Drones for Smart Cities: Issues in Cybersecurity, Privacy, and Public Safety

Edwin Vattapparamban, İsmail Güvenç, Ali İ. Yurekli, Kemal Akkaya, and Selçuk Uluağaç
Department of Electrical and Computer Engineering, Florida International University, Miami, FL, USA
Email: {evatt001,iguvenc,ayurekli,kakkaya,auluagac}@fiu.edu

***Abstract*—It is expected that drones will take a major role in the connected smart cities of the future. They will be delivering goods and merchandise, serving as mobile hot spots for broadband wireless access, and maintaining surveillance and security of smart cities. However, pervasive use of drones for future smart cities also brings together several technical and societal concerns and challenges that needs to be addressed, including in the areas of cybersecurity, privacy, and public safety. Drones, while can be used for the betterment of the society, can also be used by malicious entities to conduct physical and cyber attacks, and threaten the society. The goal of this survey paper is to review various aspects of drones in future smart cities, relating to cybersecurity, privacy, and public safety. We will also provide representative results on cyber attacks using drones.**

***Index Terms*—Drones, Internet of Things (IoT), privacy, search and rescue, security, UAVs, VPN, WiFi Pineapple.**

I. Introduction

An unmanned aerial vehicle (UAV), also known as drone, is an aircraft with no pilot on board. Enabled by recent technological advances, miniaturization, and open-source hardware/software initiatives [1]–[3], UAVs have found several key applications recently [4]–[10]. Their use in several different contexts are quickly transforming from a futuristic idea to reality. Amazon, for example, claims that seeing its *Prime Air* order delivery UAVs in the sky is expected to be as conventional as seing mail trucks on the road within the next few years[1]. Google and Facebook have been investigating the use of a network of high-altitude balloons[2] and drones[3] over specific population centers for providing broadband connectivity. Such solar-powered drones are capable of flying several years without refueling. UAVs can also be used to deliver broadband data rates in emergency and public safety situations through low-altitude platforms [11].

With the emerging proliferation of drones, it is expected that they will take a major role in the connected smart cities of the future. However, pervasive use of drones for future smart cities also brings together several technical and societal concerns and challenges that needs to be addressed, related to cybersecurity, privacy, and public safety. Drones, while can be used for the betterment of the society, can also be used by malicious entities to conduct physical and cyber attacks, and threaten the society. As the number of drones are increasing, it becomes difficult to identify and interdict potentially harmful drones that can cause threats [12]. In [13], [14], various attack paths to drones have been studied, leading to a complete threat analysis of recently popular commercial UAVs. For example, dependency of drones on GPS is investigated in [15], which warns about threats such as GPS spoofing that may result in loosing control of drones to malicious attackers. Vital information can also be obtained from drones using network exploits and malware based attacks.

The goal of this survey paper is to review various different challenges related to use of drones in future smart cities, related to cybersecurity, privacy, public safety, and forensics. We will also provide representative results on cyber attacks using drones. Rest of the paper is organized as follows. In Section II, recent Federal Aviation Administration (FAA) regulations related to use of drones are summarized. Section III reviews few of the major small commercial drones which are more pervasively available in the market. Section V discusses how drones can be used as cyber attack tools, while Section IV is on vulnerabilities of drones to cyber attacks. Detection and interdiction of unauthorized and potentially malicious drones are discussed in Section VI. Section VII lists some other applications of drones in smart cities, such as for search and rescue, forensics, and public safety communications. Finally, the last section provides some concluding remarks.

II. Recent Regulations on Drones

For maintaining the safety of manned aircrafts and the public, FAA in the United States have developed rules to regulate the use of small UAVs. For example, FAA recently required each small Unmanned Aircraft Systems (UAS) that weighs more than 0.55 lbs and below 55 lbs to be registered in their system[4]. If not complied with the FAA regulations, the owner of a drone can face civil and criminal penalties. The FAA has also released a smartphone application B4UFLY[5] which provides drone users awareness about any restrictions in the location they are planning to operate the drone. The *Know Before You Fly*[6] campaign by FAA aims to educate public about UAV safety and responsibilities.

Overall, FAA regulations for small UAVs include flying them under 400 feet with no obstacles around, maintaining a line of sight with the UAV at all times, not flying UAVs within 5 miles from an airport unless permission is received from the airport and control tower, avoiding endangering of people or aircraft, and not flying near people and stadiums. FAA exempts public aircraft operations by issuing a Certificate of Waiver or Authorization (COA), which allows operators to use airspace for safety provisions. Most of the public uses of UAVs include firefighting, search and rescue, and disaster relief. For civil operations, FAA authorization can be received either by Section 333 Exemption (i.e., by issuing a COA), or by Special Airworthiness Certificate (SAC) in which applicants describe about their design, software development, and control, along with how and where they intend to fly. FAA also enforces Federal Aviation Regulations along with Law Enforcement Agencies (LEAs) to deter, detect, investigate, and stop unauthorized and unsafe UAV operations[7].

