Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles

Charan Gudla[*], Md. Shohel Rana, and Andrew H. Sung
School of Computing Sciences and Computer Engineering, The University of Southern Mississippi,
Hattiesburg, MS 39406, U.S.A.

Abstract - *Unmanned aerial vehicles (UAVs) or drones serve a wide range of applications from surveillance to combat missions. UAVs carry, collect, or communicate sensitive information which becomes a target for the attacks. Securing the communication network between the operator and the UAV is therefore crucial. So far, the networks used in most UAV applications are static, which allows more time and opportunity for the adversary to perform cyber-attacks on the UAV. In this paper we propose to study Moving Target Defense (MTD) technique against cyber-attacks on the drones including wireless network encryption and intrusion detection system. MTD technique change the static nature of the systems to increase both the difficulty and the cost (effort, time, and resources) of mounting attacks. For illustration purpose, a well-known cyberattack is performed on a popular commercial drone and results are presented to show the network vulnerabilities, damages caused due to the attacks and defense techniques to prevent the attacks.*

Keywords: Unmanned Aerial Vehicle (UAV), cyber-attacks, Moving Target Defense (MTD).

1 Introduction

Unmanned Aerial Vehicles (UAVs) or Drones are widely increasing in its population [1]. Due to fact that they are efficient, low cost, light weight and easy to control, drones serve in applications such as military [2], monitoring [3] [4], disaster relief [5] and rescue operations [6]. UAV is used to extend the wireless network coverage in telecommunications field [7]. Amazon prime air [8] is a future service by amazon which uses drone to deliver packages.

Though there are many advantages of drones, they are prone to various physical and cyberattacks. The common forms of communication over a network to send and receive data are Satellite, Cellular, Wi-Fi, GPS, ZigBee. In 2009, Iraqi insurgents hacked predator drone feeds [9]. In 2011, a computer virus has infected networks used by pilots controlling US air force drones at Creech air force base in Nevada [10]. In 2011 itself an American Lockheed Martin RQ-170 Sentinel unmanned aerial vehicle was captured by cyberwarfare unit of Iranian forces in Iran [11]. The predator drone video feeds were exposed online without the knowledge of the operator [12]. Wireless network jammers and GPS spoofing devices available at low costs are used to perform such kind of attacks.

In this paper, we discuss various vulnerabilities of UAV's and the hacking techniques are explored. Existing defense techniques which help in defense against cyber-attacks are reviewed. To show the vulnerabilities of the drone and exploitation, we created a base station and a well-known hacking technique is implemented on UAV Parrot AR Drone. By implementing hacking technique, it shows that the attacker can make severe damage to the drone or take control over it by compromising the wireless network between the operator and drone. The experiment helps to understand the importance of securing UAV systems against cyber-attacks.

The rest of the paper is organized as follows. Section 2 introduces the related work done to prevent cyber-attacks on drones. Section 3 presents various hacking techniques which can be implemented to crash or take control over the drone. Section 4 demonstrates a hacking technique experiment implemented on the AR Drone. In Section 5 we discuss about Defense techniques against cyber-attacks on drones and the results are elaborated.

2 Related work

Various defense techniques have been proposed against these attacks on drones. In [13] Nils Miro Rodday et al. suggested the use of secure encryption schemes for Wi-Fi access point. In [14] Johann Pleban et al. showed a method of encrypting the wireless network where the drone acts as client and RC as an access point. The open Wi-Fi network is encrypted by WPA supplicant to stop the attacker hacking the drone. In [15] Chaitanya Rani et al. illustrated vulnerabilities of drone and suggested encryption, Intrusion detection systems as defense mechanisms. Kim Hartmann and Christoph Steup [16] developed a risk assessment scheme on services and communication infrastructure. James Goppert et al. [17] evaluated cyberattack severity by establishing a metric to indicate the time of complete failure of the system. In [18] Robert Mitchell and Ing-Ray Chen developed behavior rule-based UAV intrusion detection system for capturing malicious behavior when UAV is under attack and prohibit its continuation.

3 Hacking techniques

In this section, UAV wireless network attacking techniques are discussed. Our experiment of hacking is applied on most popular drone and results are illustrated.

Drone wireless network can be hacked when the attacker knows the MAC address of specific drone he wants to hack.

