DroneJack: Kiss your drones goodbye!

Guillaume Fournier, Paul Audren de Kerdrel, Pascal Cotret, Valérie Viet Triem Tong

DroneJack: Kiss your drones goodbye!

Guillaume Fournier[1], Paul Audren de Kerdrel[1], Pascal Cotret[2], and Valérie Viet Triem Tong[3]
guillaume.fournier@supelec.fr
paul.audrendekerdrel@supelec.fr
pascal.cotret@centralesupelec.fr
valerie.viettriemtong@centralesupelec.fr

[1] CENTRALESUPELEC, Rennes, France
[2] SCEE CENTRALESUPELEC/IETR/CNRS, Rennes, France
[3] EPC CIDRE CENTRALESUPELEC/INRIA/CNRS/University of Rennes 1

Abstract. The commercial drone market has significantly taken off for a few years. In 2016, sales of drones used for commercial and enterprise purposes was worth 3.4 billion dollars [3]. This fast-growing field raises many questions regarding security since damages caused by such drones could be disastrous. Knowing that in some cases, transmission range is so wide (7 kilometers for a DJI Phantom 4 Pro) and that some drones can lift off more than 30 kg worth of equipment, we cannot deny that there will be (and already are) unexpected and unwanted uses of such a technology. In this article, we introduce DroneJack, an automatic anti-drone solution that can protect an area from being flown over. Using DroneJack, you can conduct a predefined defense over foreign drones as shutting them down, pilot them instead of the true user, direct them towards some GPS coordinates. You can also exploit data owned by the drone to recover photos, videos or flight logs. Even better, you can configure your own attacks on foreign drones and deploy them on DroneJack. Let's play!

1 Introduction

Unmanned aerial vehicles (UAV) were originally made for the military market for training, reconnaissance missions or bomb transports. Nowadays, drones are mainly used by civilians for aerial pictures, wildlife discovering, hunting, search and rescue missions.

Drone manufacturers, such as Parrot or DJI, are in a constant competition resulting in incredible toys able to fly several kilometers away from their base station; however, security is not often taken into account: for instance, between October 2014 and February 2015, 17 nuclear plants have been flown over in France [6]. Another example is the famous drone that crashed on the White House lawn in June 2015 [8]. Fortunately, those

stories had harmless endings. But we claim that under precise circumstances as the defense of sensitive areas we need practical solutions to take control of foreign drones. We present here DroneJack as an off-the-shelf anti-drone solution for protecting a given area. DroneJack automatically detects and takes the control of multiple foreign drones relying on WiFi communications that cut across a given area. We particularly focus on Parrot AR Drone and Bebop, widely spread commercial drones.

Section 2 presents some existing anti-drone solutions. Main lines of DroneJack are detailed in Section 3. Finally, Section 4 explains how DroneJack can be used to control captured drones.

2 Existing anti-drone solutions

Being able to stop a drone flying over a given area has become a security and a privacy question whose importance has grown for the last few years. As stated before, we particularly focus here on commercial drones that can be bought by anyone. These devices are equipped with specific autonomous features such as altitude stabilization, take-off and landing, automatically landing upon loss of control signal, Return-to-home, Follow-me, GPS navigation, orbit around an object. These devices can also obey to remote orders to accomplish various tasks such as mapping, surveillance, search or tracking operations. In this context, there are two main ways to prevent drone from flying over a given area. First, we can try to physically capture the drone: for instance, the Dutch National Police Force has trained eagles to help take out illegal drones [9]. We can also use a bigger drone equipped with a huge net meant for capturing and disabling smaller drones [7].

The second approach consists in taking control of the device without physical interactions. This approach exploits the fact that the mode of communication between the drone and its master is wireless. The main goal of existing tools of this second approach is to disrupt the communication between the drone and its master intentionally by causing interferences or collisions at the receiver side.

Drones communicate with their operators at common frequency bands (2.4 GHz in Europe[4]). DroneWatch [4] is a full anti-drone solution. This project can detect, track and identify many types of civilian drones. It uses optical and radio frequency based technologies in order to provide an accurate position of a malicious drone. Unfortunately, it appears

[4] If you are familiar with frequencies, you may already know that 2.4 GHz is the frequency used by the WiFi protocol, this will be important in the following

that the only countermeasure implemented is a jammer. In other words, DroneWatch is an accurate drone detector but does not provide any real world solution once the drone has sneaked into a restricted area. DroneDefender is another solution that works by directing radio energy at the drone, disrupting the remote control link between the drone and the operator [2].

