Int. J. Adv. Eng. Pure Sci. 2024, 36(3): <211-223>
DOI: 10.7240/jeps.1459595

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

An Implementation-Based Study of the Detection of and Recovery from GPS Spoofing Attacks for Unmanned Aerial Vehicles

Lina AL-SOUFI [1], Talha DEMIRSOY [1], Ece GELAL SOYAK [2]

[1]*Bahcesehir University, Faculty of Engineering and Natural Sciences, Cyber Security, Istanbul, Turkey*

[2]*Bahcesehir University, Faculty of Engineering and Natural Sciences, Computer Engineering, Istanbul, Turkey*

Abstract
Unmanned Aerial Vehicles (UAV) are expected to be a critical component for logistics, agriculture, defense and enabling connectivity for post-5G communications. The utilization of drones in diverse sectors raises concerns about their vulnerability to potential attacks that disrupt or obstruct their operational mechanisms. In this work, we first demonstrate how navigation attacks can compromise a drone's system, using GPS jamming and spoofing attacks via HackRF One PortaPack Software Defined Radio (SDR) device. Next, we propose a mechanism called "Return-to-Start", which can protect a drone from loss by responding promptly to such widely spread navigational attacks. We evaluate the effectiveness of our solution through experiments on a Raspberry Pi-based drone we developed. Our experiments validate the robustness of Return-to-Start functionality in a variety of attack scenarios with different durations and GPS geolocations.
Keywords: Drone, UAV, GPS spoofing, GPS jamming, Software Defined Radio (SDR)

I. INTRODUCTION

Drones, also known as unmanned aerial vehicles (UAVs), will fly in urban airspaces in the coming decade(s). Their ability to capture footage or data from unique perspectives, as well as their increasing autonomy and precision, make them valuable tools in civilian applications such as agriculture, construction, delivery, surveillance, and search and rescue. UAVs are also employed in military operations; tactical drones, also known as medium-altitude long endurance drones (MALE) are used for reconnaissance and combat. Additionally, the ongoing research in post-5G vertical heterogeneous networks envision UAV base stations and relays to handle communication requirements and provide edge intelligence [1].

A critical component for using UAVs in such long range and long duration applications is being equipped with a sensor core comprising the Inertial Measurement Unit (IMU) and a Global Positioning System (GPS) system, which are integrated to calculate the moving drone's position, velocity, and altitude. The IMU and GPS are generally integrated to create a sensor fusion system, allowing the drone to benefit from both short-term reliable accuracy of the IMU and the absolute positioning information provided by GPS. This integrated approach enhances overall navigation accuracy and reliability, especially in scenarios where GPS signals may be temporarily lost or degraded.

As drones gain wide use in both civilian and military contexts, the threat of malicious activities directed towards these systems becomes increasingly terrifying. The impact of such attacks on under-prepared UAVs could result in theft, property damage, or injury/death of bystanders. Several attack vectors have even been proven successful in the field [2]. Among the critical attacks on UAVs is GPS spoofing. One of the most serious UAV security attacks was the capture of the US RQ-170 military UAV in 2011 [3]; another incident happened where a drone with radioactive material landing on the roof of the private residence of the Japanese prime minister [4]. For safety and privacy protection, some government regulators have encouraged drone manufacturers to build geo-fencing constraints into UAV navigation systems that would override the commands of the unsophisticated operator,

Sorumlu Yazar: ECE GELAL SOYAK, **Tel:** 0212 381 5709, **E-posta:** ece.gelalsoyak@bau.edu.tr
Gönderilme: 02.04.2024 **Düzenleme:** 15.06.2024, **Kabul:** 09.07.2024

preventing UAVs from flying into protected airspaces. For example, drone producer DJI currently uses geo-fencing to prevent its drones from operating in the Washington D.C. area and nearby airports. Given how vulnerable GPS and other Global Navigation Satellite System (GNSS) are to jamming and spoofing attacks, an increasing focus has surfaced on designing UAV navigation and control systems that can operate in GNSS- denying environments. Unlike military UAVs' GPS signals, which are encrypted and cannot be modified [5], civil UAVs use civil signals that are unencrypted, unauthenticated, and predictable, allowing a user to produce or modify signals at will. As a result, tampering with them and using fake or false signals could alter and influence the movement of the civil UAV, steering it to an undesired target site [6].

This paper explores the extent of UAV vulnerability to signal blockage and fake GPS signals as a result of jamming and spoofing attacks. We have implemented a Raspberry Pi based drone, Tale, with a mechanism that allows it to fly and return to start position without relying on GPS when it is jammed. We have conducted field experiments on two test subjects, Tale and an a commercially available off-the-shelf drone, validating Tale's mechanism of recovery from GPS spoofing attacks, and we discussed the results. The main contributions of this work are summarized as follows:

- Developing GPS jamming and spoofing attacks to target UAV GPS receivers, showcasing the validity of the vulnerability,
- Developing a unique Raspberry Pi drone,
- Implementing the original Return-to-Start point function that can prevent and protect a drone from loss,
- Conducting field experiments to examine the effectiveness of the proposed approach in detecting and recovering from GPS jamming and spoofing attacks, and
- Promoting awareness among the public, the scientific community, and manufacturers that professional UAV systems should integrate a higher degree of security by proving the potential of such attacks and proposing a viable solution.

The rest of the paper is organized as follows: Section II presents background on drone classification, types, usage, communication method, the GPS mechanism, and GPS attacks. Section III summarizes related prior art. Section IV presents the hardware and software utilized and the solution approach. Section V describes the conducted experiments and discusses their results. Finally, Section VI concludes the paper and discusses possible future work.

II. BACKGROUND

We provide brief background on the systems enabling drone navigation, and we describe known navigational attack strategies.

2.1. Drone Navigation

UAVs need accurate navigation to operate autonomously or semi-autonomously and fly long distances. The Inertial Measurement Unit (IMU) in drones plays a crucial role in navigation, stability, and control. It typically consists of sensors like accelerometers and gyroscopes that measure the drone's acceleration and rotation rates. The IMU provides essential data to the flight controller, helping the drone maintain its orientation and stability in the air. By continuously monitoring changes in velocity and rotation, the IMU enables the drone to make real-time adjustments to its motors and control surfaces, ensuring precise and stable flight. Additionally, the IMU contributes to the drone's ability to navigate accurately, as it helps calculate changes in position over time, allowing for more reliable and autonomous flight operations. In many drone systems, the IMU and GPS are integrated to create a sensor fusion system, which allows the drone to benefit from both short-term reliable accuracy of the IMU and the absolute positioning information provided by GPS. This integrated approach enhances overall navigation accuracy and reliability, especially in scenarios where GPS signals may be temporarily lost or degraded.