The type of attacks on wireless network of drones are as follows:

a. Data packet capture
b. Denial of service (DoS) attack
c. Man-in-the-middle attack (MIMA)

3.1 Data packet capture

The hacker gathers the required information about the target by data packet capture method. The wireless network of the drone sends out the beacons frames which can be captured, and it consists of MAC addresses of the drone and remote-control device operating the drone, the type of encryption (WEP/WPA/WPA2/OPN) and the wireless network channel it is operating on. Aircrack-ng, Wireshark are the tools used to capture the wireless network frames.

3.2 Denial of service (DoS) attack

The wireless network [19] access points are hacked by de-authentication flood attacks (DoS) [20]. Continuous de-authentication requests are sent to the targeted access point exhausting its memory. Due to this the clients cannot contact the access point since, there is no memory left to reconnect with the clients which leaves no connection between them. The de-authentication attack will target MAC address of the access point which is called as BSSID (captured from data packet capture) so that, all the clients are disconnected from the access point or using MAC address of a specific targeted client is disconnected. The clients try to reconnect with the access point, but they will fail until the de-authentication attack is stopped.

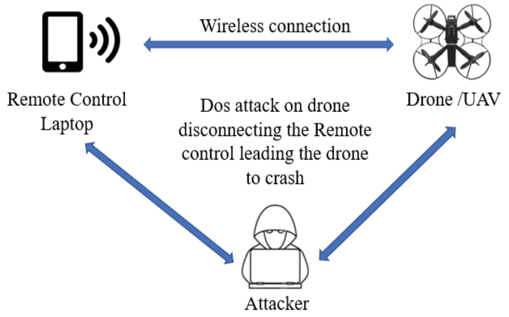

Wireless connection
Remote Control Laptop
Drone /UAV
Dos attack on drone disconnecting the Remote control leading the drone to crash
Attacker

Fig. 1. Denial of Service (DoS) attack

3.3 Man-in-the-middle attack

The attacker spoofs and gain control over the communication network between the drone and remote control (RC) device user. The system details gathered from the initial data capture helps him sending the authentication commands to the drone as if he is the original RC user. The data feed, location from the drone will be seen by the hacker without the knowledge of both drone and RC user. If the wireless network is protected with a password, then by handshake protocol the keys for authentication can be obtained by Aircrack-ng and crunch tools.

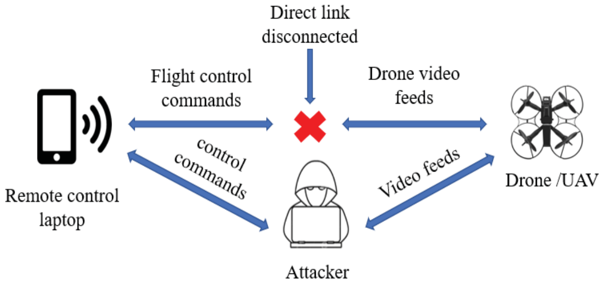
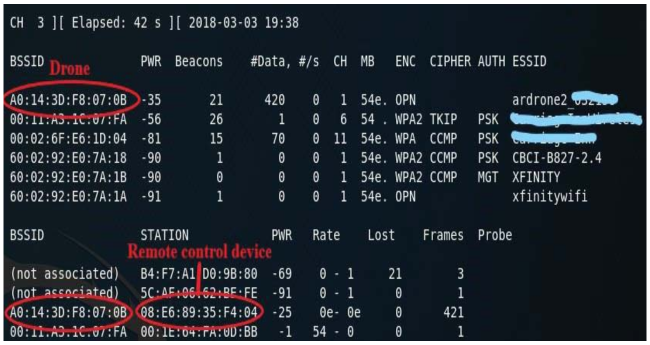


