UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Santiago Andres Sarmiento Bernal

Detection solution analysis for simplistic spoofing attacks in commercial mini and micro UAVs

Master's Thesis (30 EAP)

Supervisor: Olaf Manuel Maennel, Ph.D.

Co-supervisor: Raimundas Matulevičius, Ph.D.

Tartu 2016

Detection solution analysis for simplistic spoofing attacks in commercial mini and micro UAVs

Most of UAVs are GPS navigation based aircrafts that rely on a system with lack of security, their latent risk against malicious attacks has been raised with the recent progress and development in SDRs and GNSS simulation software, facilitating to amateurs the accessibility of equipment with spoofing capabilities. The attacks which can be done with this setup belong to the category simplistic, however, during this thesis work there are validated different cases of successful results under certain GPS receivers' state or configuration.

This work analysis several spoofing detection methods found in the open literature, and selects the ones which can be suitable for mini and micro UAV technical specifications and operational scenario, for proposing a GPS spoofing detection solution developed in the application layer of an open source code Ground Control Station software SDK. The detection solution is intended to monitor and correlate abrupt, abnormal or unreasonable values of different sensors of the UAV with data obtained from available additional sources.

The conducted tests validate the cases and circumstances where the spoofing attacks were successful. Limitations include the lack of mechanisms to access GPS values which can be useful for detection spoofing attacks, but reside in the data bit or signal processing layer of the GPS and can not be retrieve to the layer where the SDK in computing all data of other sensors.

Keywords: Spoofing detection, simplistic GPS spoofing attack, UAV, Cybersecurity, Information and Communication Technology.

CERCS-code: P170

Veaavastus, analüüs ja lahendused lihtsakoelise saatja aadressi võltsimise vastu kommertskasutuses olevate mini- ja mikrodroonides

Enamus droone kasutab lennundusest pärit GPS navigatsiooniseadmeid, millel puuduvad turvaprotokollid ning nende riskioht pahatahtlike rünnakute sihtmärgina on kasvanud hüppeliselt lähimineviku arengute ja progressi tõttu SDR ja GNSS simulatsioonitarkvara valdkonnas. See on loonud ligipääsu tehnikale amatöörkasutajatele, millel on saatja aadressi võltsimise jõudlus. Need potensiaalsed rünnakud kuuluvad lihtsakoeliste kategooriasse, kuid selle uurimustöö tulemusena selgus, et nendes rünnakute edukuses on olulised erinevused teatud GPS vastuvõtjate ja konfiguratsioonide vahel.

See uurimustöö analüüsis erinevaid saatja aadressi võltsimise avastamise meetodeid mis olid avatud kasutajatele ning valis välja need, mis on sobilikud mini- ja mikrodroonide tehnonõuetele ja operatsioonistsenaariumitele, eesmärgiga pakkuda välja GPS aadresside rünnakute avastamiseks rakenduste tasandil avatud allikakoodiga Ground Control Station tarkvara SDK. Avastuslahenduse eesmärk on jälgida ja kinnitada äkilisi, abnormaalseid või ebaloogilisi tulemväärtusi erinevates drooni sensiorites lisaallkatest pärit lisainfoga.

Läbiviidud testid kinnitavad, et olenevalt olukorrast ja tingimustest saavad saatja aadressi võltsimise rünnakud õnnestuda. Rünnakud piiravad GPS mehanismide ligipääsu, mida saab kasutada rünnakute avastuseks. Neid rünnakuid puudutav info asetseb infovoos või GPSi signaalprotsessi tasandis, kuid seda infot ei saa haarata tasandile kus SDK tarkvara haldab kõigi teiste sensorite infot.

Märksõnad: Saatja aadressi võltsimisrünnakute avastus, lihtsakoelised GPS saatja aadressi võltsimisrünnakud, Droonid, Küberturve, Info- ja kommunikatsioonitehnoloogia

CERC S-Kood: P170

Table of contents

List of figures

List of tables

1 Introduction

Currently, GPS is the Global Navigation Satellite System most used all over the world, a couple of decades ago it was a tool used mainly for certain governments or corporate organizations, but today particular individuals can easily access to their Position, Velocity and Time (PVT) solution; not only because the GPS receivers are every time cheaper and smaller, but also because theirs signals are always expected to be found in the Radio Frequency environment of the public domain, which means that is freely available, triggering that a wide range of different and significant services are designed and rely on GPS.

Between those services, positioning is not the unique role of GPS in the world, because GPS receivers can be synchronized with the extremely precise satellites atomic clocks, users can determine time within 100 billionths of a second, capability used for the operation of multiple meaningful activities like: financial networks and stock market time stamping, electrical power grids, CDMA cell phone towers and digital broadcast radio services [1], even 65 percent of NTP stratum-1 servers pool are using GPS for time synchronization. [2].

On the other side, great quantity of navigation systems has been being designed or redesigned in strict dependence or high companionship of the Positioning and Velocity GPS solution, as example: broadly all transportation industry; from ADS-B, until map apps on mobile devices, going through self-driving cars, maritime navigation or UAVs are using GPS services as main positioning system input.

For instance, GPS is deeply attached to the functioning of our normal daily lives, however is not a fully secured system. Back in the seventies, when GPS was designed by the United Stares Defence Department, the future relevance and importance of the system for the civilian users was underestimated and cybersecurity was not a concern or a situation the designers were aware of, so that, security flaws in the fundamentals were going to emerge, which solution would require changes in the basics of the GPS architecture. [3]

The consequences for civilian users is the lack of authentication in GPS signals, reflected in the vulnerability that all GPS receivers are subject of, which is being spoofed. Spoofing is the injection of counterfeit readable and structured signals in order to provide fake positioning and timing information for the end user. Unfortunately, today is easy than ever do this kind spoofing attacks, because of recent developments, there has been a substantial decrease in the prices of equipment to setup or buy spoofers compared with previous years, consequently, an amateur devious malefactor with few resources and knowledge can conduct this attacks unscrupulously.

The design and constitution of Unmanned Aerial Vehicles differs from the other types of drones not only because their proliferation and application spectrum is wider, but also because during an intentional or unintentional emergency situation, security to people has to be warrantied, for the fact that they are flying objects with range and endurance limitations, for example, in the case of a power unit failure or a devious communication jamming attack, the UAV should land safely because further than it can not simply stay in the air for undetermined time, speed and range can propend terrible accidents and incidents, consequently, flight safety is vital and must be reassure for aerial vehicles operations.

The widespread rising of Unmanned Aerial Vehicles initiated in the military industry, because of the clear advantages over manned aviation, essentially that their operational cost was much lower, they can enter to environments which may pose risk to the life of the aircraft operator and the endurance was extended beyond human limits. These were the upholder reasons that next, busted and expanded the phenomenon of UAV towards diverse fields: cinematographic, GIS, Search and Rescue, urban surveillance, gas and oil pipelines surveillance among many others; a future can be forecasted when there will no be sky landscape without a couple or maybe hundreds of drones flying above us.

There is a special connotation with GPS in Unmanned Aerial Vehicles: the pilot is not on-board, the aircraft is commanded remotely and usually it is not under any visual control. So, further than, GPS has been the most accurate world wide solution to navigate, UAVs have been designed under high dependability as the only effective navigation system, raising a latent vulnerability for GPS spoofing attacks with notorious high impacts in the operation.

In the open literature there is a vast library of GPS countermeasures and methods to increase security, but very few practical implemented solutions; so worriedly, performing a GPS spoofing attack has become a very accessible task but in the other hand detection or mitigation solutions appears to be only on scientific literature or used by exclusive or private organization, not accessible for an end user public.

The purpose of this work is to facilitate an immediate response for the problem stated, designing and creating a GPS spoofing detection solution, based on multiple techniques in different layers of the GPS operation, and applying specially the benefit of networked GPS detection solutions.

1.1 Problem Statement

From all the GPS dependable and security susceptible industries, there is one particular thing of drones, GPS is fundamental to accomplish a successful safe mission, moreover when the UAVs flies at distances that the operator cannot track or follow, it is the essential tool to route the aircraft displacement and orientation towards the desired destination, not only because the operator navigates the vehicles remotely and it is forced to trusts in the information provided of the GNSS solution, but also:

- GPS does not drift, unlike Inertial Measure Unit sensors, like gyroscopes, accelerometers and pitot static systems.
- It is not limited by weather conditions as clouds or fog unlike like camera or video systems.
- It is accurate and precise, not as magnetic compass systems.
- Complete GPS modules implementations are compact and portable, suitable for the small size and limited payload of UAVs, in comparison to radars, VOR, DME or NDB radio navigation systems.

Alarmingly, GPS authenticity has vulnerabilities by design, and different than the newest GNSSs, GPS it is the most popular and widely used, not only because it has been the fully operational for more than three decades, but also because specific and detailed description of its operation is publicly disclosed. In this situation, one not positive side of the fact that more studies, development, research and software has been created it is that low cost equipment can be used to create malicious attacks against a wide spectrum of unprotected end users.

Although, an optimistic forecast is expected with the European GNSS GALILEO that with its encrypted navigation service (PRS) for civilian users, will substantially increase the complexity to perform a successful spoofing attack. It is not available yet, since it is planned to be fully operational until 2018-20 [4].

There is a big risk when the vehicle does not have pilot on-board and it is mainly navigated based on data lacking of authenticity; unfortunately, this is exactly what is happening nowadays, because the broadcasting signal which is used for most UAV, is freely accessible and transmitted unencrypted, thus the feasibility for this services to be deviously disrupted is very high, furthermore, recent development on SDRs and the disclosure of free GPS simulator software, makes easier the task to conduct a spoofing attack to GPS.

The GPS spoofing detection and mitigation solutions do not have practical implementations, most of the solutions are theoretical, or are for exclusive, proprietary or private use, therefore, most of UAV are dispensing of a proper countermeasure making them vulnerable to an easy-to-do attack, additionally, end users and drone operators have not situational awareness of threats, posing a latent risk for UAV flights. There is an existent asymmetry of the easiness of performing a GPS spoofing attack against the unavailability of an implemented solution to protect from it.

1.1.1 Motivation

This work describes an analysis and a proposed a software solution for the uprising problem of the todays easiness to perform a GPS spoofing attack. The reason for conducting this research is the latent security gap in a satellite navigation system that is fundamental and necessary for the accomplishment of UAV missions.

For example, in case of GPS failure caused by unintentional reasons like GPS chipset damage or unintentional interference, the usual emergency procedure implies return home; so even if the system has video link capabilities and the landmarks on the terrain can be compared with a priori saved maps in the GCS, the pilot manoeuvring capabilities are tested, and there is high uncertainly for avoid accidental endings. Worst situation is if this GPS signals are effectively spoofed, because in this case there is complete incapability for the pilot to maintain flight safety; except if a detection solution can alert from the attack and the aircraft is set into manual mode, then a similar procedure as the GPS failure can be followed, the problem is that no such a detection solution is yet implemented.

Between all the disastrous situations, hypothesis examples can be: force the UAV to fly until runs out fuel until crash, force the aircraft to fly into prohibited or restricted areas like airports or make the UAV fly outside national boarders, trespassing into other county airspace.

Such security threats can pose a grave challenge to UAVs in delivering safe flights, an example is the debatable and controversial case of the hijacked US drone in Iran disclosed real possibilities for a UAV to be stolen by injecting counterfeit GPS signals. Although this was one of the first successful attacks claimed to be done by spoofing GPS, there is not certain or official verifications that the incident happened caused by this means, however academics state that it could have been done [5].

1.1.2 Research questions

How can GPS navigation be more secure against GPS spoofing attacks in mini and micro UAVs?

RQ1: In what circumstances are mini and micro UAVs vulnerable or susceptible to GPS spoofing attacks?

What types of GPS spoofing attacks are? What are the prominent threat vectors for a UAV which uses GPS to navigate? How vulnerable are a GPS navigation based UAV to this threat vector?

