GPS SPOOFING FRAMEWORK TO ATTACK CIVILIAN GPS RECEIVERS ON DRONES AND OTHER SYSTEMS

Dr. Sunny Arora[1], Dr.Ashwani Sethi[2]
[1,2]Guru Kashi University, Talwandi Sabo

Abstract

Drones are becoming more popular, with a variety of uses in both commercial and military applications. Unmanned aerial vehicles (UAVs) are already being utilized in battle and may carry a variety of missiles, such as the USA's "MQ-8B Fire Scout." Indeed, even new warrior jets have been altered to work as completely independent automated flying vehicles (UAVs). We show how to introduce programming for GPS signal age and transmission, as well as a Python script for recovering robot information. We utilize the Python module Pymavlink to get a robot's status, for example, position and speed data from the GPS crude info or intertwined information from the EKF, utilizing the MAVLink convention on a UDP port. We research weakness in these automated frameworks from both a product and equipment viewpoint, with a specific accentuation on the security of non military personnel GPS recipients on customer drones that use the increasingly ubiquitous software-defined radio cards. We talked about GPS location ideas and data formats, as well as the software and hardware platforms used in GPS spoofing attacks. and the control and communication protocol for a consumer drone. Then, using trials, we proposed a realistic GPS spoofing attack framework. Our findings reveal that the drone is subject to such attacks and that it is possible to cause the drone to divert from its intended path.

Keywords: GPS Spoofing, attack, civilian, receiver, drone, system, etc

1. INTRODUCTION

Drones are becoming more popular, with a variety of uses in both commercial and military applications are possible. Over 10,000 robots are presently filling in as high-data transmission portable web spines, security reconnaissance, salvage administrations, independent air taxicabs, and compassionate activities, according to some estimates. around the world. Furthermore, by 2024, the drone market is expected to be worth $1.85 billion USD. They're utilized in the military for observation, tracking, and delivering armed payloads. Unmanned aerial vehicles (UAVs) are already being utilized in battle and may carry a variety of missiles, such as the USA's "MQ-8B Fire Scout." Even new fighter jets have been adapted to operate as completely autonomous unmanned aerial vehicles (UAVs). Guidance, navigation, and control are all largely reliant on the Global Navigation Satellite System (GNSS) in modern UAVs (GNC). Among the GNSS decisions, the Global Positioning System (GPS) is the most far reaching and generally utilized satellite route framework. Independent UAVs depend vigorously on flight helps like autopilot, route, and dynamic situating frameworks. GPS utilizes on-board nuclear clocks to offer time synchronization with an accuracy of about 10 billionth of a second, in addition to its well-known precise locating function.

1.1 GPS Spoofing's Impact on Unmanned Aerial Vehicles

Over the last few years, a variety of Unmanned Aerial Vehicle (UAV) models have emerged, each with its own set of flying capabilities as well as flight controllers Quadcopters, sometimes known as multi-rotor helicopters, have risen in popularity because to their wide a wide range of applications, a simple mechanical design, flying capabilities, a wide range of solutions, and inexpensive cost. Due to its movement versatility, having 6 degrees of freedom, this type of vehicle has a wide range of commercial, industrial, and academic applications (i.e., capable of moving and rotating along three axes). Because of its agility, which encompasses even and vertical flight, vertical landing and take-off, and drifting, it is a solid contender for independent flights.Because these systems have all of the elements required for autonomous flight, they are vulnerable to hostile acts aimed at individuals or facilities, such as hijacking and controlling the vehicle, tracking people, shooting them down, or eavesdropping on them. These vehicles are typically simple and inexpensive to construct, requiring only a few sensors such as Inertial Measuring Units (e.g., gyrator, accelerometer), Barometers, and GPS, which are expected to be used independently flying. The aforesaid security risks are typically overlooked when designing a flight controller, as dealing with unstable conditions and defective components or sensors is already a difficult effort. In fact, the complexity of these systems is typically extremely considerable, which increases the risk of security issues. Sensor fusion is commonly used by UAVs to cope with their unstable surroundings and defective components. They estimate their current state based on previous vehicle positions, which are compared to the outputs of a sensor fusion algorithm (e.g., Extended Kalman Filter (EKF)), which takes the outputs of many sensors (e.g., Inertial Measurement Unit (IMU), Barometer). as inputs, as well as GPS readings.

