Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.3, Jun. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.3.431

GPS 스푸핑 공격 취약점 분석 및 실증: 상용 드론을 대상으로*

윤 진 서,[1†] 김 민 재,[2] 이 경 률[3‡]
[1]전남대학교 (학생), [2,3]국립목포대학교 (학생, 교수)

Analysis and Demonstration of GPS Spoofing Attack: Based on Commercial Drones*

Jinseo Yun,[1†] Minjae Kim,[2] Kyungroul Lee[3‡]
[1]Chonnam National University (Undergraduate student),
[2,3]Mokpo National University (Undergraduate student, Professor)

요 약

최근 드론은 공공의 목적을 넘어, 다양한 산업에서 활용되며, 민간 분야까지 확대되어 상용화되는 실정이다. 현재 상용화되는 대부분 드론은 사용자에게 드론의 위치를 알리기 위한 목적으로, 인공위성으로부터 위치 신호를 수신하는 GPS 수신기를 장착하지만, 인공위성으로부터 위치 신호를 전달받는 거리가 멀다는 단점과 이로 인하여 수신하는 위치 신호의 세기가 약하다는 단점이 존재한다. 이러한 단점들로 인하여, 인공위성으로부터 수신하는 위치 신호보다 더욱 강한 신호를 드론에서 수신한다면, 의도하지 않은 위치정보를 수신하는 위치 조작과 재밍 공격이 가능하다. 따라서, 본 논문에서는 GPS를 기반으로 위치정보를 활용하는 드론에 대한 안전성 평가 및 무선 통신 상황에서 발생 가능한 취약점에 대응하기 위한 목적으로, 상용 드론들을 대상으로, GPS 스푸핑 공격에 대한 가능성을 분석하고 실증한다. 본 논문의 결과는 더욱 현실적인 취약점 분석 및 안전성 평가를 위한 실험과 그 결과를 도출하기 위한 선행 연구로 활용될 것으로 사료된다.

ABSTRACT

Drones in the contemporary landscape have transcended their initial public utility, expanding into various industries and making significant inroads into the private sector. The majority of commercially available drones are presently equipped with GPS receivers to relay location signals from artificial satellites, aiming to inform users about the drone's whereabouts. However, a notable drawback arises from the considerable distance over which these location signals travel, resulting in a weakened signal intensity. This limitation introduces vulnerabilities, allowing for the possibility of location manipulation and jamming attacks if the drone receives a stronger signal than the intended location signal from satellites. Thus, this paper focuses on the safety assessment of drones relying on GPS-based location acquisition and addresses potential vulnerabilities in wireless communication scenarios. Targeting commercial drones, the paper analyzes and empirically demonstrates the feasibility of GPS spoofing attacks. The outcomes of this study are anticipated to serve as foundational experiments for conducting more realistic vulnerability analysis and safety evaluations.

Keywords: Drone, Wireless communication, GPS spoofing attack, Vulnerability Analysis

Received(01. 18. 2024), Modified(03. 28. 2024), Accepted(03. 28. 2024)

* 본 논문은 2023년도 한국정보보호학회 호남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임

* 본 과제(결과물)는 2024년도 교육부의 재원으로 한국연구재단의 자원을 받아 수행된 지자체-대학 협력기반 지역 혁신 사업의 결과입니다. (2021RIS-002)

† 주저자, 202800@jnu.ac.kr

‡ 교신저자, carpedm@mnu.ac.kr(Corresponding author)

I. 서 론

최근 드론은 해경의 수색이나 재난 상황 발생 시, 현장 점검 및 감시, 순찰과 채증 목적을 넘어, 인력난 해결과 생산성 향상을 위한 농업 분야, 건설 노동자의 안전 및 진척도 관리를 위한 건설 분야, 운송업체의 물품 배송 서비스와 같은 다양한 산업과 민간 분야에서 활용되는 실정이며, 이러한 장점으로 인하여 드론이 더욱 상용화되는 추세이다[1].

