# 전장에서 드론을 활용한 보안 위협과 시나리오

박 근 석*, 천 상 필**, 김, 성 표***, 엄 정 호****

## 요 약

1910년대부터 드론은 군사용으로 주로 정찰, 공격 표적 등의 특수 목적으로 사용되다가 현재는 재난 방재, 탐사, 방송 촬영, 우범지역 감시 등 다양한 분야에서 유용하게 활용되고 있다. 드론의 활용이 군수분야부터 민간분야 이르기까지 폭넓게 사용됨에 따라 드론을 표적으로 한 전파교란, GPS 스푸핑, 하이재킹 등 해킹이 발생하기 시작했다. 최근에는 무선 네트워크 해킹에 드론을 사용한 사례가 발표된 바 있다. 특히, 군사 분야에서 드론에 인공지능 기술이 적용될 경우에는 드론에 의한 무인전투체계 해킹이 발생하게 될 것이다. 또한, 드론이 무선통신 중계소 역할을 하는 것처럼 해킹 프로그램을 탑재한 드론이 원거리에 위치하고 있는 해킹 실행 드론까지 해킹 프로그램을 중계하는 기능도 가능할 것이다. 아울러 GPS 교란 장치를 탑재하여 무인전투체계에 대한 신호 교란도 가능하게 될 것이다. 본 논문에서는 전장에서 드론을 이용한 보안 위협과 예상되는 해킹 시나리오를 제안함으로써 드론에 의한 보안 위협의 심각성을 인지시키고자 한다.

# Security Threats and Scenarios using Drones on the Battlefield

Keun-Seog Park*, Sang-pil Cheon**, Seong-Pyo Kim***, Jung-ho Eom****

## ABSTRACT

Since 1910s, the drones were mainly used for military purposes for reconnaissance and attack targets, but they are now being used in various fields such as disaster prevention, exploration, broadcasting, and surveillance of risk areas. As drones are widely used from military to civilian field, hacking into the drones such as radio disturbance, GPS spoofing, hijacking, etc. targeting drones has begun to occur. Recently, the use of drones in hacking into wireless network has been reported. If the artificial intelligence technology is applied to the drones in the military, hacking into unmanned combat system using drones will occur. In addition, a drone with a hacking program may be able to relay a hacking program to the hacking drone located far away, just as a drone serves as a wireless communication station. And the drones will be equipped with a portable GPS jamming device, which will enable signal disturbance to unmanned combat systems. In this paper, we propose security threats and the anticipated hacking scenarios using the drones on the battlespace to know the seriousness of the security threats by hacking drones and prepare for future cyberspace.

**Key words : Security Threats, Drone Hacking, Threat Scenarios, Hacking route by Drone**

접수일(2018년 9월 30일), 게재확정일(2018년 10월 25일)

★ 이 논문은 2018학년도 대전대학교 교내학술연구비 지원에 의해 연구되었음.

* 대전대학교 군사학과 시간강사(주저자)
** 대전대학교 군사학과 초빙교수
*** 국방과학연구소 개념연구센터 책임연구원
**** 대전대학교 군사학과&안전융합학부 교수(교신저자)

# 1. 서 론

과거 군사 분야에서는 고정익형 드론을 정찰이나 공격 표적기로 활용하였으나, 현재는 정찰 및 감시와 공격 임무를 수행하고 있다. 최근에는 멀티콥터형 드론이 민간과 군사 분야에서 활용과 역할이 증대되고 있다. 민수용으로는 위험지역과 교통위반 차량 감시, 농약 살포, 방송 촬영, 공중 드론 쇼 등의 분야에서, 군수용으로는 부대 위협 지역 정찰, 사고 조사, 제독, 전략무기체계 결함 조사 등의 분야에서 역할이 증대되고 있다. 드론의 활용분야와 역할이 증가됨에 따라 그에 따른 부작용도 나타나고 있다. 최근에는 미군의 컴퓨터가 해킹을 당하면서 전투용 드론에 대한 정보가 해커에게 유출되어 드론이 위험에 노출되기도 하였다. 또한, 보안에 취약한 레저용 드론이 해킹당하기도 하였다[1,8].