2. REVIEW OF THE LITERATURE

Shah Khan, Mujahid Mohsin, and Waseem Iqbal (2021) Unmanned Aerial Systems (UAVs, Drones), which were once primarily used for military purposes, are now becoming increasingly popular in the civilian sector. Drones have already shown to be a valuable force multiplier in the military by performing autonomous, surveillance, reconnaissance, search and rescue, and even armed operations that operate around the clock, over vast distances, and with high endurance conflict. Commercial drone deployments are rising exponentially as the Internet of Things (IoT) emerges, Cargo and taxi services, as well as agriculture, disaster relief, risk assessment, and crucial infrastructure monitoring, are all available. Regardless drones are commonly entrusted with crucial safety, time, and liability considerations in the deployment sector activities, necessitating secure, resilient, and trustworthy operations. In contrast, rising demand for unmanned aerial vehicles (UAVs), along with market strain to lessen size, weight, power, and cost (SwaP-C) factors, has prompted merchants ignoring security issues, presenting genuine wellbeing and security dangers. UAVs are helpless against GPS sticking and caricaturing since they depend on the Global Placement System (GPS) for route and situating. The weakness of GPS to parodying has significant repercussions for UAVs, as demonstrated in a few scholarly examination studies utilizing industrially accessible GPS mocking gadgets, as weak robots utilizing common GPS can be diverted or even commandeered for criminal reasons. Other GPS-reliant platforms, such as piloted aircraft, ground vehicles, and cellular networks, are vulnerable to GPS spoofing attacks as well. This paper investigates GPS caricaturing dangers top to bottom, with an exceptional accentuation on their pertinence to automated airborne vehicles (UAVs) and different GPS-subordinate portable devices.

Eric Horton and Prakash Ranganathan (2018) The Worldwide Positioning System (GPS) is a satellite route framework (GPS) Spoofing assaults imperil the advancements on which our cutting edge civilisation is assembled. To sufficiently build cautious frameworks against these assaults, techniques for reenacting the assaults and recognizing them from typical GPS activity should be created. This paper centers around the bit by bit execution of minimal expense GPS parodying and undeniable level caricaturing information gathering hardware to display a straightforward mocking attack that might be done with few assets. The created caricaturing gadget was utilized to effectively attack a DJI Matrice 100 quadcopter, and an example of the ridiculing information was obtained. is given.

Jie Su, Jianping He, Peng Cheng, and Jiming Chen (2016) An Unmanned Aerial Vehicle's autopilot relies heavily on GPS (UAV). Due to the susceptibility of civilian GPS signals, a GPS spoofing attack on a UAV has recently piqued researchers' interest. This paper describes a situation in which a GPS spoofing attacker attempts to fly a UAV equipped with a fault detector to any random location without activating the detector. We define the challenge as a constrained optimization problem and offer a practical solution for computing the false GPS measurements at each time instant. In addition, we investigate and compute the UAV's biggest reachable location set under GPS spoofing attack, which quantifies the GPS spoofing attack's capabilities under the fault detector restriction. To verify the results, numerical simulations with various parameter settings are run.

Andrew Kerns, Daniel Shepard, Jahshan Bhatti, and Todd Humphreys (2014) The theory and practise of capturing and controlling unmanned aerial vehicles (UAVs) using GPS signal spoofing are explored and proven. The purpose of this study is to see how vulnerable UAVs are to misleading GPS (Global Positioning System) is a satellite navigation system (GPS) Spoofing attacks endanger the technologies on which our modern civilisation is based. In order to effectively construct defensive systems against these assaults, strategies for reproducing the assaults and recognizing them from typical GPS activity should be created. This work centers around the bit by bit execution of minimal expense GPS parodying and undeniable level mocking information gathering hardware to demonstrate a straightforward ridiculing attack that might be done with restricted assets. The created satirizing mechanical assembly was effectively used to go after a DJI Matrice 100 quadcopter, and an example of the ridiculing information was obtained are considered both overt and covert spoofing tactics. The spoofer's capacity to covertly capture a mobile target is assessed by analysing and testing GPS receiver tracking loops.