This approach seems to have been chosen by Airbus Defence and Space [1]. However, it presents several problems. First, it requires a defender agent and a clear line-of-sight to be effective. Therefore, drones detection is performed with naked eyes. It can only deal with one drone at a time: the defender must wait until the targeted drone has landed before taking care of another one. Such rifles can only land a drone or return it back to its owner, the defender cannot control it as he wants.

Drones commonly communicate with their operators thanks to wireless connection. SkyJack [5] exploits this feature to remotely take the control of foreign drones. More precisely, SkyJack is a kind of guardian drone that flies over a monitored area and seeks the wireless signal of any other drone in this area. Once detected, SkyJack disconnects the wireless connection of the true owner and authenticates himself with the target drone. SkyJack can thus feed commands to the captured drone. SkyJack is available on Github at `https://github.com/samyk/skyjack`, it is a Perl application that uses `aircrack-ng` (`https://www.aircrack-ng.org/`) which is a complete suite of tools to assess WiFi network security.

From our point of view, SkyJack is an appealing approach allowing to take the control of foreign drones without leaving home. Unfortunately, and as far as we know, this solution lacks essential features to be considered as a real anti-drone system, the defender does not have any control over the drone once it has been compromised. The only thing SkyJack can do is trigger a hard-coded animation of the drone after which the control is lost. Moreover, the real owner can reconnect to his drone a few seconds after the beginning of SkyJack attack. It means, for instance, that he can trigger a *Return home* order immediately after regaining control, this way, the SkyJack attack would become useless.

3 DroneJack

This work presents DroneJack a complete anti-drone solution dedicated to the prevention of unwanted drones flight over. DroneJack allows to detect, track, take over and control drones using WiFi communications. It implements deauthentication attacks to disconnect true users of multiple

drones and prevents their reconnection. DroneJack is developped from scratch and become an off-the-shelf component with a web interface that permits a defender to cope with multiple drones. DroneJack implements various features as tracking the drone flight on a map, taking over the video stream produced by the drone, ordering the target drone to *go-home*, to *kill himself* or to go to specific GPS coordinates. Moreover, the number of attacks is not limited: the defender can install new features since DroneJack website accepts uploads of new attacks and installs them on all connected DroneJack instances.

DroneJack is a mobile protection system composed of a collection of Raspberry Pi 3 (DroneJack Probes) that have to be placed on the area to defend and a web server responsible of these Raspberry management. DroneJack is not limited by the number of DroneJack Probes, allowing it to cover an area as large as needed. Moreover, using the website interface, the operator does not have to be on site to manage threats. Figure 1 gives an overview of the global architecture of DroneJack.

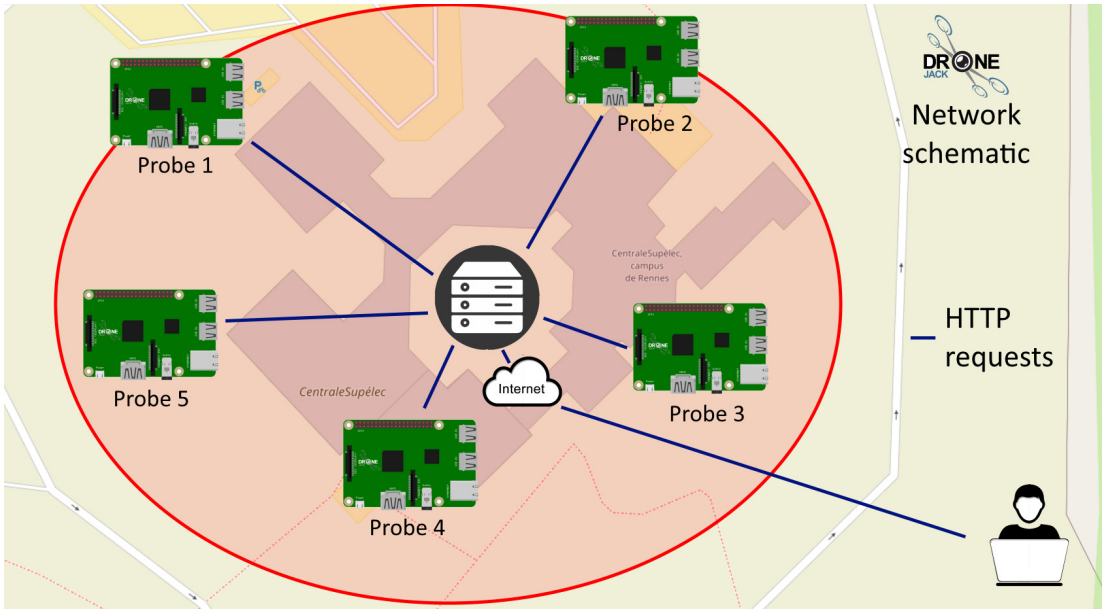

Fig. 1. DroneJack architecture

DroneJack distinguishes 3 main phases in a successful attack on a drone: Detection/ Takeover / Attack performed on the drone. This section describes how the first two phases work and how they are synchronized in order to have a continuous drone scanner.

