AN IMPLEMENTATION-BASED STUDY OF THE DETECTION AND RECOVERY FROM GPS SPOOFING ATTACKS FOR UNMANNED AERIAL VEHICLES

LINA AL-SOUFI

JUNE 2022

AN IMPLEMENTATION-BASED STUDY OF THE DETECTION AND RECOVERY FROM GPS SPOOFING ATTACKS FOR UNMANNED AERIAL VEHICLES

A THESIS SUBMITTED TO THE

GRADUATE SCHOOL

OF

BAHÇEŞEHİR UNIVERSITY

LINA AL-SOUFI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR

THE DEGREE OF SCIENCE

IN THE DEPARTMENT OF CYBER SECURITY

JUNE 2022

T.C.

BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL

MASTER THESIS APPROVAL FORM

Program Name:	Cyber Securıty
Student's Name and Surname:	Lina Al-Soufi
Name Of The Thesis:	An Implementation-Based Study of the Detection and Recovery from GPS Spoofing Attacks for Unmanned Aerial Vehicles
Thesis Defense Date:	29.06.2022

This thesis has been approved by the Graduate School which has fulfilled the necessary conditions as Master thesis.

Prof. Dr. Ahmet ÖNCÜ

Institute Director

This thesis was read by us, quality and content as a Master's thesis has been seen and accepted as sufficient.

	Title/Name	**Signature**
Thesis Advisor's	Asst. Prof. Ece Gelal Soyak	
Member's	Asst. Prof. Tarkan Aydın	
Member's	Asst. Prof. Evşen Yanmaz Adam	

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: Lina Al-Soufi

Signature:

ABSTRACT

AN IMPLEMENTATION-BASED STUDY OF THE DETECTION AND RECOVERY FROM GPS SPOOFING ATTACKS FOR UNMANNED AERIAL VEHICLES

Al-Soufi, Lina

Master's Program in Cyber Security

Supervisor: Assist. Prof. Ece Gelal Soyak

June 2022, 57 pages

As drones have become one of the fastest spreading technologies employed in different use cases, a spike in the number of attacks has exposed the fact that rapid manufacturing has compromised drone security. An attack on a drone is a method of disrupting or obstructing the drone's operational mechanism, and these attacks may also be used to identify drone security flaws. In this thesis, an experimental study is conducted on how navigation attacks can compromise the drone's system by using GPS jamming and spoofing attacks. Blocking and creating fake GPS signals can disrupt the original GPS signal, making the drone lose connection with the user, thus losing it. We have developed a "return-to-start point" functionality that can prevent and protect a drone from loss by responding promptly to such navigational attacks. We evaluated our solution's effectiveness via experiments that were carried out on our developed Raspberry Pi drone and compared its behavior with that of a commercial drone, namely the DJI Mavic Air 2.

Key Words: Drones, GPS spoofing, GPS jamming, software-defined radio.

ÖZ

AN IMPLEMENTATION-BASED STUDY OF THE DETECTION AND RECOVERY FROM GPS SPOOFING ATTACKS FOR UNMANNED AERIAL VEHICLES

Al-Soufi, Lina
Siber Güvenlik Yüksek Lisans Programı
Tez Danışmanı: Assist. Prof. Ece Gelal Soyak

Haziran 2022, 57 sayfa

Drone'lar, farklı kullanım senaryolarında rol alan, en hızlı yayılan teknolojilerden biri haline geldiğinden, saldırı sayılarında artış görülmekte ve bu da hızlı üretimin drone güvenliğini tehlikeye attığı gerçeğini ortaya çıkarmaktadır. Bir drone'a saldırı, drone'nun operasyonel mekanizmasını bozma veya engelleme yöntemidir ve bu saldırılar, drone güvenlik açıklarını belirlemek için de kullanılabilir. Bu tezde, HackRF One PortaPack Yazılım Tanımlı Radyo (SDR) cihazı aracılığıyla GPS boğma (jamming) ve sahtekarlık (spoofing) saldırılarını kullanarak navigasyon saldırılarının drone'un sistemini nasıl tehlikeye atabileceği üzerine deneysel bir çalışma yapılmaktadır. Orjinal GPS sinyallerinin alımı engellenip sahte GPS sinyalleri oluşturulması, drone'nun kullanıcı ile bağlantısını ve dolayısıyla onu kaybetmesine neden olabilir. Bu tür geniş çapta yayılan seyir saldırılarına anında yanıt vererek bir dronun kaybolmasını önleyebilen "Başlangıç Noktasına Dönüş" özelliği geliştirilmiş, Raspberry Pi drone üzerinde denenmiştir; ve geliştirilen davranış, DJI Mavic Air 2 isimli ticari drone davranışı ile karşılaştırılmıştır.

Anahtar Kelimeler: Drone'lar, GPS sahtekarlığı, GPS boğma, yazılım tanımlı radyo.

I dedicate my thesis to my dear mother Orouba, my father Khaled, my siblings Doa’a, Rana, Ruba, Omar, and Ehab, and finally to my friends for always being there for me and supporting me. A particular sense of thanks goes out to myself, who have always been committed to completing this master's degree. This degree will be a source of pride for all of us.

ACKNOWLEDGMENT

I want to acknowledge and give my dearest thanks to my supervisor Dr. Ece Gelal Soyak. Her guidance and support got me through every step of writing my master's thesis. Also, I want to thank my friend Talha Demirsoy for his unwavering support, kind patience, and technical guidance that made this work possible. I would also like to give special thanks to my family one by one and my friend Moussa for their continuous support and understanding when undertaking and writing my thesis. Finally, I would like to thank God for leading me through all the difficulties and allowing me to complete my degree.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

GPS	Global Positioning System
UAV	Unmanned Aerial Vehicles
SDR	Software-Defined Radio
UAS	Unmanned Aerial System
UAS	Unmanned Aircraft System
IMU	Inertial Measurement Unit
FAA	Federal Aviation Administration
DoD	Department of Defense
MAV	Micro Aerial Vehicles
MALE	Medium Altitude Long Endurance
HALE	High Altitude Long Resistance
WWII	World War Two
INS	Inertial Navigation Systems
GNSS	Global Navigation Satellite System
PVT	Position, Velocity, and Time
PNT	Positioning, Navigation, and Timing
PCIe	Peripheral Component Interconnect Express
LiDAR	Light Detection and Ranging Sensor
GHz	Gigahertz
OS	Operating System

Chapter 1

Introduction

Unmanned Aerial Vehicles (UAVs), more commonly known as drones, are a type of aircraft that can be described as flying robots that can be remotely controlled or fly autonomously using a built-in flight plan software known as the autopilot that operates with onboard sensors and the global positioning system (GPS) without the need of human interaction.

UAVs have recently gained public attention due to the technology's increasing affordability for individuals, professionals, and organizations. Not to mention that drones were originally intended to be used as weapons in military operations, among other things. Drones are expected to expand and grow substantially in number in the following years. More customized and innovative forms of this aerial vehicle are targeted to be sold for various civilian tasks since they could be used in various industries.

Throughout the past few years, studies have confirmed that many attacks against drones are closely related to the vulnerabilities of the civil GPS and that they cannot be regarded as safe, but what was always lacking is a feasible solution. Given that the value of a drone rises as its functions improve, professional drones would be regarded as more important than consumer drones. Their capabilities are more advanced and sensitive, and their cost can be magnitudes higher. Professional drones carry out vital missions to maintain security, protect humans from danger, save lives, and make jobs easier.

Professional drones have been employed in monitoring security, guarding important figures, surveillance, rescue, delivery, and various other critical jobs that assist us in our daily lives. Thus, the impact of professional drones being vulnerable to attacks could compromise the drone and its surroundings as well. Resulting in significant damage that extends to many levels and layers of our life. Such as financial, physical, ethical, reputational, risk of human life, and much more that goes beyond an insecure device.

Losing the connection with a drone puts the consumer at risk, whether they are individuals or large organizations. When a drone is lost, one's privacy may easily get

violated. Also, the three fundamental IT security principles: availability, integrity, and confidentiality of a drone's data, will be heavily questioned. As a result, their security is critical since good use can be reversed once a hacker has taken control of a drone.

UAVs need accurate navigation to operate autonomously or semi-autonomously; thus, the Global Navigation Satellite System (GNSS), which includes the GPS, is an essential component for both military and civil UAVs. Unlike military UAVs' GPS signals, which are encrypted and cannot be modified (Parkinson et al., 1996), 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 (Seo et al., 2015).

Currently, the most popular way to guarantee accurate UAV navigation has been to establish a sensor core comprised of an inertial measurement unit (IMU) and a GPS receiver to provide high accuracy measurements, as a navigation processor uses them to calculate the moving object's position, velocity, and attitude in relation to a given starting position, velocity, and attitude. (Abdelfatah et al., 2011) (Woodman & J., 2007).

Given the extent of how vulnerable the GPS and other GNSS are to signal jamming and spoofing attacks, an increased focus on designing a UAV navigation and control system that can function in GNSS-denied environments has surfaced (Abdelfatah et al., 2011) (Kendoul, 2012) (Bachrach et al., 2011) (Weiss et al., 2011). Supported by the broad range of studies and field experiments done on various UAV GPS-operated devices that continuously showcase that GPS navigational attacks affect us on a deep level, and it being relatively feasible to test its applicability on the real ground has drawn many researchers into the subject. Such as, using low-cost equipment for GPS spoofing, where fake GPS signals are created and broadcasted to manipulate a target receiver's reported position, velocity, and time (PVT), could make an attack highly achievable (Humphreys et al., 2008) (Shepard & Humphreys, 2011) (Shepard et al., 2012a) (Shepard et al., 2012b).

1.1 Purpose of Study

This thesis explores the extent of unmanned aerial vehicle (UAV) vulnerability to signal blockage and fake GPS signals as a result of jamming and spoofing attacks by (1) establishing the necessary conditions for capturing the UAVs via GPS jamming and spoofing, (2) demonstrating the field experiments on both of our test subjects DJI Mavic Air 2 and Tale, (3) investigating and comparing the results, (4) validating the detection and recovery mechanism from GPS spoofing attacks for the newly developed Unmanned Aerial Vehicles Tale.

1.2 Contributions

This research contributes to the body of UAV detection and recovery from GPS jamming and spoofing attacks area of study. We have conducted field experiments to show the effectiveness of our solution, which is integrated into the newly developed Raspberry Pi drone, Tale. The main contributions of this thesis are:

- Developing a GPS jamming and spoofing attacks to target UAV GPS receivers, showcasing the validity of the vulnerability.
- Proving that the professional UAV used in this thesis is vulnerable to jamming and spoofing attacks.
- 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 solution approach in detecting and recovering from GPS jamming and spoofing attacks.
- Promoting awareness among the public, the scientific community, and manufacturers that professional Unmanned Aircraft System should integrate a higher degree of security by proving the potential of such attacks and proposing a viable solution.

1.3 Thesis Overview

This thesis is arranged into five chapters. Chapter 2 presents background on drone classification, types, usage, communication method, the Global Positioning System, and GPS attacks. Chapter 3 presents the hardware and software utilized and the solution approach. Chapter 4 showcases the experiments conducted and discusses their results. Chapter 5 discuss the conclusion and possible future work.

Chapter 2

Background and Related Work

2.1 Drones

2.1.1 Terminology. According to the Federal Aviation Administration (FAA), "drone" is an overarching colloquial term for all remotely piloted aircraft, which signifies an umbrella term, including many technical terms beneath it (e.g., UAS, or UAV), used in our daily lives by different types of users. (FAA Safety Briefing & Federal Aviation Administration, 2021)

The terms "Unmanned Aircraft System" (UAS) and "drone" are used interchangeably, although a UAS is a three-part "system," with "drone" referring to the aircraft itself. The UAS contains, in addition to the drone (aircraft), the control station and the communication connection between the control station and the aircraft. (FAA Safety Briefing & Federal Aviation Administration, 2021). Also, the "Unmanned Aircraft System" (UAS) term was put together and defined by the United States Department of Defense (DoD) as a "system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft." ("DOD Dictionary of Military and Associated Terms (June 2018)," 2018)

The industry interchangeably uses the terms "unmanned aerial vehicle" (UAV) and "unmanned aerial system" (UAS); however, the FAA has opted to define "unmanned aircraft" (UA) as the aircraft itself, to separate the system from the aircraft. (FAA Safety Briefing & Federal Aviation Administration, 2021) Also, according to the United States DoD, an Unmanned Aircraft (UA) is defined as an "aircraft that does not carry a human operator and is capable of flight with or without a human remote control." ("DOD Dictionary of Military and Associated Terms (June 2018)," 2018). Both the industry's UAV and the FAA's UA terms refer to the same thing: a UAS. Fixed-wing UAs, which resemble airplanes, or rotorcraft, such as quadcopters or other multirotor aircraft, may be referred to by either title. UAVs are most often linked with military aircraft, although they may also be employed for several other functions. UAVs may also be semi-autonomous, which means they operate with the help of

sensors, a ground control system, and custom-designed software. (FAA Safety Briefing & Federal Aviation Administration, 2021).

2.1.2 Drone classification, types, and usage. Depending on their duties, drones are built with various most suitable technologies and electronic communication capabilities for functioning an intended task. They are frequently equipped with a range of cameras with varying sizes, weights, designs, motor types, sensor systems, and other features depending on the activity to be performed. Drones are classified based on their functionality and purpose of use, in this section two classification methods have been studied. The first one, classifies the drones aaccording to their methods of operation and the second one according to the load they can carry (Arteaga et al., 2019) (H. Gran, & Mickols, 2020).

- Manual mode: During the whole flight, the aircraft is controlled by a radio-control station.
- Assisted mode: The pilot specifies a goal in the radio-control position, and a self-pilot conveys those actions to the aircraft.
- Automatic mode: The pilot creates a "flight plan," and the aircraft takes off on its own. At all times, the pilot is in command. Except in the event of a loss of communication control between the aircraft and the pilot in an emergency.
- Strict autonomous mode: Similar to automatic, it establishes a flight plan, but once begun, the pilot cannot interfere in the control.

In 2006, the European Association of Unmanned Vehicle Systems (EUROUVS) created a categorization that divided UAVs into four main categories. The categorization was on a drone’s characteristics based on the "Maximum Take Off Weight (kg)", "Maximum Flight Altitude (m)", "Endurance (hours)" and "Data Link Range (km)" (Brown, 2020) (Arteaga et al., 2019) (Hassanalian, 2018) (Castrillo et al., 2022).

- Micro and small drones: They range in weight from 100 grams to 30 kilos and can fly up to 300 meters in height. They are also known as (MAVs).

- Tactical drones: They weigh between 150 and 1,500 kg and can fly at altitudes ranging from 3000 to 8000 meters. They are also known as Long Resistance Altitude or Medium Altitude Long Endurance drones (MALE). They are mostly employed in the military and are referred to as combat drones.
- Strategic Drones: These are massive and heavy gadgets that may weigh up to twelve tons and fly at a maximum height of 20,000 meters; they are also known as High Altitude Long Resistance or High Altitude Long Endurance (HALE) and are employed in the military.
- Special Task UAVs: These drones perform specific military operation, it includes Lethal (LET), Decoys (DECs), Stratospheric (Strato) and Exo-Stratospheric (EXO) UAVs.

2.1.2.1 Recreational drones. Recreational drones, also known as personal drones, hobbyist drones, and consumer drones, are UAVs built for the mass market and are only used for enjoyment purposes. (“Recreational Use of Drones,” n.d.) (Wigmore, 2013).

2.1.2.2 Commercial drones. A commercial drone, also known as a professional drone, is a drone that is used for work purposes. Commercial drones contain both professional-grade drones designed for certain sorts of work tasks and consumer-grade drones that may be utilized in professional situations, such as DJI's Mavic Air 2. (“Best Commercial Drones & Professional Drones Of 2022 (New Guide),” n.d.)