RQ2: How can a software implementation actively detect GPS spoofing attacks in mini/micro UAV flights?

What solutions or theories can detect GPS spoofing attacks? What solutions can be integrated in a single algorithm that detects GPS spoofing attacks suitable for the technical specifications of mini/micro UAVs? What type of procedures can be executed once GPS spoofing attacks have been detected to ensure flight safety in UAV?

RQ3: How effective is the GPS spoofing detection software solution?

In what scenarios can the GPS spoofing detection algorithm work? What is the applicability of this software solution? What limitations does the software solution have?

1.2 Risk overview

Navigation is the act of finding and directing from one place to another, for UAV, GPS is an essential tool to achieve the desired destination. In order to identify, analyse and prevent from the GPS spoofing attacks with more impact and likeliness in mini and micro UAV, it is necessary to overview and understand its threat vectors, vulnerabilities and risks.

1.2.1 Threat vectors

A GPS spoofer like a GPS jammer are devices that cannot be bought by that names, although there are multiple options to purchase a Privacy Portable Device that in the case of the Jammer is essentially the same. On the other hand, a GPS spoofer is not as simple as a device that broadcast noise to produce a Denial of Service; a GPS spoofer has to emit structured and readable signals that emulate a complex moving satellites constellation.

Cracking the GPS as a system has been doing gradually, it can be reflected on decreasing price of the commercial GNSS simulators, in 2008 was about 400.000 USD [6] today can be acquire from approximately 4000 USD; even more recently, open source software has been made available that requires about 400 USD for special hardware; this equipment acquired by scientist, researchers, academicians, or hobbyist as well as by unscrupulous malefactors.

Different type of attacks can be achieved depending on the means the threat actor uses to inject fake GPS signal into a UAV receiver

The first option is to make and configure your own GPS spoofer. The resources needed for this script kiddie level device are a SDR card, transmission antenna and a laptop. Besides this, today there is only one available open source freeware that creates the binary GPS stream to be transmitted[1], the rest are only partially finished projects online. All the equipment can be obtained by approximately 1000 EUR plus basic knowledge on GPS is necessary. This implementation it is limited to perform only a Simplistic GPS attack.

Secondly, the attacker or threat actor, can use a commercial hardware or software GNSS simulators. These devices made essentially for research and testing are sold without restrictions, and the prices start from approx. 4000 EUR to even ten of thousands for a more sophisticated solution. Some equipment is already offering real time signal generation.

Following commercial simulator, the threat actor could take advantage of the developments done by university level research groups. In 2012, it was estimated that 100 universities were capable enough to develop a sophisticated spoofer within a year of dedicated effort. [3]. Today, this task should be accomplished much faster due to the constant developments of free SDR based GNSS receiver software [2].

[1] https://github.com/osqzss/gps-sim-sdr

[2] https://github.com/gnss-sdr/gnss-sdr

Finally, the fourth GPS spoofing source can be through the capacity of a private corporation or government level. The information about the GPS spoofing capabilities is classified, but can be assumed that can have access to sophisticated spoofers, considering they usually are developing cutting military edges technologies and count with practically no limitation in recourses [8].

1.2.2 Vulnerabilities

GPS as system

Civil GPS as a system miss security concept in the nature of its design which allows exploitable vulnerabilities. Standard receivers have the task of detecting a satellite signal sent from satellites orbiting the earth at roughly 20'000 kilometres of altitude, the received signal strength RSS on the Medium Sea Level is about -130 dBm, which is weak enough to be disrupted by thick cloud coverage, make it unavailable indoors, or be easily overwhelmed or overlapped by different that the legit sources. [9] In addition, detailed and specific technical data of its operation is widely available, like PRN signals, transmit frequency, signal bandwidth, Doppler range, signal strength, almanac and ephemeris; so there is not secrecy of the GPS operation for a deep understanding of the system, facilitating the functions emulation and architecture design to construct a spoofer. In the same way, GPS receivers have an AGC that balances power by automatically selecting the strongest available signal, propending the vulnerability of acquiring the stronger spoofed GPS signal [8].

The danger starts immediately after the spoofer captures the correlation peak of the target receiver, the spoofer induce a fake position and velocity, taking control and command of the drones heading, because the spoofer operator effectively has broken the UAV autopilot feedback control loop [10].

In the L2 signal a GPS spoofing attack is nearly impossible because the military signals are encrypted and therefore unpredictable for a spoofer, all it can be done it capture and replay existing signals (meaconing attack), instead, the civil GPS signal is publicly known and readily predictable [10] [11].

UAV operations

Nearly in every occurrence, nor the pilot or the autopilot software is aware when there are GPS spoofing attacks, because if conducted properly, the transition from using legit to fake signals will be end user transparent; [3]. In a not transparent transition, will be notable a period of time without service, cause by a force reacquisition technique; it has not necessarily to raise concern of spoofing or attack because interference of signals is produced not only intentionally but produced unintentional, caused by solar radiation bursts or by equipment broadcasting carelessly or uncontrolled signals in the same frequency of GPS.

Once interference is detected during a UAV flight flights, it is not unusual to have temporal interference in the GPS frequency, however, once alerted by the software, the situation can be overcome by conducting some flying manoeuvres or by following the stipulated emergency procedure. Initially, the navigation should be manual, considering the autopilot is based on the not available or not trustworthy GPS coordinates; for the case Line-of-Sight LOS drones, one of the procedures is to follow the transmitted beam of the communication channels towards the broadcasting origin, which is essentially a known reference location where usually a directional antenna is located; for the Beyond-Line-of-Sight BLOS drones, the satellite communication channel is encrypted and provides alternative geolocation.

If during a UAV flight a spoofing attacks is detected, the operation will be cancelled because UAV navigation is not trustworthy, but the possibility of an accident to happened is highly reduced rather than if there is not countermeasure; however, if there would be mitigation implemented, the operation could continue bemuse the fake signals will be filtered out.

Pilots and software currently used to fly drones are blind trusting in the legitimacy of the obtained GPS PVT solutions, because there is not situational awareness or implemented detection mechanisms in the commercial micro/mini UAV that alert the presence of possible GPS spoofing attacks.

Although a simplistic GPS spoofing attack is the easiest one to detect, there has not even been sufficient acknowledgment of the spoofing threat from the manufactures to implement detection mechanisms for this type of attack or for end users to know the vulnerabilities and risks they are susceptible when flying a drone, therefore, there is an asymmetric proportion between the todays easiness to perform simple GPS spoofing attack and the few available practical and implemented solutions to protect from it.

The only known commercial manufacture that has recently released a firmware version with antispoofing detection solution is U-Blox. On February 2016, the new 3.01 firmware version for the 8M series of the GPS chipsets is launched, this software has the capability to flag possible GPS spoofing situation. The detection solution algorithm relies on multiple GNSS and is no fool proof[1] [12].

When attacking there can be two main objectives: (1) fooling the receiver, by means of successfully inject fake signal into the hardware and software of the UAV, or (2) fooling the operator, where the pilot is not aware that is under attack, and therefore does not react accordingly. If there is not any countermeasure implemented, the pilot as well as the autopilot are completely unprotected to succumb. If there is a detection technique implemented the attack will be flagged, so even if the UAV autopilot is fooled, the operator will be alerted and will be able to act in order to protect the safety of the mission, for example by changing the flight mode to manual where GPS is not used. The safest mission is when a mitigation solution is available, so nor the pilot or the autopilot will be fooled with the spoofing attack. It is important to remark that this hypothesis contemplates ideally effective countermeasures that in practice are not considered to exist.

To conclude, there is a latent security vulnerability for all the mini/micro drones that are using GPS to navigate, moreover today, that resources are not a barrier when the threat actor can use cheap SDR cards and freeware downloadable on internet.

1.2.3 Risk

In this section will be mentioned practical factors that can affect the impacts of the attack and the operational risks a UAV is subjected when using GPS to navigate.

The impact in the operation objectives can be significant, varying from permanent to temporal disruption on the mission, like:

- Stealing the aircraft, by hijacking the navigation system and making it land in attacker desired location, as claimed by the Iran case in 2011 [3]. The aircraft should be flying outside the operator sight monitoring range in order to avoid the pilot change the flight mode into manual. Additionally, the injection of the counterfeit PVT solution has had to be meticulously planned and the provided the spoofer have to learn the target flight pattern, if and a stable covert post-capture is desired [13].

[1] https://www.u-blox.com/en/press-release/u-blox-m8-multi-gnss-receivers-achieve-higher-level-performance-embedded-security

- Crashing the aircraft, by injecting fake elevation values into the GPS, in a usual autopilot behaviour the aircraft will dive to reach the commanded altitude, although there are barometric altitude sensors, they are not as accurate as the GPS elevation, therefore, usually GPS solution prevails as a reference. This could be accomplishing by injecting altitude values lower than the ground elevation, so the autopilot will try to reach the desired height of flight, making the aircraft to dive into a crash. Crashing is easier than controlling.
- Confusing, disorientating or misleading the aircraft trajectory, disqualifying the capacity to properly conduct the mission, considering that the UAV will not be able to accurate point, follow and track on specific area, by injecting randomly fake PVT data into the receiver target.

There is not a fool proof solution for securing GNSS from spoofing, securing GNSS signal authentication is about conjugate existing mitigation and detection techniques and set them up with the appropriate thresholds, becoming them a fundamentally a problem of statistical decision theory, to accurate understanding possible false alarm [14].

1.3 Project context definition

There is a wide variety of environments and conditions that can make the difference when conducting the GPS spoofing attack. In this sense, it is important to narrow the extent of the project and define the scheme, the function, the use, the creator and the recipient for this situation. In this section will be distinct the circumstances where the analysis and the final software solution will have applicability.

Although most UAV are using GPS to navigate [15], for the purposes of this analysis, it is only taken into consideration the Micro/Mini UAV groups, with some applicable extended until the Short Range (SR) subgroup, excluding all UAVs placed above of the Tactical category. The reason for discarding Tactical, Strategic and Operational Task UAVs is because they are of exclusive use, their distribution spectrum is outside the range of an average person (the threat vector for this thesis), and they belong mostly to intergovernmental organizations or particular companies, because of elevated prices, high maintenance costs and restricted sale.

Additionally, Tactical, Strategic and especial task UAVs are less prone to GPS amateur attacks than mini/micro UAVs because:

- Their operational scenario is located in remote or restricted areas like vessels, jungle or military compounds, so that, physical security covers wide ranges from their take-off or landing location, in addition, their maximum and operational altitude can exceed 3000 meters, making the interaction with public not likely.
- Their position can be provided by different sources than GNSS, like the encrypted satellite communications telemetry channel or alternative ground based triangulation stations.
- Because of the more Maximum Take of Weight capabilities, they can carry more variety or robust equipment, like radio navigation instruments like the conventional aircrafts, which may provide alternatives to navigate without GPS.
- They are flown by skilled pilots, which require certifications and certain experience to fly, so that, they are prepared to identify and react for emergencies, besides the fact that the software of the control station and the firmware of the aircraft is smart to manage different contingency scenarios.

On the other hand, mini/micro UAV subgroup have flexibility and dynamic components, are relatively cheap and have worldwide commercialization, becoming them in the adequate group to test and experiment. Besides that, mini/micro UAVs have great advantages when developing customized applications because are usually operated under open source software licences, have big development and support communities online, different manufactures use same standard software and protocols, they have detailed manuals and their patches and upgrades distribution can be applied immediately, also there are multiple options for spare parts and new version hardware can be bought and adapted without changing the drone architecture.

Following the logic for the UAV subgroup selection, the spoofer used for this project will be the most affordable and easy to implement and manipulate for an amateur threat actor. This spoofer is setup using SDR cards and free software, and its attacking capabilities the corresponds to a simplistic spoofing attack.

