

chapter 2

무인기의 안전한 운영을 위한 보안 기술



왕기철 || 한국전자통신연구원 책임연구원

이병선 || 한국전자통신연구원 실장

김성창 || 한국전자통신연구원 실장

I. 서론

드론이라 불리는 무인기(Unmanned Aerial Vehicle)는 파일럿 없이 자율적으로 비행하거나 파일럿이 원격으로 조종하여 비행하면서 탑재된 임무장비를 통해 임무를 수행하는 비행체를 의미한다. 원래 무인기는 군에서 감시정찰, 관심지역의 조사 및 촬영, 정밀 타격 등의 용도로 사용되어 왔다. 최근에는 무인 배달, 3차원 공간지도 작성, 임무장비를 이용한 과학 조사 활동, 정밀 농업, 정밀 수산업, 재난 예측 및 대응 등과 같은 다양한 민간 응용들에 활용되고 있다.

무인기들을 일반공역에 진입시켜 다양한 응용에 활용하기 위해서는 다음과 같은 핵심기술들이 성숙되어야 한다. 먼저, 통신 및 보안기술로, 이는 무인기와 조종기 및 무인기 간에 데이터를 신뢰성 있게 교환하기 위한 기술이다. 탐지 및 인식 기술은 무인기가 가진 센서를 통해 무인기의 외부 환경을 인식하는 기술을 의미한다. 자율비행 기술은 무인기의 임무

* 본 내용은 왕기철 책임연구원(☎ 062-970-6531, gcwang@etri.re.kr)에게 문의하시기 바랍니다.

** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

*** 본 연구는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 5G 드론 시스템 및 원격운영시스템 개발사업의 연구결과임(NRF-2020M3C1C2A01080836).

를 수행하기 위한 비행경로 계획을 세워 비행하되 실시간으로 바뀌는 환경을 인식하여 비행경로를 동적으로 변경하는 기술이다. 무인기의 비행시간을 증대시킬 수 있는 무인기 동력원의 기술 개발 또한 매우 중요하다. 안티 드론 기술은 보호 구역에 난입하는 무인기를 실시간으로 인식하고 추적하여 파괴적 혹은 비파괴적으로 대응하는 기술이다. 비행 제어 기술은 숙련된 조종사의 조종 행위를 모사하는 고난이도 비행 모사와 외부 환경 변화에 강인하게 대응하는 적응형 제어 기술이다. 자율 착륙 기술은 무인기가 탑재된 센서에 기반하여 착륙 지점을 자율적으로 선정하고 자율무인차량, 자율무인선박 등에 안전하게 착륙하는 기술이다[1]. [표 1]은 위에서 언급한 핵심 기술들을 표로 정리한 것이다.

[표 1] 무인기의 활용을 위한 핵심 기술

분류	설명
통신 및 보안 기술	무인기와 조종기 및 무인기 간에 데이터를 안전하고 신뢰성 있게 교환
탐지 및 인식 기술	센서를 통해 무인기의 외부 환경을 인식
자율비행 기술	비행경로 계획을 세워 비행하되 실시간으로 바뀌는 환경을 인식하여 비행경로를 동적으로 변경
동력원 기술	무인기에 적합하면서 임무 수행 시간을 증대시킬 수 있는 동력원
안티 드론 기술	보호 구역에 난입하는 무인기를 실시간으로 인식하고 추적하여 파괴적 혹은 비파괴적으로 대응
비행제어 기술	숙련된 조종사의 조종 행위를 모사하는 고난이도 비행 모사와 외부 환경 변화에 강한 적응형 제어
자율착륙 기술	탑재된 센서에 기반하여 착륙 지점을 자율적으로 선정하고 자율무인차량, 자율무인선박 등에 안전하게 착륙

〈자료〉 한국전자통신연구원 자체 작성

본 고에서는 위에서 언급한 다양한 무인기 핵심 기술들 중에서 무인기 운영의 신뢰성과 안전성을 담보하는 보안 기술을 다룬다. 먼저 무인기 시스템의 구성 요소들을 살펴보고, 무인기 시스템의 구성 요소에 따른 보안 취약점을 소개한다. 다음으로 식별된 무인기의 보안 취약점을 이용한 공격 방법들을 자세히 설명한다. 마지막으로 앞에서 설명한 공격 방법들에 대한 알려진 대응 방안들을 제시한다.

