International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXIX No 3 2023

A STUDY REGARDING THE IMPACT OF NAVIGATION DATA MANIPULATION ON UNMANNED AERIAL VEHICLE GNSS SENSORS

Alexandru-Gabriel ROMANIUC*, Vlad-Cosmin VASILE, Elena-Monica BORDA***

***Technical University of Cluj-Napoca, Romania**
****"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania**
romaniuc_alexandrugabriel@yahoo.com, vladut.vasile@yahoo.com, monica.borda@com.utcluj.ro

Abstract: *Nowadays, Unmanned Aerial Vehicle systems have proven to be very useful in a variety of applications, such as monitoring and surveying an area of interest, mapping inaccessible terrain, real-time traffic monitoring, reconnaissance missions, transport of loads, and also for military purposes. The movement and stability in the air of these systems is dependent on the on-board sensors such as GNSS sensors, proximity sensors, accelerometer, gyroscope, light and temperature sensors. GNSS sensors are vital devices capable of processing navigation signals to determine the position, orientation and speed of the UAV system during operation. GNSS sensors are also used in many applications that require navigation data as well as highly accurate synchronization data. Both GNSS systems and the sensors that process their data have been shown to be vulnerable to jamming and spoofing attacks. GNSS sensors are of particular importance and the information provided by them requires protection. Considering these things, this paper aims to carry out a study in which several UAV systems will be exposed to signal samples with manipulated navigation data. This study will help us to assess the impact of exploiting GNSS sensor vulnerabilities and the effects it can have during the operation of UAV systems.*

Keywords: GNSS, UAV, GNU Radio, navigation data, spoofing

1. Introduction

Global Navigation Satellite Systems (GNSS) provide highly accurate navigation and synchronisation data globally. This category includes several systems with global coverage, namely: GPS, Galileo, GLONASS and Beidou [1]. Each of these critical systems transmits navigation data to GNSS receivers on the ground via radio signals. Based on complex algorithms, GNSS receivers perform some calculations to determine navigation data such as speed, position, time, or direction of travel. The information provided by these systems has applications in many critical areas such as road, sea and air navigation, military, telecommunications, computer networks, Unmanned Aerial Vehicle (UAV) systems, and many others [2]. Also, this information is also very important, especially for certain systems that depend on accurate navigation and synchronization data. Recent research [3], [4], [5] has shown that these systems are vulnerable, and the navigation data sent by them can be manipulated. Manipulation of this information can cause serious problems in terms of safety, security and other critical domains. Therefore, it is important to carry out tests to assess this risk to which systems using GNSS receivers are exposed.

Unmanned Aerial Vehicle systems, for example, are systems dependent on the

DOI: 10.2478/kbo-2023-0077

information provided by GNSS systems. Each of them has a GNSS sensor that provides the necessary navigation data to the control unit so that the UAV system can be operated safely [6]. In principle, these systems are controlled remotely via a physical control unit or via automatic control software. For example, to perform a mission in which the system must move along a travel route or to follow certain checkpoints, the system depends on the geolocation process offered by GNSS sensor. Considering these things, we propose to analyze some scenarios in which some UAV systems are exposed to some navigation signal samples in which the geolocation information is modified. To put this into practice, we will need a real-time navigation signal emission system and the UAV systems under test.

2. UAV Systems under Test

The UAV systems that will be subject to the navigation signal tests are two systems, namely a system from the manufacturer DJI model Mavic Air 2 and a Do-It-Yourself (DIY) type system built in the laboratory.

2.1. DJI Mavic Air 2 System

The first system is a Mavic Air 2 model from DJI, shown in Figure 1, together with the remote control unit.

Figure 1: DJI Mavic Air 2 drone with remote control unit

This model stands out for its high mobility and high performance. The model can be controlled remotely via a remote control to which a mobile terminal will be connected. The model also features a dual-band GNSS sensor whose manufacturer has not been disclosed. The sensor is compatible with GPS and GLONASS constellations. This UAV system can be controlled remotely via a remote control. The remote control unit requires the connection of a mobile terminal on which a dedicated application such as DJI Fly must be installed.