According to their civil application, from reconnaissance and surveillance to payload delivery, the wide range of commercial drone capabilities enable us to employ them in different fields such as disaster management, construction, and infrastructure inspection, healthcare, agriculture, building, waste management, mining, film and television production, utility inspecting, urban planning, geographic mapping, wildlife conservation, commercial photography, law enforcement, and weather forecasting. (Höglund Gran, & Mickols, 2020) (Sivakumar, & TYJ, 2021).

According to the FAA, there is a fine line between recreational drones and commercial drone use, and fliers must be aware of the rules and regulations that distinguish between them. (“Recreational Flyers & Modeler Community-Based Organizations,” 2019)

2.1.2.3 Military drones. The concept of an unmanned aircraft arose during WWI when both the United States and France focused on constructing an autonomous airplane. In the end, France was the one who was able to create such a device. It was named Voisin BN3 biplane, and it could only fly for around 100 kilometres. The significant casualties and losses suffered during WWII due to reconnaissance aircraft drove the need to build unmanned aerial vehicles. The unfortunate sequence of events forced the development of UAVs that would eliminate the necessity for a pilot. They essentially intended to preserve people's lives so that they could avoid human casualties when an aircraft happened to get shot. Despite the fact that this technology has been in development for many years, the first-time drones were deployed for surveillance was in 1973, during the Vietnam War (Brown, 2020).

UAVs make a lot of sense in the current time, particularly on the battlefield. Using them is very advantageous since you do not have to worry about sending troops behind enemy lines. Although these advantages do not come without dispute. The ethics of using these aerial vehicles are often the subject of heated political controversy. Much of this argument centered around the idea that unmanned drones make military attacks much too simple. Military leaders may be ignorant of the true repercussions of their combat, it may result in a form of assault with unknown implications and collateral damage, and in worst scenarios, civilian casualties may be involved (Brown, 2020).

Military UAVs may be classified according to the unique tasks they are intended to perform in different military missions. We have the following UAVs based on these qualifications: (Brown, 2020)

- Target and decoy UAVs may offer both ground and aerial gunnery at a target, as well as imitate an enemy missile or aircraft.
- Reconnaissance UAVs are employed to give information on the battlefield.
- Combat UAVs are employed to provide offensive capabilities for high-risk operations.

The communication between the drone and controller could take a place in the following three ways. In radiofrequency drones, the controller delivers a radio signal

from the remote control (RC) to the drone, instructing it on what to perform; Wi-Fi drones are usually used to stream footage to a smartphone, PC, or tablet and those same gadgets may be used as a controller remotely control the drone; GPS drones are equipped with a GPS module that enables them to know their location depending on a network of orbiting satellites (Cast, 2021) (Ciobanu, 2020). In this work, we focus on GPS drones, which are explained in detail in Section 2.2.

2.2 Global Navigation Satellite System (GNSS)

The GNSS is a constellation of satellites that broadcast positioning and timing data from space to GNSS receivers. The receivers then use this information to calculate the required position. GNSS is also used as an umbrella term since it provides worldwide coverage. Europe's Galileo, the United States' NAVSTAR Global Positioning System (GPS), Russia's Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS), and China's BeiDou Navigation Satellite System are all examples of GNSS. The four primary systems use various modulation algorithms and have different carrier frequencies. (“What Is GNSS?,” 2016) (Maksutov et al., 2019).

2.2.1 Global positioning system (GPS). 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, providing positioning, navigation, and timing (PNT) services to users since its primary purpose is to accurately pinpoint locations around the globe by measuring the distance between satellites. Figure 1 shows how the satellites in the GPS constellation are arranged into six equally spaced orbital planes, consisting of 21 satellites and three active spares. This 24-slot arrangement guarantees that users would receive information from at least four satellites from any point on earth. (Sivakumar, & TYJ, 2021) (“Recreational Flyers & Modeler Community-Based Organizations,” 2019) (Watts et al., 2012) (Brown, 2020).

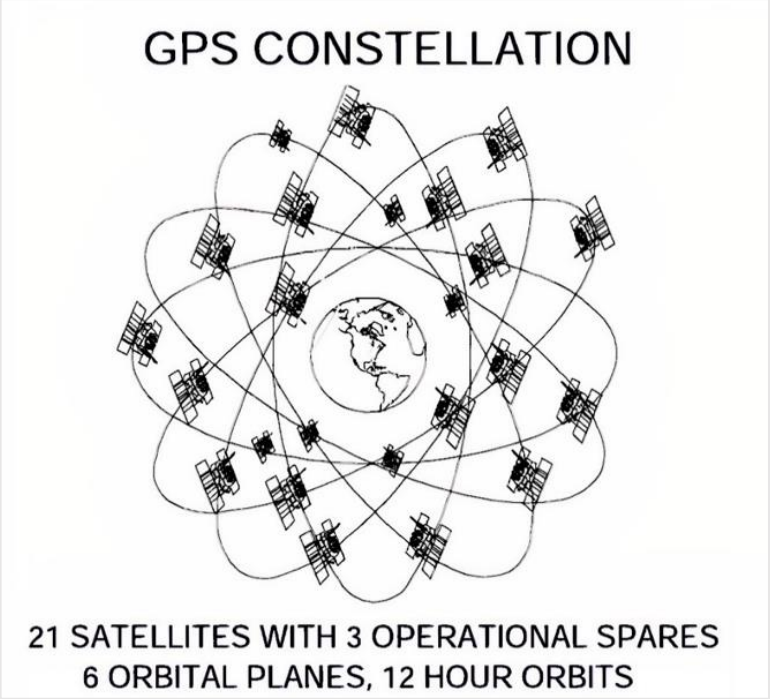


Figure 1. GPS satellite constellation (Dana, 1997).

The GPS consists of three segments, the space segment, the user segment, and the control segment. The GPS space segment consists of a constellation of satellites that send radio one-way signals to the users. It monitors the condition of satellites, changes their locations and timings, and shares their data with users to improve the system's performance. Whereas the user segments are GPS receivers that assist users in determining their worldwide coordinates and synchronizing their time. The United States Space Force is the ones who oversee the development, maintenance, and operation of the space and control segments. (“GPS Overview,” 2019) (“Space Segment,” 2019). Moreover, the control segment is in charge of monitoring and guaranteeing the GPS's integrity by exerting command and control over the GPS constellation. It is made up of a global network of ground facilities that gather telemetry in order to monitor and analyze the broadcast signal, as well as issue orders and upload navigation messages as needed (Purwar et al., 2016).

The GPS in drones is often the key to securely flying the UAV in many of its applications, such as reconnaissance, surveillance, mapping, spatial information acquisition, and geophysics exploration, as it is used as the primary sensor for the localization process of the drone (Sinopoli et al., 2001) (TerrisGPS, n.d.).

GPS is used with Inertial Navigation Systems (INS) to provide more complete UAV navigation functionality GPS in UAVs is vital whether the UAV is remote-controlled, autonomous, or semi-autonomous. GPS navigation algorithms may provide continuous accuracy as long as adequate satellite signals are available during the UAV flight. (TerrisGPS, n.d.).

GPS is a critical component of most UAV navigation systems, as it is used to identify the vehicle's location. The UAV GPS is also used to calculate the vehicle's relative location and speed. The receiver's location may be used to monitor the UAV or, in combination with an automated guidance system, to guide the UAV (TerrisGPS, n.d.).

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. 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 (TerrisGPS, n.d.).

From the collected data, the UAV GPS receiver can also provide UAV's precise location and time stamp for the functionalities the UAV provides. Such as earth observation measurements or simply for any photo that was taken. (TerrisGPS, n.d.).

GPS drone is also capable of navigation by Waypoints. A flight route or a mission may be planned by instructing the drone to go to specified GPS locations along with a predefined path using its autopilot mode; this functionality is known as waypoints. GPS also allows a drone to execute a position hold, which enables the drone to retain a stable location point, an altitude hold, which also 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 (Ciobanu, 2020).

2.2.2 Drone GPS attacks.

2.2.2.1 GPS jamming. GPS jamming transmits random noise interfering signals that block the reception of the genuine GPS signals, broadcasting those signals at a higher intensity than the genuine signals interfere with GPS receivers' ability to detect legitimate signals; thus, the receiver will not be able to function. Besides that, the signal intensity of legitimate GPS signals is very low in nature; therefore, it is relatively easy to achieve (Purwar, Joshi, & Chaubey, 2016).

GPS jamming is one of the major attacks that severely impacts systems' availability. Jammers operate against receivers, not transmitters, they can be used to block all wireless communication in a certain area. This attack causes communication failure due to packet corruption or loss. A random noise signal is an artificially generated radio signal, its amplitude and frequency are both random. It often spans all available communication frequencies and prohibits transmission and reception at any frequency, and it can be used to degrade all signal types (Shashok, 2017) ("Cyber security threat analysis and attack simulation for unmanned aerial vehicle network," 1) (Javaid, 2015).

GPS jamming equipment is widely accessible on numerous platforms and websites, as it can also be performed using a wide range of devices while utilizing different jamming methods and techniques. ("DEF CON 25 - David Robinson - Using GPS Spoofing to Control Time," 2019).

2.2.2.2 GPS spoofing. GPS spoofing poses a bigger threat than GPS jamming since a spoofer could lead the target to produce an inaccurate PVT solution or even achieve total control over a drone's flight path by re-broadcasting or transmitting fake GPS signals (Horton & Ranganathan, 2018). Not to mention that GPS spoofing is a more challenging and threatening electronic attack than jamming is since it could easily go undetected causing major damage to the victim's receiver. In addition, a failed spoofing attack would still result in a jamming attack effect as its by-product (Faria, Silvestre, Correia, & Roso, 2018).

Spoofers transmit radio signals conveying fake GPS location information, to overpower the relatively weak GNSS signals in two main ways. The first one is known as "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 to lure it into the desired location or a landing zone. ("About: Meaconing," n.d.) ("Meaconing (US DoD Definition)," n.d.).

The second spoofing attack has been described in many ways and terms. In short, in a GPS spoofing attack, a radio transmitter is used to send what could be described as a counterfeit GPS signal, a fake GPS signal, or a false GPS signal is generated to manipulate a target receiver's position or time. GPS spoofing takes advantage of the inherent vulnerability of civilians' GPS, as the spoofing signals provide the drone with a false and inaccurate impression of its actual physical location. As a result, a drone diverges from its original route and is very susceptible to loss. ("What Is GPS Spoofing?" 2020) ("What Is Spoofing and How to Ensure GPS Security?" n.d.) ("Cyber security threat analysis and attack simulation for unmanned aerial vehicle network," 1).

2.3 Related Work

2.3.1 Previous work on creating spoofing. Thanks to hardware cost reduction and open-source software, UAVs are now more easily accessible to the public. Which, unfortunately, may have contributed to misuse. Several research efforts aimed to put spoofing attacks into good use in counterattacking and protecting the different GEO Zones from malicious drones. In ways where they can neutralize, take down, reroute, or gain control over a drone.

(J. Gaspar et al., 2018) uses low-cost programmable Software Defined Radio (SDR) platforms for simulating GPS signals to transmit false signals and induce a location error on the targeted GPS receiver. Based on it, a defensive system was implemented which can divert or even take control of unauthorized UAVs whose flight path depends on the information obtained by GPS.

(D. He et al., 2019) present a new GNSS spoofing-based system that can take control of an autonomous non-cooperative UAV. The proposed method can control the UAV to fly to a specified location for capturing the drone. Using an off-the-shelf GPS signal simulator, location spoofing signals are continuously generated through an

adaptive algorithm so that the drone moves toward the specified location. The effectiveness of the proposed technique has been demonstrated via simulations.

(M. Ceccato et al., 2020) studied spoofing a drone swarm to divert its route without disrupting its formation. The authors proposed what they called spatial spoofing, where, instead of tracking the movement of each drone and transmitting an individual spoofing signal per drone, they made sure that at any point where drones move, a fake position for that point has been estimated.

More recently, (H. Alamleh and N. Roy, 2021) exploited the lack of source authentication in GPS systems to address the problem of drones flying in restricted areas or using the camera to spy on individuals and entities. A technique to ground and find the launch location of violating drones has been proposed. The technique works by invoking the rescue mode and employing RF software-defined radios to broadcast manipulated GPS signals by an algorithm. The algorithm can ground violating drones and find the drone's launch location.

2.3.2 Previous work on detecting spoofing. Threats to the performance of GNSS via intentional RF interference have been studied. One of the first studies is (M. L. Psiaki et al., 2016), where a detailed description of the operation of different commercial jammers was presented. The specific feature of signal spoofing attacks is their identity structure; they carry false information about the user's navigation parameters.

(A. P. Melikhova and I. A. Tsikin, 2018) proposed a probabilistic algorithm to detect GNSS spoofing attacks. This integrity monitoring procedure was implemented using a small-sized antenna array. Ideally, the acceleration and (angular) velocity measured by motion sensors can be compared with the position reported by GPS to detect whether the drone has been hijacked. However, the position estimation by motion sensors demonstrates inaccuracy due to accumulating errors over time.

(Z. Feng et al., 2021) propose a novel method to detect hijacking based on motion sensors measurements and GPS, which overcomes the accumulative error problem by computing estimates of linear accelerations and, based on them, determines whether hijacking has happened. 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.

In detecting spoofing, machine learning techniques may be used. (A. Shafique et al., 2021) used several learning algorithms on signal features such as jitter, shimmer and modulation variants. (G. Aissou et al., 2021) compared several tree-based machine learning models in terms of accuracy of detecting GPS spoofing attacks.

2.3.3 Previous work on recovery from GPS spoofing attacks. (I. G. Ferrão et al., 2020) design and develop a resilient architecture for UAVs that dynamically manages the network, even when subjected to an attack during a mission, integrating security methods and safety. This work also investigates incorporating safety and security as a unified concept in developing UAVs.

(M. Barbeau et al., 2019) 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.

(B. Bera et al., 2021) proposed to use smart contracts and Blockchain to render the drone network more resilient against attacks.

Chapter 3

Methodology and Solution Approach

In this section, we introduced the software, hardware, and setup that was used for the GPS attack experiment. Also, the technique that was followed throughout the attack's implementation was introduced, and the developed solution design was provided.

3.1 Software and Hardware Platform

Implementation is done on both hardware and software. Table 1 shows the hardware requirements for this implementation procedure, and Table 2 shows the software requirements for this implementation procedure.

Table 1

Hardware Requirements

No.	Hardware	Specification
1.	Laptop MSI MS-16R3	SigintOS.
2.	SDR HackRF	Mayhem firmware.
3.	Drone (DJI Mavic Air 2)	Flight Controller 5.8 GHz aircraft transmission system.
4.	Drone (Tale)	Raspberry Pi 3G/4G & LTE Base HAT.

Table 2

Software Requirements

Software	Interface	Purpose	Specification
SigintOS	Graphical	Attack Implementation	v1.1

Table 2 (cont.d)

Software	Interface	Purpose	Specification
GPS-SDR-SIM	Command line and console based	Attack Implementation	-
Mission Planner	Graphical	Ground Control Stations (GCSs).	v1.3.77
Raspberry Pi OS	Graphical	Operating the drone	Debian v11 Kernel v5.15
PX4-Autopilot	Command line and console based	Flight control solution	v1.12.3

3.1.1 Drones and drones' systems. First, we introduce the DJI Mavic Air 2 system, and its various components. Then, we introduce the Tale system and its components.

3.1.1.1 DJI Mavic Air 2 drone.

Figure 2. System overview of the DJI Mavic Air 2.
("Mavic air 2," n.d.)