II. 무인기 시스템 및 보안 취약점

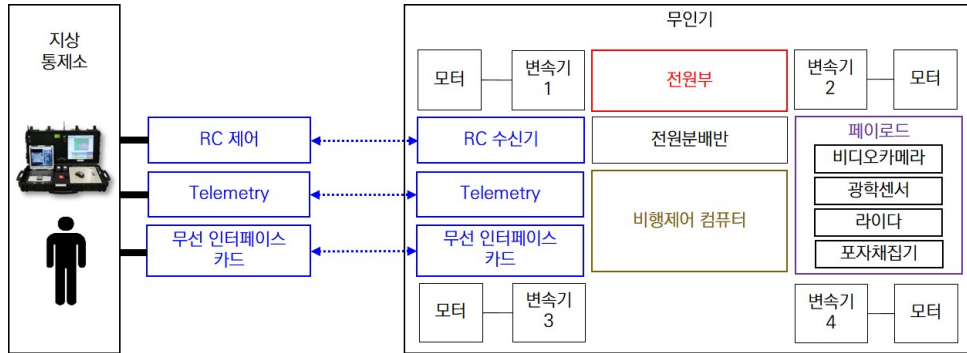
1. 무인기 시스템

일반적으로 무인기 시스템은 무인기 기체, 무인기를 제어하고 그 상태를 감시하는 지상 통제소, 그리고 무인기 기체와 지상통제소 간의 데이터 통신 링크로 구성된다[2].

무인기 기체는 무인기의 두뇌인 비행제어 컴퓨터(Flight Control Computer: FCC), 각 부품에 전원을 공급하는 전원부, 전원을 각 부품에 분배하는 분배반, 그리고 지상통제소와 통신을 수행하는 통신부, 무인기를 비행하게 하는 구동부, 무인기의 임무 수행을 위한 페이로드(payload)로 구성된다. 비행제어 컴퓨터는 무인기의 자세를 측정하는 자세 및 방위기준시스템(Attitude and Heading Reference System: AHRS), 위치를 측정하는 GNSS(Global Navigation Satellite System) 수신기, 고도를 측정하는 고도계(Barometer/Altimeter) 센서 등으로 구성된다. 비행제어 컴퓨터는 지상통제소로부터 전달받은 조종 명령어 혹은 자동비행경로를 위치 및 자세 추정값과 비교하고, 그 차이를 모터의 회전속도로 바꿔서 구동부에 전달한다. 구동부는 비행제어 컴퓨터로부터 받은 신호에 따라 모터를 회전시키는 작업을 수행하며, 이를 위해 모터, 프로펠러, 변속기(Electronic Speed Controller: ESC)를 가진다. 통신부는 지상통제소의 조종기로부터 조종 명령어를 수신하는 RC(Remote Control) 수신기, 무인기의 위치, 자세, 속도, 전원 잔량 정보를 지상으로 송신하는 텔레메트리(telemetry) 송신기, 직접 혹은 네트워크형 통신을 수행하기 위한 인터페이스 카드 등으로 구성된다. 페이로드는 다양한 영상 센서들, 라이다(lidar), 합성개구 레이더(Synthetic Aperture Radar: SAR), 포자채집기, 가스분석기, 농약살포기 그리고 이들의 흔들림을 방지하기 위한 짐벌장치 등으로 구성된다.

지상통제소는 무인기를 원거리에서 조종하기 위한 원격 조종기, 무인기로부터 수신된 텔레메트리 정보를 수신하기 위한 텔레메트리 수신기, 무인기로부터 직접 혹은 네트워크형 통신을 통해 데이터를 수신하기 위한 인터페이스 카드와 데이터를 처리하고 시각적으로 표현하기 위한 정보처리 및 도식장치로 구성된다.

통신 링크는 무인기와 지상통제소 사이에서 데이터를 전달하기 위한 통로로서 조종 신호를 전달하기 위한 통신은 2.4GHz와 같은 ISM(Industrial Scientific and Medical)



(자료) 한국전자통신연구원 자체 작성

[그림 1] 무인기 시스템의 구성

대역을 주로 사용한다. 무인기의 위치, 자세, 속도, 전원 잔량 정보를 수신하기 위한 텔레메트리 통신은 433MHz나 900MHz 대역을 사용하며, 직접 통신 혹은 네트워크형 통신은 WiFi, LTE, 5G 등의 기술이 사용된다. [그림 1]은 무인기 시스템의 구성요소를 도식화한다.