2.2. UAV system built in the laboratory

The second UAV system is a drone built in the laboratory using components available on the market. The system offers superior performance but also many functionalities and capabilities. The flight controller of the UAV system is a Pixhawk model and has many sensors installed on it. Also, the system has a GNSS sensor model M8N compatible with all four global navigation constellations. Compared to the first UAV system, it can be controlled in two modes:

- the first mode (Figure 2) involves the use of a remote control unit that offers a minimum set of operations that can be performed on the UAV system;

Figure 2: Pixhawk DIY drone–remote control

- the second mode (Figure 3) involves the use of a telemetry system connected to a computer station which has a dedicated application such as Mission Planner installed. This mode provides some system control functionalities such as mission planning, checkpoints, flight route and many others.

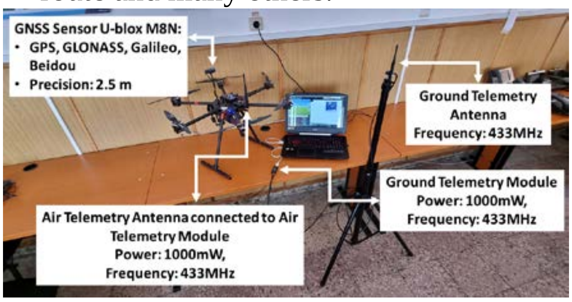

Figure 3: Pixhawk DIY drone–telemetry control

Compared to other systems available on the market, the cost of such a system is much lower. Moreover, the system is capable of lifting medium loads, a useful aspect when it is desired to transport various packets. The performance and functionalities offered is sometimes superior, but it depends very much on the technical skills of the builder and also the quality of the components.

3. Navigation Data Manipulation System

The method used to manipulate navigation data involves generating signal samples using raw navigation files. These files are called ephemerides and contain the parameters of satellites from a constellation. The parameters from these files refer to the exact position of the satellites at a given time, the precise orbital parameters of the satellites and other important data [7]. The files are constantly provided by the Crustal Dynamics Data Information System called CDDIS. Thus, by extracting information from these files it is possible to generate navigation signal samples for a given location on Earth. After generating the raw files, the GNU Radio utility will be used to build a transmission system for the GPS L1 band on the 1575.42 MHz frequency shown in Figure 4. Also, the device used to transmit the signals is the HackRF One SDR (Software Defined Radio) which has installed a TCXO oscillator (Temperature Compensated Crystal Oscillator) needed to generate accurate and stable frequency signals. Signal transmission requires to connect the SDR to an USB 3.0 port in order to ensure a high transfer rate.

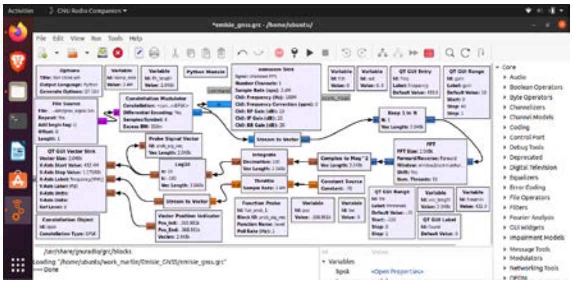

Figure 4: GNU Radio – Navigation signal samples emission blocks

During transmission, the GNU Radio application displays the navigation signal in real time in the frequency domain. Figure 5 shows the interface of the application for transmitting navigation signals.

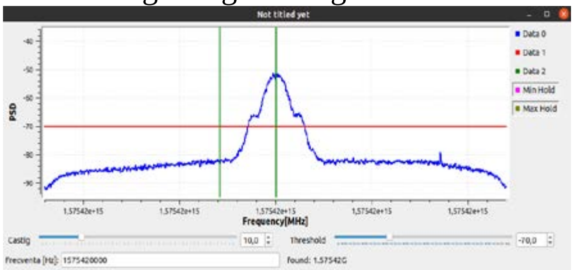

Figure 5: GNU Radio – Navigation signal samples emission interface

4. Testing Scenarios and Results

4.1. DJI Mavic Air 2 System under Test

The first system under test is the DJI model and the test scenario will follow the architecture shown in Figure 6 where the UAV system will be controlled by an operator via the control unit. Also, in the vicinity of the UAV system there is a station with the navigation data exploiting application installed.