The final user of the contributions proposed in this work, can oscillate since a well versed hobbyist until some who ignores the technical details and basics of UAV systems, or from a professional video shooting operator until a traditional drone user that has not GPS knowledge to interpret suspicious GPS spoofing signs like constant intermittent signal in clear sky, abrupt discrepancies between sensors, or uncontrolled displacement of the drone caused by fake coordinates into the autopilot software.

The attacker is a devious amateur individual that is going to take advantage of the commodities of technological developments that today facilitate to anyone to competence of creating a GPS spoofer, to interfere with the normal happening of a UAV mission.

The location for the attack to be performed is anyplace outdoors where even restricted, there is not strict control of emission in the Radio Frequency environment from the authorities. In general, there is contemplated ideal to normal conditions, with a flexible but not extreme weather and without third cases interferences of signal obstructions. Additionally, range and distance between actors will no be relevant considering it depends mostly on the antenna [16].

1.4 Related work

Several detection techniques have been proposed in the open literature by different research Groups and universities [3,6,8,9,10,11,17,18,24,31,33] On the Requirements for Successful GPS Spoofing Attacks, Assessing the Spoofing Threat], in this works the spoofer used to validate the spoofing attacks or the detection theories are custom or property receiver-based spoofers or high-end GNSS simulators; nevertheless, some detection theories are only theoretical and not implemented.

The work done by the Radio Navigation Department of the University of Texas, with several papers describes the vulnerabilities and details capture and control of an Unmanned Aircraft [17], highlighting work when successfully spoofed a drone in a distance of about 600 meters with the own developed intermediate spoofer [10].

ETH Zurich, with the paper "On the Requirements for Successful GPS Spoofing Attacks", considers attacks on single and groups of GPS receivers and discuss topics as the require precision on the attackers spoofers signals. The hardware used is the GSS7700, capable of simulating two constellation of SV, where on simulates legit GPS signal and the other one simulates the signals of attacker [11].

Important event happened during the DEFCON23, Unicorn team, Qihoo 360 Technology Co. Ltd., presented how anyone could perform a GPS spoofing attack, by using SDR cards and a MATLAB code not disclosed that simulated the GPS signal. However, recent software of Takuji Ebinuma is available for downloading in GitHub. [1]

[1] https://github.com/osqzss/gps-sdr-sim].

Oleg Petrovsky, Senior Security Researcher of HP realised the paper “Map is not a territory: How to spoof GPS on a shoestring” on February 2016. This paper shows the effectiveness of the SIM-GPS software on different version of GPS chipsets of the same manufacturer and some mobile devices, however focus mainly on the precision needs of a specific SDR card, and the tests are done without considering that the receiver can be locked already into the correlation peak of legit GPS signals, situation that would normally happened when flying a drone outdoors [18].

All works above only consider and focused on attacks of intermediate or in some cases sophisticated GPS spoofing attacks, which are more effective and difficult to detect but also, are more difficult to implement than simplistic attacks; an analysis for that recent publicly disclosed GPS spoofing threats is disregarded, moreover, there is not any solution proposed for the case of mini and micro UAVs.

1.5 Objectives and contributions

The main objective of this thesis is to increase the security of flights in GPS navigation based UAVs by the delivering the following contributions (1) An analysis of the effects and detection techniques of GPS spoofing attacks in UAVs and (2) creating the design and the implementation of a monitoring solution suitable for the performance specifications of mini and micro UAV, aimed to detect their prominent GPS spoofing threat vector.

The research is focused on proposing a software solution based on the different GPS spoofing detection methods found in the open literature that will be implemented in a mini/micro UAV platform. The solution approaches the problem from different layers of the GPS operation architecture and will have a scalable design for similar commercial UAVs. Herein, the word “prominent”, refers to the easiest spoofing attack to setup, therefore it is the one with more likeliness to happen for this type of UAV, considering the recent developments in SDRs and the realising of free GPS simulation software.

For the present paper, the analysis has been performed in Line of Sight propagation environment and no over-the-air tests were conducted to avoid violating possible FCC regulations by broadcasting in the GPS band; hence, the transmission hardware will not be discussed further, but there is a description of the controlled environment setup.

The scope of the thesis discards any mitigation capabilities, and as any other of the countermeasures, the solution is not expected to be fool proof. The solution design is the result of the conjugation of GPS spoofing detection methods, selected by the limitations on standard mini/micro UAV hardware and application complexity. The implementation will be done based on a commercial default configuration UAV that has open source software development model [1].

During the validation process, the GPS spoofing attack will be based on the easiest-to-get spoofer, capable only to conduct a simplistic attack. Security or availability in communication telemetry channels, additional kinetic or non-kinetic attacks, indoor scenarios, irregular weather or unusual environmental conditions will not be relevant for the analysis of the project or operational schema.

1.6 Methodology

To solve the problem statement, it will be used the Design Science research methodology.

[1] https://3dr.com/open-source/

The first stage is a research, in the open literature, about the state of the art of the problem statement and its extent: a clear picture has to be found out of the different GPS spoofing attacks and detections solutions in the UAV context, characteristics and technical limits. The purpose is to gather and identify and analyse the available countermeasures that can detect the attacks, to comprehend how do they work and interact within different variables.

During the research process specific and technical information about the functioning of the GPS technology will acknowledge, to understand the capabilities and limitations of the UAV hardware and software that will be used in the project.

Considering the vast literature available in the topic, the sources will be mainly found on internet: withe and grey literature, academic search engines, research institutes online sites, universities publications, journals and scientific magazines.

Once there is a clear overview about the GPS spoofing attacks types and solutions, the second stage will be classifying and comparing which of that solutions can be combined in a single detection software suitable for the technical specification if the mini and micro UAV categories, and discard the solutions that will not be employed either for high complexity or not practical use.

After identifying and validating the vulnerabilities of the UAV for the prominent GPS spoofing threat vector, the next stage is where the designing and implementation of the GPS spoofing detection solution will take place. This is solution will be based on the open source SDK of the Command and Control software of a particular UAV platform and will integrate the detection techniques selected in previous step.

Finally, the evaluation method will be a controlled experiment that will prove the efficacy of the GPS spoofing detection solution in the setup used to identify the UAV vulnerabilities. The validation setup is based on real scenario in a controlled environment and the tests would be limited by the local regulations of broadcasting RF signals.

2 State of the art of GPS spoofing detection in UAV

In this chapter is described the state of the art of GPS Spoofing detection in UAV. Firstly, there is a research and classification about the theoretical solutions for detecting GPS spoofing attacks found in the open literature.

Secondly, there is an overview of GPS Spoofing detection research groups in different universities, overview description of implemented available solutions, and related work done by security research or academics in the field.

2.1 Technical Background

Technical overview on Global Positioning System functioning, UAV operational categorization and GPS spoofing attacks are explained in this chapter in order to understand the key concepts for this thesis project.

2.1.1 GPS technical overview

GPS is a satellite dual use navigation system designed and developed in the seventies by the Department of Defence of the United States. It provides separate services for the military and the civil users. The Standard Positioning Service SPS broadcasted at 1575.6 MHz (L1 signal, unauthenticated) and is designed for the use of the civilian community modulated by the C/A, whereas the Precise Position System PPS transmitted at 1227.6 MHz (L2 signal, authenticated) and is designed to be used by US military and selected government agencies (it does not mean that it is used by all military institutions), L2 signal in modulated by P code that offers additional encryption capabilities.

The system consists of 31 satellites constellation that omits the earth with the purpose of providing an uninterrupted PVT solution anywhere in the world, using the Time of Arrival (TOA) range concept to determine receivers position.

TOA range concept involves measuring the time taken for a signal transmitted by the satellite to reach the receiver in a known location. This time, known as propagation time, is multiplied by the speed of the signal, speed of light, to obtain the distance travelled. When is calculated the distance of more than four emitters is possible to obtain a 3D location of the receiver, by solving an equation system. The more satellites are used to determine the PVT solution the results the more accurate the results are.

The resulting distances are also related to an imperfect alignment of the receivers' time scale to the satellites accurate atomic clock time scale. Each satellite transmits within the 1575.42 MHz frequency, but it is distinguished because is modulating the signal with different ranging codes, identifiable with an equivalent and unique PRN number.

Corse/Acquisition (C/A) code

Transmitted at 1.023 Megabits per second, each satellite has a unique PRN code that only correlates when they are almost precisely aligned within alike one. There is no possible and alignment between of satellites PRN codes.

Navigation Message

C/A and P code signals are modulated at 50 Hz, to obtain the navigation message. This message has necessary information to obtain precise transmission time (almanac) and location of each satellite (ephemeris). It also contains information that may be required to to assist the equipment in acquiring new satellites, to translate from GPS system time to UTC and indications to correct for a number of errors that affect the range measurements. The entire message broadcast requires uninterrupted 12.5 minutes of transmission [19].

Signal Acquisition and Tracking Phase

After the GPS reviver is turned on, there is a series of steps that must happen before it can access to the information of the signal and provide a PVT solution. Most of this steps occurs in the acquisition phase, making it more complex and recourses expensive than the tracking phase because it has to search and match the signals in wide spectrum.

During the acquisition, the receiver performs a search in two dimension. Firstly, it needs to find the Doppler offset and where is the beginning point of C/A code [19]. To accomplish this, it searches for the correlation peak in the signal by trying al possible values in the 1023 possible slots in the Pseudo Random Number PRN of each satellite, in addition, it has to search in a frequency range of ± 10kHz due to the Doppler effect. After that, the receiver sets an internal clock to match the correlation peak, at this point there is a synchronization between the receiver internal clock and the satellite atomic clock.

Once the signals are acquired, the tracking phase two loops are required to track each satellite signal. One loop tracks the beginning of the C/A code or pseudo-ranges, this is known as DLL; the other one tracks the Doppler carrier or pseudo-rates known as FLL [20].

Time to First Fix (TTFF)

The time to first fix (TTFF) is the time required for a GPS receiver to obtain satellite signals, navigation data and calculate its current position (fix) since the acquisition phase has started. To calculate a two dimensional position, the receiver needs to know the position of at least three satellites and calculate their distance to them. The position of a satellite is calculated based on ephemeris data, which is very precise orbital and clock correction data for the satellite. Each satellite broadcasts only its own ephemeris data within a navigation message. The navigation message contains also almanac data that is used by the receiver to predict approximate positions of the satellites. The usual cold, warm and hot start types used to calculate the TTFF are not definite in any official standard.

In a cold start, the receiver has not saved its last time or position, and doesn't have almanac or ephemeris data. Typically, a cold start is performed whenever the receiver has been powered down for more than two weeks or the battery backup of the memory is lost. The complete navigation message is not necessary. Considering the transmission rate of 50 bps for each satellite to send its 900 bits long navigation data message, the minimum time to achieve a cold start 18 seconds, although an expected average could about 45 seconds.

A warm start is performed whenever the receiver has stored useable almanac data, time and the its last position. While the ephemeris data is missing, it has to be downloaded it from at least three satellites, similar process as the cold start, and same minimum of 18 seconds time. Almanac data allows the receiver to predict which satellite signals it should be able to receive, and thereby, the receiver can acquire signals faster then in a cold start.

A hot start happens when the GPS receiver has ephemeris and time previously stored. The receiver gets the signal of at least three satellites and calculate the position. Reported time for manufactures is usually from 1 to 3 seconds range [21].

2.1.2 GPS Spoofing attacks types

Spoofing is the intentional transmission and injection of counterfeit GNSS signals into a GPS receiver for providing false Position, Velocity and Time (PVT) solution. The goal of GPS spoofing is to stealthily force a receiver to track a devious signal.