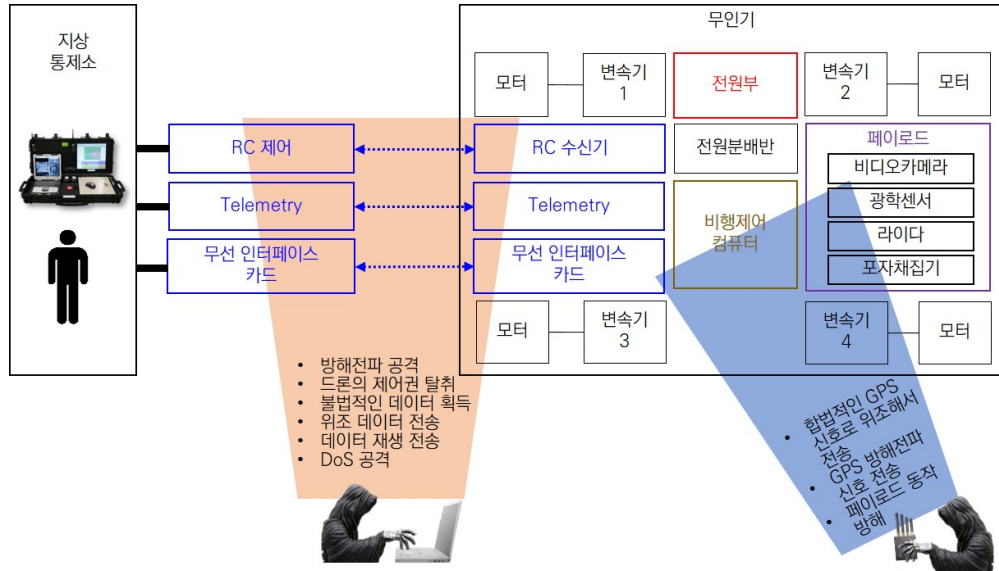
2. 무인기 시스템의 보안 취약점

무인기 시스템이 처한 보안 위협은 무인기와 지상통제소 간의 통신에 가해지는 보안 위협, 무인기의 비행제어 컴퓨터 내에 있는 센서들에 가해지는 보안 위협, 그리고 무인기의 페이로드에 가해지는 보안 위협으로 나눌 수 있다.

첫 번째, 무인기와 지상통제소 간의 통신은 공격자의 방해 전파에 의해 아예 신호 전송이 어려워지거나 신호 전송이 가능하더라도 제어권 분실, 도청, 전송 데이터 위조, 데이터 전송 부인, DoS(Denial of Service) 공격과 같은 보안 위협이 존재한다.

두 번째, 무인기의 비행제어 컴퓨터 내에 존재하는 자이로스코프, 가속도계, 전자 나침반, 고도계 등은 무인기의 3축 각속도 및 가속도, 진북 정보, 자세 정보, 고도 정보 그리고 이들을 보조하기 위한 정보를 제공하는데, 이 정보들이 오염되는 경우에는 무인기의 구동에 오동작이 발생하여 정상적인 비행이 어렵다.

세 번째, GNSS 수신기는 인공위성으로부터 발사된 전파를 수신하여 무인기의 위치를 결정하는데, 이 수신기의 동작을 방해하는 간섭 신호 혹은 위조 신호를 전송하여 무인기에



〈자료〉 한국전자통신연구원 자체 작성

[그림 2] 무인기 시스템의 보안 위협

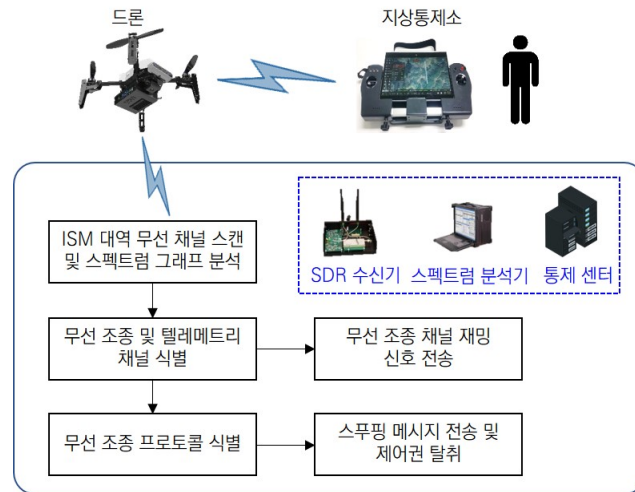
게 할당된 비행경로를 이탈할 수 있는 보안 위협이 존재한다.

