IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

SPECIAL SECTION ON HEALTHCARE INFORMATION TECHNOLOGY FOR THE EXTREME AND REMOTE ENVIRONMENTS

Received March 23, 2019, accepted April 12, 2019, date of publication April 15, 2019, date of current version April 29, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2911526*

# Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo

**SANDRA PÉREZ ARTEAGA[1], LUIS ALBERTO MARTÍNEZ HERNÁNDEZ[1], GABRIEL SÁNCHEZ PÉREZ[1], ANA LUCILA SANDOVAL OROZCO[2], AND LUIS JAVIER GARCÍA VILLALBA[2], (Member, IEEE)**

[1]Instituto Politécnico Nacional, Sección de Estudios de Posgrado e Investigación, Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán, Ciudad de México 04260, México

[2]Group of Analysis, Security and Systems (GASS), Department of Software Engineering and Artificial Intelligence (DISIA), Faculty of Computer Science and Engineering, Office 431, Universidad Complutense de Madrid (UCM), 28040 Madrid, Spain

Corresponding author: Luis Javier García Villalba (javiergv@fdi.ucm.es)

This work was supported in part by the European Union's Horizon 2020 Research and Innovation Programme under Grant 700326, in part by the National Science and Technology Council of Mexico (CONACyT), and in part by the Instituto Politécnico Nacional.

**ABSTRACT** At present, the boom in unmanned aerial vehicles (UAV) has been increasing in recent years, placing them in an important way in the commercial market. The use of UAV in the daily tasks of industry, commerce or as entertainment for children and adults becomes more recurrent. Each of the UAVs has a specific task, depending on the technologies that are provided, in addition to their basic functions with which they were manufactured. However, in most cases the security of these UAVs is not usually taken into account since some of them are inexpensive and do not have a robust security system that protects the data they send or receive for their operation, that can cause its communication system or the operating system that controls its basic functions of flight, landing, among others, to be compromised. These computer attacks could cause physical or moral harm to people around the same operator of the UAV because they could steal information related to the locations they have visited, or intercept images or videos taken by the UAV. This paper shows the exploitation of GPS vulnerability in the commercial drone of the company 3D Robotics, this vulnerability can cause a malicious user to have control of their autonomy, and carry out illicit activities, such as overflying in spaces not allowed as an airport and private areas. The exploitation of this vulnerability is important to make known that the UAVs should have a more robust security system and also give importance to the security of GPS since the only one that has security is the military GPS.

**INDEX TERMS** UAV, GPS, GPS spoofing, hijack, Maldrone, vulnerabilities.

## I. INTRODUCTION

The uses to which it can be attributed to unmanned aerial vehicles (UAV) are very diverse in different areas of research, such as military use, civil protection, border surveillance, traffic control, meteorology, control of fires, in agriculture to spread pesticides in crops, locating people among others. However, there are ill-intentioned people who use UAVs to misuse them in violation of the law or the privacy of people. The demand for UAV has been growing since some of them are low cost and accessible to users. This growing popularity is due to the fact that they use common technologies such as WiFi for their communication, GPS for positioning and navigation, putting aside costly technologies, and with this, reducing production costs, as well as the different sizes or shapes making them easier. to transport them. However, when using more common technologies, the risks of vulnerabilities are raised, since there are numerous attacks that affect these technologies such as signal blocking attacks, signal spoofing, etc.

Due to the great variety of uses that can be attributed to the UAVs, it has been tried to violate the security of these, causing vulnerabilities that allow the attackers to manipulate them remotely to give them different uses ranging from espionage (taking photographs or video of a person) until they are used in a kamikaze manner (a word used to refer to all kinds of suicide or terrorist attacks), causing physical and/or moral damage to the people who are involved. Some of the companies dedicated to the production of UAV recommend that the default password of the WiFi network be changed to

The associate editor coordinating the review of this manuscript and approving it for publication was Sabah Mohammed.

prevent access to its communication network, but users ignore this, causing security breach. of these. On the other hand, this can be exploited for the exploitation of vulnerabilities, since, if in any case the users do not change the password by default or it is changed by a common word, known attacks towards WiFi technology can be used to try to guess the password such as brute force attacks and access to the network, this is due to the fact that an additional protection mechanism is not added to stop this type of attacks. There are also users who carry out illicit activities such as flying over an unauthorized area or flying over the UAV over too many people without knowing it, since they do not know that there are laws and rules to use a UAV. Some laws vary depending on the type of aircraft used, regardless of the common flight rules.

This work shows the exploration of a GPS (GPS Spoofing) vulnerability in the ''Solo'' UAV of the company 3D Robotics since it is one of the three main UAVs used by users in the market. The exploration of this vulnerability consists of impersonating the original GPS signal by a false one, created with the help of a low-cost USB Software Defined Radio (SDR). The signal emitted by the SDR contains among its frames coordinates of a different place than the one in which the UAN is actually located. Once the coordinates are recognized by the GPS of the UAV, you can take these coordinates as true because it does not have another location system that performs a check of these coordinates which can cause it to fly over an unauthorized area believing that It is in an authorized place. Based on this you can hijack the UAV or have your autonomy. This document also mentions the three most popular UAVs among users, as well as mentioning some of the vulnerabilities that can be exploited in commercial UAVs, such as those attributed to the Parrot UAV. With which it can be demonstrated that these devices are vulnerable and that malicious people can have access to them and alter their functioning.