드론은 일반적으로 구동부, 제어부, 페이로드, 통신부로 각각의 특징에 따라 분류되며, 구동부는 드론 기기를 구동하는 모터나 프로펠러, 배터리 등으로 구성되어 비행과 호버링 기능을 수행한다. 제어부는 구동부의 기능을 제어하며, 가속도센서, 자이로센서, GPS(Global Positioning System) 센서 등을 포함한다. 페이로드에는 드론의 사용 목적에 따라 추가될 수 있는 장비로 구성되며, 영상 촬영 목적의 카메라나 적외선 카메라, 농약 살포기 등으로 구성된다. 마지막으로 통신부는 드론의 데이터 송수신과 명령어를 수신하며, RC 수신기나 비디오 송신기, LTE, WiFi로 구성된다[2].

대부분 드론은 비행 제어 및 유지를 위하여, GPS 수신기를 장착하여 인공위성으로부터 수신되는 신호를 분석함으로써, 자신의 위치 좌표와 고도를 측정하고, 비행할 거리를 파악한다. 그러나 GPS 수신기의 경우, 인공위성과 드론이 약 2만 km 정도의 거리에 위치하는 특징으로 인하여, 지상에서 GPS 신호를 수신하는 세기가 약하다는 문제점이 발생한다. 이러한 문제점에 따라, GPS 수신기에는 신호를 증폭하여 수신하기 위한 증폭기가 설치되며, 만약 GPS 수신기가 정상 GPS 신호보다 세기가 강한 위변조된 신호를 수신하면, GPS 위치의 조작이 가능하며, GPS 교란 신호에 의하여 드론의 위치를 조작하는 GPS 스푸핑 공격이나 통신을 방해하는 재밍 공격과 같은 보안 위협이 발생할 수 있다[3].

이와 같이, GPS 신호를 조작하는 공격은 특별한 기술이 요구되지 않아, 누구나 악의적인 목적으로 위치정보를 조작하거나 전파를 방해할 수 있으며, 조작된 위치정보로 인하여 드론을 비정상적으로 비행하도록 유도하는 행위나 사용자의 목적과 다르게 드론을 제어하는 행위, 드론의 조종을 무력화하고 탈취함으로써 내부에 저장된 민감한 정보를 탈취하는 악의적인 행위가 가능하다.

이러한 드론의 GPS 신호 조작에 따른 취약점으로 인한 보안위협에 대응하기 위하여, 본 논문에서는 GPS를 기반으로 위치정보를 송수신하는 드론의 안전성 향상과 무선 통신에서 발생하는 취약점에 대응하기 위한 목적으로, GPS 스푸핑 공격에 대한 취약점을 분석하고 실증한다.

II. 관련 연구

GPS는 인공위성으로부터 전달되는 위치정보를 실외 환경에서 원활하게 사용하도록 제공하는 위치추정 방식으로, 실외 환경이 아닌 건물 내부나 구조물이 많은 외부에서는 위치 신호가 원활하게 수신되지 않아 위치를 추정하기 어려운 한계점이 존재한다. GPS 신호를 수신하는 과정의 일례를 Fig.1.에 나타내었다. 드론은 비행 시에 사용자와 정보를 지속적으로 공유하여야 하기 때문에, 이러한 정보를 전달하기 위한 방안이 필수적으로 요구된다.

따라서, 드론이 사용자와 통신하는 상황에서 발생 가능한 보안위협은 주로 통신 프로토콜 자체의 취약점을 이용하거나 드론이 사용하는 네트워크에서 발생하는 공격에 대한 연구가 주를 이룬다. 특히, 드론이 WiFi 통신을 사용하는 경우, 네트워크 공격이나 패킷을 캡처함으로써, 드론으로 송수신하는 정보를 탈취하거나, 드론의 가용성을 방해하는 공격을 주요하게 다루고 있다.