네 번째, 무인기는 자신의 임무를 수행하기 위해서 비디오카메라, 광학 센서, 라이다, 포자채집기, 농약살포기 등의 장비들을 싣고 비행하는데, 이 장비들이 오작동 혹은 파손되는 경우에는 임무 수행이 불가능하게 된다. [그림 2]는 무인기 시스템의 보안 위협을 보여 준다.

III. 무인기 시스템에 대한 공격 및 대응 방안

1. 무인기 시스템에 대한 공격

무인기와 지상통제소 간의 통신은 무인기와 지상통제소가 일대일로 직접 통신하는 방법과 5G와 같은 지상의 이동 통신망을 이용하여 일대다로 통신하는 방법으로 나뉜다. 일대일로 직접 통신하는 방법에서 공격자는 무인기 조종 신호에 강한 간섭을 발생시켜 출발지로의 복귀를 유도하거나 위조된 무인기 조종 신호를 전송하여 자신이 원하는 곳으로 무인

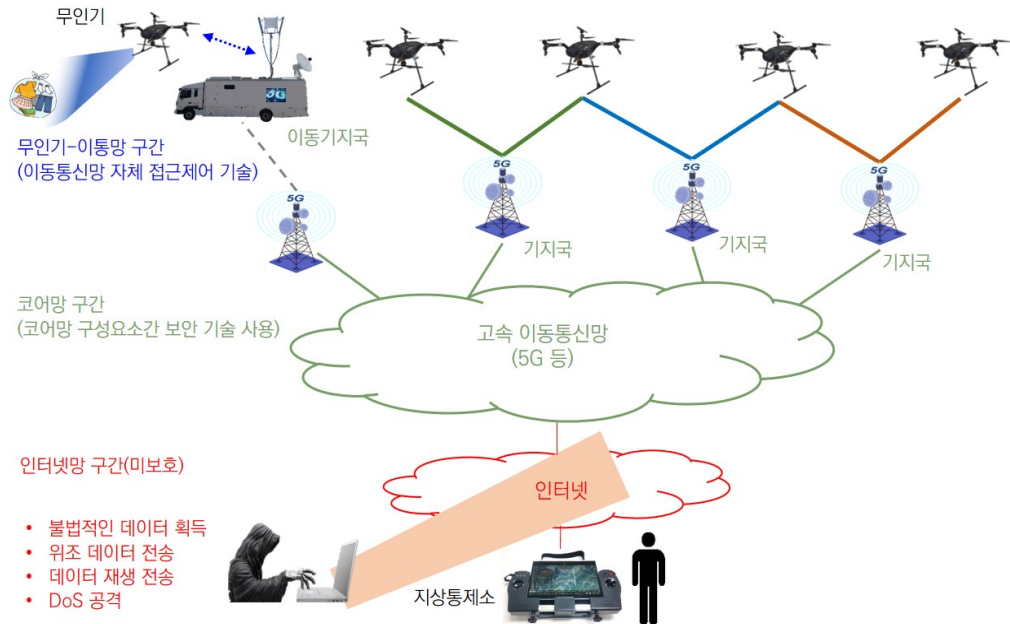


〈자료〉 한국전자통신연구원 자체 작성

[그림 3] 무인기-지상통제소 간 직접 통신에서의 공격

기를 이동시킬 수도 있다. 대부분의 무인기 조종 신호는 433MHz, 2.4GHz, 5GHz와 같은 ISM 대역에서 동작하고, 이 대역에서 동작하는 무인기 조종 프로토콜들은 잘 알려져 있기 때문에, 공격자들이 이러한 공격들을 쉽게 감행할 수 있다[3]. 즉, 공격자는 ISM 대역에서 방송되는 신호를 스캔하여 스펙트럼 그래프를 분석하고 무인기의 조종 채널과 텔레메트리 채널을 식별한다. 이후에 공격자는 식별된 채널에 강한 재밍(jamming) 신호를 전송하고, 무인기는 더 이상 지상통제소와 통신이 불가하므로 출발지로 복귀하게 된다. 또한, 공격자가 무인기의 조종 채널을 분석하여 어떤 조종 프로토콜이 사용되는지 파악하면, 프로토콜의 조종 메시지를 위조하여 무인기의 조종 제어권을 불법으로 획득할 수 있다[3]. [그림 3]은 무인기와 지상통제소 간의 직접 통신을 사용하는 경우의 통신 링크 공격을 보여준다.