3. OBJECTIVES

- To study GPS Spoofing's Impact on Unmanned Aerial Vehicles
- To evaluate an attack on a receiver using GPS spoofing.

4. RESEARCH METHODOLOGY

4.1 Software Setups

We show how to set up software for GPS signal creation and transmission, as well as a Python script for retrieving drone information.

- **Generation and Transmission of GPS Signals**

Figure 1 depicts the course of our research project's spoofing GPS signal generation and transmission.

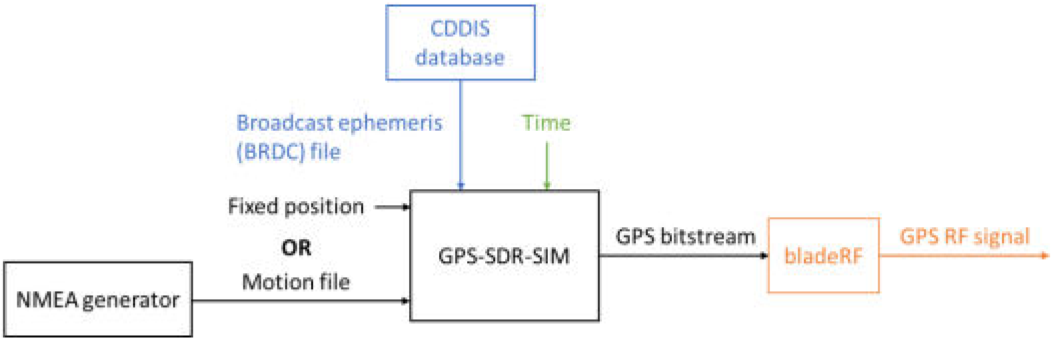


Figure 1: Flowchart of GPS signal generation and transmission

- **Data on Drone Status fetched**

Through the MAVLink convention on a UDP port, we use the Pymavlink is a Python library that might be utilized to recover a robot's status, like position and speed data from GPS crude info or melded information from the EKF. The Python code underneath concentrates and stores information from the robot, for example, time, GPS fix type, EKF status, and GPS position, to a CSV file. Furthermore, we may utilise Python's Matplotlib to show data in a variety of plots.

4.2 Assessment

We need to assess two features of our GPS spoofing attack framework: GPS signal transmission accuracy and attack efficacy method.