Firstly, the mobile device, this system is compatible with any iOS or Android mobile device running iOS 11+ or Android 6.0 and higher. DJI Mavic Air 2 has its own smartphone application that needs to be installed before usage, which can be downloaded for Android from the main website and for iOS from the App Store.

Secondly, the controller, which is the primary means of communication with the drone. Moreover, the drone connects to the controller's built-in Wi-Fi hotspot, which operates and issues commands and settings to the drone at 2.400GHz-2.483GHz and 5.725GHz - 5.825GHz through radio transmission.

Lastly, the drone receives radio signals from the controller which directs its movement. To resist environmental factors, it employs a mix of onboard sensors such as GPS and barometer readings to maintain a steady flight. Furthermore, the DJI Mavic Air 2 has various "Smart" capabilities, such as "Return to Home", which enable the drone to fly autonomously to a predetermined point. The drone sends back flight data and sensor readings, as well as a live video stream to the mobile device ("Review: The DJI Mavic Air 2 is the best all-around drone for most people," 2020).

3.1.1.2 Tale drone. Tale is a Raspberry Pi drone that has uniquely novel programmed software. It was developed with on drone frame and many different electronic cards and components. The main building blocks for developing Tale were the Raspberry Pi 4, GPS module, flight control board, Raspberry Pi 4GLTE Cellular Modem Kit, and radio telemetry. Tale drone can be seen in Figure 3 below.

Figure 3. Tale drone.

3.1.1.2.1 Hardware and software system components. As previously mentioned, an unmanned aerial system (UAS) is a three-part system comprised of a drone, a ground control station (GCS) that monitors and regulates the movements of a drone, and a communication protocol via which these two can interact.

First and foremost, starting from the drone core, as we know every computer needs an operating system and so applies to Raspberry Pi 4. the Raspberry Pi OS, previously known as Raspbian, which is the official supported operating system was chosen since it meets a wide range of usage cases. C, C++, and Python programming languages were used in developing Tale.

Drones are autonomous platforms that can be programmed to carry out operations with or without the assistance of a pilot relying on the help of artificial intelligence (AI) that allows them to navigate through a wide range of situations. Drones utilize specific hardware and software known as autopilot, to control and monitor them, while it is used to connect them with the ground control station through telemetry or Wi-Fi communication.

The PX4 autopilot was chosen from among several open-source autopilot projects, including ArduPilot, Paprazzi UAV, Dronecode, and LibrePilot. PX4 Autopilot is part of the Dronecode project, which is a platform presented by the Linux foundation. PX4 is a flight control software for drones and other unmanned vehicles. PX4 has over 300 global contributors since it offers a versatile collection of tools for drone developers to share innovations and create customized solutions. Using PX4 provides easy integration for the other tools used in the Tale system, such as the communications protocol (MAVLink) and a ground control station (Mission Planner) (Esch & Den Heuvel, 2021) (Dronecode Foundation, 2021).

Mission Planner is a fully-featured Ground Control Station (GCS) that is compatible with different autopilot software, such as PX4 and ArduPilot. GCS allows users to initiate, configure, test, and tune a UAV. Advanced packages, that could be set up before an operation, enable autonomous flight planning, execution, and post-flight analysis. In general, GCS software can run on computers or mobile devices, for Mission Planner it can only run-on Windows ("ArduPilot documentation — ArduPilot documentation," 2022).

Micro Aerial Vehicle Link (MAVLink) protocol is a lightweight message serialization protocol designed for small UAVs as the name indicates. It was released

by Lorenz Meier in 2009 under the LGPL license as a communication protocol that establishes and retains a connection between the drones and ground stations (Koubaa et al., 2019). Figure 4 shows a diagram of Tale system that includes the computer, PX4 autopilot software, flight controller, communication protocols, and the ground control station.

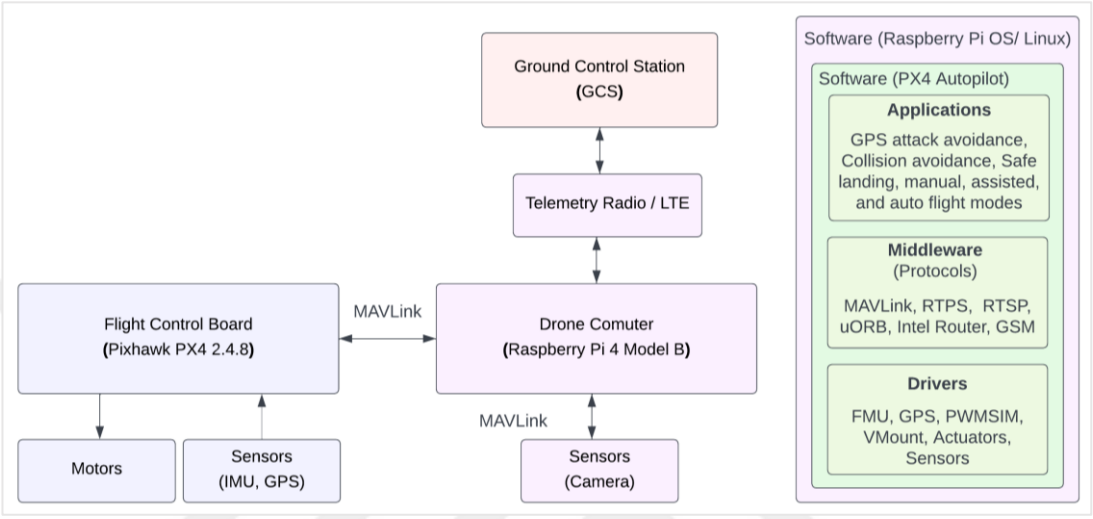


Figure 4. Tale system architecture.

Figure 5 shows the main hardware components used in developing Tale system.

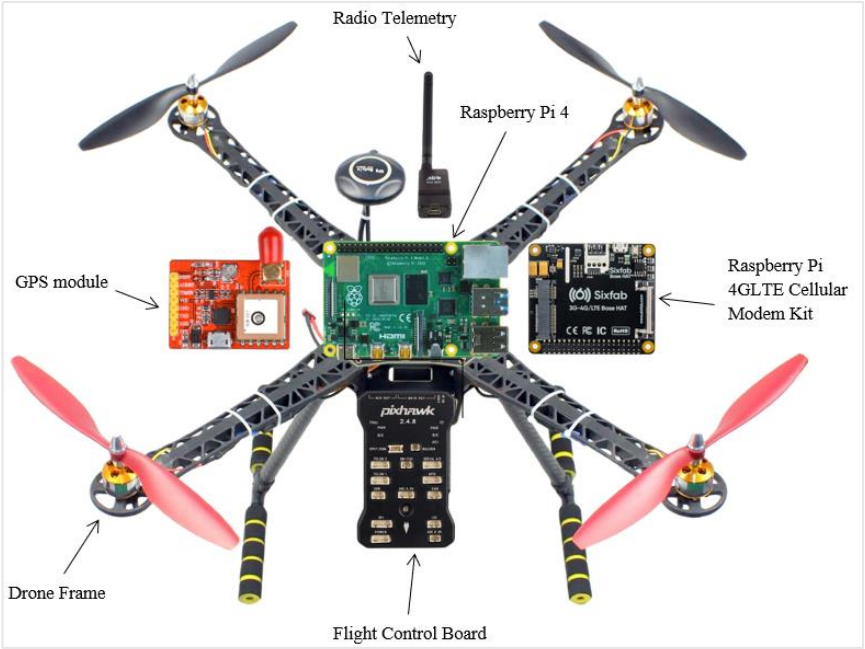


Figure 5. Tale system hardware overview.

Starting from the most important piece in the drone hardware components, that is Raspberry Pi 4 Computer Model B. Generally, the Raspberry Pi is an inexpensive, mini-sized computer that uses Linux operating system, it can be connected to a display, a keyboard, and a mouse, and gives the best performance. Focusing on the Raspberry Pi 4 Model B which is the fourth generation of Raspberry Pi devices, it offers the newest wired and wireless communication technologies needed for making and developing a wide range of customized computers and experiments (Doole, 2020) (Raspberry Pi 4 Computer Model B, 2019) (Westover, 2021).

Moving on to the Flight Control Board (PIXHAWK PX4). The flight controller, known as FC, is considered the aircraft's brain. It's a circuit board with a variety of sensors that detect drone movement as well as a user's instructions. It then uses this data to regulate the speed of the motors, causing the vehicle to move as commanded. The Flight Control Board also serves as a hub for other peripherals such as the GPS module, Radio Telemetry, Raspberry Pi 4G LTE Cellular Modem Kit, different sensors, and everything else. For the Tale system, Pixhawk PX4 Flight Controller Autopilot PIX 2.4.8 was used (Westover, 2021) ("3DR Pixhawk 1 · PX4 v1.9.0 user guide," 2020) (Pixhawk, n.d).

Next, is the GPS Module, the NEO-M8 module series, specifically NEO-M8N, was used for developing Tale. It is built on the high-performing u-blox M8 GNSS engine, as it provides concurrent GNSS reception for up to three GNSS systems. It detects several constellations at the same time and gives exceptional positioning accuracy in urban and rural areas where different circumstances of weak signals exist. The NEO-M8 series also has data integrity protection, geofencing, and GPS signals attack detection such as GPS spoofing and jamming. As well as, it has an adjustable interface setting to accommodate a wide range of customer applications (U-Blox, n.d.).

In addition, we have the Raspberry Pi 4G LTE Cellular Modem Kit. The Sixfab 3G/4G & LTE Base HAT provides an interface bridge between the PCIe cellular modems with a compatible Raspberry Pi computer. It enables the Raspberry Pi-based applications to connect with high-bandwidth data networks across the globe via the modems that are placed into the Base HAT (Marco, 2020) (Sixfab, n.d.).

Lastly, the Radio Telemetry device. In developing Tale, the CUAV P9 Radio data link communication module was used. It provides high power output, ultra-speed, and high reception sensitivity. Not to mention that it is compatible with the used

Pixhawk flight control board. It stands out for its extremely long-range, with a maximum reach of up to 60 kilometres. Thus, it is highly beneficial for drones' communication systems. Radio Telemetry mainly supports the LTE signal, strengthening it, so the drone would be able to reach very far distances. CUAV P9 Radio's working frequency ranges from 902 – 928MHz being able to work with the LTE signal frequency that for 3G operated in the 800 MHz, 850 MHz, 900 MHz, 1,700 MHz, 1,900 MHz, and 2,100 MHz bands while for 4G 850 MHz and 1800 MHz (CUAV, n.d.) (GSMA, 2017) (HBR, n.d.).

In the current unmanned ariel vehicles, many sensor technologies are used in a variety of ways, the same applies to Tale. Tale incorporates a set of sensors, such as LiDAR, Gyroscope, Accelerometer, and Piezoresistive Accelerometers. Nonetheless, LiDAR will only be introduced. LiDAR is the abbreviation for the Light Detection and Ranging Sensor. Lidar emits eye-safe laser beams that create a three-dimensional image for the world, giving machines and computers a precise picture of the scanned environment. To be more specific, the LiDAR system operates by generating pulsed light waves into the surroundings. Those same light energy pulses travel to the ground or nearby objects and then bounce off them, returning back to the LiDAR sensor. This method allows the sensor to calculate the distance between the vehicle and the ground or any other object, using the time it took for each pulse to return to the sensor. A detailed, real-time 3D map of the surrounding environment is created by repeating this method millions of times per second (Fahad, 2021) (Velodyne Lidar, Inc, 2022). Table 3 shows the used system components for developing the Tale drone and their specifications.

Table 3

Tale Hardware Components Specifications

Hardware	Specification
Raspberry Pi	Version 4, 4 GB
Flight Control Board	Pixhawk PX4 2.4.8

Table 3 (cont.d)

Hardware	Specification
GPS Module	Ublox Neo-M8N, Flash FW SPG 3.01 firmware version
Raspberry Pi 4G LTE Cellular Modem Kit	Raspberry Pi 3G/4G & LTE Base HAT.
Radio Telemetry	CUAV P9 Radio Drone Telemetry

3.1.1.2.1 Tale communication mechanism. Standard drones are radio-controlled air vehicles, which means they can be operated remotely using radio transmitter controllers. The controller transmitter communicates directly with the drone's receiver using signals, and vice versa. It's a two-way communication mechanism with no intermediate devices.

What differentiates Tale from other drones is mainly two things. Unlike other drones, Tale can maintain its connection regardless of the distance since it relies on using a 4G network for its controller-drone communication mechanism. Most importantly, Tale has its original return-to-start point function, which is described in section 3.3.3 Developed Solution Design.

3.1.2 GPS-SDR-SIM. GPS-SDR-SIM provides GPS baseband signal data streams that may be translated to radiofrequency (RF) utilizing software-defined radio (SDR) platforms. The produced GPS broadcast ephemeris is used to indicate the GPS satellite constellation, and faked coordinates, and can be used to specify a stationary point or a trajectory ("gps-sdr-sim: Software-defined GPS signal simulator," 2019).

3.1.3 Software-Defined Radio (SDR) Devices. Software-Defined Radios are radio frequency (RF) transceivers that allow for the speedy development and implementation of sophisticated wireless applications. SDRs are utilized in wireless communications, signal intelligence systems, and as building blocks for multichannel testbeds. There are different examples of SDR devices, such as HackRF, BladeRF, and

USRP. The device that will be used in the experiment is HackRF One SDR, see Figure 6 below ("Category," n.d.).

HackRF is a low-cost open-source software-defined radio platform that covers the frequency spectrum of GPS transmissions and works across a broad range of frequencies from 1 MHz to 6 GHz. It also has a built-in USB 2.0 port that works as an interface for data transmission and power supply. While it only supports half-duplex operation, which means it cannot transmit and receive signals simultaneously. HackRF could be used for many other purposes, such as a radio receiver, signal scanning (e.g., AM/FM radio), Ham radio, analog tv signal, and a satellite signal receiver. For example, it can receive signals from images (weather satellites) or GSM signals. In addition, HackRF can be used for jamming selected frequencies. Such as implementing GPS spoofing attacks (“HackRF One - Great Scott Gadgets,” n.d.) (“What Is SDR and What Can You Do with SDR?” 2020).

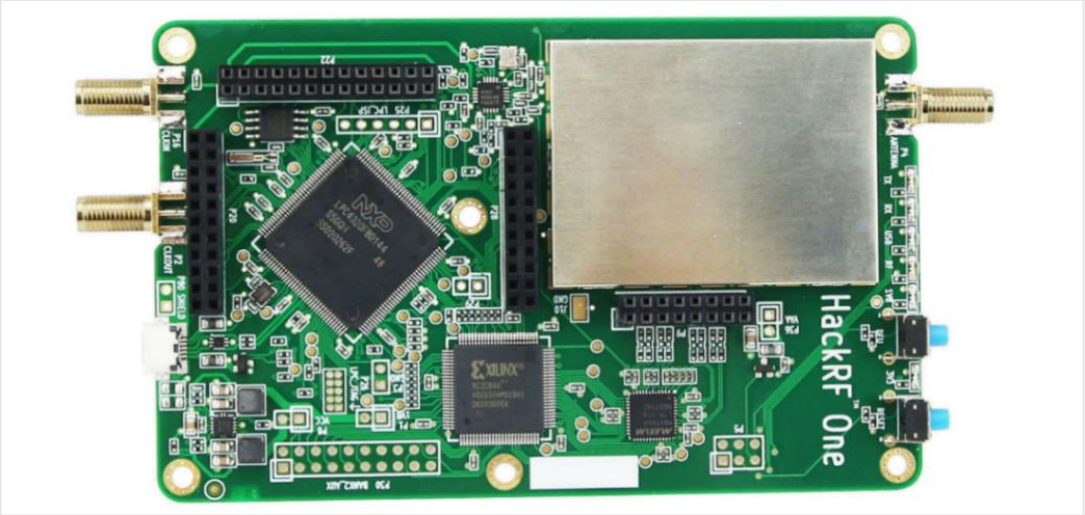


Figure 6. HackRF One software-defined radio.
(Schafer, 2021)

The PortaPack is used to convert the HackRF from a computer to a portable device, adding a touch LCD, several buttons, a headphone jack, a micro-SD card slot, and a custom aluminium case, see Figure 7 below. To be able to put the HackRF PortaPack device to its full potential use, third-party custom firmware is needed. E.g., MAYHEM (“Testing the Mayhem Firmware on a HackRF Portapack,” 2020).