지상통제소가 여러 무인기를 동시에 운용하는 경우에는 5G와 같은 고속의 지상 이동통신 네트워크를 사용하는데, 이 통신 방법은 무인기와 지상통제소 사이에 [그림 4]와 같이 세 개의 통신 구간으로 구성된다. 첫째, 무인기-이동통신망 구간은 이동통신망 사업자가 단말의 이동통신망 접근을 제어하는 자체 프로토콜에 의해 보호가 된다. 다음으로, 이동통신망의 코어망 구간은 코어망의 구성 요소들 간에 IPSec(IP Security)과 같은 종단 보안 프로토콜을 적용하여 보호가 가능하다[4]. 마지막으로, 네트워크형 통신의 경우에 지상통제소는 인터넷과 같은 공용망을 통해 이동통신망에 연결되고, 결국은 무인기와 연결되는

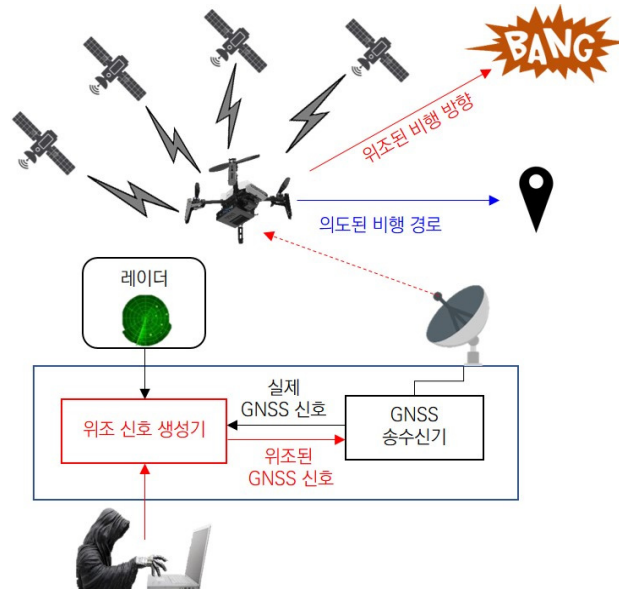


〈자료〉 한국전자통신연구원 자체 작성

[그림 4] 네트워크형 통신 방식에서의 공격

구조를 가진다. 공용망에서 무인기와 지상통제소 간에 통신 보호장치가 없으면, 공격자는 무인기와 지상통제소 간의 통신 내용을 불법으로 도청하여 위조된 데이터의 전송, 세션 탈취, 서비스 거부 공격 등을 수행할 수 있다.

공격자에게 있어서 무인기 자체도 좋은 공격 대상이 되는데, 특히 비행제어 컴퓨터와 모터 변속기(ESC) 등이 주요한 공격 목표가 된다. 비행제어 컴퓨터의 자이로스코프는 무인기의 3축 각속도를 측정하는데, MEMS(Micro-Electro-Mechanical Systems) 기반의 취약한 각속도계는 소음에 의해 오동작하며 정상적인 비행이 불가능한 문제를 발생시킨다[5]. 또한, GNSS 수신기는 4개의 위성으로부터 수신된 신호의 거리 측정을 통해 수신기(무인기)의 위치를 측정하는데, 공격자는 같은 주파수 대역의 강력한 재밍 신호를 전송하여 무인기의 GNSS 신호 수신을 막을 수 있다. [그림 5]에서처럼, 공격자는 위조된 GNSS 신호를 발생시켜 무인기가 잘못된 방향으로 비행하게 할 수 있다[6],[7]. 임의의 악의적인 공격자는 EMP(Electromagnetic Pulse) 신호 혹은 마이크로파를 비행 중인 무인기에 발사하여 무인기의 비행제어 컴퓨터의 전자회로를 교란시킬 수 있다. 이 경우에 무인기는



