Bulletin of the *Transilvania* University of Braşov • Vol. 13 (62) No. 2 - 2020
Series I: Engineering Sciences
https://doi.org/10.31926/but.ens.2020.13.62.1.8

ANTIDRONE WIRELESS PERSONAL SHIELD

M. IVANCIU [1] M. ALEXANDRU [2]

Abstract: *The evolution of small drone technology raises new challenges regarding personal privacy due to the acquisition and flight of unlicensed small drones. Many of these small drones are controlled over Wi-Fi connection making them inexpensive and easy to control. Latest discoveries in vulnerabilities of wireless network protocols give us the advantage to use cyber-attacks as a method of defense. This paper is addressing general audience on how to create a personal shield against small drones with the advantage of being nonintrusive to the other surrounding wireless networks and, at the same time, protecting your personal privacy of a rogue drone.*

Key words: *drone technology, privacy, wireless networks, and cyber-attacks.*

1. Introduction

Small drone technology is developing really fast and it’s becoming more popular than ever. With small comes the challenge of using more light components and small chips to control them. The 802.11 b/g/n wireless network standard is widely used for controlling drones. The basic control of a quadcopter is done over 4 channels.

Types of drones: recreational vs. commercial

Recreational: this types of drones are also called mini or micro drones (under 250 g) and they are pretty inexpensive, with prices from $30 to $150.

Commercial or professional: used for aerial photography, thermal vision, 3D mapping for construction companies, agriculture, with prices starting from $2000 and more. Usually you cannot fly these drones without a drone pilot license [4].

The use of both types of drones is strictly regulated in every county to protect important sites and privacy of individuals [5].

Using high end drones that are also equipped with GPS is relatively easy and you cannot fly over critical sites and forbidden areas like airports due to geotagging restrictions embedded in their software [6]. The example is presented in Figure 1.

[1] Dept. of Electronics and Computers, *Transilvania* University of Braşov, Romania.

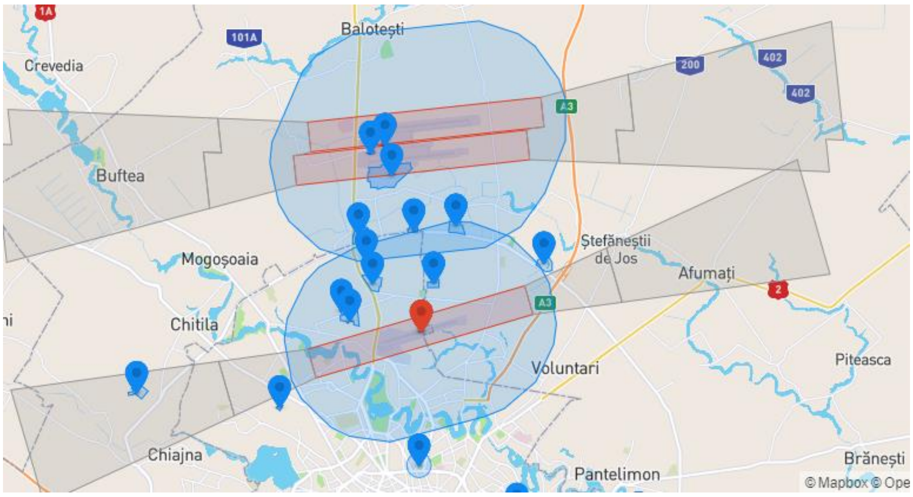


Fig. 1. *Example of DJI drone manufacturer GEO zones that prohibit flight over protected site*

Counter drone technologies classification:

1. Drone monitoring equipment: Radio Frequency Analyzers, Acoustic Sensors, Optical Sensors, Radar.

2. Drone countermeasures equipment: Physically destroying the drone, neutralizing the drone, Taking control of the drone.