HackRF PortaPack Mayhem is an improved derivative of the original PortaPack firmware. This firmware enables the user to receive, decode, and re-transmit a vast

range of wireless protocols without ever needing to connect to a computer (Nardi, 2020).

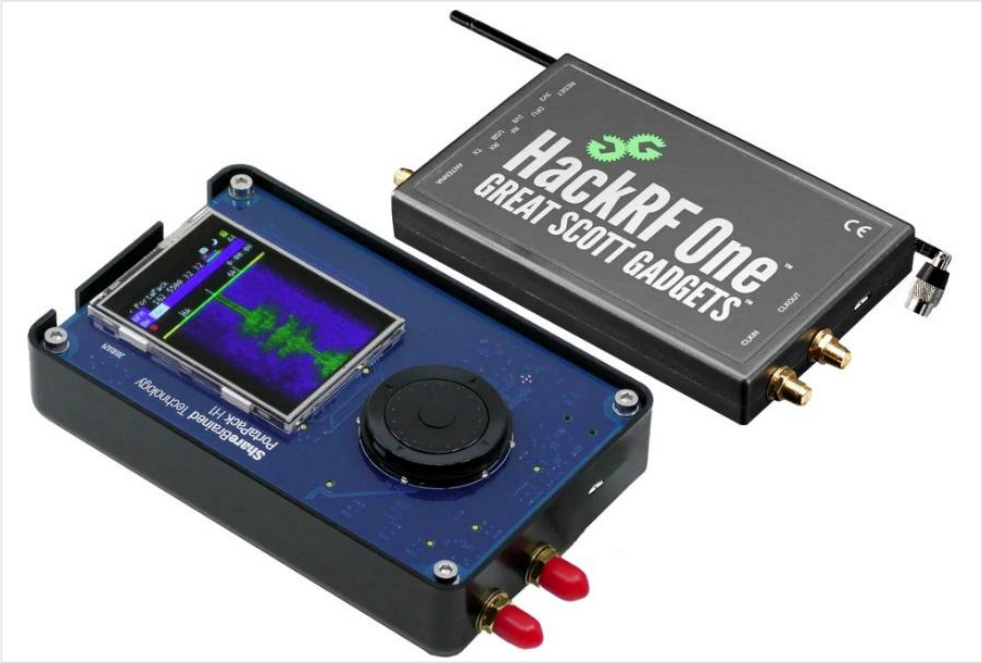


Figure 7. PortaPack for HackRF One.

("PortaPack for HackRF one," n.d.)

3.2 Attack Environment Setup

3.2.1 Operating system software. SigintOS is a Linux distribution built on the Ubuntu Linux operating system. This Linux system is intended for signal intelligence and contains capabilities that enable signal intelligence operations feasible by leveraging the usage of the installed SigintOS software. Many of the signal intelligence information processing tasks in Linux might be accomplished via the use of a graphical interface or the command line. ("SigintOS: Signal intelligence via a single graphical interface," 2021)

The drivers for the signal intelligence equipment such as HackRF, BladeRF, LimeSDR, and much more have been installed, and the major operations that will be used in our experiments are radio frequency jamming and GPS spoofing.

3.2.2 Setup. The system to be set up for this experiment is a strategy for GPS jamming and GPS spoofing attack that makes use of HackRF as well as various software and hardware components. This gadget allows this system to test attacks on the DJI Mavic Air 2 and Tale drone to investigate the signal flow and signal continuity on regular and irregular GPS signals. The GPS-SDR-SIM software is used by the HackRF device to create a GPS baseband signal data stream that could be converted to Radiofrequency using the Software-Defined Radio platform. Lastly, GPS jamming and spoofing attacks are carried out. Figure 8 depicts an overview of the drone GPS attack setup.

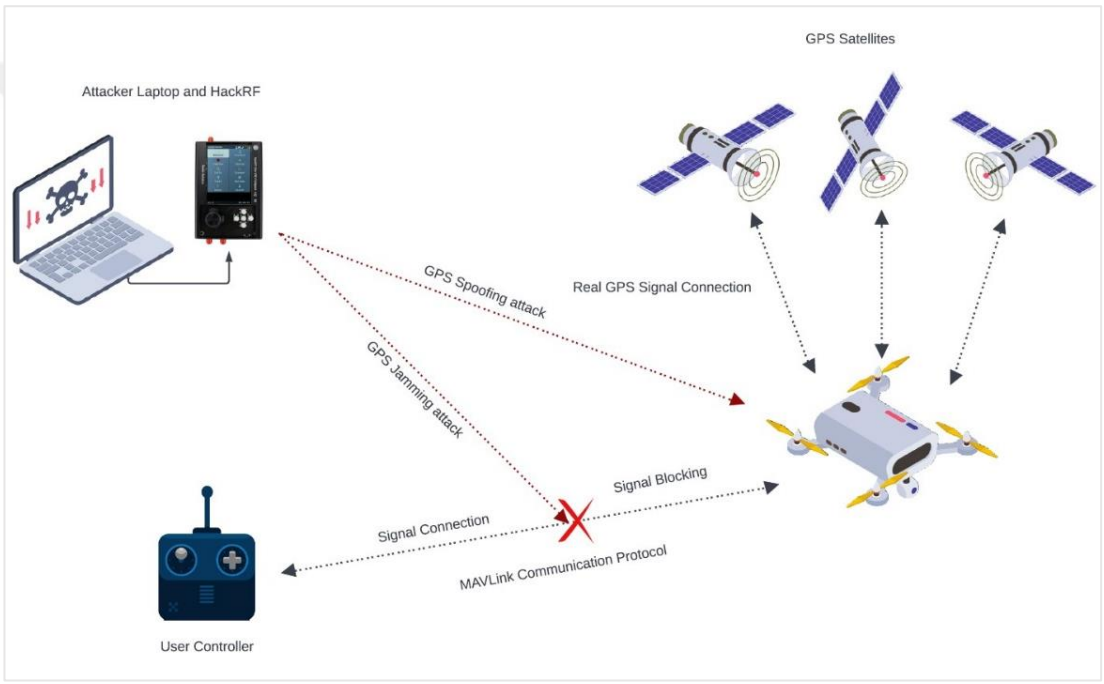


Figure 8. Overview of the drone GPS attack setup.

3.3 Attack Design

3.3.1 GPS spoofing attack. In general, a flying drone that encounters problems such as loss of control and loss of GPS signal from the RC or sudden GPS coordinate changes will often land at its current location due to the problem. We will take advantage of the vulnerability of the no-fly zone, known as Geofenced zones, to force the drone to land immediately. A no-fly zone is an area of airspace where civilian drones are not allowed to fly. For military areas, modern drones have built-in maps with added no-fly zones that, in normal situations, they avoid or quickly try to leave once entered, see Figure 9.

As for the GPS spoofing attack, while the targeted drone is flying, fake GPS signals will be transmitted to indicate that the drone has entered a no-fly zone location. Using different Geofenced zones and permitted flying areas coordinates in the attacking process. Due to the tendency of attackers to try different fake GPS locations till they succeed with their GPS spoofing attack since not all drones are built and programmed in the same way. For instance, an attack using a certain no-fly zone, such as an authorization zone, might land a drone but not another, thus all scenarios will be tested to verify the efficiency of an attack. In addition, attacking using different no-fly zones widens the possibility of success considering that some drones have unlocked some Geofenced zones. A detailed flowchart of the attack generation and the drone behaviour during the GPS spoofing attack is illustrated in Figure 10.

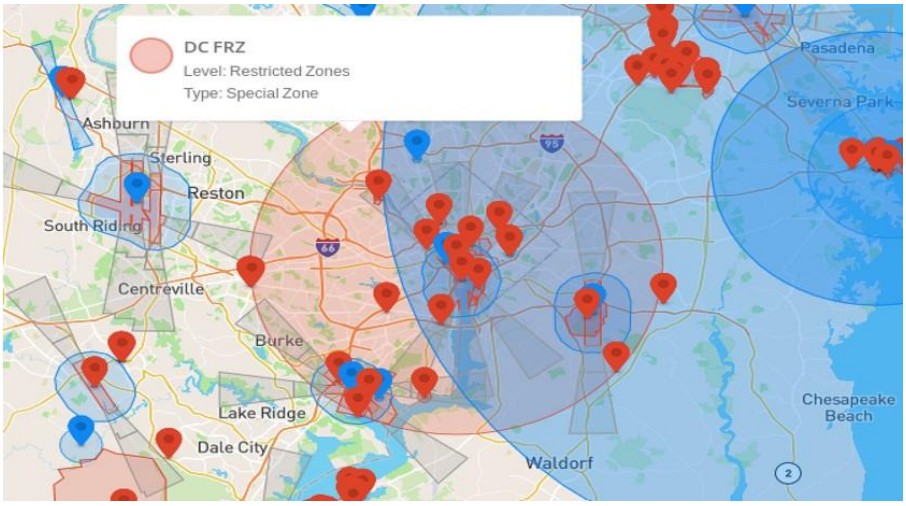


Figure 9. A screenshot of the Fly Safe Geo Zone Map

("Geo zone map - Fly safe - DJI," n.d.)

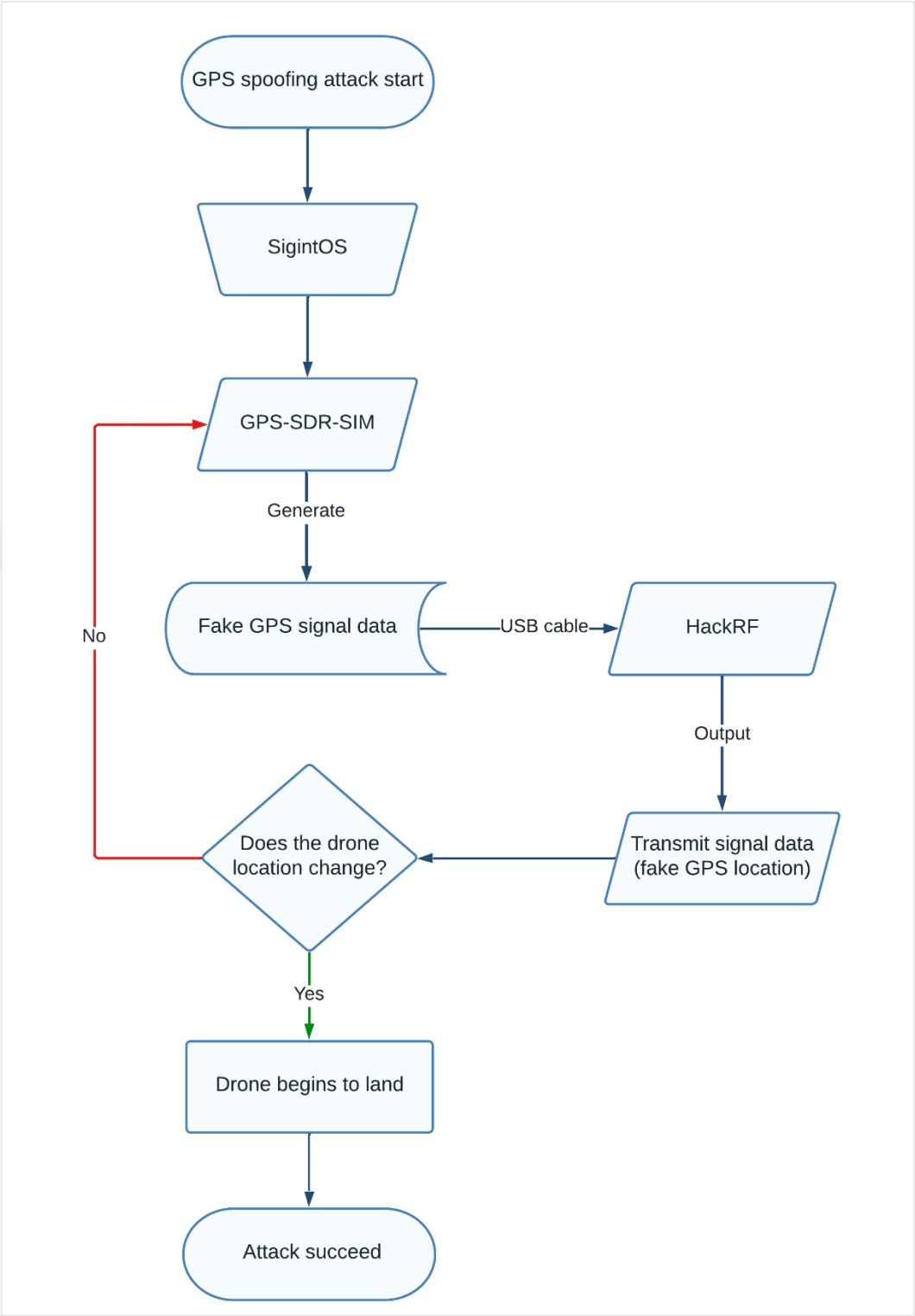


Figure 10. GPS spoofing attack flowchart.

3.3.2 GPS jamming attack. GNSS receivers in drones can be particularly vulnerable to external sources of interference. In open areas, signals from jammers can spread over much longer distances than they can on land from being obstructed. Jamming is a type of signal attack that will be implemented on the drones, forcing them to land by jamming their signals, blocking the transfer of stream materials from the drone to the operator, and making the drone operator completely lose control over the drone. A flowchart of the attack generation and the drone behaviour during the GPS jamming attack is illustrated in Figure 11.