The communication between a drone and its controller could take a place in different ways including a direct radio signal or via a Wi-Fi network. Most drones are equipped with a GPS module that enables them to know their location depending on a network of orbiting satellites. GPS location signal, when paired with data from an inertial measurement unit (IMU), gives accurate information that could be used for control purposes. A GPS-equipped UAV may offer both position and altitude information and essential vertical and horizontal coverage levels. In addition, it is always important to be aware of the UAV location, to prevent incidents in an area densely inhabited by other UAVs or manned vehicles. In fact, GPS in UAVs is vital whether the UAV is remote-controlled, autonomous, or semi-autonomous.

GPS is a United States-owned constellation of 31 satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location. It has at least 24 operational satellites that circle the globe once every 12 hours, guaranteeing that users would receive information from at least four satellites from any point on earth. With UAVs, GPS is often critical to safely flying the UAV as it is used as the primary sensor for the localization of

the drone [7]. In normal operation, GPS receivers deduce their position by calculating their distance from several satellites at once. Each satellite carries an atomic clock and broadcasts its location, the time, and a signature pattern of 1,023 plus and minus signs known as a pseudorandom noise code (or PRN code) [8].

GPS drone is also capable of navigation by *waypoints*, where a flight route may be planned by instructing the drone to go to specified GPS locations along with a predefined path using its autopilot mode. GPS also allows a drone to execute a position hold, which enables the drone to retain a stable location point and an altitude hold, which also enables the drone to maintain a set altitude while in flight mode, mapping, and reporting, which allows the drone to keep a record log for each flight.

Autonomous UAVs often depend on a GPS location signal, which, when paired with data from an inertial measurement unit (IMU), gives accurate information that could be used for control purposes. A GPS-equipped UAV may offer both position and altitude information and essential vertical and horizontal coverage levels. GPS navigation algorithms may provide continuous accuracy as long as adequate satellite signals are available during the UAV flight.

2.2. Drone GPS Attacks

2.2.1. GPS Jamming

GPS receivers in drones can be particularly vulnerable to external sources of interference. GPS jamming is one of the major attacks that severely impacts systems' availability. It is performed by transmitting random interfering signals with high strength such that the GPS signals and noise are indistinguishable. As the signal intensity of legitimate GPS signals is very low in nature, generating jamming signals at a higher intensity is relatively easy to achieve [9]. Jamming signals may be generated by simply re-broadcasting the GPS carrier signal, or by broadcasting it upon adding random noise.

Jammers operate against receivers, not transmitters. They can be used to block all wireless communication in a certain area. In open areas, signals from jammers can spread over much longer distances compared to that on land with obstructions. Upon losing the GPS signal, drones can no longer maintain the correct position; they may land or drift in the wind, potentially causing physical damage to people or buildings, or causing sensitive information to be seized by malicious actors.

2.2.2. GPS Spoofing

All cryptographic methods are vulnerable to attacks by specialized systems that can intercept a signal and retransmit it with greater power, thereby causing the receiver to switch from the legitimate signal to the delayed replica [8]. GPS spoofing happens as radio signals conveying fake GPS location information are transmitted, to overpower the relatively weak GPS signals in two main ways. One approach is *meaconing*, where an attacker merely intercepts the legitimate GPS signals and rebroadcasts them on the victim's receiving frequency at a higher power than the original signal confusing the receiving navigation system. Another approach is using a radio transmitter to send what could be described as a *counterfeit (fake) GPS signal*, to manipulate a target receiver's position. The spoofing signals provide the drone with a false impression of its actual physical location, and as a result, the drone diverges from its original route and becomes susceptible to loss.

GPS spoofing poses a bigger threat than GPS jamming, since a spoofer could lead the target to produce an inaccurate PVT (Position, Velocity, Time) solution or even achieve total control over a drone's flight path by re-broadcasting or transmitting fake GPS signals.

III. RELATED WORK

In this section we present related prior work on causing and detection of GPS jamming and spoofing attacks on UAVs, and related work that studied UAV behavior postattack.

3.1. Previous Work on Creating Spoofing

Due to the decrease in hardware expenses and the availability of open-source software, unmanned aerial vehicles (UAVs) have gained accessibility over the last decade; this also contributed to their misuse. To assess the impact of attacks, several research efforts aimed to put spoofing attacks into good use, such as protecting the different GEO zones from malicious drones by means of neutralizing, taking down, or rerouting a drone [10], [11]. As an example, [12] presents a GPS spoofing based counter-UAV defense system that can remotely control a non-cooperating UAV to fly to a specified location for capture.

In recent years there has been a growing interest in the use of multiple drones, which coordinately move as a swarm, for covering a wide area in disaster management, traffic control, etc. applications. The study of spoofing a drone swarm using spatial spoofing has been proposed [13]. The idea in this work is, instead of tracking the movement of each drone and transmitting an individual spoofing signal per drone, estimating a fake position for each point where drones move. A technique for grounding violating drones and computing their launch location has been proposed in [14]. More recently, a Drone Position Manipulation (DPM) system that exploits the entire stack of sensing, state estimation, and navigation control have been proposed [15].

3.2. Previous Work on Detecting Spoofing

Ideally, in order to detect detect whether a drone has been hijacked, the acceleration and angular velocity reported by motion sensors can be compared with the position reported by GPS. However, since the position estimation via motion sensors may be inaccurate due to error accumulation over time, a method that estimates linear acceleration has been proposed [16]. The proposed method has been implemented on a Quadrotor drone, showing that the false-positive cases that happened with the straightforward comparison of the inertial navigation system with the GPS have been eliminated.

Another probabilistic algorithm to detect Global Navigation Satellite System (GNSS) spoofing attacks was proposed in [17]. The proposed integrity monitoring procedure was implemented using a small-sized antenna array and it utilizes Angle of Arrival (AoA) integrity-monitoring method. Other techniques utilizing the difference in the signal strengths of authentic GPS and spoofing signals, detecting the presence (or absence) of background noise, using radar ground stations that track UAV's perceived position information find outliers have also been proposed [18].

More recently, machine learning techniques have been used for detecting spoofing. [19] used several learning algorithms on signal features such as jitter, shimmer and modulation variants. [20] compared several tree-based machine learning models and [21] compared three ensemble models (Bagging, Stacking, and Boosting) in terms of accuracy of detecting GPS spoofing attacks.

3.3. Previous Work on Recovery from GPS Spoofing Attacks

Given the extent of how vulnerable the GPS and other GNSS are to signal jamming and spoofing attacks, and the potential damage to the environment, an increased focus on designing a UAV navigation and control system that can function in GNSS-denied environments has surfaced [22], [23].

In one previous work, the authors proposed to detect GPS spoofing based on the monocular camera and IMU sensor of a UAV, and then presented an image localization approach to support UAV's autonomous return using error reduction via computer vision [24]. The performance of the proposed mechanism was evaluated on a DJI Phantom 4 drone.