다양한 분야에서 활용되는 드론의 기능을 확장시키고 보다 정밀한 비행과 임무수행을 위하여 최첨단 정보통신기술이 적용될 것으로 전망된다. 예를 들면, 드론의 자율 비행을 위해서 비행 방해물을 인식할 수 있는 딥러닝 알고리즘, 위성항법시스템의 한계를 극복하고 자율 경로를 생성하여 비행을 가능하게 해주는 심층 신경망 알고리즘, 심화 검색, 학습을 통해 수집한 정보 중에 드론의 임무와 상관있는 정보만 필터링하는 빅데이터 기술 등이 있다[1,9].

아직까지는 드론을 표적으로 한 해킹이 큰 이슈가 되고 있지만, 앞으로는 드론을 이용한 해킹이 보다 심각한 문제로 대두될 것이다. 최첨단 정보통신 기술이 적용된다면, 드론에 해킹 프로그램을 탑재하여 해킹 수단으로 활용할 수 있다. 2011년 블랙햇 컨퍼런스에서는 드론을 이용하여 무선 네트워크 AP를 해킹하여 접속 정보를 수집하였으며, 얼마 전에는 드론의 통신 네트워크를 내부 네트워크를 위장하여 불법 접속한 사례도 있었다. 앞으로 드론의 역할이 증대되고 다양한 정보통신기술이 접목됨으로써 드론을 이용하여 드론 해킹이나 무선 네트워크를 해킹하는 방법과 기술이 더욱더 정교화될 것으로 예측된다[5,6].

본 논문에서는 드론을 이용한 보안 위협의 중요성을 인식시키기 위해서 전장에서 드론을 이용한 보안 위협을 설명하고 그에 따른 보안 위협 시나리오를 제시할 것이다. 논문 구성은 2장에서 군사용 드론 기술의 진화를 알아보고 3장에서 드론을 이용한 보안 위협을 설명하며, 4장에서 예상되는 보안 위협 시나리오를 제시하고 5장에서 결론을 맺는다.

# 2. 군사용 드론 기술의 진화

육군은 '18년 9월 정찰드론, 전자전드론, 무장드론 등으로 구성된 드론봇 전투단을 창설하였다. 드론봇 전투단은 4차 산업혁명기술을 기반으로 현재와 미래의 불특정 복합 위협과 비대칭 위협을 능동적으로 대응하는 것이 주 임무이다[12]. 드론 개발 초창기에는 대공 표적과 정찰 등 특수임무에 국한되었던 것이 인공지능, IOT, 빅데이터, 센서 기술 등과 접목되면서 다양한 임무에 활용 영역을 넓혀나가고 있다.

드론에 인공지능 기술이 적용됨에 따라 드론 스스로 주변 환경을 분석하여 장애물이나 기상변화를 회피하는 자율 비행 능력을 갖추게 되었다. 아울러 센서를 통해 수집한 데이터나 관측 자료 등 다양한 정보를 신속하게 상호 비교 분석하고 사용용도에 맞게 가공 및 필터링할 수 있는 빅데이터 기술도 적용되고 있다. 사물인터넷(IoT) 기술은 드론의 비행 공역에 위치한 다양한 IoT 장비와 서로 데이터를 교환함으로써 보다 효과적인 드론 비행을 관리할 수 있게 된다[3,4].

4차 산업혁명을 주도하는 최첨단 정보통신기술이 군사용 드론에 적용되어 다양한 군사용도로 활용이 가능하며, 임무 수행을 신속하고 정확하게 수행할 수 있게 된다. 빅데이터와 기계학습 기술을 통해서 수집한 비정형 데이터를 통합 분석 및 가공하여 표적과 관련된 데이터만 지상통제체계에 제공할 수 있는 정찰용 드론의 기능을 향상시킬 수 있다. 또한, 사물의 핵심적인 특징을 추출하여 할당된 표적의 이미지와 비교하여 공격 대상을 정

확하게 식별하고 센서를 통해 표적의 거리, 좌표, 특성 등을 계산하여 오차를 최소화하여 정밀 공격을 가능하게 할 수 있다. 피해평가 용도의 드론에는 표적에 대한 정밀 공격 이후에 촬영한 이미지와 타격 이전의 이미지를 비교 분석하고 기존의 피해양상 데이터를 학습하여 피폭된 표적의 피해 수준을 평가할 수 있도록 할 수 있다[5,7].