[1] http://www.amazon.com/b?node=8037720011.
[2] http://www.google.com/loon/.
[3] https://info.internet.org/en/approach/.
[4] http://www.faa.gov/uas/registration/.
[5] http://www.faa.gov/uas/b4ufly.
[6] http://knowbeforeyoufly.org/.
[7] https://www.faa.gov/uas/.

978-1-5090-0304-4/16/$31.00 ©2016 IEEE

III. Review of Major Small UAVs

In this section, we will review and compare four commercially available and popular small UAVs, in terms of their basic features, wireless communications capabilities, and security vulnerabilities: Parrot AR Drone 2.0, Bebob Drone, Phantom 2 Vision Drone, and 3D Robotics Solo Drone.

A. Parrot AR Drone 2.0

Parrot AR Drone is built by a French company called Parrot and was first revealed in 2010. Subsequently, its version 2.0 was revealed at Consumer Electronics Show (CES) Las Vegas in 2012. It includes a 1 GHz 32 bit ARM Cortex A8 processor with 1 Gbit RAM and supports WiFi standards IEEE 802.11 b/g/n. It comes along with a Linux machine called BusyBox[8], which has Unix tools in an executable file and can run over various operating system interfaces like Linux and Android. This drone can be controlled using various interfaces, like using an Android or iOS app to take images and videos to be stored in the phones and also using tools like LabVIEW which has a dedicated tool kit to control it called AR Drone Toolkit[9]. In [16], AR Drones were used in unknown areas for surveillance, for spying and to detect suspicious devices and objects using an extended Kalman filter. Drones can be controlled using various other programming languages such as Python, javascript, and node.js[10]. Due to their ease of programming, AR Drones have been very popular, and have been used in events such as Nodecopter[11], where many developers come in a group of three, and are provided with AR Drones to showcase their work to other participants.

B. Bebop Drone

Bebop drone is also built by Parrot, and is much powerful compared to Parrot AR Drone 2.0. Bebop weighs around 400 g and it uses a P7 dual core CPU, quad-core GPU, and 8 GB of memory. It comes with a device called Skycontroller, which is used to improve its range. One of the important features in the drone with respect to the drone regulations is that we can select our country in the network settings of the application, which helps us to fly the drone keeping the drone regulations easy to obey in the selected country. Bebop drone uses an WiFi radio type of IEEE 802.11ac, i.e. they can be operated both in 2.4 GHz and 5 GHz range. To maximize the range it is preferable to use 2.4 GHz WiFi and for better quality of videos it is preferable to use 5 GHz WiFi. Bebop's WiFi network uses an IP address of 192.168.42.1. This drone has an open FTP server which includes images, videos and black box readings. Therefore, flight recordings, GPS locations of the drone, among other information, can be easily accessed by an outsider due to open FTP server[12].

C. Phantom 2 Vision Drone

Phantom 2 Vision is built by DJI, founded in 2006. It manufactures UAVs for aerial photography. This drone uses a mobile phone first person view (FPV) system with wireless connection range of up to 300 m, and supports 14 Megapixels image resolution. Receiver range of this drone is attained with the help of a range extender and is larger when compared to other drones. It uses a 2.4 GHz Direct Sequence Spread Spectrum (DSSS), within 2.4 GHz to 2.488 GHz band. Live video is available using the DJI Vision App, connecting the drone with the help of range extender. However, WiFi network has no security features, and WiFi network name cannot be changed because it should remain fixed to allow the drone to get associated with it. Range extender is a Linux machine that uses OpenWRT[13], which always has an IP address of 192.168.1.2. Additionally, Phantom 2 Vision has two other Linux systems: One to access the SD card to obtain the images and recordings using IP 192.168.1.1, and other system is used for recording and encoding using IP address 192.168.1.10. Therefore, it is vulnerable to attacks which allows others to access data packets and GPS coordinates of the drone[14].

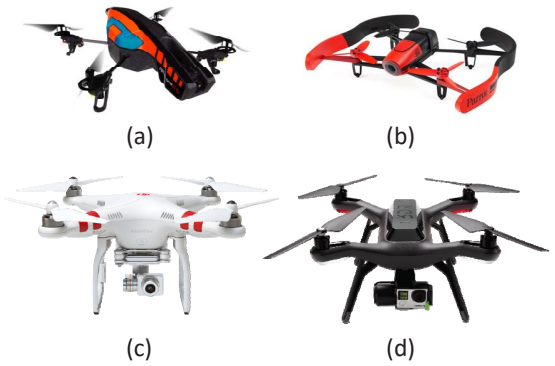


Fig. 1: (a) Parrot AR Drone 2.0 [17], (b)Bebop Drone [18], (c) Phantom 2 Vision [19], and (d) 3D Robotics Solo [20].