Another work for attack resilience was carried out in [25], where the authors proposed an information-sharing path planning algorithm for drone swarms, where drones collaboratively, step-by-step identify waypoints using geocaching and construct a path by sharing the information. The algorithm is implemented over OMNeT++ and GNSSim, which allow building network simulations including GPS jamming and spoofing attacks.

Focusing on safety and security of UAVs, a resilient architecture for UAVs for dynamically managing the network even when subjected to an attack during a mission was proposed in [26]. The behavior of the proposed scheme is analyzed in two case studies, one involving a motor failure and the other involving a GPS spoofing attack. More recently, a mechanism utilizing smart contracts and Blockchain to render the drone network more resilient against attacks was proposed [27].

IV. SYSTEM DESIGN

In this section, we first describe the system setup used in creating the GPS attacks. Next, we explain the architecture and capabilities of our custom drone, "Tale".

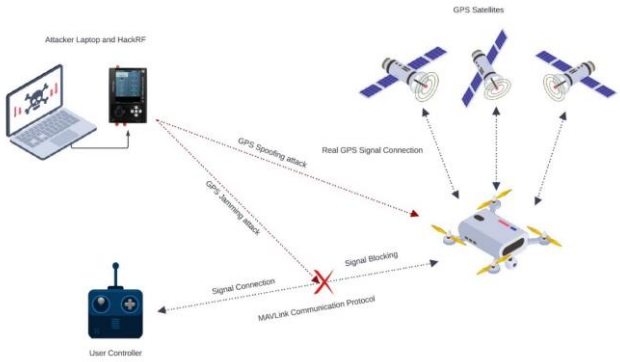

Figure 1. Overview of the drone GPS attack setup

4.1. Attack Design

As the drone relies on GPS for coordinate acquisition and control, it is possible to take over the drone with fake signals, guiding it towards a desired location. For this, the drone must lose connection to GPS signals and instead focus on a manipulated signal resembling the original GPS signal.

RF software-defined radios (SDR) can be configured to broadcast manipulated GPS signals. Our attack setup uses HackRF One, an open source SDR platform that covers the frequency spectrum of GPS transmissions. In our experiments, HackRF with the PortaPack companion has been used, to facilitate mobility. In addition, Mayhem firmware has been used with HackRF for investigating the signal flow and signal continuity on regular and irregular GPS signals. GUI-based attack implementation (using SigintOS) and command line-based attack implementation using GPSSDR-SIM [28] were performed; the former is used for viewing the trajectory and the latter is used for analyzing the signals. The setup for the GPS attacks is shown in Figure 1.

4.1.1. GPS Jamming Attack

This attack is aimed at blocking the GPS communication on the drone by drowning the GPS signals by the jamming signals, causing the operator to completely lose control over the drone, and potentially forcing the drone to land. An effective jamming attack is achieved by reducing the Signal-to-Noise-plus-Jamming Ratio (SNJR) of the target signal, to ensure that the target signal cannot be captured at the receiver. To achieve this, we increase the jamming signal strength to exceed the strength of the satellite signal on the drone. We assume that the signal strength of the GPS signals received by the drone in flight and the attacker on the ground (SDR device) are similar due to the proximity of jammers and receivers [31].

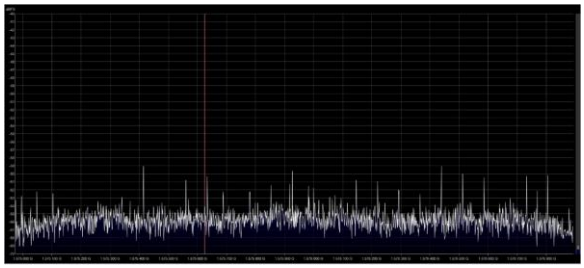

Figure 2. GPS jamming attack signal analysis. The peaks show the effect of noise generated by the attack

To generate the GPS jamming attack, we used the SigintOS to generate signals with 300 MHz bandwidth at 1.2-1.5 GHz frequency; the generated signals were transferred to HackRF over a USB connection. On the HackRF, signal was transmitted with an initial transmission power, and in a feedback loop the power of the signals were gradually increased until the receiver locked onto these new signals, causing the drone to begin its landing process. Figure 2 depicts the signal during the GPS jamming attack captured using SDRSharp software, where the peaks show the effect of noise generated by the attack. A flowchart of the attack generation and the drone behavior during the GPS jamming attack is illustrated in Figure 3.

Another critical condition in the success of a jamming attack is timing, *i.e.*, when and for how long is the exposure to jamming signal observed. There are different jamming types in the literature; two of them have been considered in this work, namely *constant jamming* and *periodic pulse jamming* attacks. With *constant jamming*, the jammer broadcasts a powerful signal continuously, to completely block the target device's packet reception. With *random* jamming, a jammer generates signals for random periods and turns to sleep for the rest of the time. *Periodic pulse jamming* is a variant of *random* jamming, with jamming and sleeping cycles alternating periodically. While the continuous approach is more effective, it consumes more energy compared to jamming in intervals; we have observed the impact of both approaches on the drones.

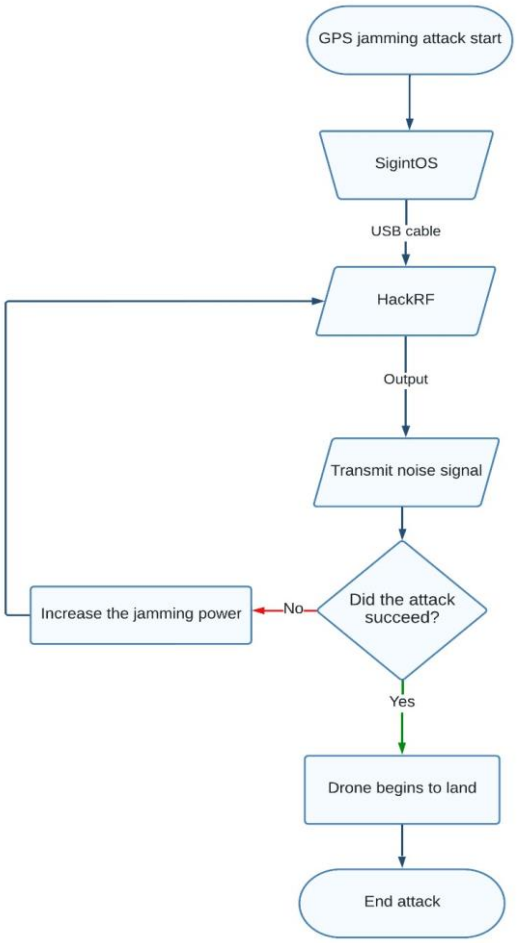

Figure 3. Flow chart depicting the steps of the jamming attack

4.1.2 GPS Spoofing Attack

For this attack, we provide the drone the GPS coordinates of a no-fly zone, *i.e.*, *geofence zone*, to force the drone to land immediately. A no-fly zone is an area of airspace where drones are allowed to fly only with special permits. While the targeted drone is flying, fake GPS signals are transmitted to indicate that the drone has entered a no-fly zone.

