와이파이 기반 드론 네트워크의 보안 취약점 분석 및 대응방안

손성호, 홍준기, 김슬기, 김태훈■
국립한밭대학교 컴퓨터공학과
{20201773, 20191759, 20211870}@edu.hanbat.ac.kr, thkim@hanbat.ac.kr

Vulnerability Analysis of WiFi-based Drone Networks and its Countermeasures

Seongho Son, Jungi Hong, Seulki Kim, Taehoon Kim■
Department of Computer Engineering, Hanbat National University

요 약

본 논문에서는 와이파이 기반 드론 네트워크의 보안 취약점을 분석하고 대응 방안에 대해 고찰한다. 실험을 통해 보다 안전한 드론 운용을 위한 대응책과 추후 연구의 방향성을 제시한다.

1. 서 론

최근 드론은 농업용, 군용, 촬영용 등 많은 분야에서 쓰이고 있으며, 여러 군집을 통한 박람회와 페스티벌(2024 대한민국 드론 박람회, 2023 빛고을 페스티벌)등 각종 문화행사에 활용되면서 그 인기가 늘어나고 있다. 또한, 드론을 취미로 이용하는 소비자들이 증가함에 따라 드론 시장이 전 세계적으로 커질 것으로 예상된다. 드론의 상용화는 보안으로 인하여 다양한 문제가 야기될 수 있다. 카메라를 장착 한 드론으로 인한 사생활 침해와 범죄행위가 늘어나고 있으며 마약, 무기 등의 밀반입 수단으로 사용하는 등 그 사용자의 의도에 따라 여러 위험요인이 발생하게 된다 [1]. 드론의 연결을 끊는 인증 해제 및 드론의 통제권을 가져오는 하이재킹을 통한 불법 영상촬영 등을 비롯하여 특정 목표물을 향한 드론의 고의적 추락 등이 발생할 경우 재산 피해와 인명 피해까지 발생할 수 있다 [2]. 실제 사례로는 2020년 9월 부산에서 입주민의 사생활을 촬영한 사건과, 인천공항의 불법 드론이 날아다녀 항공기가 회항을 하는 사건이 있었다 [3]. 이러한 사건이 일어날 경우 공격자는 수사망을 쉽게 빠져나갈 가능성도 있다. 위와 같은 드론 하이재킹을 시도하는 공격자로부터 드론의 통제권을 지키는 것 또한 중요한 보안 문제 중 하나라 할 수 있다. 본 논문에서는 와이파이 기반 드론 네트워크의 취약점을 분석하고 대응책에 대해 제시하고자 한다.

2. 드론 하이재킹

Tello 드론은 자체적으로 와이파이 AP(Access Point) 역할을 한다. 드론을 제어하기 위해 모바일 앱(APP)을 이용해 드론 AP에 접속하여 앱을 통해 제어하든지, 노트북/데스크탑을 이용해 드론 AP에 접속 후 Python API가 제공되는 SDK를 이용해 드론을 제어할 수 있다. Tello 드론은 AP역할을 할 수 있으며, 이는 다수의 단말이 드론에 접속할 수 있다는 것을 의미한다. 이 점에 착안하여 드론 AP에 드론을 제어하고 있는 제어기기 이외의 단말(공격자 또는 Attacker)이 접속한 후 공격자(Attacker)가 접속한 후 패킷을 삽입(injection)하고자 한다. 이를 하이재킹이라 일컬으며, 이 과정에서 획득한 패킷을 분석하고자 한다.

그림 3은 드론 하이재킹 실험을 위해 고려하고 있는 시나리오를 시각적으로 표현한 그림이며, 사용자는 노트북을 통해 텔로 드론을 제어하고 있는 상황이며, 공격자도 노트북을 이용해 공격을 가하고 있는 상황이다. 이 경우, 공격자는 어떠한 명령을 송신해도 기존의 드론 제어를 방해할 수는 없었으며, 인증 해제를 통해 사용자의 연결을 우선적으로 끊는 행위를 먼저 해야했다 [4]. 드론은 Python를 통해 컨트롤을 시작하면 먼저 통제권을 가져온 컨트롤러가 통제권을 유지하며, 이후에 접속을 시도하여 통제권이 없는 컨트롤러로는 신호를 보낼 수 없다.

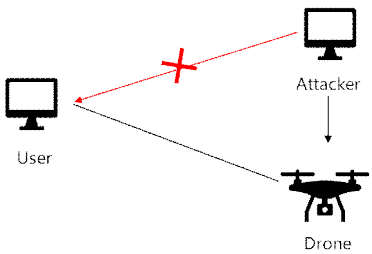

그림 1 드론 하이재킹 시나리오

그림 2는 사용자가 드론에게 보낸 패킷을 캡처한 후 분석하고 있는 과정이며, 이와 같이 패킷을 분석했을 때 사용자가 드론에게 보내는 정보가 읽기 쉽게 표시되어 있어 보안 취약점이 있었다. 이와 같이 패킷을 몰래 보는 것을 패킷 스니핑이라고 한다 [5]. 드론 AP를 반드시 암호화해야할 필요가 있다.