## 3. 드론의 보안 위협

드론의 다양한 임무 수행을 위해서는 탑재된 플랫폼에 운영체제와 기능에 따른 소프트웨어를 설치해야 한다. 아울러 지상통제소나 비행 공역 내에 있는 무인이동체계와의 데이터 전송 및 교환을 위해서 통신 및 네트워크 기술과 통신 주파수 등이 확보되어야 한다. 다양한 정보통신기술이 드론에 적용됨에 따라 취약점이 증가되고 위협이 심각지고 있다. 대표적인 드론 해킹방법은 GPS 스푸핑과 하이재킹이 있다. 이는 통신 프로토콜의 취약점을 이용하여 드론의 통제권을 빼앗는 것을 목적으로 한다[10-12].

그러나 보다 더 심각한 위협은 드론을 사이버 공격의 수단으로 이용한다는 것이다. 최근 사이버 보안 기술은 인공지능, 머신 러닝 등 최첨단 정보통신기술과 융합기술이 적용된 지능형 사이버공격 탐지 및 예측 기술, 능동형 자가 방어 기술, 사이버 변이 기술 등이 개발되고 있다[14]. 또한, 4차 산업혁명 이후에는 인간 지향적 보안 기술 개발도 예상되기 때문에 지금의 사이버공격 경로나 도구로는 사이버공격의 성공을 장담할 수 없다. 특히, 내부망을 사용하거나 폐쇄된 사이버 공간에서 운영되는 시스템을 대상으로 한 사이버공격의 성공률은 지극히 낮다. 그래서 좀 더 정교하고 은밀한 사이버공격을 위해서 다양한 침투 경로와 도구가 필요하다.

최근 사이버공격 경로는 유·무선 네트워크를 포함한 모든 전자장치와 물리적 수단을 활용하고 있다. 전자파를 비롯한 소리, 주파수, 전기선, 신호, 바코드, 사물 등을 이용하여 악성코드를 전파할 수 있다[6]. 물리적 수단으로는 악성코드가 설치된 이동저장장치의 접속과 고기능의 초소형 스텔스 이동무인체계를 공격 대상 시스템으로 이동시키는 방법도 있다. 이동무인체계는 주로 드론을 활용하게 된다. 드론을 이용한 해킹 방식은 드론의 플랫폼에 악성코드를 설치하거나 GPS 기만기를 탑재하여 데이터를 유출하거나 신호를 교란한다. 또한, 드론에 악성코드를 심은 프로그램을 설치하여 공격 대상이 위치한 지역으로 보내서 통신 네트워크의 AP(Access Point)에 접속하는 패킷에 대한 정보를 획득하거나 네트워크를 감염시킬 수 있다. 초소형 스텔스 드론은 인공지능과 머신러닝으로 인해 자율비행이 가능하고 IoT 기술과 클라우드로 연결된 초연결 통신이 가능하며, 차세대 에너지 전지를 활용하여 공격 지점까지 장기간 비행이 가능하다[9]. 악성코드는 인공지능과 머신러닝 기술이 적용되어 자가 학습과 판단이 가능하여 공격 대상 시스템의 취약점을 발견하고 침투 지점을 식별하여 내부 네트워크로 침투가 가능하다.

## 4. 전장에서 드론을 이용한 보안 위협 시나리오

앞 장에서 제시한 드론을 이용한 보안 위협은 전장에서 사이버공격 도구로 실행이 가능하다. 최근에 군에서는 지상, 해상, 공중에서 효과적인 작전 수행을 위한 무인전투체계 개발에 집중하고 있기 때문에 무인전투체계간 전투가 이루어지는 전장에서는 드론을 이용한 사이버공격이 효과적일 수 있다.

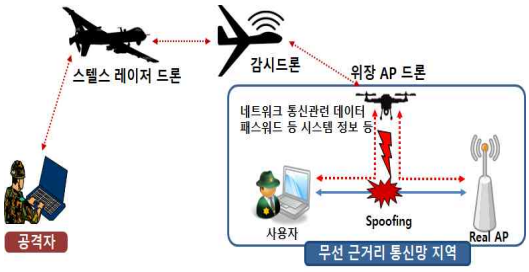
우선, 드론에 해킹 프로그램을 설치하여 공격 대상의 시스템이 위치한 지역으로 이동하여 그 시스템에 저장되어 있는 데이터를 유출한다. 즉, 공격 대상 지휘통제체계나 주요 군사시설의 통제체계를 표적으로 위장 AP 드론을 이용하여 악성코드를 내부 시스템으로 침투시켜 제어권을 획득하고 군사기밀이나 데이터를 유출하는 방법이다. 이 방법을 수행하기 위한 시나리오는 다음과 같다.