This document is organized as follows: Section II presents the classification of drones, as well as the most popular commercial drones in the market. Section III lists the vulnerabilities that have been exploited in drones. Section IV and V present the attack on the Global Positioning System (GPS) with satisfactory results in the 3D robot Robotics Solo, and Section VI shows the conclusions of this work.

## II. DRONES

The Real Academy of the Spanish Language defines the word drone to an ''unmanned aircraft''. ''Unmanned'' clearly refers to the remote management of the same or remotely (remote control). A drone is any aerial vehicle operated remotely. However, the aviation security agencies and official organisms, in the generality of the word drone, prefer to use terms such as Remote Piloted Airplane System (RASP), or Unmanned Aerial Vehicle (UAV) [1]. Based on the above, it can be defined that drones or unmanned aircraft are small flying devices that can be controlled remotely.

In 2011, the International Civil Aviation Organization (ICAO) published circular 328 entitled Unmanned Aircraft Systems (UAS) in which it recognizes unmanned aircraft as aircraft [2].

Drones can have more than two hundred applications in the future according to their types. For example, these unmanned aircraft can be used for search and rescue missions, environmental protection, mail and delivery, missions in oceans and other diverse applications. These drones can provide a quick view around the target area without any danger. Drones equipped with infrared cameras can give images in the dark [3].

### A. DRONES CLASSIFICATION

The drones are equipped with different technologies depending on the specific tasks they perform. They are usually integrated with a wide variety of cameras with suitable characteristics depending on the activity that needs to be done and with different characteristics in size, weight, design, type of motor, etc.

Depending on the size of the load up they can carry and its flight range they are classified as [4]:

- Micro and mini drones: They weigh between 100 grams and 30 kilograms and fly up to 300 meters of altitude. Known as civil drones that have no military application, with a use of filmography, cartography, play, etc.
- Tactical drones: They weigh between 150 and 1,500 Kg, they can fly at an altitude between 3000 and 8000 meters, they are known as Long Resistance Altitude or Medium Altitude Long Endurance (MALE). They are used mainly in military operations, known as combat drones.
- Strategic Drones: These are large and heavy devices that can reach up to twelve tons, can fly at a maximum altitude of 20,000 meters, they are known as a High Altitude of Long Resistance or High Altitude Long Endurance (HALE). They are used in military operations.

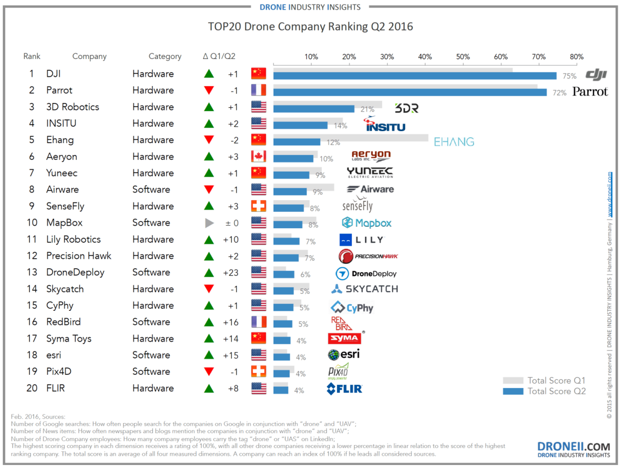
According to their wing system, they are classified as:

- Drones with multirotor system: They have several wings in different angles that rotate 360 degrees. They can have a vertical takeoff and landing so it requires less space and the possibility of flying at very low speed. At the same time they are classified depending on their number of propellers in: Trichoptera, Quadcopters, Hexacopters and Octocopters. They are the most popular in the civil and sports field.
- Drones with fixed wing system: These are systems like traditional airplanes, with wings in the shape of a cross. Being very efficient drones, they have greater autonomy, greater speed, lower sonic footprint and better tolerance to climatic changes. These drones have been used mostly in military life.

Finally, according to the means of civil operation they are classified in [5]:

- Manual mode: A radio-control station handles the aircraft during the entire flight.
- Assisted mode: Similar to the manual, but the pilot defines flight intentions in his radio-control position and a self-pilot transforms those actions into the aircraft.

- Automatic mode: The pilot establishes a “ flight plan ” and the ship flies with a self-pilot. The pilot maintains control at all times. Except in case of emergency due to loss of communication control between the ship and the pilot.
- Strict autonomous mode: Similar to the automatic where a flight plan is established, but once started, the pilot cannot intervene in the control.