Neutralizing the drone: RF jammers, GPS spoofers, High Power Microwave Devices, High Energy Lasers [9]. Almost all of this neutralizing solutions present higher disadvantages like higher costs, bigger power consumption and being disruptive to the surrounding networks and devices. They are mainly intended for military and law enforcement purposes.

But the problem remains with recreational drones that don’t have GPS and can fly unrestrictedly. One of the studies prove that safeguarding a specific site can be done using multiple platforms of raspberry pi computers that detect and take control of drones flying over [7], [8].

However a more portable (carry in the pocket) solution is needed for individual protection and so a raspberry pi zero computer connected to a power bank will do that.

Using a smartphone and a SSH session for the raspberry pi zero we can effectively stop a rogue drone.

This approach exploits the fact that the mode of communication between the drone and its master is wireless. The main goal of existing tools is to disrupt the communication between the drone and its master intentionally by causing interferences or collisions at the receiver side.

Considering the fact that every access point is aware of his „neighbors” so that it can avoid collisions on radio channels we can use a feature called „monitor mode”. By reverse engineering this „flaw” we now have a tool for selectively scanning and attacking a target, in our case the AP of a drone.

Basically a drone is actually a flying Access Point.

- **Practical solution and experimentation**

How: using the vulnerability of unprotected management frames later stipulated by 802.11 w standard [1].

Type: Denial-of-service attack through forged disassociations and deauthentications.

Hardware: raspberry pi zero w, power bank, victim drone (global drone exa GD89).

Software: kali linux pentester edition for raspberry pi zero w, airodump-ng, aireplay-ng suite [2]. The system implementation is presented in Figure 2.

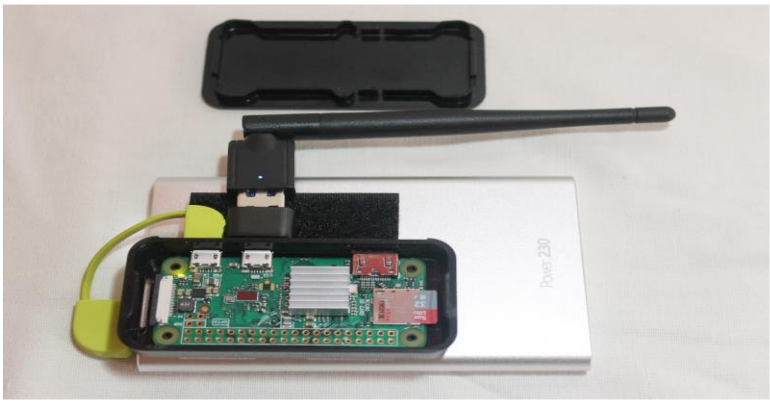


Fig. 2. *Raspberry Pi Zero W equipped with wireless card capable of packet injection*

Fig. 3. *Small low cost drone Global EXA GD 89*

- **Relatively low cost drone using only Wi-Fi control and video transmission (global drone exa GD89)**

The experimental target drone is presented in Figure 3.

The most spread out antidrone solutions imply either use of excess radiofrequency that will disturb the wireless surroundings or GPS spoofing and emissions so that the drone will be confused of its actual position.

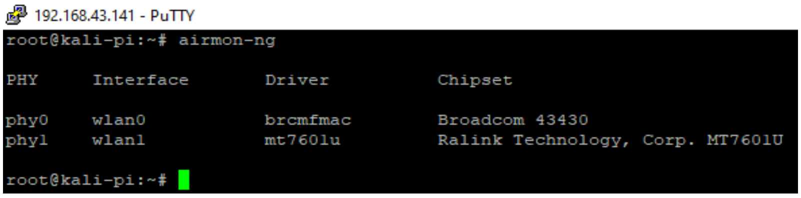
The use of excess radiofrequency power is strictly forbidden and GPS spoofing will not be effective for cheap drones not having GPS.

So the best way is to use cyber-attacks.

Due to the fact that the internal wireless card of the raspberry pi zero has a limited range it's more suited to use any USB wireless card that can work in monitor mode (promiscuous mode) and packet injection [10].