또한, 드론의 항법 제어를 위한 GPS 신호나 ADS-B(Automatic Dependent Surveillance) 신호가 암호화되지 않은 신호를 수신하거나, 수신기 자체의 취약점으로 인한 보안위협이 발생하였다. 이와 같은 GPS 스푸핑 공격을 탐지하기 위하여, 물리적 방법을 이용한 탐지 메커니즘이 제안되었지만, 드론의 GPS 수신기는 거리가 가까울 때 실제 인공위성으로부터의 GPS 신호보다 조작된 신호를 수신하는 한계점이 존재한다. 이러한 한계를 보완하기 위하여, GPS 신호를 인증하는 기술인 NMA(Navigation Message Authentication)가 추가적으로 제안되었다[4].

상기와 같은 GPS 신호의 신뢰성을 확보하기 위한 보안 메커니즘이 등장하고, 이를 드론에 적용하기 위한 다양한 연구들이 진행됨에도 불구하고, 현재 상용화된 드론을 대상으로 보안 위협에 대한 평가는 미흡하며, 특히, 보안 메커니즘이 적용되지 않아 보안 위협에 노출되고 있는 실정이다. 따라서, 본 논문에서는 일반화된 GPS 스푸핑에 대한 공격 방법을 상

용화된 다양한 드론에 적용함으로써, GPS 스푸핑 공격 가능성을 분석하고, 공격이 발생하는 근본적인 원인 및 대응방안을 고찰하고자 한다.

III. GPS 스푸핑 공격 취약점 분석

본 장에서는 다양한 상용 드론 중, F 드론을 대상으로, GPS 스푸핑 공격 가능성에 대한 분석 결과를 서술한다. 공격 가능성을 분석하기 위하여, 드론에서 GPS 신호를 수신하는 원리와 수신과정에서 발생 가능한 공격에 대한 이해가 필요하며, 이를 통하여, 드론에서 GPS 위치 신호를 수신할 때 발생 가능한 GPS 스푸핑 공격에 대한 취약점을 분석한다.

3.1 GPS 신호 수신 원리

GPS는 인공위성으로부터 전달되는 위치정보를 실외 환경에서 원활하게 사용하도록 제공하는 위치추정 방식으로, 실외 환경이 아닌 건물 내부나 구조물이 많은 외부에서는 위치 신호가 원활하게 수신되지 않아 위치를 추정하기 어려운 한계점이 존재한다[5]. GPS 신호를 수신하는 과정의 일례를 Fig.1.에 나타내었다.

GPS 신호의 수신과정을 살펴보면, GPS 수신기의 안테나는 인공위성으로부터 GPS 신호를 수신하고 다시 인공위성으로 반송한다. 여기에서 RF 부분은 코드 정보를 식별하고, 컴퓨터는 코드 정보와 반송파의 메시지를 처리하여, 수신기로부터 인공위성까지 반송되는 신호의 시간 차이를 계산한다. 이러한 측정 방법에 따라, 인공위성과 수신기의 거리를 계산하여 위치를 측정한다. 그러나 하나의 위성만으로 위치를 측정한다면, 오차가 크게 발생하므로, 더욱 정확하게 위치를 측정하고 오차를 줄이기 위하여, 3개 이상의 인공위성 신호를 사용하여 삼각 측량법으로 거리를 계산한다[6].

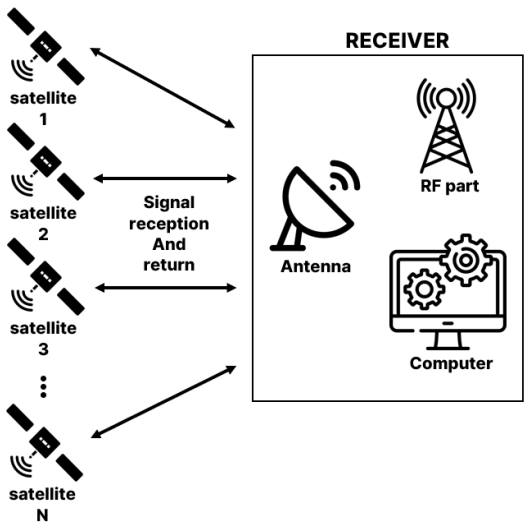

Fig. 1. GPS Signal Receiving Process

그러나 상기와 같이, GPS 신호를 송수신하는 과정은 신호에 포함된 정보를 안전하게 전달하기 위한 보안 프로토콜이 적용되지 않아, 다양한 공격으로부터 안전하지 못한 취약점이 존재한다. 특히, GPS 수신기는 인공위성과의 거리가 멀다는 특징과 이로 인하여 지상에서 수신하는 신호 세기가 약하다는 특징, 그리고 공격자가 지상에서 송신하는 신호 세기가 인공위성으로부터 수신하는 신호 세기보다 강하다는 특징이 나타난다[7].