① 임무별 드론 배치

정보 유출에 이용되는 드론은 스텔스 레이저 통신 드론, 감시 드론과 위장 AP 드론이 있다. 스텔스 레이저 드론은 공격 대상 지역에 은밀하게 침투한 위장 AP 드론과 감시 드론이 공격자의 시스템과 통신이 가능하도록 중개 역할 임무를 수행한다. 이 드론은 태양에너지를 이용하여 한번 이륙하면 임무 종료 때까지 수 개월간 공역에서 체류할 수 있으며, 18km 이상의 상공에서 작동이 가능하다. 레이저 통신 시스템을 이용하여 지상의 무선 인터넷 망과 고속으로 연결되며, 드론 상호간에도 장거리 통신을 가능하게 한다. 감시 드론은 공격 대상 지역의 상황을 판단하고 위장 AP 드론으로부터 전송받은 데이터를 스텔스 레이저 통신 드론에게 전송하는 임무를 수행한다. 위장 AP 드론은 공격 대상의 무선 근거리 통신망으로 침투하여 위장 AP의 임무를 수행하기 위해서 위장 AP 기능과 무선 통신 기능도 포함되어 있다. 아울러 공격 대상 시스템의 감시에 탐지되지 않기 위해서 스텔스 기능을 추가하고 가능한 소형으로 제작하며, 주변 지역 탐색을 위한 카메라 및 이미지 프로세싱 기능도 탑재한다. 공격자의 시스템과 스텔스 레이저 통신 드론을 통해 연결되어 수집한 정보를 전송하거나 커맨드 메시지를 수신한다.

② 스푸핑

아래는 위장(Fake) AP(Access Point) 드론을 통해서 송·수신되는 데이터를 가로채는 절차를 보여준다.

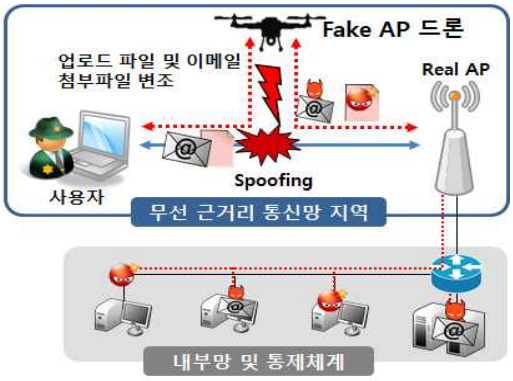



(그림 1) 위장 AP 드론의 스푸핑

위장 AP 드론은 무선 근거리 통신망 지역으로 침투하여 해당 망내의 통신을 관할하는 AP로 위장하여 통신망을 이용하는 부대나 사용자들이 송·수신하는 데이터를 탈취한다. 통신망을 이용하는 사용자들은 본인의 모바일 기기 등으로 통신망에 연결할 때 스푸핑하여 위장 AP를 진짜 AP로 혼동하게 하여 위장 AP로 연결을 유도한다.

③ 악성코드 배포

사용자가 무선망을 이용하여 외부에서 운영하는 사이트에 파일을 업로드하거나 이메일을 통해 첨부파일을 전송하는 경우에 위장 AP 드론이 중간에서 악성코드가 심어진 파일로 교체하여 전송한다. 이메일의 경우는 수신자를 다른 IP(사용자)로 하여 전송하도록 변조할 수도 있다.



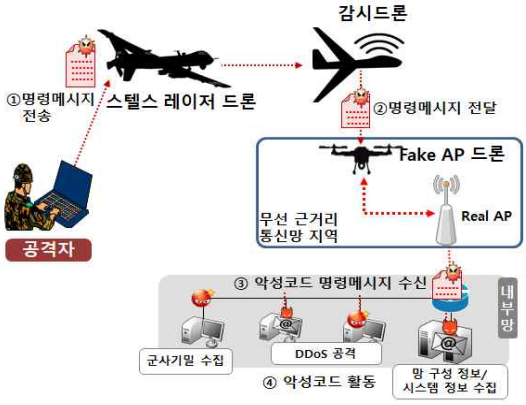

(그림 2) 악성코드 배포 절차

만약, 스푸핑을 통해서 시스템의 접속 정보와 취약점 정보를 알아냈다면 공격자는 이를 기반으로 악성코드를 공격 대상 시스템으로 해킹 메시지를 전달한다. 이 때 위장 AP 드론은 해킹 메시지의 전달자 역할을 수행한다. 침투된 악성코드는 데이터 수집이나 시스템 마비 등의 목적에 따라 다양한 기능을 수행한다.