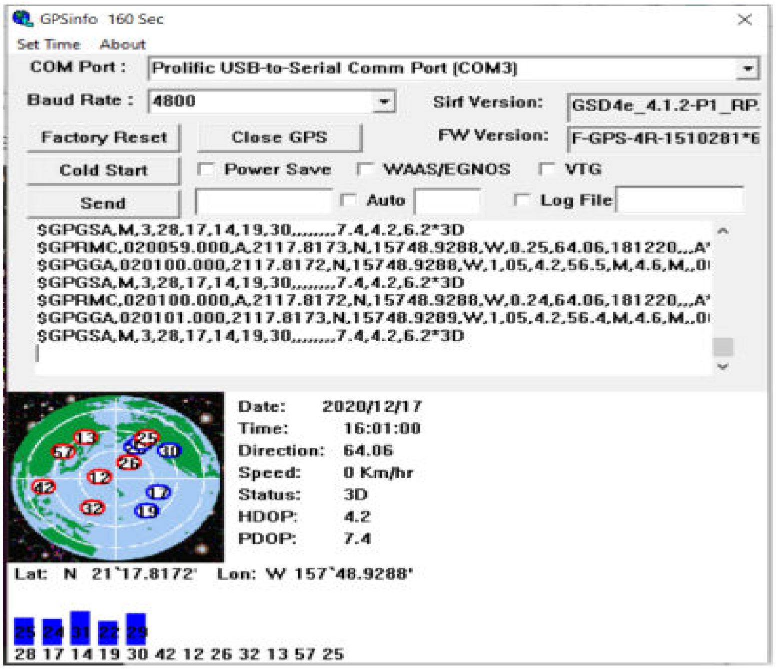
5. DISCUSSION AND RESULT

5.1 An attack on a receiver using GPS spoofing

On a GPS receiver, we present the processes and consequences of two GPS spoofing attacks: fixed position spoofing and moving position spoofing.

- ✓ **Spoofing in a Fixed Position**

To We utilized a BU-353S4 GPS beneficiary and the GPS Info instrument to show GPS data like scope, longitude, time, satellite number, signal strength, etc (as displayed in Figure 2).



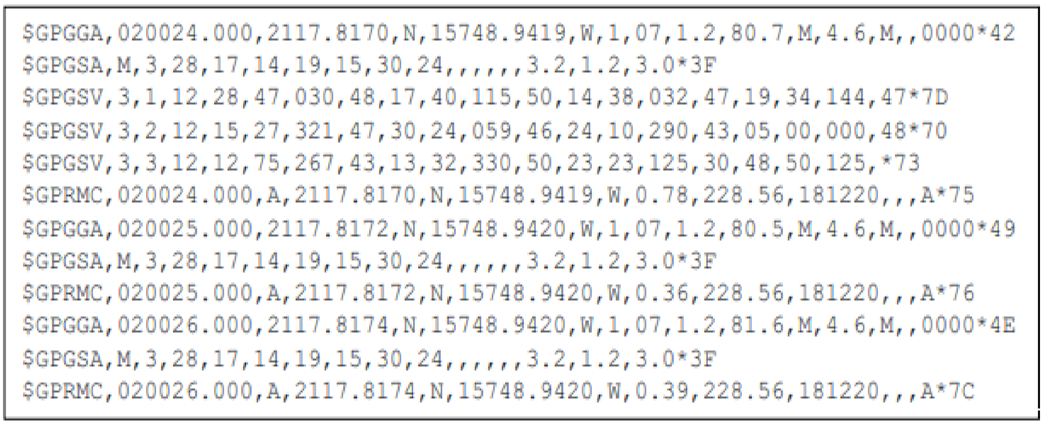
COM Port : Prolific USB-to-Serial Comm Port (COM3)
Baud Rate : 4800
Sirf Version: GSD4e_4.1.2-P1_RP.
FW Version: F-GPS-4R-1510281*6
□ Power Save □ WAAS/EGNOS □ VTG
□ Auto □ Log File

```
$GPGSA,M,3,28,17,14,19,30,,,,,,,,7.4,4.2,6.2*3D
$GPRMC,020059.000,A,2117.8173,N,15748.9288,W,0.25,64.06,181220,,,A*
$GPGGA,020100.000,2117.8172,N,15748.9288,W,1,05,4.2,56.5,M,4.6,M,,0
$GPGSA,M,3,28,17,14,19,30,,,,,,,,7.4,4.2,6.2*3D
$GPRMC,020100.000,A,2117.8172,N,15748.9288,W,0.24,64.06,181220,,,A*
$GPGGA,020101.000,2117.8173,N,15748.9289,W,1,05,4.2,56.4,M,4.6,M,,0
$GPGSA,M,3,28,17,14,19,30,,,,,,,,7.4,4.2,6.2*3D
```

Date: 2020/12/17
Time: 16:01:00
Direction: 64.06
Speed: 0 Km/hr
Status: 3D
HDOP: 4.2
PDOP: 7.4
Lat: N 21`17.8172' Lon: W 157`48.9288'