Fig. 2. Man-in-the-Middle Attack

4 Cyber-attack on drones

One of the most popular hacking technique (DoS) is implemented on drone static network. We used Parrot A.R drone for the experiment. In this technique, the remote-control device is disconnected from the drone by continuously sending the de-authentication commands. The drone will crash immediately, or the attacker will take control of drone by connecting to his device. Kali Linux in a virtual machine is used with a bridge adapter Alfa AWUS036NHA USB wireless adapter. Aircrack-ng [21] is the suite containing the necessary tools to attack the drone. The following are the commands used to attack the drone.

```
root@kali: ~# iwconfig wlan0 mode monitor
root@kali: ~# ifconfig up
root@kali: ~# aireplay-ng -9 wlan0
root@kali: ~# airodump-ng wlan0
```



```
CH  3 ][ Elapsed: 42 s ][ 2018-03-03 19:38

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

A0:14:3D:F8:07:0B  -35       21      420    0   1  54e. OPN              ardrone2_[redacted]
00:11:A3:1C:07:FA  -56       26        1    0   6  54 . WPA2 TKIP   PSK  [redacted]
00:02:6F:E6:1D:04  -81       15       70    0  11  54e. WPA  CCMP   PSK  [redacted]
60:02:92:E0:7A:18  -90        1        0    0   1  54e. WPA2 CCMP   PSK  CBCI-B827-2.4
60:02:92:E0:7A:1B  -90        0        0    0   1  54e. WPA2 CCMP   MGT  XFINITY
60:02:92:E0:7A:1A  -91        1        0    0   1  54e. OPN              xfinitywifi

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   B4:F7:A1:D0:9B:80  -69    0 - 1     21        3
(not associated)   5C:AF:06:62:BE:FE  -91    0 - 1      0        1
A0:14:3D:F8:07:0B  08:E6:89:35:F4:04  -25    0e- 0e     0      421
00:11:A3:1C:07:FA  00:1E:64:FA:0D:BB   -1   54 - 0      0        1
```

Fig. 3. Data packet capture showing MAC addresses

Executing above commands will implement the data capture attack on wireless network resulting in capturing of beacon frames consisting source and destination MAC addresses. The MAC addresses shown in Fig. 3 are the drone's MAC address and remote-control device listed as station controlling the drone.

```
root@kali: ~# aireplay-ng -0 0 -a droneBSSID -c remotecontrolBSSID wlan0
```

The above command launches the cyber-attack on the drone leading it to crash. Fig. 4 and Fig. 5 shows the communication link before and after the cyber-attack respectively.

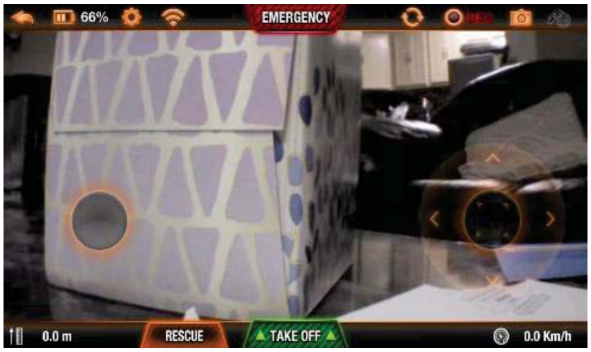


Fig. 4. Communication link before dos attack

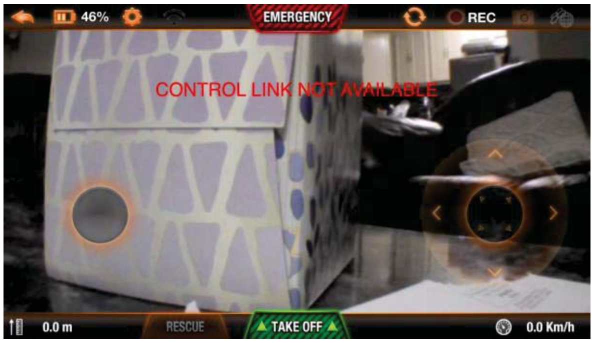


Fig. 5. Communication link after dos attack

5 Defense against cyber attacks

For enhancing the security of the drones, we propose various defense techniques listed below.

a. Wireless network encryption
b. Intrusion detection system (IDS)
c. Moving target defense (MTD)

We created a base station control system for Parrot A.R drone which consists of above security measures. The base station model is shown in Fig. 6 and Fig. 7.