④ 악성코드 실행

위장 AP 드론을 이용하면 공격목적에 따라 공격 대상 시스템을 감염시킨 악성코드에게 커맨드 메시지를 전송한다. 커맨드 메시지를 수신한 악성코드는 커맨드 메시지의 내용에 따라 임무를 수행

한다. 악성코드가 수집한 정보는 위장 AP 드론에 전달하여 공격자에게 전송된다.




(그림 3) 악성코드 실행 절차

만약, 스푸핑을 통해서 시스템의 접속 정보와 취약점 정보를 알아냈다면 공격자는 이를 기반으로 악성코드를 공격 대상 시스템으로 해킹 메시지를 전달한다. 이 때 위장 AP 드론은 해킹 메시지의 전달자 역할을 수행한다. 침투된 악성코드는 데이터 수집이나 시스템 마비 등의 목적에 따라 다양한 기능을 수행한다.

다음은 GPS 기만기를 드론에 장착하여 무선통신체계나 무인전투체계에 재밍을 실행할 수 있다. 전장에서 운용되는 무인전투체계 는 상황 판단과 전투 행동이 무선 네트워크 기반으로 이루어지기 때문에 신호를 방해하는 재밍, 전파차단, 스마트 재밍 등에 의한 전파 교란에 취약하다. 재밍은 특정 기기, 무선 네트워크나 주파수에 영향을 미칠 수 있기 때문에 전장에서 무인전투체계의 전투능력을 효과적으로 상실시킬 수 있다. 특히, 무인전투체계간 데이터 전송을 위해서 동적 무선 네트워크가 수시로 형성되기 때문에 재밍을 통해서 라우팅 동작을 방해할 수 있다. 아울러 데이터 패킷을 고의적으로 손실시킴으로써 대역폭, 메모리, 계산능력과 같은 자원을 소비시키고 네트워크 성능 저하를 유발시킬 수 있다. 보다 효과적인 재밍을 위해서는 재밍 신호가 영향을 미칠 수 있는 범위 내에 재밍 신호 발생기가 위치해야 하며 비행시간, 탑재능력, 속도 등에서 고정익 드론 수준의 성능이 전제되어야 한다. 해킹 방식은 특정 주파수에 대한 재밍 신호를 발생시켜 무인전투체계간 통신 방해, 스마트 재밍을 통한 무인전투체계의 위치정보 상실 등이 있다. 스마트 재밍은 GPS 기만기를 이용하여 무인전투체계를 재밍한다. 드론에 의한 재밍 공격 시나리오는 다음과 같다.

① 군사위성 GPS 신호 수신

스마트 재밍 드론은 군사위성이 무인항공전투체계로 송신하는 GPS 신호를 수신한다.

② 비정상 위치 정보 생성 및 삽입

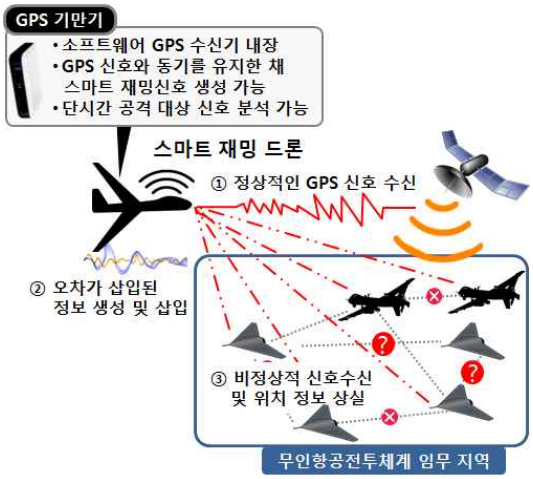
GPS 기만기는 공개된 GPS 신호구조를 이용하여 오차가 인가된 거짓 GPS 신호를 생성하여 적의 무인항공전투체계의 수신기에 송신함으로써 수신기가 잘못된 시각과 위치를 계산하게 한다. GPS 기만기는 GPS 신호를 수신하고 이를 처리할 수 있는 장비를 이용하여 임의 위성신호에 대해 오차가 삽입된 정보를 생성하고, 이를 실제 GPS 신호보다 다소 높게 송출함으로써 무인항공전투체계의 수신기가 실제 GPS 신호가 아닌 기만기가 송출한 신호를 획득 및 추적하도록 한다. 드론은 GPS 기만기를 이용하여 무인항공전투체계에 송신할 오차가 있는 위치 정보를 생성한다.