Figure 2: GPS Info, initial status after position fixed by real satellites

The GPS receiver first obtained a 3D fix to real satellites and displayed its true location. The bogus parodying satellite signs were considerably stronger than the genuine ones, so they overwhelmed the GPS stations when the transmission started, and the beneficiary was misdirected to the new area in under 20 seconds. The accompanying are the NMEA messages that correspond:



```
$GPGGA,020024.000,2117.8170,N,15748.9419,W,1,07,1.2,80.7,M,4.6,M,,0000*42
$GPGSA,M,3,28,17,14,19,15,30,24,,,,,,3.2,1.2,3.0*3F
$GPGSV,3,1,12,28,47,030,48,17,40,115,50,14,38,032,47,19,34,144,47*7D
$GPGSV,3,2,12,15,27,321,47,30,24,059,46,24,10,290,43,05,00,000,48*70
$GPGSV,3,3,12,12,75,267,43,13,32,330,50,23,23,125,30,48,50,125,*73
$GPRMC,020024.000,A,2117.8170,N,15748.9419,W,0.78,228.56,181220,,,A*75
$GPGGA,020025.000,2117.8172,N,15748.9420,W,1,07,1.2,80.5,M,4.6,M,,0000*49
$GPGSA,M,3,28,17,14,19,15,30,24,,,,,,3.2,1.2,3.0*3F
$GPRMC,020025.000,A,2117.8172,N,15748.9420,W,0.36,228.56,181220,,,A*76
$GPGGA,020026.000,2117.8174,N,15748.9420,W,1,07,1.2,81.6,M,4.6,M,,0000*4E
$GPGSA,M,3,28,17,14,19,15,30,24,,,,,,3.2,1.2,3.0*3F
$GPRMC,020026.000,A,2117.8174,N,15748.9420,W,0.39,228.56,181220,,,A*7C
```

Table 1 shows a list of satellites in various scenes based on the data obtained: Position fixed with actual satellites; position fixed using faked satellites; bitstream data created by gps-sdr-sim.

Table 1 List of Satellite PRNs in each scene

Scene	**5**	**7**	**12**	**13**	**14**	**15**	**17**	**19**	**23**	**24**	**25**	**26**	**28**	**30**	**32**	**42**	**48**	**57**
Bitstream	●	●	●	●	●	●	●	●		●			●	●				
Real satellites			○	○	●		●	●			○	○	●	●	○	○		○
Spoofed satellites	◎		◎	◎	●	●	●	●	◎	●			●	●			○	

(● = satellites both in view and in use, ◎ = satellites in view with valid SNRs but not in use; ○ = satellites in view without valid SNRs and not in use)

Because we built the GPS bitstream utilizing the latest ephemeris information and right now, the PRNs of veritable satellites in the bitstream and genuine satellites are almost comparable. Accordingly, on the grounds that the ephemeris, satellite PRNs, and time in the mocking sign are indistinguishable from those in the genuine GPS signal, we can trick the recipient with a phony position near the genuine situation in a brief timeframe when the beneficiary has gotten a position fix, a strategy known as a "hot start."

5.2 Attack on a Drone using GPS Spoofing

In the next two cases, shown in Figures 3 and 4, we while the drone was flying outside, the spoofing attack was carried out: A. We sent GPS coordinates that gradually migrated to a place in longitude and latitude a few metres distant from the initial point while the drone was hovering at a fixed site. (The altitude remains unchanged.) The drone should be flying in the opposite direction according to the drone position control algorithms, to keep its location "unchanged." This scenario is depicted in Figure 3.