- **Description**

Airmon-ng is a script used to enable monitor mode on wireless interfaces [11].

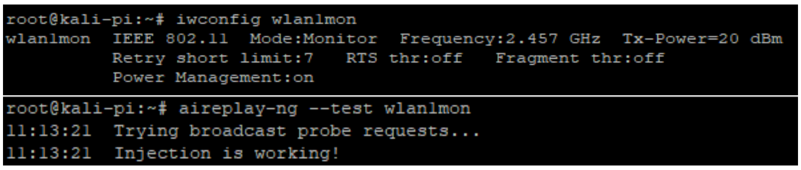


192.168.43.141 - PuTTY

```
root@kali-pi:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           brcmfmac        Broadcom 43430
phy1    wlan1           mt7601u         Ralink Technology, Corp. MT7601U

root@kali-pi:~#
```

Fig. 4. *Enabling monitor mode for the wireless interface* [11]

In Figure 4 the Ralink MT7601U chipset is capable of working in monitor mode and packet injection.

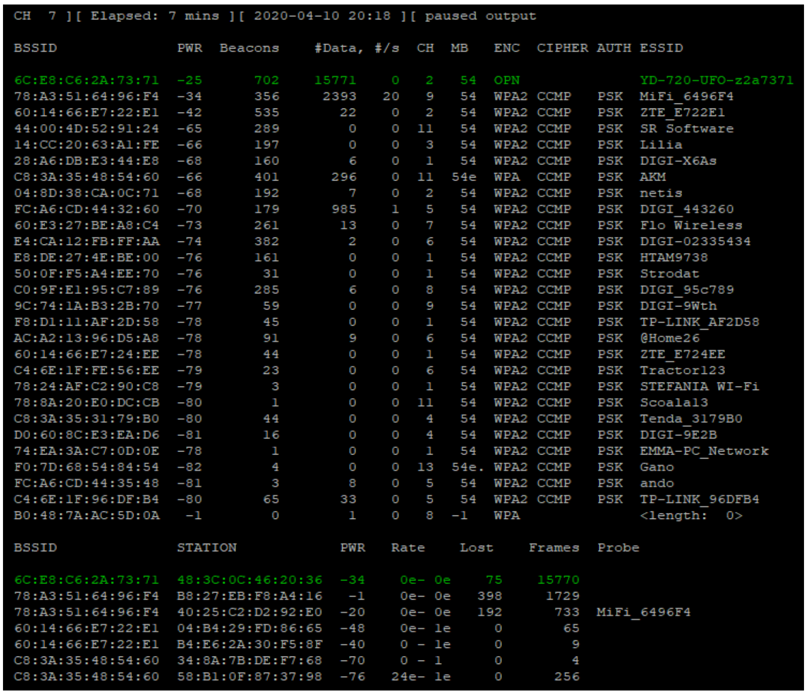


```
root@kali-pi:~# iwconfig wlan1mon
wlan1mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

```
root@kali-pi:~# aireplay-ng --test wlan1mon
11:13:21  Trying broadcast probe requests...
11:13:21  Injection is working!
```

Fig. 5. *Packet injection capability test*

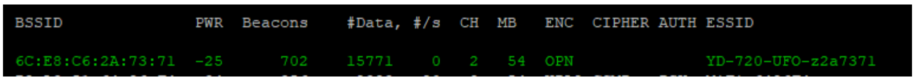
Figure 5 specifies how using "**airodump-ng**" command enables scanning for wireless networks in our surroundings. This will work only if our wireless card is working in ''monitor mode'' [12].