DRONE INDUSTRY INSIGHTS

TOP20 Drone Company Ranking Q2 2016

| Rank | Company | Category | Δ Q1/Q2 | Total Score Q2 |
|---|---|---|---|---|
| 1 | DJI | Hardware | ▲ +1 | 75% |
| 2 | Parrot | Hardware | ▼ -1 | 72% |
| 3 | 3D Robotics | Hardware | ▲ +1 | 21% |
| 4 | INSITU | Hardware | ▲ +2 | 14% |
| 5 | Ehang | Hardware | ▼ -2 | 12% |
| 6 | Aeryon | Hardware | ▲ +3 | 10% |
| 7 | Yuneec | Hardware | ▲ +1 | 9% |
| 8 | Airware | Software | ▼ -1 | 9% |
| 9 | SenseFly | Hardware | ▲ +3 | 8% |
| 10 | MapBox | Software | ▶ ± 0 | 8% |
| 11 | Lily Robotics | Hardware | ▲ +10 | 7% |
| 12 | Precision Hawk | Hardware | ▲ +2 | 7% |
| 13 | DroneDeploy | Software | ▲ +23 | 6% |
| 14 | Skycatch | Hardware | ▼ -1 | 5% |
| 15 | CyPhy | Hardware | ▲ +1 | 5% |
| 16 | RedBird | Software | ▲ +16 | 5% |
| 17 | Syma Toys | Hardware | ▲ +14 | 4% |
| 18 | esri | Software | ▲ +15 | 4% |
| 19 | Pix4D | Software | ▼ -1 | 4% |
| 20 | FLIR | Hardware | ▲ +8 | 4% |

10%
20%
30%
40%
50%
60%
70%
80%
Total Score Q1
Total Score Q2
© 2015 all rights reserved | DRONE INDUSTRY INSIGHTS | Hamburg, Germany | www.droneii.com
DRONEII.COM
DRONE INDUSTRY INSIGHTS

Feb. 2016, Sources:
Number of Google searches: How often people search for the companies on Google in conjunction with "drone" and "UAV";
Number of News items: How often newspapers and blogs mention the companies in conjunction with "drone" and "UAV";
Number of Drone Company employees: How many company employees carry the tag "drone" or "UAS" on LinkedIn;
The highest scoring company in each dimension receives a rating of 100%, with all other drone companies receiving a lower percentage in linear relation to the score of the highest ranking company. The total score is an average of all four measured dimensions. A company can reach an index of 100% if he leads all considered sources.

**FIGURE 1.** Drone company ranking 2016.

## B. POPULAR DRONES

The drones most used by users in 2016 are presented in Figure 1. It shows the ranking of the 20 most important manufacturers of drones and that the first 3 leaders in the market are DJI, Parrot and 3DR Robotics. The Chinese company DJI has positioned itself as the undisputed market leader acquiring a majority position in an iconic brand of cameras and photographic lenses [6].

### 1) DRONE DJI

On the DJI platforms, your flight and camera stabilization system redefines the positioning and movement of the camera. Capture high-end professional images, using complex technology in the devices and making them easy to use and the products combine advanced technology with dynamic designs. There are different types of DJI drones that are used in different tasks, each one has different characteristics, such as camera types, flight stabilization, return home, etc., among the most used by ordinary users is the Phantom 3 SE and Phantom 4.

- *Phantom 3 SE:* It has a flight autonomy of 25 minutes with a control range of 4 km.
- *Phantom 4:* It has a flight autonomy of 30 minutes with a range of control of 4 km, two sensors of rear vision and infrared detection systems for a total of 5 directions of detection of obstacles and 4 directions of avoidance of obstacles.

### 2) DRONE PARROT

Parrot is expanding in the market of unmanned aerial vehicles (UAV), with the Parrot AR.Drone, the first quadrocopters piloted via WiFi and also with new solutions to apply the UAV market to professional use. There are different types of Parrot drones like the FPV Disk, Bebop 2 and A.R Drone 2.0. These have different types of cameras to take videos, stabilization on the flight, geographical location, etc [7].

- Disco FPV: It has a flight time of 45 minutes, with a range of 80 km/h, designed to fly like an airplane.
- Bebop 2: It has a flight time of 25 minutes and can reach a maximum speed of 60 km/h in horizontal and 21 km/h in vertical.
- A.R Drone 2.0: It has an automatic piloting that facilitates the takeoff and landing, and you can perform pirouettes with the AR Free Flight application. It has two versions that are the Parrot AR.Drone 2.0 Elite Edition and the Parrot AR.Drone 2.0 GPS Edition.

### 3) DRONE 3D ROBOTICS

3D Robotics created the world class universal flight code, called APM. 3DR uses this code to develop the Pixhawk, to this day the world’s leading autopilot platform. This platform is used by the largest and most successful UAV companies and by research institutes around the world, as for example the National Aeronautics and Space Administration (NASA).

In 2015, the 3DR company launched Solo, the first smart drone in the world. Alone, he brought to life the first technologies and professional tools designed specifically to make photography in the drone easy for both beginners and professionals [8].

## III. VULNERABILITIES DETECTED IN DRONES

Among the vulnerabilities and attacks related to drones most used today, there are attacks on the drone’s communication system and on the operating system that controls its basic functions. With these attacks you can obtain the autonomy of the drone by giving new orders or kidnapping it to obtain private information from the owner. However, most of these attacks are aimed at the drones of the French company Parrot, since they are one of the most popular drones today because of their low price can be acquired by all users.

Most drones use the C or C ++ programming language. Drones programmed with these languages, including many civilian and military drones, have vulnerabilities. 3D Robotics is one of the companies that has programmed drones, using these development platforms, which are vulnerable to a cyber-attack.

Hackers have begun to develop drones that have the ability to hack other drones. They have also developed Maldrone, a malware specifically designed to hack drones through Internet connections. Maldrone attacks a drone like a malware attacking a computer.

Drones can be attacked by two different vectors: a physical attack vector and a logical attack vector [9].