이러한 특징들을 악용하여, 만약 공격자가 GPS 신호를 수신하는 안테나 근처에서 위변조된 위치 신호를 강하게 송신하는 경우, GPS 수신기는 인공위성의 신호보다 신호 세기가 더욱 강한 공격자의 신호를 수신하는 문제점이 나타나며, 이러한 문제점은 GPS 수신기를 장착한 다양한 기기에서 GPS 정보를 악용하는 GPS 스푸핑 공격과 같은 취약점이 발생하는 원인으로 나타난다.

3.2 GPS 스푸핑 공격 가능성 분석

본 절에서는 상기 분석한 GPS 신호의 수신 원리를 기반으로, 드론 환경에서의 GPS 스푸핑 공격 가능성에 대한 분석 결과를 서술한다. 일반적인 GPS 스푸핑 공격을 기반으로, 본 논문에서 분석한 GPS 스푸핑 공격 과정을 Fig.2.에 나타내었다.

그림을 살펴보면, 대부분 드론은 GPS 수신기를 포함하므로, 위변조된 신호를 통한 GPS 스푸핑 공격이 가능할 것으로 판단된다. GPS 스푸핑 공격 과정을 살펴보면, 크게 네 단계로 구성된다.

첫 번째 단계는 공격자가 GPS 천체력 데이터를 활용하여, NFZ(No Fly Zone)로 설정된 GPS 신호 파일을 생성하는 단계이다. NFZ는 항공 보안법상 드론과 같은 무인이동체가 비행하지 못하도록 특별하게 설정한 위치로, 만약 드론의 GPS 위치가 NFZ에 진입하는 경우, 미리 설정된 행위에 따라, 드론의 비행을 중단시키거나 이륙한 위치로 복귀시킨다.

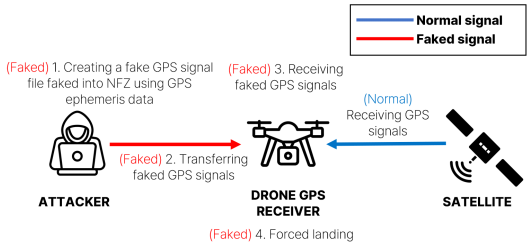

Fig. 2. Drone GPS Spoofing Attack Process

두 번째 단계는 위변조된 GPS 신호 파일을 드론 주변에 전송하는 단계이며, 세 번째 단계에서 드론의 GPS 수신기는 위변조된 GPS 신호를 수신한다. 결과적으로는 네 번째 단계에서 드론이 비행 가능한 위치에 있더라도 드론의 위치가 NFZ로 조작되어, 더 이상 비행하지 못하는 비정상적인 행위가 발생한다.

이와 더불어, 만약 공격자가 NFZ 뿐만 아니라, 공격자가 원하는 위치로 조작한다면, 드론의 제어권이나 드론 자체를 탈취함으로써, 드론의 비행 정보나 내부에 저장된 GPS 정보 및 촬영 정보와 같은 민감한 정보를 탈취하는 추가적인 공격이 가능할 것으로 판단된다.