```
 CH  7 ][ Elapsed: 7 mins ][ 2020-04-10 20:18 ][ paused output

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

 6C:E8:C6:2A:73:71  -25      702    15771    0   2  54   OPN              YD-720-UFO-z2a7371
 78:A3:51:64:96:F4  -34      356     2393   20   9  54   WPA2 CCMP   PSK  MiFi_6496F4
 60:14:66:E7:22:E1  -42      535       22    0   2  54   WPA2 CCMP   PSK  ZTE_E722E1
 44:00:4D:52:91:24  -65      289        0    0  11  54   WPA2 CCMP   PSK  SR Software
 14:CC:20:63:A1:FE  -66      197        0    0   3  54   WPA2 CCMP   PSK  Lilia
 28:A6:DB:E3:44:E8  -68      160        6    0   1  54   WPA2 CCMP   PSK  DIGI-X6As
 C8:3A:35:48:54:60  -66      401      296    0  11  54e  WPA  CCMP   PSK  AKM
 04:8D:38:CA:0C:71  -68      192        7    0   2  54   WPA2 CCMP   PSK  netis
 FC:A6:CD:44:32:60  -70      179      985    1   5  54   WPA2 CCMP   PSK  DIGI_443260
 60:E3:27:BE:A8:C4  -73      261       13    0   7  54   WPA2 CCMP   PSK  Flo Wireless
 E4:CA:12:FB:FF:AA  -74      382        2    0   6  54   WPA2 CCMP   PSK  DIGI-02335434
 E8:DE:27:4E:BE:00  -76      161        0    0   1  54   WPA2 CCMP   PSK  HTAM9738
 50:0F:F5:A4:EE:70  -76       31        0    0   1  54   WPA2 CCMP   PSK  Strodat
 C0:9F:E1:95:C7:89  -76      285        6    0   8  54   WPA2 CCMP   PSK  DIGI_95c789
 9C:74:1A:B3:2B:70  -77       59        0    0   9  54   WPA2 CCMP   PSK  DIGI-9Wth
 F8:D1:11:AF:2D:58  -78       45        0    0   1  54   WPA2 CCMP   PSK  TP-LINK_AF2D58
 AC:A2:13:96:D5:A8  -78       91        9    0   6  54   WPA2 CCMP   PSK  @Home26
 60:14:66:E7:24:EE  -78       44        0    0   1  54   WPA2 CCMP   PSK  ZTE_E724EE
 C4:6E:1F:FE:56:EE  -79       23        0    0   6  54   WPA2 CCMP   PSK  Tractor123
 78:24:AF:C2:90:C8  -79        3        0    0   1  54   WPA2 CCMP   PSK  STEFANIA WI-Fi
 78:8A:20:E0:DC:CB  -80        1        0    0  11  54   WPA2 CCMP   PSK  Scoala13
 C8:3A:35:31:79:B0  -80       44        0    0   4  54   WPA2 CCMP   PSK  Tenda_3179B0
 D0:60:8C:E3:EA:D6  -81       16        0    0   4  54   WPA2 CCMP   PSK  DIGI-9E2B
 74:EA:3A:C7:0D:0E  -78        1        0    0   1  54   WPA2 CCMP   PSK  EMMA-PC_Network
 F0:7D:68:54:84:54  -82        4        0    0  13  54e. WPA2 CCMP   PSK  Gano
 FC:A6:CD:44:35:48  -81        3        8    0   5  54   WPA2 CCMP   PSK  ando
 C4:6E:1F:96:DF:B4  -80       65       33    0   5  54   WPA2 CCMP   PSK  TP-LINK_96DFB4
 B0:48:7A:AC:5D:0A   -1        0        1    0   8  -1   WPA              <length:  0>

