적 GRS와 무인기간에 사용될 키 K^{*}_{GRS}를 생성한다.

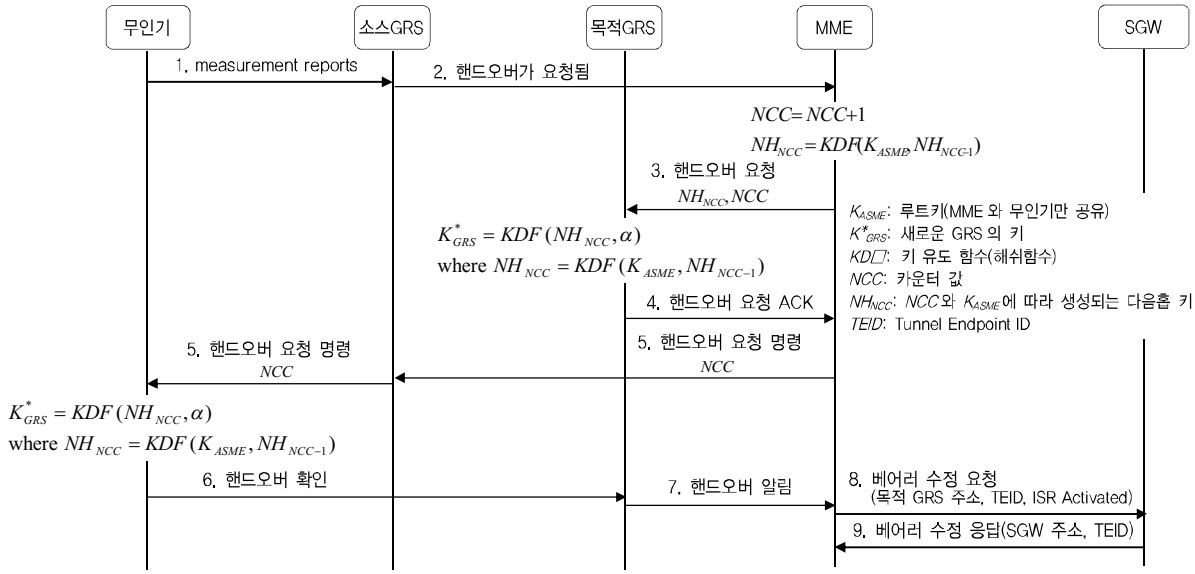
$$K^{*}_{GRS} = KDF(NH_{NCC}, \alpha) \quad (1)$$
$$\text{where } NH_{NCC} = KDF(K_{ASME}, NH_{NCC-1})$$

여기서 NCC(Next hop Chaining Counter)는 MME와 무인기간에 공유하는 카운터 값이며, NH_{NCC}(Next Hop key)는 NCC값에 대응하는 다음 홉을 위한 키이다. KDF(Key Derivation Function)는 키를 가진 해쉬함수이며 α 값은 목적 셀의 물리적 셀 식별자와 주파수등을 연접한 값이다. 즉, 목적 GRS와 무인기간의 키는 현재의 NH_{NCC}값을 키로 하여 α 값을 해쉬함수에 통과한 결과값이 되며, 현재의 NH_{NCC}값은 K_{ASME}를 키로 하여 이전 키(NH_{NCC-1})를 해쉬한 값이다. 최초의 NH_0는 K_{GRS}와 동일하다. 소스 GRS는 생성한 K^{*}_{GRS}와 NCC를 목적 GRS로 전송하고(절차 2), 목적 GRS는 수신한 K^{*}_{GRS}를 저장하고 해당 NCC를 무인기에게 전송한다(절차 3). 무인기는 같은 방법으로 K^{*}_{GRS}를 생성하고 핸드오버 확인 메시지를 목적 GRS에게 전송한다(절차 4). 이후 목적 GRS는 MME와 SGW를 통해 S1 경로 교환 및 베어러 수정(절차 5-8)을 수행한다. 마지막으로 목적 GRS는 소스 GRS에게 할당 자원을 해제하도록 요청한다(절차 9). X2 핸드오버에서는 통신에 사용되는 키 K^{*}_{GRS}가 소스 GRS에서 생성되어 목적 GRS로 전달되기 때문에, 만일 소스 GRS가 오염되면 전달되는 키도 바로 노출되는 문제점을 지닌다.

