T.C.
İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

DRONE HACKLEME YÖNTEMLERİ VE GÜVENLİK ANALİZİ

Bengü TACETTİN

DANIŞMAN
Doç. Dr. Muhammed Ali AYDIN

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

İSTANBUL-2022

Bu çalışma, 25.05.2022 tarihinde aşağıdaki jüri tarafından Bilgisayar Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği Programında Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Doç. Dr. Muhammed Ali AYDIN(Danışman)
İstanbul Üniversitesi-Cerrahpaşa
Mühendislik Fakültesi

Doç. Dr. Can EYÜPOĞLU
Milli Savunma Üniversitesi
Hava Harp Okulu

Dr. Öğr. Üyesi Özgür Can TURNA
İstanbul Üniversitesi-Cerrahpaşa
Mühendislik Fakültesi

20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi-Cerrahpaşa'nın abonesi olduğu intihal yazılım programı kullanılarak Lisansüstü Eğitim Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır..

ÖNSÖZ

Çalışma boyunca gösterdiği her türlü destek ve yardımlarından dolayı Doç. Dr. Muhammed Ali AYDIN'a, arkadaşlarıma ve tüm hayatım boyunca yanımda olan AİLEME bu süreçteki destekleri için en içten dileklerim ile teşekkür ediyorum.

Mayıs 2022 Bengü TACETTİN

İÇİNDEKİLER

Sayfa No

ÖNSÖZ ..... **iv**

İÇİNDEKİLER ..... **v**

ŞEKİL LİSTESİ ..... **viii**

TABLO LİSTESİ ..... **x**

SİMGE VE KISALTMA LİSTESİ ..... **xi**

ÖZET ..... **xiv**

SUMMARY ..... **xv**

1. GİRİŞ **1**

2. GENEL KISIMLAR **5**

2.1. İHA SİSTEMLERİ HACKLEME ÖRNEKLERİ 5

2.1.1. Iraklıların ABD'nin Predator İHA Sistemini Hacklediği Örnek 6

2.1.2. İranlıların ABD'nin RQ-170 Sentinel İHA Sistemini Hacklediği Örnek 7

2.1.3. Bilinmeyen Bir Kaynağın İsrail'in Heron 1 İHA Sistemini Hacklediği Örnek 8

2.1.4. ABD ve İngiltere'nin, İsrail ve İran'ın Hava Araçlarını Hacklediği Örnek 9

2.2. DRONE HACKLEME ÖRNEKLERİ 16

2.2.1. GPS Spoofing ile İnsansız Hava Aracı Yakalama ve Kontrol Etme 17

2.2.2. SkyJack 19

2.2.3. Nils Rodday Saldırısı 20

2.2.4. GNU Radyo ve SDR ile Drone Ele Geçirme ve Diğer IoT Cihazları Hackleme 23

2.2.4.1. SDR Metodu 24

2.2.4.2. nRF24L01+ ve Arduino Metodu 24

2.2.5. Drone Ele Geçirme - Çok Boyutlu Saldırı Vektörleri ve Karşı Önlemler 25

2.2.5.1. SDK Kimlik Doğrulama Mekanizması *26*

2.2.5.2. Firmware Analizi 26
2.2.5.3. Radyo Sinyal Analizi 26
2.2.5.4. GPS Spoofing 27
2.2.6. DroneJack 29
2.2.6.1. Aşama 1.1: Algılama 30
2.2.6.2. Aşama 1.2: Drone İzleme 31
2.2.6.3. Aşama 2: Ele Geçirme 32
2.2.6.4. Aşama 3: Saldırı 32
2.2.7. Parrot Bebop Drona Kablosuz Saldırılar 34
2.2.8. Parrot AR.Drone 2 - WiFi Saldırısı 37
2.2.9. Maldrone 38
2.2.10. NRF24L01 Modüllü DeviationTX Evrensel Uzaktan Kumanda 39
2.2.11. Icarus 40
2.2.12. E012 SDR Verici 41
2.2.13. Drone Sızma Testi 42
2.2.14. İnsansız Hava Araçlarının Güvenlik Açıkları ve Karşı Önlemler 44
2.2.15. DroneSploit ile Drone Hackleme 47
2.2.16. DRAT: Güvenlik Açığı Değerlendirmesi için Drone Saldırı Aracı 49
2.3. GÜVENLİK ANALİZİ 50
2.3.1. MAVLink Protokolü Güvenlik Analizi 51
2.3.2. Dinleme Saldırılarına Karşı Önlemler 55
2.3.3. Deauthentication Saldırılarına Karşı Önlemler 56
2.3.4. GPS Spoofing Saldırılarına Karşı Önlemler 57
2.3.5. Portlara Yönelik Saldırılara Karşı Önlemler 59
2.3.6. Ürün Yazılımına Yönelik Saldırılara Karşı Önlemler 59
2.3.7. Dronlara Yönelik Ağ Saldırılarına Karşı Saldırı Tespit Sistemleri 60
2.3.7.1. Kural Tabanlı Saldırı Tespiti 60

2.3.7.2. Anormallik Tabanlı Saldırı Tespiti 60

3. MALZEME VE YÖNTEM 62

3.1. KULLANILACAK ARAÇLAR 62

3.2. SALDIRI YÖNTEMİ 64

3.2.1. Deauthentication Saldırısı 65

3.2.2. Ping Flood Saldırısı 66

3.3. SALDIRI DÜZENEĞİNİN HAZIRLANMASI 67

4. BULGULAR 69

4.1. DEAUTHENTICATION SALDIRISI 69

4.2. PING FLOOD DOS SALDIRISI 75

5. TARTIŞMA VE SONUÇ 78

KAYNAKLAR 80

ŞEKİL LİSTESİ

Sayfa No

Şekil 2.1: General Atomics Predator B [4] **6**
Şekil 2.2: Lockheed Martin RQ-170 Sentinel [6] **7**
Şekil 2.3: RQ-170 Sentinel saldırı görseli [8] **8**
Şekil 2.4: Heron 1 (Shoval) [10] **8**
Şekil 2.5: 28 Ocak 2010'da IAI Heron TP İHA'dan alınan anlık görüntü [12] **9**
Şekil 2.6: 9 Şubat 2010'da yakalanan bir IAI Heron TP'den alınan başka bir görüntü [12] **10**
Şekil 2.7: 26 Nisan 2009'da ele geçirilen bir IAI Heron'a ait anlık görüntü [12]. **11**
Şekil 2.8: IAI Searcher MK III İHA'sına ait anlık görüntü [12]. **11**
Şekil 2.9: Aeronautics şirketi tarafından yapılan bir İHA'ya ait anlık görüntü [12]. **12**
Şekil 2.10: Aeronautics Aerostar Taktik İHA'nın ayak takımına ait anlık görüntü [12]. **12**
Şekil 2.11: 2008'in Ocak ayında İsrail'in F-16 savaş uçağından alınan anlık görüntü [12]. **13**
Şekil 2.12: 11 Mart 2012'de Suriye'nin batısında uçan İran yapımı HESA Ababil III insansız hava aracından alınan anlık görüntü [12]. **13**
Şekil 2.13: Yakalanan şifrelenmiş video sinyalinin spectrum ve video görseli [12] **14**
Şekil 2.14: Yakalanan video sinyalinin şifresi çözülmüş spectrum ve video görseli [12] **14**
Şekil 2.15: Spoofer cihaz ve hedef İHA [17] **17**
Şekil 2.16: SkyJack için örnek saldırı görseli [19] **19**
Şekil 2.17: Aerialtronics Altura Zenith [22] **20**
Şekil 2.18: İHA'nın iletişim şeması [23] **21**
Şekil 2.19: İHA'nın WEP saldırı şeması [23] **21**
Şekil 2.20: İHA'nın Xbee saldırısı [23] **22**
Şekil 2.21: Syma X5C Quadcopter [26] **23**
Şekil 2.22: Ardunio Mega ile yapılan Interceptor [29] **24**
Şekil 2.23: Raspberry Pi ile yapılan Interceptor [29] **25**
Şekil 2.24: DJI Phantom 3 [30] **25**
Şekil 2.25: Kumandaya yanlış resim gösterimi [30] **27**
Şekil 2.26: Sahte GPS noktası oluşturma [30] **28**
Şekil 2.27: Sahte GPS tespit detektör düzeneği [30] **28**
Şekil 2.28: DroneJack mimari [31] **29**
Şekil 2.29: DroneJack Probe mimari [31] **30**
Şekil 2.30: DroneJack web arayüzü [31] **31**

Şekil 2.31: Parrot Bebop Drone [33] **34**
Şekil 2.32: Parrot AR.Drone 2.0 Elite [35] **37**
Şekil 2.33: Maldrone [37] **38**
Şekil 2.34: NRF24L01 harici modülü ve Cheerson mini dronlar [25] **39**
Şekil 2.35: Icarus [40] **40**
Şekil 2.36: E012 SDR verici uygulama görseli [25] **41**
Şekil 2.37: DJI Mavic 2 Zoom [43] **42**
Şekil 2.38: DJI Phantom 4 Pro Drone [45] **44**
Şekil 2.39: Parrot Bebop 2 Drone [46] **44**
Şekil 2.40: DroneSploit konsol ekranı [48] **47**
Şekil 2.41: DroneSploit modül ekranı [48] **48**
Şekil 2.42: DRAT saldırı listesi [49] **49**
Şekil 2.43: DRAT - Kullanıcı mod arayüzü [49] **49**
Şekil 2.44: DRAT - Geliştirici mod arayüzü [49] **50**
Şekil 3.1: Syma X5UW FPV Quadcopter **62**
Şekil 3.2: Syma drone iletişim şeması **64**
Şekil 3.3: Syma drona yapılan deauthentication saldırı şeması **66**
Şekil 3.4: Syma drona yapılan ping flood saldırı şeması **66**
Şekil 3.5: HDMI ile Raspberry Pi bağlantısı **68**
Şekil 4.1: iwconfig komut çıktısı **69**
Şekil 4.2: airmon-ng komut çıktısı **70**
Şekil 4.3: airmon-ng check kill komut çıktısı **70**
Şekil 4.4: airodump-ng komut çıktısı **71**
Şekil 4.5: airodump-ng komut çıktısı - handshake **72**
Şekil 4.6: aireplay-ng komut çıktısı **73**
Şekil 4.7: Saldırıdan önce normal kullanıcı ve saldırganın drona erişimi **73**
Şekil 4.8: Saldırıdan sonra normal kullanıcı ve saldırganın drona erişimi **74**
Şekil 4.9: Syma X5UF ping komutu çıktısı **75**
Şekil 4.10: Syma X5UF hping3 --fast komutu çıktısı **76**
Şekil 4.11: Syma X5UF hping3 --faster komutu çıktısı **76**

TABLO LİSTESİ

Sayfa No

Tablo 1.1: İnsansız hava aracı ve İHA sistemi terimlerinin değerlendirmesi [1] **2**
Tablo 2.1: Ülkeler arasında yaşanan İHA sistemlerine yönelik siber saldırı örnekleri **6**
Tablo 2.2: Kullanılan saldırı yüzeylerine göre drone hackleme örnekleri **16**

SİMGE VE KISALTMA LİSTESİ

Simgeler **Açıklama**

$: Dolar

Kısaltmalar **Açıklama**

AB : Avrupa Birliği
ABD : Amerika Birleşik Devletleri
AES : Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
AP : Access Point (Erişim Noktası)
BSSID : Basic Service Set Identifier (Temel Service Kümesi Tanımlayıcı)
BRUIDS : Behavior Rule Based UAV IDS (Davranış Kuralı Tabanlı İHA Saldırı Tespit Sistemi)
CAA : Civil Aviation Authority (Sivil Havacılık Örgütü)
CBC : Cipher Block Chaining (Şifre Bloğu Zincirleme)
CIA : ABD Merkezi Haberalma Örgütü
CRC : Cyclic Redundancy Check (Döngüsel Artıklık Kontrolü)
DSSS : Direct Sequence Spread Spectrum (Doğrudan Dizi Yayılım Spektrumu)
DUML : DJI Universal Markup Language **(**DJI Evrensel İşaretleme Dili)
ECC : Elliptic Curve Cryptography (Eliptik Eğri Şifreleme)
EASA : European Aviation Safety Agency (Avrupa Havacılık Emniyet Ajansı)
FAA : Federal Aviation Authority (ABD Federal Havacılık İdaresi)
FANET : Flying Adhoc Network (Uçan Adhoc Ağı)
FDMA : Frequency Division Multiple Access (Frekans Bölmeli Çoklu Erişim)
FHSS : Frequency Hopping Spread Spectrum (Frekans Atlamalı Yayılma Spektrumu)
FPV : First Person View (Birinci Şahıs Görünümü)
FTP : File Transfer Protocol (Dosya Aktarım Protokolü)
GCS : Ground Control Station (Yer Kontrol İstasyonu)
GCHQ : Government Communications Headquarters (İngiltere Güvenlik ve İstihbarat Dairesi)
GLONASS : Global Navigation Satellite System (Küresel Uydu Konumlandırma Sistemi)

GNU : GNU's Not Unix (GNU Unix Değildir)

GNSS : Global Navigation Satellite Systems (Küresel Konum Belirleme Sistemi)

GPS : Global Positioning System (Küresel Konumlandırma Sistemi)

GSM : Global System for Mobile Communications (Mobil İletişim için Küresel Sistem)

HDMI : High Definition Multimedia Interface (Yüksek Çözünürlüklü Multimedya Arayüzü)

IAI : Israel Aerospace Industries (İsrail Havacılık Endüstrisi)

ICAO : International Civil Aviation Organisation (Uluslararası Sivil Havacılık Örgütü)

ICMP : Internet Control Message Protocol (İnternet Kontrol Mesaj Protokolü)

IDA : The Interactive Disassembler

IDS : Intrusion Detection System (Saldırı Tespit Sistemi)

IEEE : Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)

IoT : Internet of Things (Nesnelerin İnterneti)

IP : Internet Protocol (İnternet Protokolü)

İHA : İnsansız Hava Aracı

İUS : İnsansız Uçak Sistemi

JBE : Java Bytecode Editor (Java Bayt Kodu Düzenleyicisi)

M : Metre

MS : Milisaniye

MAC : Media Access Control (Medya Erişim Kontrolü)

MAV : Micro Air Vehicle (Mikro Hava Aracı)

MITM : Man In The Middle Attack (Orta Saldırıdaki Adam)

NMA : Navigation Message Authentication (Navigasyon Mesajı Kimlik Doğrulaması)

NSA : National Security Agency (Amerikan Ulusal Güvenlik Ajansı)

RC : Radio Control (Radyo Kontrolü)

RF : Radio Frequency (Radyo Frekansı)

RPA : Remotely Piloted Aircraft (Uzaktan Pilotla Kontrol Edilen Hava Aracı)

RPV : Remotely Piloted Vehicle (Uzaktan Pilotla Kontrol Edilen Araç)

RSSI : Received Strength Signal Indicator (Alınan Güç Sinyali Göstergesi)

SAE : Simultaneous Authentication of Equals (Eşit Eş zamanlı Kimlik Doğrulama)

SDK : Software Development Kit (Yazılım Geliştirme Kiti)

SDR : Software Defined Radio (Yazılım Tanımlı Radyo)

SHGM : Sivil Havacılık Genel Müdürlüğü

SİHA : Silahlı İnsansız Hava Aracı

SPI : Serial Peripheral Interface (Seri Çevre Birimi Arayüzü)

SSH : Secure Shell (Güvenli Kabuk)

SSID : Service Set Identifier (Hizmet Kümesi Tanımlayıcı)

SSM : Savunma Sanayii Müsteşarlığı

SoC : A System on A Chip (Çip Üzerinde Sistem)

SVM : Support Vector Machine (Destek Vektör Makinesi)

TPPA : Traceable and Privacy-Preserving Authentication (İzlenebilir ve Gizliliği Koruyan Kimlik Doğrulama)

TUAS : Tactical Unmanned Aircraft System

UA : Unmanned Aircraft (İnsansız Hava Aracı)

UAS : Unmanned Aircraft System (İnsansız Hava Aracı Sistemi)

UAV : Unmanned Aerial Vehicle (İnsansız Hava Aracı)

UBI : Unsorted Block Images (Sıralanmamış Blok Resimleri)

UHF : Ultra High Frequency (Ultra Yüksek Frekans)

USB : Universal Serial Bus (Evrensel Seri Veri Yolu)

WEP : Wired Equivalent Privacy (Kabloluya Eşdeğer Gizlilik)

WiFi : Wireless Fidelity (Kablosuz Bağlantı Alanı)

DRAT : Drone Attack Tool (Drone Saldırı Aracı)

DK : Dakika

GHz : Gigahertz

ÖZET

YÜKSEK LİSANS TEZİ

DRONE HACKLEME YÖNTEMLERİ VE GÜVENLİK ANALİZİ

Bengü TACETTİN

İstanbul Üniversitesi-Cerrahpaşa

Lisansüstü Eğitim Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman : Doç. Dr. Muhammed Ali AYDIN

İnsansız hava araçları (İHA), sivil ve askeri alanda oluşturduğu etkiler ile önemli bir aktör olmuştur. İHA'lar, ülkelerin savaş stratejilerinde belirleyici rol oynarken, ticari ve hobi amaçlı kullanıldığı alanlarda sağladığı avantajlar ile etki alanlarını geliştirmekte ve genişletmektedir. Ancak İHA'ların artan kullanımı, beraberinde getirdiği güvenlik zafiyetleri dolayısıyla, onların etkili oldukları alanda kullanımını olumsuz etkilemektedir. Bu tezin amacı, farklı amaçlar ile insansız hava araçlarının hacklenebileceğini göstermektir. Bu çalışmada sivil ve askeri alandaki drone ve İHA sistemleri hackleme yöntemleri incelendi. Dahası sivil alanda kullanılan dronların güvenlik analizi yapıldı. Örnek çalışma için Syma drone hackleme uygulamalı olarak gösterildi.

Mayıs 2022, 104. sayfa.

Anahtar kelimeler: Drone, İnsansız Hava Aracı, İHA, İHA Sistemleri, Drone Hackleme, Drone Güvenliği

SUMMARY

M.Sc. THESIS

DRONE HACKING METHODS AND SECURITY ANALYSIS

Bengü TACETTİN

Istanbul University-Cerrahpasa
Institute of Graduate Studies
Department of Computer Engineering

Supervisor : Assoc. Prof. Dr. Muhammed Ali AYDIN

Unmanned aerial vehicles (UAVs) have become an important actor with the effects they have created in the civil and military fields. While UAVs play a decisive role in the war strategies of countries, they develop and expand their areas of influence with the advantages they provide in areas where they are used for commercial and hobby purposes. However, the increasing use of UAVs negatively affects their use in the area where they are effective due to the vulnerabilities it brings. The aim of this thesis is to show that unmanned aerial vehicles can be hacked for different purposes. In this study, hacking methods of drone and UAV systems in civil and military fields were examined. Moreover, the security analysis of drones used in civilian areas was made. For the case study, Syma drone hacking was demonstrated in practice.

May 2022, 104 pages.

Keywords: Drone, Unmanned Aerial Vehicle, UAV, UAS, Drone Hacking, Drone Security

1. GİRİŞ

Geliştirildiği ilk yıllardan itibaren ağırlıklı olarak askeri amaçlı kullanılan İnsansız Hava Araçları (İHA'lar), mühimmat taşıma, düşman kontrolü, düşman tespiti, sınır kontrolü gibi konularda faydalanılan en önemli araçlardan birisi olmuştur. Günümüzde ise insansız hava araçlarının kapsamı ve kullanımı, sadece askeri alanda sınırlı kalmayıp sivil alanda çeşitli sektörlerde yer almaktadır. İHA'lar; kamu, altyapı, güvenlik, ulaşım, arama-kurtarma, medya, sigortacılık ve telekom sektörlerinde kullanılmaktadır. Sivil ve askeri alanda kullanılan İHA'lar, kontrol sistemleri, hız, menzil ve ağırlık bakımından farklılık göstermektedir. Bu farklılıklar sonucunda ise uzaktan kontrol edilen insansız hava sistemleri Türkiye'de ve dünyada; drone, İnsansız Hava Aracı (Unmanned Aerial Vehicle - UAV), İnsansız Uçak, İnsansız Uçak Sistemi (İUS), Otonom Hava Aracı, Uzaktan Pilotlu Araç (Remotely Piloted Vehicle - RPV), Uzaktan Pilotla Kontrol Edilen Hava Aracı (Remotely Piloted Aircraft - RPA) gibi farklı terimler ile adlandırılmaktadır [1]. Bu konuya açıklık getirmek için dünyada; Uluslararası Sivil Havacılık Örgütü (ICAO), Avrupa Birliği (AB)'nin sivil havacılık kuruluşu EASA, Amerika Birleşik Devletleri (ABD)'nin Sivil Havacılık Otoritesi FAA, İngiltere Sivil Havacılık Örgütü CAA bünyesinde, Türkiye'de ise; Sivil Havacılık Genel Müdürlüğü (SHGM) ve Savunma Sanayii Müsteşarlığı (SSM) bünyesinde terminoloji çalışmaları düzenlenmiştir [1].

Karaağaç [1] tarafından hazırlanan araştırma raporunda, Türkiye'de ve dünyadaki İHA terminolojisinin detaylı incelemesi yapılmıştır. İlgili raporda, İngiltere'yi ziyaret eden ABD Deniz Kuvvetlerinin, İngilizlerin Queen Bee'sinden (Kraliçe Arı) esinlenerek yeni başlattıkları hedef uçak projesinin ismine drone (erkek arı) terimini seçmesi ile drone kelimesinin kullanılmaya başlandığı belirtilmiştir. Sonrasında drone terimi uzun bir süre yaygın olarak kullanılmıştır. Bu terim zamanla hem hedef uçakların hem de diğer istihbarat maksatlı İHA'ların genel adı olarak kullanılmaya başlamıştır. 1990'lı yıllarda askeri İHA sektöründe büyük bir hareketlilik yaşanmış ve bu dönemde drone yerine önce Uzaktan Pilotla Kontrol Edilen Araç (RPV) terimi, daha sonra da İnsansız Hava Aracı (İHA) terimi tercih edilmiştir. 2010 yılına yaklaşırken, İHA sadece uçan platformu ifade ettiği ve uçuş için platforma ilave olarak en azından bir kontrol istasyonuna ve bir veri bağlantısına ihtiyacı olduğu için, İHA Sistemi (Unmanned Aircraft System-UAS) terimi yaygınlaşmaya başlamıştır. Bununla birlikte uçan platformun adı olarak, İHA sisteminin bir alt unsuru olan İnsansız Hava Aracı (Unmanned Aircraft-UA) terimi kullanılmaya devam edilmiştir. Uluslararası Sivil Havacılık Örgütü

(ICAO)'nün 2011 yılında yayınladığı Circular 328 adlı dokümanda önemli bir kısıtlamaya gidilmiş, insan kontrolünde olmadan görev yapabilen (tam otonom) İHA sistemleri kapsam dışı bırakılmış ve Uzaktan Pilotla Kontrol Edilen Hava Aracı (RPA) terimi literatüre girmiştir. Bu değişiklik sonrasında Uzaktan Pilotla Kontrol Edilen Hava Aracı (RPA) ifadesi, hem sivil hem de askeri İHA sektöründe kabul görmeye başlamıştır. ABD'nin 2010'lu yıllarda başta Afganistan, Irak, Pakistan, Somali ve Yemen olmak üzere birçok ülkede İHA'lar ile gerçekleştirdiği silahlı saldırılar, bu saldırılarda zarar gören siviller sebebiyle dünya medyasının ve uluslararası kamuoyunun dikkatini çekmiştir. Bu saldırılarda kullanılan sistemler drone olarak adlandırılmıştır. Zaman içinde drone terimi, silahlı İHA saldırılarıyla özdeşleşerek olumsuz bir algı oluşturmaya başlamıştır. Ek olarak, Amatör Havacılar veya Yeni Nesil Havacılar olarak adlandırılabilecek kişilerin oluşturduğu yeni havacılık alt sektöründe büyük oranda çok rotorlu (multicopter) İHA sistemleri tercih edilmekte ve bu sistemler için genellikle drone terimi kullanılmaktadır. Türkiye'de de benzer bir durum vardır. Hem ulusal medya hem de kamuoyu çoğunlukla drone kelimesini kullanmaktadır.

Karaağaç [1] tarafından hazırlanan araştırma raporunda, dünya genelinde profesyonel havacılık sektöründe yaygın bir şekilde kullanılan İnsansız Hava Aracı ve İHA sistemi terimlerinin değerlendirmesi Tablo 1.1'de gösterilmiştir. İlgili tabloda hava araçlarının bir alt kategorisinde listelenen İHA'lar, artan kullanım amaçları doğrultusunda sistem unsurları, tipleri, kalkış ve iniş yöntemleri gibi kategorilere ayrılmaktadır. İnsansız hava aracı ve İHA sistemi terimlerinin değerlendirmesi Tablo 1.1'de gösterilmiştir.

Tablo 1.1: İnsansız hava aracı ve İHA sistemi terimlerinin değerlendirmesi [1]

Terminoloji Tarihçesi	Hava Aracı Alt Kategorileri	İHA Sisteminin Unsurları	Gövde/Motor Tasarımına Göre İHA Türleri	Kalkış Yöntemine Göre İHA Türleri	İniş/Kurtarma Yöntemine Göre İHA Türleri	İHA Kategorileri	İHA Uygulamaları
Uzaktan Pilotla Kontrol Edilen Araç	İnsansız Hava Aracı	İnsansız Hava Aracı	Sabit Kanat (Uçak)	Pistten Kalkış	Pistte İniş	Mikro	Askeri
İnsansız Hava Aracı	Uzaktan Pilotla Kontrol Edilen Hava Aracı	Faydalı Yükler	Döner Kanat (Helikopter)	Dikey Kalkış	Dikey İniş	Mini	Sivil
Uzaktan Pilotla Kontrol Edilen Hava Aracı	Otonom Hava Aracı	Haberleşme Unsuru	Çok Rotorlu (Multikopter)	Basınç Değişimi	Basınç Değişimi	Küçük	Ticari
Drone		Komuta Kontrol Unsuru	Havadan Hafif (Balon)	Elle Atma	Gövde Üzerine İniş	Taktik	Eğlence (Hobi)
		Destek Unsuru	Motorlu Parafoil	Fırlatma Rampasıyla Atma	Paraşütle İniş	MALE	
			Çırpan Kanat	Tüpten Atma	Sistemle Yakalama	HALE	
			Eğilen Motor			Saldırı Muharebe	
			Eğilen Kanat				
			Hibrit				

Büyük Oranda Karşılıyor
Kısmen Karşılıyor
Büyük Oranda Karşılamıyor

Tablo 1.1'de görüldüğü üzere İHA uygulamaları askeri, sivil, ticari ve eğlence olmak üzere 4 alt kategoriye ayrılmıştır. Raporda, Türkiye'de ve dünyada, askeri İHA uygulamalara yönelik sektörde, çoğunlukla İnsansız Hava Aracı (İHA) ve İHA sistemi terimleri kullanıldığı ifade edilmiştir. Sivil, ticari ve eğlence alanındaki İHA'lar için ise "Drone" teriminin kullanıldığı belirtilmiştir. Drone teriminin "dron", "dıron", "duron" gibi farklı yazım şekilleri de görülebilmektedir. Bu değerlendirmeler dikkate alınarak tez kapsamında, sivil alandaki anlatımlarda "Drone" (Türkçe kullanımında "dron") terimi, askeri alandaki anlatımlarda "İHA Sistemleri" terimi kullanılmıştır.

Drone endüstrisi pek çok sektörde faaliyet alanlarını genişleterek hızla büyümektedir. Drone üreticisi firmalar da, kullanıcı taleplerine göre yeni özellikler geliştirerek dronları daha gelişmiş, daha kullanışlı ve daha güvenli olması için çalışmaktadır. Ancak drone firmaları tüm bu geliştirme sürecinde drone güvenliğini göz ardı edebiliyor veya aldığı tedbirler önleyici olmayabiliyor. Diğer taraftan güvenlik, belirli sektörler için çok önemli olsa da, tüm drone kullanıcıları için her zaman çok önemli değildir. Drone hacking örnekleri literatürde sıkça yer alsa da drone kullanıcıları çoğunlukla kullandıkları dronun mevcut güvenlik açıklarından ve olası etkilerinden haberdar değildir. McNabb [2], DroneLife ekibi tarafından drone pilotlarına drone platformlarındaki veri güvenliği ile ilgili soru sorduğu bir anket paylaşmıştır. Bu ankette sadece tek bir soru sorulmuştur: "Drone platformunuzdaki veri güvenliği konusunda ne kadar endişelisiniz?" McNabb [2] tarafından paylaşılan anket sonuçlarında verilen cevaplar;

- Önemli değil: %41,2
- Biraz önemli: %29,4
- Öncelikli endişem: %17,6
- Ne demek istediğinden emin değilim: %11,8

Anket sonucuna göre ticari drone pilotlarının yarıdan fazlası veri güvenliğini birincil bir endişe olarak görmemiştir. Bu mini anket sonucu, sivil alandaki tüm drone pilotlarını kapsamasa bile drone hackleme örneklerinde etkilenecek taraflardan biri olan pilotların farkındalığına örnek olabilir.

Tezin amacı, farklı amaçlar ile insansız hava araçlarının hacklenebileceğinin gösterilmesi ve bu alanda incelenen örnekler ile drone ve İHA sistemleri güvenliği hakkında farkındalığı artırmaktır. Çalışmanın genel kısımlar bölümünde sivil ve askeri alanda, literatürde yer alan drone / İHA sistemleri hackleme örneklerine yer verilmiştir. Askeri alanda örnekler içermesine rağmen bu çalışmanın yoğunlaştığı konu ise, ticari ve eğlence amaçlı kullanılan drone

hackleme örnekleri olmuştur. Drone hackleme örnekleri detaylı bir şekilde anlatılmıştır. Kullanılan metotlar ve teknikler incelenmiştir. Güvenlik analizi bölümünde incelenen saldırı yöntemleri dikkate alınarak dronlara yönelik siber saldırılara karşı alınacak önlemlere yer verilmiştir.

Malzeme ve yöntemler bölümünde, ilk olarak kullanılacak donanımlar ve yazılımlar listelenmiştir. Sonrasında çalışmanın metodolojisi anlatılmıştır. Daha sonra, bulgular bölümünde drone hackleme yöntemleri uygulanmış ve detaylı bir şekilde anlatılmıştır. Son olarak, tartışma ve sonuç bölümünde çalışmanın değerlendirilmesi yapılmış ve gelecek çalışmalar için önerilerde bulunulmuştur.

2. GENEL KISIMLAR

2.1. İHA SİSTEMLERİ HACKLEME ÖRNEKLERİ

İnsansız hava araçları, askeri alanda keşif, gözlem ve saldırı amaçlı kullanılan uçaklardır. Zorlu şartlarda etkili olabilme, yüksek irtifa, uzun süre havada kalabilme, düşük radar izi sayesinde düşman unsurlar tarafında zor tespit edilmektedir. İnsana bağlı yorgunluk, çalışma saati sınırı vb. olumsuz şartları barındırmaması, diğer savaş araçlarına göre daha düşük maliyetli olması gibi avantajları sebebi ile ülkelerin sınır ötesi operasyonlarında sıkça kullanılmaktadır.

Operasyonlarda etki ve stratejik üstünlük sağlamada önemli bir yeri olan İHA sistemleri, devletler arasında da rekabete yol açmıştır. Savaş alanında üstünlük elde etme yarışı, gelişmiş İHA ve SİHA sistemlerinin üretimini artırmıştır. Kapsama ve kullanım alanındaki bu artış, düşman unsurları tarafından tehdit olarak algılanmış ve hedef haline getirilmiştir. Bunun sonucunda ise İHA Sistemleri, günümüzde hem fiziksel hem de siber alanda saldırıya maruz kalmaktadır. Karaağaç [3] hazırladığı "İHA Sistemleri Yol Haritası" makalesinde, geleceğin muhtemel konvansiyonel savaşları için yetersiz olan mevcut insansız hava araçlarının, belirli bir seviyenin üstünde savunma gücüne sahip ülkeler tarafından kolayca etkisiz hale getirilebileceğine dikkat çekilmiştir.