D. 3D Robotics Solo Drone

Solo Drone is manufactured by 3D Robotics and is considered as the world's first smart drone with dual 1 GHz Linux computers: one on the drone and the other on the controller along with a GoPro camera attached to the drone. The HD video is obtained straight from the GoPro to 3DR solo application in an Android or an iOS phone. It uses a Pixhawk 2 autopilot with a flight time of approximately 20 minutes[15]. This drone is considered to be more secure than the drones discussed in earlier sections, because of its secured password protection. Initially, when we try to access the drone we connect to the network beginning with SoloLink with an initial password *sololink*, which can be changed later. However, since we have to keep the network name as `SoloLink_` followed by alphanumeric characters, it makes it easy to understand that its the Solo drone's network. Therefore, while cyber hacking into the drone might be difficult, a de-authentication attack can be performed to disconnect the communication link between drone and the controller.

IV. Cyber Attacks on Drones

Drones controlled by WiFi use IEEE 802.11 standards. All the communication between the drone and ground station controller typically use the WiFi network, which is vulnerable to security breaches. An IBM researcher[16] said that professional drones can be hijacked because of no encryption on their on-board chips and also can perform man-in-middle attacks with up to two kilometers away. In particular, an unencrypted Wi-Fi used with a drone allows any individual to connect and hack the drone. For example, software such

[8]https://busybox.net/about.html.
[9]https://ardronelabviewtoolkit.wordpress.com/.
[10]https://github.com/felixge/node-ar-drone/.
[11]http://www.nodecopter.com/.
[12]https://github.com/cucx/bebop.
[13]https://openwrt.org/.
[14]https://github.com/noahwilliamsson/dji-phantom-vision.
[15]https://3dr.com/solo-drone/.
[16]http://www.theregister.co.uk/2016/04/01/hacker_reveals_40_attack_to_steal_28000_drones_from_2km_away.

Fig. 2: De-authentication attack on a drone.

as Skyjack[17] can be used to seek out and wirelessly control other drones within the range, and create an army of drones. In particular, SkyJack can detect all wireless networks and can deactivate clients connected to a drone, and then use *node.js* with *node-ar-drone* to control the drone. This drawback can be solved by using Wi-Fi protected access[18], which provides password authentication to the drone and will not be easy for a hacker to gain access to the drone.

We have performed drone hijacking experiments with the help of a WiFi Pineapple[19], AR Drone, Bebop and Phantom 2 Drone. Since these drones have WiFi, they create a wireless network which allows users to connect to them. These access point (AP) names are basically the drone name followed by the last two octets of the MAC address which makes it easy to find them; otherwise, they can be found by scanning, using the Organizational Unique Identifiers (OUI) which remains the same for all the drones from a given manufacturing company. Later, we try to connect to their network using the Linux command `iwconfig` and we can check our connection using `ping` command to their IP addresses. If we receive back an IP message we can confirm that our connection is successful and we have complete control over the drone. We perform these tasks using the WiFi Pineapple device which comes with boot switches, and can run the program as soon as the device is turned on. This helps in performing automated tasks, e.g., every time a drone is found, commands will be executed automatically.

A. De-authentication Attack

As shown in Fig. 2, we can perform a de-authentication attack on drones by using *aircrack-ng*[20]. Initially, a passive scan is made to search for the wireless network. After a network is found, using *airodump-ng* (from *aircrack-ng*), packets from only that particular wireless network can be filtered and stored. Then the list of clients associated with network is available and de-authentication attack can be performed. The clients are de-authenticated using *aireplay-ng* (again within *aircrack-ng*), which sends disassociate packets to connected clients, for disconnecting them from the AP.

In Fig. 3, a screen shot of the sent de-authentication packets are shown, where `90:03:B7:70:8B:E2` is the BSSID of the drone. In this experiment, aireplay-ng software is waiting to receive a beacon frame from the Parrot AR Drone which creates an AP for the clients to connect. After a beacon frame is received it starts sending disassociate packets to its connected clients. This results in the connection between the client (in this case `BC:F5:AC:F6:C7:57`) and the drone being lost. In this case, the disassociate packets are only sent to one particular client. Even if we try to make the drone