무인기가 다른 지상무선국으로 이동할 때 양쪽의 지상무선국은 물론 MME도 같이 그 키 갱신 절차에 참여하는 S1 핸드오버를 수행할 수 있다. (그림 6)은 LTE 기반의 무인기 제어 지상 네트워크에서 S1 핸드 오버 절차를 보여준다. 먼저, 무인기는 수신된 신호세기를 소스 GRS에게 전송하고(절차 1), 소스 GRS는 핸드오버가 필



(그림 5) LTE 기반 무인기 제어 지상 네트워크의 X2 핸드오버 과정

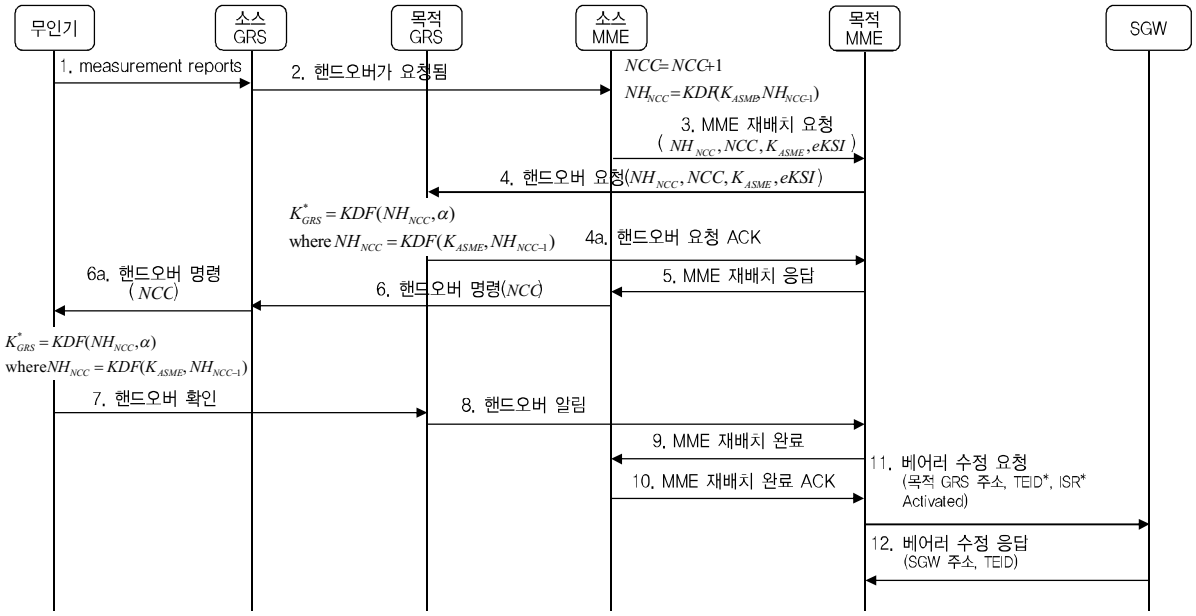


(그림 6) LTE 기반 무인기 제어 지상 네트워크의 S1 핸드오버 과정

요하다는 것을 MME에게 알린다(절차 2). MME는 새로운 NCC값과 NH_{NCC}를 계산하고 이들을 핸드오버 요청 메시지에 담아 목적 GRS에게 전송한다(절차 3). 목적 GRS는 식 (1)을 이용하여 목적 GRS와 무인기 사이에 사용될 키 K^*_{GRS}를 생성한다. 이후에 목적 GRS는 핸드오버 요청에 대한 ACK 응답을 MME에 전송하고(절차 4), MME는 소스 GRS에게 NCC값을 포함하는 핸드오버 명령을 전송하고 소스 GRS는 이를 무인기에게 전달한다(절차 5). 무인기는 식 (1)을 이용하여 목적 GRS와 동일한 키 K^*_{GRS}를 생성하고, 핸드오버 확인 메시지를 목적 GRS에게 전송한다(절차 6). 목적 GRS는 MME에게 핸드오버가 종료되었음을 알리고(절차 7), MME는 SGW와 베어러 수정과정을 수행한다(절차 8-9). 이 방법은 핸드오버가 발생할 때 마다 MME가 NCC값을 증가시켜서 목적 GRS에게 전송하고, 목적 GRS는 변경된 NCC값에 의해 새로운 키 K^*_{GRS}를 만들어내게 된다. 따라서, 소스 GRS가 오염되어도 목적 GRS의 새로운 키는 바로 노출되지 않으나, 소스 GRS로부터 얻어진 NCC값의 조작에 의해 쉽게 새로운 키를 생성해 낼 수 있다.