Başta Türk İHA/SİHA sistemleri olmak üzere, İHA sistemlerinin kullanıldığı Suriye, Irak, Yemen, Libya, Azerbaycan ve Ukrayna'daki çatışma bölgelerinde taraflara sağladığı üstünlük sonucunda uluslararası alanda tüm dikkatleri üzerine çekmiştir. Savaş stratejilerini belirlemede etkisi, onları hedef haline getirmektedir. İHA Sistemleri, fiziksel saldırıların hedefi olduğu kadar siber saldırıların da hedefi olmaktadır. Siber saldırılar, bu sistemlerde tahribat gücü yüksek yaralanma ve ölümlere sebep olabilir. Bunun dışında, casusluk veya ticari amaçlar ile yapılan siber saldırılar sonucunda stratejik öneme sahip bilgi ve teknolojik kayıplara neden olabilir. Yakın geçmişte yaşanan İHA sistemlerine yönelik bilinen siber saldırı örneklerine Tablo 2.1'de yer verilmiştir.

Tablo 2.1: Ülkeler arasında yaşanan İHA sistemlerine yönelik siber saldırı örnekleri

SALDIRAN TARAF	ETKİLENEN TARAF	TARİH	ETKİLENEN İHA SİSTEMİ	KAYNAK
Irak	ABD	2009	General Atomics - Predator	[5]
İran	ABD	2011	Lockheed Martin - RQ-170 Sentinel	[7]
Bilinmiyor	İsrail	2013	Israel Aerospace Industries - Heron (Shoval)	[11]
ABD İngiltere	İsrail	1998 - …	Israel Aerospace Industries - Heron Israel Aerospace Industries - Heron TP Israel Aerospace Industries - Searcher MK III Aeronautics - Aerostar Tactical UAS (TUAS)	[12]
	İran	1998 - …	HESA - Ababil III *(Suriye'ye ait)*	[12, 14]

2.1.1. Iraklıların ABD'nin Predator İHA Sistemini Hacklediği Örnek



Şekil 2.1: General Atomics Predator B [4]

Bu olayların ilk örneği olarak, ABD'nin CIA tarafından kullanılan Predator'lerine düzenlenen saldırılar verilebilir. 2009 yılında, Iraklı Şii direnişçilerin, 26 dolarlık bilgisayar programını kullanarak ABD'nin Predator insansız hava araçlarını hacklediği iddia edilmiştir. [5]'de yer alan habere göre, Amerikan askerlerinin direnişçilerden ele geçirdikleri dizüstü bilgisayar sistemlerinde, keşif için kullanılan ve üsse görüntüler yollayan Predator uçaklarının video kayıtlarına rastlanmıştır. Iraklı direnişçiler, Rus yazılımı olan SkyGrabber yardımıyla, Predator

uçaklarının video kayıtlarını uydudan gelen veri akışlarını yakalayıp kayıt etmeyi başarmıştır. Hedef Predator modellerinden biri örnek görsel olarak Şekil 2.1'de paylaşılmıştır.

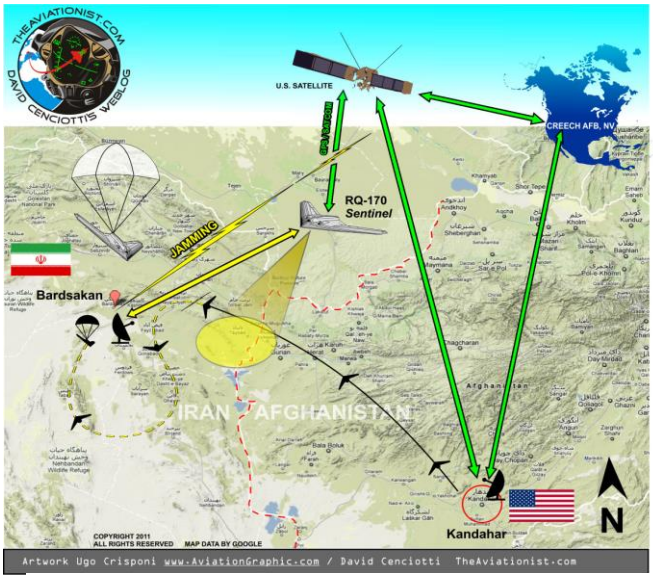
Dizüstü sistemlerdeki görüntüler 2008 yılının Aralık ayı kayıtlarına kadar uzanmaktadır. Bu da direnişçilerinin uzun zamandır bu bilgilere ulaşabildiğini göstermektedir. İlginç olan tarafı, Amerikan Hükümeti'nin bu tür güvenlik açıklarından haberdar olmasıdır. Hatta yeni insansız uçaklar olan ve Predator'un yerini alacak olan Reaper modellerde de benzer bir durum söz konusu olduğu iddia edilmiştir. Video verileri, üsse herhangi bir şifreleme işlemine tabi tutulmadan yollanmaktadır. Bu durum, teknolojiyi bilen kişilerin verilere rahatlıkla ulaşabildiğini gösterir.

2.1.2. İranlıların ABD'nin RQ-170 Sentinel İHA Sistemini Hacklediği Örnek



Şekil 2.2: Lockheed Martin RQ-170 Sentinel [6]

Siber casusluk boyutundaki diğer bir olay ABD - İran arasında gerçekleşmiştir. Yaşanan olayda ise saldırı, Iraklı direnişçilerin yaptığı gibi izinsiz erişim değil, doğrudan hackleme olduğu iddia edilmiştir. [7]'de yer alan haberde, 2011 yılında, İran'ın, CIA tarafından kullanılan RQ170 insansız hava aracını (Şekil 2.2) GPS spoofing yaparak ele geçirmiştir. İranlı mühendis, zayıf bulunan GPS navigasyonuna müdahale edebildiğini söylemiştir. İranlı uzmanların, RQ-170 Sentinel'in en zayıf noktasının, GPS'de olduğunu, daha önce düşmüş Amerikan İHA'larını Eylül ayında inceleyerek anladığı bildirilmiştir. Bu bilgiyi kullanarak, ülkede keşif işi yapan uçaklardan birine tuzak kuran İranlı mühendis, gürültü (jamming) yayarak İHA'yı otopilota geçmeye zorlamıştır. Daha sonra ekibi ile İHA'yı basitçe kendi istedikleri yere indirmek üzere programlamıştır. Ekipte yer alan mühendis tarafından, tüm sürecin bir Google hesabına girmek kadar kolay olduğu iddia edilmiştir.



Şekil 2.3: RQ-170 Sentinel saldırı görseli [8]

Saldırganın, gözetleme aracına sahte GPS sinyalleri göndererek Afganistan'daki ABD üssüne gidiyor gibi gösterip, İran'a getirildiği söylenmiştir. Habere göre saldırı başarılı olarak sonuçlanmıştır. Sentinel Afganistan'daki ana üs yerine İran'a inmiştir. RQ-170 Sentinel saldırısını anlatan görsel Şekil 2.3'de verilmiştir. Daha önce kaybedildiği söylenen İHA için daha sonra Obama resmi olarak insansız hava aracının geri iade edilmesini istemiştir. [9]'da yer alan haberde, 2016 yılında ise İran'ın 2011 yılında düşürdüğünü iddia ettiği RQ-170 insansız gözlem aracının kopyası olduğu söylenen "Saegheh" (Thunderbolt) isimli yeni insansız hava aracı tanıtılmıştır.

2.1.3. Bilinmeyen Bir Kaynağın İsrail'in Heron 1 İHA Sistemini Hacklediği Örnek

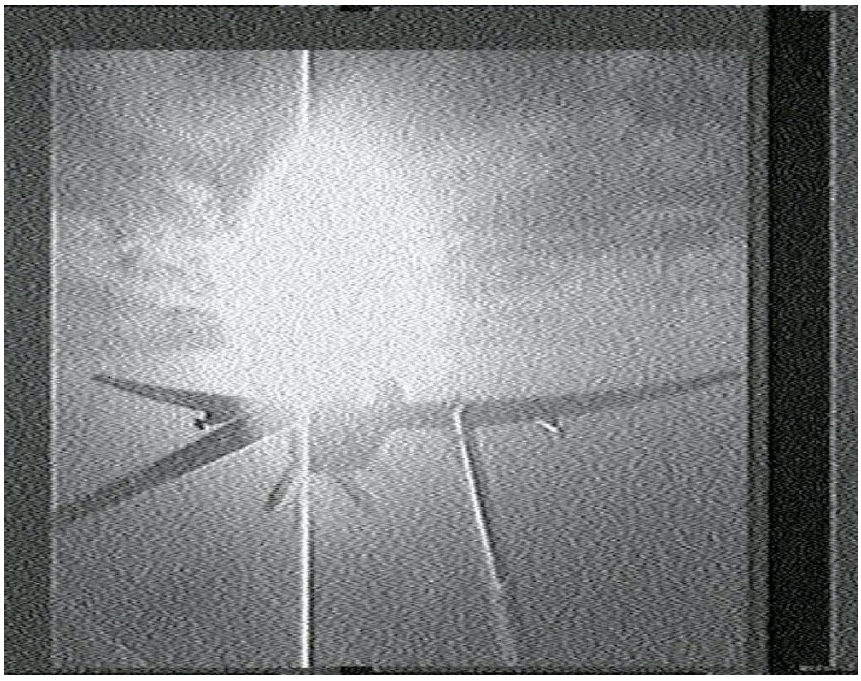


Şekil 2.4: Heron 1 (Shoval) [10]

[11]'de aktarıldığı üzere, İHA'sına saldırı yaşayan bir diğer ülke ise İsrail'dir. Bu örnekte İsrail, ABD - Irak ve ABD - İran arasında yaşanan diğer olaylarda olduğu gibi kaynak tespiti yapamamıştır. Bunun sonucunda, 2013 yılında bilinmeyen bir düşman unsuru tarafından ele geçirildiği düşünülen Şekil 2.4'de Shoval (Heron) isimli insansız hava aracını imha etmiştir. Saldırganların muhtemelen Taliban ya da Kuzey Afganistan'da faaliyet gösteren isyancı güçler olduğu düşünülmüştür.

2.1.4. ABD ve İngiltere'nin, İsrail ve İran'ın Hava Araçlarını Hacklediği Örnek

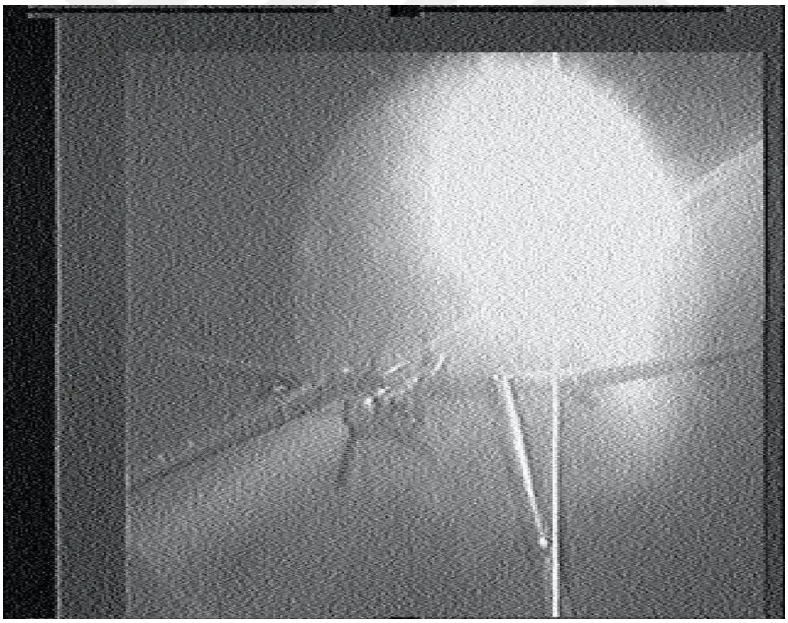
2016 yılında Amerikan internet sitesi "Intercept" ile İsrail gazetesi "Yedioth Ahronot" tarafından yayınlanan haberde, İsrail'in devletler düzeyinde casusluk olayı yaşadığı iddia edilmiştir. İngiliz GCHQ casusları ve Amerikan NSA casusları, Akdeniz'in Kıbrıs Adası'ndaki bir dağın tepesindeki dinleme noktasından 1998'den beri yürütülen "Anarşist" kod adlı gizli bir programın parçası olarak İsrail insansız hava araçları ve savaş uçaklarından canlı video toplamıştır. Currier ve Moltke [12] tarafından ele geçirilen görüntüler paylaşılmıştır. Eski NSA çalışanı Edward Snowden tarafından sağlanan dosyalar arasında, İsrail insansız hava aracı filosunu videolarından bir dizi "anlık görüntü" yer alıyor. Burada sunulan görüntüler, füze taşıyan İsrail dronlarının halka açık nadir görüntüleri de dahil olmak üzere, birkaç farklı insansız uçak türünü göstermektedir.



Şekil 2.5: 28 Ocak 2010'da IAI Heron TP İHA'dan alınan anlık görüntü [12]

28 Ocak 2010’da, Kıbrıs’daki GCHQ analistleri, devlete ait İsrail Havacılık ve Uzay Sanayii (IAI) tarafından üretilen dev bir insansız hava aracı olan Heron TP gibi görünen İHA’dan altı dakikalık bir video yakalamıştır. Şekil 2.5’de Heron TP olduğu tahmin edilen İHA’dan alınan anlık görüntü paylaşılmıştır. Video, TP’nin sağ arka dikey sabitleyicisinden çekilmiştir. Videodan alınan bu anlık görüntüde, sol tarafta füze şeklindeki büyük bir nesne açıkça görülmektedir. Bir GCHQ raporunda, 2009’da "silah taşıyan düzenli Heron TP koleksiyonlarından" bahsedilmektedir.

The Intercept tarafından danışılan drone uzmanları, görüntünün Heron TP gösterdiğini doğrulamıştır. Aviation Week editörü Bill Sweetman, "Füze şeklindeki nesneler kesinlikle silah gibi görünüyor" diyerek füzeyi doğrulamıştır. Ek olarak Sweetman, Heron-TP’nin bir İsrail stratejik istihbarat sistemi olması nedeniyle, nesnelerin İHA sinyalleri yörüngede ve havada uçuşurken İran’ın hava savunmasından bir yanıt vermeye zorlamak için kullanılan tuzaklar olabileceğini belirtmiştir.



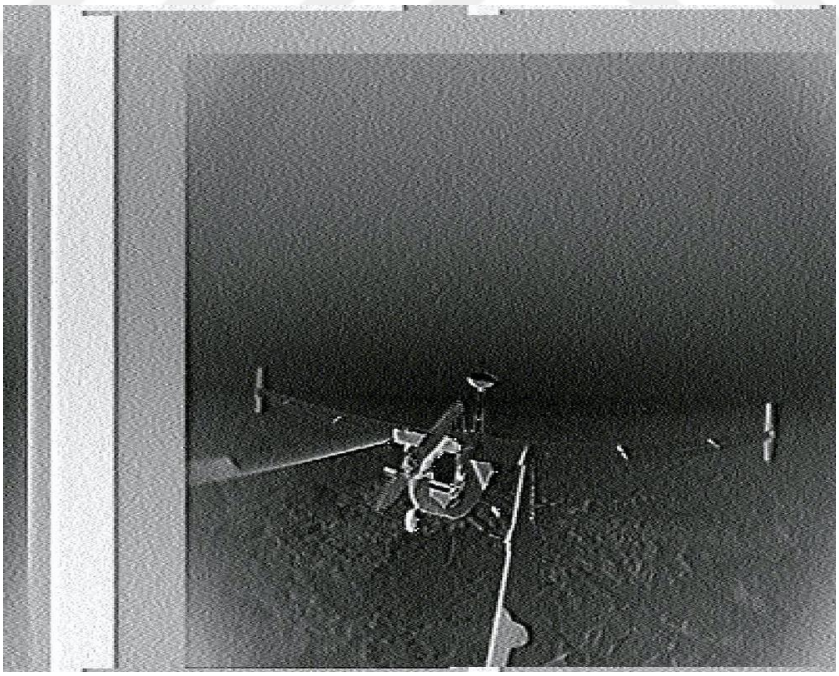
Şekil 2.6: 9 Şubat 2010’da yakalanan bir IAI Heron TP’den alınan başka bir görüntü [12]

Şekil 2.6’da, 9 Şubat 2010’da yakalanan bir Heron TP’den alınan başka bir görüntüye yer verilmiştir. Heron TP veya Eitan ("güçlü" veya "sabit" anlamına gelir) 85 fit kanat açıklığına sahiptir, 1 ton yük taşıyabilir ve 36 saate kadar havada kalabilir. Basında "İran’a ulaşabilen İHA" olarak nitelendirilmektedir. Görüntü bulanık olsa bile kanatların altında füzelerin yer aldığından bahsedilmiş. GCHQ dosyasında, sinyalin daha fazla "işlenemeyecek kadar zayıf" olduğu belirtilmiştir [12].



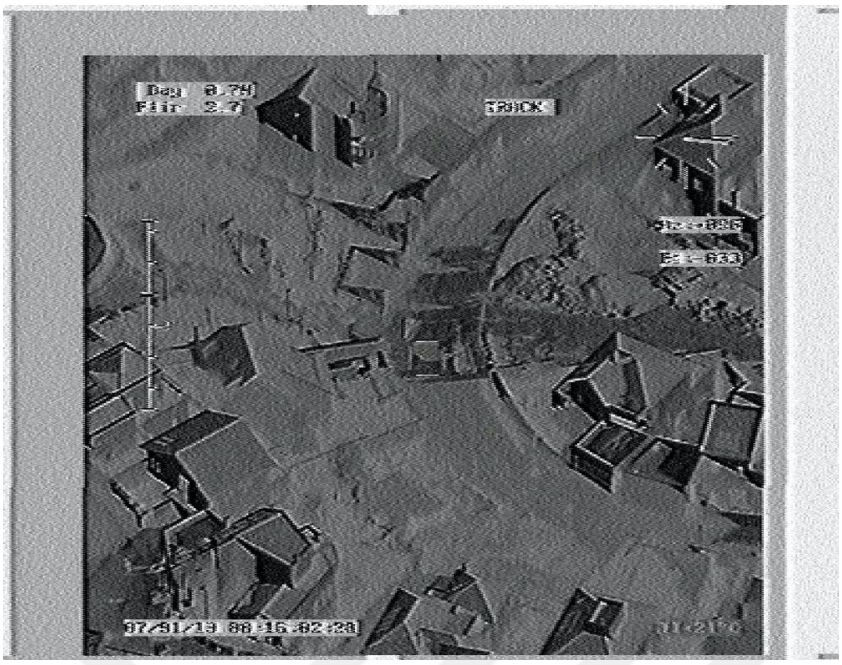
Şekil 2.7: 26 Nisan 2009'da ele geçirilen bir IAI Heron'a ait anlık görüntü [12].

Şekil 2.7'deki görüntü için Sweetman, "Bu, uydu iletişim anten kaportasının şekliyle tanınabilen standart IAI Heron'dur" demiştir [12].



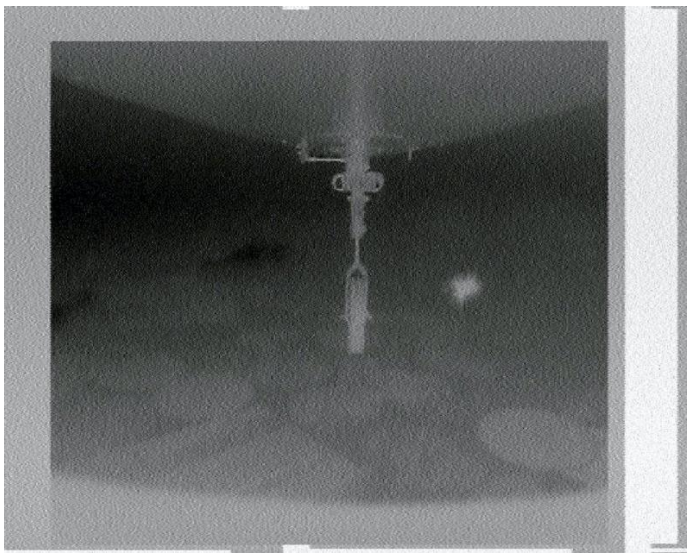
Şekil 2.8: IAI Searcher MK III İHA'sına ait anlık görüntü [12].

Şekil 2.8'de, Sweetman'a göre IAI Searcher MK III olan İHA'ya ait anlık görüntü paylaşılmıştır. Searcher 1980'lerde geliştirilmiş, ancak hala İsrail Savunma Kuvvetleri ve bir dizi başka ülke tarafından kullanılmaktadır [12].



Şekil 2.9: Aeronautics şirketi tarafından yapılan bir İHA'ya ait anlık görüntü [12].

Şekil 2.9'da yer alan görüntü 7 Ocak 2010 sabahı erken saatlerde ele geçirilmiştir. Ekrandaki işaretlere göre, sağ üst köşedeki kadran gibi, Aeronautics şirketi tarafından yayınlanan ürün videolarında benzer bir görünüm yakalandığı için görüntünün Aeronautics şirketi tarafından yapılan bir İHA'dan olduğu düşünülmektedir. 2010 tarihli bir GCHQ belgesinde, Kıbrıs'daki analistlerin, 2000 yılından beri İsrail ordusu tarafından kullanılan ve Polonya'dan Tayland'a kadar ülkelere satılan orta büyüklükte bir İHA olan Aeronautics'in Aerostar Tactical'inden sinyaller topladığı bildirilmiştir [12].



Şekil 2.10: Aeronautics Aerostar Taktik İHA'nın ayak takımına ait anlık görüntü [12].

Şekil 2.10'daki görüntünün Sweetman tarafından Aerostar Taktik İHA'nın ayak takımına ait olduğu öne sürülmüştür [12].



Şekil 2.11: 2008'in Ocak ayında İsrail'in F-16 savaş uçağından alınan anlık görüntü [12].

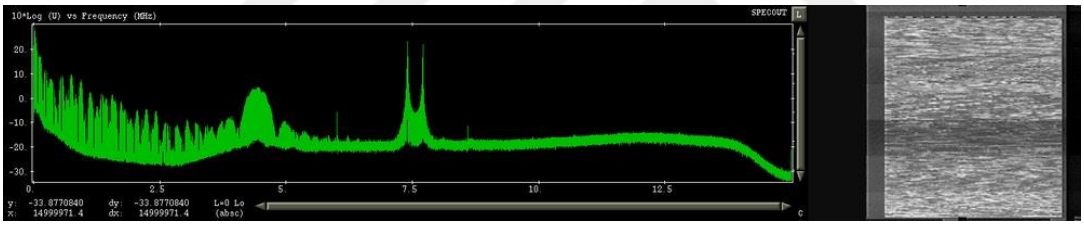
The Intercept tarafından sadece İsrail'in, İHA'ları dışında savaş uçaklarının da hedef olarak izlendiği iddia edilmiştir. Şekil 2.11'de, NSA'in 2008'in Mart ayında yayınlanan gizli raporunda [13], 3 Ocak 2018'de Filistin'in Gazze şehrinde faaliyet gösteren İsrail'in F-16 savaş uçağının kokpitinden alınan 14 saniyelik videodan anlık görüntü verilmiştir. Bu görüntü, İngiltere'deki ABD ve İngiltere'nin müşterek dinleme ve istihbarat merkezi olan Menwith Hill'deki uydu gözetleme sistemlerinin operatörleri tarafından yakalanmıştır [12].



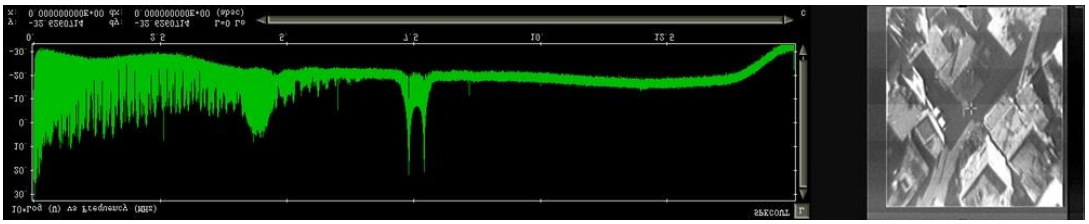
Şekil 2.12: 11 Mart 2012'de Suriye'nin batısında uçan İran yapımı HESA Ababil III insansız hava aracından alınan anlık görüntü [12].

Şekil 2.12'de NSA'in çok gizli powerpoint sunumunda [14] yer alan Suriye'nin batısında uçan İran yapımı HESA Ababil III insansız hava aracından alınan videodan kaydedilen anlık görüntü paylaşılmıştır. Görüntü Anarşist programı analistleri tarafından 11 Mart 2012'de yakalanmıştır. Ele geçirilen GCHQ belgelerinde, adı açıklanmayan yetkililerin ifadelerine ve yerdeki görgü tanıkları tarafından çekilen videolara dayanılarak Suriye Devlet Başkanı Beşar Esad'ın ordusu tarafından işletilen İran yapımı İHA olduğu rapor edilmiş [12].

The Intercept [15] tarafından paylaşılan bir diğer ele geçiriliş dosyada, Anarşist programı analistleri tarafından şifrelenmiş video kayıtlarının kodunun nasıl çözüldüğünü açıklayan eğitim kılavuzu yayınlanmış. Video karelerinin şifresini çözmek ve daha fazla işlemek için AntiSky ve ImageMagick gibi herkese açık, açık kaynaklı araçlar kullanılmış. Kılavuzda, görüntüleri neredeyse gerçek zamanlı olarak çözmek için gereken bilgi işlem gücünün önemli olduğu ancak görüntü içeriğini belirlemek için çok fazla çaba harcamadan tek tek kareleri çözmenin hala mümkün olduğu vurgulanmış [12]. Şekil 2.13 ve Şekil 2.14'de kılavuzdan görseller paylaşılmıştır.



Şekil 2.13: Yakalanan şifrelenmiş video sinyalinin spectrum ve video görseli [12]



Şekil 2.14: Yakalanan video sinyalinin şifresi çözülmüş spectrum ve video görseli [12]

Ele geçirilen savaş uçakları dahil hedef alınan çoğunluğu İsrail ve İran hava aracına ait tüm bu görseller yaşanan casusluk faaliyetinin büyüklüğünü göstermektedir. The Intercept yazarları, Anarşist dosyalarının İran'a karşı potansiyel bir saldırı için İsrail insansız hava araçlarını izlediğini ve İsrail'in dünyaya ihraç ettiği insansız hava aracı teknolojisini takip ettiğini gösterdiğini söylemiştir.

[16]'da yer alan haberde, casusluk olayının ABD ve İsrail ilişkilerine zarar vereceği iddia edilmiştir. Haaretz gazetesine konuyla ilgili konuşan bir İsrailli yetkili, "Bu olayda savunma

operasyonlarımız zarar görmedi. Ortadoğu'daki istihbarat birimleri bizim faaliyetlerimizle ilgili bilgi topluyor, tıpkı bizim yaptığımız gibi" şeklinde açıklama yapmıştır. İsrail'in o dönem Enerji Bakanı olan Yuval Steinitz, İsrail askeri radyosuna o dönem yaptığı açıklamada, ABD ve İngiliz istihbaratının İsrail'i hedef almasının kendisini şaşırtmadığını söylemiştir. Netanyahu hükümetinde enformasyon bakanı olarak da görev yapan Enerji Bakanı Yuval Steinitz, "ABD'nin dünyanın her tarafında casusluk faaliyeti yürüttüğünü biliyoruz, biz dahil bütün müttefiklerini dinliyor ve izliyor" ifadesini kullanmıştır.

Güney Kıbrıs'daki bir istihbarat merkezinden yapıldığı iddia edilen bu dinleme ve izleme faaliyetlerinin, Türkiye dahil tüm çevre ülkelerin hava unsurlarının hedef olma ihtimalini göstermektedir. Başta Türkiye olmak üzere dünyada, yüksek teknoloji ürünleri olan İHA sistemlerinde liderliğe oynayan ülkelerin, siber saldırılar dahil olmak üzere gelebilecek tüm saldırılara karşı güvenlik sistemlerini geliştirmesi ve güncellemesi bir zorunluluk olarak değerlendirilmelidir.

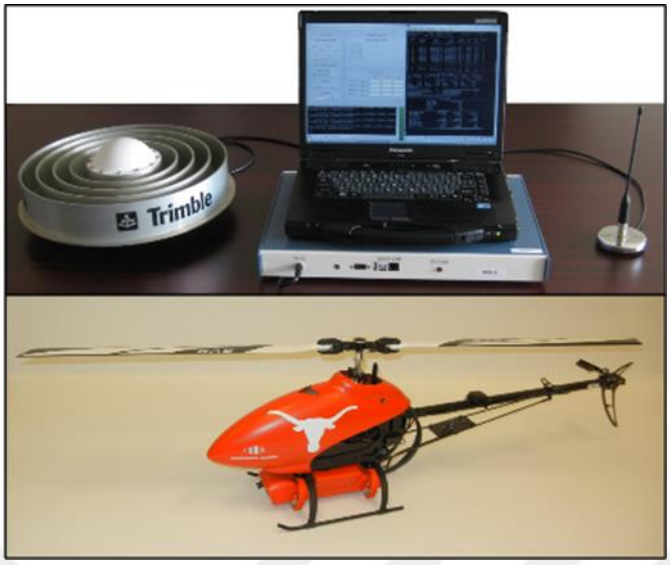
2.2. DRONE HACKLEME ÖRNEKLERİ

Bu bölümde sivil alanda yaşanılan örneklere yer verilmiştir. Tablo 2.2'de verilen örnekler, kullanılan saldırı yüzeylerine göre listelenmiştir. Gerekli araçlara ve zamana sahip olunmadığı için literatür taraması yoluyla keşfedilen ve incelenen örneklerin güvenlik açıklarından hiçbiri doğrulanmamıştır. Ayrıca, incelenen uygulama ve yöntemler zaman içerisinde güncelliğini kaybedebilir.

Tablo 2.2: Kullanılan saldırı yüzeylerine göre drone hackleme örnekleri

Saldırı Yüzeyi	Drone Hackleme Örnekleri
WiFi	2.1.2. SkyJack [20] 2.1.3. Nils Rodday Saldırısı --WEP Saldırısı [23] 2.1.6. DroneJack [31, 32] 2.1.7. Parrot Bebop Drona Kablosuz Saldırılar [34] 2.1.8. Parrot AR.Drone 2 - WiFi Saldırısı [36] 2.1.15. DroneSploit ile Drone Hackleme [48]
Radyo Frekans	2.1.3. Nils Rodday Saldırısı --Xbee Saldırısı [23] 2.1.4. GNU Radyo ve SDR ile Drone Ele Geçirme ve Diğer IoT Cihazları Hackleme [27, 28, 29] 2.1.5. Drone Ele Geçirme - Çok Boyutlu Saldırı Vektörleri ve Karşı Önlemler - Radyo Sinyali Analizi [30] 2.1.10. NRF24L01 Modüllü DeviationTX Evrensel Uzaktan Kumanda [39] 2.1.11. Icarus [41]
GPS	2.1.1.GPS Spoofing ile İnsansız Hava Aracı Yakalama ve Kontrol Etme [17, 18] 2.1.5. Drone Ele Geçirme - Çok Boyutlu Saldırı Vektörleri ve Karşı Önlemler - GPS Spoofing [30] 2.1.6. DroneJack [31] 2.1.14. İnsansız Hava Araçlarının Güvenlik Açıkları ve Karşı Önlemler - GPS Spoofing [47] 2.1.16. DRAT - GPS Spoofing [49]
Tersine Mühendislik	2.1.5. Drone Ele Geçirme - Çok Boyutlu Saldırı Vektörleri ve Karşı Önlemler -- SDK Kimlik Doğrulama Mekanizması, Ürün Yazılımı Analizi [30] 2.1.9. Maldrone [38] 2.1.12. E012 SDR Verici [42] 2.1.13. Drone Sızma Testi [44] 2.1.14. İnsansız Hava Araçlarının Güvenlik Açıkları ve Karşı Önlemler - Cracking DJI SDK [47] 2.1.16. DRAT – Malicious [49]

2.2.1. GPS Spoofing ile İnsansız Hava Aracı Yakalama ve Kontrol Etme



Şekil 2.15: Spoofer cihaz ve hedef İHA [17]

Drone: Adaptive Flight Hornet Mini UAV
Saldırı Yüzeyi: GPS (GPS Spoofing)

Texas Üniversitesi profesörü Todd Humphrey ve lisansüstü araştırmacıları, Haziran 2012'de White Sands Missile Range'de, ABD İç Güvenlik Bakanlığı tarafından denetlenen bir deney gerçekleştirdi. Bu deneyde, GPS aldatmacası (spoofing) uygulayarak sivil bir İHA'yı kontrol ettiler. Humphrey [18] ile yapılan röportaja göre, yapılan deney 1000$ civarında donanım ve dört yılda geliştirdikleri bir yazılım ile gerçekleştirilmiş. Drone olarak ise üniversitenin sahip olduğu, ticari bir İHA olan Hornet Mini kullanılmış. Hornet Mini, sivil GPS sistemini kullanan bir İHA'dır. Humphrey'in de belirttiği üzere sivil kullanımdaki GPS sinyalleri, kimlik doğrulama mekanizması olmadan, açık ve şifresiz olarak iletilmektedir. Humphrey ve öğrencileri de, bu durumu kullanarak İHA'yı kontrol etmeyi başarmıştır. Ayrıca bu deneyi, İHA'nın kaçırıldığına dair herhangi bir işaret olmaksızın gerçekleştirmiştirler. Spoofer cihaz ve hedef İHA görseli Şekil 2.15'de verilmiştir.