The physical attack vector occurs when there is physical contact with the aircraft, such as firing an unmanned aircraft with a firearm, crashing it into another unmanned aircraft and capturing it with other physical equipment. In contrast, in the logical attack vector, hackers attack a drone analytically. Drones depend on several technologies to communicate with the operator and determine their flight parameters such as speed, altitude, etc. If these parameters are influenced by an attacker, the drones will react to the attacker's command. The best example of a logical attack vector is Drone Defender invented by Ohio-based nonprofit research and development firm, Battelle. Drone Defender creates a remote control and interrupts GPS to drones up to 400 meters without any collateral damage.

Some of the attacks that have been attributed to drones are mentioned below.

### A. VULNERABLE PORTS

When a port scan is made to the drone, nmap shows two ports that can be used by an attacker. Such ports are 21 (FTP) and 23 (Telnet) among other ports that are related to the operation of the drone [10].

- File Transfer Protocol: An attack on file transfer protocol (FTP) services can be used to inject files or update some firmware. The attacker has access to the drone by connecting it to a USB stick. With this, the attacker has the ability to read, modify and delete files.
- Telnet: When an attacker uses telnet he can have full access to the drone system, allowing him to modify critical system files and Shell software script, which uses the Parrot to cause any damage. In a simple case, the attacker can restart the drone in full flight, deactivating the drone's motors causing its fall to the ground [11].

### B. FLOOD

The architecture of many of the radiofrequency communications protocols can be exploited to design methods that keep the channel occupied more efficiently than through a conventional *jamming*. The clearest example of this type of method is called *Flooding*. This method tries to flood the channel. In the case of WiFi, for example, certain types of packages containing information not relevant to the user can be used, with the intention of interrupting communication on that channel or even causing the access points to collapse. There are two methods for this type of attack [12].

- Denial of Service (DoS) Its purpose is to break in and prevent access to a certain service; generally by overloading the system's computational resources or the occupation of the available bandwidth so that the user cannot use it.

### C. ATTACKS ON THE WIRELESS NETWORK OF DRONES

One of the drones that have been attributed more vulnerabilities related to the wireless network is the AR drone 2.0 of the company Parrot. The Parrot AR dron 2.0 creates an Access Point so that a user can connect by means of his Smartphone. The access point it creates is named 'ardron2' followed by a random number. Once a user connects to the Acces Point device, an application can be run to gain control of this drone.

The attack can be carried out using a laptop, a Wifi antenna via USB. AR drone 2.0 is turned on and after a few seconds of flight, the Access point created is visible to all devices. To access the Access Point anonymously, you can use brute force methods to find the Access Point password. However, sometimes, the default password is not modified and it is enough to consult a user manual or Internet to obtain the password. When the password is obtained, Telnet can be used to make a remote connection to the drone. With this you can explore the system and in many cases, modify the basic functions of the drone. This attack can be done using a Rasberry Pi to automate the process through a Script. The attacker will have to perform the following steps to carry out the attack [13]:

1) Login via SSH to the drone using the Raspberry Pi.
2) Change directory to the desktop to execute the scripts in a simple way.
3) Create a file so that the device is automatically linked to the access point of the drone.
4) Create a file to turn off the device when it is in flight.
5) These files should be called from a script that accomplishes this task.

### D. HIJACK

This attack involves the hijacking of a drone in mid-flight. The SkyJack software created by Samy Kamkar seeks to fulfill this action. At present it has been found that the Parrot AR 2.0 is prone to this vulnerability. This attack can be done through a Raspberry Pi which will look for an open Parrot network. Once it is found, the software makes a connection to it by changing the SSID and eliminating the connected users. When it is reconnected, data can be sent via the Raspberry Pi to the hijacked drone. Once the drone is out of reach of the original user nothing can be done to regain control [14].

### E. MALDRONE

Maldrone is a more generalized software that acts as a back door. It infects the victim drone and waits for a reverse TCP connection of the drone. Once the connection is established, you can interact with the software and with the drone's controllers/sensors directly. There is a piloting program from the AR drone 2.0 that shows the back door and kills the autopilot and takes control [14] [15].

The Maldrone has the following characteristics:

- It is installed silently in a drone.
- Interact with device drivers and sensors silently.
- Master drone bot controller remotely.
- Escape from the owner's drone to bot master.
- it can have remote surveillance.
- Maldrone can be spread to other drones.

## IV. ATTACKS ON THE GLOBAL POSITIONING SYSTEM

The global positioning system (GPS) has been used in different government sectors and in companies it has been used for most of the applications that make use of positioning in real time. Some of these applications include security services such as police, fire, rescue and ambulance. They are also commonly used in passenger bus companies, in the cargo industry, in vehicles destined for delivery of parcels, in vehicles in agriculture, in private vehicles, and in all those that use GPS for navigation. As well as in the topography, cell phones, robotics, tracking of domestic animals, etc. [16].

### A. GPS OPERATION

It is a radio positioning system based on multiple satellites in which each GPS satellite transmits data that allows a user to accurately measure the distance from the selected GPS satellites to their antenna and then calculate the position, speed and time parameters with a high degree of accuracy, using known triangulation techniques [17]. This technology gives life to most applications that base their operation on the location, because it is a very precise positioning technology. GPS users have the ability to obtain a 3-D position, velocity and time fix in all types of weather, 24-hours a day. GPS users can locate their position to within ± 18 ft on average or ± 60-90 ft for a worst case 3-D fix [18].