[17]http://samy.pl/skyjack/.
[18]https://github.com/daraosn/ardrone-wpa2/.
[19]http://hakshop.myshopify.com/products/wifi-pineapple.
[20]http://www.aircrack-ng.org/.

```
root@Pineapple:~#  aireplay-ng -0 0 -a 90:03:B7:70:8B:E2 -c BC:F5:AC:F6:C7:57 wlan1mon
19:11:11  Waiting for beacon frame (BSSID: 90:03:B7:70:8B:E2) on channel 6
19:11:12  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [78|62 ACKs]
19:11:12  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [53|63 ACKs]
19:11:13  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|63 ACKs]
19:11:13  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|61 ACKs]
19:11:14  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|65 ACKs]
19:11:15  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|60 ACKs]
19:11:15  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|56 ACKs]
19:11:16  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|60 ACKs]
19:11:16  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|75 ACKs]
19:11:17  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|65 ACKs]
19:11:18  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 1|62 ACKs]
19:11:18  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 1|66 ACKs]
19:11:19  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|62 ACKs]
19:11:19  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|64 ACKs]
19:11:20  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|61 ACKs]
19:11:20  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|65 ACKs]
19:11:21  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|64 ACKs]
19:11:22  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|62 ACKs]
19:11:22  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|63 ACKs]
19:11:23  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|64 ACKs]
19:11:23  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|63 ACKs]
19:11:24  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|49 ACKs]
19:11:24  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|80 ACKs]
19:11:25  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|61 ACKs]
19:11:26  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [12|55 ACKs]
19:11:26  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 0|70 ACKs]
19:11:27  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [65|68 ACKs]
19:11:27  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [61|63 ACKs]
19:11:28  Sending 64 directed DeAuth. STMAC: [BC:F5:AC:F6:C7:57] [ 1|46 ACKs]
```

Fig. 3: De-authentication packets have been set from an attacker to a Parrot AR Drone 2.0. The MAC address of the drone is `90:03:B7:70:8B:E2`, while the MAC address of the smartphone is `BC:F5:AC:F6:C7:57`.

secure by using a WPA 2 authentication [21], it is possible to disassociate them. We can also jam the complete AP network by continuously sending disassociation packets, disallowing anyone to connect to the network. Connection is regained later once the de-authentication packets are stopped being transmitted and when the client sends an association packet to the AP. Once the client gets disconnected from the drone due to the de-authentication attack, a link lost message is displayed.

The *aireplay-ng* command[22] for the de-authentication attack firsts waits to receive beacon from the BSSID and then sends directed de-authentications as shown in Fig. 3. In particular, the command sends 128 deauth packets, out of which 64 packets are sent to the BSSID and 64 packets are sent to the selected client. In the last column of Fig. 3, first number represents the number of ACKs received from the client, while the second number represents the number of ACKs received from the UAV. The ACKs for the client can go above 64 packets when the client is actively participating with the BSSID or when ACKs from the previous packets is received. A number very smaller than 64 indicates the client is far away with weak signal strength, and zero value indicates that packets have not reached to the client.

B. GPS Spoofing Attack

GPS spoofing attack is another type of cyber attack commonly performed on drones. The communication links in drones include incoming signals from GPS satellites, signals notifying the drone's presence, and a two-way link between the ground station and the drone. GPS enables a drone's navigation, and due to no encryption of the signals they can be easily spoofed. In December 2011, Iranian forces claimed to have captured a Lockheed Martin RQ-170 Sentinel drone, operated by United States Air Force (USAF), and President Barack Obama asked for the return of the drone which was initially rejected by Iranian officials [21]. A major possibility that may have caused the loss of the drone is a cyber attack on the GPS system, which could be a GPS-spoofing attack.

The basic idea in GPS spoofing is transmitting fake GPS coordinates to the control system of the drone. This will hijack

[21]https://github.com/daraosn/ardrone-wpa2.
[22]http://www.aircrack-ng.org/doku.php?id=deauthentication.

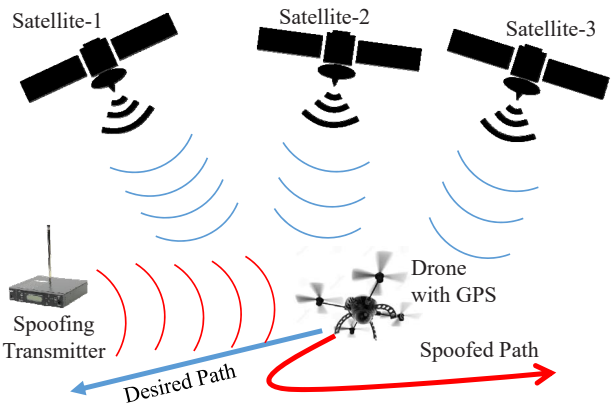


Fig. 4: GPS spoofing attack Scenario, which changes the actual path of the Drone with a spoofed trajectory.