Yapılan GPS spoofing deneyi açık sahada gerçekleştirilmiştir. Sahte GPS sinyalleri havada yaklaşık 620 m mesafeden iletilmiş ve hedef İHA'nın seyrüsefer sistemi ele geçirilmiştir. Seyrüsefer sistemi ele geçirildiğinde ise İHA, zemin seviyesinin yaklaşık 12 m üzerinde havada durmaktadır. Daha sonra, spoofer cihaz, sahte bir şekilde İHA'nın yukarıya doğru ilerlediğini gösteren konum ve hız çözümleri üretmesi için ele geçirilen GPS alıcısı uyarılmıştır. Bu uyarı sonucunda İHA, komut verilen uçuş konumundan belirgin sapmayı düzeltmek için aşağı

indirilmiştir. Spoofer cihaz, ele geçirilen İHA'nın açık döngü kontrolü gerçekleştirdiğinden, bir başka pilotun İHA'yı elle kontrolünü ele geçirmesi üzerine İHA'nın aşağı doğru hareketi sadece durdurulmuştur.

Humphrey'in öğrencileri, bu ilk denemelerinde nispeten durağan bir drona odaklanmalarına rağmen bunun yapılabileceğini göstermişlerdir. Humphrey [18] röportajda, aynı saldırıyı hareketli bir İHA üzerinde deneyeceklerini, ancak İHA düz bir rotada hareket etmeyip kaçamak hareketler yaptığı sürece deneyin daha da zorlaşacağını söylemiştir.

Daha sonra Humphrey, 2014 yılında Daniel P. Shepard ve Jahshan A. Bhatti ile birlikte GPS aldatmacasının modelleme ve analizi ile ilgili bir makale [17] kaleme almıştır. 2012'de White Sands'de yapılan deney, her ne kadar değerli ve eşi görülmemiş bir gösteri olmasına rağmen, video verilerinden başka bir şey yakalayamamıştır. Bu nedenle, Haziran 2013'de Austin, Texas yakınlarında, yazdığı makalenin modelleme ve analiz bölümlerini deneysel olarak doğrulamak için yeni bir deney gerçekleştirmiştir. Yeni denemede, sahte GPS saldırısı sırasında hedef İHA'nın GPS alıcısı ve durum tahmincisi verileri sürekli olarak kaydedilmiştir. Korunan GPS bandında yetkisiz radyo sinyali iletimini önlemek için, hava durumuna duyarlı sinyaller, İHA'nın GPS antenine doğrudan hafif bir koaksiyel kablo vasıtasıyla enjekte edilmiş ve havadaki uyduların orijinal GPS sinyalleri ile birleştirilmiştir. Hem havaya karşı önceki denemede hem de o makalenin kablolu deneyinde İHA, yakalama ve açık döngü kontrolü için analiz bölümünde açıklanan tahminlere uygun bir şekilde davranmıştır.

Humphrey ve ekibi, yaptıkları deneyi uygulayarak askeri bir uçağı kaçırma girişiminde bulunmamış ve hatta bunu yapabileceklerinden bile emin değillerdir. Ancak sivil İHA'lar için böyle düşünmemektedirler. Yapılan bu deneyde sivil İHA'ların kaçırılabileceği gösterilmiştir. Ayrıca Humphrey, GPS aldatmacası ile ilgili deneylerinde dronlar üzerinde yoğunlaşmasına rağmen, GPS aldatmacasının çevremizde GPS'e bağlı diğer sistemlerde de uygulanabileceğini söylemektedir. Sebep olarak da daha önce bahsedilen açık ve şifresiz olan sivil GPS kullanımını belirtmektedir. Ancak bahsedilen bu yöntemler askeri sistemleri kapsamamaktadır [17]. Çünkü askeri sistemler, sivil kullanımdan farklı bir frekans bandında (L2) GPS sistemi kullanmaktalar. Askeri sistemlerin kullandığı GPS şifrelenmiş ve daha karmaşık bir yapıya sahiptir. Bu sebeple GPS spoofing saldırısının askeri sistemler de uygulanması daha zor bir hale gelmektedir. Ancak daha önceki ABD - İran örneğinde [7] görüldüğü üzere imkansız değildir.

2.2.2. SkyJack



Şekil 2.16: SkyJack için örnek saldırı görseli [19]

Drone: Parrot AR.Drone 2.0

Saldırı Yüzeyi: WiFi (Deauthentication saldırısı)

Donanım: Raspberry Pi, Alfa AWUS036H, Edimax EW-7811Un Wireless Adapter

Yazılım: SkyJack, aircrack-ng, node-ar-drone, node.js

Güvenlik araştırmacısı Samy Kamkar [20], kendi geliştirdiği SkyJack yazılımını kullanarak kablosuz alanda tespit edilen dronların kontrollerini ele geçiren, köle (zombie) drone ordusu oluşturabilecek çalışmasını paylaşmıştır. Kullandığı araçları drone ile taşıyarak çevrede bulunan diğer dronları taramada avantaj elde etse bile, aynı zamanda drona gerek kalmadan yerde de, Linux Makine / Raspberry Pi /dizüstü kullanarak SkyJack ile drone avlayabilmektedir. SkyJack için örnek saldırı görseli Şekil 2.16'da verilmiştir.

Yazılım olarak Perl dili ile yazmış olduğu SkyJack yazılımını, aircrack-ng , node.js ve Node-ar-drone araçlarını; donanım olarak da Parrot AR.Drone 2, Raspberry Pi, USB batarya, Alfa AWUS036H kablosuz verici, Edimax EW-7811Un kullanmıştır. Linux kurulu Raspberry Pi 3 üzerinde SkyJack'i uygulamıştır. Raspberry Pi 3 bataryası için de bir USB batarya kullanmıştır. Alfa AWUS036H kablosuz adaptör ile monitor mod başlatılıp çevrede başka dronları aramada yararlanmıştır.

Parrot Bebop ve bazı dronların MAC adresi açık şekilde internette yer almaktadır. Bu MAC adreslerini kullanarak dronları tespit edip, bulduğu drona aireplay-ng aracı ile deauthentication paketleri göndererek gerçek kullanıcı ile bağlantısını kesmesini sağlamıştır. SkyJack'in kendi ağını başlatması için Edimax EW-7811Un kablosuz USB adaptörünü kullanmıştır. Kullanılan bu adaptör, Raspberry Pi üzerindeki ikinci bir WiFi kartı ile Raspberry Pi'ye bağlanıp, dizüstü bilgisayarından veya tabletinden SkyJack'e bağlanmasını ve node.js kütüphanesini kullanarak, kontrol edilen diğer tüm köle dronlarını izlemesini sağlamıştır [20].

SkyJack, "Drone Hacking" literatüründe sıkça atıf yapılan örneklerden biridir. Dronlar üzerindeki güvenlik eksikliğinin vurgulaması ve kullandığı yöntem ile ilgi çekici olması gibi sebeplerle pek çok kaynakta adı geçmektedir. Fournier ve diğ. [21] yapılan atıfta eleştiri olarak gerçek dünya için anti-drone bir çözüm olmadığını söylemiştir. Sebep olarak, dronun gerçek sahibi SkyJack saldırısının başlamasından birkaç saniye sonra onun dronuna bağlanabilir olması gösterilmiştir. Kontrolü tekrar ele geçirdikten hemen sonra return to home komutu ile dronun geri çağrılabileceği ve bunun da SkyJack'i kullanışsız hale getirdiği belirtilmiştir. Ancak tüm bu eksileri ve artıları ile birlikte SkyJack, "Drone Hacking" araştırmalarında önemli bir örnek olarak yer almaktadır.

2.2.3. Nils Rodday Saldırısı



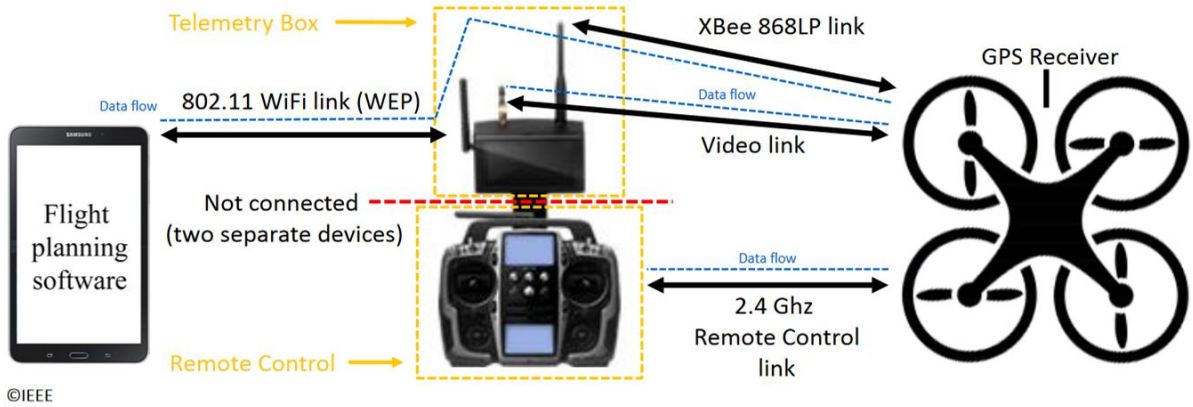
Şekil 2.17: Aerialtronics Altura Zenith [22]

Drone: Aerialtronics Altura Zenith (Law Enforcement Drone)

Saldırı Yüzeyi: WiFi (WEP saldırısı), RF (MITM)

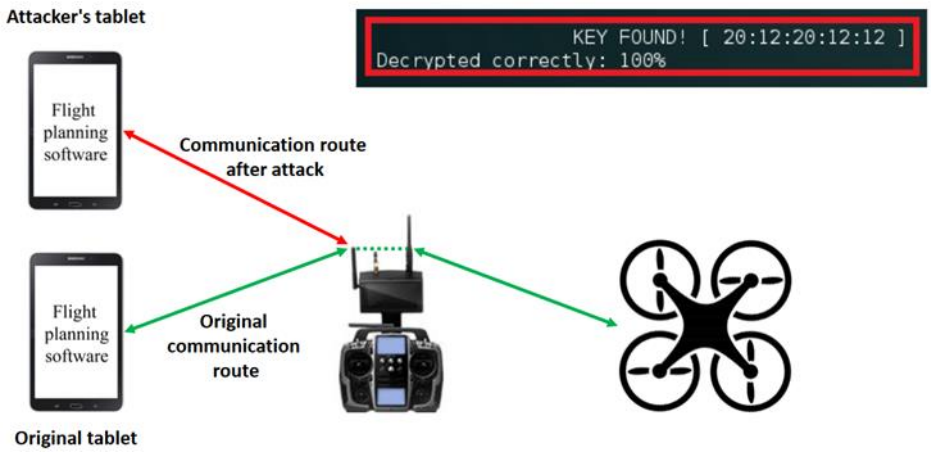
IBM güvenlik araştırmacısı Nils Rodday tarafından geliştirilen saldırının sunumunu [23], Black Hat Asia 2016 siber güvenlik konferansında sunmuştur. Araştırmacı, devlet makamları ve polis teşkilatları tarafından yaygın olarak kullanılan, fiyat aralığı 30.000-35.000 arası olan yüksek düzey İHA'ları, 40$ altında bir donanım yardımı ile 2 kilometre uzaklıktaki yerden kaçırmanın ne kadar kolay olduğunu göstermiştir. Hedef İHA Aerialtronics Altura Zenith görseli Şekil 2.17'de paylaşılmıştır.

İHA'nın iletişim şeması Şekil 2.18'de paylaşılmıştır.



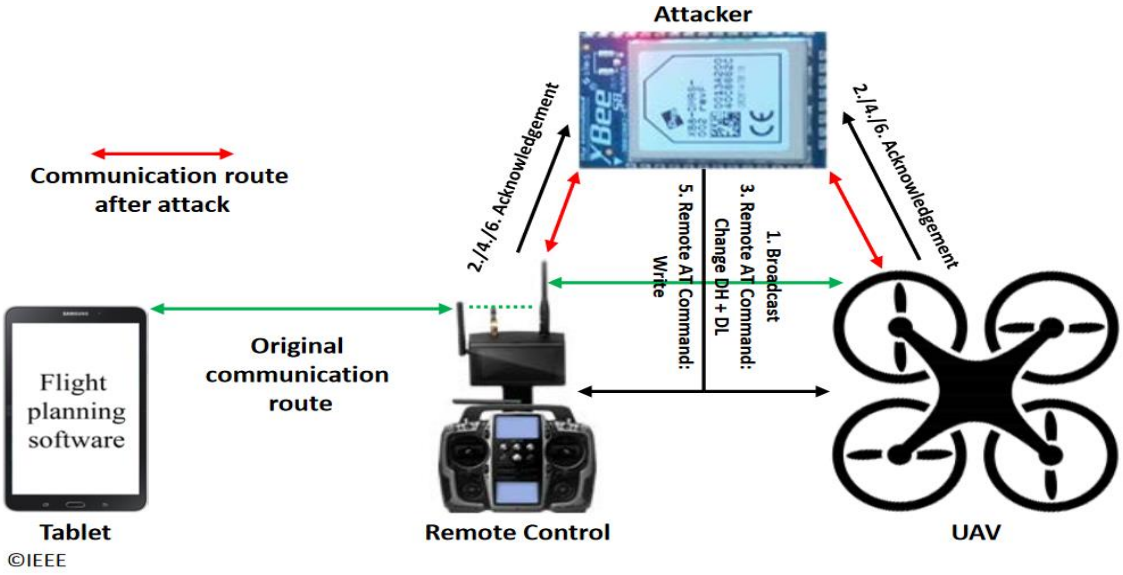
Şekil 2.18: İHA'nın iletişim şeması [23]

Rodday, test ettiği İHA'da, saniyeler içerisinde onu kontrol etmeye yarayan iki tane güvenlik zafiyeti keşfetmiştir. Birincisi, uzaktan kontrol modülü ile tablet arasında, saniyeler içerisinde kırılmasıyla ünlü WEP protokolünün kullanılmasıydı. WEP saldırı şeması Şekil 2.19'da gösterilmiştir.



Şekil 2.19: İHA'nın WEP saldırı şeması [23]

İkincisi ise, İHA ve modül arasında iletişimi daha az güvenli radyo protokolleri ile gerçekleştirmesidir. Saldırı şeması Şekil 2.20'de gösterilmiştir.



Şekil 2.20: İHA'nın Xbee saldırısı [23]

İnsansız hava araçlarında modül ve drone arasındaki iletişimde yaygın olarak Xbee çipi kullanılmaktadır. Normalde çipin iletişimi şifreleme kapasitesi vardır. Ancak İHA ve kullanıcı arasındaki gecikmeyi önlemek için kullanılmamaktadır. Bu da, bir saldırganın MITM atakları ile dronun ağ bağlantısını kesip 2 km öteden kod enjekte etmesine yol açmaktadır. Bu saldırı sonucu normal kullanıcının dronla yapabileceği her şeyi yapılabilmektedir. Ayrıca, Rodday, dronun yazılımına, ters mühendislik kabiliyetine sahip herhangi bir gelişmiş Hacker'ın seyrüsefer kontrolleri gönderebileceğini, gerçek operatöre gelen tüm komutları engelleyebileceğini ve hatta yere indirebileceğini söylemiştir.

Rodday, dronun markasını açıklamamıştır. Bununla birlikte, üç ayaklı Quadcopter'in yaklaşık 40 dakikalık bir uçuş süresine sahip olduğunu, polis ve itfaiye departmanları tarafından konuşlandırıldığını ve aynı zamanda elektrik hatları, yel değirmenleri ve hava fotoğrafçılığı gibi endüstriyel uygulamalarda kullanılmak üzere pazarlandığını ima etmiştir [24]. Walters [25] tarafından hazırlanan drone hackleme örneklerinin listelendiği sitede İHA'nın Aerialtronics Altura Zenith (Law Enforcement Drone) olduğu belirtilmiştir.

2.2.4. GNU Radyo ve SDR ile Drone Ele Geçirme ve Diğer IoT Cihazları Hackleme



Şekil 2.21: Syma X5C Quadcopter [26]

Drone: Birçok Model

Saldırı Yüzeyi: RF (SDR(1), nRF24L01+ (2))

Donanım: UmTRX(1), Arduino Mega(2), Raspberry Pi(2), Kablo(2), nRF24L01+(2), Oyun Konsolu(2)

Yazılım: GNU Radio(1), Baudline(1), RF24.cpp(2)

Arthur Garipov, Hindistan'da düzenlenen Nullcon Goa 2017'deki sunumunda GNU Radio ve SDR ile Drone Hacking ve diğer IoT cihazlarını ele geçirmeyi uygulamalı olarak göstermiştir. Garipov [27] sunumunda SDR araçlarını (HackRF One, HackRF Blue, BladeRF, RTL-SDR, nRF24, USRP vb.) ve yazılımlarını (SDR#, HDSDR, GQRX, GNU Radio, LabVIEW, Baudline) tanıtmıştır. Bu araçlar ve yazılımlarla "Hacking of wireless gadgets, GPS falsification, Sniffing GSM signals, MouseJack" gibi hackleme yöntemlerini Garipov [28] yayınlanan videosunda detaylı olarak anlatmıştır. Bahsettiği ve uyguladığı bu yöntemler sadece drone değil, kablosuz iletişim kuran IoT cihazlarını da kapsamaktadır.

Ayrıca Garipov, aynı sunumun Rusçasını "Wireless Hijack: From Quadrocopters to Computer Mouses" adıyla, 2016 yılında Rusya'da düzenlenen PHDays (Positive Hack Days) etkinliğinde gerçekleştirmiştir. Aynı etkinlikte, amacı dronun kontrolünü ele geçirmek olan "PHDays How They Stole Our Drone" adlı bir yarışma düzenlenmiştir. Bu yarışma ile ilgili Garipov ve Novikov [29] tarafından paylaşılan "Positive Technology" bloglarında "Drone Hacking" metotlarının anlatıldığı detaylı bir yazı kaleme almışlardır. Ödül olarak Syma X8C verilen yarışmada hedef drone olarak Syma X5C Quadcopter seçilmiştir. Syma X5C Quadcopter görseli Şekil 2.21'de verilmiştir. Blok yazısında SDR ve nRF24L01+ araçlarını kullanarak iki farklı metot ile drone hacklemeyi detaylı bir şekilde anlatmışlardır.

2.2.4.1. *SDR Metodu*

Bu metotta donanım olarak UmTRX SDR cihazı, yazılım olarak da GNU Radio, Baudline kullanılmaktadır. UmTRX'in spectrum taraması ile kanallar bulunup GNU Radio'da basit akış grafiği oluşturduktan sonra tespit edilen kanallar eklenmiştir. Kaydedilen verilere bakmak için ise Baudline çalıştırılıp byte hesabıyla adres hesaplanmıştır. Sonrasında ise dosya analizi yapılıp payload hazırlanmıştır. Son olarak da Syma protokolü analiz edilip uygulama gerçekleştirilmiştir.

2.2.4.2. *nRF24L01+ ve Arduino Metodu*

Bu metotta hem alıcı hem verici olarak çalışabilen nRF24L01+ modülü kullanılmaktadır. SDR yönteminin aksine, bu yöntem radyo alanında neredeyse hiç bilgi gerektirmez ve son derece ucuzdur (Arduino, $ 2, nRF24L01+, $ 1'dir). nRF24L01+ modülü kullanılarak interceptor kumanda yapılmıştır. nRF24L01+ ile analiz edilip panel tarafından kullanılan ayarlar bulunmuş ve son olarak Syma protokolü analiz edilmiştir. PHDays'de paylaşılan interceptor'un görseli Şekil 2.22'de verilmektedir.



Şekil 2.22: Ardunio Mega ile yapılan Interceptor [29]

Interceptor, Ardunio yerine Raspberry Pi ile de yapılabilir [29]. Şekil 2.23'de örneği gösterilmektedir.



Şekil 2.23: Raspberry Pi ile yapılan Interceptor [29]

2.2.5. Drone Ele Geçirme - Çok Boyutlu Saldırı Vektörleri ve Karşı Önlemler



Şekil 2.24: DJI Phantom 3 [30]

Drone: DJI Phantom 3

Saldırı Yüzeyi: Tersine Mühendislik (SDK Kimlik Doğrulama Mekanizması, Firmware Analizi), RF (Radyo Sinyal Analizi), GPS (GPS Spoofing)

Donanım: HackRF One SDR, Raspberry Pi 3

Yazılım: JBE, JD-GUI, Binwalk, IDA Pro, hexdump

2016 yılında ABD'de düzenlenen DEF CON 24 Hacking Konferansı'nda, Trend Micro'dan Aaron Luo, "Drone Hijacking"'i çeşitli metotlarla uygulamalı olarak göstermiş ve bu saldırı

tekniklerinin nasıl önlenebileceğini Luo [30] sunumunda anlatmıştır. Saldırıda kullanılan DJI Phantom 3 görseli Şekil 2.24'de paylaşılmıştır.

2.2.5.1. *SDK Kimlik Doğrulama Mekanizması*

Aoron Luo ilk olarak DJI Phantom 3A aracının SDK'sını analiz etmiştir. Düzenlediği SDK ile telefondaki uygulamayı kullanarak Phantom'a bağlanmıştır. DEFCON'da sunumda gösterildiği üzere bu yöntem ile iniş-kalkış yaptırabilmiş ve hatta belirli bir bölgeye Phantom'ı yönlendirebilmiştir. Luo, SDK saldırısını önlemek için yapılması gerekenleri aşağıda belirtmiştir;

- Kütüphane dosyasını obfuscator / packer (gizleyici araçlar) ile korumak
- Sadece uygulama ve sunucuda doğrulanması değil; uygulama, sunucu ve drone arasında, SDK kimlik doğrulama anahtarını doğrulamak için asimetrik şifreleme kullanmak

2.2.5.2. *Firmware Analizi*

Kullandığı DJI Phantom 3A adlı dronun bin uzantılı dosyasından sınırlı da olsa binwalk aracı ile verileri çıkartmıştır. Luo çıkardığı verileri, IDA Pro ile analiz edip anahtar fonksiyonunu bulmuştur. Bir ayrıştırıcı ile verileri parçalara ayırmış ve sonunda her firmware modülü ile ilgili bilgilere ulaşıp onları dosyadan çıkartmıştır. PFC300SFw3.bin dosyasından UBI dosya sistemini çıkartılmıştır. Dosya sisteminden SSH key data ve configuration, /etc/shadow… gibi önemli bilgilere ulaşmıştır. Luo, firmware saldırısını önlemek için yapılması gerekenleri aşağıda belirtmiştir;

- Firmware'yi şifrelemek
- Şifreleme anahtarını donanım üzerinde depolanmalı, ancak yine de depolama alanı hakkında güvenlik için ekstra dikkat gerekmektedir

2.2.5.3. *Radyo Sinyal Analizi*

P3A(DJI Phantom 3), 2.4GHz ISM bandıyla veri aktarmak için iki modülasyon / demodülasyon kullanmaktadır. Luo, HackRF One SDR (Software Defined Radio) aracını kullanarak P3A ve RC kumanda arasında FSSS ve DSSS frekans analizi yapıp, drone yönünü (yukarı, aşağı, sağ, sol) kontrol etmiştir. Bir SDR yazılımı ile yaptığı analiz sonucu frekansın 2.400~2.483 GHz aralığında, her kanalın yaklaşık 1 MHz olduğuna ulaşmıştır. Drondan uzaktan kumandaya

görüntü aktarımındaki değerler; Frekans 2.4015 ~ 2.4815 GHz aralığında, 6 kanala bölünmüş ve her kanal yaklaşık 10 MHz'dir. Görüntülerin checksum (toplam) mekanizması olmadığı için yanlış görüntüyü kumandaya göstererek radyo frekansı yayınını bozabilmektedir. Luo, radyo analiz saldırısını önlemek için yapılması gerekenleri aşağıda belirmiştir;

- Resim sağlama toplamını (checksum) doğrulamak
- Görüntü verilerini asimetrik şifreleme ile aktarmak (Ancak daha fazla performansa ihtiyaç duyulur, bu durumda ters modülasyon / demodülasyon zor olduğu için sadece sağlama toplamı eklemek yeterli olacaktır.)

Kumandaya yanlış resim gösterimi Şekil 2.25'de verilmiştir.



Şekil 2.25: Kumandaya yanlış resim gösterimi [30]

2.2.5.4. *GPS Spoofing*

Ticari protokollere göre GPS protokolü (C/A code) açık ve şifresiz bir protokoldür. Bu yüzden saldırganlar tarafından kolayca taklit edilebilmektedir. GitHub'da gps-sdr-sim olarak adlandırılan açık kaynaklı iyi bir GPS simülatörü vardır, ancak sahte bir konum istemeden önce I / Q verilerini oluşturmak için birkaç dakika beklemek zorunda olmakla birlikte bazı kısıtlamaları olduğu için Luo bu simülatörü kullanmamıştır. Onun yerine gerçek zamanlı olarak GPS sinyali üretmesine izin veren ve joystick ile kontrol edilebilen bir kod geliştirmiştir. Sahte GPS noktası oluşturma görseli Şekil 2.26'da paylaşılmıştır.

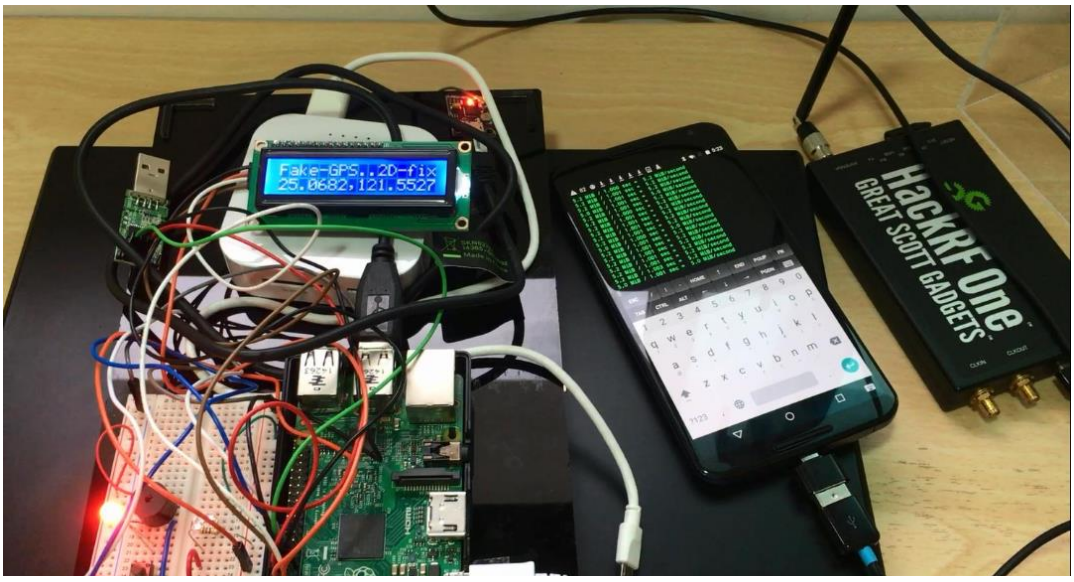


Şekil 2.26: Sahte GPS noktası oluşturma [30]

Luo, GPS saldırısını önlemek için yapılması gerekenleri aşağıda belirtmiştir;

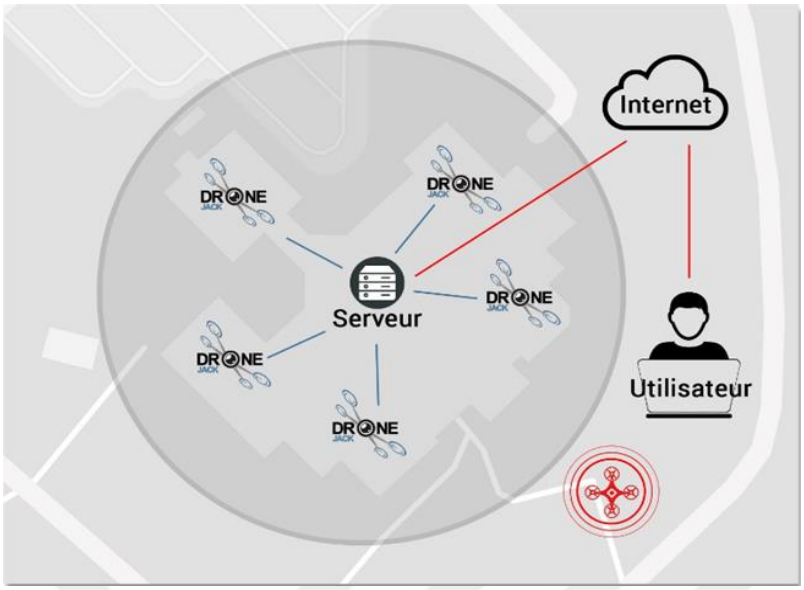
- GPS sub-frame verisini doğrulamak
- Uydu saati ile gerçek zaman arasındaki zamanı doğrulamak.
- Noktadan noktaya hareket hızını kontrol etmek. (Örneğin bir saniyede Tayvan'dan Las Vegas'a konumu değiştirmek imkansızdır.)

Luo sunumunda son olarak, Raspberry Pi 3 ve u-blox GPS modülü kullanarak yaptığı sahte GPS sinyali algılayıcısını göstermiştir. Sahte GPS tespit detektör düzeneği Şekil 2.27'de gösterilmektedir.



Şekil 2.27: Sahte GPS tespit detektör düzeneği [30]

2.2.6. DroneJack



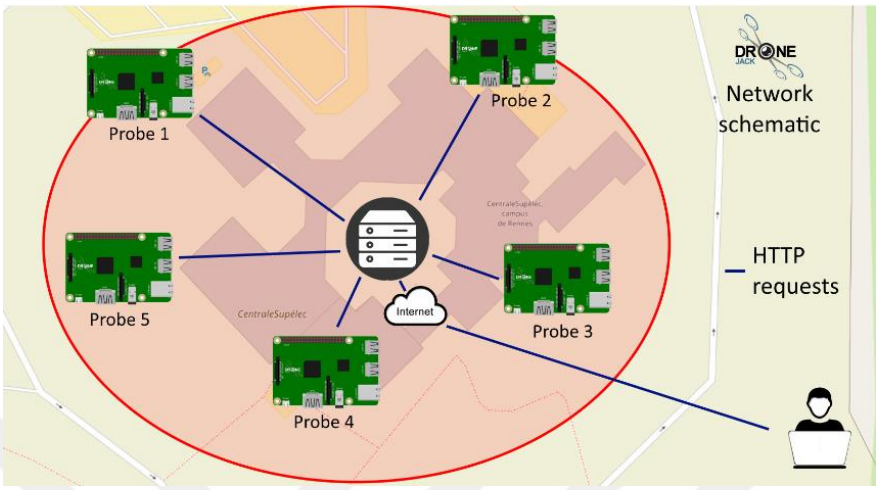
Şekil 2.28: DroneJack mimari [31]

Drone: Parrot AR Drone, Parrot Bebop
Saldırı Yüzeyi: WiFi (FTP), GPS (GPS Spoofing)
Donanım: Raspberry Pi
Yazılım: Airodump-ng Araçları

Fransız araştırma enstitüsü Centrale Supélec'den, Guillaume Fournier, Paul Audren de Kerdrel1, Pascal Cotret ve Valérie Viet Triem Tong isimli öğrenciler, DroneJack isimli otonom bir anti-drone çözümü geliştirmişlerdir. Öğrenci projesi olarak geliştirilen bu çözüm, ticari dronlar için uygulanmaktadır. Öğrenciler, 2017 Haziran ayında Fransa'nın Rennes şehrinde SSTIC (Bilgi ve İletişim Güvenliği Sempozyumu)'nda DroneJack'i anlatan bir sunum gerçekleştirdiler [32]. Fournier ve diğ. [31] tarafından SSTIC için kaleme alınan makalelerinde anlatıldığı üzere, DroneJack, üzerinden uçulan alanı koruyan, dronları normal kullanıcı gibi kontrol edebilen, GPS koordinatları verilerek doğrudan yönlendirebilen (GPS modülü olan dronlar için geçerli) ve üzerinde uçan yabancı dronları düşürebilen önceden tanımlanmış savunma yapabilen bir anti-drone çözümü olarak sunulmaktadır. DroneJack mimarisini anlatan görsel Şekil 2.28'de paylaşılmıştır.