Based on the spoofer architecture, GPS spoofing attacks can be categorized in [6]:

2.1.2.1 Simplistic attack via GPS signal simulator:

It the simplest of the attacks. Basically is the transmission of GPS signals into the radio frequency spectrum. The generated signals are not synchronized with the legit GPS signals, meaning that if the receiver is in tracking phase, the counterfeit signals will not be acquired by the receiver, therefore the fake packets injection will never be used to calculate the PVT solution, unless there is a conducted a forced reacquisition technique. On the other hand, if the receiver is in acquisition mode there might be a chance to perform successful attack. This attack can be achieved by using GNSS simulator, equipment of commercial distribution which prices have been decreasing significantly in the previous years, today the can be bought from approximately 4000EUR. In addition, recent development in Software Defined Radio hardware and GNSS open-source freeware, are lowered the price of setting up a GPS simulator by roughly 400 EUR. In this section is included the meaconing attacks, that are record and replay the complete GPS frequency in the RF spectrum [6] [22] [23].

2.1.2.2 Intermediate attack via Receiver-based spoofer:

This equipment consists of a GPS receiver connected to a spoofing transmitter. Firstly, the system synchronizes with current legit GPS signals to generate spoofing signals aligned with the real GPS satellites, knowing the approximate 3D pointing vector of its antenna towards the location of the target receiver antenna. "The spoofer has to move its correlation peak away from the authentic correlation peak in order to grab the tracking point of the target receiver PLL/DLL" [22]. If the signal power is about 10 percent stronger than the legit signals the tracking procedure can be deceived. Projecting the counterfeit signals to the target GPS receiver with correct power and signal delay in the main challenge for this the construction of this types of devices [6] [23].

2.1.2.3 Sophisticated receiver based spoofers multiple with multiple antenna:

The most advanced of all attacks, it is similar as the intermediate attack is carried out, but now using several coordinated spoofers to also emulate the spatial signal domain, making both the attack itself very difficult to carry out as well as very hard to detect for a conventional single antenna receiver. This type of sophisticated receiver based spoofers can transmit trough numerous antennas to avoid DOA antispoofing techniques. To perform this attack requires complex set ups and advanced setups.

When the receiver is in the acquisition phase is more susceptible to be effectively spoofed because still has no lock on legit signals. In this case all previous stated attacks have great chances to succeed, other factors like signal strength, signal quality enter to play a decisive role.

However, if the receiver is in tracking phase, chances to conduct a successful attack are smaller, because a higher correlation peak will not affect the tracking procedure and the receiver will stay locked to the authentic signal, unless counterfeit correlation peak is located very close to the authentic one. The spoofing signal will look like noise to receiver. In this case there can be performed to types of attacks when the receiver is in tracking mode [22]:

- Synchronous: The spoofer signal carrier phase has to be aligned with the original signal carrier phase, by precisely knowing the three dimension pointing vector from the transmission antenna in direction of the antenna of the receiver with few centimetres precision [24]. Also, the spoofer should know of the genuine signal power at its target receiver. These conditions are very hard to achieve in real world spoofing scenarios when the target is a UAV flying out of attackers' range.
- Asynchronous: In this case, the spoofer knows a rough indication of the position of the victim's receiver antenna. During an asynchronous attack, a higher power correlation peak will be generated, that will move along the signal looking for place itself on the

same position of the authentic correlation peak. This a more realistic scenario compared to the synchronous attack, although one drawback is that the generated noise before locking can be an indication of abnormal situations [22].

Several anti-spoofing techniques have been proposed in the open literature recently. These methods are usually organized in two categories: spoofing mitigation and spoofing detection. Spoofing detection focuses on discovering the spoofing attack while spoofing mitigation techniques objective is to neutralize the spoofing threat.

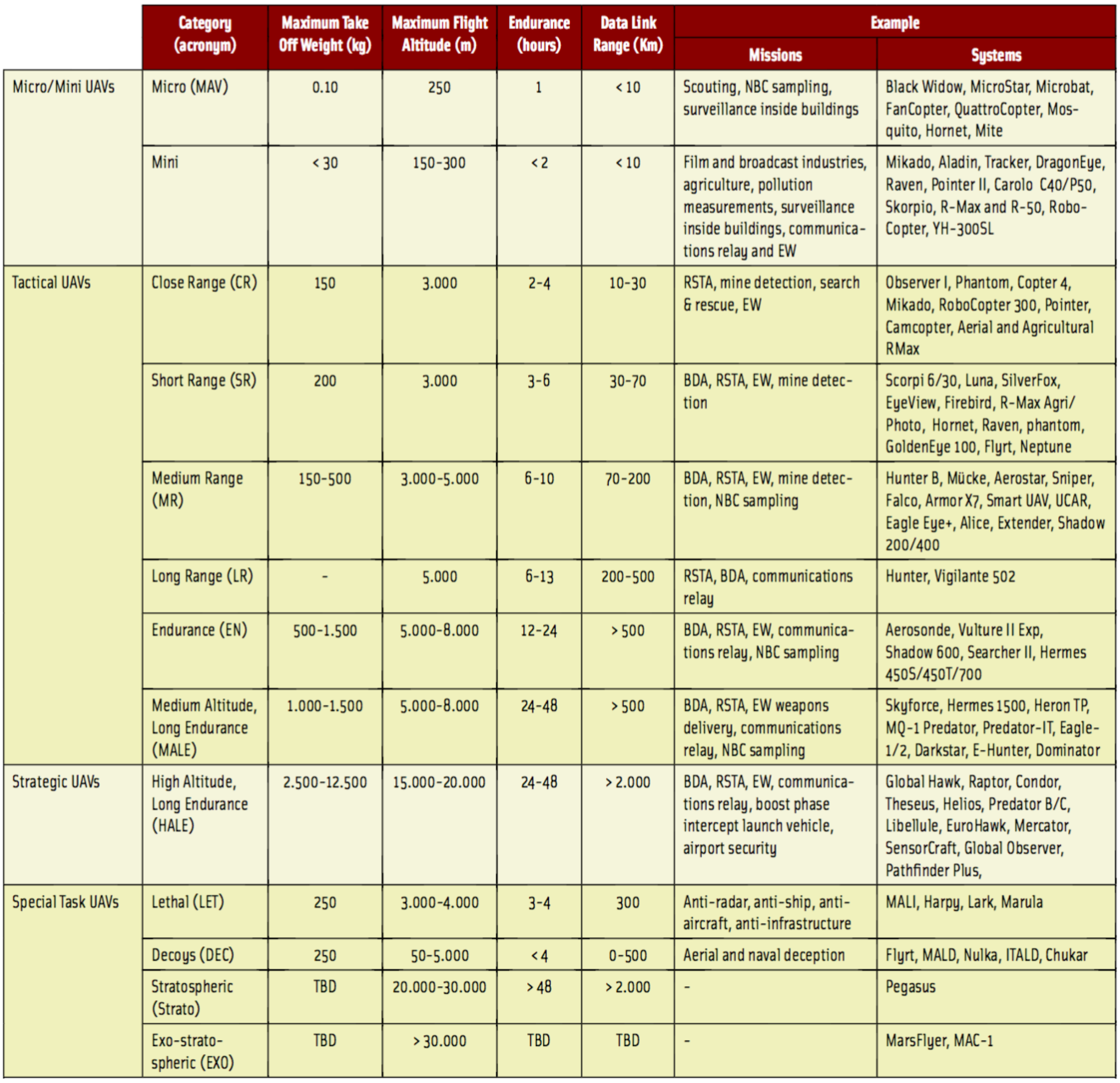
2.1.3 UAV categorization

UAV is an aerial vehicle capable of sustained flight without the need for a human operator on-board. A UAV can be remotely controlled, semi-autonomous, autonomous, or a combination of these, capable of performing as many tasks. [25]

“The connection between civil UAVs and civil GPS signal is straightforward: the vast majority of civil UAVs depend on civil GPS for navigation” [3].

UAVs can be categorized by several factors, Table 1 classification combines many aspects to make and general four big groups: Special task, Strategic, Tactical and micro or mini, according to their functions and capabilities as maximum take-off weight, maximum flight altitude, endurance, data link range and mission [25]. Usually, there is a direct proportion in size and systems complexity, where the drones with more Take of weight TOW have more backup and sophisticated equipment, are more reliable and less susceptible to attacks, besides the fact that they are out of the scope and out of range of civilian interaction and they do not belong to the easy distribution and accessibility equipment.

Table 1. UAV Classification[1]



	Category (acronym)	Maximum Take Off Weight (kg)	Maximum Flight Altitude (m)	Endurance (hours)	Data Link Range (Km)	Example	
						Missions	Systems
Micro/Mini UAVs	Micro (MAV)	0.10	250	1	< 10	Scouting, NBC sampling, surveillance inside buildings	Black Widow, MicroStar, Microbat, FanCopter, QuattroCopter, Mosquito, Hornet, Mite
	Mini	< 30	150-300	< 2	< 10	Film and broadcast industries, agriculture, pollution measurements, surveillance inside buildings, communications relay and EW	Mikado, Aladin, Tracker, DragonEye, Raven, Pointer II, Carolo C40/P50, Skorpio, R-Max and R-50, RoboCopter, YH-300SL
Tactical UAVs	Close Range (CR)	150	3.000	2-4	10-30	RSTA, mine detection, search & rescue, EW	Observer I, Phantom, Copter 4, Mikado, RoboCopter 300, Pointer, Camcopter, Aerial and Agricultural RMax
	Short Range (SR)	200	3.000	3-6	30-70	BDA, RSTA, EW, mine detection	Scorpi 6/30, Luna, SilverFox, EyeView, Firebird, R-Max Agri/Photo, Hornet, Raven, phantom, GoldenEye 100, Flyrt, Neptune
	Medium Range (MR)	150-500	3.000-5.000	6-10	70-200	BDA, RSTA, EW, mine detection, NBC sampling	Hunter B, Mücke, Aerostar, Sniper, Falco, Armor X7, Smart UAV, UCAR, Eagle Eye+, Alice, Extender, Shadow 200/400
	Long Range (LR)	-	5.000	6-13	200-500	RSTA, BDA, communications relay	Hunter, Vigilante 502
	Endurance (EN)	500-1.500	5.000-8.000	12-24	> 500	BDA, RSTA, EW, communications relay, NBC sampling	Aerosonde, Vulture II Exp, Shadow 600, Searcher II, Hermes 450S/450T/700
	Medium Altitude, Long Endurance (MALE)	1.000-1.500	5.000-8.000	24-48	> 500	BDA, RSTA, EW weapons delivery, communications relay, NBC sampling	Skyforce, Hermes 1500, Heron TP, MQ-1 Predator, Predator-IT, Eagle-1/2, Darkstar, E-Hunter, Dominator
Strategic UAVs	High Altitude, Long Endurance (HALE)	2.500-12.500	15.000-20.000	24-48	> 2.000	BDA, RSTA, EW, communications relay, boost phase intercept launch vehicle, airport security	Global Hawk, Raptor, Condor, Theseus, Helios, Predator B/C, Libellule, EuroHawk, Mercator, SensorCraft, Global Observer, Pathfinder Plus,
Special Task UAVs	Lethal (LET)	250	3.000-4.000	3-4	300	Anti-radar, anti-ship, anti-aircraft, anti-infrastructure	MALI, Harpy, Lark, Marula
	Decoys (DEC)	250	50-5.000	< 4	0-500	Aerial and naval deception	Flyrt, MALD, Nulka, ITALD, Chukar
	Stratospheric (Strato)	TBD	20.000-30.000	> 48	> 2.000	-	Pegasus
	Exo-stratospheric (EXO)	TBD	> 30.000	TBD	TBD	-	MarsFlyer, MAC-1

2.2 GPS spoofing detection techniques in the open literature

Securing GNSS signal authentication is about conjugate existing mitigation and detection techniques and set them up with the appropriate thresholds, becoming them a fundamentally a problem of statistical decision theory, to accurate understanding possible false alarm [14].

2.2.1 Classification Summarized Description

Spoofing detection solutions can be categorized in groups according to the hardware needed, the signal structure or layer level. This classification is done to understand the characteristics of each solution and comprehend their capacities and limitations.