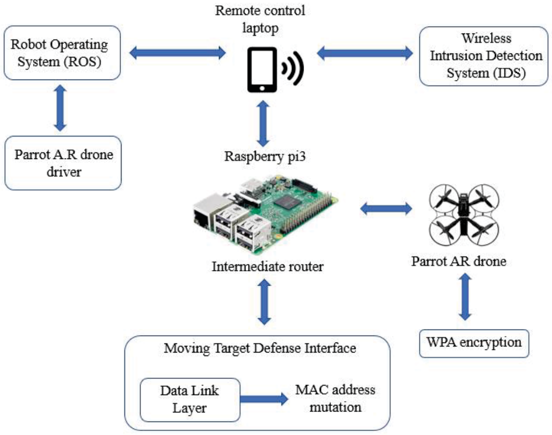


Fig. 6. Base station control system model

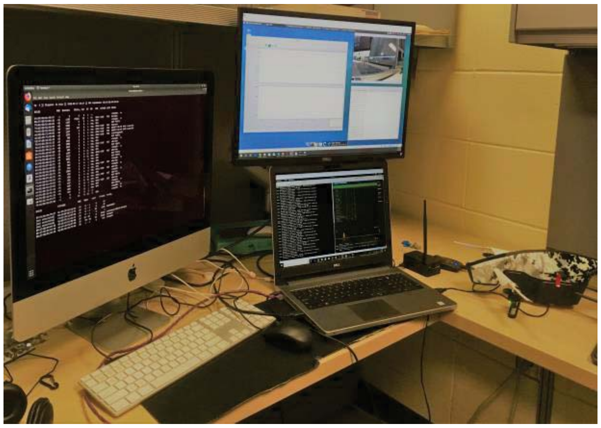


Fig. 7. Base station

Raspberry Pi is an affordable low-cost computer that can be used in different projects. We are using it as an intermediate router [22] and establish a secure wireless network between remote control and the drone. It is configured in such a way that it will act as a hotspot connecting devices into the network and make a communication link between them. The remote-control laptop sends control commands to the drone via raspberry pi router and the drone send live video feed to the laptop through raspberry pi router. The raspberry pi wireless network is secured with WPA2 encryption.

Fig. 8. Raspberry Pi

The Robot Operating System (ROS) [23] is a collection of tools and libraries that simplify the task of creating robust robotic applications. As part of this ROS consists of AR drone driver to communicate with drone and control it. Using ROS, we can develop autonomous tasks for the drone to accomplish.

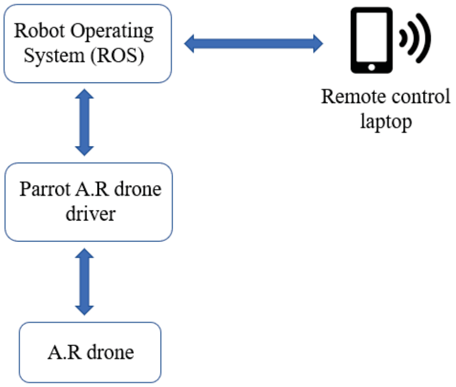


Fig. 9. ROS model

5.1 Wireless network encryption

Since, AR drone will act as an access point and its network is unencrypted and open, multiple devices can be connected to it but only device can control it. Disconnecting the authentic user and reconnecting to drone by fake user compromises the drone. The wireless network of the drone can be encrypted with WPA2 security by installing the compiled binaries of WPA supplicant [24] into the drone libraries. The binaries wpa_cli, wpa_passphrase, wpa_supplicant should be included in the bin folder of the drone in order accomplish it. After successful installation of the binaries, drone will stop acting as access point and it will connect to the provided access point name and passphrase (in our case it will connect to the raspberry pi).

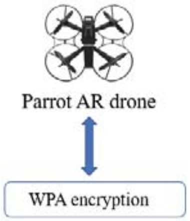


Fig. 10. WPA binaries in AR drone

5.2 Intrusion detection system

Intrusion detection system monitors the wireless network in Realtime. Intrusion is an un-authorized entry into the network without knowledge of the true owner. The systems can be spoofed, tricked leading to direct access to the malicious user. The supervision of malicious activities, attacks, spoofing on the network is Intrusion detection.

IDS are kind of defensive tools but doesn't provide preventive actions against the attacks. It's usually a software which monitors the network behavior and notify if there are any anomalies.

Kismet wireless IDS is used to monitor the drone wireless network [25]. The list of alerts is included in the configuration file of the kismet to actively monitor the network and notify in case of any suspicious activities.