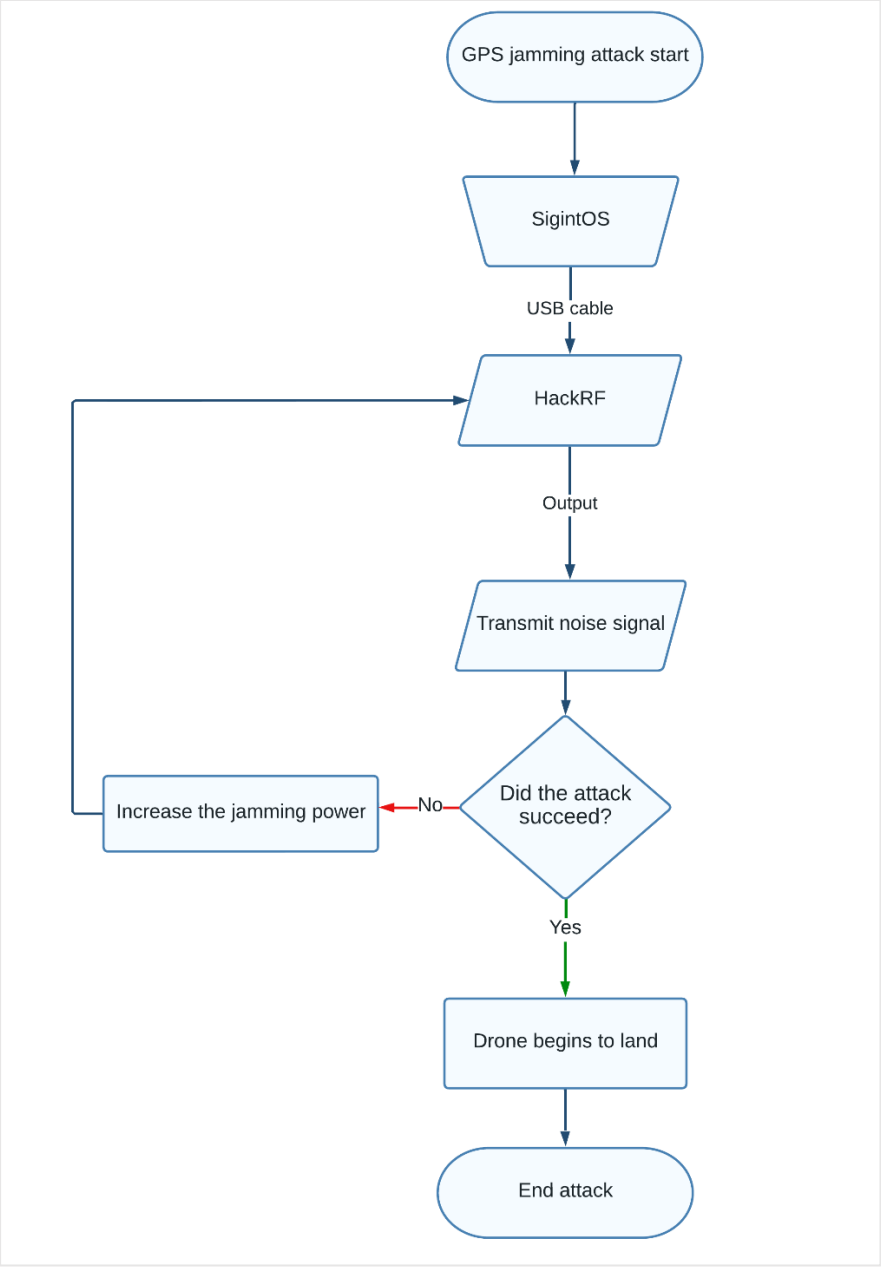


Figure 11. GPS jamming attack flowchart.

3.3.3 Experiment flight route. Figure 12 shows the drones planned route for the experiments. A flight route that is made up of a series of four waypoints described in GPS coordinates is set to be followed throughout the experiments.

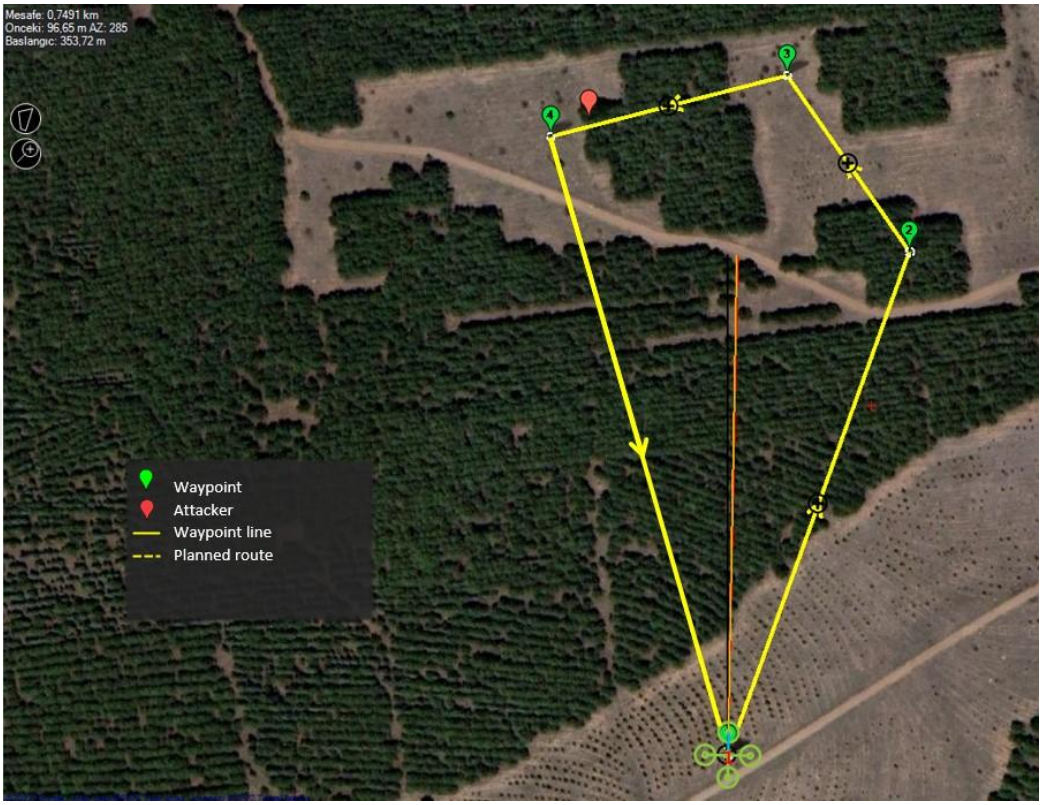


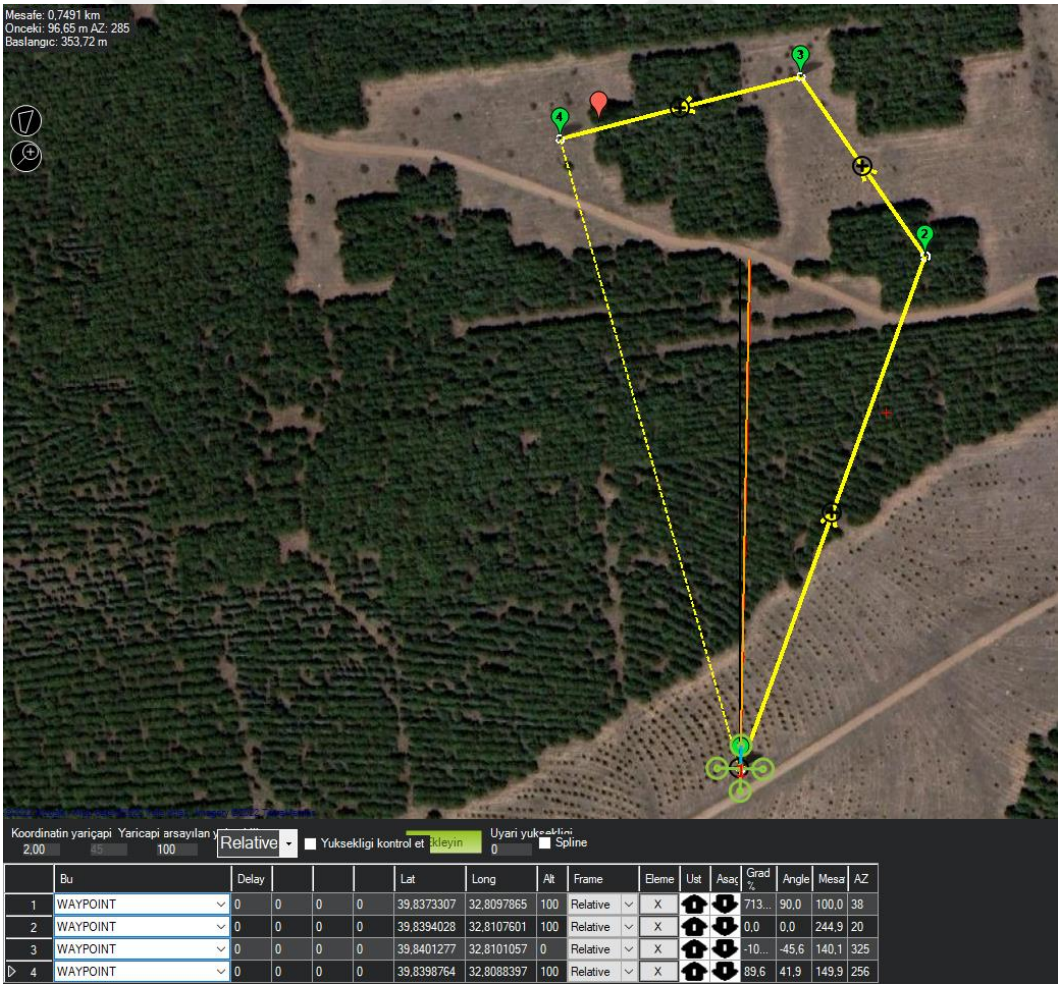
Figure 12. Planned drone flight route using Mission Planner.

3.4 Developed Solution Design: Return-to-Start Point Function (Tale)

As the drone Tale starts flying, it continuously synchronizes the GPS coordinates in real-time and records the distance and direction taken by the GPS in its memory. As soon as a GPS jamming or GPS spoofing attack occurs, it turns off the GPS function and returns using the direction and distance it has previously stored. Most importantly reaching the point where it started independently from any signal control, using its unique autopilot code.

Tale was developed to record the direction changes at 90 and 45-degree angles (y,x,z) according to the device orientation and motion. Where if it flew 10 m/min south(-z) for 10 minutes, it would fly back 10 m/min for 10 minutes in the north direction (z) right after the loss of its original signal.

Tale system benefits from the easy integration and communication that can be established between PX4 autopilot, and the ground station Mission Planner as previously mentioned. Tale sensors including the GPS work all together to calculate and compute the needed data and with the use of the flight control board (PIXHAWK PX4), it provides the latitude, longitude, altitude, the angles between the waypoints, and the distance between the waypoints as well. Sending the computed data to the Raspberry Pi computer, it stores it and communicates it with the Mission Planner. Figure 13 shows a screenshot from Mission planner, displaying some of the computed data that Tale drone utilizes in its Return-to-Start Point function. In the situation of a GPS spoofing or jamming attack, Tale disconnects the communication signal between it and between the satellite, while also disconnecting the communication signal between it and between the ground control station. Tale's recovery solution depends only on the previously saved data to make its way back to the start point.



	Bu	Delay				Lat	Long	Alt	Frame	Eleme	Ust	Asag	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 13 Mission Planner data received from Tale drone.

3.4.1 Solution working mechanism. Tale drone Return-to-Start Point function depends on the Alternate Angles Theorem using the compass to save its flight route on the map since relying on the GPS coordinates will not be sufficient in case of jamming and spoofing attacks. For instance, if the drone has received a fake GPS attack, the coordinates change, as a result, the drone can no longer depend on the same coordinates.

Whereas DJI Mavic Air 2 drone depends on GPS coordinates to utilize its RTH function, which renders it vulnerable to attacks since the GPS coordinates would be deemed invaluable in the event of a continuous GPS attack. As will be observed in the Experiment Design and Results chapter, as a result, it was concluded that the DJI drone lacks a mechanism to counter such GPS navigational attacks. The flowchart of the developed solution is shown in Figure 14.

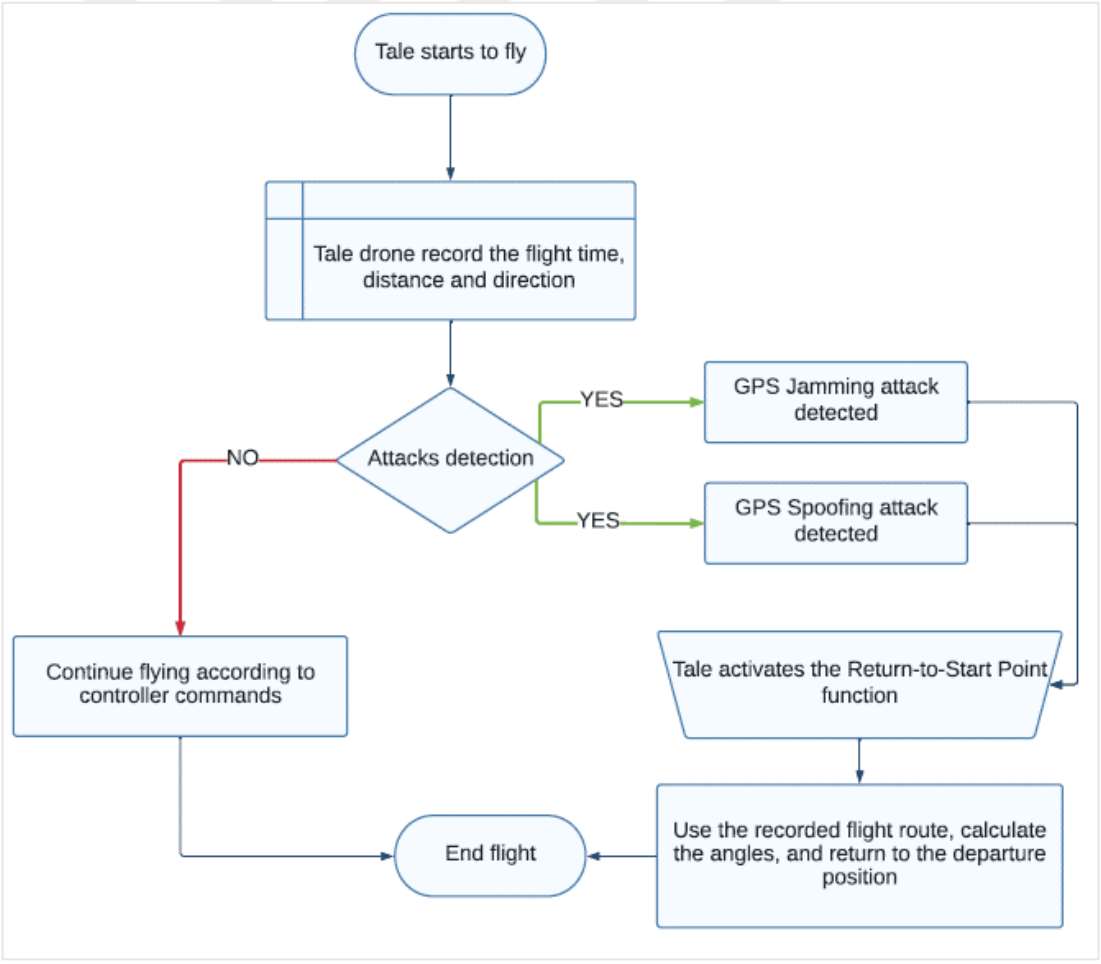


Figure 14. Tale solution design flowchart.

3.4.2 Attack detection method.

Tale technique for detecting spoofing attacks is based on phase delay measurements. The detection thresholds for spoofing are defined. When three to six GPS signals are received, the effectiveness and reliability of this method are measured in terms of the probability of false alarm and the probability of counterfeit signal detection. Tale exhibited a high probability of spoofing detection that of 99 percent through several experiments whenever the carrier-to-noise ratio is at least 43 dBHz. While for other specific attacks such as jamming, when the signal-to-noise ratio is high, the attack signal detection is expected to be at least 56 dB.

Spoofing may be detected by determining if the phase delay differences between various GPS signals and the original signal are below the defined threshold. The probability of spoofing detection becomes greater when combined with selecting accurate thresholds that are inclusive of potential phase delays. While the probability of false alarm, or inaccurate detection, may be present in different situations such as the GPS module receiving physical damage, the presence of a GPS transmitter and receiver satellite dish nearby, and if all the phase delay differences of legitimate satellite signals received are below than the set threshold. The flowchart of the developed detection method is in Figure 15.