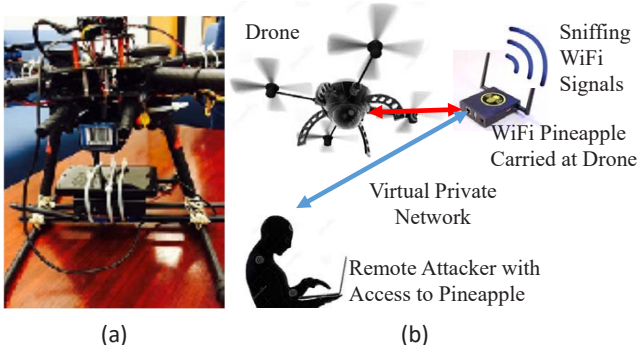


Fig. 5: (a) Experimental setup with WiFi Pineapple mounted on a drone, and (b) Attack model using a WiFi Pineapple.

the drone and subsequently it will be in complete control of the attacker. For a GPS spoofing attack, a transmitter is used to transmit false GPS signals forcing the victim to synchronize with the attacker's signals. For example, in Fig. 4, three satellites are sending true GPS signals to the drone, constantly allowing it to fly in a desired path. An attacker can use a transmitter to send false GPS signals, which deters its path and sends the drone in a direction specified by the attacker. A successful attack is conducted when attacker is very close to the drone, or by using a directional antenna with narrow beamwidth aiming the drone. Due to no authentication mechanism, civilian drones can be attacked easily by delaying signals, while attacks on military drones are complicated due to use of authentication mechanisms [22].

Researchers from UT-Austin were successfully able to demonstrate GPS spoofing attack, which can force a UAV to follow a trajectory set by the spoofer, proving that such an attack was technically and operationally feasible. For demonstration, initially the drone was made to hover in a particular location with the help of authentic signals. Later, spoofed signals were transmitted and they were aligned within the legitimate GPS signals received by the UAV. After overpowering the authentic GPS signals, spoofer changed the velocity and position of the UAV and another safety pilot was used to control it from drifting away [23], [24]. Recently in DEFCON 23, 2013, a security researcher explained how to carry out GPS spoofing attacks [25] on cars and UAVs. Initially, GPS information is captured using USRP B210 software defined radio (SDR), and it is replayed back using a bladeRF SDR. Using these devices it is also possible to change the time and date of the GPS signal.

V. Drones as Cyber Attack Tools

Drones are vulnerable to many of the attacks but can also be used in malicious and harmful ways. As discussed in[23], a young teenager was charged to modify a drone to make it a fire handgun. In DEFCON 21[24], a security researcher used a DJI Phantom mounted with a WiFi Pineapple to sniff wireless signals. Built-in tools like *airdoump-ng*, *sslstrip* were used to dissect the wireless data. The basic idea was to fly the drone and land it over a building/balcony to collect data, and bring it back to the starting position. The connection with the WiFi Pineapple is maintained over a 3G connection by Reverse SSH tunnel, i.e. by creating an SSH relay server[25]. In this section, we will provide one particular example on the use of drones as cyber attack tools: sniffing signals using a virtual private network (VPN).

A. Sniffing Signals using a Virtual Private Network

In order to sniff WiFi signals, a WiFi Pineapple carried at a drone can be utilized. In our setup, we are mounting the WiFi Pineapple on the drone along with a smartphone as shown in Fig. 5(a), where the smartphone will provide Internet connection to WiFi Pineapple. There are multiple ways in which we can access the device. One of them is using an Ethernet cable connected to the device and the laptop. And another way is connecting it wirelessly by connecting to its AP within its WiFi range.

Since the device mounted on the drone will be flying at heights and distances that may be far away, it is not possible to connect using any of the above methods. Therefore, as shown in Fig. 5(b), we created a VPN between the WiFi Pineapple and our own devices, thus making it possible to access the device from anywhere by just providing Internet connection to the WiFi Pineapple. VPN is basically used for client-server applications. The question might arise about the security of these devices and what if an intruder tries to intercept the server's communication. The OpenVPN[26], which we are using to create a virtual private network, creates a symmetric key of size 2014 bits that is exchanged between the server and the client using Diffie-Hellman key exchange.

VI. Interdiction of Unauthorized Drones

UAVs can be launched in any territory for constant surveillance and monitoring, and they can also be used to perform certain types of cyber/physical attacks that may harm property and civilians. As the cost of the drones is going down, the number of hobbyists and industries using them is increasing. Thus, it gets difficult to identify unauthorized drones and bring down such drones when necessary. They can cause danger for civilian aircrafts, and there have been reports of near misses with UAVs and aircrafts, such as the near collision incidents with Boeing 737 in the British Airport[27]. It is critical that small UAVs are restricted to enter protected areas, and an unauthorized UAV that may be a potential threat should be detected, interdicted, and brought down in a safe zone. These have also been the major goal in *MITRE*

[23]http://www.smh.com.au/technology/web-culture.
[24]https://www.defcon.org/images/defcon-21/dc-21-presentations/Hill/DEFCON-21-Ricky-Hill-Phantom-Drone-Updated.pdf.
[25]https://hak5.org/episodes/hak5-1520.
[26]https://wiki.archlinux.org/index.php/OpenVPN.
[27]http://i-hls.com/2016/02/iata-chief-drones-pose-real-threat-to-civilian-aviations/.