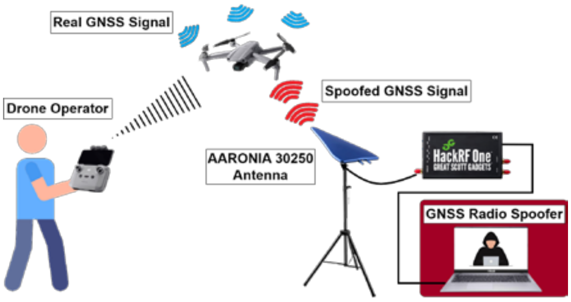

Figure 6: DJI scenario architecture

The location of the equipments from this architecture is shown in Figure 7 and is an isolated location so that signal emission does not affect other systems in the vicinity.

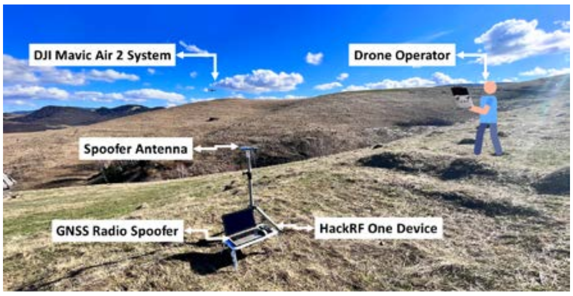

Figure 7: DJI scenario location

The location of the scenarios has the coordinates: 45°41'17.7"N, 23°59'22.0"E. Given the scenario architecture, the UAV system is lifted from the ground at low altitude and brought into close proximity to the navigation signal transmitter system. It is controlled for one minute, after which the navigation signals transmission is started. The duration of the navigation signal transmission was about 4 minutes, during which time the geolocation data of the system changed as shown in Figure 8.

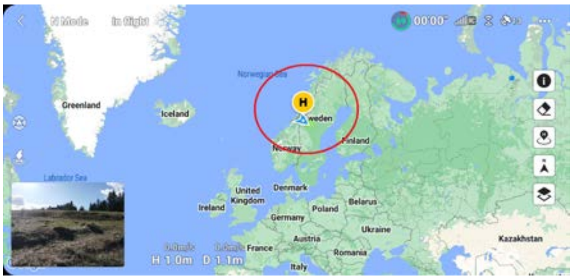

Figure 8: DJY Fly control application during the attack

Figure 8 shows the control application from the mobile terminal connected to the control unit. It can be seen that the location was changed in Norway, more precisely, on the coordinates 64°12'57.4"N 13°08'54.4"E. After these 4 minutes, signal transmission was stopped, and the location of the UAV system returned to the current location. On the ground, flight data was saved from the UAV system. These flight data are flight records containing data from the UAV system during a mission. Based on this data, a graph of the latitude and longitude data from the GNSS sensor on the UAV system was made in Figure 9.

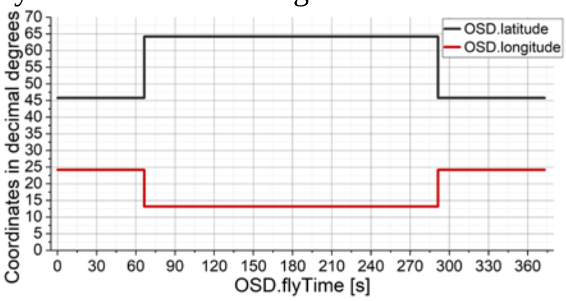

Figure 9: DJI Flight Records: On Screen Display (OSD): latitude and longitude

From the flight records, it can be seen that for the time period in which the signal emission took place, the latitude and longitude was changed. Also, for periods of time when no signal emission occurred, the geolocation data is correct according to the scenario location. Also, from the flight recordings it was possible to make a graph of the number of satellites detected by the GNSS sensor of the UAV system, as shown in Figure 10. It can be observed that, in the first minute of flight, the number of satellites fluctuates (as is normal), but for the period in which the signal was emitted, their number became constant which normally cannot happen.