In our experiments, the GPS-SDR-SIM software is used by the HackRF device to create a GPS baseband signal stream that could be converted to RF using the SDR platform. The generated GPS broadcast ephemeris indicates the GPS satellite constellation with fake coordinates; this signal can be utilized to define a stationary point or a trajectory.

Different drones may be built and programmed differently; for example, an attack using an authorization zone might land a drone but not another, or some drones may have unlocked some geofence zones. Hence, the experiments are repeated using the coordinates of different geofence zones and permitted

flying areas till the spoofing attack is successful. A detailed flowchart of the attack generation and the drone behavior during the GPS spoofing attack is illustrated in Figure 4.

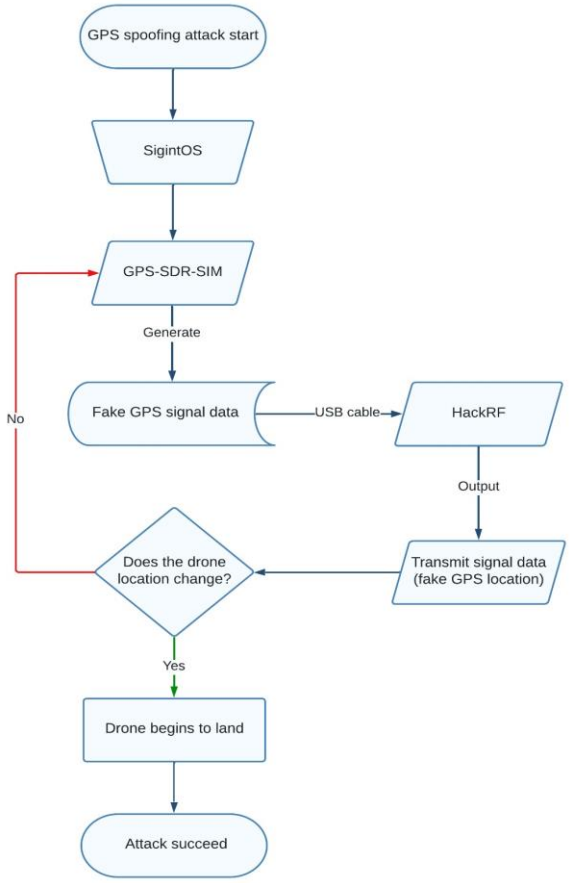

Figure 4. Flow chart depicting the spoofing attack

4.2. The Design of "Tale"

Tale is developed on a drone frame using different electronic cards and components containing Raspberry Pi 4, flight control board, Raspberry Pi 4G/LTE Cellular Modem Kit, and radio telemetry toolkit. The drone core builds on Raspberry Pi 4. From among the open-source autopilot projects (e.g., ArduPilot, Paparazzi UAV, Dronecode, LibrePilot, PX4), PX4 autopilot [29] was chosen since it offers a versatile collection of tools for drone developers and provides easy integration with the other com- ponents in Tale system such as the Ground Control Station (GCS) (*i.e.*, Mission Planner) and the communications protocol. Micro Aerial Vehicle Link (MAVLink) [30] protocol is used for establishing and retaining connection with the Mission Planner. In terms of Flight Control circuit board, Pixhawk PX4 Flight Controller Autopilot PIX 2.4.8 was used on Tale; it serves as a hub for other peripherals such as the GPS module, Radio Telemetry, Raspberry Pi 4G LTE Cellular Modem Kit, and different sensors. A summary of the hardware components of Tale are listed in Table 1 and Figure 5 demonstrates the main hardware components on the physical drone. Tale's software components are summarized in Table 2.

Table 1. Tale Hardware Components Specifications

Hardware	Specification
Raspberry Pi	Ver. 4, 4GB
Flight Control Board	Pixhawk PX4 2.4.8
GPS module	u-blox NEO-M8N, FW SPG 3.01
Radio Telemetry	CUAV P9 Radio Telemetry
Raspberry Pi 4G-LTE Cellular Modem Kit	Sixfab Raspberry Pi 3G/4G & LTE Base HAT

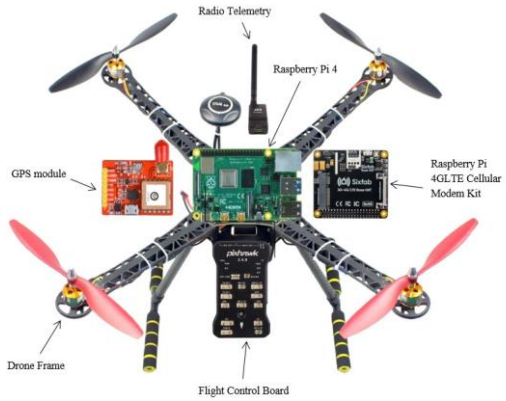

Figure 5. Tale system hardware overview

Table 2. Tale Software Components Specifications

Component	Specification
Raspberry Pi OS	Debian v11, Kernel v5.15
Mission Planner	Ground Control Station v1.3.77
PX4-Autopilot	Flight control solution v1.12.3

For communications, Tale comprises a GPS module as well as a cellular connection. The Sixfab 3G/4G/LTE Base HAT enables the Raspberry Pi to connect to the cellular data network.The CUAV P9 data link communication module is used for radio telemetry; it is compatible with the Pixhawk flight control board and supports long range. The module can operate at a variety of frequencies for 3G and LTE. For GPS, the u-blox NEO-M8N GPS module is used. In addition to yielding high positioning accuracy in urban and rural areas with varying signal strengths, the module also supports GPS signal attack detection. Tale also incorporates a set of sensors, such as LiDAR, gyroscope, accelerometer, and piezoresistive accelerometers. Figure 6 depicts the system architecture of Tale.