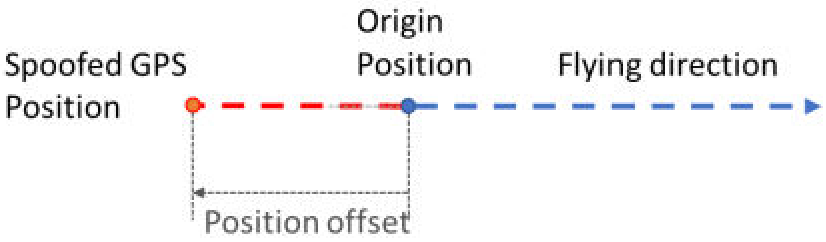


Figure 3: Hovering attack

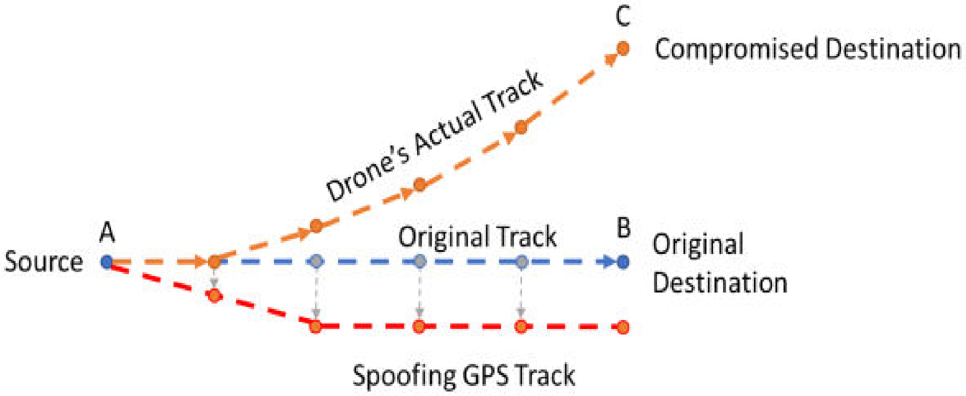


Figure 4: Mission flying attack

- **Hovering Test Result**

In the first place, we led a ground-based caricaturing test utilizing the robot to make sure that the assault plan was viable. (We led the test various times to guarantee that the outcomes were not affected by outside variables like solid breezes.) For the initial 80 seconds, the satirizing GPS position remained at the beginning spot to permit the robot to lock onto the assault signal. After then, at that point, the GPS positions were transferred 5 meters west of the beginning point in 5 seconds and stayed there for 60 seconds. The shift speed of 1m/s is excessively delayed for ArduPilot to identify. In Figure 5, the purple spots mirror the first satirizing signal we sent, while the blue focuses address the mocking sign the robot got.

Between the underlying satirizing positions sent and the positions got by the robot, there were balances (for the most part in the Y-hub). The balances, then again, were reliable and short of what one meter, showing that the mocking signs got by the robot were inside non military personnel GPS precision (10 feet), and subsequently OK.