IV. GPS 스푸핑 공격 취약점 실증

3장에서 분석한 GPS 스푸핑 공격을 실증하기 위하여, 다음과 같은 실험 환경을 구성하였으며, GPS 신호를 생성하고 송신하기 위한 HackRF One과 GPS 신호를 생성하기 위한 소프트웨어인 GPS-SDR-SIM을 사용하였고, kali linux 2022.2 버전의 운영체제에 설치하였다. 자세하게는, GPS 신호의 조작에 대한 실험 결과를 더욱 명확하게 분석하기 위하여, 조작된 GPS 신호를 수신하기 용이한 실내 환경에서 실험하였고, GPS 스푸핑 공격을 시도하는 HackRF One과 실험 대상 드론의 물리적 거리는 1m 이내로 설정하였다.

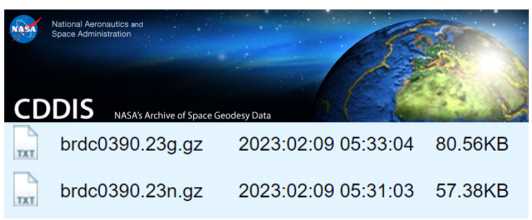

Fig. 3. NASA's Astrophysical Data

우선, GPS-SDR-SIM 소프트웨어는 GPS 위성 간 의사거리 및 도플러를 시뮬레이션하여 GPS 신호 파일을 생성하며, GPS 위치를 위한 천체력 파일이 필요하다. 이에 따라, GPS 위치를 NFZ로 위변조하기 위하여, Fig.3.과 같이 NASA에서 제공하는 천체력 데이터 파일을 다운로드하고, GPS-SDR-SIM 소프트웨어의 옵션으로 8bit 데이터 형식으로, NFZ의 위도와 경도를 설정하여 Fig.4.와 같이 위변조된 GPS 신호 파일을 생성한다.

그다음으로, 위변조된 GPS 신호 파일을 HackRF One 장치를 통하여 전송한다. 이때, GPS L1 주파수 대역인 1575.42MHz 대역에 2.6MHz 샘플 속도로 GPS 신호를 전송하였으며, GPS 스푸핑 공격의 실증 결과를 Fig.5.에 나타내었다.

Fig.6.에 나타낸 것과 같이, 위변조된 GPS 신호를 수신한 경우, 노란색으로 표시된 현재 위치와는 다르게 빨간색으로 표시된 곳으로 드론의 위치가 변경되었음을 확인할 수 있다. 이는 공격자에 의하여 GPS 신호가 NFZ인 공항으로 위변조된 신호를 드론에서 수신한 것을 의미하며, 드론의 수신기가 인공위성보다 공격자의 송신기에 상대적으로 가깝고, 더

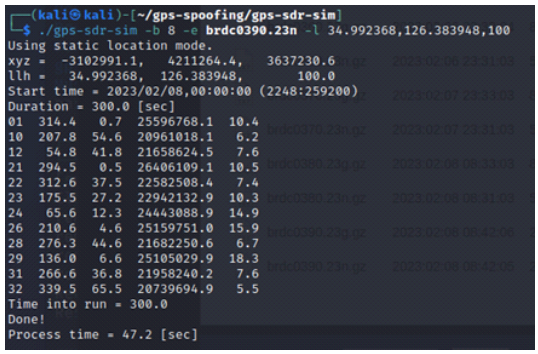

Fig. 4. The Process of Creating a Forged GPS Signal File with NFZ

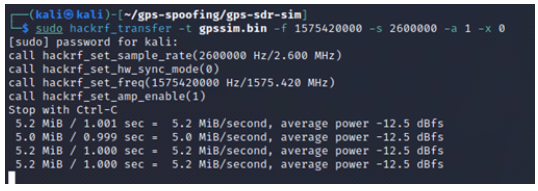

Fig. 5. Transmission Process of Forged GPS Signals

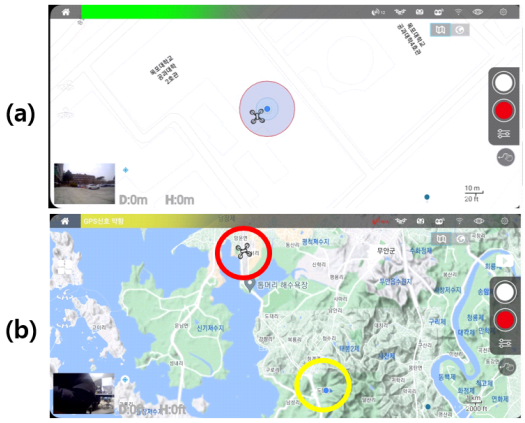

Fig. 6. GPS Spoofing Attack Experiment Results (a. Normal GPS Signals, b. Forged GPS Signals)

강한 신호를 수신한다는 점이 취약점이 발생하는 근본적인 원인으로 판단된다.