The GPS constellation needed to ensure adequate GPS coverage consists of 21 primary satellites at 10,924 nautical miles (approximately 20,200 km) in altitude. However, the satellite constellation can consist of 24 satellite positions and the 24 active satellites are generally maintained, these 24 positions have been optimized to provide the lowest possible sensitivity to the satellite failure [19]. The constellation of GPS satellites is found in six orbital planes, with four satellites in each plane. The ascending nodes of the orbital planes are equally scattered at 60° of distance, and the orbital planes are tilted to 55°. The satellites are monitored by five base stations. The main base station is located in Colorado Springs, Colorado, and the other four are located on Ascension Island (Atlantic Ocean), Diego Garcia (Indian Ocean), Kwajalein, and Hawaii (Both in the Pacific Ocean) [20].

### B. ATTACKS ON THE GLOBAL POSITIONING SYSTEM

The Global Positioning System, better known by its acronym GPS, is a radio-navigation system owned by the United States that provides reliable positioning, navigation and chronometric services, free and uninterrupted to civilian users all over the world. In addition, it is responsible for the emission of an additional signal with encryption so that it can be used for military purposes. The problem of civil GPS is a public code, without any security. Another system failure is the power with which the signal reaches the Earth's surface, about -160 dBW. GPS signals are susceptible to weaknesses from three sources: unintentional interference, intentional interference and human factors, such as design deficiencies or insufficient operator training. This facilitates attacks such as [12]:

- Signal blocking (jamming): As the name implies, it blocks the GPS signal in its entirety making a receiver and any system that depends on it unusable.
- Spoofing Signal: It involves the creation of a false GPS signal directed to the receiver. To carry out the spoofing takes advantage of the inherent vulnerabilities of the GPS system. It must be borne in mind that in many of these vulnerabilities do not affect the military signal, since it has additional security implemented with encryption and cryptographic identification. This attack is the most difficult to detect since there are no methods for it. Currently, the vast majority of GPS receivers do not have defense algorithms against this type of attack. This is because manufacturers do not see it as a potential hazard given its complexity.

## V. GPS SPOOFING

As mentioned previously, GPS technology guides map applications and location services that are used on a daily basis is provided by satellites orbiting the Earth. But it is possible to create a GPS signal from the ground that simulates the original.

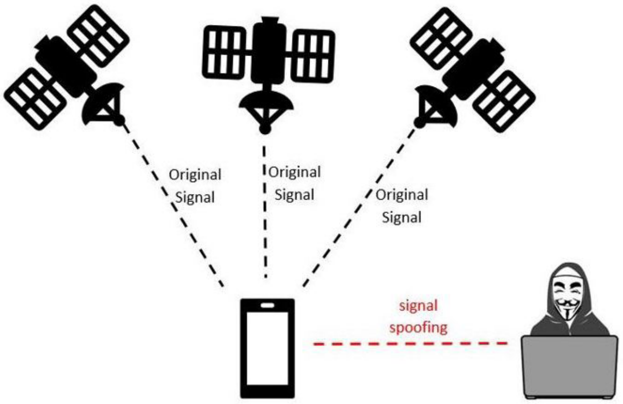


FIGURE 2. GPS attack.

GPS spoofing is the act of producing a falsified version of the GPS signal with the goal of taking control of a target GPS receiver's position-velocity-time (PVT) solution. This is most effectively accomplished when the spoofer has knowledge of the GPS signal as seen by the target receiver so that the spoofer can produce a matched, falsified version of the signal. In the Figure 2 shows how the GPS Spoofing attack works.

In the case of military signals, this type of attack is nearly impossible because the military signal is encrypted and therefore unpredictable to a would-be spoofer. The civil GPS signal, on the other hand, is publiclyknown and readily predictable [21]. In Figure 3 the attack environment is observed what is used to exploit this vulnerability.

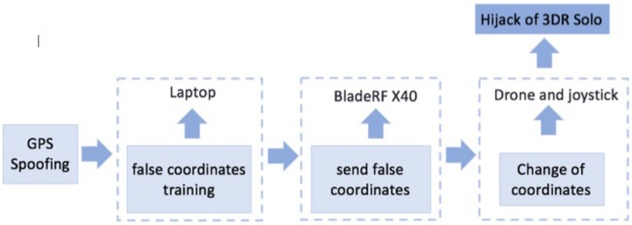
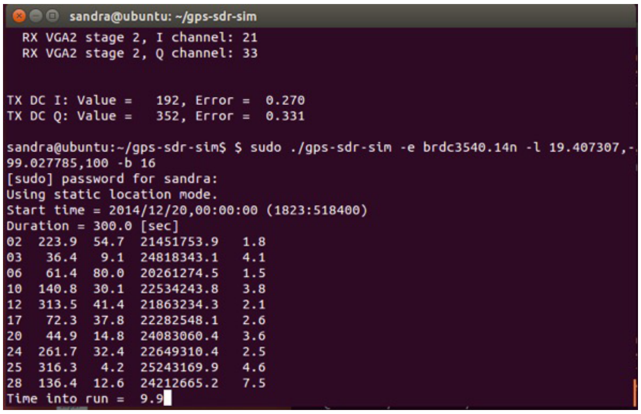