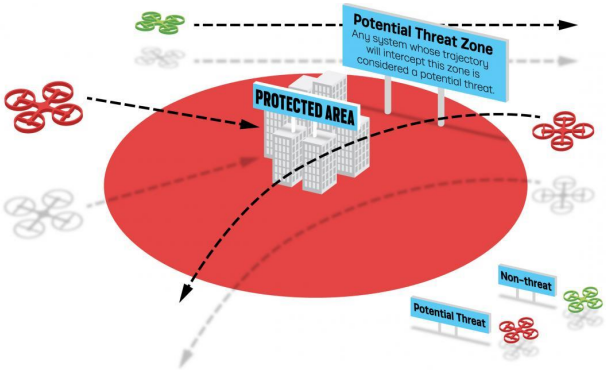
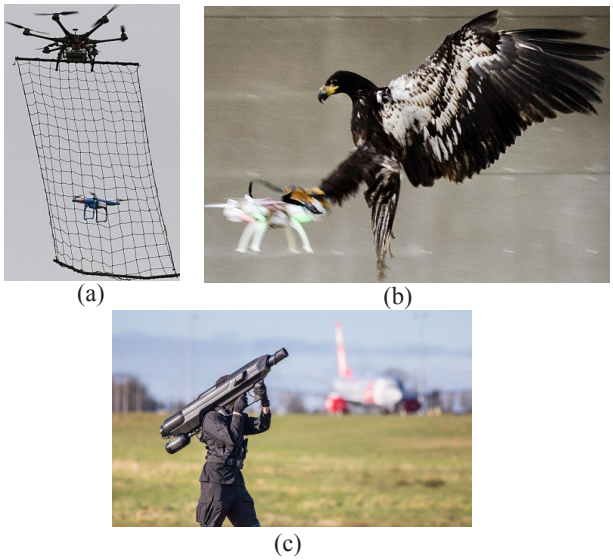


Fig. 6: Threat model for UAVs in a protected area based on *MITRE Challenge* framework [26].



(a) (b) (c)

Fig. 7: Taking down malicious drones using (a) Net traps used by other larger drones [27], (b) Eagle trained to catch a drone and place in a safe zone [28], and (c) SkyWall 100 bazooka that fires giant nets [29].

Challenge, summarized in Fig. 6 [26], where the threat model shows how the trajectory of the drone can cause a threat. If the trajectory of the UAV is outside the protected area, it is considered to be safe. If the trajectory goes within the protected area it needs to be detected and brought down outside of the protected zone.

One way in which a drone could be brought down is by using another drone. In [27], Tokyo police created a drone squad for privacy breaches. Police department were handed over net-carrying drones that will trap suspicious drones flying in the vicinity as shown in Fig. 7(a). Before any attempt to trap the drone, suspicious drone operator will be warned and if refused will be trapped and questioned further.

Cyber hacking one drone with the help of another drone is another possible alternative, because of the excess use of commercial drones using a WiFi network to control the flight. This makes them open to security vulnerabilities like de-authentication attacks or brute forcing into the drone's WiFi network. In [30], a Parrot AR Drone is interdicted using a Phantom Vision 2 equipped with a WiFi Pineapple. A shell script is used with command utility called as `empty`, which uses the concept of pseudo-terminals used on SSH sessions. Here, the Parrot drone acts as the slave and WiFi Pineapple on the Phantom drone acts as the master. Thus, as commands are entered in the master device it will be executed in the slave device, making it completely under the control of the WiFi Pineapple device.

As shown in Fig. 7(b), Scotland metropolitan police are training eagles to take down suspicious drones [28]. This idea was very much successful as it was not required to use any other devices and was very cost effective with no danger to civilians. Eagles were made to consider drones as preys so that they catch them and place them in a safe area. In [29], as shown in Fig. 7(c), operator fires a cannister with large nets and as soon as drones rotors gets tangled, a parachute brings the drone safely down to the ground.

VII. Privacy, Forensics, Search and Rescue

One of the major concerns related to the use of drones is the privacy. It is easy to mount a camera or a device to capture information, which may occasionally violate the privacy of people. To overcome such concerns, Center of Democracy and Technology (CDT) have asked FAA to issue rules on privacy and recommend using data collection statement to know whether the information collected will be retained, used or disclosed. The most suitable means to maintain privacy was considered as Privacy by Design (PbD), which helps in maintaining standards and provides remedies for security breaches. By adopting PbD principles, privacy intrusion becomes limited and privacy can be ensured at an early stage [31].