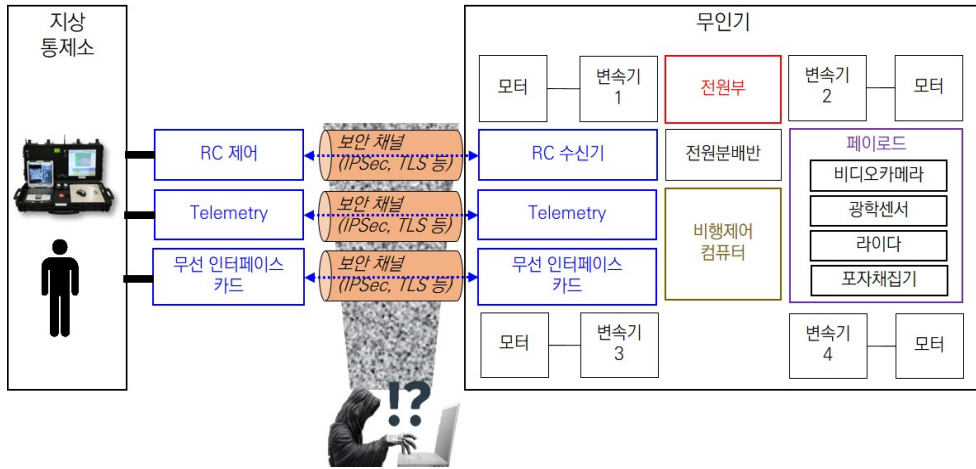
〈자료〉 한국전자통신연구원 자체 작성

[그림 5] 무인기의 GNSS 스푸핑 공격

정상비행을 수행할 수 없으며, 심지어 일부 전자회로가 파괴되어 추락할 수 있다.

2. 무인기에 대한 공격 대응

본 절에서는 3.1절에서 제시한 무인기를 목표로 하는 공격들에 대한 알려진 대응 방안들을 설명한다. 먼저, 무인기의 통신 링크에 대한 공격들에 방어하기 위해서는 무인기와 지상통제소 간에 IPsec이나 TLS(Transport Layer Security)와 같은 종단 보안 채널을 생성해야 한다. 보안 채널의 형성을 위해서는 통신 모뎀 앞단에 데이터 암호화 하드웨어를 배치해서 채널 암호화를 수행하는 방법이 있는데, 이 방법은 주로 군용 무인기 시스템에서 주로 사용한다. 다른 방법은 무인기와 지상통제소 사이에 보안 터널을 생성하여 무인기와 지상통제소 간에 교환되는 데이터를 보호하는 방법이다[4]. 이 방법은 무인기가 지상통제소와 지상 이동통신망 및 공용망을 통해 연결될 때 주로 사용하는 방법이다[4]. 무인기와 지상통제소 간에 보안 터널을 생성하는 일반적인 절차는 다음과 같다. 먼저, 무인기와 지상통제소 간에 상호 인증을 수행하고, 상호 인증이 종료되면 암호 통신을 수행하기

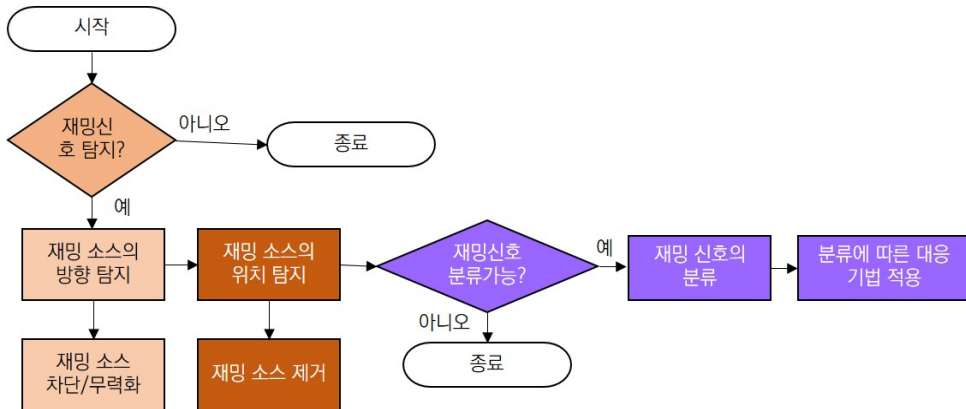


〈자료〉 한국전자통신연구원 자체 작성

[그림 6] 무인기 시스템의 통신 링크 보안

위한 통신키를 설정한다. 이후에 무인기와 지상통제소는 설정된 통신키와 암호화 알고리즘을 이용하여 상호간 통신의 기밀성, 무결성, 최신성, 부인봉쇄를 보장한다. 무인기와 지상통제소는 상호간 통신의 보안성 강화를 위해서 주기적으로 새로운 키를 수립하여 공유한다. [그림 6]은 무인기 시스템의 통신 링크 보안 방안을 보여준다.