③ 비정상 위치 정보 송신

오차가 삽입된 신호를 실제 GPS 신호보다 강하게 송출하여 무인항공전투체계의 신호 수신기가 GPS 기만기에서 송출된 신호를 수신할 수 있도록 한다. 오차가 있는 신호를 수신 받은 무인항공전투체계는 원래 위치 정보를 상실하고 상호간에 신호 교환에 오류가 발생하거나 잘못된 위치 정보로 인해서 협력적인 전투수행이 불가능하게 된다.

통신 재밍은 재밍기를 드론에 장착하여 무선 애드 혹 네트워크를 마비시킨다. 무선 애드 혹(Ad-hoc) 네트워크는 유선 네트워크나 무선 네트워크에 비해 무선 채널 환경이 개방되어 있고 동적인 네트워크 토폴로지 형태이며, 분산 협력 통신 구조이기 때문에 안정성 측면에서 취약하다. 그래서 무인전투체계간 통신을 하기 위해서 무선 애드

혹 네트워크 형태의 통신체계가 일시적으로 구성되는데, 이때 라우팅 정보를 변경하거나 패킷을 손실시키면 통신장애가 발생하게 된다. 즉, 통신 중에 강한 데이터 신호를 발사하게 되면 일시적으로 패킷 전송이 늦어지거나 손실되어 통신이 불가능하게 된다.




(그림 4) GPS 기만기에 의한 신호 재밍

이 밖에도 4차 산업혁명의 원동력이 되는 인공지능, 딥러닝, 상황인식, 자율제어 등의 기술들이 무인전투체계에 적용된다는 것을 가정할 경우에 해킹 임무용 드론을 이용하여 무인항공전투 전력을 무력화시킬 수도 있다. 인간의 직관적이고 명시적인 판단이 개입되지 않는 무인 전장 환경에서는 송·수신되는 작전 및 전술 정보를 가로채 잘못된 정보를 삽입한다거나 비정상적인 임무 메시지를 전파한다면, 신속하게 메시지 인증이나 데이터의 오류를 검사를 할 수 없게 되어 정상적인 임무 수행을 불가능하게 할 수 있다.

해킹 임무용 드론은 전장지역에서 교전하는 것처럼 비행하면서 상대편의 무인항공전투체계의 무선 통신망의 취약점을 찾아내서 지능형 자율 악성코드를 전파한다. 지능형 자율 악성코드는 무선 애드혹(Ad-hoc) 네트워크를 통해 송·수신되는 패킷이 AP에 송·수신될 때, 인공지능형 알고리즘으로 패킷을 분석하여 내부로 침투한 후 자가 학습형 알고리즘을 통해 무인항공전투체계의 구성요소로 인식할 수 있게끔 자가 변이를 한다. 이 때, 악성코드가 아측의 무인항공전투체계에 침투하지 못하도록 인공 지능적인 알고리즘을 통해 적·아 네트워크 식별할 수 있도록 한다. 상대편의 무인항공전투체계가 악성코드에 감염되면 삽입된 오정보로 인해서 정확한 위치정보를 알 수 없게 되어 상호 충돌하게 된다. 또한, 상대편의 무인항공전투체계에 대한 원격 제어가 필요할 경우에 해킹 임무용 드론을 중계기로도 활용할 수 있다. 공격자로부터 전송된 원격 제어 명령 신호를 수신한 상대편의 무인항공전투체계는 악성코드에 의해 통신 및 제어 권한을 빼앗겼기 때문에 수신된 원격 제어 명령을 유효하게 판단하고 시스템의 제어권을 넘겨준다.

## 5. 결 론

드론의 활용은 새로운 정보통신기술이 적용됨에 따라 다양한 분야로 확대될 것이며, 성능도 첨단화될 것이다. 군사 분야에서의 드론의 활용은 군사작전과 연계하여 기존의 무기체계 플랫폼과 협업하거나 그 역할을 대신할 수 있을 것으로 전망된다.