2.2.1.1 Classification by Categories:

[1] Source: taken from Bento, M., "Unmanned Aerial Vehicles an Overview", 2008, p. 2, at http://www.insidegnss.com/auto/janfeb08-wp.pdf

Cryptographic or not cryptographic

Cryptographic methods rely on the unpredictability of security codes, such as P(Y), that modulate the GPS signal. For a spoofer to successfully attack would need to estimate the unpredictable chips on the-fly or perform a meaconing attacks, which is record and replay the complete spectrum of the GPS signal. It should be noted that GPS signal authentication is probabilistic, therefore it is not completely invulnerable [26]. On the other side, non cryptographic detection does not depend on encryption or digital signatures, nor security enhanced GPS signals.

Networked or stand alone

A networked GPs spoofing detection method requires a link to a communications network to download, for example, time, ephemeris or almanac data from a verified source on the internet whereas a stand-alone defense operates in isolation of any additional network [3].

Multi antenna o single antenna

Multi antenna or array processing methods are suited to detect and mitigate spoofing attacks by utilizing its spatial dimension. Using an array antenna, the individual direction of arrival of the satellites can be estimated together with the attitude of receiver attitude [27]. By comparing the transmitted satellite position information in the GNSS message to the previously projected, the spoofer can be detected and even blocked by constraining an adaptive beam-forming process [28].

2.2.1.2 Classification by layers

GPS spoofing can be investigated in the following operational layers: signal processing, data bit and position/navigation solution levels [8]

Signal Processing Level

This level is related to the structure of GPS L1 signals, including the modulation type, Doppler range, PRN signals, frequency, bandwidth, signal strength and many other features are publicly known (IS-GPS-200G & IS-GPS-705C). Therefore, knowing the structure and operational basics of the civilian GPS receivers, a spoofer can produce counterfeit signals that are like to the authentic GPS signals to mislead its target GPS receivers. Examples include: Power based methods, Signal Quality Monitoring methods (SQM), Time of Arrival (TOA) methods, Special processing methods and vestigial signal detection, among others. [8]

Data Bit level

Data bit level layer refers to processing of the GPS signals structure containing the GPS navigation message. In the L1 signal, it includes ephemeris data, almanac data, time parameters, service parameters and ionosphere parameters, distributed in five sub frames [19]. Examples of detection techniques are: Consistency check of received ephemeris, GPS clock consistency check and cryptographic authentication [8].

Position solution and Navigation Level

The final spoofing detection level, occurring during the time and position calculation solution is done to be presented to the application, it can be considered along to an application layer. Examples include: Receiver Autonomous Integrity Check (RAIM) and consistency check with other solutions like other GNSS, IMU, compass, Wi-Fi position and cellular networks positioning [8].

2.2.2 Description of GPS spoofing detection techniques

In this section are briefly described the detection method found in the open literature.

2.2.2.1 Low-complexity gps anti-spoofing method using multi-antenna array

Method based on an antenna array processing technique. This technique has basically three parts, the first one refers to detection while the second and third refers to mitigation: (1) Spoofing Spatial Signature Vector (SSV) estimation: The proposed method is established based on the fact that all noisy PRN codes are broadcasted from the same source in space; (2) Null steering Unit: steers a null toward a spatial area where the highest spatial energy is coming from; (3) Power Maximization Unit: To avoid unintended reduction of real signals, the received power of each legit signal is amplified individually after the spoofing mitigation [23].

2.2.2.2 Data bit latency defense

In this method "*the receiver looks for a data bit sign change between consecutive accumulations at the C/A code-length interval. If a sign change is detected at other than an expected data bit boundary, then the target receiver raises a flag*" [6].

2.2.2.3 Vestigial Signal Defense

The fundament of this technique is the strain of suppressing the legit signal after effective lift-off of the DLL tracking points. The receiver inspects the presence of legit vestige signals to distinguished more than one correlator peaks or monitors previously determined non-tracked signals until a threshold is reach [6].

2.2.2.4 Antenna-based joint attitude estimation

The principel of this method is on the use of estimated Directions of Arrival for differencing the spoofing and legit GNSS signals. The projected DOAs which are then compared with the projected directions of the satellites calculated with the ephemeris data of the navigation message [28].

2.2.2.5 Correlator output distribution analysis

This detection method monitors the distribution of each correlator output. If the distribution differs from the distribution of the authentic signal a spoofing attacks can be triggered. A spoofing attack is spotted if this distribution considerably diverges from the one of the authentic signal. The proposed antispoofing technique detects when the spoofing attack is using fake correlation peak, and as mitigation technique, the vector based receiver tells to regress to the measurements of the discarded tracking loops [22].

2.2.2.6 Detection of Spoofed GPS signals at code and carrier tracking level

Intermediate spoofing attacks affect the usual signal processing of code and carrier tracking loops, the proposed detection method can be implemented at this level to discover spoofed GPS signals, by characterizing the Cross Ambiguity Function (estimate of a function when the first correlation peak is detected) distortion in the signal lift off [29].

2.2.2.7 Receiver Autonomous Integrity Monitoring RAIM

When the number of spoofed pseudo range measurements is 1 or 2, the RAIM techniques can distinguish and remove the counterfeit spoofed measurements. However, when there is higher number of spoofed measurements, RAIM methods may not discover the presence of spoofing signals [8].

2.2.2.8 Spoofing Discrimination Based On Absolute Power Monitoring

By monitoring the noise floor to detect uncommon noise level increments caused for the spoofing interference. The noise floor of the receiver can be raised by the the interference produced by the spoofer. Furthermore, the receiver should have the capability to discriminate the signals which absolute power is two decibels higher than the greatest possible power of L1 C/A signal on earth surface, which is 153 dBw [31].

2.2.2.9 GPS Spoofing Detection using RAIM with INS Coupling

By monitoring discrepancies between GPS spoofed measurements and Inertial Navigation System measurements, there is proposed a set of equations to measure the likelihood that the position error exceeds an acceptable limit. In this detection method, RAIM redundancy is provided by INS measurements, different than their conventional employment where detection is delivered through satellite redundancy. To improve the detection abilities, a time history of GPS measurements can be used to estimate the position vector [32].

2.2.2.10 Monitor the relative GPS signal strength

Most GPS receivers measure C/N0 as a parameter to determine signal quality. In Sky clear condition there will be only slightly changes in this indication, however during spoofing attacks a higher power signal is needed to deceive the receiver where abrupt changes in signal power can flag the presence of an attack [23], therefore the average signal strength could be recorded and compared periodically within a predetermined threshold, otherwise flag can be raised to alert possible attack [33].

2.2.2.11 Monitor the signal strength of each received satellite signal

In some cases, spoofers make the signals from each replicated satellite of similar strength. Real GPS signals vary from satellite and change during time [33].

2.2.2.12 Monitor SV identification codes and number of received signals

The number of simulated satellites by a spoofer can have limitations and their behaviour can be different from legit satellites signals. Monitoring over time the number of satellite signals received and the satellite IDs may demonstrate attacks attempts. This is particularly right on the case of an unsophisticated spoofing attack, where there is not input from the real satellite constellation at a specific time [33].

2.2.2.13 Check the time intervals

This method refers to monitoring the behaviour of most satellite simulators or some GPS spoofers, it is perceived when a GPS receiver acquires all the satellite signal simultaneously, in normal conditions the receiver pick up the signal from each satellite at different moments [33].

2.2.2.14 Received Power Variations versus Receiver Movement

Considering only one source broadcasting all the fake satellite GPS signal, the movement of the receiver in relation to the spoofer can change the signal power received from spoofing signals, where in normal conditions (low multipath, clear sky, etc.) no considerable changes in signal power will occur, because the distance is irrelevant compared with the distance from where the real satellites are [23].

2.2.2.15 L1/L2 Power Level Comparison

Monitor the difference of power signal between L1 and L2 bands looking for amoralities in the predefined power difference, when usually spoofers only emulate the civil band of GPS [8].

2.2.2.16 Multi antenna Spoofing Discrimination

An antenna array structure detects spoofing signals contemplating their spatial correlation, GPS correlators are applied to various beam outputs to sense and pinpoint spoofer [34].

2.2.2.17 PRN Code and Data Bit Latency

Time of Arrival technique, that checks the data bit latencies in periods of more than 20 microseconds between the authentic GPS signal and the unavoidable delay generated by the spoofer when recreating a fake data bit structure. A drawback in this technique the predictability of GPS signal structure because the low update frequency of the frames [23].

2.2.2.18 L1/L2 Signals Relative Delay

Time of Arrival Technique, it is constantly checking between the already known correlation peak difference of L1 and L2, looking for abrupt changes in this value [23].

2.2.2.19 Distribution Analysis of the Correlator Output

This function is used to detect the presence of spoofing signals, by monitoring the fluctuations of a chi-squared distribution expected for the correlator output, during the different phases of a spoofing attack. A drawback of this technique is the fluctuations resented during multipath propagation can also change the chi squared distribution, so the methods work only in LOS conditions [23].

2.2.2.20 Consistency Check with Other GNSS

Constant checks against PVT solutions of other GNSS can determine spoofing threats. It is within the category of standalone detection solution because modern receivers are coming with multi GNSS reception. Generally, a spoofer only emulates GPS L1 signal, by comparing with other GNSS solution can be determined if the receiver is being subject of a spoofing attack, this is useful to identify of being target of an attack [23]. However, the effectiveness of this method is limited by the difficulty of mounting a spoofing attack only increases linearly with the number of new signal ensembles [3].

2.2.2.21 Consistency Check with Other position technologies

The GPS positioning can be compared with the position solution obtained by mobile or Wi-Fi networks, it is limited by their service coverage and accuracy.

2.2.2.22 Consistency Check with Other technologies

Besides location solutions, networked detection implementations can be used to compare GPS data from a third party sources looking for inconsistencies. One possibility is to compare time from NTP online services, using stratum 1 servers time (corrected with the packet delivery timestamp) with the GPS received time can detect rudimentary and non accurate GPS spoofing attacks. Other alternative is to verify the integrity of ephemeris or almanac data comparing it with a trust source from the internet [33].

2.2.2.23 Consistency Check with other sensors

Analysing data from auxiliary devices such as pitot static or barometric instruments, IMU or compass can help to determine a spoofing attack, by comparing and predicting abrupt or unexpected changes with the PVT solution extracted form the GPS receiver [23].

2.2.2.24 Spread-Spectrum Security Codes on L1C (SSSC)

Cryptographic method which requires that a digital key generated by Spread-Spectrum Security Codes to be transmitted the over the navigation message. The implementation time is estimated in years and needs changes in the GPS interface specification [35] [36].

2.2.2.25 Navigation Message Authentication (NMA)

The Navigation Message Authentication method inserts public-key digital signatures inside the GPS civil navigation message, which offers a convenient delivery for such signatures, using the undefined messages in the GPS Interface Specification. The implementation is estimated to be in years [K. Wesson, M. Rothlisberger, and T. E. Humphreys, [26] [37].

2.2.2.26 Received Ephemeris Consistency Check

Check if there is presented inconsistencies between the extracted ephemeris data of different satellites [23].

2.2.2.27 GPS Clock Consistency Check

Check if there is presented inconsistencies between the extracted time of different satellites to alert from a spoofing attack. It depends on incapability of the spoofer to keep the consistency of the data [23].

2.2.2.28 Detecting False Signals with Automatic Gain Control AGC

Using the Automatic Gain Control component, found in many GPS receivers, to detect possible spoofing and jamming attacks by flagging drastic changes in their values, it should be noted that this changes can be causes by thermal variations. [Detecting False Signals with Automatic Gain Control, 2012, By Holly Borowski, Oscar Isoz, Fredrik Marsten Eklцf, Sherman Lo, and Dennis Akos]. The weakness, is that by only monitoring the AGC voltage or the called RF power, will be possible to face constant false alarms cause by for example Solar Radio Burst or by jammers [14].