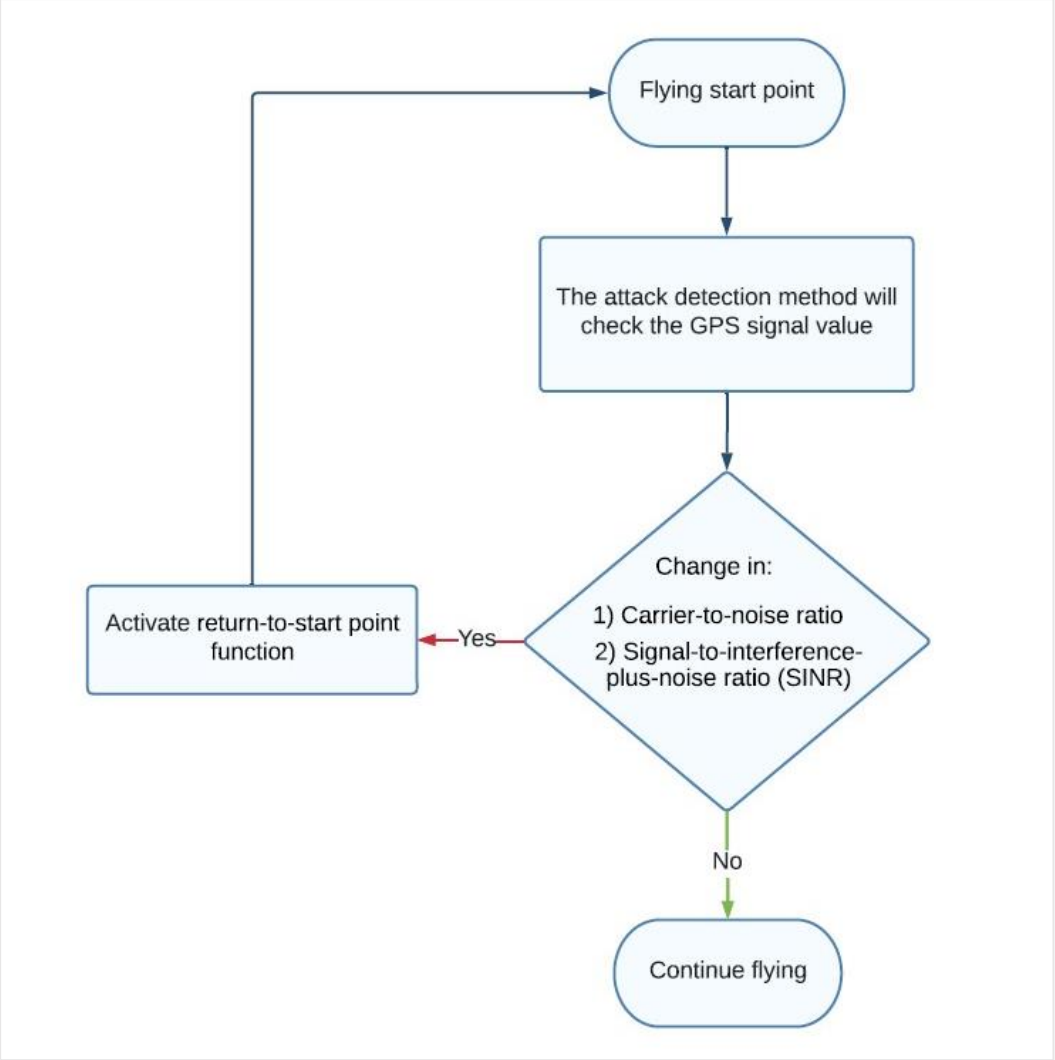


Figure 15 Tale GPS attack detection method flowchart.

Chapter 4

Experiment Design and Results

In this section, two experiments on GPS navigation attacks were designed, implemented, and studied. Also, their results are discussed.

4.1 Experiment No.1: GPS Navigational Attacks on DJI Mavic Air 2

4.1.1 GPS spoofing attack implementation. The DJI drone was attacked for two minutes throughout the attack test. During that time, the victim notices a sudden change in the GPS location, which simply indicates a fake GPS location. Several observations have shown that the drone landed when the attack started. The attack, using HackRF, produced a high number of satellite signals with the help of a highly effective transmitting antenna. In the experiment, producing fake GPS signals, it was observed how the drone reacted at every stage of the attack for different GEO Zones. Such as Restricted Zones, Altitude Zones, and Authorization Zones. These experiments were designed to be carried out for specific time intervals of attacking and stopping time between them. This was done to examine the behaviour of a drone during the attack and after it. Figure 16 was retrieved from “DJI Fly” application, as it shows the real location of the drone, before any attack occurred, in the before attack phase of the experiment.

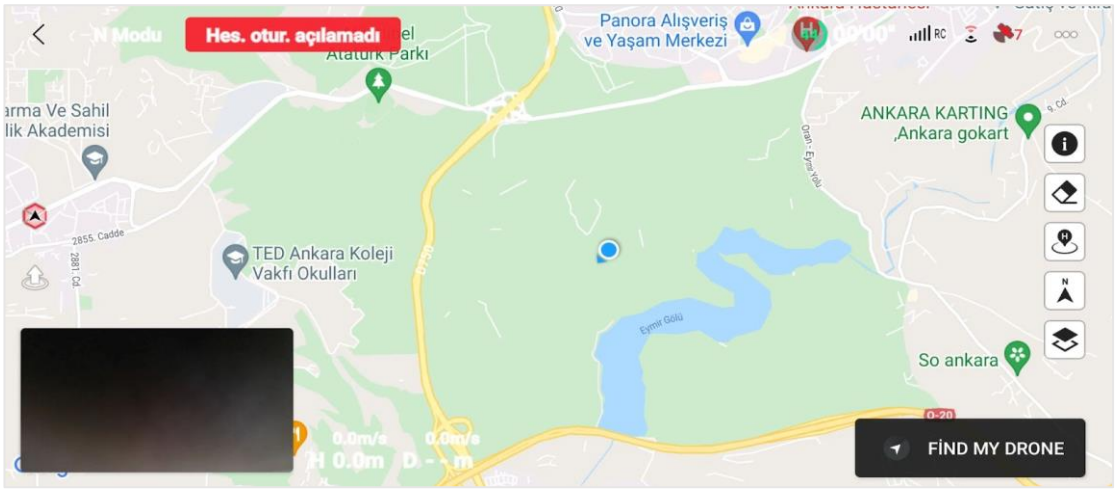


Figure 16. DJI drone real location.

In figure 17 we can see that the GPS spoofing attack has started. At this stage, three different experiments were carried out.

Figure 17. GPS spoofing attack on DJI Mavic Air 2.

Table 4

GPS Spoofing Attack Parameters

Experiment Phases	Before Attack	During Attack	After Attack
Observation Duration	-	0 s – 15 s	15 s – 30 s
Total Observation Time	30 seconds		

For the first experiment, the GPS spoofing attack was started by transmitting fake GPS coordinates for a permitted flying area for fifteen seconds, and as a result, the drone could not be controlled by its user for the duration of the attack. Although it was observed that after the fifteen-second attack has ended, the drone control was resumed normally.

For the second experiment, the GPS spoofing attack location that was transmitted was one of an Authorization Zone. As a result, a warning was prompted for the drone user to leave the area within thirty seconds. For the duration of fifteen 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 observed fifteen seconds the communication was re-established, and it was allowed to leave the area.

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

Figure 18 shows the signal analysis during the GPS spoofing attack phase, which was performed using SDRSharp software, where the peak indicates the start of the attack.

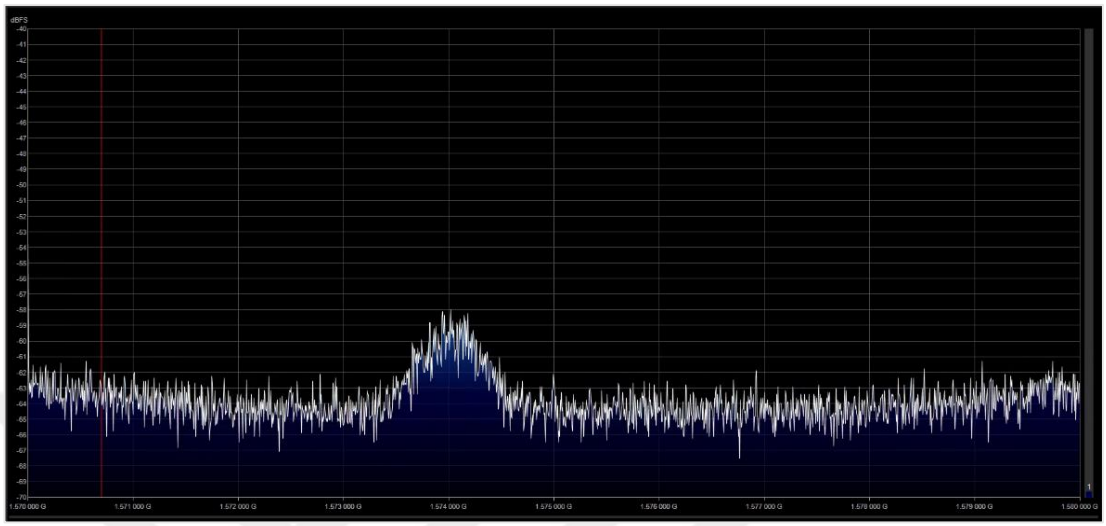


Figure 18. GPS spoofing attack signal analysis

Figure 19 Shows the change of DJI drone location due to the GPS spoofing attack in the second phase of the expedient, more precisely, it shows how fake GPS signals manipulate a target receiver's position.

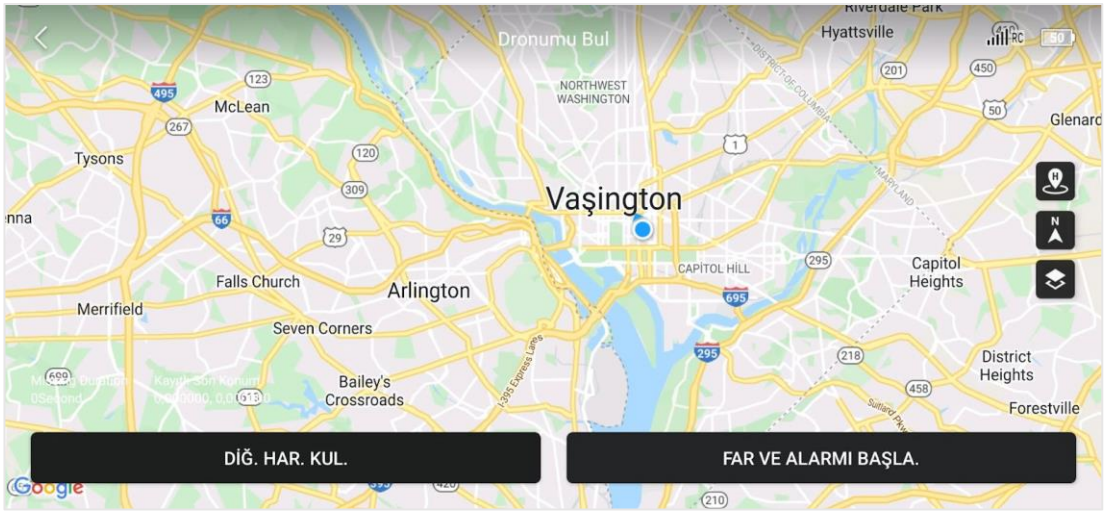


Figure 19. DJI drone location during the GPS spoofing attack.

4.1.2 GPS jamming attack implementation. After the GPS jamming attack started, the attack continued without interruption. It was observed how the drone reacted to the jamming attacks that were launched at different times and different lengths. These experiments observed how the drone responded over that period of time. Figure 20 shows that the jamming attack has started. At this stage, four different experiments were performed. Table 5 clarifies the attack time intervals.

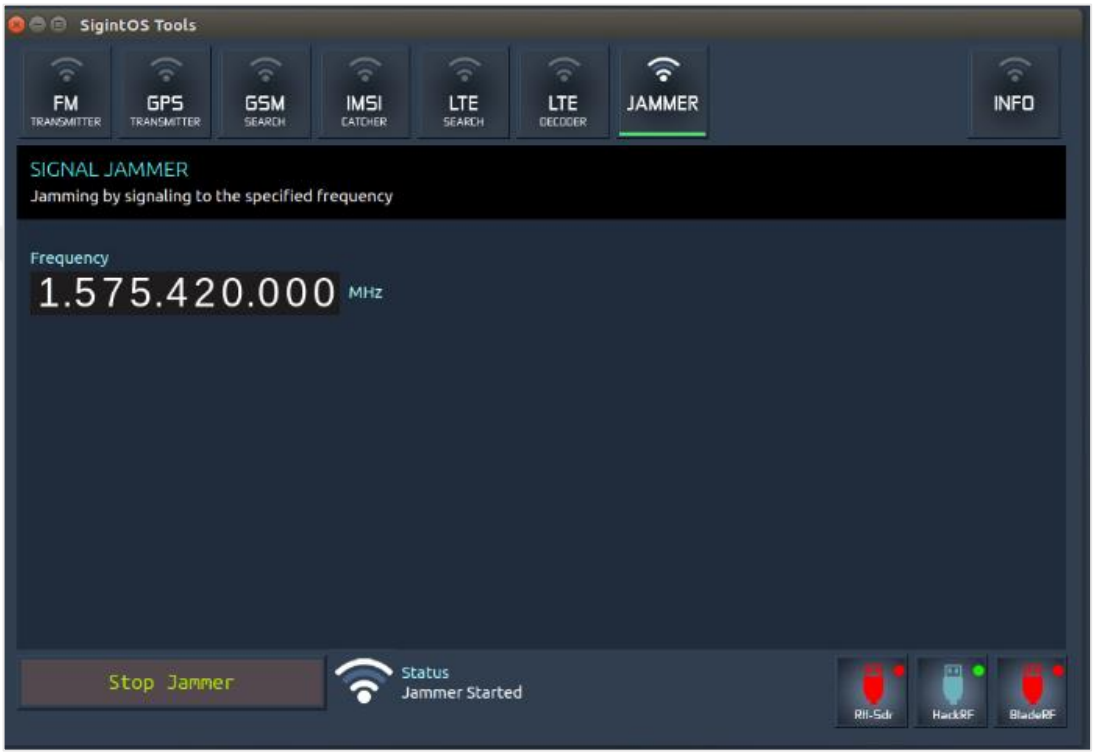


Figure 20. GPS jamming attack on DJI Mavic Air 2.

Table 5

GPS Jamming Attack Time Intervals

Experiment No.	Expt. 1	Expt. 2	Expt. 3	Expt. 4
Attack Time	3 sec	5 sec	10 sec	3 min
Stopping Time	2 sec	5 sec	10 sec	-
Loop Time	3 min	3 min	3 min	-
Total Observation Time	3 min	3 min	3 min	3 min

For the first experiment, a GPS jamming attack was initiated every three seconds and stopped for two seconds, for a total of three minutes. During the three-second interval, the signal between the drone and the controller was always blocked, where the drone remained to hover stable since it lost its communication. For the two seconds intervals where the attack stopped, it was seen that the drone was continuously seeking to reconnect with its user, sometimes failing and others succeeding. During the times the drone reconnected in the two seconds, the user was able to move the drone, but it was instantly stopped again by the coming attack interval.

For the second experiment, the jamming attack was initiated every five seconds and stopped for five seconds, for a total of three minutes. It was observed that the drone stopped its flight movement and remained to hover stably every five seconds interval where it was attacked just like in the first experiment, but for the five seconds interval where the attack stopped the drone succeed to regain its connection with the user.

For the third experiment, the jamming attack was initiated every ten seconds and stopped for ten seconds, for a total of three minutes. Due to that, the drone landed in the area it was in within the ten seconds attack interval, whereas in the ten seconds of stopping the attack interval, the drone was able to regain its connection with the user and continue flying again.

For the fourth experiment, after the jamming attack that started and continued without stopping, it was seen that the drone landed in the area it was in and found due to it completely losing its communication signal.

4.1.3 Results. From the previous implementation of GPS jamming and GPS spoofing attacks experiments on the DJI drone. The drone behaviour and how it reacts were observed and studied throughout the different attack phases.

In short, because of the GPS spoofing attack, where fake GPS coordinates are broadcasted to the targeted drone, it was observed that the DJI drone generally cannot escape from this attack in different GEO Zones since it loses its signal and control during the attack time.