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 6C:E8:C6:2A:73:71  48:3C:0C:46:20:36  -34    0e- 0e    75    15770
 78:A3:51:64:96:F4  B8:27:EB:F8:A4:16   -1    0e- 0e   398     1729
 78:A3:51:64:96:F4  40:25:C2:D2:92:E0  -20    0e- 0e   192      733  MiFi_6496F4
 60:14:66:E7:22:E1  04:B4:29:FD:86:65  -48    0e- 1e     0       65
 60:14:66:E7:22:E1  B4:E6:2A:30:F5:8F  -40    0 - 1e     0        9
 C8:3A:35:48:54:60  34:8A:7B:DE:F7:68  -70    0 - 1      0        4
 C8:3A:35:48:54:60  58:B1:0F:87:37:98  -76   24e- 1e     0      256
```

Fig. 6. *Scanning for wireless access points and stations*

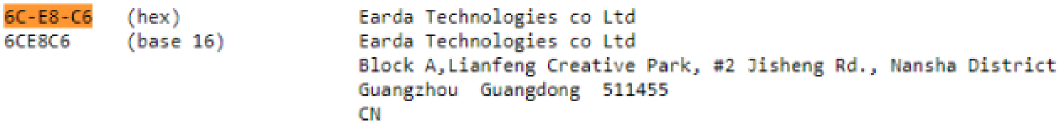
In Figure 6 we can see the Access Point of a drone and the station associated with it.



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

6C:E8:C6:2A:73:71  -25      702    15771    0   2   54  OPN              YD-720-UFO-z2a7371
```

Fig. 7. *Wireless controlled drone discovered and the MAC address*

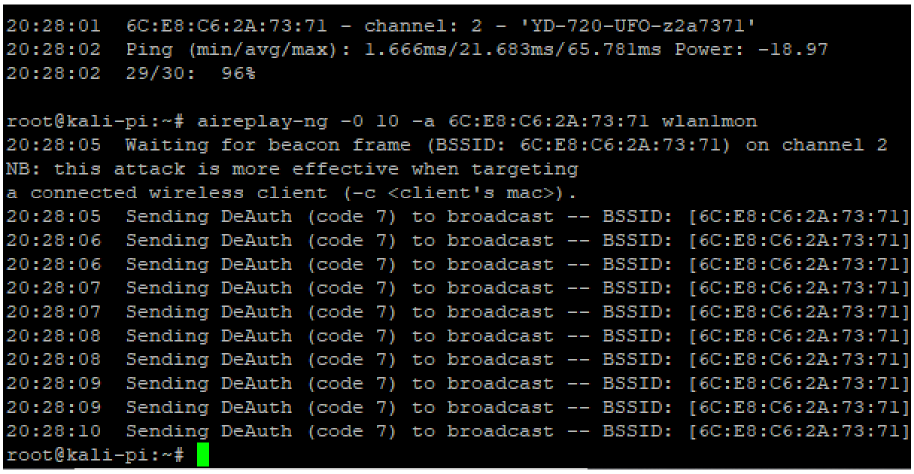
Figure 7 presents the MAC address of the drone we now can selectively target and deauth the drone.



```
6C-E8-C6   (hex)          Earda Technologies co Ltd
6CE8C6     (base 16)      Earda Technologies co Ltd
                          Block A,Lianfeng Creative Park, #2 Jisheng Rd., Nansha District
                          Guangzhou  Guangdong  511455
                          CN
```

Fig. 8. *International database of drone MAC producers*

Figure 8 presents the producer of this drone according to international regulations [14].



```
20:28:01  6C:E8:C6:2A:73:71 - channel: 2 - 'YD-720-UFO-z2a7371'
20:28:02  Ping (min/avg/max): 1.666ms/21.683ms/65.781ms Power: -18.97
20:28:02  29/30:  96%

root@kali-pi:~# aireplay-ng -0 10 -a 6C:E8:C6:2A:73:71 wlan1mon
20:28:05  Waiting for beacon frame (BSSID: 6C:E8:C6:2A:73:71) on channel 2
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
20:28:05  Sending DeAuth (code 7) to broadcast -- BSSID: [6C:E8:C6:2A:73:71]
20:28:06  Sending DeAuth (code 7) to broadcast -- BSSID: [6C:E8:C6:2A:73:71]
20:28:06  Sending DeAuth (code 7) to broadcast -- BSSID: [6C:E8:C6:2A:73:71]
20:28:07  Sending DeAuth (code 7) to broadcast -- BSSID: [6C:E8:C6:2A:73:71]
20:28:07  Sending DeAuth (code 7) to broadcast -- BSSID: [6C:E8:C6:2A:73:71]
20:28:08  Sending DeAuth (code 7) to broadcast -- BSSID: [6C:E8:C6:2A:73:71]
20:28:08  Sending DeAuth (code 7) to broadcast -- BSSID: [6C:E8:C6:2A:73:71]
20:28:09  Sending DeAuth (code 7) to broadcast -- BSSID: [6C:E8:C6:2A:73:71]
20:28:09  Sending DeAuth (code 7) to broadcast -- BSSID: [6C:E8:C6:2A:73:71]
20:28:10  Sending DeAuth (code 7) to broadcast -- BSSID: [6C:E8:C6:2A:73:71]
root@kali-pi:~#
```