DroneJack, savunma için bölgeye konması gereken Raspberry Pi 3 (DroneJack Probes) ve bu Raspberry yönetiminden sorumlu bir web sunucusundan oluşan bir mobil koruma sistemidir. DroneJack, DroneJack probları sayısı ile sınırlı değildir. Bu sayede ihtiyaç duyulan alanı geniş

bir alana yayabilmektedir. Ayrıca, web sitesi arayüzünü kullanarak operatörün tehditleri yönetmek için sitede olması gerekmemektedir. Şekil 2.29'da, DroneJack'in küresel mimarisine genel bir bakış sunulmaktadır.



Şekil 2.29: DroneJack Probe mimari [31]

DroneJack, WiFi iletişimi kullanarak dronları algılama, izleme, ele geçirme ve kontrol etmeyi sağlamaktadır. Buradan da anlaşılacağı üzere, WiFi iletişimi olan dronlarda kullanılabildiği söylenebilir. Birden çok dronun gerçek kullanıcılarının bağlantısını kesmek için deauthentication saldırıları uygulamaktadır ve bağlantılarını engellemektedir. DroneJack sıfırdan geliştirilen ve savunucunun birden fazla drone ile baş etmesine izin veren web arayüzü ile bir bileşen şeklinde kullanılmaktadır. DroneJack, haritada drone akışını izlemek, drone tarafından üretilen video akışını ele geçirmek, hedef drona geri dön (gohome), kendini öldür (kill himself) veya belirli GPS koordinatlarına gitmek gibi çeşitli özellikleri uygulayabilmektedir. Dahası, saldırıların sayısı sınırlı değildir. Savunma yapan operatör (defender), DroneJack web sitesine yeni saldırılara ve tüm DroneJack örneklerine bağlı yüklemelere izin verdiğinden yeni özellikler yüklenebilmektedir. DroneJack, başarılı bir drone saldırısını 3 ana aşamaya ayırmaktadır: Drone üzerinde Algılama/Devralma/Saldırı gerçekleştirmedir. Analizlerin aşamaları aşağıda verilmiştir.

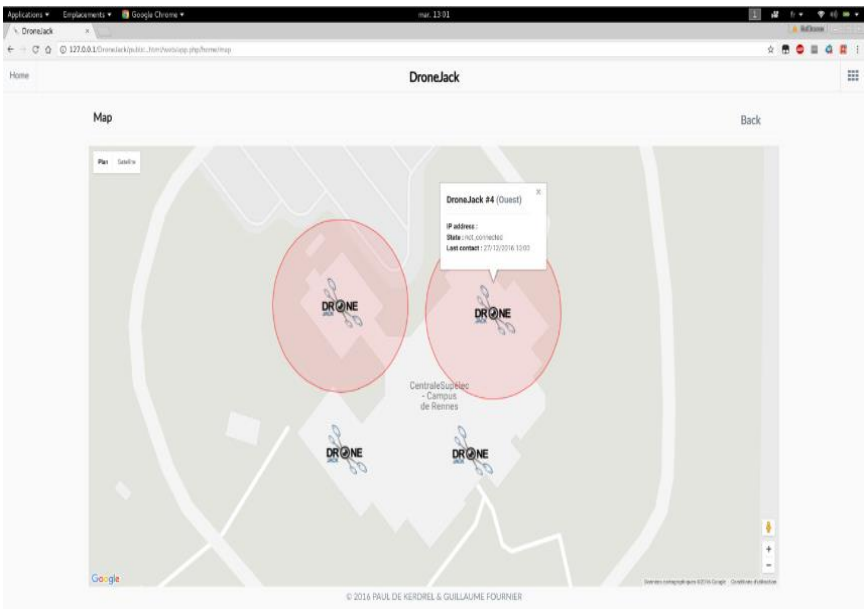
2.2.6.1. *Aşama 1.1: Algılama*

WiFi tabanlı drone algılamanın ilk adımı, neye bakılacağını bilmektir. Bu bölümde, dronlardan gelen WiFi erişim noktalarını keşfedilmektedir. Bu amaçla DroneJack, WiFi ağ güvenliğini değerlendirmek için airodump-ng araçlarına (SkyJack gibi) güvenmektedir. DroneJack sürekli

olarak WiFi iletişimini izlemekte ve WiFi tarayıcısı her 5 saniyede erişim noktalarının bir listesini üretmektedir. Bu listede drone tespit etmek, bir drone şirketinin bir MAC adresinin sahibi olup olmadığını kontrol etmek kadar basittir. Neyse ki, sahip olunan MAC adresleri herkese açıktır ve çevrimiçi olarak bulunabilmektedir. Örneğin, IEEE Standartlar Birliği Kayıt Kuruluşu'na göre, Parrot'un beş MAC adres aralığı vardır. Bir drone tespit edildiğinde, aşama 2'ye geçilmektedir. Aşağıdaki alt bölümlerde görülebileceği üzere, 2. aşamada bu dronları sıralı olarak işlemektedir. Bununla birlikte, eğer bir drone izlenirse (aşama 3) ve başka bir drone bulunursa, ikincisi bekleme durumuna geçmektedir. Sahibi ile bağlantısı kesilir ve drone, ilk drone ele geçirilene kadar havada gezinir.

2.2.6.2. *Aşama 1.2: Drone İzleme*

Aşama 1'in bir diğer ilginç özelliği drone izleme sistemidir. Drone tarafından gönderilen RSSI (Alınan Güç Sinyali Göstergesi) sinyallerin kullanılarak, her DroneJack düğümü ile tespit edilen drona olan mesafeyi hesaplamaktadır. Ardından DroneJack web arayüzü tüm verileri merkezileştirmektedir. Ancak DroneJack düğümlerinin GPS koordinatlarının bilinmesi şarttır. Kaç tane DroneJack düğümünün drone tespit ettiğine bağlı olarak, web arabirimi, yarıçapı drona olan uzaklık olacak şekilde bir daire çizmektedir veya dronun doğru konumunu hesaplamaktadır (Şekil 2.30). DroneJack, yeni keşfedilen her dronu izlemek için bir kez daha bir işlem başlatır.



Şekil 2.30: DroneJack web arayüzü [31]

2.2.6.3. *Aşama 2: Ele Geçirme*

Bir drone tespit edildiğinde, aşama 2 başlatılmaktadır. Bu aşamanın 2 basamağı vardır:

1. İlk olarak DroneJack, sahibi ile drone arasındaki bağlantısını kesmek için kimlik doğrulama paketleri kullanmaktadır. Bu paketler, aireplay-ng kullanılarak 3. aşamanın sonuna kadar sürekli gönderilmektedir. Bu adımı takiben, hemen hemen her ticari drone, gökyüzünde uçarak sahibinin yeniden bağlanmasını beklemektedir.

2. Daha sonra, DroneJack tespit edilen drona bağlanmakta ve aşama 3'e geçilmektedir. DroneJack sadece güvenli olmayan ağlara (şifresiz iletişim kullana) bağlanabilmekte, ancak bu çok sayıda drone modellerini ile kapsamaktadır. Örnek olarak Parrot AR Drones ve Bebop gibi. Erişim noktası WPA ile sabitlendiğinde, DroneJack ilk adımdan sonra durmaktadır.

DroneJack, süreklilik sağlayan bir koruma sistemidir, yani bir drone ele geçirildiğinde (devralındığında) Aşama 1'i durdurmamaktadır. Bu nedenle, yeni dronlar diğerleri zaten ele geçirilirken algılanabilmektedir. DroneJack bu durumu şu şekilde ele almaktadır: ilk önce tespit edilen drone, 2. ve 3. aşamaya geçiyor ancak bu dronda 3. aşama tamamlanmadığı sürece, tespit edilen diğer dronlar sadece 2. aşamanın ilk adımına geçmektedir. Diğer bir ifade ile tespit edilen her dronun sahibinden kopuk olduğu ve bu nedenle DroneJack öncekini ele geçirilene kadar huzur içinde gökyüzünde ilerlediği anlamına gelmektedir.

2.2.6.4. *Aşama 3: Saldırı*

DroneJack hedefli bir dronu ele geçirmeye başladıktan sonra, operatör tarafından yakalanan drona pilotluk yapma olanağı vermektedir. Operatör tarafından, nerede olursa olsun, dronun video akışı ile kontrol edilmesine olanak tanıyan bir web arayüzü geliştirilmiştir. Bunun ötesinde, operatör aynı anda birden fazla dronun saldırısıyla baş etmek zorunda kalabilmektedir. Bu amaçla DroneJack Aşama 3 birçok otomatik saldırıya ayarlanacak şekilde geliştirilmiştir. Eklenen üç ana davranış ise şunlardır:

1. Kill anahtarı: Parrot dronlarda motorları derhal durduran acil durum butonu vardır. Bu saldırı seti ile DroneJack sadece bu acil durum prosedürünü harekete geçirmekte ve tespit edilen tüm dronlar gökyüzünden yere çakılmaktadır.

2. Eve Git: Bu saldırı, dronu yalnızca başlangıç GPS koordinatlarına geri gönderiyor. DroneJack'in en az saldırgan koruması bu olmaktadır.

3. GPS koordinatlarına gidin: Bu saldırı dronu her DroneJack yapılandırmasında önceden ayarlanan GPS koordinatları grubuna göndermektedir.

Ek olarak, DroneJack, herhangi bir geliştiricinin web sitesi aracılığıyla kendi saldırı yöntemini yüklemesine imkân sağlamaktadır. DroneJack problar, bir ağ yapılandırmasında kullanılıyorsa, sürümler ve yapılandırma ayarları otomatik olarak senkronize edilebilmektedir. DroneJack yazılımının gereksinimlerini takiben, bir operatör Kali Linux tarafından çalıştırılabilir herhangi bir programlama diliyle kodlanmış yazılımı yükleyebilmektedir. Saldırı tamamlanır tamamlanmaz çıktı web sitesine yüklenecek şekilde ayarlanmıştır.

DroneJack geliştiricileri makalelerinde, bu özellik ile neler yapılabileceğinin bir örneği olarak iki özel saldırı sunmuştur;

1. nmap taraması: Bu saldırı tetiklendiğinde, DroneJack dron için tam bir nmap taraması yapacaktır. Bu taramayı kullanarak operatör, drone işletim sistemi hakkında çalışan servisler, açık portlar vb. gibi daha fazla bilgi edinebilir.

2. Tüm kayıtları silme: Mümkünse, bu saldırı drone üzerindeki tüm video kayıtlarını silecektir. Örneğin, bu saldırı Parrot'ın, hem AR Drone hem de Bebop dronlarında, istenilen herhangi bir dosyayı silebilecek açık FTP sunucusu çalıştırdığından oldukça basit bir şekilde yapılabilir [32].

İncelendiği üzere DroneJack, diğer drone ele geçirme vakalarından daha farklı bir çizgide yer almaktadır. Üzerinde uçulan belli bir bölgeyi yabancı dronlara karşı koruma sağlayan bir anti-drone çözümü olarak sunulmaktadır. Birden fazla drone üzerinde eşzamanlı algılama, izleme ve ele geçirmeyi yapabiliyor olması ve web arayüzü kullanılarak yönetilebilmesi sebebi ile diğer örneklerden avantajlı bir poziyonda yer almaktadır. Ayrıca bu web arayüzüne yeni saldırı çeşitlerinin yüklenebilmesi uygulama kapsamını artırmaktadır. Ancak bu avantajların yanında bazı dezavantajları da vardır. DroneJack, görüldüğü üzere sadece şifresiz iletişim kuran WiFi kontrollü ve drone tespitte kullandıkları MAC adresinin halka açık olan ticari dronlar üzerinde etkili olabilmektedir. Zaten çalışmalarında da Parrot AR Drone ve Bebop gibi sıkça kullanılan dronlar üzerinde yoğunlaştıklarını söylemişlerdir. Bu durumda RC dronlar üzerinde etkili

olamayacaktır. Ancak bu dezavantajlarına rağmen diğer örneklerdekinden ayrı olarak WiFi, GPS saldırı yüzeylerindeki yöntemleri birlikte kullanabilmesi ve bu saldırı çeşitlerine eklemeler yapıp, sıfırdan geliştirdikleri web arayüzünde yeni saldırı çeşitlerinin eklenebiliyor olması ve birden fazla dronu kapsayacak şekilde uygulanabiliyor olabilmesi açısından literatürde önemli bir yere sahiptir.

2.2.7. Parrot Bebop Drona Kablosuz Saldırılar



Şekil 2.31: Parrot Bebop Drone [33]

Drone: Parrot Bebop
Saldırı Yüzeyi: WiFi (FTP, Deauthentication Saldırısı)
Donanım: Wireless Adaptor
Yazılım: Aircrack-ng Araçları

[34]'de kullanıcının telefonla kontrol ettiği Parrot Bebop adlı dronun bağlantısının kesilip, kontrolün saldırganın telefona geçmesi detaylı bir şekilde anlatılmaktadır. İkinci bölümde ise FTP saldırısı ile drondaki medya dosyalarına erişilmiştir. Böylelikle kayıtlı resim ve videoları kendi bilgisayarımıza indirilebilir ya da drona zararlı yazılımlar yüklenebilir olduğu gösterilmiştir. Kullanıcı ise tercihini Parrot Bebop'daki bir video ile kendi bilgisayarındaki videosunu değiştirerek kullanmıştır. Saldırıda kullanılan örnek Parrot Bebop Drone görseli Şekil 2.31'de paylaşılmıştır.

[34]'de ilk bölümde Parot Bebop üzerinde bir saldırı gerçekleştirmiştir. Bu saldırı çeşidi şifresiz iletişim kuran çoğu WiFi dronlar üzerinde gerçekleştirilebilir. Saldırıda Kali Linux'de yüklü aircrack-ng araçları kullanılmaktadır. Bu araçlardan biri olan aireplay-ng kullanılarak hedef drona deauthentication paketleri gönderip normal kullanıcı ile drone arasındaki iletişimi durdurmuştur. Paket gönderilmeye devam ettiği için normal kullanıcı telefonu ile drone iletişimi kesilmiştir. Kullanıcı kendi telefonuna yüklediği Parrot Bebep kontrol uygulaması ile dronu kontrol etmiştir. Anlatılan bu işlemleri yapan komutlar sırasıyla şöyledir;

airmon-ng start [interface] *// WiFi kartını, çevre ağları dinlemeyi sağlayan monitör moda alır.*
airmon-ng check kill *// Çatışan tüm işlemleri sonlandırır.*
airodump-ng [interface] *// Kurbanında bulunduğu çevre ağları tarar, bulduktan sonra ctrl+c ile işlemi durdurur.*

airodump-ng -c [#] --bssid [DRONE MAC] -w [filelocation/name] [interface] *// Bir önceki komutta yakalanan dronun -c parametresi ile kanal numarası, --bssid ile hedef dronun MAC adresi, -w parametresi ile de yakalanan verilerin kaydedileceği dosyayı belirler. (-w zorunlu değildir), [interface] monitör modda yer alan arayüz belirtilir.*

aireplay-ng -0 0 -a [DRONE MAC] [VIC MAC] [interface] *// Yeni bir konsol ekranı açarak -0 <count> paremetresi ile deauthenticate paketleri yollanacağı, -a parametresi ile BSSID (Drone MAC adresi), [VIC MAC] ile bir önceki komut çıktısındaki STATION kısmında yakalanan normal kullanıcının telefon MAC adresi ,[interface] monitor modda yer alan arayüz belirtilir.*

[34]'de, ikinci bölümde ise bir FTP saldırısı düzenlemiştir. FTP, dosya transferinde kullanılan bir protokoldür. Yapılan işlemlerde ilk iki komutta, birinci bölümdeki saldırıda kullanılan airmon-ng check kill komutu ile başlatılan monitor modu kapatılmıştır, airmon-ng check kill komutu ile kapatılan NetworkManager servisi başlatılmıştır. Daha sonra Parrot Bebop üzerinde nmap taraması yapıldığında FTP portunun açık olduğu görülmüştür ve bu açık port, drona dosya gönderme ve drone üzerinde kayıtlı dosyaları alma izni vermektedir. Kullanılan komutlar şöyledir;

airmon-ng stop wlan1mon *// Monitör modu durdurur.*

service NetworkManager start *// NetworkManager servisini başlatır. Daha sonra bilgisayardan drona bağlanılır.*

ifconfig *// IP'yi bulur.*

nmap -sn [X.X.X.1-254] *// Tüm subnetleri taratır, bağlı tüm cihazları listeler.*

nmap [x.x.x.1] *// Listede bağlı olan cihazı taratır.*

ftp [IP] *// ftp komutu ile bağlantı sağlanır.*

ls *// ls komutu ile drondaki dosyalar listelenir.*

cd [klasör] *// Listelenen klasöre erişilir.*

get [dosya ismi] *// Dosyada yer alan kayıtları bilgisayara indirir.*

put [dosya ismi] *// Drone üzerinde erişilen dosyaya istenilen dosya yüklenir.*

[34]'de üçüncü bölümünde, saldırılardan korunmak için Parrot Bebop'un ağ ayarları sayfasında şifresiz iletişim yerine WPA 2 kullanılabileceği gösterilmiştir. Ancak uyarı olarak kullanılan basit parolaların da kırılabileceğini belirtilmektedir. Bunu uygulayarak göstermek için parola olarak password1234 seçilmiştir. Birinci bölümde yer alan komutların aynısını ve ek olarak sadece aircrack-ng komutunu kullanarak bu basit parola kırılmıştır. Ek olan komut ise şöyledir;

aircrack-ng -w /root/dictionaries/rockyou.txt /root/Desktop/DRONE-01.cap
// -w parametresi ile kullanılacak kelime listesinin bulunduğu dosya seçilir, son dosya yolu olarak da daha önceden -w parametresi ile kayıt edilen cap dosyası yazılır.

[34]'de kullanıcı, bu saldırıları Parrot Bebop üzerinde detaylı olarak anlatmıştır. Drone üzerinde gerçekleştirilebilecek WiFi, FTP saldırılarını anlatan güzel bir örnektir. Videoda drone olarak Parrot Bebop kullanılsa da, şifresiz iletişim kuran, FTP portu açık çoğu korunaksız drone üzerinde gerçekleştirilebilirdir. Ancak bazı firmalar, bu saldırıları önlemek için yapılan yeni güncellemeler ile bu güvenlik açıklarını kapatabilmektedir.

2.2.8. Parrot AR.Drone 2 - WiFi Saldırısı



Şekil 2.32: Parrot AR.Drone 2.0 Elite [35]

Drone: Parrot AR.Drone 2
Saldırı Yüzeyi: WiFi (FTP, Telnet)
Yazılım: Aircrack-ng Araçları, nmap, Wireshark

Szabo [36], Mayıs 2016 yılında, Budapeşte'de Ethical Hacking Conference isimli etkinlikte Parrot AR.Drone 2.0 ele geçirmeyi göstermiştir. Parrot AR.Drone 2.0 Elite görseli Şekil 2.32'de verilmektedir. Szabo [36] konferanstaki sunumunun anlatımını kendi Github hesabında ayrıntılı bir şekilde paylaşmıştır.

WiFi aracılığıyla dronun mobil uygulamasına bağlanıp hedef dronu kontrol edebilmiştir. drone açık yani şifresiz bir iletişim kurmaktadır. Szabo nmap aracı kullanarak drone üzerindeki açık porta sahip FTP ve Telnet servislerini tespit ettikten sonra FTP bağlantısını denemiştir. Basitçe herhangi bir kullanıcı adı veya şifre olmadan 192.168.1.1'e (drone IP) bağlanıp, kaydedilen videoları sakladığı drone dizinine erişmiştir. Szabo, Telnet ile root (en üst yetki sahibi) olarak erişim sağladıktan sonra bu noktada dronu düşürebileceğini ancak araca zarar vermemek için başka yöntem deneyeceğini söylemiştir.

Wireshark ile drone ve telefon arasındaki paket trafiğini analiz ettikten sonra pakette iki komut yakalamıştır: PCMD_MAG ve REF komutu. PCMD_MAG, dronun hızını her yönde ayarlar. REF, "take off", "emergency stop / reset" veya "land" gibi yüksek seviyeli komutlar vermek için kullanılmaktadır. Birden çok telefonun, dronu kontrol etmeye çalışmasını önlemek için, drone sadece kontrolörün kaynak IP'sinden gelen paketleri kabul eder (Kontrol cihazı, kontrol paketleri göndermeye başlayan ilk cihaz olarak tanımlanmaktadır.). Kaynak IP'yi kendi telefonu üzerine almak için REF komutunu kullanarak geliştirdiği python scriptleri ile sahte paket gönderip kontrolü ele geçirmiştir.

2.2.9. Maldrone



Şekil 2.33: Maldrone [37]

Drone: Parrot AR Drone 2.0, DJI Phantom

Saldırı Yüzeyi: Tersine Mühendislik (Arka kapı)

Nullcon Goa 2015 konferansındaki sunumda Rahul Sasi, dronlar için geliştirilen ilk arka kapı (backdoor) olma özelliği taşıyan payload'unu tanıtmıştır. Bu arka kapı Wi-Fi kontrollü Parrot AR Drone üzerinde denense de tüm linux arm sistemlerde çalışan dronlarda kullanılabilmektedir. Maldrone saldırısında kullanılan Parrot AR Drone 2.0 görseli Şekil 2.33'de paylaşılmıştır. Maldrone, dronu sıfırlamaya (reset) karşı kalıcı bir arka kapı oluşturmaktadır. Google'ın geliştirdiği GO dili ile de yazılmış bir program kullanılmıştır. Sasi [38] Maldrone'nu tanıtan bir blok yazısı kaleme almıştır. Bu yazıda Maldrone'nun özellikleri şu şekilde anlatılmaktadır;

- Maldrone bir drona sessizce kurulur
- Aygıt sürücüleri ve algılayıcılarıyla sessizce etkileşimde bulunur
- Bot ana denetleyicisini uzaktan drona izin verir
- Drone sahibinden Bot yöneticisine kaçış
- Uzaktan gözetim
- Diğer dronlara yayılma

Anlatılan tüm bu olumlu özellikler dışında Maldrone'nun kullanımda bir sınırı vardır. Maldrone dinamik bir analiz gerçekleştirememektedir. Bunun dışında Sasi, Samy Kamkar'ın geliştirdiği SkyJack exploiti ile kullanımında Maldrone'nun iyi arkadaş olabilecek bir payload olduğunu belirtmiştir.

2.2.10. NRF24L01 Modüllü DeviationTX Evrensel Uzaktan Kumanda



Şekil 2.34: NRF24L01 harici modülü ve Cheerson mini dronlar [25]

Drone: Birçok model (Attop, Bayang, Cheerson, Eachine, Floueron, Hisky, JJRC, JD, Syma & WLToys vb)
Saldırı Yüzeyi: RF (nRF24L01+)
Donanım: nRF24L01+, Walkera Devo TX(Devo 7e)

[39]'da bir blok adresinde yayınlanan makalede uzaktan kumandalı araçları (drone, helikopter, araba vb) ele geçirmeye yarayan evrensel kumanda yapımı anlatılmaktadır. Araç olarak Devo TX bir kumanda, açık kaynaklı bir yazılım ve 5$'lık bir modül kullanılmıştır. Kullanılan Walkera Devo TX, açık kaynaklı Deviation firmware ve NRF24 harici modülünün kombinasyonu ile evrensel kumanda oluşturulmuştur.

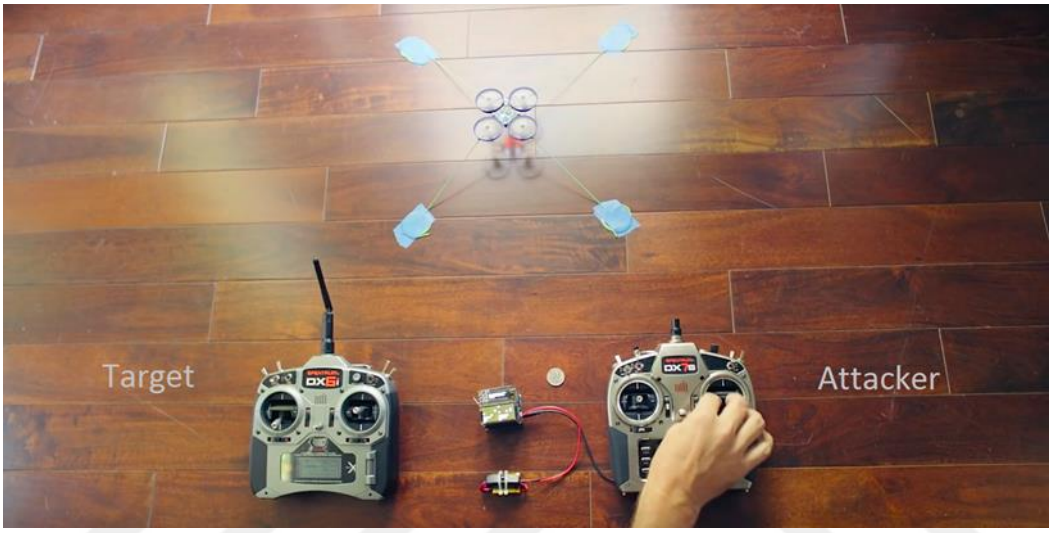
Walters [25] tarafından ise bu kumanda ile Attop, Bayang, Cheerson, Eachine, Floueron, Hisky, JJRC, JD, Syma & WLToys gibi birçok markanın araçlarının ele geçirilmesinin mümkün olduğu paylaşılmıştır. NRF24L01 harici modülü ve Cheerson mini dronlar görseli Şekil 2.34'de paylaşılmıştır.

RC oyuncak dronlarında kullanılan protokollerde güvenlik denetimi yoktur. Daha eski bazı dronlarda sabit adres kimliğine sahiptir ve en güçlü vericinin kaçırılması ya da drone ile etkileşime girmesini sağlayacak frekans atlaması kullanmamaktadır. Kumandaya entegre edilen NRF24L01+ modülü ile rastgele ID ve kanal atlaması oluşturarak sabit kimlik geçersiz kılarak, her başlatıldığında drone ve kumanda ile arasında bir eşleşme sağlamaktadır. Kurbandan önce bağlanmayı sağlayacak bir zaman aralığı vardır. Bu araçlarda ilk bağlanan kumanda kontrolü

sağlamaktadır. Gerçek kullanıcıdan önce kumanda ile eşleşme sağlarsanız kurbanın kumandası kullanılamayacaktır ve dronun kaçırılması gerçekleşecektir.

Yapılan çalışmada her ne kadar birkaç Devo TX modeli desteklense de, yazarın önerisi Devo 7e'dir. E modeli önemlidir. Çünkü bir Devo 7 DeviationTX uyumlu değildir. Bu model çok sayıda saldırı için en yaygın ve en ucuz Devo RC kontrol birimlerinden birisidir.

2.2.11. Icarus



Şekil 2.35: Icarus [40]

Drone: DSMx protokolünü kullanan birçok hobi / profesyonel drone ve RC araçlar
Saldırı Yüzeyi: RF

Icarus ile ilgili Öztürk [41] haberine göre, güvenlik araştırmacısı Jonathan Andersson, Icarus adını verdiği küçük bir cihaz geliştirmiştir. Bu küçük alet hali hazırda uçurulan bir dronu ele geçirmek için kullanılmaktadır. Alet sayesinde dronun asıl sahibinin kontrol mekanizması devre dışı bırakılabilmekte ve tüm kontrol saldırgana geçebilmektedir. Icarus'u anlatan görsel Şekil 2.35'de verilmiştir. Trend Micro şirketinde TippingPoint DVLab bölümü yöneticisi olan Andersson, bulduğu bu yeni yöntemi Tokyo'da 2016'da düzenlenen PacSec Güvenlik Konferansı'nda tanıtmıştır.

Bulunan yeni yöntemler sadece dronlar için kullanılmamaktadır. Radyo sinyalleri ile kontrol edebilen pek çok araç bu yöntemle ele geçirilebilir. Örneğin helikopterler, arabalar, tekneler yani kısacası günümüzde oldukça popüler olan kablosuz iletim kontrol protokolü (DSMx) kullanan bütün uzaktan kumandalı araçlarda işe yaramaktadır. Andersson'un bulduğu bu cihaz,

drone sinyallerinin arasına girmek için geliştirilen ilk cihaz değildir. Fakat bundan önce bulunan cihazlar, drone ile asıl kumandanın arasındaki bağlantıyı bozup, dronun işe yaramaz hale gelmesini sağlamaktadır. Andersson ise araya girdikten sonra dronu kullanım dışı bırakmadan ele geçirmeyi başarmıştır.

Icarus, DSMx'i istismar (exploit) ederek çalışmakta ve saldırganlara yavaşlama, hızlanma, yere indirme gibi bir drone kumandasıyla yapılabilecek bütün yetkileri vermektedir. Bunun mümkün kılan güvenlik açığı ise DSMx protokolünde bulunmaktadır. DSMx gizli anahtarı uzaktan kumandadan cihaza şifrelemeden göndermektedir. Bu da saldırganın araya girip bu gizli anahtarı çalmasına olanak sağlamaktadır. Icarus bahsi geçen gizli anahtarı ele geçirdikten sonra dronu kontrol eden asıl kumandaya zararlı paketler göndererek onu devre dışı bırakmıştır. Meşru kullanıcı devre dışı kaldıktan sonra drone saldırganın komutlarına yanıt vermeye başlamıştır [41].

2.2.12. E012 SDR Verici



Şekil 2.36: E012 SDR verici uygulama görseli [25]

Drone: Eachine E012 Mini Quadcopter
Saldırı Yüzeyi: RF (SDR)
Donanım: BladeRF X40 SDR , Wireless XBox 360 Gamepad
Yazılım: GNURadio, Qt 5.7

[42]'de SDR aracı kullanarak Eachine E012 mini Quadcopter'i kontrol edilme yöntemini paylaşılmıştır. Bu uygulamada araç olarak, BladeRF X40 SDR, wireless XBox 360 gamepad

ve gnuradio 3.7.11 kullanılmıştır. Kısa ve öz olan içeriği aşağıda adım adım aktarılacaktır. E012 SDR verici uygulama görseli Şekil 2.36'da verilmiştir.

İlk olarak Linux veya Windows üzerinde Gnuradio gfsk_tx.grc'yi açıp, daha sonra E012_transmitter.exe'yi oluşturup, Quadcopter'a pil bağlanıp çalıştırılmıştır. Sonraki aşamada bir oyun konsolu ile bağlantı kurulup, başlat düğmesine basılarak bind paketleri gönderilerek oyun konsolu çalıştırılmıştır. Konsol hareketleri ise şöyledir;

- Sağ analog irtifayı kontrol eder (throttle).
- Sağ hareketli düğme X ekseninde sağa ve sola hareketi kontrol eder (roll).
- Sağ hareketli düğme Y ekseninde yukarı ve aşağı hareketi kontrol eder (pitch).
- Sol hareketli düğme X , sağa ve sola dönüşleri (yaw) kontrol eder.