2.2.2.29 Consistency check of data within the GPS PVT solution

Monitors expected and normal behaviour of the Position, Velocity and Time solution, considering normal conditions, so abrupt changes in speed, or drastic changes in altitude or position can be signal of and successful GPS spoofing attack.

2.2.3 Summary table

In this section it is a summary of the detection methods investigated from the open literature, and are discriminated by the receiver requirement capability, if the method is cryptographic, networked, multi or single antenna and the layer of where they belong.

Table 2. GPS Spoofing detection methods summary

Name	Description	Encrypted	Networked or stand alone	Single or multi antenna	Layer	Receiver required capability
A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array	Estimates the direction where all spoofing pseudo random noise codes are transmitted, considering they all come from the same source in space and steer a null value to them	No	Stand alone	Multi	Signal processing	Multiple receiver antennas
Data Bit Latency Defence	The target receiver continuously monitors the bit lock in the C/A code length, looking for data bit sign changes	No	Stand alone	Single	Data bit	Monitors the bit lock in the C/A code length
Vestigial Signal Defence	Monitor the presence of legit vestige signals to distinguished more than one correlator peaks	No	Stand alone	Single	Signal processing	Filter out vestige legit GPS signals
Antenna-based joint attitude estimation	Using the estimated DOA for discriminating between authentic GNSS and the spoofing signals.	No	Stand alone	Multi	Data bit	Miniaturized antenna array

Correlator output distribution analysis	Detects if this correlator output distribution considerably deviates from the distribution of the authentic signal.	No	Stand alone	Single	Signal processing	Monitor the distribution of the correlator output
Detection of Spoofed GPS signals at code and carrier tracking level	Monitors the distortion during the signal lift off that happens in intermediate spoofing attacks.	No	Stand alone	Single	Signal processing	Requires special signal processing capabilities
Receiver Autonomous Integrity Monitoring RAIM	Detects spoofed signal when there is only two PRN	No	Stand alone	Single	Position solution and navigation level	RAIM implemented
Spoofing Discrimination Based On Absolute Power Monitoring	Monitors absolute signal power, between the typical and maximum possible values, with an uncertainty of 2dB	No	Stand alone	Single	Signal processing	Receiver should capable to analyse the absolute received power and noise floor
GPS Spoofing Detection using RAIM with INS Coupling	Monitors discrepancies between GPS spoofed measurements and Inertial Navigation System measurements, obtained by RAIM algorithm.	No	Stand alone	Single	Position solution and navigation level	IMU sensors and RAIM implemented
Monitor the relative GPS signal strength	Monitor the abrupt changes in signal power that happen during spoofing attacks	No	Stand alone	Single	Signal processing	Signal strength monitoring
Monitor the signal strength of each received satellite signal	Monitor the signal strength of each received satellite signal	No	Stand alone	Single	Signal processing	Signal strength monitoring
Monitor satellite identification codes and number of satellite signals received	Tracking the number of satellite signals received and the SV IDs codes over time can detect attacks attempts	No	Stand alone	Single	Signal processing	Monitor SV PRN
Check the time intervals	Check the time intervals between the acquisition of each satellite signal	No	Stand alone	Single	Signal processing	Monitor intervals between SV fix time
Received Power Variations versus Receiver Movement	Monitor considerable and abnormal changes in signal power when the receiver is in movement	No	Stand alone	Single	Signal processing	Antenna Movement and Monitor Signal Strength
L1/L2 Power Level Comparison	Monitor the difference of power signal between L1 and L2 bands looking for amoralities in the predefined power difference	No	Stand alone	Single	Signal processing	Receiver must process L1/L2 bands
Multi-antenna Spoofing Discrimination	GPS correlators are applied to numerous beam outputs to spot and locate spoofer	No	Stand alone	Multi	Signal processing	Multiple receiver antennas
PRN Code and Data Bit Latency (TOA)	Checking unavailable time delays of the spoofer data bit boundaries with respect to the authentic ones	No	Stand alone	Single	Signal processing	Time of Arrival Analysis and Monitoring
L1/L2 Signals Relative Delay (TOA)	Monitors the already known correlation peak difference of L1 and L2, looking for abrupt changes in this value.	No	Stand alone	Single	Signal processing	Receiver must process L1/L2 bands and Time of Arrival Analysis and Monitoring
Distribution Analysis of the Correlator Output	Monitors the fluctuations of a chi-squared distribution of the correlator output	No	Stand alone	Single	Signal processing	Distribution analysis of correlator outputs
Consistency Check with Other GNSS	Constant checks against PVT solutions of other GNSS	No	Stand alone	Single	Position solution and navigation level	Multiple GNSS receiver chipset

Consistency Check with Other position technologies	Comparison of the position solution with the obtained by mobile or Wi-Fi networks	No	Networked	Single	Position solution and navigation level	Internet connection
Consistency Check with Other technologies	Comparison of GPS data integrity with the obtained of third party sources (ephemeris, almanac, time)	No	Networked	Single	Position solution and navigation level	Internet connection
Consistency Check with other sensors	Analysing and comparing GPS data with auxiliary devices like IMU, compass or pitot static instruments.	No	Networked	Single	Position solution and navigation level	A devices like IMU, compass or pitot static instruments
Defence Based on Spread-Spectrum Security Codes on L1C (SSSC)	Transmission of a digital key generated by Spread-Spectrum Security Codes over the navigation message	Yes	Stand alone	Single	Signal processing	Modification in the GPS IS: L1C Data Channel Spreading Code
Defence Based on Navigation Message Authentication on L1C, L2C, or L5 (NMA)	Insertion of a public-key digital signatures inside the GPS civil navigation message	Yes	Stand alone	Single	Signal processing	Modification in the GPS IS: 2 New CNAV Messages
Received Ephemeris Consistency Check	Inconsistencies between the extracted ephemeris data of different satellites	No	Stand alone	Single	Data bit	Monitor and compare ephemeris
GPS clock Consistency Check	Inconsistencies between the extracted time of different satellites	No	Stand alone	Single	Data bit	Monitor and compare time
Detecting False Signals with Automatic Gain Control	Monitors abrupt changes in the Automatic Gain Control values to detect the presence of signal interference	No	Stand alone	Single	Signal processing	Monitor AGC
Consistency check of data within the GPS PVT solution	Monitors normal and expected behaviour of the PVT solution	No	Stand alone	Single	Position solution and navigation level	Monitor PVT

3 Solution Development

3.1 Scenario description and definition

In this section is described the situation framework where the spoofing attacks is conducted. Firstly, a schema is defined for picturing the interaction among the participants and their capabilities for delimitating their involvement and role in the analysed scenario.

Secondly, there is a technical description of the threat actor equipment, its attack strategy, the Unmanned Aerial System to be attacked plus its capabilities and the detection strategy.

3.1.1 Schema

In order to determine and limit the interaction between the participants and their capabilities in the GPS spoofing attack scenario the schema defines the RF environment, the trust radios and the UAS WLAN network which is technically the UAS itself.

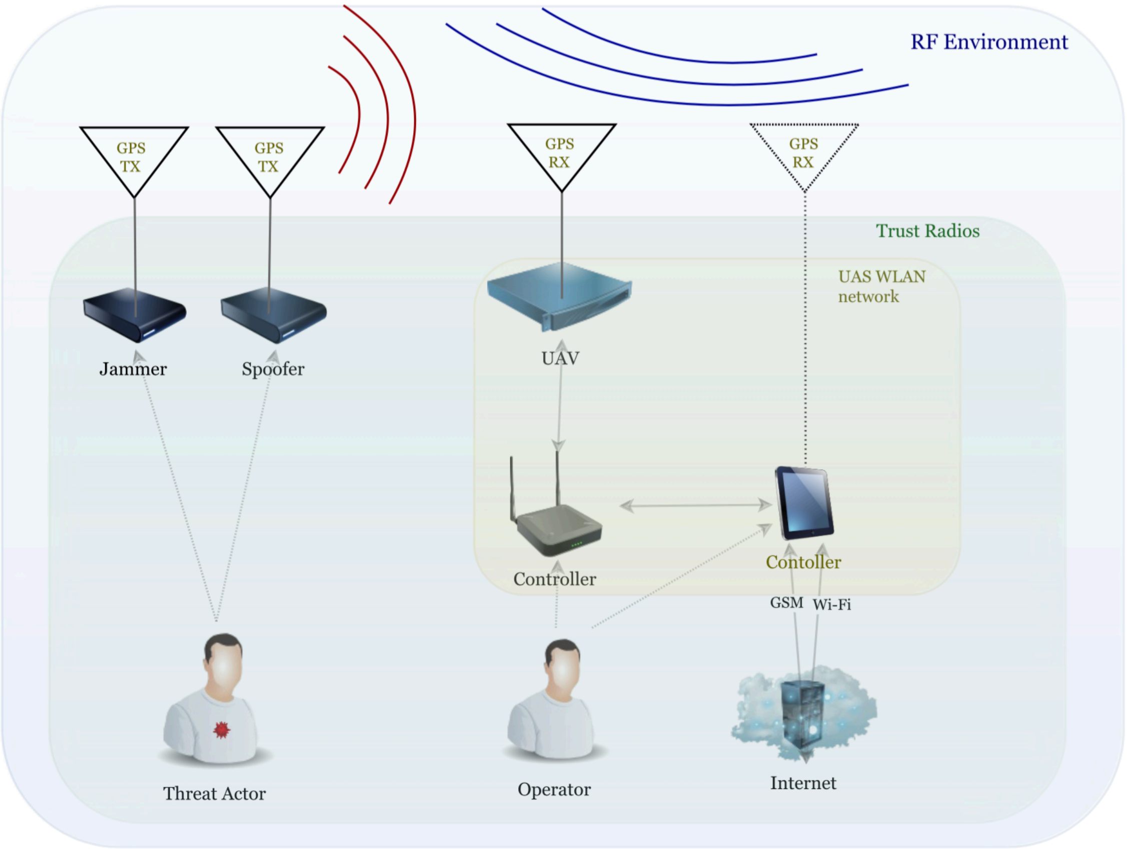


Figure 1. Spoofing attack schema

The Radio Frequency environment is the outer level, and represents the freely uncontrolled spectrum where the attack takes place, because the authentic signal coming from the GPS constellation can be counterfeited and interfered by devious signal coming from the threat actor. The environment conditions are considered to be normal: with a flexible but not extreme weather and without third cases interferences or signal obstructions. Simplistic and meaconing GPS spoofing attacks do not synchronize correlation peaks because the legit signal is drowned by counterfeit signals, so that, distance and direction between actors will no be relevant. Range depends on hardware antenna to produce signal power.

The Trust Radios level encloses where the security is not relevant and consider to be ideal, so there is no inquiring about safety in the telemetry, communication channel and hardware or integrity, availability and authenticity in the data. Finally, the UAS WLAN network defines the hardware components of the UAS, important to remark that not only the Ground Control Station can control the UAV, but the smartphone can also be used and works harmonically as and add-on in the system, in the smartphone is the only mean for the operator to watch the video camera feedback.

3.1.2 Threat Actor

The threat actor or attacker is the external entity responsible to execute the GPS spoofing attack to the UAV in order to counterfeit and take control of the GPS PVT solution with devious purposes. In this case the attacker has a GPS spoofer and a GPS jammer.

The spoofer used in this project consists of the open source Github projects sdr-gps-sim, developed by Takuji Ebinuma, that generates binary data representing the GPS satellites stream at specified location or at simulated trajectory[1], which will be broadcasted through the Nuand BladeRF x40, a full-duplex Software Defined Radio card serving as a transmitter[2]. BladeGPS is similar project also done by Ebinuma, which main difference is that it doesn't have the 3 minutes' binary file creation limitation presented in the sdr-gps-sim, because it creates and transmits the signal in real time.