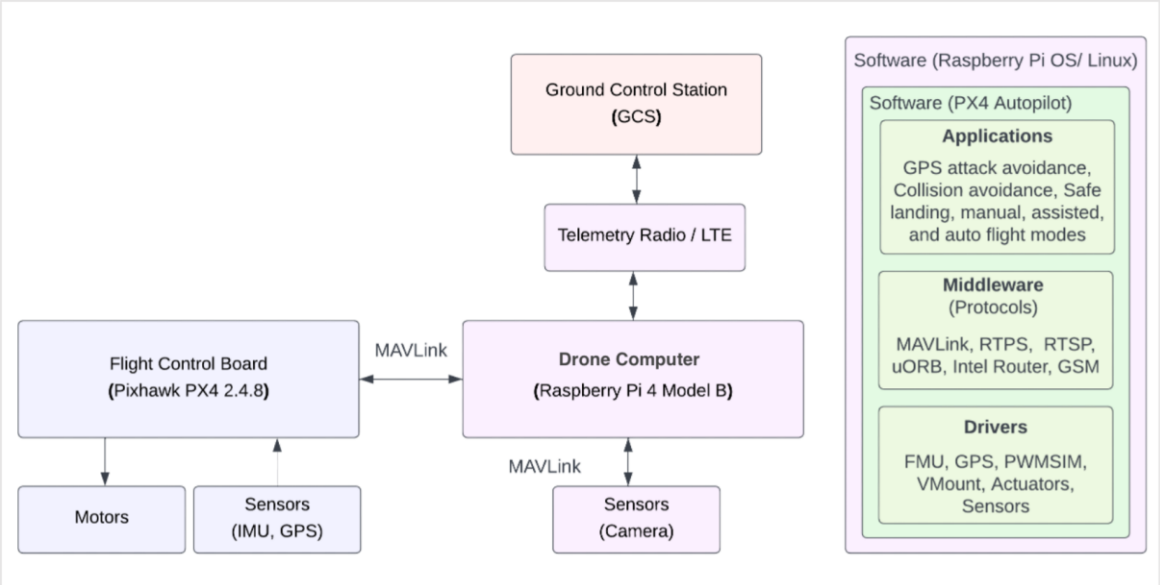

Figure 6. Tale system architecture

4.2.1. Detecting GPS Attacks

On Tale, the detection of GPS spoofing attacks relies on phase delay measurements. The detection thresholds for spoofing are defined. If the phase delay difference between the received GPS signals and the original signal are below the defined threshold, spoofing detection event is raised. The probability of spoofing detection becomes greater when combined with selecting accurate thresholds that are inclusive of potential phase delays. Figure 7 shows the signal during the GPS spoofing attack phase, which was performed using SDRSharp software, where the peak indicates the start of the attack.

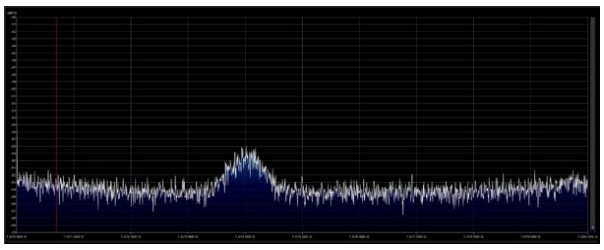

Figure 7. GPS spoofing attack signal analysis on Tale

The effectiveness and reliability of this method have been quantified in terms of the ratio of false alarms and the probability of counterfeit signal detection. False alarm or inaccurate detection may happen in the case of the GPS module receiving physical damage, in the presence of a GPS transmitter and receiver satellite dish nearby, or if the phase delay differences between received legitimate satellite signals are below the specified threshold. Through several experiments, Tale exhibited 99% spoofing detection accuracy when the carrier to noise ratio was at least 43 dBHz. The flowchart of the developed detection method is in Figure 8.

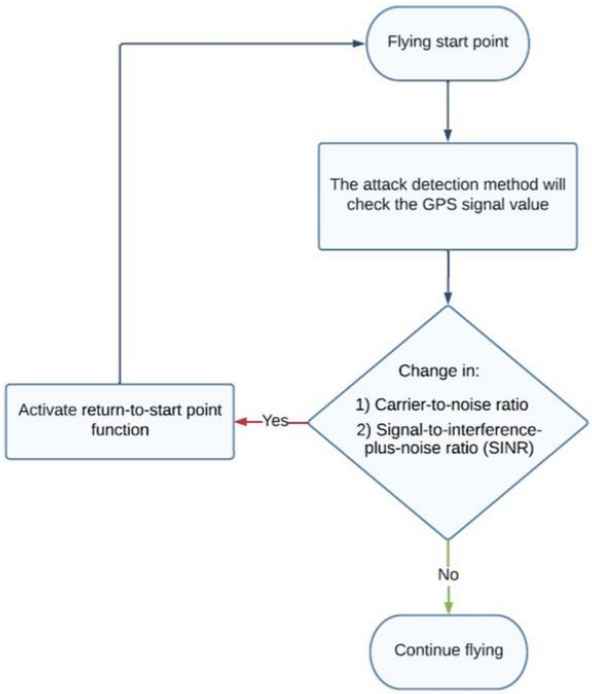

Figure 8. Tale GPS attack detection method flowchart

4.2.2. Return-to-Start Function

As Tale starts flying, it continuously synchronizes the GPS coordinates in real-time and records the distance and direction information acquired via the GPS. Tale records the direction changes at 45◦ and 90◦ angles according to the device orientation and motion. Towards this, Tale benefits from the integration of and the communication between the PX4 autopilot and the ground station Mission Planner. Tale sensors including the GPS work all together to provide the needed data and with the use of the flight control board (PIXHAWK PX4), the latitude, longitude, altitude, the angles

between the waypoints, and the distance between the waypoints are calculated. Tale stores the computed data and communicates it to the Mission Planner. Figure 9 shows a screenshot from Mission Planner, displaying some of the computed data that Tale utilizes in its Return-to-Start function.

Tale's recovery solution depends only on the previously saved data to make its way back to the start point. As soon as a GPS jamming or GPS spoofing attack is detected, Tale disables the GPS function and navigates using the (inverse) directions and distances recorded during the flight. For example, if it flew with 10 m/min south(-z) for 10 minutes, it would fly back with 10 m/min for 10 minutes in the north direction (z) right after disabling the GPS.Using this unique autopilot code, Tale is able to safely reach its starting point independently from any control signals.

The Return-to-Start function depends on the Alternate Angles Theorem, which states that when two parallel lines are cut by a transversal, then the resulting alternate interior angles or alternate exterior angles are congruent. Tale records its flight route using its compass, since relying on the GPS coordinates would be erroneous in case of jamming or spoofing attacks.

V. EXPERIMENTS

We have designed a setup for evaluating the behavior of our custom developed drone, Tale, under GPS jamming and GPS spoofing attacks. To assess the observed behavior, we have performed the same set of experiments on a COTS (commercial off-the-shelf) drone as well, which allowed us to observe and discuss the behavior of both drones under attack. Figure 11(a) shows the drones' planned route for the experiments, in terms of a series of four waypoints described in GPS coordinates.