Uygulamayı gerçekleştirirken yürütülebilir dosyayı oluşturmada oyun konsolu desteği için Qt 5.7 ve bazı gereksinimler vardır. Visual Studio 2015 + Qt entegrasyon eklentisiyle e012_transmitter.sln, qmake veya Qt ile e012 transmitter.pro kullanılmalıdır.

2.2.13. Drone Sızma Testi



Şekil 2.37: DJI Mavic 2 Zoom [43]

Drone: DJI Mavic 2 Zoom
Saldırı Yüzeyi: Tersine Mühendislik
Donanım: USB Explorer 200 USB 2.0 Protocol Analyzer
Yazılım: Ghidra, IDA Pro

Edström ve Zeynalli [44]'nin hazırladığı çalışmada, DJI Mavic 2 Zoom üzerinde tersine mühendislik yöntemi ile zafiyet bulup, üretici DJI firmasına bildirmişlerdir. Yaptıkları incelemeler sonucunda DJI Mavic 2 Zoom ve kontrol kumandası arasında iletişimde WiFi protokollerinin kullanılmadığı, bunun yerine DJI sisteminde kullanılan DUML (DJI Evrensel İşaretleme Dili) tescilli protokolünü kullandığı belirtilmiştir. Protokolün donanım yazılımı yükseltmeleri, video iletimi, drone kontrolü vb. gibi çeşitli görevler için kullanıldığı da keşfedilmiştir. Uzaktan kumanda ve drone arasındaki iletişim OcuSync adlı şirket içi geliştirilmiş bir SDR uygulaması tarafından yönetilmektedir. Saldırıda kullanılan örnek DJI Mavic 2 Zoom görseli Şekil 2.37'de verilmiştir.

Çeşitli DJI dronlar ve kumandalarda, ürün yazılımı hem şifrelenir hem de dijital olarak imzalanır. Bu, yetkisiz aygıt yazılımı dosyalarının SoC-sistem yongasına flash olarak gönderilmesini önlemek içindir. Araştırmacılar, Ghidra ve IDA Pro gibi araçları kullanarak, donanım yazılımı yükseltmelerinden (upgrade) sorumlu tersine mühendislik dosyalarıyla, yükseltme sırasında drone / uzaktan kumandaya bir imza dosyasının gönderildiğini keşfedilmiştir. Hem imza hem de ürün yazılımı dosyalarının DJI tarafından dijital olarak imzalandığı ve ilgili cihazlarda doğrulandığı tespit edilmiştir. Bu dosyalardan bazıları şifrelenebilirdir. Firmware dosyalarının binary yapısı hakkındaki bilgiler, firmware dosyalarını işleyen ve şifresini çözen tersine mühendislik prosedürleri aracılığıyla keşfedilmiştir.

Çalışma bulgularına göre, hem imza hem de firmware dosyaları, sihirli sabit "IM*H" ile başlayan, DJI tarafından geliştirilen binary bir yapıda paketlenmiştir. Kullanılan şifreleme anahtarı "enc_key" girişi ile belirlenmiştir. İlk imza dosyasında olduğu gibi yapının hiç şifrelenmemesi de mümkündür. Veriler şifrelenmişse, "enc_key" içinde belirtilen anahtar ile "scram_key" içindeki verilerin şifresi çözülerek bir anahtar türetilmektedir. Şifre çözme, blok şifresi olarak CBC ile ve sıfır başlatma vektörüne sahip olan simetrik şifreleme şeması 128-bit AES uygulanarak gerçekleştirilmiştir. Önceden türetilmiş anahtarı ("scrum_key") kullanarak, sıfır başlatma vektörü ile 128-bit AES ile veri yığınlarının şifresini çözmenin mümkün olduğu belirtilmiştir. Çalışmada yapılan değerlendirmeye göre firmware dosyalarının şifresi çözüldüğünde, drone / uzaktan kumanda üzerinde çalıştırılacak programların yanı sıra SDR firmware üzerinde tersine mühendislik saldırısı yapmak mümkündür.

Ek olarak araştırmacılar, firmware analizleri sonucunda GPS dosyalarına erişmişlerdir. Uydudan şifresiz veri iletimi yapan GPS protokolünün spoofing saldırılarına açık olduğu

belirtilmiş, ancak GPS spoofing saldırısı uygulanmamıştır. Daha önce gerçekleştirilen GPS spoofing saldırıları örnek gösterilerek DJI Mavic 2 Zoom için de GPS protokolünün saldırı yüzeyi olacağı varsayılmıştır [44].

2.2.14. İnsansız Hava Araçlarının Güvenlik Açıkları ve Karşı Önlemler



Şekil 2.38: DJI Phantom 4 Pro Drone [45]

Drone: DJI Phantom 4 Pro
Saldırı Yüzeyi: Tersine Mühendislik (Cracking DJI SDK)(1), GPS (Spoofing) (2)
Donanım: LabSat3 kiti(2), RLACS198 Anten(2)
Yazılım: Jd-gui(1), Java bytecode editör(1), rkflashtool(1), LabSat SatGen(2)



Şekil 2.39: Parrot Bebop 2 Drone [46]

Drone: Parrot Bebop 2
Saldırı Yüzeyi: WiFi (Telnet, FTP), Tersine Mühendislik
Yazılım: Airdump-ng araç seti, Nmap

Dey ve diğ. [47], DJI Phantom 4 Pro ve Parrot Bebop 2 güvenlik açıklarını araştırmıştır. Yapılan incelemelere göre dronların güvenlik düzeyi karşılaştırılmıştır. Daha sonra saldırılara karşı alınabilecek önlemler sıralanmıştır. Hedef dronlar, DJI Phantom 4 Pro görseli Şekil 2.38'de, Parrot Bebop 2 görseli Şekil 2.39'da paylaşılmıştır.

DJI Phantom 4 Pro üzerinde GPS spoofing ve tersine mühendislik saldırıları uygulanmıştır. Cracking DJI SDK saldırısı, DJI uygulaması ve DJI sunucusu arasındaki kimlik doğrulamanın kaldırılmasına dayanmaktadır. DJI sitesinde, özelleştirilmiş Android ve iOS uygulamaları oluşturmak için bir SDK sunmaktadır. Bu, kodun bölümlerinin derlenmesi ve yamalanması yoluyla SDK'nın değiştirilmesini sağlamaktadır. İncelemeleri sonucunda DJI Go'nun veya DJI-SDK kullanan herhangi bir özelleştirilmiş uygulamanın ilk kullanımı, bir kerelik kayıt ve aktivasyon gerektiği anlaşılmıştır. Araştırmacılar daha sonra DJI'ın sitesinden indirdikleri DJI SDK kütüphane jar dosyasını Jd-gui ile decomplier etmişler ve Java bytecode editör ile kodu düzenlemişlerdir. Kimlik doğrulama ile ilgili elde ettikleri 2 fonksiyonu (shouldAllowAccessSDK(), hasSDKRegistered()) daha fazla izin denetimi yapmaması için her zaman true değerini döndürecek şekilde düzenlemişlerdir. Böylece DJI uygulaması ve DJI sunucusu arasındaki kimlik doğrulamasını etkin bir şekilde kaldırmışlardır.

Çalışmada, DJI firmware'in şifrelenmiş ve dijital olarak imzalandığı tespit edilmiştir. Araştırmacılar daha sonra rkflashtool aracı ile DJI firmware'in binary dosyasını unpacked işlemi ile çıkartmış ve bazı imaj(image) dosyalarına ulaşmıştır. Çıkan embedded-update.img dosyası ayrıca boot.img, recovery.img, system.img dosyalarına çıkartılmıştır. Ancak araştırmacılar, binary dosyanın şifresi tamamen çözülmemiş veya standart araçlar tarafından çıkartılamamış (unpacked) olduğu için bu noktadan sonra ilerleyememişlerdir.

Çalışmada uygulanan bir diğer yöntemde, DJI Phantom 4 Pro üzerinde GPS saldırı yüzeyi kullanılarak GPS spoofing saldırısı gerçekleştirilmiştir. Araştırmacıların aktardıklarına göre, DJI Phantom 4 Pro, J/N izleme yardımıyla jamming tespit etme yeteneğine sahip u-blox NEO 8M GPS alıcısı ile birlikte gelmektedir. J/N izleme, alınan güç tetikleme eşiğinden fazlaysa alarmı tetikleyerek, jamming ve ardından spoofing türünde bir saldırıyı önlemektedir. DJI'ın geliştirdiği bu önleme rağmen araştırmacılar GPS spoofing saldırısını gerçekleştirmişlerdir. İlk olarak, LabSat kiti ile sağlanan aktif anten RLACS198 kullanılarak gerçek GPS sinyalleri kaydedilmiştir. LabSat ile sağlanan SatGen yazılımını kullanılarak da sahte GPS sinyalleri

üretilmiştir. Dronun konumu, LabSat tarafından başarıyla taklit edilmiştir. İletilen sinyalin gücü çok düşük olduğundan, DJI Phantom 4 Pro, J/N izlemeli bir u-blox GPS modülüne sahip olmasına rağmen spoofing tespit edilememiştir. Saldırı senaryosu olarak sahte GPS konumunu Yasak Bölge (NFZ - No Fly Zone)'ye gönderme ve yasak bölgeye iniş yapması gibi senaryolar denenmiştir. Asıl konumu Singapur'da olan drone, GPS spoofing saldırısı sonucunda konumunun NFZ alanı olan Changi havalimanında olduğu gösterilmiştir.

Araştırmacıların Parrot Bebop 2'de buldukları zafiyetlerin çoğu ise WiFi saldırı yüzeyinde gerçekleştirilmiştir. Parrot Bebop 2 ile kontrol uygulaması arasındaki iletişim açık WiFi protokolü ile yapılmaktadır. Parrot üreticilerinin WPA/WPA2 özelliği eklemeyi tanıtmıştır, ancak bu özellik ile menzil ve hızın açık bir şekilde düştüğü aktarılmıştır. Bu özellik ile de saldırılara karşı savunmasızdır. Zayıf parolalar aircrack-ng gibi araçlarla kırılabilir. Araştırmacılar, nmap ile ağ taraması yaptığında FTP, Telnet ve Tor-SOCKS servis portlarının açık olduğunu görmüşlerdir.

Herhangi bir kimlik doğrulama olmadan bağlanılan Parrot Bebop 2'ye birden fazla istemci bağlanabilmekte ve kontrol edebilmektedir. Dahası, airodump-ng araç seti kullanılarak deauthentication saldırısı düzenlenmektedir. Böylece asıl kullanıcının dronu kontrol etmesi önlenmekte ve saldırganın kontrol etmesi sağlanmaktadır.

Çalışma bulgularına göre herhangi bir doğrulama olmadan bağlantı sağlayan telnet üzerinden dronun dosya sistemlerine root yetkisiyle erişim sağlanabilmektedir. Tüm sistemi kontrol eden dragon-prog işlemi sonlandırılarak drone motoronun durması ve aniden yere çakılması sağlanabilir. Ayrıca, araştırmacıların keşfettiği /usr/bin/ardrone3 shutdown.sh ve usr/bin/DragonStarter.sh gibi dronun açılmasını ve kapatılmasını sağlayan scriptler ile dronun yere çakılması sağlanabilir.

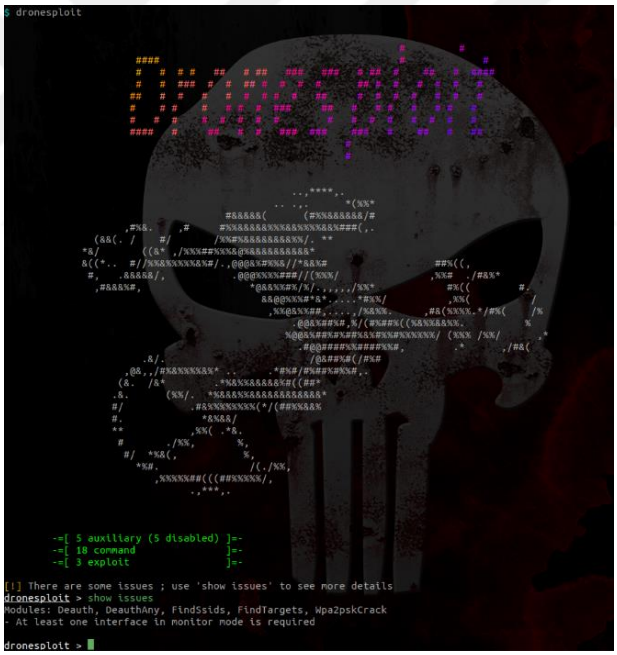
Araştırmacıların bulduğu FTP servisinin açık portu ile herhangi bir kimlik doğrulama olmadan saldırganların WiFi'ye bağlanabileceği ve medya, uçuş verileri gibi kişisel verileri çalmak için FTP'ye giriş yapabileceği aktarılmıştır. Fabrika ayarlarına göre FTP ile sadece görüntülerin, videoların ve diğer yararlı dosyaların (örn. pud dosyaları) kaydedildiği /data/ftp/internal 000 FTP dizinine erişim izni verilmiştir. Araştırmacılara göre sınırlı FTP erişimi ile /etc/inetd.conf dosyası saldırgan tarafından düzenlenerek ele geçirilebilir.

Parrot Bebop 2 dronun bir diğer saldırı yüzeyi ise tersine mühendislik saldırılarıdır. Çalışma sonuçlarına göre Bebop 2 donanım yazılımının (firmware) tamamen tersine çevrilebilir,

kolayca değiştirilebilir ve yeni binary dosya yeniden yüklenebilirdir (reflash). Donanım yazılımının tersine çevrilmesi, saldırganın güvenlik açıklarından yararlanmasını ve belirli yerleri hedeflemesini kolaylaştıran drone iş akışı ve dosya sistemi hakkında fikir vermektedir.

Hem Phantom 4 Pro hem de Bebop 2 dronlarının güvenlik özelliklerinin analiz edildiği çalışma sonucunda, Phantom 4 Pro dronun Bebop 2 drondan daha güvenli olduğu vurgulanmıştır. Phantom 4 Pro'da GPS spoofing saldırısı için gerekli olan araçların maliyetli olması, donanım yazılımını şifrelemesi ve imzalaması, FPGA video şifreleme algoritmasına sahip olması bakımından daha güvenli bulunmuştur. Bebop 2'nin ise çeşitli kablosuz saldırılara karşı savunmasız olması ve çabuk ulaşılabilen açık kaynak araçlar ile kolayca ve maliyetsiz saldırıların gerçekleştirilmesi sebebiyle daha savunmasız olduğu vurgulanmıştır.

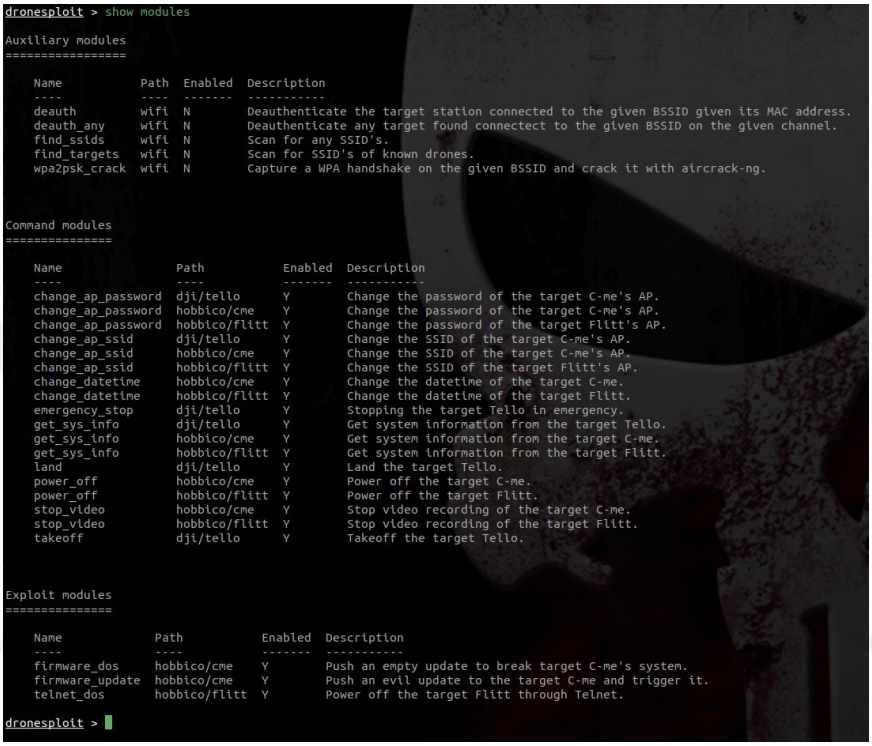
2.2.15. DroneSploit ile Drone Hackleme



Şekil 2.40: DroneSploit konsol ekranı [48]

Drone: WiFi kontrollü ticari dronlar (AR Drone, DJI Tello, Mavic Mini, Hobbico C-me, Hobbico Flitt vb.)
Saldırı Yüzeyi: WiFi (FTP, Telnet, Deauthentication ve parola bulma saldırıları)
Yazılım: DroneSploit

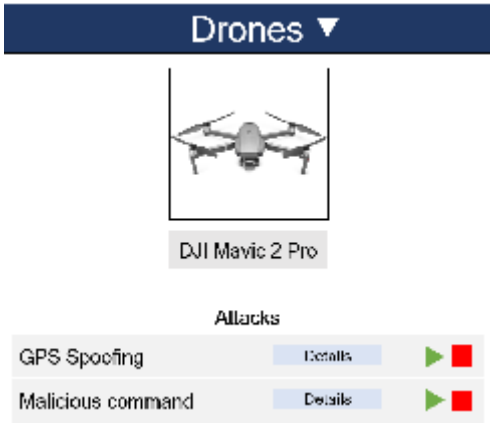
2019 yılındaki BlackHat konferansında WiFi kontrollü ticari dronlar için geliştirilmiş DroneSploit: Drone Pentesting frameworkü sunulmuştur. DroneSploit, WiFi iletişimli ticari dronlara yapılan saldırıları otomatize eden metasploit benzeri olarak geliştirilmiş bir araçtır. Radyo kontrollü dronları kapsamamaktadır. [48]'de Github'da açık kaynak olarak paylaşılmaktadır. DroneSploit konsol ekranı Şekil 2.40'da gösterilmiştir.



Şekil 2.41: DroneSploit modül ekranı [48]

DroneSploit, her WiFi iletişimli dronu kapsamamaktadır. DJI Tello, Hobbico C-me, Hobbico Flitt için drona özgü saldırıları ve WiFi saldırılarını otomatize etmek için hazır modüller geliştirilmiştir. Dronlarda bulunan açık port (FTP, Telnet), zayıf veya dafault parola kullanımı, şifresiz iletişim gibi dronlara özgü zafiyetleri içerisindeki hazır modülleri kullanarak tarama, deauthentication ve parola bulma saldırıları yapılmaktadır. DroneSploit modül ekranı Şekil 2.41'de paylaşılmıştır. Saldırılar sonucunda drone SSID'si değiştirilebilir, drone kontrol edilebilir veya kapatılıp yere çakılabilir. Bunun dışında yeni modüller eklenerek tanımlı olmayan dronlar dışındaki dronlara da saldırı geliştirme imkanı sunmaktadır. Geliştirici ekibin hedefleri arasında drone kapsamının artırılması, yeni saldırı özelliklerinin eklenmesi ve radyo kontrollü dronlar için de saldırı yöntemlerinin geliştirilmesi bulunmaktadır.

2.2.16. DRAT: Güvenlik Açığı Değerlendirmesi için Drone Saldırı Aracı

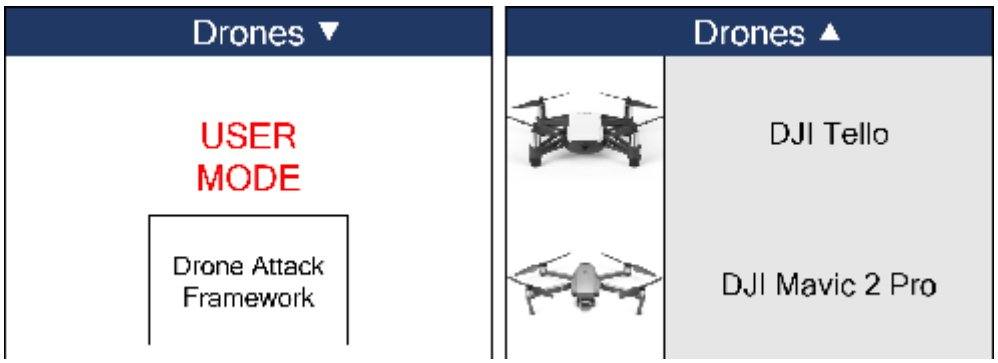


Şekil 2.42: DRAT saldırı listesi [49]

Drone: DJI Mavic 2 Pro

Saldırı Yüzeyi: GPS (GPS Spoofing), Tersine Mühendislik (Malicious)

Bin Mohammad Fadilah ve diğ. [49] tarafından sunulan DRAT (A Drone Attack Tool) Framework'ü, dronlara yönelik güvenlik değerlendirilmesinin yapılması amacıyla geliştirilen bir başka sızma testi (pentest) aracıdır. DRAT kullanıcı dostu bir arayüz sunmaktadır. Kullanıcıların arayüz üzerinden komutlara gerek kalmadan kolayca drone saldırılarının yapılmasını sağlamaktadır. DRAT saldırı listesine gösteren görsel Şekil 2.42'de verilmiştir.



Şekil 2.43: DRAT - Kullanıcı mod arayüzü [49]



Şekil 2.44: DRAT - Geliştirici mod arayüzü [49]

Araç, kullanıcı modu ve geliştirici modu olmak üzere iki moddan oluşmaktadır. DRAT kullanıcı mod arayüzü Şekil 2.43'de, geliştirici mod arayüzü görseli Şekil 2.44'de gösterilmiştir. Tipik bir kullanıcı, açılır menüden drone listesi seçebilmektedir. Bir drone seçtiğinde, kendisine gerçekleştirilebilecek saldırıların bir listesi sunulmaktadır. Geliştirici modda, kullanıcı testi için araca yeni dronlar ve saldırılar eklenebilmektedir.

Çalışmada DJI Mavic 2 dronuna odaklanılmıştır. Bu drona karşı geliştirilecek tekrarlama saldırısı (replay attack), GPS Spoofing, yan kanal saldırılarına (zararlı android uygulaması) örnek verilmiştir. Araç, araştırma ve geliştirme aşamasındadır. Araştırmacılar, gelecekte yeni drone ve saldırı yöntemlerinin eklemeyi hedeflemektedir.

2.3. GÜVENLİK ANALİZİ

Genel kısımların ilk iki bölümünde askeri ve sivil alanlarda yaşanan drone hackleme örnekleri incelenmiştir. Yaşanılan ve gelecekte yaşanılması kuvvetle muhtemel olan insansız hava saldırıları olaylarını önlemek için çeşitli çözümler üretilmiştir. Sınırlı alanlarda, haritalama, gözetim, arama, izleme, hackleme ve hatta saldırı işlemleri gibi çeşitli görevleri yerine getirmek ile birlikte uzaktan emirlere de uyabilen, donanım tabanlı araçlardan oluşturulan sistemler hala geliştirilmektedir. Çoğunluğu askeri alanda insansız hava aracı saldırılarına karşı geliştirilen bu çözümler, konu kapsamı dışında olduğu için bu çalışmada incelenmeyecektir. Ayrıca, askeri amaçlı kullanılan gelişmiş İHA sistemlerinin çeşitliliği ve ayrı bir tez çalışması olabilecek önemli bir konu olması sebebiyle İHA sistemlerinin güvenlik analizi bu tez için kapsam dışında

tutulmuştur. Tüm bölümlerde, çoğunlukla sivil alanda ticari ve hobi amaçlı kullanılan dronların güvenliği üzerine yoğunlaşılmıştır.

İnsansız hava araçlarındaki her bir bileşen ve kullanılan her bir teknoloji bir saldırı alanı oluşturmaktadır. Bu alanlara yönelik gerçekleştirilebilecek tüm tehdit ve saldırılar derinlemesine araştırma gerektirmektedir. İnsansız hava araçları, İHA tiplerine, kontrol türlerine ve kullanım amaçlarına göre çeşitli şekillerde sınıflandırılmaktadırlar. Askeri, ticari, finansal ve kişisel amaçlar ile hedef haline getirilmektedirler. Dronlara ve İHA Sistemlerine yönelik gerçekleştirilen saldırılarda yazılımları, donanımları, kontrol cihazları, iletişimleri, verileri ve doğrudan insansız hava araçlarının kendileri hedef alınmaktadır. Çeşitli siber saldırı yöntemleri ile hedef alınan drone ve İHA sistemlerine yönelik saldırıların kapsamı ve karşı tedbirleri farklı olmaktadır. Bu bölüm içerisinde dronlara yapılan çeşitli saldırı türlerine yönelik alınacak karşı tedbirler aktarılacaktır.

2.3.1. MAVLink Protokolü Güvenlik Analizi

Yer Kontrol İstasyonu (GCS) tabanlı drone kontrolü için en yaygın kullanılan protokollerden biri olan Mikro Hava Aracı Bağlantısı (MAVLink) protokolü en ünlü İHA protokolüdür. 2009 yılında Lorenz Meier tarafından geliştirilen mesaj tabanlı bir İHA iletişim protokolüdür. Bu protokol, mevcut DroneCode projesinin bir parçasıdır ve binlerce geliştirici tarafından kullanılmaktadır. Ardupilot Mega, pxIMU Autopilot ve SLUGS Autopilot gibi çok sayıda otopilot tabanlı sistemde de kullanılır. MAVLink paketleri, bir İHA ve bir GCS arasında çift yönlü olarak başlık tabanlı mesajlar olarak aktarılır. GCS, İHA'ya görev komutları gönderir ve İHA, sensör değeri ve mevcut konum dahil durum bilgilerini GCS'ye iletir [50].

MAVLink çok verimli bir protokoldür. MAVLink 1 ve MAVLink 2 olmak üzere iki sürümü vardır. MAVLink 1, başlangıç işareti ve paket bırakma tespiti dahil, paket başına yalnızca 8 bayttır. MAVLink 2, yalnızca 14 bayt ek yüke sahiptir (ancak çok daha güvenli ve genişletilebilir bir protokoldür). MAVLink, herhangi bir ek çerçeveleme gerektirmediğinden, çok sınırlı iletişim bant genişliğine sahip uygulamalar için çok uygundur [51].

MAVLink protokolünün güvenlik zafiyetleri İHA topluluğu arasında iyi bilinmektedir. Protokol ne kimlik doğrulama ne de şifreleme içermez. MAVLink protokolünün daha yeni sürümleri için çeşitli çözümler önerilmiştir. Ancak bu çözümler tam olarak uygulanmamıştır.

Ek olarak, MAVLink yapısal sınırları ve performans kısıtlamaları diğerlerini MAVLink'den vazgeçmeye ve GIDL gibi özel protokoller geliştirmeye itmiştir [52].

Marty [53], MAVLink protokolünün güvenlik zafiyetlerini kapsamlı bir şekilde inceleyen Amerikan Hava Kuvvetleri Teknoloji Enstitüsü'nde yayınlanan tez çalışmasını paylaşmıştır. Araştırmada MAVLink protokolünü kullanan insansız hava aracı ile yer kontrol istasyonu arasındaki iletişimdeki gizliliği, bütünlüğü ve kullanılabilirliği tehlikeye atan üç istismar sunulmaktadır. Ek olarak, MAVLink protokolünün bütünlüğe yönelik saldırılara karşı savunmasızlığı, saldırganın İHA'yı GCS'inden etkin bir şekilde ele geçirmesine izin verdiği gösterilmiştir. Dahası, MAVLink protokolünün GCS'i tarafından kontrol edilecek bir İHA'nın DoS saldırılarına karşı kırılganlığı gösterilmiştir. Ağ saldırıları olarak Hedefe Erişme (Yerel ve Uzaktan Saldırılar), Ortadaki Adam Saldırısı (Dinleme ve Hijacking) ve Hizmet Dışı Bırakma saldırıları (DoS Saldırısı – Denial Of Service Attack) incelenmiştir. Araştırmada MAVLink protokolünü güvenceye almak için kullanılabilecek dört farklı şifreleme uygulaması önerilmektedir: NaCl, AES-GCM, Rabbit cipher ve XXTEA. Bu araştırma, önerilen bu çözümlerin hiçbirini doğrulamamasına rağmen, MAVLink protokolünü gerçekten güvence altına aldığı belirtilmiş ve önerilen çözümlerin uygulanmasının maliyetini değerlendirmek için ileride incelenmek üzere deneysel olarak test etmiştir. İki noktaya dikkat çekilmiştir; Birincisi, NaCl ve AES-GCM tarafından sağlanan kimliği doğrulanmış şifreleme, İHA'nın OSI Katman-2 ve üstü iletişim ile ilgili olarak mevcudiyetini korumasına rağmen, İHA, C^2 iletişimini güvenceye almak için kullanılan yöntemden bağımsız olarak OSI Katman-1 saldırılarına karşı savunmasız kalmaktadır (örneğin, frekans jamming). İkincisi, erişebilirlik, seçilen savunma protokolünden bağımsız olarak UHF kanalının içeriğinden de etkilenmektedir. MAVLink protokolünün güvenliğini sağlama maliyetini ağ gecikmesi, güç tüketimi ve yararlanma başarısının ölçülmesi yoluyla ölçmek için bir metodoloji önerilmiştir. Bu araştırmada yapılan testlerde, APM 2.5'in, NaCl ve muhtemelen başka kriptografik yöntemler kullanarak MAVLink C2 protokolünü emniyete almak için yeterince donatıldığı gösterilmiştir.

Won ve diğ. [54], dronlar ve akıllı nesneler arasında güvenli iletişim protokolü sunmaktadır. Kimliği doğrulanmış anahtar, inkar edememe ve kullanıcı iptali gibi gerekli güvenlik işlevlerini desteklemek için Certificateless Signcryption Tag Key Encapsulation Mechanism (eCLSC-TKEM) önerilmektedir. eCLSC-TKEM akıllı nesnede hesaplama yükünü en aza indirerek drone ve akıllı nesne arasında paylaşılan bir anahtar oluşturmak için gereken süreyi azaltmaktadır. Ayrıca, araştırmacılara göre protokol birçok akıllı nesnenin aynı anda eCLSC-TKEM yürütmesine izin veren çift kanal kullanarak dronun verimliliğini artırmaktadır.

Protokol piyasada bulunan AR. Drone2.0 ve TelosB üzerinde test edilmiştir. Deneysel sonuçlarında protokolün, diğer protokoller [55]'deki CLSC-TKEM, [56]'daki CL-AKA ve [57]'deki CL-AKA'dan sırasıyla 1.3, 1.5 ve 2.8 kat daha iyi olduğu iddia edilmektedir.

Rajatha ve diğ. [58], Yer Kontrol İstasyonu (GCS) ve Mikro Hava Aracı (MAV) arasındaki iletişim için MAV iletişim protokolünde güvenliğin artırılmasını önermektedir. Önerilen yöntem, güvenli bir anahtarla Sezar veri şifreleme yönteminin uygulanmasını içermektedir. Şifreleme yöntemi, iletişimin başında Mikro Hava Aracı'nın kimlik doğrulaması için kullanılır. Daha sonra aynı, çeşitli frekanslarda kritik komut, kontrol ve parametre mesajları için kullanılır. Yazarların amacı, savunma ve diğer yüksek güvenlik gerektiren uygulamalarda sistemin güvenliğinin ve güvenilirliğinin artırılmasıyla sonuçlanmasıdır. Önerilen şemada, Sezar şifreleme kullanılarak MAVLink iletişiminin doğrulanması tasarlanmış, mesaj parametreleri, MAVLink kontrol ve komut mesajlarından oluşan simülasyon şeması için simüle edilmiştir. Sonuç yazarlar için oldukça tatmin edicidir ve pratik uygulamada büyük potansiyele sahip olduğu belirtilmiştir. Makaleye göre, bu teknik kullanılarak, GCS ve MAV arasında güvenli iletişim oluşmaktadır. GCS tarafından oluşturulan veriler, GCS tarafından oluşturulan şifreleme metnine benzer bir şifre metni gönderilerek doğrulanmadıkça MAV tarafından alınmamaktadır. Bu yöntemin MAVLink protokolünde uygulanması, savunma uygulamaları gibi güvenliğin önemli bir rol oynadığı uygulamalarda MAVLink protokolünün kullanılmasına neden olacaktır. Ancak yazarlara göre bunun için çeşitli senaryolarla ayrıntılı test ve doğrulama gerekmektedir. Aynı durum birkaç uçuş aracı kurulumunda tekrarlanmalıdır.