V. 상용 드론에 적용한 GPS 스푸핑 공격 결과 분석

상용 9개 드론을 대상으로, GPS 스푸핑 공격을 시도하였으며, 보안상 공개가 가능한 3개의 공격 결과를 Table 1.에 나타내었다. 4장의 “GPS 스푸핑 공격 취약점 실증”과 마찬가지로, 공격 과정 일례는 위변조할 NFZ의 위도와 경도를 찾기 위하여 NASA의 천체력 데이터를 다운로드하는 1단계, 천체력 데이터를 활용하여 위변조된 GPS 신호 파일을 생성하는 2단계, HackRF One 장치를 통하여 위변조된 GPS 신호 파일을 전송하는 3단계, 마지막으로 위조된 신호를 수신하는 4단계로 공격 과정을 구성하여 상용 드론에 적용하였다.

표를 살펴보면, GPS 수신기가 드론 내부에 포함된 드론은 GPS 스푸핑 공격에 성공하였다. 이는 드론이 GPS 수신기를 포함할 경우, 위변조된 GPS 신호를 현재 위치로 인식함으로써 위치정보가 교란되어 정상 비행경로를 이탈할 가능성이 존재한다. 예를 들어, 위변조된 GPS 신호를 수신할 경우, 드론이 실제 위치와 다르게 위변조된 위치로 인식하며, 비행 시도 시, 비행이 제한된 구역이라는 경고 메시지나 이륙이 불가하다는 메시지가 함께 나타난다. 만약, 드론이 비행 중일 경우, 위변조된 GPS 신호를 전송하면, 실제 위치가 변경되며, 드론의 비행이 제한된 곳이므로 비행하지 못하도록 자동 착륙한다. 따라서, 잘못된 위치를 인지한 사용자가 드론의 조작이나 이륙을 시도하면, 드론의 위치가 NFZ로 변경되었기 때문에, 이륙이 제한되고 공격자에 의하여 드론이 탈취될 가능성이 존재한다.

Table 1. Results of GPS Spoofing Attack on Commercial Drones

Drone	GPS presence	Attack result (S/F)	Landing state after attack	Flight state after attack
A	○ (IN)	S	Restricted area text, Change of map location, Notice of flight restrictions during takeoff attempts, Disabling takeoff	Auto landing
F	○ (IN)	S	Change of map location	Change of map location
G	○ (IN)	S	Change of map location	Auto landing

S: Success, F: Fail

VI. 결 론

대다수 드론이 비행 과정에서의 위치정보를 획득하기 위하여, GPS 수신기를 사용한다. GPS 수신기는 신호를 수신할 수 있는 범위 내의 모든 신호를 수신하기 때문에, 상대적으로 더 강한 신호를 수신한다면, 그 신호를 신뢰한다는 문제점이 발생한다. 따라서, 본 논문에서는 GPS 위치정보를 사용하는 드론에 대한 안전성 향상 및 무선 통신 상황에서 발생 가능한 취약점에 대응하기 위하여, 상용 드론을 대상으로 GPS 스푸핑 공격을 분석하고 실증하였다.

실증 결과, 공격자가 악의적인 목적으로 비정상행위를 유발하는 위변조된 GPS 신호를 드론에 송신하는 경우, 실제 위치와는 다르게 드론에서 위변조된 위치로 변경되는 결과를 실증하였다. 만약 이러한 취약점을 공격자가 악용하는 경우, 공격자가 원하는 위치로 드론을 이동시키거나 군사 목적 및 감시, 채증 목적으로 활용되는 드론을 탈취하는 것과 같은 비정상적인 행위를 유발하는 것이 가능할 것으로 사료된다.