Furthermore, it was also observed that the return-to-home function did not do much protection for the DJI drone since it was forced to land the moment it lost its GPS signal whenever an attack continuously lasted for approximately 10 seconds or more.

Moreover, when the GPS Jamming attack continued for certain intervals over the drone such as in experiments one and two, it was observed that the communication was not interrupted immediately, but after it got interrupted the communication between the drone and the controller was made to be delayed.

To sum up, it proved that the precautions taken by DJI for GPS jamming and spoofing attacks do not work against spoofing and continuous jamming attacks due to the signal control being completely blocked and lost.

4.2 Experiment No.2: GPS Navigational Attacks on Tale

4.2.1 GPS spoofing attack implementation. In the experiment conducted, the fake GPS signals were transmitted in the launched attack. How the drone reacted at different stages for different GEO Zones, such as Restricted Zones, Altitude Zones, and Authorization Zones, were observed similarly to what was done in the first experiment. Figure 21 shows that the GPS spoofing attack has started. At this stage, three different experiments were carried out.

Figure 21. GPS spoofing attack on Tale.

In the first experiment, the GPS spoofing attack was started by transmitting fake GPS coordinates for a permitted flying area. As a result, the drone signal was lost in its first seconds, and it could not regain its connection with its user. Nonetheless, the drone returned to its start location according to the Return-to-Start Point function from the moment it received the attack.

In the second experiment, the fake GPS attack location was established to be an Authorization Zone, consequently, the communication signal was abruptly cut, and the drone returned to the flying position from where it had started, as in the first experiment.

In the third experiment, Restricted Zone GPS coordinates were transmitted in the fake GPS attack. As a result, as in previous experiments, the signal was disconnected without warning and the drone returned to the point it started flying from.

4.2.2 GPS jamming attack implementation. In this experiment, how the drone responded and reacted over time to the jamming attacks that were delivered at various periods and durations was observed. Figure 22 was retrieved from “Mission Planner” software, it shows the real location of the drone before any attack occurred.

Figure 22. Real location of Tale Drone.

Figure 23 shows that the jamming attack has started. At this stage, three different experiments were performed.

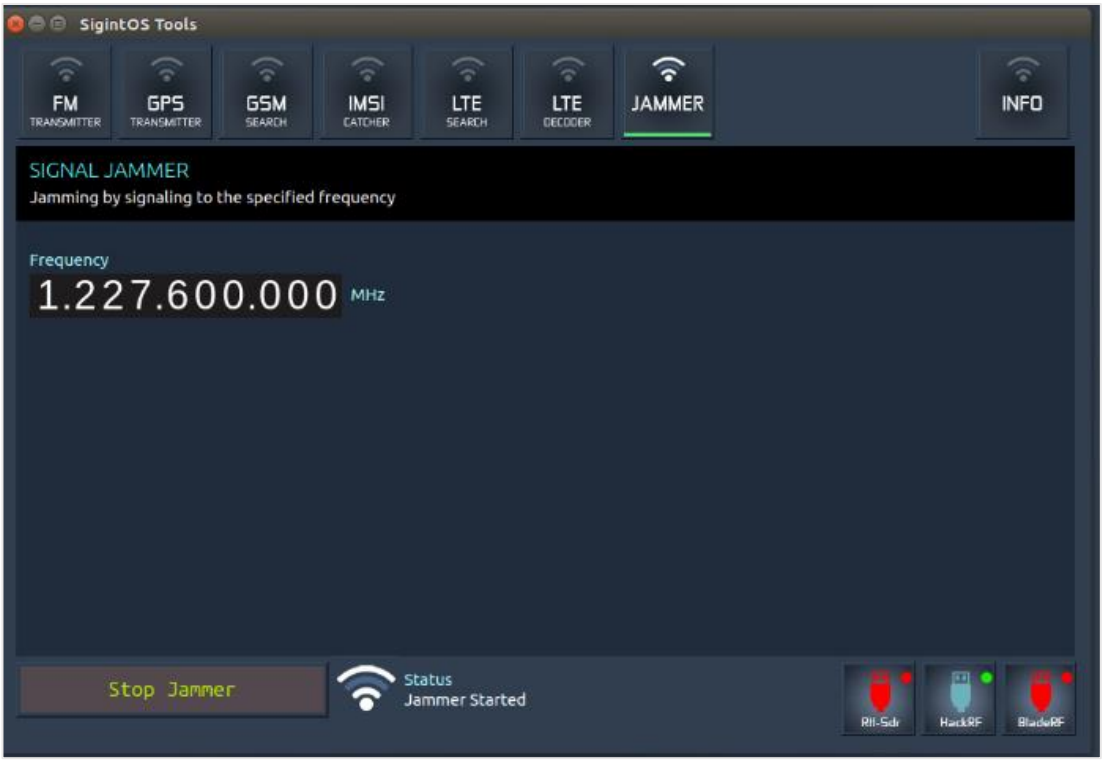


Figure 23. GPS jamming attack on Tale.

For the first experiment, the same scenario of initiating a GPS jamming attack every three seconds and stopping it for two seconds, for a total of three minutes was intended to be followed, however, the drone signal was almost immediately cut when it received the attack. Even though the attack had a duration of where it stopped, Tale couldn't regain its communication signal with its user. the drone returned to the flying position from where it had started.

For the second experiment, the GPS jamming attack was initiated every five seconds and stopped for five seconds, for a total of three minutes, whereas in the third experiment an attack was initiated every ten seconds and stopped for ten seconds, for a total of three minutes. However, in both scenarios, as previously happened in the first experiment, Tale couldn't regain its signal and returned to the flying position from where it had started.

For the fourth experiment, after launching a continuous jamming attack, Tale also once again lost its communication signal with its user and flew right back to the starting position.

Figure 24 shows the signal analysis during the GPS jamming attack, that was performed using SDRSharp software, where peaks show the effect of noise generated from the attack

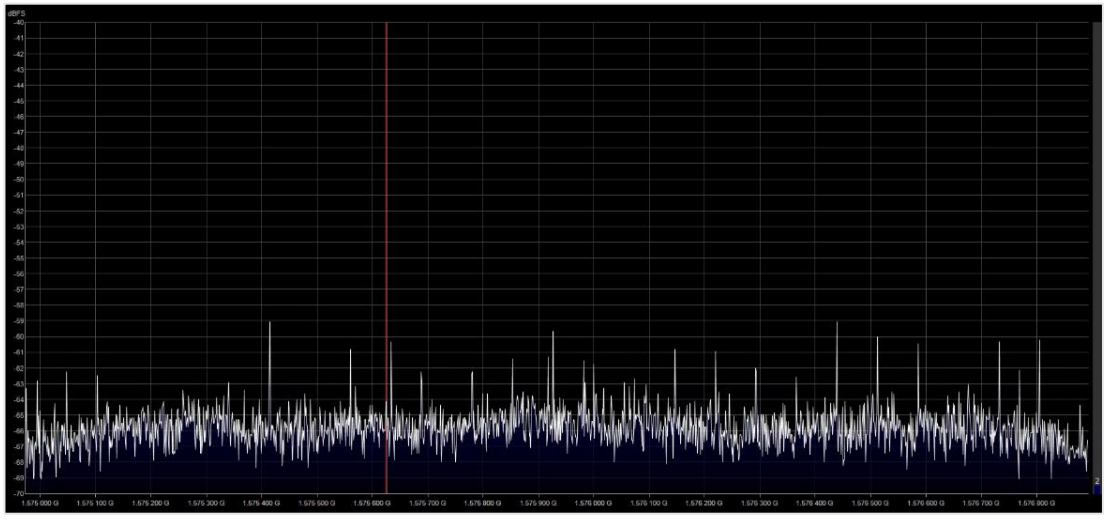


Figure 24. GPS jamming attack signal analysis

Figure 25 shows how Tale reacted to the GPS jamming attack using the Return-to-Start Point function.

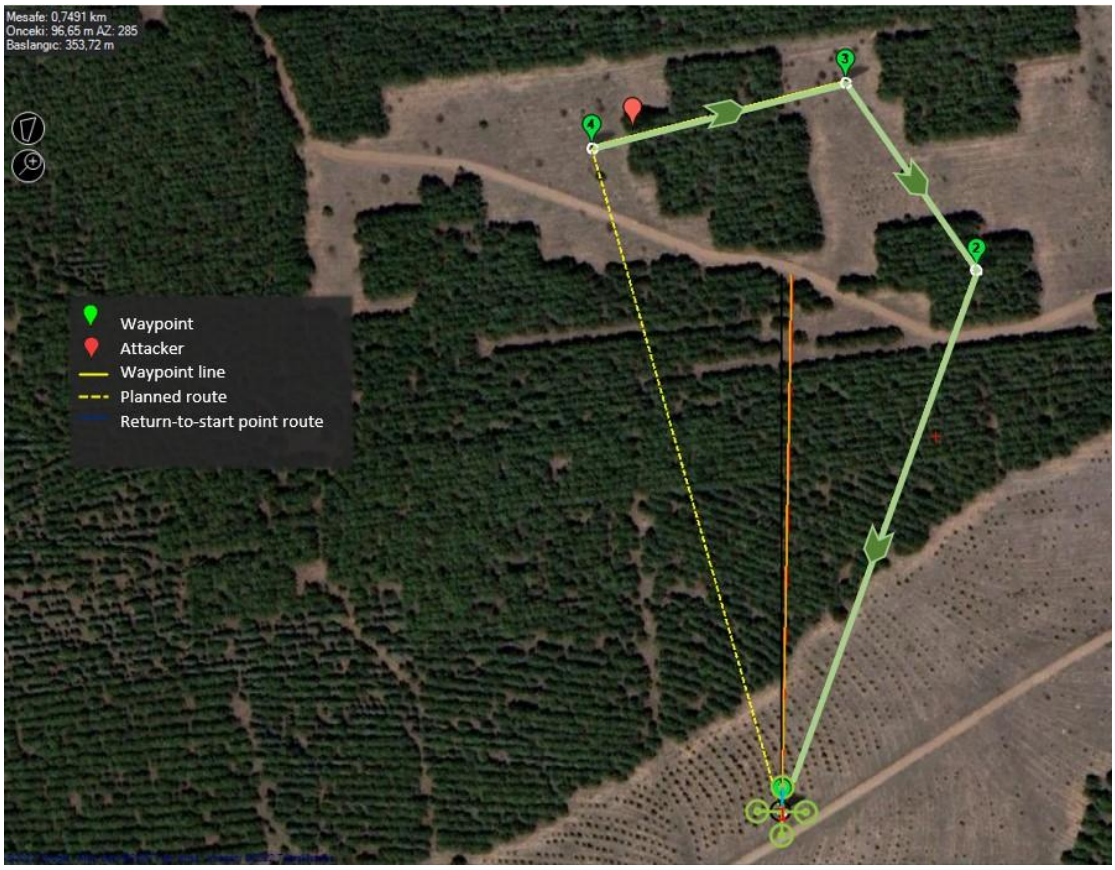


Figure 25. Tale drone Return-to-Start Point function.

4.2.3 Results. From the previous implementation of GPS jamming and GPS spoofing attacks experiments on Tale drone. Throughout the various attack stages, the drone's behaviour and reaction were observed and examined.

Firstly, for the GPS spoofing attack, it was observed that the Tale drone reacted identically to the different attacks of 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. Making its way back to the starting position only relying on the built-in Return-to-Start Point function

Secondly, for the GPS Jamming attack, it was observed that in the case of a continuous stream of jamming attacks, Tale will not be affected any differently than in the case of a single jamming attack. Since it loses its control signal and blocks the connection as soon as it senses an attack, till it reaches the flight starting location

relying on the Return-to-Start Point function, thus the number of the received attacks doesn't make a difference against Tale. Along with it, it should be noted that, once Tale's connection is interrupted, the connection could not be established till it reaches the start point again.

4.3 Discussion of Experiment Results

This section provides a comparison between the two performed experiments. First, the GPS navigational attacks on DJI Mavic Air 2, and second, the GPS navigational attacks on Tale. Focusing on the behavior of DJI Mavic Air 2 return-to-home function against GPS attacks and the behavior of Tale return-to-start point function against GPS attacks as the main points of comparison.

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 DJI Mavic Air 2 drone software prevent the DJI drone from flying in those GEO zones, mostly giving a short warning, or forcing it to land at its current location.

Whereas, 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. Which leads Tale to return to the point of departure, by turning off the GPS module and cutting the signal communication. This way it could be said that it is also acting as its own jammer, only depending on its return-to-start point function.

As a result of the signal attacks on the DJI Mavic Air 2 and Tale, we can conclude that on one hand, the attacks affected the DJI drone in different ways. When the attacks were performed and were stopped in some cases, the communication was restored between the controller and the drone and it was able to use its Return-to-Home function, but in other cases, the drone was more vulnerable to different attacks and the attacker was able to land the drone. On the other hand, no matter what type of navigation attack Tale received, when responding to one, it returned to the point of departure without using signal communication, solely depending on the Return-to-Start Point function.

Differing from the DJI drone, if the attack has stopped on the Tale drone, the communication between the controller and the drone will not be restored. Also, a new

signal communication request cannot be established since Tale already had cut off the signal communication. In such cases, the drone will return to the point where it took off, and then it can be restarted and used again.

It was concluded that the Tale drone was able to detect and recover from the GPS signal attacks, ultimately evading being captured, but was negatively affected because of the time loss that was spent during the return-to-start point function, due to the signal communication being completely cut off.

Lastly, Table 6 below summarizes the difference between the two experimental results and how each drone reacted to the GPS navigational attacks.

Table 6

Comparison Between DJI Mavic Air 2 and Tale Drone

Comparison Points	DJI Mavic Air 2 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-Home Function	Activated in response to attacks	-
Return-To-Start Point Function	-	Activated in response to attacks
GPS Related Vulnerability	Depends on the GPS connection in its return-to-home function. Thus, vulnerable to GPS attacks.	-
Loss of Signal Communication After an Attack	No	Yes

Table 6 (cont.d)

Comparison Points	DJI Mavic Air 2 Drone	Tale Drone
Depending On GPS Communication in Flight Mode	Yes	Yes
Depending On GPS Communication in Returning to start point	Yes	No
Returning Possibility	Low	High

Chapter 5

Conclusion and Future Work

In this thesis, we introduced the well-known DJI Mavic Air 2 drone as well as the Tale drone which was developed as a solution to counter the effect of navigational attacks on drones, as Tale provides a detection and recovery mechanism from GPS spoofing attacks.

Based on the findings of this thesis attacks experiments, it was concluded that drones have security vulnerabilities regarding GPS communication thus they are prone to GPS jamming and GPS spoofing attacks. Thus, a solution was proposed and tested, and evaluated.

Tale drone solution design covers the vulnerability of the weak GPS signals communication and ensures that a drone recovers from GPS jamming and spoofing attacks making it infallible to control or destroy. It also, ensures that the drone is protected against any new future attacks based on signals communication, and prevents property theft and privacy violation.

Two distinct types of signal attacks have been discussed, an attack design has been set, and an experiment has been conducted, demonstrated, and analyzed in terms of hardware and software platforms on these two drones. The attack framework was mainly created and performed to assess the drones' reaction and how do they behave in a critical condition such as a signal blockage.

To bring things together, and upon analyzing the facts, a comparison between the DJI Mavic Air 2 return-to-home function against GPS attacks and between Tale return-to-start point function against GPS attacks was conducted and presented.

The limitations of the study that provides an opportunity for future work are:

- As Tale drone cuts off its communication signal, and once the threat has passed, no signal reaches the drone till it goes back to the starting point.
- If the battery is not enough for the returning distance, the drone will drop since it exhausts its battery on the return path.