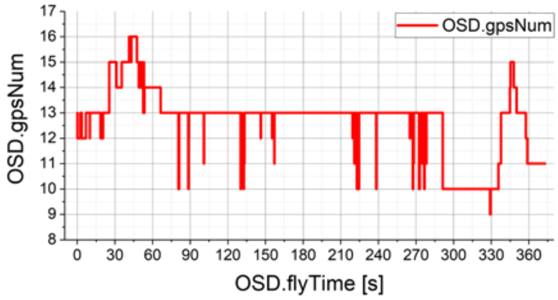

Figure 10: DJI Flight Records: On Screen Display (OSD): number of satellites

4.2. DIY Drone System under Test

For the second UAV system under test, the same topology will be considered as in the DJI system scenario. For this UAV system, both remote control and telemetry control modes will be tested. For the first control mode, the topology of the scenario is shown in Figure 11.

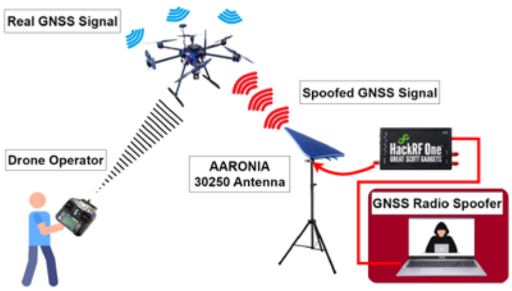

Figure 11: Pixhawk DIY drone –scenario architecture for remote control unit mode

The specificity of this control mode is that, in addition to the basic control, flight modes such as Return to Home, Altitude Hold, Automatic Mode and many others can be activated from the remote control unit. These modes are dependent on the GNSS sensor and the information it provides. Also, the location of this scenario is the same as in the previous scenario and is shown in Figure 12. The navigation signal transmission system is configured with a different location than in the previous scenario.

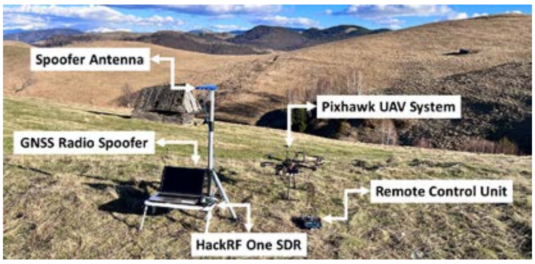

Figure 12: Pixhawk DIY drone –scenario location for remote control unit mode

Given this architecture, the Pixhawk UAV system is lifted from the ground via the remote unit and held in the air for approximately 20 minutes. After this, the transmission of the navigation signal for the coordinates 67°14'47.5"N 39°57'35.6" E is started. The signal transmission was carried out for about 14 minutes and then we stopped it. From the flight records files extracted from the drone, it can be seen that, for the periods of time when we do not transmit the navigation signal, the UAV system was correctly located. From figure 13 it can be seen that for the time period when the navigation signal was emitted, the coordinates were changed.

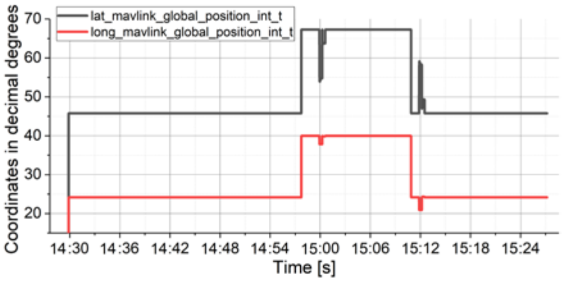

Figure 13: Pixhawk Flight Records for remote control unit mode: latitude and longitude

Also, from the graph we can see some fluctuations that most likely come from the geolocation process of the sensor.
Moreover, for this scenario, we can plot a graph of the number of satellites in the visibility area of the UAV system. Therefore, in Figure 14 it can be seen that for the time periods when no navigation signals were emitted, the number of satellites fluctuated (as is normal). For the period when signals were emitted, the number is constant.

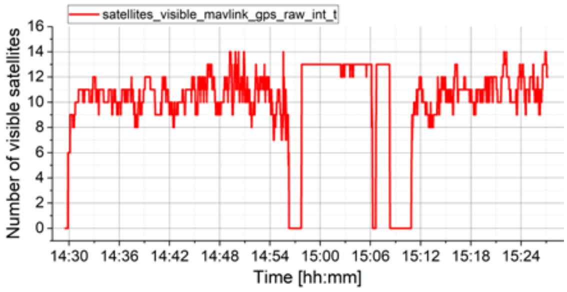

Figure 14: Pixhawk Flight Records for remote control unit mode: number of satellites

For the second control mode, the topology of the scenario is shown in Figure 15.