Phase 1.1: Detection The first step in WiFi based drone detection, is to know what to look for. In this study, we aim at discovering WiFi access points coming from drones. For that purpose, DroneJack relies (as SkyJack) on `airodump-ng` a complete suite of tools to assess WiFi network security. DroneJack monitors WiFi communication continuously and our WiFi scanner produces every 5 seconds a list of the surrounding access points. Detecting a drone in this list is as simple as checking if one MAC address is owned by a drone Company. Fortunately, owned MAC addresses are public and can be found online. For instance, according to the IEEE Standards Association Registration Authority, Parrot owns five MAC address ranges. Once a drone has been detected, a semaphore releases phase 2. As it can be seen in the following sub-sections, phase 2 handles those drones sequentially. However, if a drone is being monitored (phase 3) and another one is found, then the second one is put in a waiting state: the owner is disconnected and the drone hovers until the first drone has been handled.

Phase 1.2: Drone tracking Another interesting feature of phase 1 is a drone tracking system. Knowing a drone is trespassing is one thing, but being able to track it in real time is undeniably better.

Using the RSSI *(Received Strength Signal Indicator)* of the beacons sent by the drone, each DroneJack node computes the distance to the detected drone. Then, the DroneJack web interface centralizes all the data and triangulates the drone position (provided that the GPS coordinates of DroneJack nodes are known). Depending on how many DroneJack nodes detected the drone, the web interface draws a circle, which radius is the distance in meter to the drone, or the accurate position of the drone (Figure 2). Once again, DroneJack uses a new thread to track each newly detected drone.

Phase 2: Takeover Once a drone has been detected, phase 2 is launched. This phase has 2 steps:

1. First, DroneJack uses desauthentication packets to disconnect the owner from the drone. Those packets are sent continuously until the end of phase 3 using `aireplay-ng`. After this step, almost every commercial drones hover in the sky waiting for their owner to reconnect.
2. Then, DroneJack connects to the detected drone and releases phase 3. DroneJack can only connect to unsecured networks, but this concerns a lot of drone models: Parrot AR Drones and Bebop for instance. In case the access point is secured with WPA, then DroneJack stops after the first step.