REFERENCES

3DR Pixhawk 1 · PX4 v1.9.0 user guide. (2020, October 28). Retrieved June 11, 2022, from https://docs.px4.io/v1.9.0/en/flight_controller/pixhawk.html

A. P. Melikhova and I. A. Tsikin, "Optimum Array Processing with Unknown Attitude Parameters for GNSS Anti-Spoofing Integrity Monitoring," 2018 41st International Conference on Telecommunications and Signal Processing (TSP), 2018, pp. 1-4.

A. Shafique, A. Mehmood and M. Elhadef, "Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models," in IEEE Access, vol. 9, pp. 93803-93815, 2021.

Abdelfatah, W., Georgy, J., Iqbal, U., & Noureldin, A. (2011). FPGA-Based Real-Time Embedded System for RISS/GPS Integrated Navigation. Sensors, 12(1), 115-147. doi:10.3390/s120100115

About: Meaconing. (n.d.). Retrieved May 26, 2022, from dbpedia.org website: https://dbpedia.org/page/Meaconing

ArduPilot documentation — ArduPilot documentation. (2022, June 16). Retrieved June 17, 2022, from https://ardupilot.org/ardupilot/

Arteaga, S. P., Hernandez, L. A. M., Perez, G. S., Orozco, A. L. S., & Villalba, L. J. G. (2019). Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo. IEEE Access, 7, 51782–51789. https://doi.org/10.1109/access.2019.2911526

Arteaga, S. P., Hernandez, L. A., Perez, G. S., Orozco, A. L., & Villalba, L. J. (2019). Analysis of the GPS spoofing vulnerability in the drone 3DR solo. IEEE Access, 7, 51782-51789. doi:10.1109/access.2019.

B. Bera, M. Wazid, A. K. Das and J. J. P. C. Rodrigues, "Securing Internet of Drones Networks Using AI-Envisioned Smart-Contract-Based Blockchain," in IEEE Internet of Things Magazine, vol. 4, no. 4, pp. 68-73, December 2021.

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. https://doi.org/10.1002/rob.20400

BEST COMMERCIAL DRONES & PROFESSIONAL DRONES OF 2022 (NEW GUIDE). (n.d.). Retrieved May 26, 2022, from www.flyability.com website: https://www.flyability.com/commercial-drones

Brown, J. (2020, February 22). Types of Military Drones: The Best Technology Available Today. Retrieved from My Drone Lab website: https://www.mydronelab.com/blog/types-of-military-drones.html

Cast, N. (2021, October 3). How Drones Communicate With the Controller? Retrieved May 25, 2022, from Remoteflyer website: https://www.remoteflyer.com/how-drones-communicate-with-the-controller/#h-communication-between-the-drone-and-controller

Castrillo, V. U., Manco, A., Pascarella, D., & Gigante, G. (2022). A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones. Drones, 6(3), 65.

Category. (n.d.). Retrieved from https://www.ni.com/en-tr/shop/hardware/software-defined-radios-category.html#

Ciobanu, E. (2020, November 21). What Are GPS Drones, and Why Does It Matter. Retrieved from Droneblog website: https://www.droneblog.com/what-are-gps-drones-and-why-does-it-matter/#:~:text=GPS%20drones%20are%20equipped%20with

Ciobanu, E. (2020, November 21). What are GPS drones, and why does it matter. Retrieved from https://www.droneblog.com/what-are-gps-drones-and-why-does-it-matter/#how-it-works

CUAV. (n.d.). CUAV P9 radio drone telemetry | High power high speed ultra-vision UAV data link communication module. Retrieved from https://store.cuav.net/shop/p9

Cyber security threat analysis and attack simulation for unmanned aerial vehicle network. (1, 1). Retrieved from https://www.semanticscholar.org/paper/Cyber-security-threat-analysis-and-attack-for Javaid/dcef4aaabd40e78bdaa73b2746df2c8f5d9710e9

D. He et al., "A Friendly and Low-Cost Technique for Capturing Non-Cooperative Civilian Unmanned Aerial Vehicles," in IEEE Network, vol. 33, no. 2, pp. 146-151, March/April 2019.

Dana, P. (1997). Global Positioning System (GPS) Time Dissemination for Real-Time Applications. Real-Time Systems, 12, 9–40. Retrieved from http://www.pdana.com/PHDWWW_files/Rtgps.pdf

DEF CON 25 - David Robinson - Using GPS Spoofing to control time. (2019, October 5). Retrieved May 26, 2022, from www.youtube.com website: https://www.youtube.com/watch?v=CRXVEdJtYgg

DOD Dictionary of Military and Associated Terms (June 2018). (2018, June 1). Retrieved May 25, 2022, from www.hsdl.org website: https://www.hsdl.org/?abstract&did=813130

Doole, G. (2020). Raspberry Pi 4 Pinout, Features and Peripherals. Retrieved 11 June 2022, from https://microcontrollerslab.com/raspberry-pi-4-pinout-description-features-peripherals-applications/

Dronecode Foundation. (2021, March 17). PX4 System Architecture. Retrieved June 11, 2022, from https://docs.px4.io/v1.9.0/en/flight_controller/pixhawk.html

Esch, G. V., & Den Heuvel, D. V. (2021). PX4 AUTOPILOT ON A UAV CONTROLLER Flying a Xilinx ZU7EV based processing board. Retrieved from https://topic-nl.s3-eu-west-1.amazonaws.com/public/files/2021-topic-white-paper-px4-autopilot-on-a-uav-controller.pdf?v=1614169505

FAA Safety Briefing, & Federal Aviation Administration (Eds.). (2021). FAA Safety Briefing | SHARING THE SKIES SAFELY. Retrieved May 25, 2022, from Faa.gov website: https://www.faa.gov/news/safety_briefing/2021/media/MayJun2021.pdf

Fahad, E. (2021, April 2). What is LiDAR? LiDAR working, TF mini LiDAR with Arduino connection & code. Retrieved June 18, 2022, from https://www.electroniclinic.com/what-is-lidar-lidar-working-tf-mini-lidar-with-arduino-connection-code

Faria, L. D. A., Silvestre, C. A. D. M., Correia, M. A. F., & Roso, N. A. (2018). Susceptibility of GPS-dependent complex systems to spoofing. Journal of Aerospace Technology and Management, 10.

G. Aissou, H. O. Slimane, S. Benouadah and N. Kaabouch, "Tree-based Supervised Machine Learning Models For Detecting GPS Spoofing Attacks on UAS," 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2021, pp. 0649-0653.

Geo zone map - Fly safe - DJI. (n.d.). Retrieved from https://www.dji.com/flysafe/geo-map

GPS Overview. (2019). Retrieved from Gps.gov website: https://www.gps.gov/systems/gps/

Gps-sdr-sim: Software-defined GPS signal simulator. (2019, February 21). Retrieved from https://securityonline.info/gps-sdr-sim-software-defined-gps-signal-simulator/

GSMA. (2017, February). Introducing radio spectrum primer series. Retrieved from https://www.gsma.com/spectrum/wp-content/uploads/2017/04/Introducing-Radio-Spectrum.pdf

H. Alamleh and N. Roy, "Manipulating GPS Signals to Determine the Launch Location of Drones in Rescue Mode," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-5.

HackRF One - Great Scott Gadgets. (n.d.). Retrieved from greatscottgadgets.com website: https://greatscottgadgets.com/hackrf/one/

Hassanalian, M. (2018). Conceptual Design, Bioinspiration, and Multidisciplinary Analysis of Drones. New Mexico State University.

HBR. (n.d.). UMTS Frequency Bands. Retrieved from https://halberdbastion.com/technology/cellular/3g-umts/umts-frequency-bands

Höglund Gran, T., & Mickols, E. (2020). Hacking a Commercial Drone.

Horton, E., & Ranganathan, P. (2018). Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter. The Journal of Global Positioning Systems, 16(1). https://doi.org/10.1186/s41445-018-0018-3

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (2008, September). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008) (pp. 2314-2325).

I. G. Ferrão et al., "STUART: ReSilient archiTecture to dynamically manage Unmanned aeriAl vehicle networks under atTack," 2020 IEEE Symposium on Computers and Communications (ISCC), 2020, pp. 1-6.

J. Gaspar, R. Ferreira, P. Sebastião and N. Souto, "Capture of UAVs Through GPS Spoofing," 2018 Global Wireless Summit (GWS), 2018, pp. 21-26.

Javaid, A. Y. (2015). Cyber security threat analysis and attack simulation for unmanned aerial vehicle network (Doctoral dissertation, University of Toledo).

Kendoul, F. (2012). Survey of advances in guidance, navigation, and control of unmanned rotorcraft systems. Journal of Field Robotics, 29(2), 315–378. https://doi.org/10.1002/rob.20414

Koubaa, 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. doi: 10.1109/access.2019.2924410

M. Barbeau, J. Garcia-Alfaro and E. Kranakis, "Geocaching-inspired Resilient Path Planning for Drone Swarms," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2019, pp. 620-625.

M. Ceccato, F. Formaggio and S. Tomasin, "Spatial GNSS Spoofing Against Drone Swarms With Multiple Antennas and Wiener Filter," in IEEE Transactions on Signal Processing, vol. 68, pp. 5782-5794, 2020.

M. L. Psiaki, T. E. Humphreys and B. Stauffer, "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," in IEEE Spectrum, vol. 53, no. 8, pp. 26-53, August 2016.

Marco, A. D. (2020, April 3). Raspberry Pi - Sixfab 3G/4G & LTE Base HAT [Web log post]. Retrieved from https://di-marco.net/blog/it/2020-04-03-raspberry_pi_sixfab_3g_4g_lte_base_hat/

Mavic air 2. (n.d.). Retrieved from https://store.dji.com/product/mavic-air-2?site=brandsite&from=buy_now_bar&vid=91071

meaconing (US DoD Definition). (n.d.). Retrieved May 26, 2022, from www.militaryfactory.com website: https://www.militaryfactory.com/dictionary/military-terms-defined.php?term_id=3298

Nardi, T. (2020, November 28). HackRF PortaPack Firmware Spoofs All The Things. Retrieved from Hackaday website: https://hackaday.com/2020/11/28/hackrf-portapack-firmware-spoofs-all-the-things/

Parkinson, B., Spilker Jr., J., Axelrad, P., Bradford W., B., & Enge, P. (1996). Global Positioning System (Vol. 1). Washington: AIAA. Retrieved 4 9, 2022

Pixhawk. (n.d.). Open source autopilot for drones PX4 autopilot. Retrieved from https://px4.io/

PortaPack for HackRF one. (n.d.). Retrieved from https://lab401.com/products/portapack-for-hackrf-one?variant=40442957005000

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

PX4 Autopilot User Guide (master). (2021, June 9). Retrieved June 11, 2022, from https://docs.px4.io/master/en

Raspberry Pi Trading Ltd. (2019). Raspberry Pi 4 Computer Model B [Ebook]. Retrieved 11 June 2022, from https://static.raspberrypi.org/files/product-briefs/Raspberry-Pi-4-Product-Brief.pdf

Recreational Flyers & Modeler Community-Based Organizations. (2019, August 13). Retrieved from Faa.gov website: https://www.faa.gov/uas/recreational_fliers/

Recreational Use Of Drones. (n.d.). Retrieved May 25, 2022, from UAV Systems International website: https://uavsystemsinternational.com/blogs/drone-guides/recreational-use-of-drones

Review: The DJI Mavic air 2 is the best all-around drone for most people. (2020, April 30). Retrieved from https://www.dpreview.com/reviews/review-the-dji-mavic-air-2-is-the-best-all-around-drone-for-most-people

Schafer, G. (2021, April). Random Quote Board. Retrieved May 26, 2022, from www.site2241.net website: http://www.site2241.net/april2021.htm

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. https://doi.org/10.11003/JPNT.2015.4.2.057

Shashok, N. (2017). Analysis of vulnerabilities in modern unmanned aircraft systems. Tuft University, 1-10.

Shepard, D. P., & Humphreys, T. E. (2011, September). Characterization of receiver response to a spoofing attacks. In Proceedings of the 24th International

Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011) (pp. 2608-2618).

Shepard, D. P., Humphreys, T. E., & Fansler, A. A. (2012b). Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. International Journal of Critical Infrastructure Protection, 5(3-4), 146–153. https://doi.org/10.1016/j.ijcip.2012.09.003

SigintOS: Signal intelligence via a single graphical interface. (2021, December 17). Retrieved from https://resources.infosecinstitute.com/topic/sigintos-signal-intelligence-via-a-single-graphical-interface/

Sinopoli, B., Micheli, M., Donato, G., & Koo, T. J. (2001, May 1). Vision based navigation for an unmanned aerial vehicle. https://doi.org/10.1109/ROBOT.2001.932864

Sivakumar, M., & TYJ, N. M. (2021). A Literature Survey of Unmanned Aerial Vehicle Usage for Civil Applications. Journal of Aerospace Technology and Management, 13.

Sixfab. (n.d.). Raspberry Pi 3G/4G-LTE base HAT. Retrieved June 11, 2022, from https://sixfab.com/product/raspberry-pi-base-hat-3g-4g-lte-minipcie-cards

Space Segment. (2019). Retrieved from Gps.gov website: https://www.gps.gov/systems/gps/space/

TerrisGPS. (n.d.). USING UAV GPS. Retrieved from TerrisGPS website: http://www.terrisgps.com/how-is-gps-used-in-uav/

Testing the Mayhem Firmware on a HackRF Portapack. (2020, December 3). Retrieved May 26, 2022, from rtl-sdr.com website: https://www.rtl-sdr.com/testing-the-mayhem-firmware-on-a-hackrf-portapack/

U-Blox. (n.d.). NEO-M8 u-blox M8 concurrent GNSS modules DataSheet. Retrieved from https://content.u-blox.com/sites/default/files/NEO-M8-FW3_DataSheet_UBX-15031086.pdf

Velodyne Lidar, Inc. (2022, February 2). What is LiDAR? Learn how LiDAR works. Retrieved from https://velodynelidar.com/what-is-lidar/

Watts, A. C., Ambrosia, V. G., & Hinkley, E. A. (2012). Unmanned Aircraft Systems in Remote Sensing and Scientific Research: Classification and Considerations of Use. Remote Sensing, 4(6), 1671–1692. https://doi.org/10.3390/rs4061671

Westover, B. (2021, May 28). Raspberry Pi 4 model B review. Retrieved from https://www.tomsguide.com/reviews/raspberry-pi-4-model-b

What is GNSS? (2016, March 1). Retrieved from www.euspa.europa.eu website: https://www.euspa.europa.eu/european-space/eu-space-programme/what-gnss

What is GPS spoofing? (2020, August 25). Retrieved May 26, 2022, from McAfee Blog website: https://www.mcafee.com/blogs/internet-security/what-is-gps-spoofing/#:~:text=GPS%20Spoofing%20101&text=GPS%20spoofing%20happens%20when%20someone

What is SDR and what can you do with SDR? (2020, May 25). Retrieved from Latest open tech from seeed studio website: https://www.seeedstudio.com/blog/2020/05/25/what-is-sdr-and-what-can-you-do-with-sdr/

What is spoofing and how to ensure GPS security? (n.d.). Retrieved May 26, 2022, from www.septentrio.com website: https://www.septentrio.com/en/learn-more/insights/what-spoofing-and-how-ensure-gps-security#:~:text=Types%20of%20Spoofing&text=There%20are%20two%20ways%20of

Wigmore, I. (2013, December). What is personal drone? - Definition from WhatIs.com. Retrieved May 25, 2022, from WhatIs.com website: https://www.techtarget.com/whatis/definition/personal-drone

Woodman, & J., O. (2007). An introduction to inertial navigation. Cambridge: University of Cambridge, Computer Laboratory. doi:10.48456/tr-696

Z. Feng et al., "Efficient drone hijacking detection using onboard motion sensors," Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017, 2017, pp. 1414-1419.