무인기의 GNSS 수신기에 대한 공격 대응은 GNSS 재밍 신호에 대한 대응 방안과 스푸

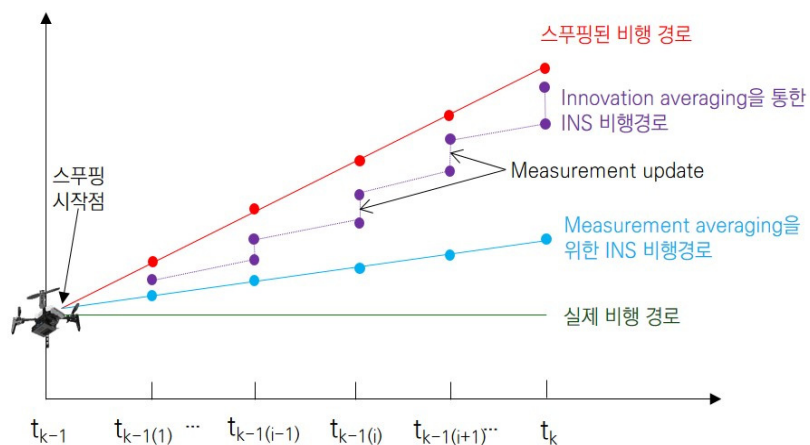


〈자료〉 R. M. Ferre, P. Richter, E. Falletti, A. D. Fuente, "A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft," IEEE Communications Surveys and Tutorials, Vol.22, No.1, First quarter 2020, pp.249-291.

[그림 7] GNSS 재밍 공격에 대한 대응

핑(spoofing)된 GNSS 신호에 대한 대응 방안으로 구분된다. GNSS 재밍 공격을 탐지하기 위해서는 재밍 반송파 주파수 및 대역 파라미터들을 이용하여 재밍 신호들을 수학적으로 모델링하고, 이 모델들과 거의 일치하는 신호가 수신되면 GNSS 재밍을 당하고 있음을 인지한다. 이 경우에, 재밍 신호의 방향을 탐지할 수 있고 방해 전파를 송출할 수 있는 장비가 있다면, 해당 방향으로 방해 전파를 전송하여 재밍 신호의 무력화를 시도한다. 만일, GNSS 재밍 신호의 방향을 식별할 수 없다면, 재밍 신호의 분류가 가능한지를 점검한다. GNSS 재밍 신호의 분류가 가능하면, GNSS 수신기의 구성 요소들(전단부, 선행연관부, 후행연관부, 항법부)에 대한 공격 위치에 따른 경감대책을 수립하여 적용한다[8]. [그림 8]은 GNSS 재밍 공격에 대한 대응 방안을 보여준다.

무인기에서 GNSS 스푸핑 탐지 방법은 클록 동기화 신호 기반의 방법과 칼만 필터(Kalman Filter) 기반의 방법으로 나뉜다. 무인기가 정상적인 클록 동기화 신호를 받을 때 가지는 클록의 편이(bias)와 표류(drift)를 모델링하여 시그니처로 저장한 후에, 실제 무인기의 비행에서 이와 유사한 시그니처를 가지는 동기화 신호만 받아들이는 방법이다. 무인기의 이동방향, 이동경로, 이동속도를 유지하는 관성측정장치(Inertial Measurement Unit)는 그 측정값을 관성항법시스템(Inertial Navigation System)에 되먹임시켜 무인기가 할당된 경로를 유지하게 한다. 칼만 필터는 측정값들을 시간을 두고 지속적으로 관찰



(자료) Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, "Analysis of Kalman Filter Innovation-Based GNSS Spoofing Detection Method for INS/GNSS Integrated Navigation System," IEEE Sensors Journal, Vol.19, No.13, Jul. 2019, pp.5167-5178.