Hamsavahini ve diğ. [59] yazarlar da, GCS ve MAV arasındaki iletişim için MAV iletişim protokolünde güvenliğin artırılmasını önermektedir. Önerilen yöntem [58]'deki çalışmaya benzer şekilde, güvenli bir anahtarla Sezar veri şifreleme yönteminin uygulanmasını içermektedir. Çalışmaları sonucunda, herhangi bir yetkisiz erişim olmayacak şekilde Sezar şifreleme kullanılarak iletişimi güvence altına aldıklarını iddia etmişlerdir. Bu yöntem ile korunacak komutlar hayati önem arz edebilecek GPS koordinat bilgilerini içermektedir. Bu nedenle, MAV'ın sadece GCS'ye iletişimin canlı olduğunu göstermekle kalmadığı, aynı zamanda kalp atışı (heartbeat) paketi ile birlikte yerini düzenli olarak bildirdiği vurgulanmaktadır. Çalışmada ek olarak kullanıcı dostu bir arayüz geliştirilmiştir. Ayrıca kullanıcı, bu arayüzü uygulamalarına göre değiştirebilmektedir. Çalışma sonucunda geliştirilen protokolün hafif (lightweight) olduğunun kanıtlandığı savunulmuştur.

Davanian ve diğ. [52], dronlar için güvenlik çözümünün gereklilikleri değerlendirmiş ve daha sonra geleneksel şifreleme çözümlerinin dronun trafik hacmi ve enerji tüketimi üzerindeki etkisini analiz etmiştir. Hareketli Hedef Savunması (Moving Target Defence) ile, drone güvenliği için taşınabilir ve ek yükü olmayan yeni bir talimat çeşitliliği çözümü önerilmiştir. Bu çözüm genel amaçlı ve hedefe yönelik saldırılara karşı makul bir güvenlik sunarken, sıfır performans ek yükü sağlamaktadır. Çalışma içeriğinde İHA ele geçirme örnekleri ve MAVLink için mevcut güvenlik çözümleri incelenmiştir. Sonraki bölümlerde İHA sistemleri için tehdit modeli, güvenlik çözümlerinin İHA sistemleri için göz önünde bulundurması gereken performans kısıtları incelenmiştir. Tehdit olarak İHA sistemlerine kaba kuvvet saldırıları (brute force attack) ve dinleme saldırılarına odaklanılmıştır. Sonrasında güvenlik analizleri sunulmuş ve İHA çözümü geliştirilmiştir. İHA saldırılarına sağlam bir çözüm olarak, MAVLink komutunun belirtilen tehditlere karşı dirençli olacak rastgele permütasyondaki argümanları da içermesi önerilmiştir. Makalede bu çözümün, kaba kuvvet saldırısının arama alanını, pratikte kaba olmayan bir kaba arama yapmayı olanaksız kılan 256 bite (Message ID + Payload) yükselteceği ve bilinen düz metin saldırılarının da etkili olmayacağı belirtilmiştir. Dahası, bu çözümün talimat yükü (payload) kesinlikle SHA ve AES'den daha az olduğu; bu çözümün bir yükü yeniden inşa etmesi gereken 256'dan daha fazla şifreleme talimatı gerektirdiği belirtilmiştir. Son olarak, çözümlerinin mevcut çözümlerden daha iyi performans gösterdiğini ve saldırganlara karşı nasıl kabul edilebilir bir savunma sunduğu savunulmuştur. Saldırganlar bazı komutları bulmada kısmen başarılı olsalar bile, olaya müdahale etmenin mümkün olduğu, çünkü saldırının gizli olmadığı aktarılmıştır.

Allouch ve diğ. [60], MAVLink protokolünün güvenlik açıklarını ele almakta ve MAVLink için İHA'lar ve GCS'ler arasında paylaşılan MAVLink mesajlarının korunmasını sağlamak için şifreleme algoritmalarının kullanımını artıran, güvenlik entegre bir mekanizma olan MAVSec'i önermektedir. İHA'lar ve GCS'ler arasında paylaşılan mesajların gizliliğini sağlamak için şifreleme mekanizmalarına sahip MAVLink'in geliştirilmiş bir versiyonu olarak tanımlanmıştır MAVSec. MAVLink protokolünde uygulanabilecek, yakalama (sistem gizliliğine karşı saldırılar), değiştirme (sistem bütünlüğüne karşı saldırılar), hizmet reddi (sistem erişebilirliğine karşı saldırılar) gibi olası farklı tehdit yöntemleri incelenmiştir. MAVSec'i doğrulamak için araştırmacılar Ardupilot'da uygulamış ve farklı şifreleme algoritmalarının (AES-CBC, AES-CTR, RC4 ve ChaCha20) performansını bellek kullanımı ve CPU tüketimi aralıklarıyla değerlendirilmiştir. Deneysel çalışma, MAVLink kaynak kodunda şifreleme algoritmaları kullanılarak gerçekleştirilmiştir. Sonuçlar, ChaCha20'nin daha iyi bir performansa sahip

olduğunu ve diğer şifreleme algoritmalarından daha verimli olduğu aktarılmıştır. ChaCha20'yi MAVLink'e entegre etmenin, daha az bellek ve CPU tüketimi tüketirken, performansını etkilemeden mesajların gizliliğini garanti altına alınabileceği, böylece belleği ve pili, kaynak kısıtlamalı drone için koruyacağı savunulmuştur.

2.3.2. Dinleme Saldırılarına Karşı Önlemler

Drone ağları çeşitli güvenlik tehditlerinden ve sorunlarından muzdariptir. Drone iletişiminde gizlice dinleme, trafik analizi ve ağ saldırılarında verilerin açık metin olarak iletildiği durumlarda saldırganlar kolaylıkla verilere erişebilmektedir. Bu gibi durumlar için kriptografik yöntemler önerilmektedir. Kriptografik yöntemler, bilginin gizliliğini korumanın yanı sıra ileten kaynağın kimliğini doğrulamak için etkin bir şekilde kullanılabilir. Simetrik şifreleme, özellikle seçilen düz metin/şifreli metin saldırıları açısından güvenlik sorunlarından muzdaripken, asimetrik şifreleme, depolama ek yüküne ek olarak yüksek hesaplama ve kaynak yükünden muzdariptir. Geleneksel kriptografik yöntemler, veri aktarım hızı, paket büyüklüğü vb. iletim maliyetlerini artırmaktadır. Pille çalışan cihazlarda uzun mesafelerde çalışan drone iletişiminin güvenliği, hafif (lightweight) kriptografik algoritmalar ve protokoller gerektirmektedir. Mevcut gizliliği koruyan kimlik doğrulama protokolleri, minimum gecikme için bu tür hafif şifreleme algoritmalarından yararlanabilir. Ayrıca, çok faktörlü kimlik doğrulama için fiziksel katman parametreleri kullanılabilir [61].

Chen ve diğ. [62], İHA iletişim kontrol sistemleri için İzlenebilir ve Gizliliği Koruyan Kimlik Doğrulama (TPPA) şemasını sunmaktadır. TPPA, İHA uygulamaları için Eliptik Eğri Şifreleme (ECC), dijital imza, hash fonksiyonu ve diğer şifreleme mekanizmalarını entegre etmektedir. Bu şema, özellikle DoS ve spoofing saldırılarına karşı düşük hesaplama ve iletişim maliyetleriyle gizlilik, bütünlük, erişebilirlik, anonimlik ve reddedilmeme sağlamaktadır.

Dinleme saldırılarına karşı diğer yöntem ise FSSS (Frekans Atlamalı Yayılma Spektrumu) ve DSSS (Doğrudan Dizi Yayılım Spektrumu) [63]. Bu yöntemlerin düzgün çalışması için, verici ve alıcı tarafından önceden bilinen bir yayılma koduna veya atlama düzenine ihtiyaç vardır. Sonuç olarak, yayılma kodu veya atlama düzeni hakkında bilgisi olmayan birinin iletişimi dinlemesi zordur.

2.3.3. Deauthentication Saldırılarına Karşı Önlemler

Hizmet Dışı Bırakma (DoS) saldırısı, bir saldırganın hedefi isteklerle doldurması ve erişebilirliğini kesintiye uğratmak için kaynaklarını aşırı yüklemesi anlamına gelir. Dronun şifresiz veya WEP tarafından korunan kablosuz erişim noktalarına erişmek son derece kolay olduğundan hedef nokta olarak seçilir. Böyle bir saldırının dronlar üzerindeki etkileri, pilin bitmesi, artan gecikme, zayıf uygulama performansı, düşük video akışı kalitesi, aşırı ısınma, motorun durması ve bunların sonucunda çakılması olabilir. Drone ve yer kontrol istasyonları arasındaki iletişim bu saldırıya karşı oldukça savunmasızdır. Bu iletişimler genellikle WiFi bağlantıları aracılığıyla yapılır.

Dronlar esasen uçan erişim noktalarıdır. Özünde kullanıcı ve drone kendi ağlarını oluştururlar. WPA 2 protokolü, drone ve yer kontrolörleri arasında güvenli veri aktarımı için etkili yaklaşımlardan biridir. Ancak, şifreleme anahtarının uzunluğu kaba kuvvet saldırılarına karşı dayanıklı olacak şekilde uygun şekilde seçilmelidir. Kuşkusuz, kaba kuvvet saldırısının daha uzun anahtarları kırması daha uzun zaman ve işlem gerektirir. Elbette, WPA 2 şifrelemesi ancak ilk etapta İHA'nın ağını koruyan şifre kadar iyidir. Zayıf şifreleri olan ve kırılması son derece kolay olan kullanıcılar, ilk etapta şifresi olmayan bir İHA kadar savunmasız olacaktır ([20, 34] örneklerinde olduğu gibi). WPA 2'ye göre daha güvenli kabul edilen WPA 3 deauthentication saldırılarına karşı kullanılabilir. Eşit Eş zamanlı Kimlik Doğrulama (SAE) protokolü ve kişiselleştirilmiş veri şifreleme özellikleri ile daha güvenli bir iletişim sağlar. Ayrıca bir kullanıcının yalnızca bir tahminde bulunmasına izin vererek çevrimdışı şifre tahminlerine karşı koruma sağlar, böylece daha güçlü kaba kuvvet saldırı koruması sağlar.

Barker [64], WPA 3'e geçiş henüz mümkün değilse, parolanın bir programa göre değiştirilmesini önermektedir. Bu yöntem, basit parola oluşturan kullanıcılar veya default parola ile kimlik doğrulama yapan dronlar için, daha önce ağa giren saldırganlara karşı güçlü caydırıcı olabilir.

Manesh ve Kaabouch [63], kimlik doğrulama saldırılarını önlemek için güvenilir kullanıcılarla bağlantı kurulduktan sonra erişim noktasını gizlemek için dronun SSID yayınını devre dışı bırakmayı önermiştir. Diğer bir önerilen yaklaşım, erişimi yalnızca önceden kaydedilmiş medya erişim denetimi (MAC) adresleri ile sınırlamaktır.

DoS saldırılarına karşı tedbirler, genellikle, saldırı tespiti, trafik sınıflandırması, frekans atlama tekniklerinin kullanılmasını içermektedir. Ek olarak, dronlarda paket yönetimi ile bir paketin

ne kadar büyük olabileceği konusunda sınır belirlenebilir ve bu sınırı aşan paketler saldırıyı önlemek için reddedilebilir. Diğer bir yöntem, kullanıcı yönetimidir. Drone, bir kullanıcıyı barındırdığını zaten biliyorsa ve ağına katılmak için başka bir istek alırsa, kullanıcı yönetimi bu isteği otomatik olarak reddedebilir. Kullanıcı yönetimi, dronların asıl kullanıcı ile güçlü bir bağlantı kurmasını sağlarken, ikinci bir kullanıcının erişim kazanmasını engelleyecektir.

Bahsedilen teknikler kullanılarak, dronun çok sayıda paketle başa çıkabileceği ürün yazılımı ya da donanımı geliştirilebilir. Bunlar, meşru olduklarını belirledikleri trafik akışına izin vermeyi ve diğer trafikleri engellemeyi amaçlar.

2.3.4. GPS Spoofing Saldırılarına Karşı Önlemler

Sivil alanda kullanılan GPS genel yapısı sebebiyle güvenli değildir. Dronlarda yaşanan GPS spoofing saldırısı, saldırganın sahte GPS sinyalleri oluşturması ve bunları geçerli sinyaller olarak hedef drona göndermesidir. GPS Jamming / Spoofing saldırılarında drone fiziksel zarar görebilir ya da [9, 18, 30, 32, 47, 49] örneklerinde olduğu gibi drone ve İHA sistemi kaçırılabilir. GPS spoofing saldırısından önce, hedef drone ve alıcısı arasındaki iletişim ortamını GPS jamming saldırısı ile bozulur. Bu saldırılar tespit edildikten sonra uygulama üzerinden return to home moduna geçerek korunma sağlanabilir. Ancak saldırının tespiti ve saldırı ile eş zamanlı olarak RTH veya manuel kontrol her zaman mümkün olmayabilir. GPS spoofing saldırılarını önlemek için çeşitli araştırmalar yapılmıştır.

Luo [30] çalışmasında, DJI Phantom 3 üzerinde GPS spoofing saldırısı gerçekleştirmiştir. Korunma yöntemi olarak, GPS sub frame verisini ve uydu saati ile gerçek zaman arasındaki zamanın doğrulamasını, noktadan noktaya hareket hızının kontrol edilmesini önermiştir. Örneğin bir saniyede İstanbul'dan Bakü'ye konumunuzu değiştirmek imkansızdır.

Guo ve diğ. [65], GPS spoofing saldırısını önlemek için etkin yöntemlerden biri uygun şifreleme yoluyla elde edilebilen kimlik doğrulama yöntemini önermiştir.

GPS iletişimlerinin yayın özellikleri bu sistemlerde kriptografik yaklaşımların uygulanmasını zorlaştırsa da bu konuda yapılmış çalışmalar bulunmaktadır. Wesson ve diğ. [66], kriptografik kod bazlı kimlik doğrulamasını, kod zamanlaması kimlik doğrulaması ile bütünleştiren GPS sinyalinin kimliğini doğrulamak için olasılıklı modellere ve istatistiksel hipotez testlerine dayanan bir teknik tanımlamışlardır.

Giray [67], GPS ve kriptografik doğrulama sinyali analizi (ortalama güç, zaman aralığı, tanımlama kodu izleme) gibi yaklaşımları, GPS spoofing saldırılarına karşı önlem olarak önermiştir. [68, 69]'de verilen çalışmalarda, kaçırma tespit ve kurtarma teknikleri formüle edilmiş ve test edilmiştir.

Kerns ve diğ. [70], GPS spoofing saldırılarının tespitini kolaylaştırmak için asimetrik kriptografiye dayalı bir yöntem önermiştir. Bu yöntem, yayın verilerinin geri kalanını imzalamak için kullanılan periyodik bir imza için sivil navigasyon mesajlarındaki ayrılmış mevcut bitleri kullanmaktadır. Alıcı imzayı ve GPS sinyalinin kaynağını doğrular. Bu yöntem aynı zamanda Navigasyon Mesajı Kimlik Doğrulaması (NMA) olarak da adlandırmaktadır.

Zheng ve Sun [71], dronların navigasyon sistemlerinin nasıl daha iyi güvenlik altına alınacağı konusunda öneriler sunmuştur. İlk öneri olarak, dronlar, sinyallerini farklı bantlarda ileten en az iki tip GNSS ile donatılmalıdır. Rus Küresel Navigasyon Uydu Sistemi (GLONASS), parazite karşı daha yüksek bir dirence sahip olan frekans bölmeli çoklu erişim (FDMA) tekniğini kullanarak sinyalini kodlar. Uydu sinyalini farklı GNSS'lerden almak, saldırganlar tarafından sahtekarlığı (spoofing) zorlaştırmaktadır. İkinci önerileri, IoT aracılığıyla konum bilgisi üzerinde verimli bir çift kontrol mekanizması ile sınırlı kaynak sorununu çözmektir.

GPS saldırılarını tespit etmek için makine öğrenmesi tabanlı yöntemler de kullanılmaktadır. Makine öğrenimi algoritmaları, veri kümeleme, veri sınıflandırma ve örüntü tanıma gibi birçok amaç için kullanılabilir. Bu algoritmalar, alınan GPS verileri gibi bir dizi verideki mevcut gizli kalıbı belirleyebilir ve anormallikleri bulabilir [63].

Panice ve diğ. [72], İHA üzerindeki GPS spoofing saldırılarını tespit etmek için Destek Vektör Makinesi (SVM) kullanarak durum tahmini analizine dayalı bir yöntem önermişlerdir. Bu yöntem, GPS ve İHA'nın navigasyon sistemi arasındaki hata dağılımından yararlanmaktadır. Yazarlar, GPS spoofing saldırılarının varlığında bu dağılımın değiştiğini bulmuşlardır.

Manesh ve diğ. [73] tarafından, GPS sinyallerini kaydedip tekrar oynatarak başlatılan GPS saldırılarını tespit etmek için denetimli yapay sinir ağına dayalı bir makine öğrenme yöntemi önerilmektedir. GPS sinyallerini sınıflandırmak için sözde menzil, Doppler kayması ve taşıyıcı faz gibi çeşitli özellikler kullanılmıştır. Çeşitli sayıda gizli nöron içeren bir ve iki gizli katmanlı sinir ağlarının etkinlikleri analiz edilmiş ve karşılaştırılmıştır.

2.3.5. Portlara Yönelik Saldırılara Karşı Önlemler

Bir drone güvenliğini etkileyen en büyük faktörlerden biri drone üzerindeki portların yönetimidir. Uçuş sırasında, yalnızca kritik portlar kullanıma açılmalıdır. FTP, SSH ve Telnet gibi hizmetlerin tümü kısıtlanmalı ve ikinci bir kimlik doğrulama düzeyi gerektirmelidir. Kullanıma açılması gereken portlar sadece dronun uçuşu için gerekli olan portlardır. Port güvenliğinin uygulamaması önemli bir sorundur ve çok sayıda güvenlik açığından yararlanılmasının nedenidir. [32, 34, 36, 48]'de incelenen çalışmalarda, sınırlanmayan FTP, Telnet portları sebebiyle kişisel verilere, dosyalara izinsiz erişim sağlandığı ve drone kontrolünün ele geçirildiği gösterilmiştir.

Bir dronun kullanabileceği yüzlerce, hatta binlerce port olabilir. Port güvenliğini sağlamak için Rudo ve Zeng [74] tarafından dinamik port güvenliği yöntemi önerilmiştir. Servis, belirli bir algoritmaya göre hangi porttan sinyal gönderip alacağını değiştirecektir. Kullanılmayan portlar yine kapatılacak, ancak artık saldırganlar yalnızca bir portu hedefleyecektir. Saldırganın herhangi bir sonuç elde etmek için birden çok porta saldırmaya çalışması gerekecektir. Böyle bir taktik kullanıldığında, büyük ölçekte fuzzing ve flood saldırıları başlatmak çok daha zor olacaktır. Bir drone sürüsü dinamik port güvenliği kullanıyorsa, bir flood saldırısı tüm sürüyü etkileyemeyecektir. Rastgele gibi görünen zamanlarda her cihaz farklı bir port kullandığında, saldırganın her bir cihazın güvenliğini ihlal etmesi son derece zor olacaktır.

2.3.6. Ürün Yazılımına Yönelik Saldırılara Karşı Önlemler

[38, 44, 47] çalışmalarında incelendiği üzere, dronların ürün yazılımlarına yönelik tersine mühendislik yöntemleri kullanılarak, dronların sistem dosyalarına, konfigürasyon dosyalarına, kişisel verilere izinsiz erişim yapılabildiği ve saldırgan tarafından dronun kontrolünün ele geçirilebildiği gösterilmiştir. Bu saldırılara karşı alınacak önlemler ile saldırıların etkisi zayıflatılabilir.

Tersine mühendislik saldırılarını önlemek için firmware şifrelenmeli ve dijital olarak imzalanmalıdır. Güçlü obfuscator / packer ile dosyaların geri çözülmesi güçleştirilmelidir. Uygulama, sunucu ve drone arasındaki SDK kimlik doğrulama anahtarını doğrulamak için asimetrik şifre kullanılmalıdır [30].

2.3.7. Dronlara Yönelik Ağ Saldırılarına Karşı Saldırı Tespit Sistemleri

İnsansız hava araçları, önceki bölümlerde incelendiği üzere çeşitli saldırılara maruz kalmaktadır. Dronlara / İHA'lara yönelik kötü niyetli faaliyetleri tespit etmek için Saldırı Tespit Sistemleri (IDS'ler) geliştirilmiştir. Tipik olarak, bir IDS gelen ve giden ağ trafiğini izler ve anormallikleri tespit etmek için bunları analiz eder. Amaçları, farklı ağ bölümlerinde toplanan veri izlerini inceleyerek siber saldırıları tespit etmek ve tanımlamaktır. Drone ağlarını saldırganlara karşı korumak için farklı IDS yaklaşımları bulunmaktadır [61].

2.3.7.1. *Kural Tabanlı Saldırı Tespiti*

İHA alanında kural tabanlı saldırı tespit sistemleri kullanılmaktadır. Strohmeier ve diğ. [75] bir İHA ve yer istasyonu arasındaki iletişimi korumak için kural tabanlı saldırı tespit şeması geliştirmiştir. Amaçları, özellikle sinyal gücünü hedefleyen yanlış veri enjeksiyon saldırılarını tespit etmektir. Saldırganların 40 saniye içinde tespit edilebileceğini kanıtlamışlardır.

Mitchell ve Chen [76] tarafından İHA'lardaki kötü niyetli eylemleri tespit eden uyarlanabilir davranış kuralı tabanlı IDS olan BRUIDS (Behavior Rule Based UAV IDS) sunulmuştur. Yazarlar ayrıca İHA'nın kötü niyetli saldırılara karşı hayatta kalmasını hızlı bir şekilde değerlendirmek için BRUIDS'in pervasız, rastgele ve fırsatçı saldırgan davranışları üzerindeki etkinliğini araştırmıştır. Simülasyon sonuçlarında, BRUIDS'in çoklu güven anomalisi tabanlı IDS yaklaşımına kıyasla daha yüksek bir algılama oranı ve daha düşük bir false positive oranı elde ettiğini göstermiştir. Ancak, kural tabanlı IDS'ler, kural yapılandırması için insan müdahalesini gerektiren karmaşıklık yönetiminden muzdariptir. Ayrıca, bu tür IDS, bilinmeyen saldırıları tespit edemez.

2.3.7.2. *Anormallik Tabanlı Saldırı Tespiti*

İHA sistemindeki, anormallik tabanlı tespit IDS'si, esas olarak jamming saldırılarını önlemek için kullanılmaktadır. Rani ve diğ. [77] tarafından İHA düğümlerini (nodes) DoS ve DDoS saldırılarına karşı korumak için anomali tabanlı bir öğrenme algoritması sunulmuştur.

Lu ve diğ. [78] tarafından insansız hava araçlarında, sıcaklık kaydı için DS18B20 sensörleri ve işleme için raspberry pi CPU kullanarak drone motorlarının anormal sıcaklıklarda çalışmasını engelleyen, pekiştirmeli öğrenme tabanlı motor-sıcaklık anormalliği algılama sistemi sunulmuştur. Bu sistem, aşırı ısınma durumunda dronu yere indirerek motor arızasını önleme

imkanı sunar; ancak, sorunu tam olarak engellemez. Deneysel sonuçlarda yazarlar, sensörlerin bilgilerine dayanarak dronu güvenli bir şekilde kontrol etme yeteneğini ortaya koymuştur.

Condomines ve diğ.[79] tarafından Uçan Adhoc Ağdaki (FANET) İHA ağları içinde, anormallik tahmini için spektral trafik analizine ve güçlü bir kontrolöre dayalı hibrit IDS sunulmuştur. Bu teknik, Dağıtık DoS saldırılarını hedeflemiştir ve etkinliği gerçek zamanlı trafik üzerinde test edilmiştir. Çalışma sonuçlarında, farklı anomali türlerinin doğru bir şekilde tespit edildiği aktarılmıştır. Bununla birlikte çalışmada, etkinliğini sağlamak için daha fazla test yapılması gerektiği vurgulanmıştır.

3. MALZEME VE YÖNTEM

3.1. KULLANILACAK ARAÇLAR



Şekil 3.1: Syma X5UW FPV Quadcopter

Drone hackleme, Syma firmasına ait Syma X5UW Drone üzerinde gerçekleştirildi. Syma X5UW FPV Quadcopter görseli Şekil 3.1'de paylaşılmıştır. Kontrolü için Google Play Store'da yüklü olan Syma Go uygulaması kullanıldı. Uygulamada ele geçirilen Syma X5UW dronun özellikleri;

- RC Kumanda ve WiFi kontrolü
- 2.4 GHz, 4 kanal, 6 Eksenli jiroskop
- FPV
- Başsız mod (Kullanıcı yönüne göre hareket kabiliyeti)
- Havada sabit kalma
- Tek tuş kalkış ve iniş
- Geri dönüş modu
- Belirlenen konuma uçuş
- 360 derece takla atma
- HD Kamera
- Uçuş süresi:10 dk
- Kontrol mesafesi: max 150m
- WiFi video mesafe: 40m

- Şarj süresi < 150 dk
- Ağırlık: 127gr

Linux Dağıtımı;

- Kali Linux (kali-linux-2021.2-rpi4-nexmon-64.img)

Donanımlar;

- Syma X5UW Drone
- İki android telefon
- Raspberry Pi 3
- Dark RangeMax Duo kablosuz adaptör

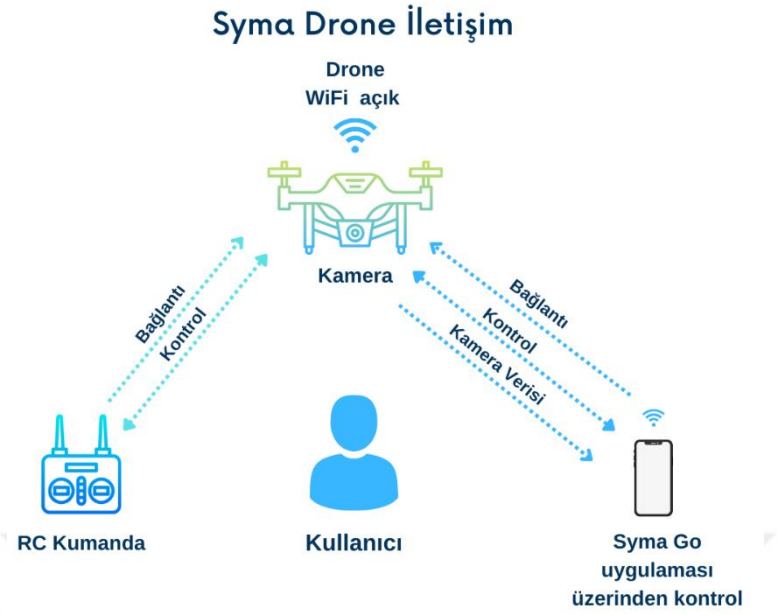
HDMI Ekran Bağlantısı için;

- Kablosuz klavye (+Mouse TouchPad)
- USB Mouse
- USB Batarya
- HDMI Bağlantılı Ekran

Araçlar;

- airmon-ng
- airodump-ng
- aireplay-ng
- hping
- Syma Go

3.2. SALDIRI YÖNTEMİ



Şekil 3.2: Syma drone iletişim şeması

Kullanılacak hedef Syma drone, hem Syma Go mobil uygulaması hem de RC kumandası ile kontrol edilebilmektedir. Şekil 3.2'de Syma drone iletişim şeması gösterilmiştir. Drone açıldığında, 2.4 GHz 802.11 Wi-Fi hotspot görevi görür. Syma Go yüklü telefondan dronun şifresiz WiFi hotspotuna bağlanıldığında, drone uygulama üzerinden kontrol edilmektedir. Nmap taraması sonucunda açık port veya istismar edilecek herhangi bir servis bulunmadı. Bu sebeple saldırı yüzeyi olarak, DoS (Denial of Services - Servis Dışı Bırakma) saldırı türlerine açık olan WiFi protokolü üzerinden sağlanan mobil uygulama kontrolü seçilmiştir. Hedef drone üzerinde, DoS saldırı türlerinden deauthentication ve ping flood saldırıları uygulanacaktır. Yeterli zaman ve SDR olmadığı için RC kumanda üzerinden benzer saldırı senaryoları uygulanamadı.

DoS saldırıları temel olarak sistem kaynaklarını veya bant genişliği tüketerek servislerin hizmet dışı bırakılmasıdır. Tek bir kaynaktan tek bir hedefe yöneliktir. Saldırı paketleri doğrudan hedef sisteme gönderilir. DoS saldırıları meşru kullanıcıların sistemlere erişmesini engelleme girişimi olarak tanımlanabilir.

3.2.1. Deauthentication Saldırısı

Deauthentication saldırısı, bir kullanıcının ağ bağlantısını kesen hizmet dışı bırakma saldırısıdır. 802.11 Wi-Fi Protokolü'nün güvenlik açısından yetersiz olmasından dolayı bu saldırı kablosuz ağa sızmadan, yalnızca hedef sistemin MAC adresini bilerek gerçekleştirilebilir. Deauthentication saldırısını yapabilmek için ilk olarak saldırıyı yapacak hedef ağ hakkında bilgiye sahip olmak gerekmektedir. Bunun için ise kablosuz ağlar ile ilgili bilgi toplama işlemini uygulamak gerekmektedir. Deauthentication saldırısını gerçekleştirirken kullanılan araç seti: Aircrack-ng. Kali Linux'da kurulu olarak gelen, Wi-Fi hackleme için sık kullanılan bir araçtır. Aircrack-ng paketi, paketleri ve el sıkışmalarını yakalamaya, bağlı istemcilerini kimlik doğrulamasını kaldırmaya ve trafik üretmeye yardımcı olan araçlar içermektedir. Ayrıca kaba kuvvet ve sözlük saldırıları gerçekleştirmek için araçlar da vardır. Kısaca Aicrack-ng, aşağıdaki araçları ve diğerlerini içeren hepsi bir arada bir settir.

airmon-ng ; Sahte bağlantı noktaları oluşturur, monitor modu başlatır.

airplay-ng ; Trafiği ve istemci kimlik doğrulamasını oluşturur.

airdump-ng ; Etraftaki tüm kablosuz bağlantıları görüntüleyip paketleri dinlemeye, kanal ve BSSID'lerini gözlemlemeye yarar. Airodump'daki parametrelerin anlamları:

BSSID : AP (Access Point)'nin MAC Adresi

PWR : Sinyal Seviyesi

CH : Kanal No(Channel Number)

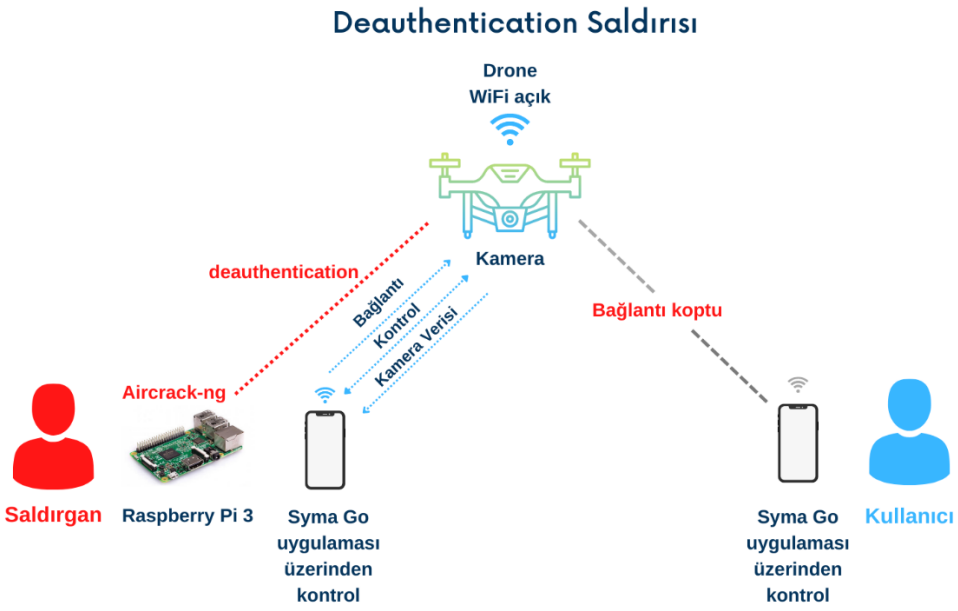
MB : AP tarafından desteklenen en fazla hız

ENC : Kullanımdaki Şifreleme Algoritması. OPN:Şifre Yok. WEP?: WEP

ESSID : SSID olarak da bilinir. Kablosuz ağın ismidir.