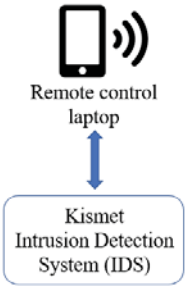


Fig. 11. Kismet IDS

5.3 Moving target defense

Moving Target Defense [26] is a technique where system characteristics are changed from static to dynamic, thus increasing the complexity for the hacker to attack. The network between any two nodes is considered static until now. This gives ample time for the attacker to gather the information regarding system configuration like OS, Network IP address, MAC address, etc. The information gathered is sufficient for the attacker to exploit vulnerabilities and launch attacks on the network. Moving target defense techniques completely change the game by implementing randomness in the system configuration which makes it less static, less deterministic and less homogenous [26]. This takes the attacker to spend more time, thus increasing the operational cost and complexity in understanding.

We used raspberry pi to implement moving target defense by changing MAC address periodically. Fig. 12 shows the moving target defense model.

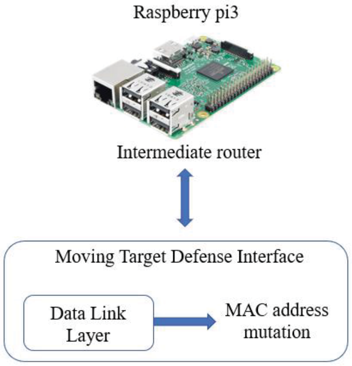


Fig. 12. Moving Target Defense model

6 Configuration

The following changes are made to “kismet.conf” file to detect and monitor the wireless network. The following alerts will be generated in case of corresponding malicious activities on the network.

```
#kismet.conf

alert=NETSTUMBLER,10/min,1/sec
alert=WELLENREITER,10/min,1/sec
alert=LUCENTTEST,10/min,1/sec
alert=DEAUTHFLOOD,10/min,2/sec
alert=BCASTDISCON,10/min,2/sec
alert=CHANCHANGE,5/min,1/sec
alert=AIRJACKSSID,5/min,1/sec
alert=PROBENOJOIN,10/min,1/sec
alert=DISASSOCTRAFFIC,10/min,1/sec
alert=NULLPROBERESP,10/min,1/sec
alert=BSSTIMESTAMP,10/min,1/sec
alert=MSFBCOMSSID,10/min,1/sec
alert=LONGSSID,10/min,1/sec
alert=MSFDLINKRATE,10/min,1/sec
alert=MSFNETGEARBEACON,10/min,1/sec
alert=DISCONCODEINVALID,10/min,1/sec
alert=DEAUTHCODEINVALID,10/min,1/sec

# Do we have a GPS?
gps=false
```

```
# Log file directory
configdir=/var/log/kismet/
```

MAC address mutation in the layer 2 of OSI model is accomplished using compiled libraries of macchanger tool in raspberry pi by executing following script.

```
#! /bin/bash
macchanger --show wlan0
Ifconfig wlan0 down
macchanger -r -b wlan0
Ifconfig wlan0 up
macchanger --show wlan0
sudo service network-manager start
```

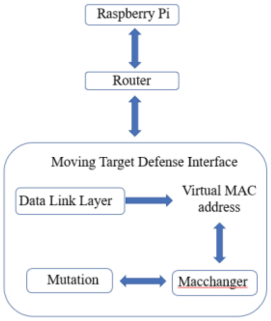
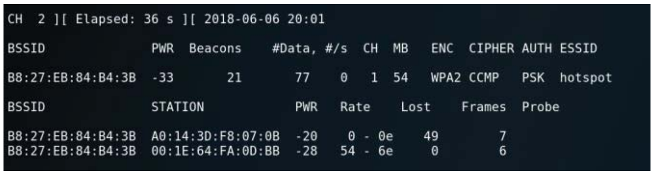


Fig. 13. MAC address mutation model

7 Results

In this section we show the implementation of defense techniques against cyber-attack on parrot AR drone wireless network and alerts produced by IDS which is monitoring the drone wireless network. The data capture attack gathers the required information about the network to launch the attack as shown in Fig. 14. The wireless network is encrypted with WPA2 security which can be seen under ENC column in Fig. 14 so that the attacker cannot directly connect or intercept the wireless network.