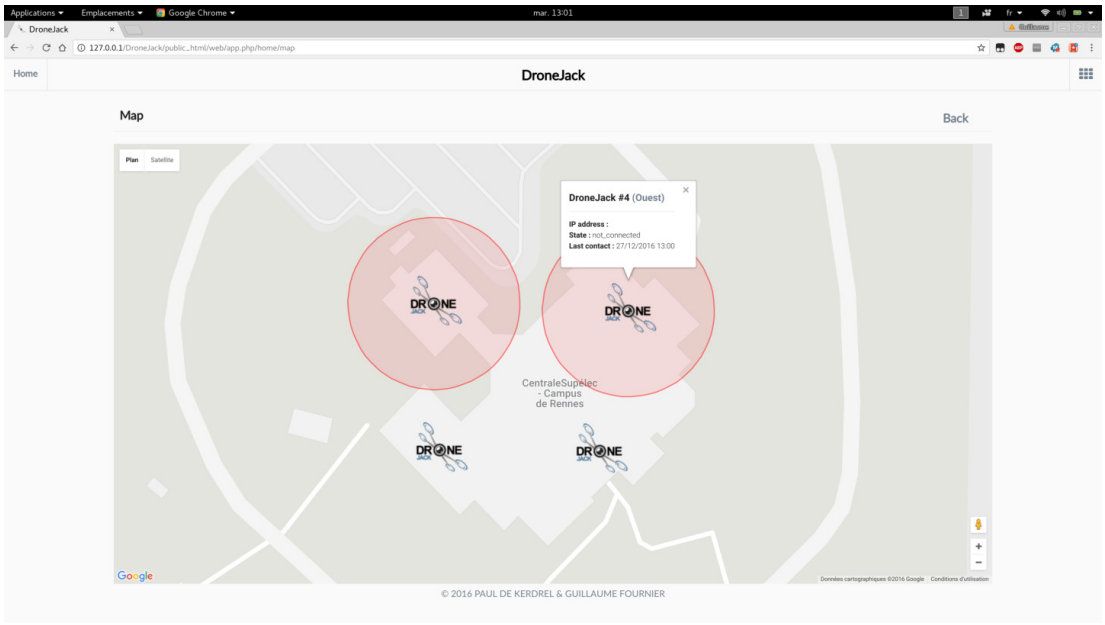

Fig. 2. DroneJack website - map

This work is a continuous protection system, which means that taking over a drone does not stop phase 1. Therefore, new drones can be detected while others are already being handled. Here is how DroneJack takes care of this situation: the first detected drone is the first one to go through phase 2 and 3, but as long as phase 3 is not completed on this drone, the other detected drones go only through the first step of phase 2. In other words, it means that each detected drone is disconnected from its owner and therefore hovers peacefully until DroneJack is done with the previous ones.

4 Turning Drones into Zombies

Once DroneJack has taken over a targeted drone, it gives the ability to the defender to pilot the captured drone. A complete web interface has been developed allowing the defender, wherever he might be, to control the drone with a video stream.

Beyond that, the defender may have to cope with an attack of multiple drones at the same time. For that purpose, DroneJack phase 3 can be set to many other automated attacks. The three main behaviors already added are the following:

1. The kill switch: Parrot Drones have an *emergency* button that immediately stops the rotors. With this attack set, DroneJack will simply

trigger this emergency procedure and all detected drones will fall like stones from the sky.
2. Go Home: this attack simply sends the drone back to its home GPS coordinates. This is the least offensive defense of DroneJack.
3. Go to GPS coordinates: this attack sends the drone to a set of GPS coordinates you previously set in each DroneJack configuration.

Moreover, DroneJack offers the possibility to any developer to upload home-made attacks through the website. Versions and configuration settings are automatically synchronized if DroneJack Probes are used in a network configuration. Following the requirements of DroneJack software, an operator can upload software coded with any programming language executable by Kali Linux. As soon as the attack finishes, the output will be uploaded to the website.

We presented two custom attacks as an example of what can be done with this feature:

1. `nmap` scan: when this attack is triggered, DroneJack will perform a full `nmap` scan of the drone. Using this scan the operator can learn more about the operating system of the drone as well as the services running, the open ports...
2. Delete all recordings: when possible, this attack will delete all video recordings on the drone. On Parrot drones for instance, this attack is quite simple as both AR Drones and Bebop drones run an open FTP server from which you can delete any file you want.

5 Conclusion

Drone protection systems are bound to be a fast-growing field in the next few years. With always more powerful performances, drones are becoming a real security threat. Knowing that drone manufacturers are probably going to step up the security of their drones, there will be a real need to defend critical sites, such as nuclear plants or other hazardous industrial sites. In this article, we have proposed DroneJack a complete anti-drone solution allowing a defender to prevent overflight of a specific zone. DroneJack relies on its DroneJack Probes which monitor the wireless communications and can track, takeover and control multiple foreign drones. DroneJack exploits as most as possible vulnerabilities of current commercial drones. It prove by example that widespread commercial UAV can escape to their legitimate user. In this context, it permits to protect a sensitive area but, in another context, it may appear as a serious security flaw.

References

1. Kelsey Atherton. Airbus introduces a system to jam drones out of the sky. http://www.popsci.com/airbus-wants-to-jam-drones-out-sky, January 2016.
2. Kelsey Atherton. This device turns any gun into an anti-drone ray. http://www.popsci.com/dronedefender-is-an-anti-drone-rifle-attachment, February 2016.
3. Valour Consultancy. The future of commercial and industrial uavs. http://www.valourconsultancy.com/wp-content/uploads/2015/12/The-Future-of-Commercial-and-Industrial-UAVs-2016-Information-Brochure.pdf, August 2016.
4. DroneWatch. Dronewatch. https://www.droneshield.com/dronegun, January 2015.
5. Samy Kamkar. Skyjack. http://samy.pl/skyjack/, December 2013.
6. LeMonde. Au total, 17 sites nucléaires ont été survolés par des drones depuis octobre. http://www.lemonde.fr/planete/article/2015/01/29/dix-sept-sites-nucleaires-ont-ete-survoles-par-des-drones-depuis-octobre_4565967_3244.html, January 2015.
7. Bryan Lufkin. The anti-drone drone - a bigger, badder flying copter debuts to catch trespassers. https://www.scientificamerican.com/article/the-anti-drone-drone/, February 2016.
8. Zeke Miller. Drone that crashed at white house was quadcopter. http://time.com/3682307/white-house-drone-crash/, January 2015.
9. James Vincent. Dutch police are training eagles to take out drones. http://www.theverge.com/2016/2/1/10884586/drone-vs-eagle-dutch-police, February 2016.