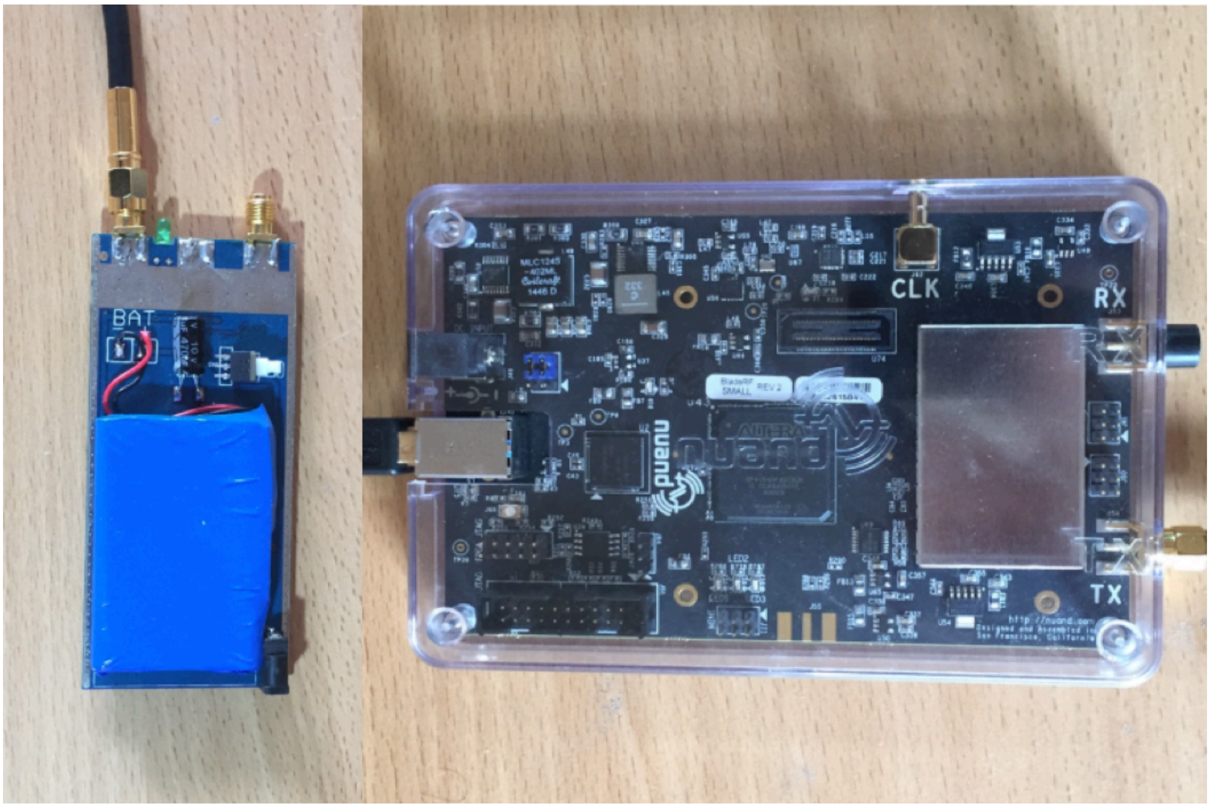


Figure 2. Jammer and Spoofer SDR card

The spoofer is capable of recreating readable and structured GPS satellites L1 that allows a simplistic GPS spoofing attack. Not other GNSS or military GPS signal can be simulated in the current version.

[1] https://github.com/osqzss/gps-sdr-sim

[2] https://www.nuand.com/blog/product/bladerf-x40/

Instead of real time satellite ephemeris data, the software requires ephemeris RINEX files, archive maintained and publish by the NASA every 24 hours[1], this meant that the data in the daily archive can be off as much as 24 hours from the real satellites locations[18].

In the simulated PVT solution, the time is determined by the information on the ephemeris data file, however, the date can be manipulated by changing the GPS week field and the hour by specifying it with a sdr-gps-sim command. On the other hand, velocity and position input data can be a fix location, plain coordinates and altitudes from a set of 3d locations or positions in the $GPGGA of the NMEA format.

3.1.3 Attack strategy

In order to undesiring how to achieve a successful GPS spoofing attack, it has to be considered the practical limitations of a simplistic spoofing attack, which essentially is that if the receiver is in tracking phase, the counterfeit signals will not be acquired by the receiver, without force-reacquisition technique [22].

The spoofer operates by transmitting structured fake GPS signals which are interpretable by the GPS receivers. The target receiver can be considered captured when attackers PVT solution is being injected into the UAS. The position velocity and time data is not indented to match the legit signal used by the receiver at that moment, because the drone location should be known a priori or complex radar setup should be needed, besides the accuracy required is a challenge out of the scope of this project. This means that hijacking the drone without abrupt changes in the PVT solution or without noticeable DoS cannot be accomplished.

There are two attacking scenarios that could take place based on the schema and spoofer characteristics, and depend on the GPS receiver acquisition or tracking phase. During the acquisition phase the counterfeit signals are competing against the legit GPS signals, only one can be successfully be acquired by the receiver and then continue with the process to deliver the PVT solution. The signal selection decision is influenced by the higher power spoofing signals, since the AGC automatically regulates the receiver incoming gain according to the stronger signals [8] [38], and as said before legit GPS signal strength are weak enough to be easily overlapped by any radio transmitting at similar frequencies.

It is important to remark that receivers have hot, warm and cold start modes. This modes configuration varies depending on the vendor, but generally when the GPS performs a cold start no previously stored information is used; in a warm start caching is quite common and is the reason a warm-boot of a GPS receiver takes less time to acquire lock [Tyler Nighswander, GPS software attacks] it can store time, position, ephemeris and/or almanac data; and in a hot start all possible information is stored and used to calculate the new PVT solution when the receiver is turned on. The implications can be prolonged latencies for acquiring an initial GPS lock or infinite loops as reported in some cases of spoofing when initiated the receiver with a warm start [2].

If the spoofer which emits signal at simplistic spoofing attacks level when the GPS receiver is on tracking mode, there is no chance to successfully take control of the receiver because the is already a GPS lock, therefore the counterfeit signals will be read but not processed and the the noise floor variable will increase considerably [8].

3.1.4 UAS

[1] http://cddis.nasa.gov/Data_and_Derived_Products/GNSS/broadcast_ephemeris_data.html

The UAS in what this project was based on is the quad copter 3DRobotics solo[1], which results can also apply to other similar designed UAVs, those whose firmware and communication protocol also use or are based on the Dronecode Software Platform. This suite encompasses open source development projects that control flight and enable mission planning, or define standard communication protocols like MAVLink. Besides 3DRobotics, the Dronecode platform has been adopted by many of the most representative organizations of drone technology, like Parrot, Qualcomm, Intel, DroneDeploy, Yuneec and Walkera[2].

3.1.4.1 Architecture System Diagram

The 3DR solo Unmanned Aerial System is composed by the UAV and the controller, optionally, the Solo App and a GCS can be used either for visualize the video stream or as an interface for controlling the drone by connecting to the WLAN of the UAS[3]. In Figure 2, Solo refers to the UAV, the controller is the joystick where the communications are concentered from all the devices, the App is hosted in a smartphone or tablet and the GCS refers to a software that resides in a laptop.

[1] https://3dr.com/solo-gopro-drone-specs/

[2] https://www.dronecode.org/dronecode-software-platform

[3] https://dev.3dr.com/concept-architecture.html

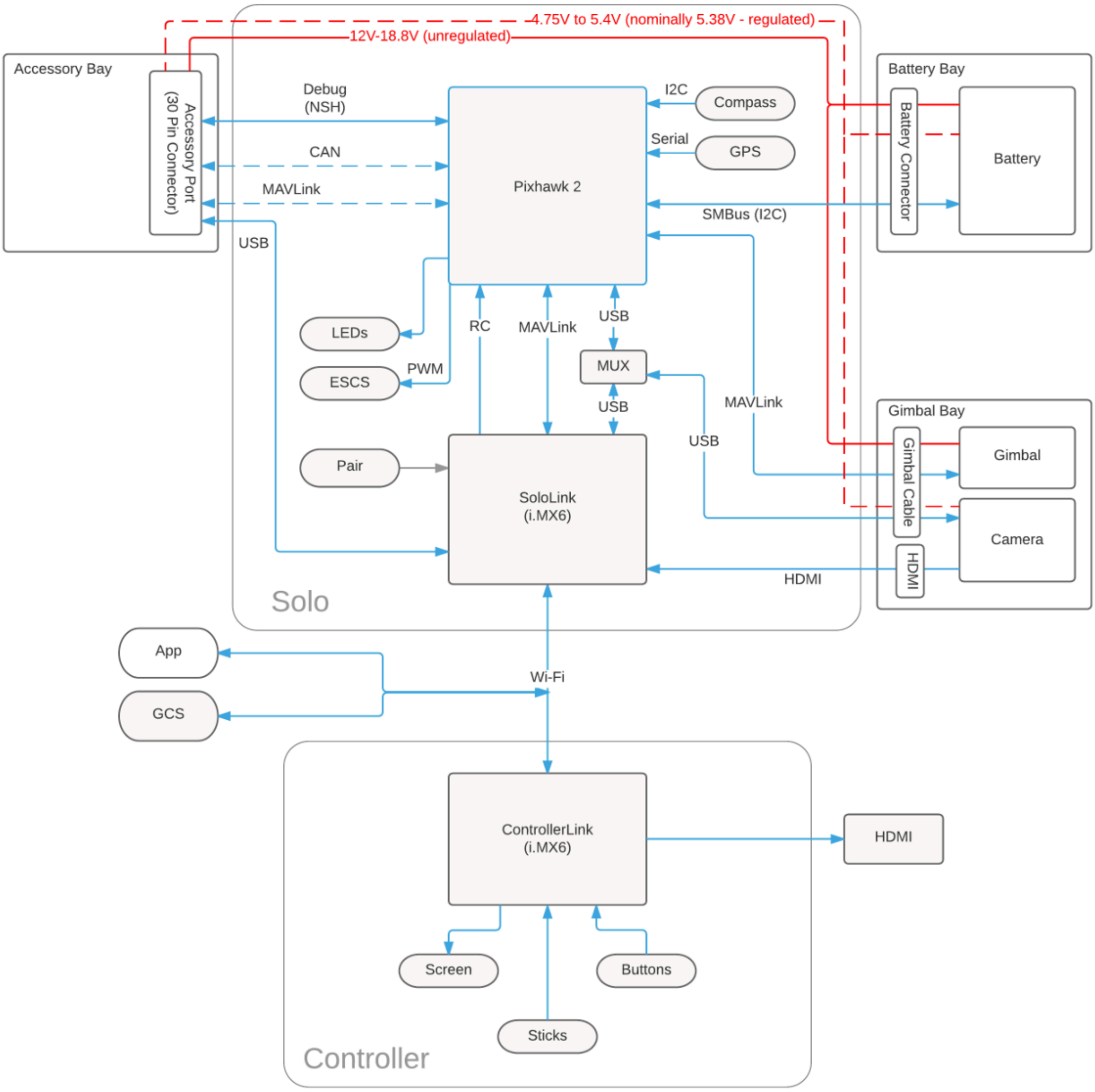


Figure 3. Solo System Architecture[1]

.

3.1.4.2 UAS hardware components description

The drone is a quad copter designed carry a camera as a payload. The navigation is GPS based but can has manual mode fly option. The relevant technical speciation as an aircraft for further analysis in the project are that can fly within ranges up to 8 km, its maximum speed is 89 km/h, maximum ascent speed 10 m/s and altitude limit is hardcoded to be up to 46 meters, this information will be used to determine the alert limits and thresholds at which is physically not possible the drone to fly[2].

Barometric pressure sensor is use to calculate the pressure altitude of the drone, this measure is susceptible to drifting and depends on temperature measure, therefore is it not as accurate as

[1] Taken from https://dev.3dr.com/concept-architecture.html
[2] https://3dr.com/solo-gopro-drone-specs/

GPS altitude indication. Some UAVs uses inputs the measurements into Kalman filter get the final altitude [10].