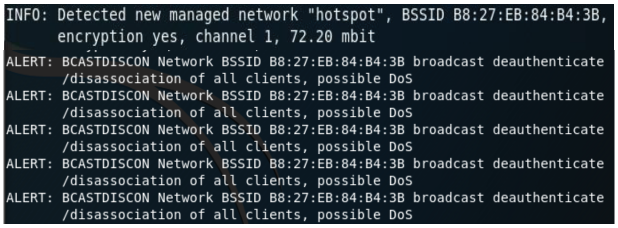
```
CH  2 ][ Elapsed: 36 s ][ 2018-06-06 20:01

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

B8:27:EB:84:B4:3B  -33       21       77    0   1  54   WPA2 CCMP   PSK  hotspot

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B8:27:EB:84:B4:3B  A0:14:3D:F8:07:0B  -20    0 - 0e    49       7
B8:27:EB:84:B4:3B  00:1E:64:FA:0D:BB  -28   54 - 6e     0       6
```

Fig. 14. Data capture attack

```
root@kali: ~# aireplay-ng -0 0 -a droneBSSID -c remotecontrolBSSID wlan0
```

Using above command, Dos attack can be implemented on the drone wireless network. Since the drone and remote-control laptop are connected to raspberry pi, cyber-attack will be launched on the MAC address of the raspberry pi. The wireless network is named as “hotspot” as shown in Fig. 14. The associated drone and remote-control laptop MAC addresses are listed under STATION column.

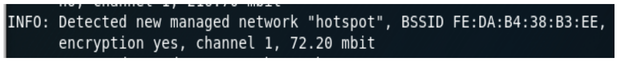
Since, the wireless network is monitored by the kismet IDS, it will detect and alert the user about the malicious activity on the network as shown below in Fig. 15.



```
INFO: Detected new managed network "hotspot", BSSID B8:27:EB:84:B4:3B,
      encryption yes, channel 1, 72.20 mbit
ALERT: BCASTDISCON Network BSSID B8:27:EB:84:B4:3B broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID B8:27:EB:84:B4:3B broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID B8:27:EB:84:B4:3B broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID B8:27:EB:84:B4:3B broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID B8:27:EB:84:B4:3B broadcast deauthenticate
       /disassociation of all clients, possible DoS
```

Fig. 15. Kismet IDS alerts

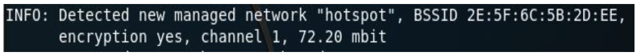
Moving target defense technique is implemented to mutate MAC address of the raspberry pi. Now that the MAC of raspberry pi is changed, the cyber-attack will fail because the attack is launched on previous MAC address. The MAC address of the raspberry pi after random mutation is shown in Fig. 16 detected by kismet IDS.



```
INFO: Detected new managed network "hotspot", BSSID FE:DA:B4:38:B3:EE,
      encryption yes, channel 1, 72.20 mbit
```

Fig. 16. New MAC address after mutation

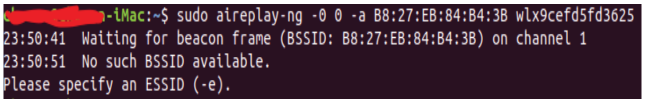
The mutation of MAC address make kismet to detect the wireless network with same domain name but with different MAC as shown in Fig. 17.



```
INFO: Detected new managed network "hotspot", BSSID 2E:5F:6C:5B:2D:EE,
      encryption yes, channel 1, 72.20 mbit
```

Fig. 17. New MAC address after mutation

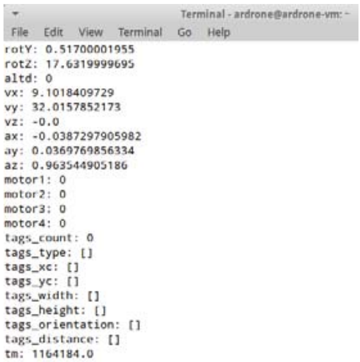
When the hacker attacks the wireless network with the same initial MAC address without the knowledge that the MAC address is changed, the deployed hacking technique will fail to engage as shown in Fig. 18 saying no such BSSID available.



```
[redacted]-iMac:~$ sudo aireplay-ng -0 0 -a B8:27:EB:84:B4:3B wlx9cefd5fd3625
23:50:41  Waiting for beacon frame (BSSID: B8:27:EB:84:B4:3B) on channel 1
23:50:51  No such BSSID available.
Please specify an ESSID (-e).
```

Fig. 18. Failure of cyber-attack

The navigational data transmitted from the drone to the base station contains the acceleration, velocity, altitude and the 4 motors rotational speeds as shown in Fig. 19.


