Information Security in the use of drones: Research Tools to Maintain Route Integrity

Rilmar Pereira Gomes
rilmargomes@hotmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Aline Siqueira Tavares
alinesiqtav@gmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Eny Alves Martins
enyalvesmartins@gmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Matheus da Silva Pereira Alves
matheuspcj@gmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Jean Mark Lobo de Oliveira
jeanlobolive@gmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

David Barbosa de Alencar
David002870@hotmail.com
Institute of Technology and Education Galileo of Amazon - ITEGAM, BRAZIL

Abstract

Drones have increasingly become part of many people's daily lives and can have many uses, but there are inherent risks to their use that cannot be ignored. This article aims to present some vulnerability risks present in drones and find tools to ensure the integrity of routes traveled by a drone.

Keywords: School Driving; GPS; System; Technology and Traffic;

1. Introduction

The technology market has provided civilians with easy access to drones of different categories that imply their ability to use. Drones ranging from small flights and minutes in duration to hours of flight and cargo transport. Control and programming systems have been improving over time in terms of safety and integrity, for example. However, there is still a deficiency regarding drone attacks by hackers, which aim to affect, mainly, the integrity of the data that is transmitted between the operator and the drone, causing the drone to deviate from its programmed path. With this scenario, a study was carried out where each tool presented in this article has the ability to help together in the fight against attacks that seek to send false GPS signals to divert drones from their original route.

2. Theorical Reference

The drone is one of the components of a UAS (Unmanned Aerial System, or Unmanned Aerial System, in Portuguese), which is summarized in an architecture of three elements: the Drone, Control Station, and the communication data link.

2.1 Drones

Drones are available in several categories (YAACOUB, Jean-Paul et al, 2020) to the public today. We can highlight the three main categories: Multi-Rotor Drones (they are drones capable of maintaining a fixed position, due to their rotating propellers), Fixed Wing Drones (they are more economical because they can glide and reach high speeds), Hybrid Wing Drones (they are the most recent ones, manage to add the characteristics of the previous models).

2.2 Control Station

The control station is the central operation system. She who will control the launch, flight and recovery of the drone. To accomplish this task, it does: drone status reads and controls, displays and controls payload data, map for mission planning, monitoring location and current UAV flight path, and data link system ground terminal. Control stations can come in various complexities and sizes and their shape can vary from backpack-sized to permanent construction.

2.3 Communication Data Link

Communication between the drone and its operator is done through the data link (911 Security, 2020). The data link uses a radio frequency transmission to transmit and receive information. This information can include location, remaining flight time, airspeed, and many other parameters.

2.4 Requirements for a UAV (Unmanned Aerial Vehicle)

For an air vehicle to be characterized as a potential drone (ABDELMABOUD, 2021) some requirements are required and they are basically divided into two:

1. Communication Requirements
2. Security Requirements

When referring to communication requirements, the focus is on: seamless coverage, real-time and remote communication, HD image/video transmission, drone identification and regulation, high-precision positioning.

When attention is directed to security requirements, we are talking about the main pillars of information security: authenticity, confidentiality, availability, integrity and non-repudiation.

The focus of this article will be on security requirements. Especially in the principle called Integrity. This principle ensures that data maintains its original characteristics, as defined at the time it was created, and is therefore protected against unauthorized alteration.

2.5 Ways to Hack Drones

Like computers, drones can be hacked. This is especially true if we note that security against cybercrime was not taken into account during its design. Some potential threats to data integrity are listed below:

2.5.1 GPS tampering

Drone navigation is done by GPS. The GPS (Global Positioning System) is one of the existing satellite navigation systems. All these systems work in a common way, which is to obtain the desired location through trilateration. For this to happen, at least 3 satellites are used; these provide time data to determine latitude, longitude and altitude with an accuracy of a few meters. The receivers use the time signals received from the satellite to accurately calculate the time and position they are in. This determines the location. This interaction between satellites and receivers can be visualized in figure 1.

Figure 1 - Triangulation from the satellites
Source: Net Office

In the brain of the drone, the flight controller, information is received from the GPS module, the remote control and the obstacle sensors (Blog ELETROGATE, 2020). Then, the information is processed, which is passed on to the Electronic Speed Controls (ESCs) to control the engines, even if it is windy enough, the drone remains faithful to its exact position. As the ESC receives signals from the flight controller, it changes the power supplied to each engine. In this way, the information process is not interrupted and all information is received as delivered.