다□무선 구간의 MME 간의 이동성 지원 보안 기술

(그림 7)은 LTE 기반의 무인기 제어 지상 네트워크에서 MME 간의 핸드오버 절차를 보여준다. 먼저, 무인기는 수신된 신호세기를 소스 GRS에게 전송하고(절차 1), 소스 GRS는 핸드오버가 필요하다는 것을 MME에게 알린다(절차 2). 소스 MME는 새로운 NCC값과 NH_{NCC}를 계산하고 이들을 MME 재배치 요청 메시지에 담아 목적 MME에게 전송한다(절차 3). 목적 MME는 소스 MME로부터 수신한 값들을 이용하여 목적 GRS에게 핸드오버 요청 메시지를 전송한다(절차 4). 목적 GRS는 식 (1)을 이용하여 목적 GRS와 무인기 사이에 사용될 키 K^*_{GRS}를 생성한다. 이후에 목적 GRS는 핸드오버 요청에 대한 ACK 응답을 목적 MME에 전송한다(절차 4a). 목적 MME는 MME 재배치 응답을 소스 MME에게 전송하고(절차 5), 소스 MME는 핸드오버 명령 메시지에 NCC값을 담아서 소스 GRS를 통해(절차 6) 무인기에게 전달한다(절차 6a). 무인기는 식 (1)을 이용하여 목적 GRS와 동일한 키 K^*_{GRS}를 생성하고, 핸드오버 확인



(그림 7) LTE 기반 무인기 제어 지상 네트워크의 MME간 핸드오버 과정

* TEID(Tunnel Endpoint ID) * ISR(Idle state Signaling Reduction)

메시지를 목적 GRS에게 전송한다(절차 7). 목적 GRS는 목적 MME에게 핸드오버가 종료되었음을 알리고(절차 8), 목적 MME는 소스 MME와 더불어서 MME 재배치 절차를 완료한다 (절차 9-10). 마지막으로 목적 MME는 SGW와 베어러 수정 과정을 수행한다(절차 11-12).

3. 무인기 제어 지상 네트워크 구간의 보안 기술

무인기 제어용 통합 네트워크에서 무인기 제어 지상 네트워크는 추후에 무인기의 보급이 활발해지고 다양한 응용이 구현되어서 동시에 다수의 무인기를 조종 및 제어할 수 있도록 하는 데 필요한 기반 통신구조이다. 본고에서는 이러한 기반 통신구조로서 LTE를 선정하였으나, LTE 네트워크의 내부 구성요소 간 통신은 그 자체로 인증, 기밀성, 무결성, 부인봉쇄와 같은 보안서비스들을 제공하지 않는다. 그래서, LTE 표준 규격들에서는 네트워크의 구성요소간 안전한 통신을 위해서 IPSec과 같은 표준 보안프로토콜을 이용하도록 권고하고 있다. 즉, 무인기 제어 지상 네트워크에서 각 구성요소는 상호간에 IPSec을 통한 인증을 수행하고, 인증의 결과로 생성된 세션키를 이용하여 상호 간에 전송되는 데이터의 기밀성, 무결성, 소스인증, 부인봉쇄, 최신성 등을 제공할 필요가 있다. 또한 이러한 세션키는 공격자의 암호학적 해석을 통해 밝혀질 수도 있으므로 IKEv2를 이용한 주기적인 키 갱신을 수행함으로써 이러한 취약점을 보완할 수 있다.

4. 지상통제소와 무인기 제어 지상 네트워크 간의 보안 기술

무인기를 조종하고 제어하는 지상통제소는 공용 IP 네트워크를 통하여 무인기 제어 지상 네트워크의 PGW와 연결될 것으로 예상된다. 임의의 두 통신 노드를 공용 네트워크를 통하여 안전하게 연결하기 위해서는 가상 사설 네트워크(VPN: Virtual Private Network) 기술을 이용해야 한다. 가상 사설 네트워크는 통신 프로토콜 스택상의 여러 계층에서 구현될 수 있으나 본고에서는 네트워크 계층에서 IPSec 기술을 적용하는 것을 가정한