**FIGURE 3.** GPS attack diagram spoofing.

```
$ ./gps-sdr-sim -e brdc3540.14n
      -l 19.407350,-99.027718,100 -b 16
```

**Command 1.** Command for the creation of gps-sdr-sim script.



```
  RX VGA2 stage 2, I channel: 21
  RX VGA2 stage 2, Q channel: 33


TX DC I: Value =   192, Error =  0.270
TX DC Q: Value =   352, Error =  0.331

sandra@ubuntu:~/gps-sdr-sim$ $ sudo ./gps-sdr-sim -e brdc3540.14n -l 19.407307,-
99.027785,100 -b 16
[sudo] password for sandra:
Using static location mode.
Start time = 2014/12/20,00:00:00 (1823:518400)
Duration = 300.0 [sec]
02  223.9  54.7  21451753.9   1.8
03   36.4   9.1  24818343.1   4.1
06   61.4  80.0  20261274.5   1.5
10  140.8  30.1  22534243.8   3.8
12  313.5  41.4  21863234.3   2.1
17   72.3  37.8  22282548.1   2.6
20   44.9  14.8  24083060.4   3.6
24  261.7  32.4  22649310.4   2.5
25  316.3   4.2  25243169.9   4.6
28  136.4  12.6  24212665.2   7.5
Time into run =  9.9
```

**FIGURE 4.** Creation of the gps-sdr-sim script.

In this attack environment there are four phases which are:

- Training false GPS coordinates with the help of a laptop.
- Coordinates are sent using the BladeRF for transmission.
- Subsequently, the drone recognizes the transmitted coordinates as if they were sent by the satellite.
- Finally, a Drone Hijack can be performed.

For the exploitation of this vulnerability, a laptop with a virtual machine with a Linux operating system was required, in this case, Ubuntu 14.04 and a BladeRF X40 to be able to transmit the false coordinates. For the transmission of these coordinates, the necessary libraries were installed to work with the bladeRF [22].

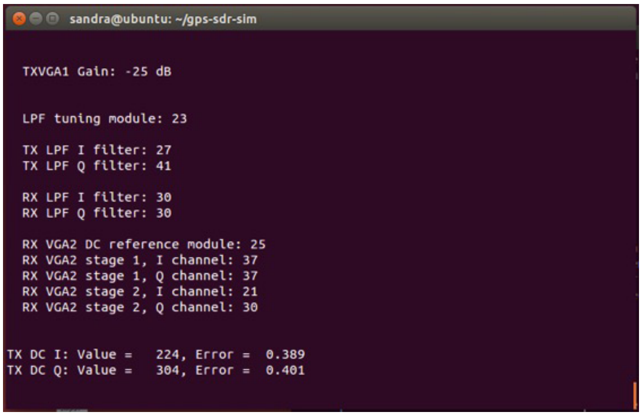
It should be noted that there are different software versions for the Field Programmable Gate Arrays (FPGA) and firmware that can be installed on the bladeRF. In this case you must have a version of FPGA and specific firmware so that the operation of the bladeRF is correct which in this case the X40 is used, but there is also version x115.

Once the bladeRF is recognized in the system, the training of false coordinates is performed by means of the use of scripts dedicated to simulate the parameters that the drone receives when it requests its location via GPS.

Subsequently, the file is created with the corresponding coordinates. In this case coordinates are placed belonging to the Mexico City. It should be mentioned that the coordinates can be anywhere. The creation of the script uses the command 1.

```
$ bladeRF-cli -s bladerf.script
```

**Command 2.** Command for the transmission of the gps-sdr-sim script.



```
 TXVGA1 Gain: -25 dB

 LPF tuning module: 23

 TX LPF I filter: 27
 TX LPF Q filter: 41

 RX LPF I filter: 30
 RX LPF Q filter: 30

 RX VGA2 DC reference module: 25
 RX VGA2 stage 1, I channel: 37
 RX VGA2 stage 1, Q channel: 37
 RX VGA2 stage 2, I channel: 21
 RX VGA2 stage 2, Q channel: 30


TX DC I: Value =   224, Error =  0.389
TX DC Q: Value =   304, Error =  0.401
```

**FIGURE 5.** Transmission of gps-sdr-sim script.

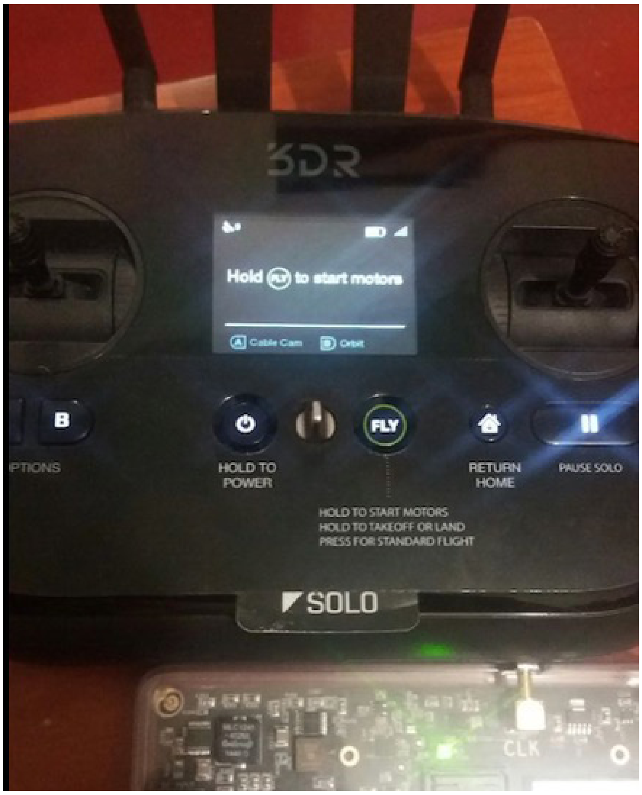


**FIGURE 6.** False GPS signal recognized by the drone.

The realization of the script with the false coordinates has a training time of 300 seconds as can be shown in Figure 4.