Privacy was considered a major concern when a UAV goes beyond line of sight, but non line of sight operation is also typically required for UAVs, such as for search and rescue or taking a survey of an area. In early 2012, when a person flew a UAV over a slaughter house he found a pipe going to the nearby rivers. While this was reported as a case for endangering public health, it also created complex issues since anyone can inspect such violations by overflights. Continuous use of such overflights can reveal trade secrets and if these photos go on the Internet, they can affect the businesses of companies [32].

Drones have various other applications in smart cities related to search and rescue, forensics, and public safety. During a war or in any emergency situation surveillance of a city becomes a challenging task. In such scenarios drones can be used conveniently to avoid human casualties. Most drones come with HD cameras which provide real time videos back to the ground station when they are flying. With advances in aerial technology, drones can be used in public safety communications. During natural disasters, there can be communication difficulties for public safety and in such times drones prove to be a viable solution in creating unmanned aerial base stations (UABs). Deploying drones in such scenarios can improve throughput coverage and help in saving lives [33], [34].

In [35], use of drones for spectrum monitoring and forensics have been studied. Spectrum measurements collected by drones can be compared to a database, which may help in detecting and solving the interference problems. A prototype was built in [35] using a DJI Phantom 2 to collect raw I/Q samples and obtain the spectrogram data which was used for signal identification. When the drone is launched it starts looking for interference, and when found it will try to localize the interferer. It will also change the flight plan to get next meaningful measurement point reducing flight time

Microdrones[28] can be used for surveillance, search, and rescue operations. They are easy to deploy and have been tested under various climatic conditions. They provide live camera feed in disastrous situations such as wildfire or heavy snow, and can also carry thermal image cameras to identify lost or missing people. To better the search and rescue operations with drones, in [36], algorithms have been taught to UAVs for autonomous flying through forests. The Search with Aerial RC Multirotor (SWARM)[29] team have dedicated themselves in search and rescue operations with drones. This worldwide network is spread across 33 countries with over 600 drone pilots. A related organization is UAViators[30], whose mission is "to promote the safe, coordinated and effective use of UAVs for data collection, payload delivery and communication services in a wide range of humanitarian and development settings".

VIII. Conclusion

Drones will be more pervasively used in future smart cities for communication and surveillance, and the need for security measures for drones is evident. In this paper, we provided a survey on some commonly used small UAVs, possible ways to perform cyber attacks on them, and potential interdiction mechanisms for malicious drones. We also demonstrated de-authentication attacks to drones, and VPN based sniffing using a WiFi Pineapple carried on a drone. Our future work includes testing a wide variety of other attacks on drones such as jamming and GPS spoofing.

Acknowledgement

This research was supported in part by the NSF under the grant numbers CNS-1453678 and CNS-1446570.

References

[1] M. Asadpour, B. Van den Bergh, D. Giustiniano, K. A. Hummel, S. Pollin, and B. Plattner, "Micro aerial vehicle networks: An experimental analysis of challenges and opportunities," *IEEE Commun. Mag.*, pp. 1–11, 2014.

[2] İ. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying ad-hoc networks (FANETs): a survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, 2013.

[3] J. M. Sullivan, "Revolution or evolution? The rise of the UAVs," in *Proc. Int. Symp. Technology and Society Weapons and Wires: Prevention and Safety in a Time of Fear (ISTAS)*, 2005, pp. 94–101.

[4] J. Villasenor, "Drones and the future of domestic aviation," *Proceedings of the IEEE*, vol. 102, no. 3, pp. 235–238, Mar. 2014.

[5] Z. Sun, P. Wang, M. C. Vuran, M. A. Al-Rodhaan, A. M. Al-Dhelaan, and I. F. Akyildiz, "BorderSense: Border patrol through advanced wireless sensor networks," *Ad Hoc Networks*, vol. 9, no. 3, pp. 468–477, 2011.

[6] C. Barrado, R. Messeguer, J. López, E. Pastor, E. Santamaria, and P. Royo, "Wildfire monitoring using a mixed air-ground mobile network," *IEEE Pervasive Computing*, vol. 9, no. 4, pp. 24–32, 2010.

[7] I. Maza, F. Caballero, J. Capitán, J. Martínez-de Dios, and A. Ollero, "Experimental results in multi-UAV coordination for disaster management and civil security applications," *J. Intelligent & Robotic Systems*, vol. 61, no. 1-4, pp. 563–585, 2011.

[8] E. Semsch, M. Jakob, D. Pavlicek, and M. Pechoucek, "Autonomous UAV surveillance in complex urban environments," in *IEEE Int. Conf. Web Intelligence and Intelligent Agent Technologies (WI-IAT)*, vol. 2, 2009, pp. 82–85.

[9] H. Xiang and L. Tian, "Development of a low-cost agricultural remote sensing system based on an autonomous unmanned aerial vehicle (UAV)," *Biosystems Engineering*, vol. 108, no. 2, pp. 174–190, 2011.