GPS jamming was performed by signaling the L1 frequency at 1.575.420.000 Hz and L2 frequency at 1.227.600.000 Hz. In the GPS jamming attack experiments, four different attack strategies are applied, with the signals being generated according to the intervals listed in Table 3. The first three types aim to observe the behavior of the devices under test when jamming attacks are launched at different times and for different durations. Some drone types try to re-connect to controller upon regaining GPS connectivity; our experiments were repeated with varying attack and pause times, and we present the three scenarios that present different behaviors. The fourth jamming type transmits the jamming signal for the duration of the attack.

In the spoofing experiments, the coordinates of different geo-zones were specified to the target. We have experimented with fake GPS coordinates representing "permitted zones" (*i.e.,* areas where flying a drone is allowed according to local regulations), "restricted zones" (*i.e.,* areas where drone flights are restricted or subject to specific conditions such as altitude, time of day, or obtaining special permissions from aviation authorities) and specifically "altitude zones" (*i.e.,* areas with restricted flight altitude), and "authorization zones (*i.e.,* areas where drone flights must be explicitly authorized by aviation authorities). In these experiments, the target drones were attacked for 2 minutes, with 15 seconds of attack and 15 seconds of pause duration. During the attack, the victim notices a sudden change in the reported GPS location.

Table 3. GPS Jamming Attack Time Intervals

Jamming Type	Attack Time	Pause Time	Total Observation Duration
Pulsed jamming #1	3 sec.	2 sec.	3 min.
Pulsed jamming #2	5 sec.	5 sec.	3 min.
Pulsed jamming #3	10 sec.	10 sec.	3 min.
Continuous jamming	3 min.	-	3 min.

5.1. GPS Navigation Attacks on Commercial Drone

The first drone used in the experiments is a commercial over the counter UAV. This device was chosen due to being relatively inexpensive and supporting a functionality that enabled it to fly back to the point where it last received a moderately strong GPS signal. The drone relies on the controller to direct its movement. In addition, the drone also relies on data from onboard sensors such as GPS and barometer readings to maintain a steady flight; in these experiments, it was configured to be controlled only via GPS.

	Bu	Delay				Lat	Long	Alt	Frame	Eleme	Ust	Asaç	Grad %	Angle	Mesa	AZ
1	WAYPOINT	0	0	0	0	39,8373307	32,8097865	100	Relative	X			713...	90,0	100,0	38
2	WAYPOINT	0	0	0	0	39,8394028	32,8107601	100	Relative	X			0,0	0,0	244,9	20
3	WAYPOINT	0	0	0	0	39,8401277	32,8101057	0	Relative	X			-10...	-45,6	140,1	325
4	WAYPOINT	0	0	0	0	39,8398764	32,8088397	100	Relative	X			89,6	41,9	149,9	256

Figure 9. Mission Planner data received from Tale drone

5.1.1. GPS Jamming Experiments

In the first experiment (*i.e.*, pulsed jamming #3), a periodic GPS jamming attack was initiated, with jamming signal transmission for 3 seconds and pausing for 2 seconds, repeating for a total duration of 3 minutes. During the 3-second interval where the jamming signal was transmitted, the connection between the drone and the GPS controller was blocked, and the drone remained to hover stable since it lost its communication. During the 2-seconds intervals where the attack was stopped, it was observed that the drone continuously sought to reconnect with the controller, intermittently succeeding and failing. Within this attack-paused interval when the drone reconnected to its controller, the user was able to move the drone, but it instantly stopped again with the next attack interval.

A similar pattern was observed in the second experiment (*i.e.*, pulsed jamming #3), where it was observed that the drone stopped its flight movement and remained to hover stably for 5 seconds, then regaining connection with the controller when the attack was paused where the flight movement could resume until it was re-attacked. It was observed that the drone was able to successfully reconnect to the controller approximately 2.5 seconds after the attack was paused; thus, while the connectivity was intermittent in experiment #1, it always succeeded in experiment #2.

In the third experiment (pulsed jamming #3), the behavior changed as the jamming attack duration was longer (10 seconds). This time the drone landed in the area it was in within the 10-second attack interval, then re-connecting to its controller in the pause interval and taking off to continue flying again, until the next attack period.

Finally, in the fourth experiment, after the jamming attack that started and continued without stopping, the drone landed in the area it was in, and did not fly again as it completely lost its communication signal.

5.1.2. GPS Spoofing Experiments

Upon losing GPS connection, this drone is able to resume flight once it reconnects to GPS; hence, GPS spoofing attack has been repeated in three different experiments to assess behavior with different attack durations.

In the first experiment, the GPS spoofing attack was launched by transmitting fake GPS coordinates for a *Permitted* flying area for 15 seconds, and as a result, the drone could not be controlled by its user for the duration of the attack. After the 15-second interval, it was observed that the drone control resumed normally.

In the second experiment, the GPS coordinates for an *Authorization Zone* were transmitted. As a response, a warning was prompted to the user to control the drone to leave the area within 30 seconds. For the duration of 15 seconds of attack time, communication could not be established between the user and the drone, but as soon as the attack stopped, for the following 15 seconds the communication was re-established, and the drone was allowed to leave the area.

In the third experiment, a *Restricted Zone* fake GPS coordinates were transmitted during the attack. As a result, a 15 seconds of signal communication was lost again, and when the attack ended the communication was re-established with the drone, and control was restored.

Several repetitions of these experiments demonstrated that this drone always landed upon experiencing a spoofing attack. A capture retrieved from its user application (Figure 10(a)) shows the real location of the drone, before any attack occurred, demonstrating the change of drone location due to the GPS spoofing attack in the second phase of the experiment, more precisely, it shows how the fake GPS signals manipulate a target receiver's position during the attack time (Figure 10(b)).

As we mentioned, the selected commercial drone was in fact potentially capable of moving to the *last known good* location. Our experiments showed that this feature relies on GPS coordinates to complete. This renders the drone vulnerable to being damaged or captured, shall it lose its GPS connectivity upon a malicious attack that transmits wrong coordinates for 10 seconds or more.

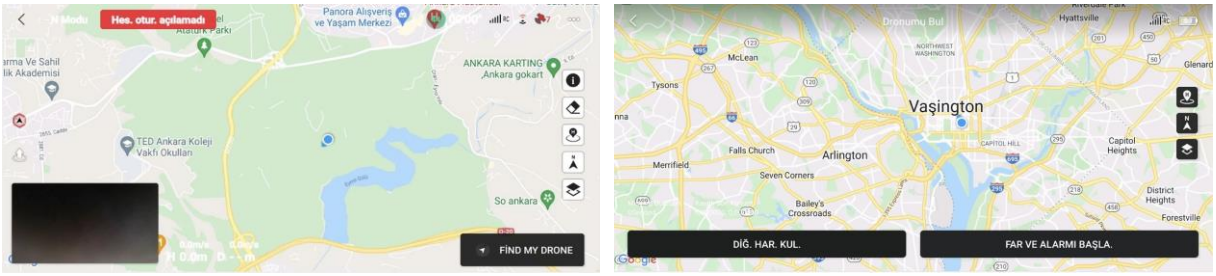

Figure 10. The actual and spoofed locations with the commercial drone

Figure 11. The planned drone flight route using Mission Planner, and the route that was followed with Return-to-Start functionality

5.2. GPS Navigation Attacks on Tale

In the following, we explain how Tale performed under both attack scenarios; and in particular, we validate the performance of Return-to-Start functionality.