Once the script is carried out, the transmission of the coordinates to the drone is continued with the help of the bladeRF, the transmission is carried out with the command 2.

The transmission of the script as shown in Figure 5, it has an estimated time of five minutes in which the coordinates are sent to the drone and after those minutes the script has to be re-executed as many times as necessary so that the drone picks up the false signal.

Once the above is done, it is expected that the drone captures the data transmitted by the bladeRF, it may vary some minutes but the result is satisfactory.

In the exploitation of this vulnerability the control captures the false signal that is transmitted by the bladeRF until the GPS signal finds a total of 9 satellites or more as shown in Figure 6, and the drone will be ready to fly and perform its basic functions.

A small observation is that at the moment of exploiting the vulnerability the bladeRF must be a short distance from the drone so that the intense of the signal is favorable in the attack.

## VI. CONCLUSION

Due to the great popularity of drones in all areas of research, these are very useful for users who use them as in agriculture or photography. However, the vulnerabilities mentioned in this paper can be easily exploited by the technologies used by companies for the communication and control of the drone. Some of these vulnerabilities are in the wireless network and in GPS. These vulnerabilities can be easily exploited because the security of these aerial devices is not given much importance because some are inexpensive or they are used as a toy. In the research carried out, it can be deduced that the drone with the most known and exploited vulnerabilities satisfactorily are those created by the French company Parrot. This is due to the great popularity of these drones among people and the low cost they have. Vulnerabilities to be exploited can have the autonomy of the drone and thus be able to perform actions that may even harm third parties both physically and morally or simply hijack the air vehicle.

However, it was possible to perform a GPS Spoofing successfully in the 3D Rootics Solo drone, in which it can be shown that the control captured the false GPS signal as authentic, allowing it to control the aircraft without any type of anomaly. The exploitation of this vulnerability in a satisfactory manner is due to the fact that the power of the GPS signal when arriving at the devices is low and all this is due to the geographical distance and position in which the GPS satellites are located and these do not have an encryption. compared to the GPS service dedicated for military use. By making a signal closer to the target, the power of the false signal is higher when executing the GPS Spoofing. This makes the attack possible and effective, allowing ill-intentioned people to hijack the drone and send it to another place or make it fly over an unauthorized place.

From the above it can be concluded that, although drones can be very useful for people and companies that use them in their daily activities. They can also be a starting point for an attacker to seek to violate the privacy of people by obtaining confidential data or physically damaging them if it is used in a kamikase mode.

## REFERENCES

[1] E. Drone. (2018). *Eldrone*. [Online]. Available: http://eldrone.es/que-es-un-drone/
[2] P. Rojas and J. Duvan, "Drones en las Geociencias. Guía de Implementación en la Cartografía," Facultad de Ciencias Agropecuarias, Univ. de Cundinamarca, Fusagasugá, Colombia, 2017.
[3] M. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones: A review," *Progr. Aerosp. Sci.*, vol. 91, pp. 99–131, May 2017.
[4] O. Cantos, "Drones y su aplicación en materia de seguridad y salud en el trabajo," Facultad de Medicina, Univ. Miguel Hernandez, Alicante, España, 2015.
[5] M. Mulas, *Aplicación de los Drones en mHEALTH: Una Realidad sin Normativa Legal*. Madrid, España: Universidad CEU San Pablo, 2016.
[6] Waldraff. *Los drones, la Tecnologia más Sobrevalorada del CES*. Accessed: Feb. 15, 2019. [Online]. Available: http://techcetera.co/los-drones-la-tecnologia-mas-sobrevalorada-del-ces/
[7] *The Future of Possible*. [Online]. Available: https://3dr.com/about/
[8] 3D Robotics. *About 3DR, Learn About 3DR and the People who Made it Possible*. [Online]. Available: http://www.dji.com/company
[9] M. Manimaran, "Cybersecurity in drones," M.S. thesis, Utica College, Utica, NY, USA, 2016.
[10] E. Deligne, "ARDrone corruption," *J. Comput. Virol.*, vol. 8, nos. 1–2, pp. 15–27, 2012. Accessed: Jan. 12, 2018. doi: 10.1107/s11416-011-0158-4.
[11] J.-S. Pleban, R. Band, and R. Creutzburg, "Hacking and securing the AR.Drone 2.0 quadcopter: Investigations for improving the security of a toy," *Proc. SPIE*, vol. 9030, Feb. 2014, Art. no. 90300L.
[12] X. W. Casanovas, "Análisis de vulnerabilidades en sistemas de drones," M.S. thesis, Polytech. Univ. Catalonia, Barcelona, Spain, 2016.
[13] B. Chapman. *Build a WiFi Drone Disabler with Raspberry Pi*. Accessed: Feb. 12, 2018. [Online]. Available: https://makezine.com/projects/build-wi-fi-drone-disabler-with-raspberry-pi/
[14] F. Trujano, B. Chan, G. Beams, and R. Rivera, "Security analysis of DJI phantom 3 standard," Massachusetts Inst. Technol., Cambridge, MA, USA, 2016.
[15] S. Kamkar. *Maldrone the First Backdoor for Drones*. Accessed: Feb. 17, 2019. [Online]. Available: http://garage4hackers.com/entry.php?b=3105
[16] U. S. Department of Defense. (2018). *Global Positioning System (GPS) 2008*. [Online]. Available: https://www.gps.gov/congress/reports/2008/biennial-gps-report.pdf
[17] A. K. Brown and M. A. Sturza, "Vehicle tracking system employing global positioning system (GPS) satellite," U.S. Patent 5 225 842, Jun. 7, 1993.
[18] US Air Force. *Schriever Air Force Base*. Accessed: Sep. 17, 2018. [Online]. Available: https://www.schriever.af.mil/GPS/
[19] C. G. B. Green, P. D. Massatt, and N. W. Rhodus, "The GPS 21 primary satellite constellation," *Navigation*, vol. 36, no. 1, pp. 9–24, 1989.
[20] G. Xu and Y. Xu, *GPS: Theory, Algorithms and Applications*. Springer, 2016, pp. 2–4.
[21] 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 *Proc. ION GNSS*, Nashville, TN, USA, Sep. 2012, pp. 3591–3605.
[22] W. C. Kang and S. P. Aimin, "Time and position spoong with open source projects," in *Proc. Black Hat Eur.*, vol. 148, 2015, pp. 1–8.