다. 다시 말해서, 지상통제소와 무인기 제어 지상 네트워크의 PGW는 IPSec의 상호인증 과정을 수행하여 상대방의 적법성을 확인한 후에, 상호인증의 결과로 생성된 키를 이용하여 지상통제소와 PGW간의 데이터에 대한 기밀성, 소스인증, 무결성, 최신성 등을 제공 한다. IPSec의 운영은 전송모드 혹은 터널모드로 운영될 수 있다. 터널모드는 기존헤더에 새로운 소스와 목적지가 기록된 헤더를 앞에 덧붙이기 때문에 트래픽의 원천지와 목적지를 숨길 수 있는 보안상 이점이 있다. 무인기 제어 통합 네트워크에서 지상통제소와 PGW는 무인기 조종 및 제어를 위한 가장 핵심적인 요소들이기에 노출이 되면 공격자들의 집중 공격대상이 된다. 따라서 이들은 IPSec의 터널모드를 통하여 보호될 필요가 있다. 터널모드는 기존의 헤더에 추가적으로 헤더를 하나 덧붙이게 되므로 오버헤드가 증가하는 문제점이 있으나, 지상통제소와 무인기 제어 지상 네트워크는 유선 네트워크로 연결되기에 이러한 오버헤드가 성능에 크게 영향을 미치지는 않는다.

V. 결론

본고에서는 무인기의 국가공역 진입 및 운행을 위한 무인기 제어용 통합 네트워크의 보안 적용 구간을 분류하고 각 구간별 보안 서비스들을 식별하였다. 이후에 각 구간별로 요구되는 보안 서비스들을 만족시키기 위해 가용한 기술들과 적용방법을 기술하였다.

향후에 무인기 제어용 통합 네트워크의 보안성을 더욱 향상시키기 위해서는 다음과 같은 문제점들이 해결되어야 한다. 먼저, 무인기와 무인기 제어용 지상 네트워크 간에 상호인증 및 키설정 절차를 수행할 때 내부의 공격자에 의한 공격의 위험이 존재하기에 보다 향상된 상호인증 및 키설정 절차가 고안되어야 한다. 또한, 핸드오버를 위한 키갱신의 경우에도 기존의 방법들은 오로지 전방향 보안성만 지원하기에 역방향 보안성도 지원할 수 있는 향상된 키 갱신 기법이 고안되어야 한다.

약어 정리

AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
CK	Cipher Key
CMAC	Cipher-based Message Authentication Code
CNPC	Control and Non-Payload Communications
ESP	Encapsulating Security Payload
GCM	Galois Counter Mode
GCS	Ground Control Station
GRS	Ground Relay Station
HMAC	keyed-Hash Message Authentication Code
HSS/AuC	Home Subscriber Server/Authentication Center
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IK	Integrity Key
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
IPSec	Internet Protocol Security
ISR	Idle state Signaling Reduction
KDF	Key Derivation Function
LTE	Long-Term Evolution
MME	Mobility Management Entities
NAS	Non Access Stratum
NASA	National Aeronautics and Space Administration
NCC	Next hop Chaining Counter
NH	Next Hop key
P2P	Point-to-Point
PGW	Packet Gateway
ROHC	Robust Header Compression
RRC	Radio Resource Control
SANDRA	Seamless Aeronautical Networking through integration of Data links, Radios and Antennas
SGW	Serving Gateway
SHA	Secure Hash Algorithm
TC	Tele-command
TEID	Tunnel Endpoint ID
TM	Telemetry

UDP User Datagram Protocol
VPN Virtual Private Network

참고문헌

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

[2] R.J. Kerczewski and J.H. Griner, "Control and Non-payload Communications Links for Integrated Unmanned Aircraft Operations," *Proc. Join Conference-18th Ka and Broadband*, Sept. 2012, Ottawa, Canada, pp. 24-27.

[3] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," IETF RFC 4301, Dec. 2005

[4] I. Vidal et al., "Design and Practical Deployment of a Network-Centric Remotely Piloted Aircraft System," *IEEE Communications Magazine*, vol. 52, no. 10, Oct. 2014, pp. 22-29.

[5] S. Plass et al., "Flight Trial Demonstration of Seamless Aeronautical Networking," *IEEE Communications Magazine*, vol. 52, no. 5, May 2014, pp. 119-129.

[6] 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.

[7] 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.

[8] S.N. Marwat et al., "Congestion-Aware Handover in LTE-Systems for Load Balancing in Transport Network," *ETRI Journal*, vol. 35, no. 5, Oct. 2014, pp. 761-771.