Terminal - ardrone@ardrone-vm: ~
File Edit View Terminal Go Help

```
rotY: 0.51700001955
rotZ: 17.6319999695
altd: 0
vx: 9.1018409729
vy: 32.0157852173
vz: -0.0
ax: -0.0387297905982
ay: 0.0369769856334
az: 0.963544905186
motor1: 0
motor2: 0
motor3: 0
motor4: 0
tags_count: 0
tags_type: []
tags_xc: []
tags_yc: []
tags_width: []
tags_height: []
tags_orientation: []
tags_distance: []
tm: 1164184.0
```

Fig. 19. Navigational data from the drone

The navigational data from the drone contains acceleration and estimated velocity values which are plotted as shown in the Fig. 20.

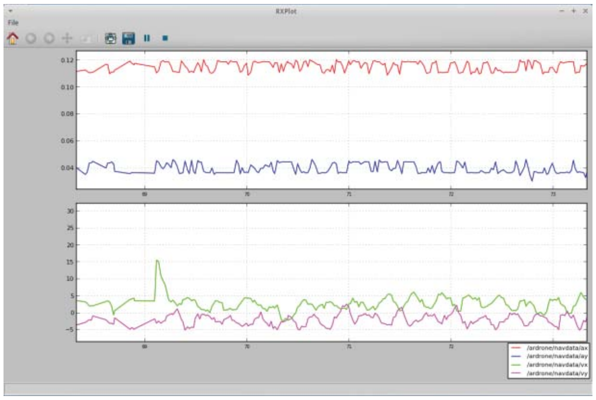


Fig. 20. Acceleration and velocity plots

8 Conclusion

The commercial, civilian, and military applications of UAVs are increasing rapidly, and the vulnerabilities of UAVs create risks to public and private sectors as drones can carry payloads as well as sensitive information, picture, and video feeds, etc. To mitigate the risk, we need to analyze the various vulnerabilities and attack techniques and develop defense techniques for drones against physical and cyber-attacks.

Cyberattacks on UAVs can easily exploit the static nature of wireless network connecting remote control devices and UAVs. The experiments reported in this paper illustrate various vulnerabilities of the network which can be exploited to crash the drone or to take over its control. By implementing wireless encryption, intrusion detection system, MTD technique the system becomes more complex for the attacker to exploit any vulnerabilities and implement/launch attacks. Even though the attacker collects the required information to implement a cyberattack, the network characteristics will be changed, and the attack will fail to engage or execute. In this way the wireless network is hardened to protect the drones against different cyberattacks.

In addition to the military, homeland security organizations are also interested in R&D on moving target defense techniques [27], as the name UAV suggests, unmanned aerial vehicles can accomplish a wide range of missions without the high cost or risks of manned flights. Thwarting cyberattacks on drones is therefore critical for successful deployment of UAVs and a comprehensive study, implementation, analysis and evaluation of MTD techniques outlines the scope of future work of this project. Application of protected management frames (PMF) service to the network will also defend against cyber-attacks. Future work will study software and platform based moving target defense techniques for drones.

9 References

[1] “FAA estimates 7 million drones by 2020”, https://gcn.com/articles/2016/03/28/faa-drone-projections.aspx (28 March 2016, accessed 06 June 2018)

[2] Udeanu, Gheorghe, et al. “Unmanned Aerial Vehicle in Military Operations.” Scientific Research and Education in the Air Force, vol. 18, no. 1, 2016, pp. 199-206., doi:10.19062/2247-3173.2016.18.1.26

[3] Kafi, Mohamed Amine, et al. “A Study of Wireless Sensor Networks for Urban Traffic Monitoring: Applications and Architectures.” Procedia Computer Science, vol. 19, 2013, pp. 617–626., doi: 10.1016/j.procs.2013.06.082