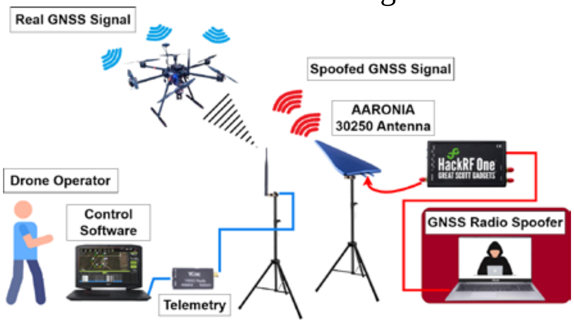

Figure 15: Pixhawk DIY drone –scenario architecture for telemetry control mode

For this architecture, the UAV system will be controlled by the operator via control software called Mission Planner. This control software uses the telemetry module to transmit commands to the UAV system in real time. Next, the location of the equipments for this architecture is the same as in the previous scenario. The navigation signal transmission system is configured in the same mode.

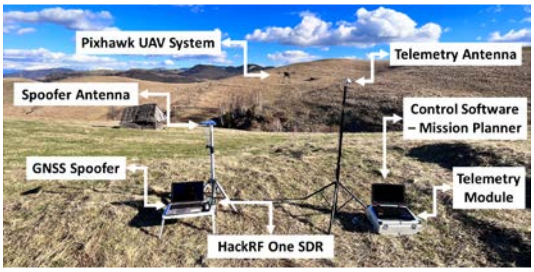

Figure 16: Pixhawk DIY drone –scenario location for telemetry mode

Through the Mission Planner application we can set missions, checkpoints, flight routes and other flight parameters. The application offers an advanced control of the UAV system and also allows viewing the execution of missions in real time.

Figure 17: Mission Planner control application during the attack.

Next, by using this application, the movement of the UAV system will be set to a point on the map. After the system has moved to this point, the navigation signals are emitted during which, the geolocation data of the UAV system has been modified as can be seen in Figure 17.

5. Conclusions

Based on the scenarios presented, the drones and their control modes were tested in the vicinity of the spoofer system. Due to the low transmit power of the HackRF One system, the drones had to be placed at distances of up to 20 meters. Also, the geolocation data used in the scenarios were extracted from ephemerides and converted into binary format. By transmitting these samples in GNU Radio, parameters such as latitude, longitude and number of satellites were affected. Moreover, these methods and techniques presented in the paper could be weaponized and used against these systems. Also, this can be useful for defending against hostile drones.

References List

[1] Hegarty C. Satellite Navigation Systems. In: P. Teunissen, & O. Montenbruck, Eds. Springer Handbook of Global Navigation Satellite Systems. Edition. Springer, Cham; 2017. pp 197-301. https://doi.org/10.1007/978-3-319-42928-1_7

[2] Ahme, F., Mohanta J.C., et al. Recent Advances in Unmanned Aerial Vehicles: A Review. Arab J. Sci. Eng. 47. 2022. https://doi.org/10.1007/s13369-022-06738-0

[3] Kerns A., Shepard D., Bhatti J. & Humphreys T. Unmanned Aircraft Capture and Control Via GPS Spoofing. Journal of Field Robotics. 2014. 31. 10.1002/rob.21513.

[4] Horton E. & Ranganathan P. Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter. The Journal of Global Positioning Systems. 2018; 16. 10.1186/s41445-018-0018-3.

[5] Khan S.Z., Mohsin M. & Iqbal W. On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. PeerJ Comput Sci. 2021; 7:e507. doi: 10.7717/peerj-cs.507. PMID: 34013033; PMCID: PMC8114815.

[6] Patrik A., Utama G., Gunawan A.A.S. et al. GNSS-based navigation systems of autonomous drone for delivering items. Journal of Big Data 6. 2019. 53. https://doi.org/10.1186/s40537-019-0214-3.

[7] Choi J.H., Kim G., et al. Study on Optimal Broadcast Ephemeris Parameters for GEO/IGSO Navigation Satellites. Sensors (Basel). 2020 Nov 16;20(22):6544. doi: 10.3390/s20226544. PMID: 33207807; PMCID: PMC7697757.