[10] "Amazon Prime Air." [Online]. Available: http://www.amazon.com/b?node=8037720011

[11] I. Bucaille, S. Hethuin, T. Rasheed, A. Munari, R. Hermenier, and S. Allsopp, "Rapidly deployable network for tactical applications: Aerial base station with opportunistic links for unattended and temporary events ABSOLUTE example," in *Proc. Military Commun. Conf.*, Nov. 2013, pp. 1116–1120.

[12] A. Wright, "Drones offer risks, underwriting challenges," Jan. 2015. [Online]. Available: http://www.riskandinsurance.com/drones-offer-risks-underwriting-challenges/

[13] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *Proc. IEEE Conf. Homeland Security (HST)*, 2012, pp. 585–590.

[14] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks-An approach to the risk assessment," in *Proc. IEEE Conf. Cyber Conflict (CyCon)*, 2013, pp. 1–23.

[15] S. M. Giray, "Anatomy of unmanned aerial vehicle hijacking with signal spoofing," in *Proc. IEEE Recent Advances in Space Technologies (RAST)*, 2013, pp. 795–800.

[16] M. Ma'sum, M. Arrofi, G. Jati, F. Arifin, M. Kurniawan, P. Mursanto, and W. Jatmiko, "Simulation of intelligent Unmanned Aerial Vehicle (UAV) for military surveillance," in *Proc. Int. Conf. Advanced Computer Science and Information Syst. (ICACSIS)*, Sep. 2013, pp. 161–166.

[17] Parrot AR Drone 2.0. [Online]. Available: http://ardrone2.parrot.com/

[18] Bebop Drone. [Online]. Available: http://store.parrot.com/uk/accueil/336-bebop-drone.html

[19] Phantom 2 vision. [Online]. Available: https://www.dji.com/product/phantom-2-vision

[20] 3D robotics solo. [Online]. Available: https://3dr.com/solo-drone/

[21] CNN Wire Staff, "Obama says U.S. has asked Iran to return drone aircaft," Dec. 2011. [Online]. Available: http://www.cnn.com/2011/12/12/world/meast/iran-us-drone/

[22] "Hacking drones: Overview of the main threats," Jun. 2013. [Online]. Available: http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/

[23] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[24] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," in *Proceedings of the ION GNSS Meeting*, vol. 3, 2012.

[25] H. Lin and Y. Qing, "GPS spoofing," 2013. [Online]. Available: https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Lin-Huang-Qing-Yang-GPS-Spoofing.pdf

[26] (2016) The MITRE challenge: Countering unauthorized unmanned aircraft systems. [Online]. Available: http://www.mitre.org/research/mitre-challenge

[27] S. Liberatore, "How do you catch a drone? with an even bigger drone and a giant net," Dec. 2015. [Online]. Available: http://www.dailymail.co.uk/sciencetech/article-3356746

[28] T. Witherow, "Police set to use eagles to foil terrorist drone attacks," Feb. 2016. [Online]. Available: http://www.dailymail.co.uk/news/article-3436572

[29] M. Burns. (2016, March) The skywall 100 bazooka captures drones with a giant net. [Online]. Available: http://techcrunch.com/2016/03/04/the-skywall-100-bazooka-captures-drones-with-a-giant-net/

[30] D. Kitchen, "Drones hacking drones," HAK5, Dec. 2013. [Online]. Available: https://hak5.org/episodes/hak5-1518

[31] A. Cavoukian, "Privacy and drones: Unmanned aerial vehicles," Technical Report, Ontario, Canada, Aug. 2012.

[32] J. Villasenor, "Observations from above: unmanned aircraft systems and privacy," *Harv. JL & Pub. Pol'y*, vol. 36, p. 457, 2013.

[33] A. Merwaday and I. Guvenc, "UAV assisted heterogeneous networks for public safety communications," in *Proc. IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2015, pp. 329–334.

[34] K. Guevara, M. Rodriguez, N. Gallo, G. Velasco, K. Vasudeva, and I. Guvenc, "UAV-based GSM network for public safety communications," in *Proc. IEEE Conf. Southeast*, 2015, pp. 1–2.

[35] A. Anderson, X. Wang, K. R. Baker, and D. Grunwald, "Systems for spectrum forensics," in *Proceedings of the 2nd International Workshop on Hot Topics in Wireless*. ACM, 2015, pp. 26–30.

[36] A. Brokaw, "Autonomous search-and rescue drones outperform humans at navigating forest trails," Feb 2016. [Online]. Available: http://www.theverge.com/2016/2/11/10965414/autonomous-drones-deep-learning-navigation-mapping

[28] https://www.microdrones.com/en/home/.

[29] http://sardrones.org/.

[30] http://uaviators.org/.