[그림 8] Innovation averaging을 이용한 GNSS 스푸핑(spoofing) 탐지

하여 알려지지 않은 값들을 추정하게 되는데, 위치와 속도 오류, 자이로스코프의 편이, 무작위 소음 오류, 가속도계 변이 오류 등을 계산한다. 이러한 칼만 필터에 의한 오류값들을 충분히 긴 시간 동안 보정하였을때, GNSS 스푸핑에 의한 측정값에 근사하게 되어 스푸핑을 탐지할 수 있게 된다. 이 방법을 innovation averaging[9]이라 칭하는데, [그림 8]은 innovation averaging 기반의 GNSS 스푸핑 탐지 방법을 보여 준다. 무인기가 GNSS 스푸핑 공격을 받는 경우에, 여러 개의 GNSS 수신기를 이용하여 의심스런 신호를 배제할 수 있다. 또한, 라이다(lidar)와 같은 센서들을 이용하여 원래의 비행경로로 복귀를 시도할 수 있다. GNSS 스푸핑을 원천적으로 차단하기 위해서는 위성이 GNSS 신호를 보낼 때 개인키로 서명해서 보내고, 무인기는 위성의 공개키로 복호화가 되는 경우에만 GNSS 신호를 받아들이면 된다. 그러나, 이 방법은 군용 위성에서만 적용된다[6].

소음을 통해 무인기의 자이로스코프에 오동작을 유발시키는 공격에 대응하기 위해서는 다음과 같은 방법들을 사용할 수 있다[5]. 첫 번째, 자이로스코프 회로를 보호 차폐물 안에 넣어서 소음으로부터 보호할 수 있다. 다음으로, 추가적인 자이로스코프를 배치하여 공명 주파수에만 반응하도록 함으로써 원래의 자이로스코프 공명 출력을 제거할 수 있다. 또한, 자이로스코프의 감지 전극에 콘텐서를 추가로 배치하여 공명 효과를 감소시킬 수 있다.

IV. 결론

본 고에서는 하늘을 나는 IoT 장치로서 활용 분야를 크게 넓히고 있는 무인기 시스템의 보안 취약점들과 이 취약점들을 이용하여 수행되고 있는 다양한 공격들을 소개하였다. 이어서 앞서 소개된 다양한 공격들에 대응하기 위한 알려진 방법들을 또한 설명하였다. 필요한 시간에 장소를 변경하면서 대량의 데이터를 수집할 수 있는 무인기의 활용을 실생활에 더욱 확장하기 위해서는 무인기 비행의 안전성, 신뢰성, 그리고 수집 데이터의 보안성을 더욱 향상시켜야 한다. 이러한 측면에서, 무인기 시스템의 잠재된 보안 취약점을 선제적으로 파악하고, 이러한 취약점에 기반한 공격들을 효과적으로 방어하기 위한 보안 기술들이 개발되어야 한다.

[참고문헌]

- [1] 왕기철, 이병선, 안재영, “무인기 자율비행 기술 동향,” 스마트 트렌드 디바이스 매거진, Vol.36, 2019. 10. 16, pp.18-23.
- [2] 김성훈, 김준현, 손호웅, 이강원, “무인비행장치 측량,” 시그마프레스, 2019. 1. 31, ISBN: 9791162261392, pp.33-53.
- [3] X. Yue, Y. Liu, J. Wang, H. Song, and H. Cao, “Software Defined Radio and Wireless Acoustic Networking for Amateur Drone Surveillance,” IEEE Communications Magazine, Vol.56, No.4, Apr. 2018, pp.90-97.
- [4] 왕기철, 이병선, 임광재, 안재영, “무인기 제어용 네트워크의 보안 기술 동향”, 한국전자통신연구원, 전자통신동향분석, 32권, 1호, 2017. 2, pp.82-92.
- [5] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, “Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors,” 24th USENIX Security Symposium, Washington, D.C., USA, Aug. 2015, pp.881-896.
- [6] K. Wesson and T. Humphreys, “Hacking Drones,” Scientific American Online, Nov. 2013, pp.55-59.
- [7] D. He, S. Chan, and M. Guizani, “Security in the Internet of Things Supported by Mobile Edge Computing,” IEEE Communications Magazine, Vol.56, No.8, Aug. 2018, pp.56-61.
- [8] R. M. Ferre, P. Richter, E. Falletti, A. D. Fuente, “A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft,” IEEE Communications Surveys and Tutorials, Vol.22, No.1, First quarter 2020, pp.249-291.
- [9] Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, “Analysis of Kalman Filter Innovation-Based GNSS Spoofing Detection Method for INS/GNSS Integrated Navigation System,” IEEE Sensors Journal, Vol.19, No.13, Jul. 2019, pp.5167-5178.