본 논문에서는 드론의 활용 분야와 성능이 발달됨에 따라 드론을 해킹 수단으로도 활용할 수 있다는 가능성을 제시하였다. 전장에서 무인전투체계의 활용도가 증가됨에 따라 무인전투체계의 작전 무력화를 목적으로 한 해킹기술에 대한 연구도 활발히 진행되고 있다. 해킹기술 중에서 가장 성공확률이 높을 것으로 보이는 기술은 드론에 악성코드를 심어 공격 대상 무인전투체계나 통신체계를 감염시켜 정보를 유출하고 통신을 마비시키는 것이다. 또한 드론에 GPS 기만기를 설치하여 정상적인 신호를 조작한 후에 드론의 위치 정보를 상실시킬 수도 있다. 해킹 수단으로써 드론을 이용한 보안 위협과 시나리오의 제안은 전장에서의 무인전투체계에 대한 보안 위협의 심각성을 인지시키고 미래 사이버전 대응책을 수립하는데 동인을 제공하고자 한다.

## 참고문헌


[1] 장태진, “4차 산업혁명의 도래와 드론”, Aviation Issue, No.13 pp.1~12, 2017.

[2] 차동완 외 4명, “군사용 드론 현황 및 대 드론 대책”, 국방과 기술, Vol.471 pp.140~153, 2018.

[3] 조현석, “인공지능, 자율무기체계와 미래 전쟁의 변환”, 21세기정치학회보 8(1), pp.115-139, 21세기정치학회보 8(1), 2018.

[4] 김대우 외 11명, “인공지능 기반 드론 목표물 추적 시스템의 설계 및 구현", 한국통신학회논문지 42(12), pp.2391-2401, 2017.

[5] 손경환 외 10명, "드론 활용 목표물 추적 응용에서의 인공지능 작업 실행 효율 비교 분석", 한국통신학회논문지 43(1), pp.143-151, 2018.

[6] Chang-Hoi Hur, Seong-Pyo Kim and Jung-Ho Eom, “Changes of Cyber-Attacks Techniques and Patterns after the Fourth Industrial Revolution” Proceedings of the 5th International Conference on FiCloud, 2017.

[7] 박종훈, “최신 ICT 이슈”, 정보통신기술진흥센터 주간기술동향 제1846호, pp.36-39, 2018.http://www.itfind.or.kr/WZIN/jugidong/1846/file3518932204085386397-184606.pdf, (검색일: 2018.9.28.)

[8] https://www.anadronestarting.com/%ED%95%B4%ED%82%B9/, (검색일: 2018.7.14.)

[9] https://www.slideshare.net/wanggukang/4-74536043 (4차산업혁명과 드론의 역할), (검색일: 2018.8.16.)

[10] https://www.ahnlab.com/kr/site/securityinfo/secunews/ secuNewsView.do?menu_dist=1&curPage=&columnist=&series_key=&seq=22615, (검색일: 2018.8.16.)

[11] https://www.youtube.com/watch?v=mmy-Q0taPOY, (검색일: 2018.8.18.)

[12] http://www.etnews.com/20151019000014, (검색일: 2018.9.28.)

[13] http://news.chosun.com/site/data/html_dir/2018/09/28/2018092801050.html, (검색일: 2018.9.28.)

[14] https://www.bloter.net/archives/269792, (검색일: 2018.9.29.)


## [저 저 소 개]

박 근 석 (Keun-Seog Park)
1989년 2월 금오공과대학교 기계공학과 학사
2001년 2월 군사과학대학원 항공우주공학과 석사
2017년 2월 대전대학교 군사학과 박사
email : pksm06@naver.com

천 상 필 (Sang-pil Cheon)
1984년 2월 공군사관학교 기계공학과 학사
1994년 2월 연세대학교 기계공학과 석사
2015년 2월 대전대학교 군사학과 박사
email : skyfeel69202@naver.com

김 성 표 (Seong-Pyo Kim)
1987년 2월 공군사관학과 국제관계학과 학사
1996년 7월 오클라호마 주립대 전자공학과 석사
2004년 7월 미주리대학교 컴퓨터공학과 박사
email : spkim35@add.re.kr

엄 정 호 (Jung-ho Eom)
1994년 2월 공군사관학교 항공공학과 학사
2003년 2월 성균관대학교 전기전자 및 컴퓨터공학과 석사
2008년 2월 성균관대학교 컴퓨터공학과 박사
email : eomhun@gmail.com