GPS를 기반으로 위치정보를 송신하는 드론에서의 GPS 위변조 공격에 대응하기 위하여, 드론의 GPS 신호를 처리하고 분석함으로써, 스푸핑 공격을

탐지하기 위한 신뢰할 수 있는 신호처리와 관련된 연구와 인공지능을 활용함으로써 드론이 GPS 신호를 수신할 때 정상 신호와 이상 신호를 분류하여 GPS 스푸핑 공격을 탐지하는 방안에 대한 연구가 필요할 것으로 사료된다.

본 논문에서는 GPS 신호의 조작에 대한 실험 결과를 더욱 명확하게 분석하기 위한 목적으로, 조작된 GPS 신호를 수신하기 용이한 실내 환경에서 실험하였고, 물리적 거리를 한정하였다. 향후, 실외 환경에서 정상적인 GPS 신호를 수집하여 실내 환경의 드론에 전송하는 연구와 거리에 따른 GPS 스푸핑 공격의 유효성 변화를 고려함으로써, 더욱 현실적인 요소를 반영하는 연구를 진행할 예정이다.

References

[1] Hyun-ji Cho and Ji-young Kim, "Analysis and outlook of the industrial drone market," *KIPE MAGAZINE,* 10(2), pp. 45-48, Feb. 2020

[2] KISA, "Cyber security for drone," KISA, Dec. 2020, pp. 1-92, Dec. https://www.kisa.or.kr/2060205/form?postSeq=9&lang_type=KO, accessed on (May 28, 2024)

[3] Chang-Kyung Choi, Yun-hoo Na, and Ki-bum Park, "A study on drone GPS attack types and countermeasures," *Jounal of The Korea Society of Information Technology Policy & Management*, 15(2), pp. 3245-3255, Jun. 2023

[4] Seong-Min Cho and Seung-Hyun Seo, "The current status of cryptographic techniques applied to drone security," *REVIEW OF KIISC,* 30(2) pp. 11-19, Apr. 2020

[5] Hyun-soo Yang and Dong-joon Lee, "Drone flight control and condition estimation basis," *The journal of The Korean Institute of Communication Sciences*, 32(2), pp. 86-92, Jan. 2016

[6] Kyu-in Ji and Young-jae Lee, "Global Positioning System(GPS) : principles and applications," *Journal of Institute of Control, Robotics and Systems*, 2(2), pp. 10-18, Mar. 1996.

[7] Sung-jae Choi, Jung-Min Roh, and Sang-Ha Kim, "A study on effective countermeasures against cyber threats to drones," *Korean Journal of Military Art and Science*, 78(3), pp. 301-328, Oct. 2022

〈저자소개〉

윤 진 서 (Jinseo Yun) 학생회원
2020년 3월~현재: 전남대학교 자율전공학부 학사과정
〈관심분야〉 정보보호, 취약점 분석, Offensive security

김 민 재 (Minjae Kim) 학생회원
2021년 3월~현재: 국립목포대학교 정보보호학과 학사과정
〈관심분야〉 정보보호, 취약점 분석, Offensive security

이 경 률 (Kyungroul Lee) 정회원
2008년 8월: 순천향대학교 정보보호학과 공학사
2010년 8월: 순천향대학교 정보보호학과 공학석사
2015년 2월: 순천향대학교 정보보호학과 공학박사
2011년 5월~2011년 12월: (미)퍼듀대학교 방문연구원
2015년 6월~2016년 2월: 순천향대학교 박사후연구원
2016년 3월~2020년 8월: 순천향대학교 연구 조교수
2020년 9월~2022년 2월: 대구가톨릭대학교 컴퓨터소프트웨어학부 조교수
2022년 3월~현재: 국립목포대학교 정보보호학과 조교수
〈관심분야〉 정보보호, 취약점 분석, 시스템 보안, 하드웨어 보안, 역공학, Offensive Security