STATION : AP ile ilişkilendirilmiş MAC adresleri için kullanılır.

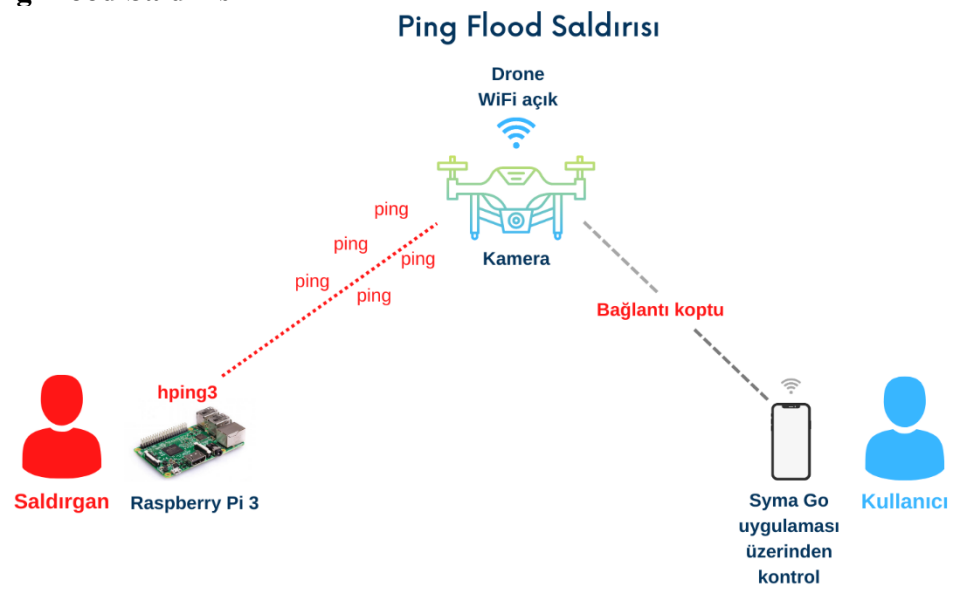
aircrack-ng ; Kablosuz bağlantı şifrelerini kırar.



Şekil 3.3: Syma drona yapılan deauthentication saldırı şeması

Deauthentication saldırısında, Raspberry Pi üzerinden hedef dronu ele geçirip saldırgan tarafından kontrol edilmesi anlatılacaktır. Şekil 3.3'de Syma drona yapılan deauthentication saldırı şeması gösterilmiştir. Amaç kablosuz ağ bağlantı zafiyetini kullanarak normal kullanıcı ile drone arasındaki bağlantıyı kesmektir. Bağlantı kesildikten sonra kullanıcı kontrolü kaybedecek ve drone ele geçirilecektir. Daha sonra dronun Syma Go mobil kontrol uygulamasının yüklü olduğu telefon üzerinden ileri, geri, sağ, sol, yukarı ve aşağı gibi yönlendirmeler gerçekleştirilecektir. Kontrol edilen dronun hareketleri normal kullanıcı gibi yönetilecektir.

3.2.2. Ping Flood Saldırısı



Şekil 3.4: Syma drona yapılan ping flood saldırı şeması

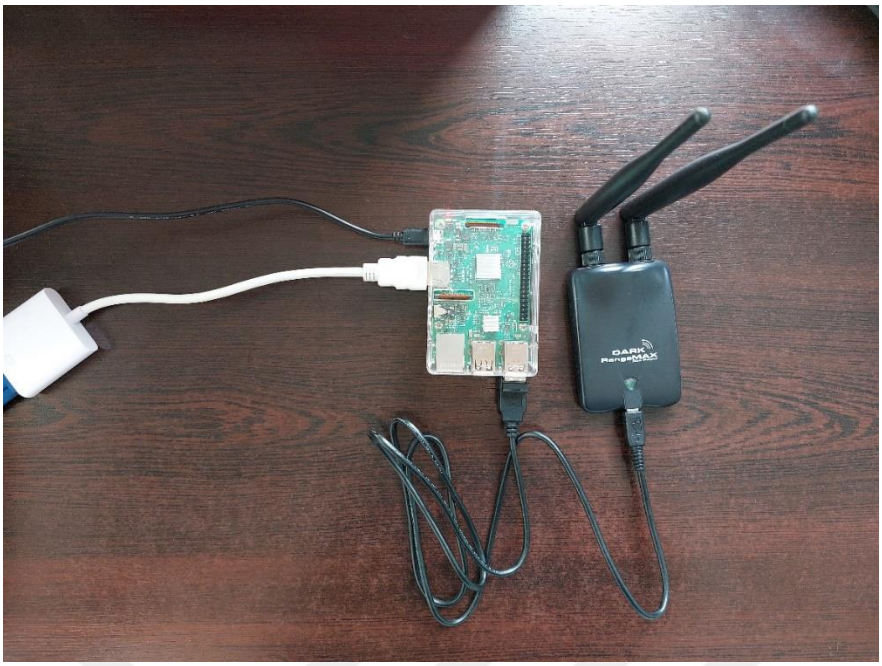
Ping Flood DoS saldırısında, doğrudan hedefe yöneltilen sayısız veya belirlenen sayıdaki ICMP (Internet Control Message Protocol) paketleri gönderilir. Bu, ICMP paketlerinin (ping'lerin) herhangi bir yanıt beklemeden çok hızlı bir şekilde gönderileceği anlamına gelir. Hedef drone, gelen isteklerle boğulur ve bu da başka hiçbir iletişim için erişilemez hale gelmesine neden olur. Meşru kullanıcı tarafından gönderilen kontrol edilemeyen drone bulunduğu yere çakılacaktır. Çalışmada hping3 aracı kullanarak, basit bir ping seli başlatılacaktır. Fast veya faster gibi farklı parametreler kullanılarak paketlerin hızı belirlenebilir. Şekil 3.4'de Syma drona yapılan ping flood saldırı şeması gösterilmiştir.

3.3. SALDIRI DÜZENEĞİNİN HAZIRLANMASI

Bu çalışmada yapılanlar, Kali Linux yüklü herhangi bir bilgisayarda da uygulanabilir olmasına rağmen isteğe bağlı olarak Raspberry Pi 3 üzerinde gerçekleştirecektir. Dağıtım olarak da Kali Linux Nexmon dağıtımı kullanıldı. Bunun sebebi, Nexmon dağıtımında yüklü olarak gelen ayarlar sayesinde kablosuz adaptörünü uyumlu bir şekilde kullanabilmektir. Bir diğer avantajı, kullanılacak araçlar Kali'de yüklü gelmekte ve bu yüzden pratiklik sağlamaktadır. Saldırı aircrack aracının olduğu ve monitor modun tanındığı sistemlerde de uygulanabilmektedir.

Uygulamaya başlarken ilk önce Raspberry Pi'ya Kali Linux yüklenmelidir. Bunun için Raspberry Pi da kullanılacak SD karta Kali Linux'un Nexmon (kali-linux-2021.2-rpi4-nexmon-64.img) dağıtımı yüklendi. Bu dağıtımın seçilme sebebi monitor modu kullanmaya yarayan yamaların yüklü olarak gelmesidir. SD kart boot edildikten sonra, sıra Raspberry Pi'ın çalıştırılmasına gelmiştir. Bu noktada Raspberry'ye HDMI ile bağlanılacaktır. Diğer ethernet, VPN bağlantıları bu çalışmada ağ işlemleri durdurulduğu için kullanılamayacaktır.

HDMI kablosuyla, HDMI girişli herhangi bir ekrana bağlanılıp, mini kablosuz klavye ve mouse USB girişleri takıldıktan sonra güç kaynağına bağlanarak Raspberry Pi başlatıldı. Ek olarak monitör modun başlatılması Raspberry'nin kendi WiFi kartı ile birlikte kablosuz USB adaptörü kullanıldı. Bu işlemden sonra Kali Linux'da yüklü gelen kablosuz ağ saldırılarında sıkça kullanılan aircrack-ng paketi kullanıldı. HDMI bağlantı görseli Şekil 3.5'de verilmiştir.



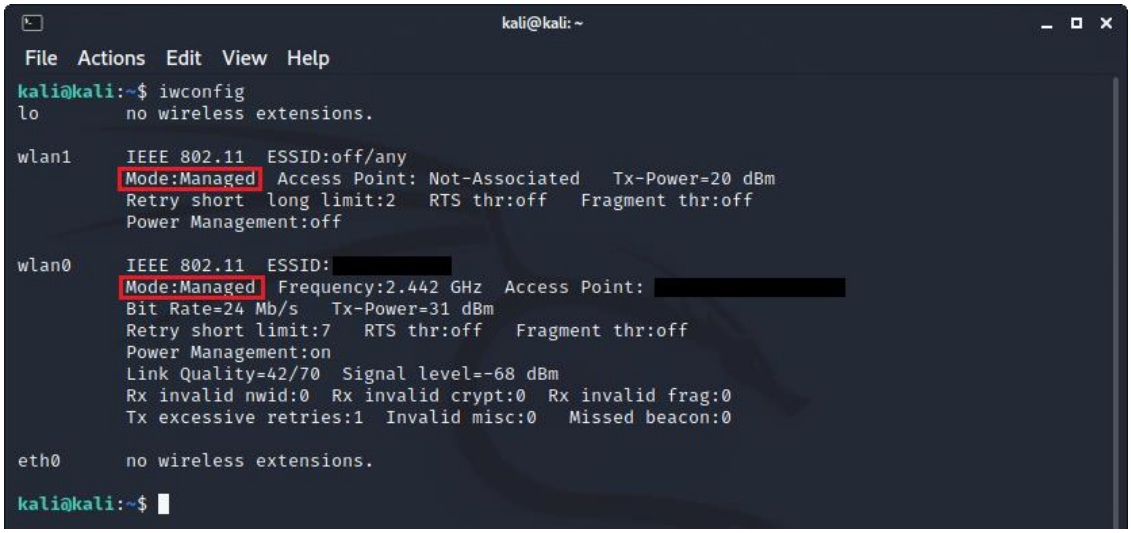
Şekil 3.5: HDMI ile Raspberry Pi bağlantısı

4. BULGULAR

4.1. DEAUTHENTICATION SALDIRISI

Komutlara geçmeden önce hedef Syma X5UW dronun çalışır vaziyette ve android telefon üzerinden Syma Go uygulamasıyla kontrol edildiği bilinmelidir. Raspberry Pi başlatıldıktan sonra uç birim açılmıştır. Tanımlı arayüzleri görmek için aşağıdaki komut verilmiştir;

Komut: iwconfig

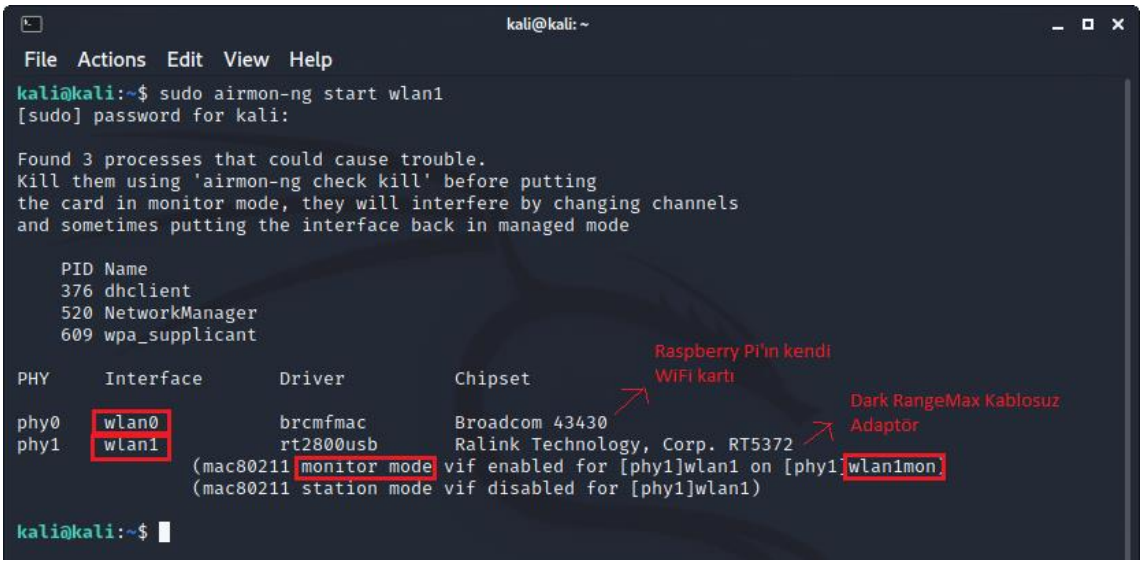


Şekil 4.1: iwconfig komut çıktısı

Komutun ekran çıktısından, bağlı olan kablosuz adaptörün isminin ***wlan1*** *olduğu* öğrenilmiştir. Farklı cihazlarda tanımlı olarak *ath0, mon0 vb.* gibi isimler alabilir. Şekil 4.1'de Raspberry'nin kendi WiFi kartı ise ***wlan0*** üzerinde çalıştığı görülmektedir. Başlangıçta ***wlan0*** ve ***wlan1*** "Managed" modundadır.

Şimdi sıra havadaki sinyalleri ağa bağlı olmadan yakalayan monitör (dinleyici) modunu başlatmaktadır. Aşağıdaki komut ile airmon-ng yazılımı ağ adaptörünün arayüzü ***wlan1*** üzerinden çalıştırıldı. Komut çıktısı Şekil 4.2'de verilmektedir.

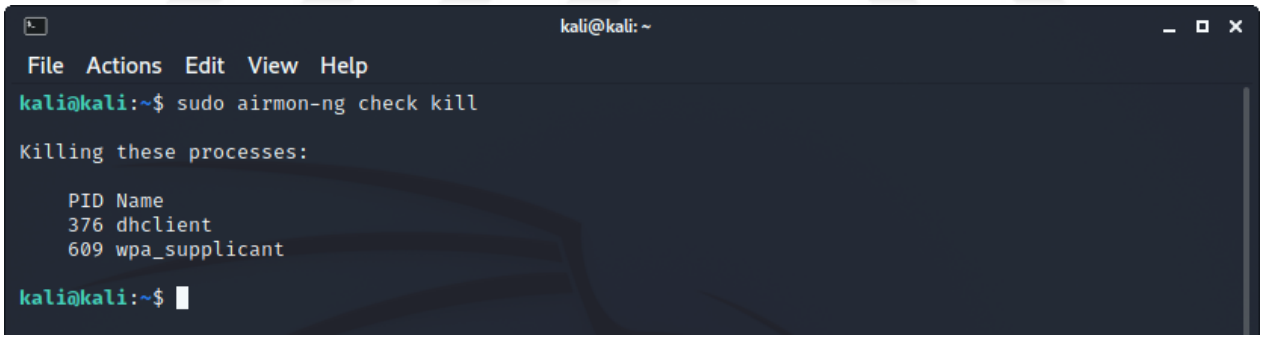
Komut: sudo airmon-ng start wlan1



Şekil 4.2: airmon-ng komut çıktısı

Bu komut sonrası monitör modda aktif olan arayüz ismi öğrenilecektir. Şekil 4.2'de ***wlan1mon*** olduğu görünmektedir. Komutun tam olarak çalışabilmesi için aşağıdaki komut ile ağı kullanan işlemler durduruldu (Şekil 4.3).

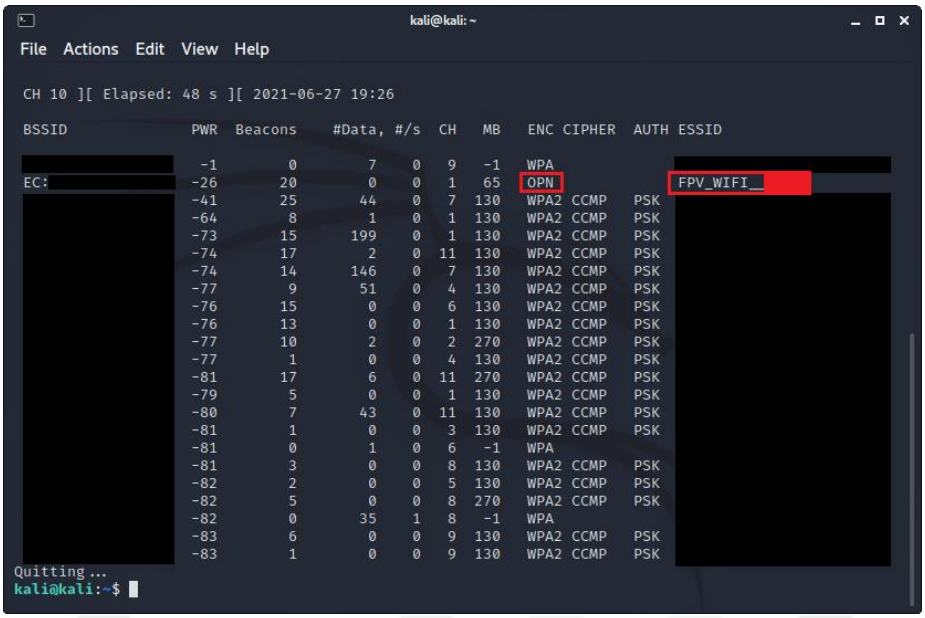
Komut: sudo airmon-ng check kill



Şekil 4.3: airmon-ng check kill komut çıktısı

Aşağıdaki komut çevredeki kablosuz ağları dinlemeye, kanallarını , BSSID'lerini öğrenmeyi sağlayacaktır. Şekil 4.4'de komut çıktısı verilmektedir. ***EC*** ile başlayan MAC adresi ***FPV_WIFI__XXXX*** isimli drona aittir.

Komut: sudo airodump-ng wlan1mon



Şekil 4.4: airodump-ng komut çıktısı

Burada hedef dronun istismar edilecek önemli bir zafiyeti göze çarpmaktadır. Syma X5UW isimli dronun MAC adresi, kanal numarası ile birlikte iletişiminin OPN yani açık olduğu öğrenildi.

WiFi kontrollü çoğu drone da bu şekilde şifresiz iletişime sahiptir. Bunun sebebi ise kontrolün eş zamanlı ve hızlı bir şekilde sağlanma çabasıdır. Önlem olarak farklı modellerde bağlantıyı şifrelemek mümkün olsa da çoğunlukla şifresiz bir iletişim tercih edilmektedir. Ancak Rodday [23] şifreli iletişim kuran saldırı örneğinde bahsedildiği gibi WEP ile şifreli iletişim kuran İHA'yı da etkisiz hale getirmek mümkündür. Bunun için ise şuan uygulamada kullanılacak komutlara sadece aircrack-ng komutu ekleyerek brute force saldırısı yapmak yeterli olacaktır.

Artık hedef drone ile ilgili istenilen bilgileri elde ettikten sonra dronu özel olarak dinlemek için işlem durdurulmuştur. Aşağıdaki komut ile hedef drone özel olarak dinlemeye alınmıştır;

Komut: sudo airodump-ng -c kanaladresi –bssid macadresi -w /root/Desktop/Drone wlan1mon –ignore-negative-one

Kullanılan parametrelerin anlamları;

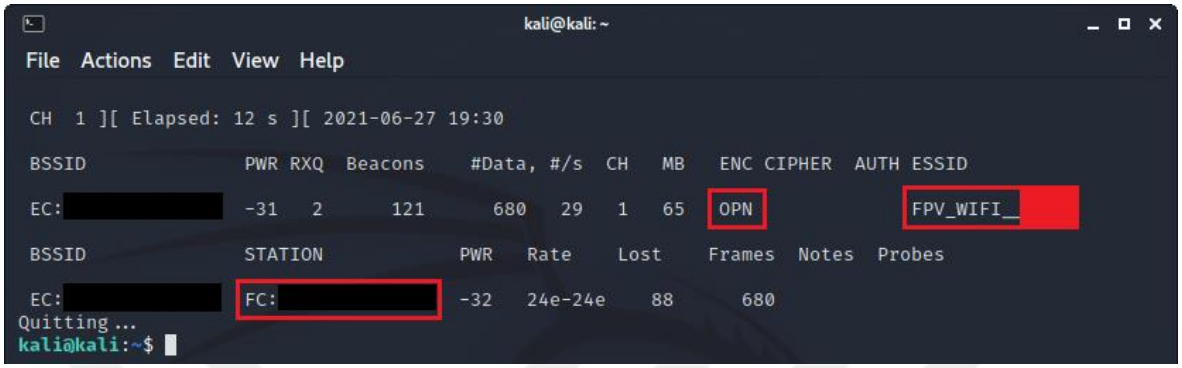
-c : Dronun bulunduğu kanal

--bssid : Dronun MAC adresi

-w : Kayıtların tutulacağı yer

-- ignore-negative-one : Negative One hatasını önler

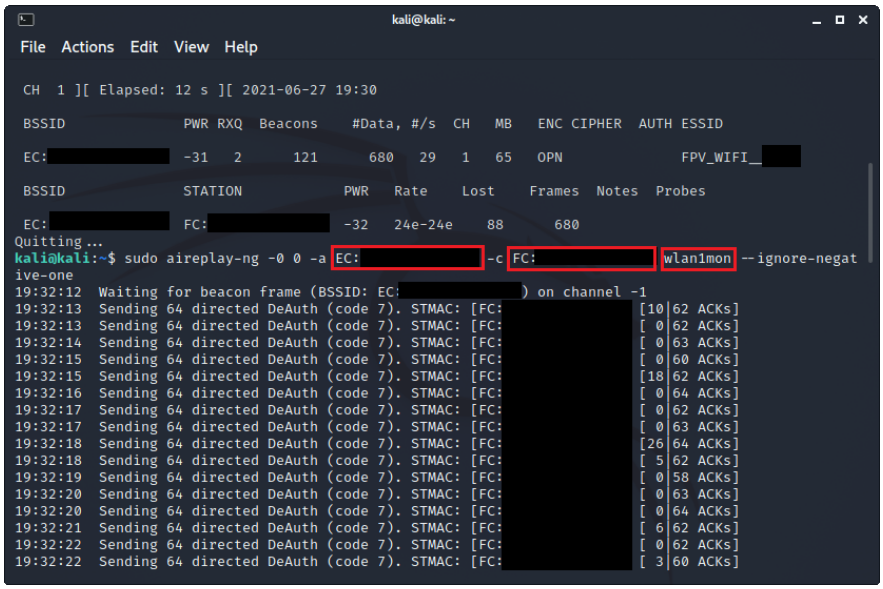
Yukarıdaki komut ile kablosuz adaptörün wlan1mon üzerinden el sıkışma (handshake) bulunmaya çalışıldı. Eşleşme yakalandı. Şekil 4.5'de STATION kısmında bağlanılan telefonun MAC adresi görülmektedir. Şekilde görülen ***EC*** ile başlayan adres drona, ***FC*** ile başlayan adreste eşleşme sağlanan cihaza (bu örnekte normal kullanıcı) aittir.



Şekil 4.5: airodump-ng komut çıktısı - handshake

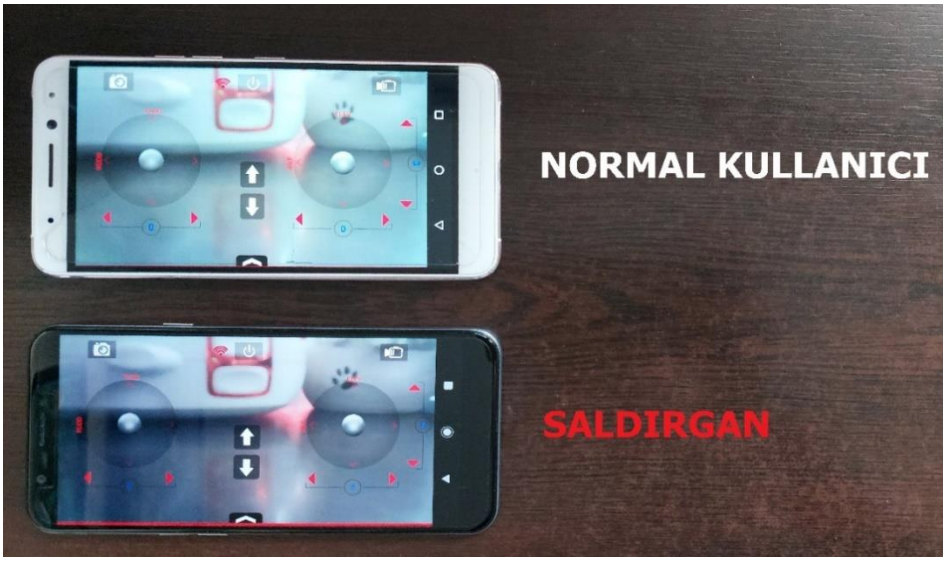
Şimdi sıra trafik oluşturup drone ile eşleşen telefon arasındaki bağlantının kesilip saldırgan telefon ile bağlanmak için aireplay-ng aracı kullanmaya geldi. Burada Raspberry'nin kendi WiFi kartının wlan0 arayüzü kullanılıp deAuth paketleri gönderilmesine rağmen bağlantıyı kesmediği görüldü. Bu sebeple tekrardan kablosuz ağ adaptörünün wlan1mon arayüzü kullanılarak işlem gerçekleştirildi. Aşağıdaki komut ile drona deAuth paketleri gönderildi (Şekil 4.6) ve sahte bir trafik oluşturuldu. Normal kullanıcının, drone ile olan bağlantısı kesildi. Bu sırada saldırganın telefonuna Google Play Store üzerinden yüklediği Syma Go uygulamasıyla drone uzaktan kontrol edilip yönlendirildi.

Komut: sudo aireplay-ng -0 0 -a [Drone MAC] -c [Telefon MAC] wlan1mon –ignore-negative-one



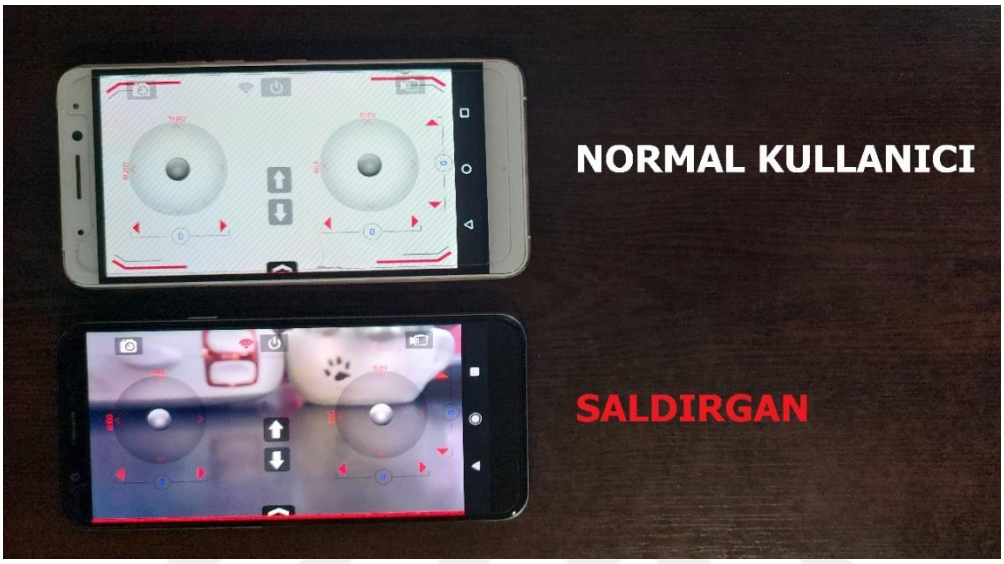
Şekil 4.6: aireplay-ng komut çıktısı

Şekil 4.7'de paket yollanmadan önceki durum gösterilmiştir. Her iki telefonda da görüldüğü üzere saldırgan dronun markasını öğrenip (WiFi taraması sonucu öğrendiği bağlantı isminden veya internette bulunan MAC adresinden) şifresiz iletişim kuran dronun kamera modülüne erişip izleme yapabilmektedir. Ancak kamera erişimi sağlasa da kontrol yine normal kullanıcının elindedir. Bunun sebebi de kontrol cihazının, kontrol paketleri göndermeye başlayan ilk cihaz olarak tanımlanması ve bu durumda ilk bağlananın normal kullanıcı olmasıdır. Saldırgan dronu kontrol etmek için ya normal kullanıcıdan önce bağlanmalı ya da bu örnekte görüldüğü üzere DeAuth paketleri yollayarak normal kullanıcının bağlantısını kesmelidir.



Şekil 4.7: Saldırıdan önce normal kullanıcı ve saldırganın drona erişimi

Paket göndermeye devam ettiği sürece normal kullanıcı drona bağlanamayacaktır. Artık kontrol saldırganın elindedir. Şekil 4.8'de normal kullanıcının hem kontrol hem de kamera erişimini de kaybettiği görülmektedir. Normal kullanıcı gibi drone ile fotoğraf ve video çekimi yapıp istediği şekilde yönlendirebilecektir. Saldırgan dronu ele geçirmiş ve drone hackleme gerçekleştirilmiştir.



Şekil 4.8: Saldırıdan sonra normal kullanıcı ve saldırganın drona erişimi

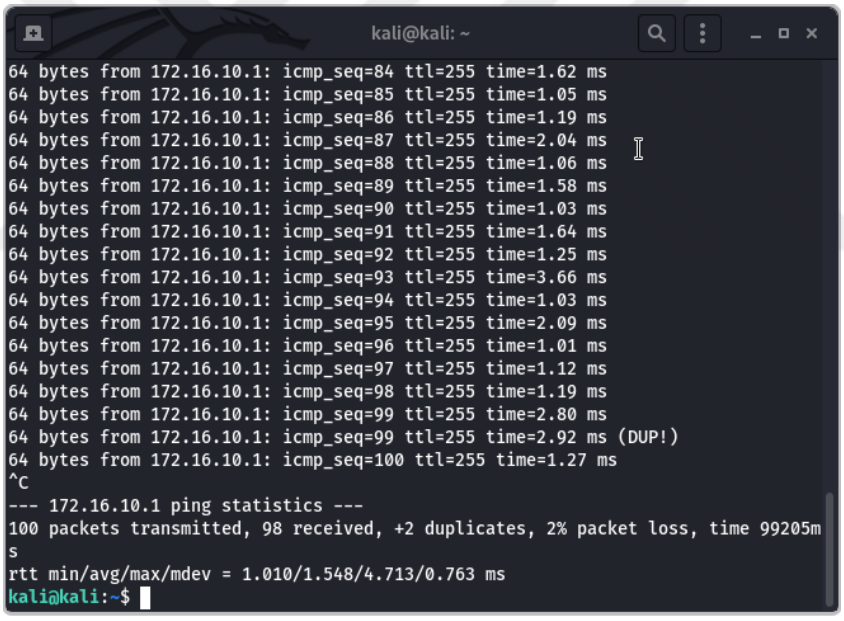
Uygulama sonucunda Syma Go uygulamasına meşru kullanıcı ve saldırganın aynı anda bağlanabildiği görülmüştür. Syma Go uygulamasına ilk bağlanan dronu kontrol etmektedir. Ancak sadece ilk bağlanmak kontrol için yeterli değildir. Başka bir cihaz drona bağlansa hatta uygulamasını açsa bile kontrolün sağlandığı start ekranına gelmeden dronu kontrol edememektedir. İlk bağlanan ve uygulamada kontrol ekranını ilk açan dronu yönetmektedir. Uygulamanın kontrol ekranından çıkıldığında drone ve uygulama eşleşmesi bitmektedir. Ayrıca, eşleşmeyen cihazlar da kameraya erişebilmektedir ve hatta kamera ve video kaydı alabilmektedir. Kayıtlar telefona kaydedilmektedir. Saldırgan, dronda SD Kart varsa uygulama üzerinden kayıtlara erişememektedir.