**SANDRA PÉREZ ARTEAGA** received the degree in computer engineering in 2015 and the M.Eng. degree in security engineering and information technology from the Instituto Politécnico Nacional, Mexico, in 2018. In 2017, she completed a research stay with the Group Analysis, Security and Systems (GASS), Universidad Complutense de Madrid, for six months. In 2018, she participated with a team in the Hackdef 2018 classification round of the 6th Information Security Congress organized by the Instituto Politécnico Nacional through the Sección de Estudios de Posgrado e Investigación of the Escuela Superior de Ingeniería Mecánica y Eléctrica, being in second place. Her main research interests include information security and security in unmanned aerial vehicle technologies in their different applications.

**LUIS ALBERTO MARTÍNEZ HERNÁNDEZ** received the degree in computer engineering and the M.Eng. degree in security and information technology from the Instituto Politécnico Nacional, Mexico, in 2015 and 2018, respectively. He made a research stay with Group Analysis, Security and Systems (GASS), Universidad Complutense de Madrid, in 2017. He also did courses on network security with the Escuela Complutense de Verano and the Escuela Complutense Latinoamericana. In 2018, he participated with a team in the Hackdef 2018 classification round of the 6th Information Security Congress organized by the Instituto Politécnico Nacional through the Sección de Estudios de Posgrado e Investigación of the Escuela Superior de Ingeniería Mecánica y Eléctrica, being in second place. His main research interests include information security, mobile network technologies, and their applications.

**GABRIEL SÁNCHEZ PÉREZ** received the degree in computer engineering from the Instituto Politécnico Nacional, Mexico, where he is currently pursuing the Ph.D. degree in communications and electronics. He did a research stay at the University of Electro-Communications (UEC), Tokyo, Japan, in 2001. He was a Postdoctoral Researcher with the Instituto Nacional de Astrofísica, Optica y Electronica, Mexico, from 2008 to 2009. His research interests include biometric security, and the development of information security strategies applied to governmental and private entities.

**ANA LUCILA SANDOVAL OROZCO** was born in Chivolo, Magdalena, Colombia, in 1976. She received the degree in computer science engineering from the Universidad Autónoma del Caribe, Colombia, in 2001, the Specialization Course in computer networks from the Universidad del Norte, Colombia, in 2006, and the M.Sc. degree in research in computer science and the Ph.D. degree in computer science from the Universidad Complutense de Madrid, Spain, in 2009 and 2014, respectively, where she is currently a Postdoctoral Researcher. Her main research interests include coding theory, information security, and its applications.

**LUIS JAVIER GARCÍA VILLALBA** received the degree in telecommunication engineering from the Universidad de Málaga, Spain, in 1993, and the M.Sc. degree in computer networks and the Ph.D. degree in computer science from the Universidad Politécnica de Madrid, Spain, in 1996 and 1999. He was a Visiting Scholar at Computer Security and Industrial Cryptography (COSIC), Department of Electrical Engineering, Faculty of Engineering, Katholieke Universiteit Leuven, Belgium, in 2000 and a Visiting Scientist at IBM Research Division, IBM Almaden Research Center, San Jose, CA, USA, in 2001 and 2002. He is currently an Associate Professor with the Department of Software Engineering and Artificial Intelligence, Universidad Complutense de Madrid (UCM) and the Head of the Group of Analysis, Security and Systems (GASS), School of Computer Science, UCM. His professional experience includes research projects with Hitachi, IBM, Nokia, and Safelayer Secure Communications.