5.2.1. GPS Jamming Experiments

The same four set of jamming experiments (as listed in Table 3) have been repeated on Tale.

For the first experiment, the plan was to repeat the same scenario of initiating a GPS jamming attack every 3 seconds and stopping for 2 seconds, repeatedly for a total of 3 minutes. However, the drone signal was almost immediately cut when it received the attack. Even after the attack stopped, Tale could not regain its communication signal with its user. The drone returned to the flying position from where it started, confirming the successful execution of the Return-to-Start function.

Similarly, in both the second experiment (jamming for 5 seconds and pausing for 5 seconds, for a total of 3 minutes) and the third experiment (jamming for 5 seconds and pausing for 5 seconds, for a total of 3 minutes), Tale could not regain connection to its user and successfully returned to the flying start position using the Return-to-Start function.

In the fourth experiment, after the continuous jamming attack was launched, Tale once again lost its communication signal with its user and flew right back to the starting position. Figure 11(b) shows how Tale reacted to the GPS jamming attack using the Return-to-Start function.

5.2.2. GPS Spoofing Experiments

In these experiments, fake GPS signals corresponding to different GEO zones such as Restricted Zones, Altitude Zones, and Authorization Zones were transmitted in the launched attack.

First, the GPS spoofing attack was started by transmitting fake GPS coordinates for a *Permitted* flying area. Tale drone lost the GPS signal in its first seconds and consequently, stopped all connections with the user controller. Tale returned to its start location according to the Return-to-Start function, following the inverse path from the moment it received the attack.

In the next experiment, the fake GPS attack location was established to be an *Authorization Zone*. The communication signal was abruptly cut, and the drone returned to the initial position as in the first experiment.

Finally, *Restricted Zone* GPS coordinates were transmitted in the fake GPS attack. As was observed in the previous experiments, the signal was disconnected without warning and the drone returned to the point it started flying from.

5.3. Observations

We summarize our observations on the responses of the two drones to GPS navigational attacks and highlight the benefits of Tale's Return-to-Start function.

The same implementations of GPS jamming and GPS spoofing attacks were repeated on both devices. Overall, the drones were affected from the attacks in different ways. When the GPS jamming attack was performed in periodic pulses in the first three experiments on the COTS drone, the drone was temporarily able to restore communication with its controller and resume flight towards the last known good location, until it was attacked again. With the continuous attack, as the drone did not have GPS connectivity, it landed where it was attacked. On the other hand, Tale was affected similarly from both continuous jamming and periodic pulse based jamming attacks. Differing from the COTS drone, the communication between the controller and the drone would not be restored when the attack stopped. In both cases, Tale blocked the connection as soon as it detected an attack, and it continued its flight using the Return-to-Start function. Hence, the number of the received attacks did not make a difference for Tale.

When a GPS spoofing attack occurs and the fake GPS signals reach a drone, the GPS location appears as if the drone is in a Restricted Zone, an Altitude Zone, or an Authorization Zone. The geolocation fields in the COTS drone software prevent it from flying in those GEO zones, mostly giving a short warning, or forcing it to land at its current location. However, since those GEO zones are not specified in the software of the Tale drone, it perceives the GPS spoofing attack as an abnormal signal change, leading the Tale drone to return to the point of departure by turning off the GPS module and only depending on its Return-to-Start function to navigate. This feature offers the drone a way to recover from jamming or spoofing attacks.

It was observed that the Tale drone reacted identically to the attacks with different GEO zones. At the same time, it was made clear that at the time of an attack, Tale would lose its control signal with its user and would cease to connect again, until completing its way back to the starting position only relying on the built-in Return-to-Start function.

No matter what type of navigational attack Tale received, when responding to one, it returned to the point of departure without using signal communication, solely depending on its Return-to-Start functionality. Tale drone was able to detect and recover from the GPS signal attacks, ultimately evading being captured. Table 4 summarizes the differences between the two experiments and how each drone reacted to the GPS navigational attacks.

VI. CONCLUSION

Unmanned Aerial Vehicles (UAVs) or drones find an increasing number of use cases in communications, surveillance, delivery, agriculture and airborne fog computing systems. The continuous functionality and mobility of drones are critical in each of these scenarios; unfortunately, GPS navigational attacks on such drones are rather easy to achieve.

In this work, we implemented GPS navigation attacks on a commercially available drone and a custom drone named Tale that was developed to counter the effect of navigational attacks with its recovery mechanism. Tale solution design ensures that the drone recovers from GPS jamming and spoofing attacks, alleviating vulnerability against property theft and privacy violation. Two distinct types of signal attacks have been designed, and related experiments have been conducted, demonstrated, and analyzed on these two drones. The attack framework was mainly created and performed to assess the drones' reaction and how they behave in critical conditions such as signal blockage. To bring things together, and upon analyzing the facts, a comparison between the two drones against GPS attacks was conducted and presented.

This paper aims to contribute to the growing body of research addressing the critical issue of drone security by experimentally analyzing the detection of and recovery from spoofing attacks. As drones become increasingly integral to our daily lives, safeguarding their operation from adversarial interventions becomes imperative, underscoring the urgency and relevance of our investigation in the face of emerging security threats.

Table 4. Summary of Comparison Between the Two Drones That Were Tested

Comparison Points	COTS Drone	Tale Drone
GPS spoofing attack	Forced to land	Evaded landing
GPS jamming attack	Forced to land	Evaded landing
Landing	Yes	No
Attack detection	Yes	Yes
Recovery possibility	Low	High
Return-To-Start function	-	Activated in response to attacks
GPS related vulnerability	Depends on GPS connection; vulnerable to GPS attacks.	-
GPS communication in flight mode	Yes	Yes
GPS communication when returning to start point or last good coordinates	Yes	No
Possibility of returning to start	Low	High

There are two limitations of this study that provides an opportunity for future work: First, currently Tale cuts off its communication signal upon inferring an attack, and no signal can reach the drone until it goes back to the starting point, even if the threat has passed. Second, if the battery is not enough for the returning distance, the drone will have to force land or fall since it exhausts its battery on the return path. Future improvements can include estimating the distance that can be traveled with the remaining battery and warning the user to land at a waypoint on the return path before reaching the start location if the battery is insufficient to fly the drone back to the start location.