Spoofing happens when a GPS receiver receives incorrect data, which has been manipulated, either by a person or a program, to look similar to normal GPS data. Or when true GPS signals, captured from other locations and under other circumstances, are injected and transmitted to receivers to mislead them.

An attacker who has knowledge of the system parameters and is able to gain access to the flight controller can carry out a modification attack, intercepting system calls issued to the kernel and replacing the genuine recording with a modified one. As a consequence of this attack, the drone may be landed in a different location than originally planned (ALTAWY and YOUSSEF, 2016). That is, instead of the drone following

the path it was programmed to follow, it is moving in a completely opposite direction.

2.5.2 Repeat Attacks

This type of attack uses a fake "time of flight" to give the impression that the receiver is further away than it actually is (DRONE TECH PLANET, 2019). It does this by collecting the true signal and sending it with a certain delay, which can lead to the drone's loss of performance and the failure of its mission.

The other form of this attack is when it corrupts the drones' sensors. The recorded data is used to replace real data so that the controlled system suffers some type of compromise without the supervisory unit's knowledge, for example, the system can be driven to another point of operation, or some act of theft or similar can be carried out.

3. Methodology

For this article, a search was made of projects and studies already developed that served to ensure the integrity of the data and also of available technological tools that had the premise of keeping the real-time monitoring of the drone so that, if an attempt to deviate from the route happened, , the control station quickly managed to stop such an onslaught. In addition, we sought to find solutions for real tracking of GPS coordinates.

Based on the objective of monitoring in real time the path taken by the drone, two streaming tools were used: Amazon IVS and Restream. For tracking via GPS coordinates, the Trackimo tool was used.

3.1 Amazon IVS

Amazon Interactive Video Service (IVS) is an ultra-low latency managed live video streaming service. It supports the most common secure ingestion protocol used in streaming software and hardware, RTMPS (Real-Time Messaging Protocol over a TLS/SSL connection). Its management does both the video transcoding and its global distribution. It provides out-of-the-box interfaces and components, which allows the author to just focus on his audience's experience. (Amazon Web Services, 2022).

To use Amazon IVS, as per the AWS documentation, we follow a few steps:

Step 1 is to create an AWS account and in step 2 you must configure IAM (Identity and Access Management) permissions and add a policy that gives the user access to create an Amazon IVS channel.

To automatically write to Amazon S3, you must also add the appropriate permissions for that. To do this, we follow these steps:

- Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
- In the navigation pane, choose Users and then choose Add user.
- In the Add User window, enter the new username to be created.
- Verify programmatic access and access to the AWS Management Console.
- Choose Next: Permissions.
- Under Set Permissions, enable Append existing policies directly and choose Create Policy . A Create Policy window opens and in it you must choose the JSON tab and paste the IVS policy that is available

and ready to be used in the original AWS documentation. This policy covers standard video and auto-recording functionality on S3.

- After that, a channel with optional recording must be created.
- Configure streaming software.
- View your live stream.

3.2 Restream

Restream is a complete professional live streaming suite. And it can be deployed in various environments such as cloud, SaaS or web-based. To configure the Restream tool, follow these steps:

- Navigate to the Restream panel and click the "Add Destination" button. (Figure 2)

Figure 2 - Add Target Tool Screen
Source: Restream

- Select the "Custom RTMP" option from the list of options, as shown in the figure 3.

Figure 3 - List of options
Source: Restream

- Fill in the RTMPs URL and the transmission key that is provided by the platform the user is connecting to, and confirm by clicking "Add Channel", according to figure 4.

Figure 4 - URL input screen
Source: Restream

After that, the Restream stream will be configured to go directly to Amazon IVS.
At first, it was concluded that the ideal software for real-time transmission of drone images would be AWS IVS, as it is a dedicated service for live video streaming and has super low latency. In addition, it has the ease of configuration to allow data recording to be done directly in an AWS S3 bucket, a much-needed feature as it allows drone images to be recorded in real time in the cloud. Although DJI Drones have a native recording function, this recording is stored locally on the SD card that is in the drone itself and this may not be the best option, because, for example, if the drone falls into a lake, the images will be lost. However, with the possibility of recording in the cloud automatically by Amazon IVS, the footage is saved in a decentralized way and can be easily retrieved.
Although AWS IVS has several positives in its favor, according to Gaessler (2022), it was discovered during development and testing that DJI (drone) provided live streaming support only for RTMP protocol URLs, which made the AWS IVS is incompatible for the purpose of the experiment, since such a tool operates through the secure RTMPS protocol. That way, streaming to it directly from the drone could not be performed. (Tommy Gaessler, 2022).