Fig. 9. *Attacking the drone over a wireless connection*

This solution can be repeated indefinitely and can disable a rogue drone without interfering with any other device. The main purpose is to „disable” the drone from moving forward not to take it down. The example is presented in Figure 9.

The name „personal shield” resembles the fact that this kind of solution creates a barrier for the drone so it cannot continue to move towards you. The great advantage is that it is effective regardless of the encryption level of the wireless link between the master and the drone.

- **Future work**

Creating a script so that the scanning and attacking feature to work automatically when detecting a specific drone MAC (if it's in my wireless range it means it's invading my privacy).

Exploring more types of wireless attack vectors like: ARP poisoning, buffer overflow, downgrade attacks, port scans and obtaining a „shell”.

2. Conclusions

By using this kind of device you can control the wireless environment surrounding you. Small drones create access points and are controlled via wireless connections. Cyber-attacks can be extremely efficient against this kind of devices and present an even greater advantage of being nonintrusive to the other wireless networks nearby.

The aim is to disable a rogue drone so it cannot communicate with its master without interfering with the surrounding environment. Scanning the MAC address of a drone will enable a directed attack, making this kind of device efficient and reliable.

To effectively prevent a deauthentication attack, both client and access point must support the 802.11w standard with protected management frames (PMF). This standard is rarely used and so creates the perfect conditions for this kind of method.

This solution is addressing the problem of dealing with the majority of inexpensive drones controlled only on Wi-Fi channels, not having GPS geotagging restrictions and being able to fly even in airports.

This is a personal „carry in the pocket” solution that can be powered from a simple small power bank!

References

1. https://standards.ieee.org/standard/802_11w-2009.html. Accessed: 10.02.2020.
2. https://www.kali.org/penetration-testing-with-kali-linux/. Accessed: 10.02.2020.
3. https://github.com/seemoo-lab/nexmon. Accessed: 10.02.2020.
4. https://uavcoach.com/types-of-drones/. Accessed: 09.04.2020.
5. https://dronerules.eu/en/recreational. Accessed: 09.04.2020.
6. https://www.dji.com/flysafe/geo-map. Accessed: 09.04.2020.
7. https://hal.inria.fr/hal-01635125/document. Accessed: 09.04.2020.
8. https://www.youtube.com/watch?v=eAjKE3QyJR8&t=12s. Accessed: 09.04.2020.
9. https://www.robinradar.com/press/blog/9-counter-drone-technologies-to-detect-and-stop-drones-today. Accessed: 09.04.2020.
10. https://miloserdov.org/?p=2196. Accessed: 09.04.2020.
11. https://www.aircrack-ng.org/doku.php?id=airmon-ng. Accessed: 09.04.2020
12. https://www.aircrack-ng.org/~~V:/doku.php?id=airodump-ng. Accessed: 09.04.2020.
13. https://www.aircrack-ng.org/doku.php?id=deauthentication. Accessed: 09.04.2020.
14. http://standards-oui.ieee.org/oui/oui.txt. Accessed: 09.04.2020.