ACKNOWLEDGEMENT

This study was performed within the scope of graduate thesis (ID 753606) in Bahcesehir University [32].

REFERENCES

[1] Kurt, G. K., Khoshkholgh, M. G., Alfattani, S., Ibrahim, A., Darwish, T. S., Alam, M. S., ... & Yongacoglu, A. (2021). A vision and framework for the high altitude platform station (HAPS) networks of the future. *IEEE Communications Surveys & Tutorials*, *23*(2), 729-779.

[2] Altawy, R., & Youssef, A. M. (2016). Security, privacy, and safety aspects of civilian drones: A survey. *ACM Transactions on Cyber-Physical Systems*, *1*(2), 1-25.

[3] Iran–U.S. RQ-170 incident. (2024, June 7). In *Wikipedia*. https://en.wikipedia.org/wiki/Iran–U.S._RQ-170_incident

[4] Sturdivant, R. L., & Chong, E. K. (2017). Systems engineering baseline concept of a multispectral drone detection solution for airports. *IEEE Access*, *5*, 7123-7138.

[5] Spilker Jr, J. J., Axelrad, P., Parkinson, B. W., & Enge, P. (Eds.). (1996). *Global Positioning System: Theory and Applications, volume I*. American Institute of Aeronautics and Astronautics.

[6] Seo, S. H., Lee, B. H., Im, S. H., & Jee, G. I. (2015). Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal. *Journal of Positioning, Navigation, and Timing*, *4*(2), 57-65.

[7] Courbon, J., Mezouar, Y., Guénard, N., & Martinet, P. (2010). Vision-based navigation of unmanned aerial vehicles. *Control engineering practice*, *18*(7), 789-799.

[8] Psiaki, M. L., Humphreys, T. E., & Stauffer, B. (2016). Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies. *IEEE Spectrum*, *53*(8), 26-53.

[9] Purwar, A., Joshi, D., & Chaubey, V. K. (2016). GPS signal jamming and anti-jamming strategy—A theoretical analysis. In *2016 IEEE Annual India Conference (INDICON)* (pp. 1-6).

[10] Gaspar, J., Ferreira, R., Sebastião, P., & Souto, N. (2018). Capture of UAVs through GPS spoofing. In *2018 Global Wireless Summit (GWS)* (pp. 21-26).

[11] Shijith, N., Poornachandran, P., Sujadevi, V. G., & Dharmana, M. M. (2017). Spoofing technique to counterfeit the GPS receiver on a drone. In *2017 International Conference on Technological Advancements in Power and Energy (TAP Energy)* (pp. 1-3).

[12] He, D., Qiao, Y., Chen, S., Du, X., Chen, W., Zhu, S., & Guizani, M. (2018). A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles. *IEEE Network*, *33*(2), 146-151.

[13] Ceccato, M., Formaggio, F., & Tomasin, S. (2020). Spatial GNSS spoofing against drone swarms with multiple antennas and Wiener filter. *IEEE Transactions on Signal Processing*, *68*, 5782-5794.

[14] Alamleh, H., & Roy, N. (2021, April). Manipulating GPS signals to determine the launch location of drones in rescue mode. In *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)* (pp. 1-5).

[15] Chen, W., Dong, Y., & Duan, Z. (2022, January). Accurately redirecting a malicious drone. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)* (pp. 827-834).

[16] Feng, Z., Guan, N., Lv, M., Liu, W., Deng, Q., Liu, X., & Yi, W. (2017, March). Efficient drone hijacking detection using onboard motion sensors. In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017* (pp. 1414-1419).

[17] Melikhova, A. P., & Tsikin, I. A. (2018, July). Optimum array processing with unknown attitude parameters for GNSS anti-spoofing integrity monitoring. In *2018 41st International Conference on Telecommunications and Signal Processing (TSP)* (pp. 1-4).

[18] Restivo, R. D., Dodson, L. C., Wang, J., Tan, W., Liu, Y., Wang, H., & Song, H. (2023, May). GPS spoofing on UAV: A survey. In *IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*(pp. 1-6).

[19] Shafique, A., Mehmood, A., & Elhadef, M. (2021). Detecting signal spoofing attack in uavs using machine learning models. *IEEE access*, *9*, 93803-93815.

[20] Aissou, G., Slimane, H. O., Benouadah, S., & Kaabouch, N. (2021, December). Tree-based supervised machine learning models for detecting GPS spoofing attacks on UAS. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 0649-0653).

[21] Gasimova, A., Khoei, T. T., & Kaabouch, N. (2022, January). A comparative analysis of the ensemble models for detecting gps spoofing attacks on uavs. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0310-0315).

[22] Bachrach, A., Prentice, S., He, R., & Roy, N. (2011). RANGE–Robust autonomous navigation in GPS-denied environments. *Journal of Field Robotics*, *28*(5), 644-666.

[23] Kendoul, F. (2012). Survey of advances in guidance, navigation, and control of unmanned rotorcraft systems. *Journal of Field Robotics*, *29*(2), 315-378.

[24] He, D., Qiao, Y., Chan, S., & Guizani, N. (2018). Flight security and safety of drones in airborne fog computing systems. *IEEE Communications Magazine*, *56*(5), 66-71.

[25] Barbeau, M., Garcia-Alfaro, J., & Kranakis, E. (2019, April). Geocaching-inspired resilient path planning for drone swarms. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 620-625).

[26] Ferrão, I. G., Pigatto, D. F., Fontes, J. V., Silva, N. B., Espes, D., Dezan, C., & Branco, K. R. (2020, July). STUART: ReSilient archiTecture to dynamically manage Unmanned aeriAl vehicle networks under atTack. In *2020 IEEE Symposium on Computers and Communications (ISCC)* (pp. 1-6).

[27] Bera, B., Wazid, M., Das, A. K., & Rodrigues, J. J. (2021). Securing internet of drones networks using ai-envisioned smart-contract-based blockchain. *IEEE Internet of Things Magazine*, *4*(4), 68-73.

[28] "Software-defined GPS signal simulator." GitHub repository, https://github.com/osqzss/gps-sdr-sim, 2018.

[29] G. van Esch and D. van den Heuvel (2021). *PX4 autopilot on a UAV controller*, Topic Embedded Systems [White paper].

[30] Koubâa, A., Allouch, A., Alajlan, M., Javed, Y., Belghith, A., & Khalgui, M. (2019). Micro air vehicle link (mavlink) in a nutshell: A survey. *IEEE Access*, *7*, 87658-87680.

[31] Pirayesh, H., & Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE communications surveys & tutorials*, *24*(2), 767-809.

[32] L. Al-Soufi (2022), "An implementation-based study of the detection and recovery from GPS spoofing attacks for unmanned aerial vehicles", MSc Thesis, Bahcesehir University, Turkey.