That said, in order to reach the ultimate goal of real-time transmission of drone images, we sought to combine the Restream tool with the use of AWS IVS. This lives platform was used as a bridge between the RTMP protocol and the RTMPS protocol. After that, it became possible to transmit from the drone to the Restream and then from the Restream to the IVS, as shown in Figure 5, where DJI refers to the drone, which sends its live stream to Restream, and from there the sending is made from Restream to IVS.

Figure 5 - Configuration Architecture between Software
Source: Tommy Gaessler - Notion

3.3 Trackimo

Trackimo's 3G GPS Drone Tracker is a small smart tracking device that keeps drones safe and ensures their speedy recovery. It works all over the world, indoors and outdoors (Trackimo, 2022). Such a device provides accurate location tracking via the Trackimo app or website and is particularly useful because it uses Wi-Fi, GPS and 3G GSM Cellular technology to acquire very accurate and consistent positioning data. According to the documentation provided by the company, it is important to follow some steps for the best use of the device. First, the device must have its battery charged, since when it is unpacked for the first time it will be discharged. To do this, just follow a few steps:

- Install the battery by removing the back cover and inserting the battery. To remove the back cover, gently push it in the middle and slide it out.
- To charge, connect one end of the data cable to the charger port on the bottom of the device and the other end to a USB power adapter.
- Then connect the USB adapter to an electrical outlet. The device must be charged for 12 hours.
- After charging it is recommended that the device receives its first GPS signal before activating it. To do this, the device must be placed in an open area with strong cellular service and a clear, unobstructed view of the southwest sky (satellite location). Wait at least 15 minutes. At the end of this step, it will be ready to be configured.
- To configure it is very simple:
- Activate the Trackimo GPS drone tracking device by registering the device on the Trackimo website, iOS or Android app.

This is done as follows:

1. Power on the device by holding down the red button on the front for 3-4 seconds.
2. Create an account at www.trackimo.com, press "Activate Device" to start the activation process.
3. Identify Trackimo's "Device ID". This is a 7-digit number located on the inside of the Trackimo under the battery and printed on the packaging. Enter this number in "Device ID", as shown in Figure 6.

Figure 6 - Screen to enter device id
Source: Trackimo - User Guide

4. After entering the device ID, the system will check the connectivity of Trackimo to the GSM network. This may take a few minutes. If the device is not connected to the GSM network, you will be asked to take a few short steps and try the connection again.

5. Once this is done, the system needs to verify that the device is really in the possession of whoever is configuring it. This is accomplished by physically associating such a device with the user's account. To do so, you must follow the steps on the website screen, as shown in figure 7, and click on the SOS button on the device to associate it with the account.

Figure 7 - Pairing Stage
Source: Trackimo - User Guide

6. The payment stage is reached. The Trackimo device includes a 12 month prepaid tracking subscription and the user is not required to enter payment information at this time.

7. Finally, we arrive at the success message that completes the device configuration, as shown in figure 8. And so, it is ready to use. In this final step, the user can still provide a nickname for their device and (optionally) enter the phone number to receive alerts and notifications directly on their phone.

- After setup in software, Trackimo GPS drone tracking device must be connected to drone with specially designed drone accessory.

4. Results

During the development of the options chosen in the project (Gaessler, 2022), it was noted that the Amazon IVS facilitated the real-time monitoring of the drone, which favors tracking and allows quick action to be taken to avoid route deviation. by the drone, ensuring its integrity. It was noted that this tool had several positives in its favor, mainly due to the fact that it allows a live video stream to be done effortlessly and set up in an instant. This is possible because Amazon IVS eliminates the cost and complexity of configuring live video streams. A transmission key is provided, this is sent to the ingestion point of an encryption software. Then a playback URL is generated. Such a URL is used with the IVS player SDK and the live stream is ready to be seen across the global network.