Bu uygulama RC ve WiFi kontrollü drone üzerinde gerçekleştirildiği için WiFi kontrolü hacklendiğinde RC kumanda başlatıldığı zaman kontrolün yine normal kullanıcıya geçtiği gözlenmiştir. Buna çözüm olarak ise incelenen RC saldırıları veya evrensel kumanda saldırıları gerçekleştirilebilir. Ancak sadece WiFi kontrolü olan dronlarda (Cheerson CX10W'de denenmiştir) ise bu avantaj kullanılamayacak ve tam bir drone hackleme gerçekleştirilecektir.

4.2. PING FLOOD DOS SALDIRISI

DoS saldırılarından biri olan ping flood saldırısı, hedef drone ile kullanıcısı arasındaki iletişimi kesmesi ve dronun erişilemez olması için kullanılacaktır. Belirli sayıda gönderilen ICMP paketleri sonucunda drone cevap veremeyecektir. Drone görüntü aktarımında kesilmeler olacak, komutlara cevap veremeyecektir.

Bir DoS saldırısının dronu nasıl etkilediğini anlamak için düzenli kullanım sırasındaki normal ağ gecikmesinin toplanması gerekiyordu. ICMP ping'leri kullanılarak ağ gecikmesini ölçmek için ortalama RTT (Gidiş Dönüş Süresi) kullanıldı. RTT, bir ping'in hedef makineye gitmesi ve bir yanıtın geri gitmesi için geçen süre için bir ölçümdür. Syma X5UW için normal RTT, ICMP paketlerini dronların ağ arayüz kartına göndermek için ping komutu kullanılarak ölçüldü. Sonuçlar Şekil 4.9'da gösterilmektedir.

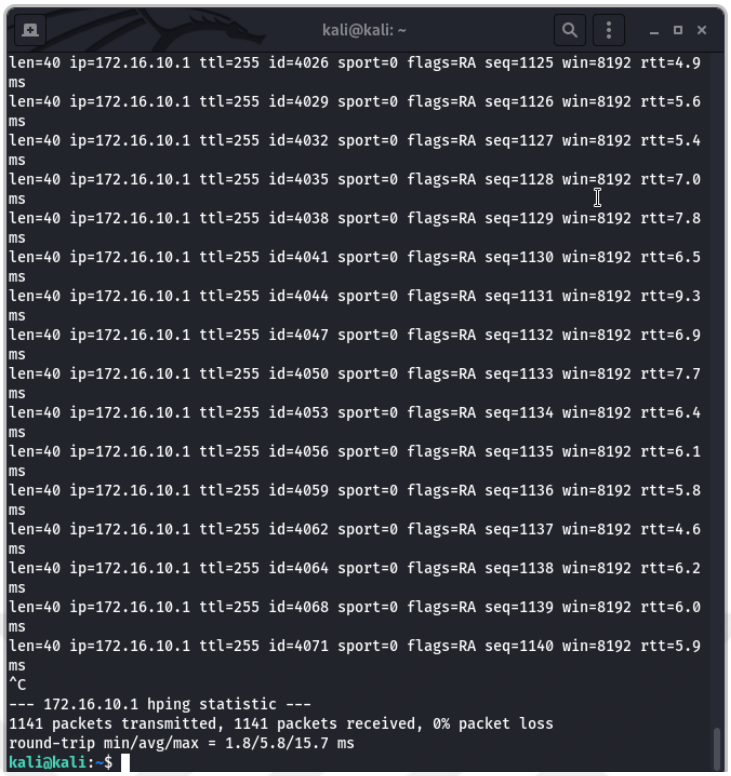


Şekil 4.9: Syma X5UF ping komutu çıktısı

Komut: ping 172.16.10.1

Çıktı: rtt min/avg/max/mdev = 1.010/1.548/4.713/0.763 ms

Yukarıda görüldüğü gibi, standart işlemler sırasında ortalama RTT yaklaşık 1.548 ms'dir. Dronun aşırı bir ICMP paketi artışıyla nasıl başa çıkacağını araştırmak için bir paket üreteci ve analiz komut aracı hping3 kullanılacaktır. Araç, –fast parametresi ile saniyede 10 paket ve --faster parametresi ile saniyede 100 paket hızında ICMP paketleri akışı oluşturacaktır.

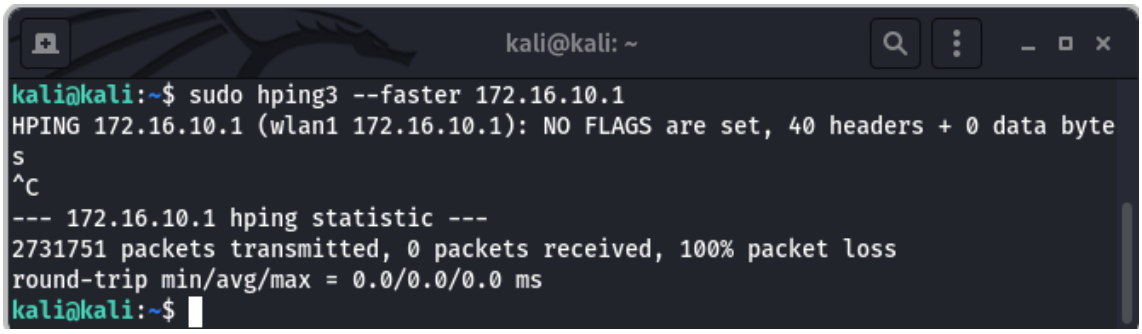


Şekil 4.10: Syma X5UF hping3 --fast komutu çıktısı

Komut: sudo hping3 --fast 172.16.10.1

Çıktı: round-trip min/avg/max/ = 1.8/5.8/15.7 ms

--fast parametresi ile yapılan DoS saldırısı sırasındaki ortalama RTT 5.8 ms ile artış gösterdi. Ancak dronun görüntü aktarımında ve kontrolünde gözle görülür bir değişiklik olmadı. Sonuçlar Şekil 4.10'da gösterilmektedir.



Şekil 4.11: Syma X5UF hping3 --faster komutu çıktısı

Komut: sudo hping3 --faster 172.16.10.1

Çıktı: round-trip min/avg/max/ = 0.0/0.0/0.0 ms

--faster parametresi ile yapılan DoS saldırısında, dronun hiçbir çıktı vermediği ve yanıt vermeyi bıraktığı gözlendi. Saldırılar sırasında drone, kontrolörü ile bağlantısını arada kaybetmiştir.

Dahası, drone DoS dışı koşullarda olduğu kadar hızlı yanıt vermedi. DoS sırasında dronun motoru çok kez durdu. Bununla birlikte, drondan akıllı telefona gönderilen görüntüler gözle görülür şekilde daha yavaştı. Ayrıca DoS saldırısı sırasında dronun sıcaklığı belirgin bir şekilde arttı. Sonuçlar Şekil 4.11'de gösterilmektedir.

Ping flood saldırısı ile pilotun Syma drone kontrolünü kaybedeceği gösterilmiştir. Bunun sonucunda, görüntü aktarımı yavaşlaması sebebiyle zamanında manevra yapamayan, motoru duran, kontrol edilemeyen bir drone yere çakılabilir veya kazaya sebep olabilir.

5. TARTIŞMA VE SONUÇ

Üretildiği ilk yıllardan itibaren askeri amaçlar için kullanılan insansız hava aracını tanımlayan "Drone" kelimesi artık günümüzde sivil alanda ticari ve eğlence uygulamalarında sıkça karşılaşılabilen uzaktan kontrollü çok rotorlu hava araçları için kullanılmaktadır. Askeri faaliyetler için üretilen İHA sistemleri ile hobi, spor ve eğlence amaçları ile üretilen dronlar arasında ciddi farklar olsa da en büyük farkın güvenliklerine verilen önem olduğu rahatça söylenebilir.

Literatürdeki araştırmalar sonucunda askeri ve profesyonel kullanım amaçları olan İHA sistemleri şifreli iletişim kullanırken, hobi ve eğlence amaçlı kullanımı olan dronların sıklıkla şifresiz iletişimi tercih ettiği gözlenmiştir. Bu sebeple uzaktan kontrollü kablosuz haberleşme sağlayan hava araçlarındaki güvenlik açıklarını istismar etmenin, profesyonel kullanım amaçları olan İHA sistemlerine göre daha kolay olduğu görünür bir gerçektir. Ancak [4, 6, 9, 12, 23] benzeri örneklerde görüldüğü üzere imkansız değildir.

Bu çalışma kapsamında, WiFi ve radyo kontrollü drone kullanılarak, Raspberry Pi üzerinde Kali Linux'de yüklü araçlarla, fazla karmaşık sistemlere ve yazılımlara gerek duymadan kolay bir şekilde uygulanabilecek temel saldırı yöntemleri kullanılmıştır. Uygulanan DoS saldırıları, gelecekte kullanımının artacağı öngörülen kablosuz cihazlar üzerinde de etkili olabilecek temel yöntemlerdir.

Kullanılan metotlarla ve yapılan güvenlik analizleri ile birlikte, çevremizde tespit edilen kablosuz bağlantılı dronlara uzaktan izinsiz erişip yönlendirmenin ve pilotun drone kontrolünü kaybetmesinin mümkün olduğu gösterilmiştir. Uygulanan DoS saldırıları ile Syma drondaki güvenlik zafiyeti istismar edilmiş ve bu tür zafiyetlerin diğer pek çok drone çeşidinde de istismar edilebileceği örnekler ile kablosuz haberleşme sağlayan dronlardaki güvenliğin yeterli olmadığı ispat edilmiştir. Araştırılan örnek drone hackleme olayları dikkate alınarak dronların güvenlik analizi yapılmıştır. Çeşitli saldırı yöntemlerine karşı sunulan önlemler incelenmiştir. Sonuç olarak, farklı amaçlar ile insansız hava araçlarının hacklenebileceği gösterilmiştir.

Askeri alanda yaşanan hackleme örnekleri incelendiğinde, devletlerin İHA sistemleri, bölgelerinde ya da bölgeleri dışındaki ülkeler için askeri ve ticari amaçlarla önemli bir hedef olarak değerlendirilmektedir. Önümüzdeki yıllarda, askeri alanda ülkemizde de çalışmaları yapılan insansız savaş uçakları, kamikaze ve sürü İHA teknolojilerinin yapay zekâ

uygulamaları ile birlikte gelişmesi ve kullanıldığı sahaların artması ile birlikte İHA sistemlerinde siber güvenlik konusunun önemi artacaktır.

Ülkemizde üretilen yerli ve milli İHA sistemlerinin kullanıldığı sahalarda oyun değiştirici etkiye sahip olması uluslararası alanda adının sıkça duyulmasına sebep olmuştur. Tehdit oluşturduğu unsurlar tarafından insansız hava araçlarına yönelik gerçekleştirebilecek saldırılar göz önüne alındığında, bu araçların siber güvenlik açısından çok detaylı test edilmesi ve siber güvenlik test standartlarının geliştirilmesi bir gereklilik olarak değerlendirilmelidir.

Yaşanılan İHA saldırıları, sivil ve askeri alanda yeni çözümler üretilmesi gerekliliğini zorunluluk haline getirmiştir. Kullanımı alanı yaygınlaşan insansız hava araçlarına karşı geliştirilen güvenlik çözümleri tespit, etkisiz hale getirme, ele geçirme ve yok etme şeklinde tekil veya çoklu olarak gerçekleştirilmektedir. Bu alanda söz sahibi olmak isteyen her ülke ve kuruluş kendilerine özgü sistemler geliştirmektedir. Özellikle sürü ve kamikaze İHA kullanımı düşünüldüğünde anti-drone sistemleri, ülkelerin sahip olmak istediği kritik bir ihtiyaçtır.

Son olarak, tezin ağırlıkla incelediği sivil alanda kullanılan dronlara yönelik siber saldırılara karşı iki çalışma önerisi sunulacaktır;

- **Drone Pentest Aracı:** Gelecek çalışmalarda, sivil alanda kullanılan WiFi ve radyo kontrollü dronların güvenlik zafiyetlerini, mevcut örneklerinden daha kapsamlı, drone veritabanı geniş, manuel veya otomatik analiz eden ticari veya açık kaynaklı metasploit benzeri bir framework geliştirilmelidir.
- **Mobil Drone Saldırı Tespit ve Önleme Sistemi:** Dronlara yönelik saldırıları, pilota gösteren ve saldırıları önleyen yapay zeka destekli anti-drone sistemi geliştirilmelidir. Sürü dronların gelişimi düşünüldüğünde sivil alanda bireysel koruma sağlayabilmesi için mobil / taşınabilir bir sistem olarak geliştirilmelidir. Bu sistem ile drone kapsam alanında gerçek zamanlı saldırı tespit edilmeli ve önlenmelidir. Algılanan saldırı pilota veya kullanıcıya anlık olarak bildirilmelidir. Saldırı türlerine göre pilota dronu başlangıç noktasına gönderme (RTH) veya manuel kontrol vb. seçenekleri sunularak insansız hava araçlarının kontrolünün güvenliği sağlanmalıdır.

KAYNAKLAR

[1] Karaağaç, C., Ocak 2018, *Drone Kelimesi Odağında Türkçe Terminoloji Tartışması*. STM ThinkTech Yayınları: https://thinktech.stm.com.tr/tr/drone-kelimesi-odaginda-turkce-terminoloji-tartismasi [Son Ziyaret Tarihi: 09.05.2022].

[2] McNabb, H., 2020, *How Worried are Drone Pilots About Data Security? The DRONELIFE Minute Survey.* DroneLife Web Sitesi: https://dronelife.com/2020/09/27/how-worried-are-drone-pilots-about-data-security/ [Son Ziyaret Tarihi: 09.05.2022].

[3] Karaağaç, C., 2016, *İHA Sistemleri Yol Haritası - Geleceğin Hava Kuvvetleri 2016-2050*. STM Yayınları: https://thinktech.stm.com.tr/tr/gelecegin-hava-kuvvetleri-2016-2050- [Son Ziyaret Tarihi: 09.05.2022].

[4] 2022, *General Atomics Predator B,* General Atomics: https://www.ga-asi.com/remotely-piloted-aircraft/mq-9a [Son Ziyaret Tarihi: 09.05.2022].

[5] 2009, *Predator'ler Hacklendi*. Milliyet Web Sitesi: https://www.milliyet.com.tr/predator-ler-hacklendi-teknoloji-haber-1177263/?Page=125 [Son Ziyaret Tarihi: 09.05.2022].

[6] Peters R., 2011, *Ralph Peters: Twilight of the Drones – Recent Loss of RQ 170 In Iran a Possible Game-changer*, http://armchairgeneral.com/ralph-peters-twilight-of-the-drones-recent-loss-of-rq-170-in-iran-a-possible-game-changer.htm [Son Ziyaret Tarihi: 09.05.2022].

[7] Tecca, 2011, *Iran may have captured U.S. stealth drone by hacking its GPS*. Yahoo: https://www.yahoo.com/news/blogs/technology-blog/iran-may-captured-u-stealth-drone-hacking-gps-030447469.html [Son Ziyaret Tarihi: 09.05.2022].

[8] Cenciotti, D. 2016, *Iran unveils new UCAV modeled on captured U.S. RQ-170 stealth drone*, https://theaviationist.com/2016/10/02/iran-unveils-new-ucav-modeled-on-captured-u-s-rq-170-stealth-drone/ [Son Ziyaret Tarihi: 09.05.2022].

[9] 2016, *İran, ABD saldırı drone'unun kopyasını yaptı*. Haber7 Web Sitesi: https://www.haber7.com/asya/haber/2150227-iran-abd-saldiri-droneunun-kopyasini-yapti [Son Ziyaret Tarihi: 09.05.2022].

[10] Rees, C. 2012, *Israel Unveils Enhanced Heron 1 Air and Maritime Surveillance UAV*, https://www.unmannedsystemstechnology.com/2012/10/israel-unveils-enhanced-heron-1-air-and-maritime-surveillance-uav/ [Son Ziyaret Tarihi: 09.05.2022].

[11] Silverstein R., 2013, *Advanced Israeli Drone Hijacked by Iran or Hezbollah, Then Destroyed by Israel.* Richard Silverstein Web Sitesi: https://www.richardsilverstein.com/2013/05/11/advanced-israeli-drone-hijacked-by-unknown-hostile-party-then-destroyed-by-israel/ [Son Ziyaret Tarihi: 09.05.2022].

[12] Currier, C. Moltke H., *Anarchist Snapshots - Hacked Images From Israel's Drone Fleet*, 2016. The Intercept; https://theintercept.com/2016/01/28/hacked-images-from-israels-drone-fleet/ [Son Ziyaret Tarihi: 09.05.2022].

[13] Currier, C., 2016, *F-16-FISINT2-Redacted.* The Intercept; https://www.documentcloud.org/documents/2699849-F-16-FISINT2-Redacted.html [Son Ziyaret Tarihi: 09.05.2022].

[14] Currier, C., 2016, *6-Months-Overview-Redacted.* The Intercept; https://www.documentcloud.org/documents/2699852-6-Months-Overview-Redacted.html [Son Ziyaret Tarihi: 09.05.2022].

[15] Currier, C., 2016, *Anarchist-Training-mod5-Redacted-Compat.* The Intercept; https://www.documentcloud.org/documents/2699846-Anarchist-Training-mod5-Redacted-Compat.html [Son Ziyaret Tarihi: 09.05.2022].

[16] 2016, *ABD İsrail'e ait "Heron TP"yı "anarşist"le hedef aldı.* NTV; https://www.ntv.com.tr/dunya/abd-israili-anarsist-operasyonuyla-hedef-aldi,LpYrPQ_SpUiwE_DU2oXORw [Son Ziyaret Tarihi: 09.05.2022].

[17] 2014, Shepard D. P., Bhatti, J. A., Humphreys T, *Unmanned Aircraft Capture and Control via GPS Spoofing,* J. Field Robotics , Semantic Scholor

[18] Dye, L., 2012, *Drone Aircraft Hijacked by Students in Test; Could Iran Do It?*. ABCNews Web Sitesi: https://abcnews.go.com/Technology/hijacking-drone-uav-aircraft-texas-students-prove-hackers/story?id=16699686 [Son Ziyaret Tarihi: 09.05.2022].

[19] Puiu, A., 2013, *SkyJack – Şi dronele sunt vulnerabile la hacking, cu uneltele potrivite*, https://playtech.ro/2013/skyjack-si-dronele-sunt-vulnerabile-la-hacking-cu-uneltele-potrivite/ [Son Ziyaret Tarihi: 09.05.2022].

[20] Kamkar, S., 2013, *SkyJack*, Samy.pl Kişisel Web Sitesi: http://samy.pl/skyjack/ [Son Erişim Tarihi: 09.05.2022].

[21] Fournier G., Kerdrel P. A.,Cotret, P., Tong, V. V. T., 2017, *DroneJack: Kiss your drones goodbye!*. Symposium sur la sécurité des technologies de l'information et des communications, SSTIC Web Sitesi: https://www.sstic.org/media/SSTIC2017/SSTIC-actes/dronejack/SSTIC2017-Article-dronejack-fournier_cotret_audren-de-kerdrel_viet-triem-tong.pdf [Son Ziyaret Tarihi: 09.05.2022].

[22] Tattler, T. 2014, *Conservation: Unmanned Aerial System – Demo Invite*, https://www.tourismtattler.com/news/trade-news/conservation-unmanned-aerial-system-demo-invite/ [Son Ziyaret Tarihi: 09.05.2022].

[23] Rodday, N., 2016, *Nils Rodday Attack*. Black Hat Asia 2016, Black Hat Asia Web Sitesi: https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf [Son Ziyaret Tarihi: 09.05.2022].

[24] Khandelwal, S., 2016, *Hacker Hijacks a Police Drone from 2 Km Away with $40 Kit*. The Hacker News Web Sitesi: https://thehackernews.com/2016/04/hacking-drone.html [Son Ziyaret Tarihi: 09.05.2022].

[25] Walters, S., 2016, *How Can Drones Be Hacked? The updated list of vulnerable Drones & attack Tools*. Medium Web Sitesi: https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809 [Son Ziyaret Tarihi: 09.05.2022].

[26] Paredes, J. A., Álvarez, F. J., Aguilera, T., & Villadangos, J. M. (2017). 3D indoor positioning of UAVs with spread spectrum ultrasound and time-of-flight cameras. Sensors, 18(1), 89.

[27] Garipov, A., 2017, *Drone Hijacking And Other IoT Hacking With GNU Radio And SDR* . Nullcon Goa 2017, Nullcon Web Sitesi: https://archive.nullcon.net/website/archives/pdf/goa-2017/drone-hijacking-and-other-IoT-hacking.pdf [Son Ziyaret Tarihi: 09.05.2022].

[28] Garipov, A., 2017, *"Drone Hijacking And Other IoT Hacking With GNU Radio And SDR"* . Youtube: https://www.youtube.com/watch?v=qBYgXwnsbd4 [Son Ziyaret Tarihi: 09.05.2022].

[29] Garipov, A., Novikov,P., 2016, *How They Stole Our Drone* . Positive Security, Positive Security Web Sitesi: https://www.phdays.com/en/press/news/phd-vi-how-they-stole-our-drone/ [Son Ziyaret Tarihi: 09.05.2022].

[30] Luo, A., 2016, *Drone Hijacking-Multi Dimensional Attack Vectors and Countermeasures*. DEF CON 24 Conference, DEFCON Web Sitesi: https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEF%20CON%2024%20-%20Aaron-Luo-Drones-Hijacking-Multi-Dimensional-Attack-Vectors-And-Countermeasures-UPDATED.pdf [Son Ziyaret Tarihi: 09.05.2022].

[31] Fournier, G., de Kerdrel, P. A., Cotret, P., & Tong, V. V. T. (2017, June). DroneJack: Kiss your drones goodbye!. In SSTIC 2017-Symposium sur la sécurité des technologies de l'information et des communications (pp. 1-8).

[32] Fournier G., Kerdrel P. A., Cotret, P., Tong, V. V. T., 2017, *DroneJack*. SSTIC 2017, SSTIC Web Sitesi: https://www.sstic.org/media/SSTIC2017/SSTIC-actes/dronejack/SSTIC2017-Slides-dronejack-fournier_cotret_audren-de-kerdrel_viet-triem-tong.pdf [Son Ziyaret Tarihi: 09.05.2022].

[33] 2014, *Prise en main du Parrot Bebop Drone, le drone sous Android compatible avec la réalité virtuelle,* https://www.frandroid.com/android/251087_prise-en-main-du-parrot-bebop-drone-drone-android-compatible-realite-virtuelle [Son Ziyaret Tarihi: 09.05.2022].

[34] Havoque Inc, 2016, *How to Hack a Drone with Kali Linux - Wireless Attacks on the Parrot Bebop Drone*. Youtube: https://www.youtube.com/watch?v=qYL23IGPz30 [Son Ziyaret Tarihi: 22.12.2017].

[35] 2017, *Parrot AR Drone 2.0 Elite Edition,* https://www.amazon.com.tr/Parrot-Drone-2-0-Elite-G%C3%BCm%C3%BC%C5%9F-PF721801/dp/B00FS7SU7K [Son Ziyaret Tarihi: 09.05.2022].

[36] Szabo, M., 2016, *Drone Hacking*. Ethical Hacking Conference Budapest, Github: https://github.com/markszabo/drone-hacking [Son Ziyaret Tarihi: 09.05.2022].

[37] Khandelwal, S. 2015, *MalDrone — First Ever Backdoor Malware for Drones,* https://thehackernews.com/2015/01/MalDrone-backdoor-drone-malware.html [Son Ziyaret Tarihi: 09.05.2022].

[38] Sasi, Rahul., 2015, *Maldrone the First Backdoor for Drones*. Garage4hackers Web Sitesi: https://www.garage4hackers.com/entry.php?b=3105 [Son Ziyaret Tarihi: 09.05.2022].

[39] garagedrone , 2016, *DeviationTX with NRF24L01 module, the universal drone remote control*. Dronegarageblog Web Sitesi: https://dronegarageblog.wordpress.com/2016/06/07/deviationtx-with-nrf24l01-module-the-universal-drone-remote/ [Son Ziyaret Tarihi: 22.12.2017].

[40] 2016, *There's a new way to take down drones, and it doesn't involve shotguns,* Ars Technica web sitesi: https://arstechnica.com/information-technology/2016/10/drone-hijacker-gives-hackers-complete-control-of-aircraft-in-midflight/ [Son Ziyaret Tarihi: 09.05.2022].

[41] Öztürk, E., 2016, *Uçan Bir Drone Ele Geçirilebilir*. Cyberage Technology Web Sitesi: https://blog.cyberage.com.tr/2016/10/28/ucan-bir-drone-ele-gecirilebilir/ [Son Ziyaret Tarihi: 09.05.2022].

[42] goebish, 2017, *E012-SDR-transmitter*. Github: https://github.com/goebish/E012-SDR-transmitter [Son Ziyaret Tarihi: 09.05.2022].

[43] 2022, *DJI Mavic 2 Zoom Smart Controller, DJI Store Türkiye:* https://www.djistoreturkiye.com/dji-mavic-2-zoom-smart-controller-6958265175657 [Son Ziyaret Tarihi: 09.05.2022].

[44] Edström, V., and Zeynalli, E. (2020). Penetration testing a civilian drone: Reverse engineering software in search for security vulnerabilities.

[45] 2022, *DJI PHANTOM 4 PRO, Vatan Bilgisayar:* https://www.vatanbilgisayar.com/dji-phantim-4-pro-multikopter-seti.html [Son Ziyaret Tarihi: 09.05.2022].

[46] 2022, *Parrot Bebop 2 FPV Drone, Drone;* https://www.drone.net.tr/drone-modelleri/profesyonel-drone/parrot-bebop-2-fpv-drone.html [Son Ziyaret Tarihi: 09.05.2022].

[47] Dey, V., Pudi, V., Chattopadhyay, A., & Elovici, Y. (2018, January). Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study. In 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID) (pp. 398-403). IEEE.

[48] 2019, *DroneSploit,* Github: https://github.com/dhondta/dronesploit [Son Ziyaret Tarihi: 09.05.2022].

[49] bin Mohammad Fadilah, M. S., Balachandran, V., Loh, P., & Chua, M. (2020, March). DRAT: A drone attack tool for vulnerability assessment. In Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy (pp. 153-155).

[50] Kwon, Y. M., Yu, J., Cho, B. M., Eun, Y., & Park, K. J. (2018). Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles. IEEE Access, 6, 43203-43212.

[51] 2022, MAVLink: https://mavlink.io/en/ [Son Ziyaret Tarihi: 09.05.2022].

[52] Davanian, A., Massacci, F., & Allodi, L. (2017, January). Diversity: A Poor Man's Solution to Drone Takeover. In PECCS (pp. 25-34).

[53] Marty, J. A. (2013). Vulnerability analysis of the mavlink protocol for command and control of unmanned aircraft. AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT.

[54] Won, J., Seo, S. H., & Bertino, E. (2015, April). A secure communication protocol for drones and smart objects. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (pp. 249-260).

[55] Seo, S., & Bertino, E. (2013). Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing. CERIAS, West Lafayette, IN, USA, Tech. Rep. CERIAS TR, 10, 2013.

[56] Sun, H., Wen, Q., Zhang, H., & Jin, Z. (2013). A novel pairing-free certificateless authenticated key agreement protocol with provable security. Frontiers of Computer Science, 7(4), 544-557.

[57] Yang, G., & Tan, C. H. (2011, March). Strongly secure certificateless key exchange without pairing. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (pp. 71-79).

[58] Rajatha, B. S., Ananda, C. M., & Nagaraj, S. (2015, May). Authentication of MAV communication using caesar cipher cryptography. In 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM) (pp. 58-63). IEEE.

[59] Hamsavahini, R., Praneeth, V., & Narayana, S. (2016). Development of light weight algorithms in a customized communication protocol for Micro Air Vehicles.

[60] Allouch, A., Cheikhrouhou, O., Koubâa, A., Khalgui, M., & Abbes, T. (2019, June). MAVSec: Securing the MAVLink protocol for ardupilot/PX4 unmanned aerial systems. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 621-628). IEEE.

[61] Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, 11, 100218.

[62] Chen, C. L., Deng, Y. Y., Weng, W., Chen, C. H., Chiu, Y. J., & Wu, C. M. (2020). A traceable and privacy-preserving authentication for UAV communication control system. Electronics, 9(1), 62.

[63] Manesh, M. R., & Kaabouch, N. (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. Computers & Security, 85, 386-401.

[64] Barker, N. V. (2020). Development of a Drone-Mounted Wireless Attack Platform.

[65] Guo, R., Wang, B., & Weng, J. (2020, April). Vulnerabilities and attacks of UAV cyber physical systems. In Proceedings of the 2020 International Conference on Computing, Networks and Internet of Things (pp. 8-12).

[66] Wesson, K., Rothlisberger, M., & Humphreys, T. (2012). Practical cryptographic civil GPS signal authentication. NAVIGATION, Journal of the Institute of Navigation, 59(3), 177-193.

[67] Giray, S. M. (2013, June). Anatomy of unmanned aerial vehicle hijacking with signal spoofing. In 2013 6th International Conference on Recent Advances in Space Technologies (RAST) (pp. 795-800). IEEE.

[68] Feng, Z., Guan, N., Lv, M., Liu, W., Deng, Q., Liu, X., & Yi, W. (2017, March). Efficient drone hijacking detection using onboard motion sensors. In Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017 (pp. 1414-1419). IEEE.

[69] Yoon, K., Park, D., Yim, Y., Kim, K., Yang, S. K., & Robinson, M. (2017, April). Security authentication system using encrypted channel on uav network. In 2017 First IEEE International Conference on Robotic Computing (IRC) (pp. 393-398). IEEE.

[70] Kerns, A. J., Wesson, K. D., & Humphreys, T. E. (2014, May). A blueprint for civil GPS navigation message authentication. In 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014 (pp. 262-269). IEEE.

[71] Zheng, X. C., & Sun, H. M. (2020). Hijacking unmanned aerial vehicle by exploiting civil GPS vulnerabilities using software-defined radio. Sensors and Materials, 32(8), 2729-2743.

[72] Panice, G., Luongo, S., Gigante, G., Pascarella, D., Di Benedetto, C., Vozella, A., & Pescapè, A. (2017, September). A SVM-based detection approach for GPS spoofing attacks to UAV. In 2017 23rd International Conference on Automation and Computing (ICAC) (pp. 1-11). IEEE.

[73] Manesh, M. R., Kenney, J., Hu, W. C., Devabhaktuni, V. K., & Kaabouch, N. (2019, January). Detection of GPS spoofing attacks on unmanned aerial systems. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-6). IEEE.

[74] Rudo, D., & Zeng, D. (2020). Consumer UAV cybersecurity vulnerability assessment using fuzzing tests. arXiv preprint arXiv:2008.03621.

[75] Strohmeier, M., Lenders, V., & Martinovic, I. (2015, July). Intrusion detection for airborne communication using PHY-layer information. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 67-77). Springer, Cham.

[76] Mitchell, R., & Chen, R. (2013). Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. IEEE transactions on systems, man, and cybernetics: systems, 44(5), 593-604.

[77] Rani, C., Modares, H., Sriram, R., Mikulski, D., & Lewis, F. L. (2016). Security of unmanned aerial vehicle systems against cyber-physical attacks. The Journal of Defense Modeling and Simulation, 13(3), 331-342.

[78] Lu, H., Li, Y., Mu, S., Wang, D., Kim, H., & Serikawa, S. (2017). Motor anomaly detection for unmanned aerial vehicles using reinforcement learning. IEEE internet of things journal, 5(4), 2315-2322.

[79] Condomines, J. P., Zhang, R., & Larrieu, N. (2019). Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation. Ad Hoc Networks, 90, 101759.