[4] Alvear, Oscar, et al. “Using UAV-Based Systems to Monitor Air Pollution in Areas with Poor Accessibility.” Journal of Advanced Transportation, vol. 2017, 2017, pp. 1–14., doi:10.1155/2017/8204353

[5] Debusk, Wesley. “Unmanned Aerial Vehicle Systems for Disaster Relief: Tornado Alley.” AIAA Infotech@Aerospace 2010, 2010, doi:10.2514/6.2010-3506

[6] Waharte, Sonia, and Niki Trigoni. “Supporting Search and Rescue Operations with UAVs.” 2010 International Conference on Emerging Security Technologies, 2010, doi:10.1109/est.2010.31

[7] Guillen-Perez, Antonio, et al. “Wi-Fi Networks on Drones”. 2016 ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT), 2016, doi:10.1109/itu-wt.2016.7805730

[8] Amazon prime air delivery using drones to deliver the ordered packages, https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011 (accessed 06 June 2018)

[9] Iraqi insurgents hacked predator drone feeds, http://www.cnn.com/2009/US/12/17/drone.video.hacked/index.html (17 December 2009, accessed 18 July 2018)

[10] Computer virus infects drone plane command centre US, https://www.theguardian.com/technology/2011/oct/09/virus-infects-drone-plane-command (9 Oct 2011, accessed 18 July 2018)

[11] American Lockheed Martin RQ-170 Sentinel unmanned aerial vehicle (UAV) was captured by Iranian forces, https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident (accessed 18 July 2018)

[12] Predator drone video feeds exposed online, https://www.bleepingcomputer.com/news/government/us-government-leaves-predator-drone-video-feeds-exposed-online/ (05 May 2015, accessed 18 July 2018)

[13] N. M. Rodday, R. D. O. Schmidt, A. Pras. "Exploring security vulnerabilities of unmanned aerial vehicles", NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium, pp. 993-994, Apr 2016

[14] J. S. Pleban, R. Band, R. Creutzburg, R. Creutzburg, D. Akopian, "Hacking and securing the AR.Drone 2.0 quadcopter: Investigations for improving the security of a toy", International Society for Optics and Photonics, pp. 90300L, feb 2014

[15] Rani C, Modares H, Sriram R, Mikulski D, Lewis FL (2016): Security of unmanned aerial vehicle systems against cyber-physical attacks. Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 2016, Vol. 13(3) 331–342 The Author(s) 2015 DOI: 10.1177/1548512915617252

[16] K. Hartmann, C. Steup, "The vulnerability of UAVs to cyber-attacks an approach to the risk assessment", Cyber Conflict (CyCon) 2013 5th International Conference on, pp. 1-23, 2013

[17] Goppert, James, et al. "Numerical Analysis of Cyberattacks on Unmanned Aerial Systems." Infotech@Aerospace 2012, 2012, doi:10.2514/6.2012-2437

[18] R. Mitchell, I.-R. Chen, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications", IEEE Trans. Syst. Man Cybern. Syst., vol. 44, no. 5, pp. 593-604, May 2014

[19] "Wi-Fi.", Microchip Developer Help, http://microchipdeveloper.com/wifi:start (accessed 12 May 2018)

[20] Compton, Stuart: 802.11 Denial of Service Attacks and Mitigation, SANS Institute InfoSec Reading Room

[21] Aircrack-ng, https://www.aircrack-ng.org/ (accessed 17 June 2018)

[22] RPI-Wireless-Hotspot for raspberry pi to convert into router, https://github.com/harryallerston/RPI-Wireless-Hotspot (accessed 18 June 2018)

[23] Robot Operating System, http://www.ros.org/about-ros/ (accessed 16 June 2018)

[24] WPA2 encryption, https://github.com/daraosn/ardrone-wpa2 (accessed 16 June 2018)

[25] Kismet wireless intrusion detection system for drone, https://raw.githubusercontent.com/kismetwireless/kismet/master/README (accessed 16 June 2018)

[26] H. Okhravi, M.A. Rabe et al., "Survey of Cyber Moving Targets", Lincoln Laboratory - Massachusetts Institute of Technology Technical Report, September 2013

[27] "Moving Target Defense", Homeland Security. https://www.dhs.gov/science-and-technology/csd-mtd (accessed 15 June 2018)