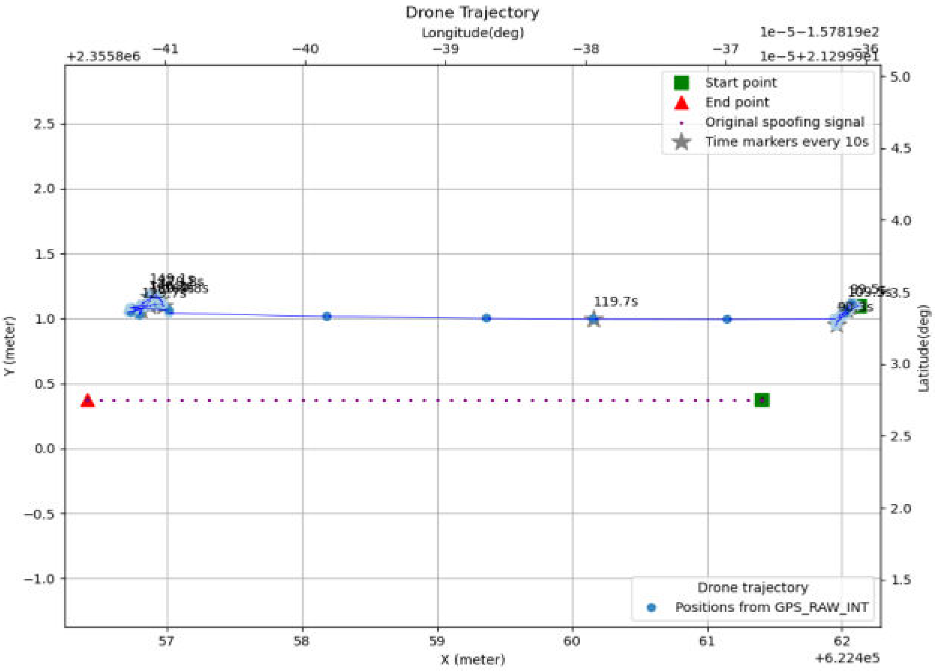


Figure 5: GPS Trajectory when the drone was sitting on the ground

6. CONCLUSION

We concentrate on weakness on these automated frameworks from both a product and equipment viewpoint, with an extraordinary accentuation on the security of non military personnel GPS recipients on buyer drones that use the increasingly ubiquitous software-defined radio cards. We talked about GPS location ideas and data formats, as well as the software and hardware platforms used in GPS spoofing attacks and the control and communication protocol for a consumer drone. Then, using trials, we proposed a realistic GPS spoofing attack framework. Our findings reveal that the drone is subject to such attacks and that it is possible to cause the drone to divert from its intended path. While software vulnerabilities in drones and unmanned automatic systems have been extensively explored, these systems' hardware vulnerabilities have not been broadly examined. In this work, we utilize the as of late well known programming characterized radio cards to examine weakness on these automated frameworks from both a product and equipment angle, with a particular spotlight on the security of non military personnel GPS recipients on buyer drones.

REFERENCES

1. Khan, Shah & Mohsin, Mujahid & Iqbal, Waseem. (2021). On GPS Spoofing of Aerial Platforms: A Review of Threats, Challenges, Methodologies, and Future Research Directions. PeerJ Computer Science. 7. e507. 10.7717/peerj-cs.507.

2. Horton, Eric & Ranganathan, Prakash. (2018). Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter. The Journal of Global Positioning Systems. 16. 10.1186/s41445-018-0018-3.

3. Su, Jie & He, Jianping & Cheng, Peng & Chen, Jiming. (2016). A Stealthy GPS Spoofing Strategy for Manipulating the Trajectory of an Unmanned Aerial Vehicle**This work is supported by National Science Foundation of China under Grant U1401253 and National Key R&D Program Under Grant 2016YFB0800204.. IFAC-PapersOnLine. 49. 291-296. 10.1016/j.ifacol.2016.10.412.

4. Kerns, Andrew & Shepard, Daniel & Bhatti, Jahshan & Humphreys, Todd. (2014). Unmanned Aircraft Capture and Control Via GPS Spoofing. Journal of Field Robotics. 31. 10.1002/rob.21513.

5. He D, Liu H, Chan S, Guizani M. 2019. How to govern the non-cooperative amateur drones?. IEEE Network 33(3):184–189 DOI 10.1109/MNET.2019.1800156.

6. Hermans B, Gommans L. 2018. Targeted GPS spoofing. Master's thesis, University of Amsterdam.

7. Guvenc I, Koohifar F, Singh S, Sichitiu ML, Matolak D. 2018. Detection, tracking, and interdiction for amateur drones. IEEE Communications Magazine 56(4):75–81 DOI 10.1109/MCOM.2018.1700455.

8. Habib B, Maqbool U, Mohsin M. 2019. Safeguarding against gnss spoofing threats-a survey of viable techniques and their tradeoffs. In: Sixth international conference on aerospace science and engineering (ICASE).

9. Hassanalian M, Abdelkefi A. 2017. Classifications, applications, and design challenges of drones: a review. Progress in Aerospace Sciences 91:99–131 DOI 10.1016/j.paerosci.2017.04.003.

10. Hofmann-Wellenhof B, Lichtenegger H, Wasle E. 2008. GNSS–global navigation satellite systems: GPS, GLONASS, Galileo, and more. New York: Springer Wien DOI 10.1007/978-3-211-73017-1_4.