Another point noted by Gaessler was the quality of the stream, as the IVS has an ultra-low latency, which makes it possible for the delay from when a camera captures a live stream to when the stream appears on a viewer's screen to be minimized. Low latency is a critical component in building good interactive user experiences that enrich the audience experience. Compared to other types of latency present in streaming tools, Amazon IVS stands out as it can deliver video with a latency of less than five seconds. In a traditional Over-The-Top (OTT) stream, on the other hand, latency can be as high as 30 seconds.

With this, the ease of configuration and use of the tool proved to be a positive point for real-time monitoring of the drone, which gives the user the expectation of guaranteeing the integrity of the route that he defined for the drone to travel.

Regarding the Trackimo tool, the app and website were found to provide excellent functionality of setting up an area that works as a geofence. This feature allows you to activate an alert whenever the device leaves a designated area. When zooming out, it was possible to observe the entire area configured for tracking on the map (Lukacher, 2017). In addition, through the application or website, it was possible to configure the tracking period or the drone's position alert, which can be from 1 minute to 1 hour. It was also possible to select the route history and its tracking, which made it possible to see several waypoints, which are basically the paths the drone took. What made the tool very valuable was realizing that as the drone moves, it locates vectors on the map, which are possible to follow through the Trackimo website or app (Lukacher, 2017).

Due to its many useful functions, Trackimo has proved to be an excellent option for those who do not want to lose their precious drone in any way. With a combination of the 3 tools listed in the study, one can certainly achieve a good protection factor, as one complements the other. In this way, it is possible to satisfactorily minimize the complete loss of a drone in a probable attempt to deviate from the route or even an accident.

5. Conclusion

In short, the present study aimed to analyze and understand the vulnerabilities present in drones and seek ways to maintain the integrity of the route defined in the flight plan. To ensure the permanence of the chosen path for the drone, based on articles and research on the subject and considering its proper tools, functionalities and usability, three specific tools were defined for the study.

About Amazon IVS, it was noted that it brought many positive points to the research in terms of functionality, collaborating with the storage of captured images in a safe place, which minimizes data deviation, and providing tools for real-time monitoring. of the drone, with the differential of having an ultra-low latency. Restream takes center stage when it comes to multi-environment deployment. This tool, like Amazon IVS, is ideal for real-time transmissions of drone images and helps to complement it. When it comes to georeferencing, Trackimo stands out for allowing you to configure tracking by geographic area, give alerts when the drone leaves the defined area, get updates every minute about the drone's movement with various waypoints that bring great detailing of the coordinates, among other features listed in the documentation. Such a tool proved to be essential when we are talking about safety in the path of a drone.

Regarding future research, it is suggested to improve cloud drone image processing and the tools associated with image generation processing. In this context, the use of these resources and tools allows the user to accomplish his goal more quickly and efficiently.

6. Acknowledgement

To the Metropolitan University of Manaus - FAMETRO, the Academic Coordination for the support and assistance in the development of teaching and research.

7. References

ABDELMABOUD, Abdelzahir. The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends. Sensors, v. 21, n. 17, p. 5718, 2021.

ALMIR AURÉLIO DAMBROSKI et al. ESTUDO COMPARATIVO DE FERRAMENTAS DE SOFTWARE PARA PROCESSAMENTO DE DADOS GEORREFERENCIADOS OBTIDOS A PARTIR DE VANTS. Revista Prociências, v. 4, n. 1, p. 54–68, 2021.

GIL, A. C. Como elaborar projetos de pesquisa. 4. ed. - São Paulo: Atlas, 2002 .

How Can Drones Be Hacked? [Complete Guide]. Drone Tech Planet, 2019. Disponível em: https://www.dronetechplanet.com/how-can-drones-be-hacked-complete-guide/. Acesso em: 02 de mar. de 2022.

Lukacher, Joel.Trackimo GPS Drone Tracker Review by LikeTECH. Youtube, 7 jul. 2017. 1 vídeo (5 min). Disponível em: https://www.youtube.com/watch?v=t_bmRWqQBnw. Acesso em: 11 de maio de 2022.

MARTINS, Samuel. Drones: o que são, como funcionam e como voam. Belo Horizonte, 16 out. 2020. Disponível em: https://blog.eletrogate.com/drones-o-que-sao-como-funcionam-e-como-voam/. Acesso em: 28 de fev. de 2022.

YAACOUB, Jean-Paul et al. Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, v. 11, p. 100218, 2020.