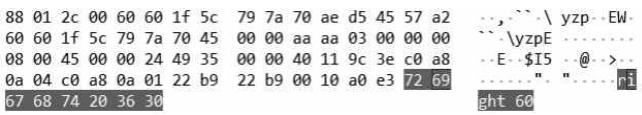

그림 2 노트북에서 드론으로 보낸 패킷 내용

3. 인증해제 공격(Deauthentication Attack)

인증해제 공격이란 공격자가 Source의 MAC을 Station의 MAC으로 위조하여 연속적으로 인증해제 메세지를 보내 Station과 AP의 연결이 끊기게 하는 공격이다 [6]. 인증 해제 공격(Deauth)을 당한 사용자가 드론 AP에 다시 연결을 시도하는 과정에서 발생하는 Handshake를 얻게된다. 만약 드론 AP가 암호 설정을 해놓았다면, 인증 해제 공격을 사용해 Handshake가 포함된 캡처

■ Corresponding Author: Taehoon Kim (thkim@hanbat.ac.kr)

파일을 얻을 수 있다. 실제 생활에서 열쇠와 자물쇠 역할을 하는 Handshake가 포함된 패킷 캡처 파일을 가지고 Brute-Force Attack 또는 Directory Attack 등을 사용하여 AP의 비밀번호를 알아낼 수 있다. 네트워크에 대한 지식이 없는 사용자가 스스로 패킷 스니핑 즉 패킷을 읽을 수 있게 만드는 것을 방지하기엔 어려움이 있다. 이에 좋은 방법은 패킷에 있는 정보를 암호화하여 스니핑을 당하더라도 정보를 읽지 못하게하는 것이다 [4]. 또한 드론과 같은 AP의 WiFi를 복잡성이 있는 비밀번호를 설정하는 것이다. 예를 들어 문자와 숫자의 무작위 조합인 10자리 비밀번호는 숫자로만 이루어진 5자리 비밀번호보다 공격자가 많은 시도를 해야한다. 드론의 통제권을 가져오기 위해선 공격자가 드론이 보내는 에 접속을 해야 하는 과정을 거쳐야 하는데 복잡성이 높은 와이파이 비밀번호를 걸게 되면 공격자는 비밀번호를 Cracking 하는데 대부분의 시간을 소비하게 될 것이다.

4. 결론 및 추후 연구

본 논문에서는 드론 하이재킹을 시도하며 알아낸 다양한 컨트롤 방식들의 장단점을 파악하고, 이를 보완하여 드론의 안전한 운용을 위한 방안을 모색해 보았다. 특히, 컨트롤러에서 드론으로 보내는 패킷을 스니핑 및 인증해제를 통해 드론의 통제권을 가져오는 과정을 분석하여 보안 취약점을 발견하고 대응 방안을 탐색했다. 이를 통해 드론 하이재킹으로 인한 피해를 최소화하고 안전한 드론 운용 환경을 조성하는 데 기여할 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 2024년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음 (2022-0-01068)

참 고 문 헌

[1] 김명수, 유일선, 임강빈, “무인이동체 드론의 취약점분석 및 대응기술 연구 동향,” 정보보호학회지, 30(2), pp. 49-57, 2020

[2] 심준형, 황의천, 손창근, 류연승, “드론 사고 사례와 기술 동향에 따른 안티드론 대응 방안,” 한국산학기술학회 논문지, 24(2), pp. 651-659, 2023

[3] 이재원. (2021). 국가 중요시설 보호를 위한 안티드론 시스템 연구 : 드론테러 방어체계의 개선방안을 중심으로 [석사학위논문, 공주대학교]. http://www.riss.kr/link?id=T15747100

[4] 이규호, 김태현, 김정훈, 방인규, 김태훈. (2023-02-08). 와이파이 기반 드론 네트워크에서 드론 하이재킹 구현에 관한 연구. 한국통신학회 학술대회논문집, 강원.

[5] 홍성혁, 서유정. (2016). 효율적인 Sniffing 공격 대응방안 연구. 융합정보논문지, 6(2), 31-36, http://dx.doi.org/10.22156/CS4SMB.2016.6.2.031

[6] 이규호, 김태현, 방인규, 김태훈. (2023-02-08). 와이파이 네트워크에서 드론 인증 해제 공격 구현에 관한 연구. 한국통신학회 학술대회논문집, 강원.