The GPS sensor which the drone has by factory configuration, is u-Blox NEO-7N-0-002 [39] this is a standalone GNSS module that even has engine for reading GPS and GLONNAS only can do it once at a time[1]. The flexibility and modularity of the system allows to upgrade the receiver by the newest version the NEO-N8M-0-01 (firmware v3.01), chipset used for following analysis and tests in this work. The main differences are the capacity of multiple GNSS reception, reception of GALILEO, and the built-in spoofing flag detection[2]. However, the method is only successful when the signal is genuine first and when the transition to the spoofed signal is being observed directly, the receiver is not working in single GNSS mode or when is being used the PRS feature of GALIEO [40] [41]. Additionally, there is not developed the capacity to bring up from the GPS receiver, the spoofing flag information to the application layer for the Solo App, the GCS or the controller.

Smartphone is an optional component of the architecture that hosts the Solo App. Using the smartphone for commanding the drone brings up additional conveniences for providing external and backup resources to the primary UAS sensors, like a Wi-Fi or GSM connectivity and an additional GNSS antenna.

3.1.4.3 UAS software components description

Solo is a Linux based system running a Yocto Distribution, connected to a Pixhawk autopilot which controls flight modes, stabilization, and recovery. Pixhawk communicates over the MAVLink telemetry protocol to both the on-board Linux computer and downstream devices like the Controller and mobile phone Solo apps. The Linux system controls high-level operation of the copter: smart shots, camera and gimbal control, mobile app communication, and accessory interaction are all implemented in this layer[3].

There is different open source flight planning GCS software for drones, like QGroundControl, Mission Planner, and Tower. The proposed solution for this work is based on the 3DR services SDK, the user interface for Dronekit and their projects Android Dronekit and Python Dronekit. Android Dronekit is the API for developing and customizing the Tower Drone Control App[4]. It is important to remark that the GPS spoofing detection solution will analyse and compare the data at the level of the 3DR services SDK, so that, it will be not possible to use the data if it resides exclusively in other layers and there is required development o specific firmware customization transport it.

MAVLink is a standard protocol used for communications by the Common Message Set list, which is the reference message set implemented by most ground control stations and autopilots. However, not all the information on the messages is always available along the different UAS platforms, it depends on the default configuration of the constructed firmware. In the case of the Dronekit Android API, all the MAVLink messages where listened to retrieve the available information for the GPS spoofing detection solution[5]. All the obtained messages containing drone values were: GPS_STATUS, AHRS, AHRS2, ATTITUDE, COMMAND_ACK, EKF_STATUS_REPORT, GLOBAL_POSITION_INT, GPS_RAW_INT, HWSTATUS, NAMED_VALUE_INT, POWER_STATUS, RADIO_STATUS, RAW_IMU,

[1] https://www.u-blox.com/sites/default/files/products/documents/NEO-7_ProductSummary_(UBX-13003342).pdf

[2] https://www.u-blox.com/sites/default/files/NEO-M8N_ProductSummary_(UBX-16000345)_5.pdf

[3] https://dev.3dr.com/concept-architecture.html

[4] https://3dr.com/3dr-releases-tower-drone-flight-control-app-3dr-services-app-store-drones/

[5] https://pixhawk.ethz.ch/mavlink/

RC_CHANNELS_RAW, SCALED_IMU2, SCALED_IMU3, SCALED_PRESSURE, SCALED_PRESSURE2, SENSOR_OFFSETS, SERVO_OUTPUT_RAW, SYSTEM_TIME, SYS_STATUS, TERRAIN_REPORT, VFR_HUD, ATTITUDE_QUATERNION. However, the relevant messages for the purpose of the project are GLOBAL_POSITION_INT, this is the filtered global position fused with other sensors like accelerometers; GPS_RAW_INT, the raw sensor values as returned by the GPS; SCALED_PRESSURE, readings for the typical setup of one absolute and differential pressure sensor; SCALED_IMU, the raw IMU reading for the accelerometer setup; and VFR_HUD which are the metrics typically displayed on a HUD.

In the scenario stated is contemplated the capacity of internet connection with either Wi-Fi or GSM networks. Internet is a big source of data ready to use in Android Studio platform, because this robust platform has extensible and diverse catalogue of libraries and API for developing applications and using desired data of the smartphone sensors. From internet websites can be retrieved data to verify the authenticity of the data obtained from the drone GPS receiver, like ephemeris, almanac and time. Although not accurate as GNSS, from the sensors can be used the location provided by Wi-Fi and GSM networks, additionally it can be extracted the GPS data (equally vulnerable to GPS spoofing attacks) and information as the GPS status like Signal to Noise Ratio, number of satellites visible and satellite PRN can be acquired by calling already designed classes or by setting up NMEA listener.

3.2 Select and compare GPS spoofing detection techniques

In this section will be described the criteria to select and implement the detection method plus a brief analysis for selecting or not each detection method.

3.2.1 Detection methods selection criteria

Basically, the criteria to select the is the detection methods to be used in the proposed solution is that the methods' requirements can be satisfied. The methods have to be suitable for the specification and configuration of this project context and scenario.

However, not only the required capability of receiver is satisfied in order to select the spoofing detection method, as the solution is done through the Android Studio software, to determine possible spoofing attacks the input data to be processed in the calculations should be able to reached the application layer where the solution is being developed, in this case the Dronekit Android API on the Android Studio platform. Therefore, the detection methods which information reside in different layers will be excluded from the final selection.

Additionally, during the selection will be discarded the encrypted, L2 signal based and multi antenna methods because of complexity. The encrypted methods require changes in the GPS architecture definition, the multi antenna solutions need sophisticated implementations out of the scope of this project and the L2 signal can be read only by military GPS receivers.

3.2.2 Analysis and selection of the GPS spoofing attack detection methods

3.2.2.1 Low-complexity gps anti-spoofing method using multi-antenna array

This method is discarded because is a multi antenna solution, additionally, input signals direction estimation complexity is out of the scope of the project.

3.2.2.2 Data bit latency defense

Monitoring the GPS receiver bit lock is out of the scope of the project, because the required data can no be brought to the Android Studio where the calculations and processing take place.

3.2.2.3 Vestigial Signal Defense

The process of filtering out vestige signal is done in the data bit layer and cannot be done in the Android Studio layer.

3.2.2.4 Antenna-based joint attitude estimation and spoofing detection

This method is discarded because is a multi antenna solution, additionally, to estimate the signal DOAs for distinguishing the spoofing and authentic GNSS signals, requires complex correlation of output distribution from different antennas.

3.2.2.5 Correlator output distribution analysis

This detection method requires monitoring the distribution of each correlator output, but information needed resides at the signal processing layer in the GPS receiver, reason why it can not be implemented in this work.

3.2.2.6 Spoofed GPS signals at code and carrier tracking level

This method does not apply for this project because in simplistic GPS spoofing attacks there is not correlator peak lift off, as this process is part or more sophisticated attacks. Additionally, in the the information cannot not be brought into the projects developing layers.

3.2.2.7 Receiver Autonomous Integrity Monitoring RAIM

Although this algorithm may detect spoofing attacks, it is accuracy is not practical [8], and the its design purpose is to filter out GPS multipath effect.

3.2.2.8 Spoofing Discrimination Based On Absolute Power Monitoring

The GPS u-Blox N8M is able to monitor the AGC and the noise floor variables used determine the absolute power, however this values reside in the GPS data bit layer and can not be brought up to the Android Studio Platform.

3.2.2.9 GPS Spoofing Detection using RAIM with INS Coupling

This method requires a set of equations that correlate RAIM with INS sensor measurements, therefore implementation requires advance processing and algorithms designs. Although this method is in the Position solution and navigation layer, its high complexity discards it from this selection process.

3.2.2.10 Monitor the relative GPS signal strength

Signal to Noise Ratio is a parameter that determine signal quality or strength, although the drones GPS provides this measurement, and the message GPS_STATUS of the MAVLink communication protocol has defined the last field for this value, it is not in the default list of MAVlink broadcasted messages through the SoloLink or Pixhawk of this UAS, therefore it cannot be brought to the Android API. On the other side, the smartphone GNSS antenna has also SNR reading capabilities which can be called directly within the class method GpsSatellite.getSnr() or by parsing information of the class GpsStatus.NmeaListener() of the Android Studio. This method is requiring information from the data bit layer that is brought up thought the NMEA protocol to the position solution and navigation layer.

3.2.2.11 Monitor the signal strength of each received satellite signal

Under the previous method philosophy, this technique can also be implemented, the difference is in the definition of thresholds values, because will apply for the SNR values of each satellite and not for the average signal strength of all SVs.

3.2.2.12 Monitor SV identification codes and number of received signals

This technique can be implemented because to keep track of the number of satellite signals received and the id codes of the SVs, it can be used the method getPrn() from the same GpsSatellite() class, this information can also be obtained from the NMEA listener of the smartphone.

3.2.2.13 Check the time intervals

Monitoring when a GPS receiver acquires all the satellite signal simultaneously can be done by correlating the number of satellites being tracked with fix taken time, during periods of time, this information can be obtained from the NMEA listener.

3.2.2.14 Received Power Variations versus Receiver Movement

It is not possible to use the noise floor and AGC values in the Android Studio layer, so that this method can not be implemented in this case scenario. Additionally, range of the drone is out of the scope of the project.

3.2.2.15 L1/L2 Power Level Comparison

This method is discarded because the receiver requires processing L1/L2 signals.

3.2.2.16 Multi antenna Spoofing Discrimination

This method is discarded because its setup requires a multi antenna array structure.

3.2.2.17 PRN Code and Data Bit Latency

This method is discarded because the time of arrival of the data bit structure can not be calculated in the Android Studio layer where the solution is developed.

3.2.2.18 L1/L2 Signals Relative Delay

This method is discarded because the receiver requires processing L1/L2 signals.

3.2.2.19 Distribution Analysis of the Correlator Output

This method is discarded because the correlator output values needed to calculate the chi-squared distribution reside in the data bit layer and can not be taken out from this layer.

3.2.2.20 Consistency Check with Other GNSS

Compares PVT solution between different GNSS to determine discrepancies and successfully detect GPS spoofing attacks, the effectiveness should be high because the spoofer used in the project is only capable of counterfeit GPS L1 signals. Although the smartphone and the drone GPS chipsets have multiple reception GNSS capabilities, this method can not be implemented because the receivers PVT solution is calculated in combination of different GNSS satellites, and the sources are not easily discriminated.

A possible solution could be compare the drone GPS and the smartphone GLONNAS, GALILEO or BeiDou PVT solutions; nonetheless, enabling or disabling specific GNSSs in the smartphone can not be done from the application layer where the GPS spoofing detection calculation takes place.

Other alternative could be using the NMEA listener to obtain particular GNSS location, time or speed, but the PVT solution is presented under the talker ID prefix GN, that indicates that the data proceed from multiple GNSS [42].

Using a different GNSS rather than GPS in the drone, it is out of the objective of the project.

3.2.2.21 Consistency Check with Other position technologies

This method can be implemented by extracting the location from the smartphone Wi-Fi and GSM. There are specific methods which allow this feature in the Android Studio platform.

3.2.2.22 Consistency Check with Other technologies

In this scenario is contemplated the access to Internet from the smartphone that host the Solo App, therefore, comparing time from NTP online services, ephemeris or almanac with the drone GPS data can be implemented.

3.2.2.23 Consistency Check with other sensors

The transmitted MAVLink messages SCALED_PRESSURE and SCALED_IMU contain information that can determine barometric altitude and attitude of the drone, consequently, is can be correlated with the GPS PVT data.

3.2.2.24 Spread-Spectrum Security Codes on L1C (SSSC)

This method is discarded because requires the implementation of a cryptographic method.

3.2.2.25 Navigation Message Authentication (NMA)

This method is discarded because requires the implementation of a cryptographic method.

3.2.2.26 Received Ephemeris Consistency Check

This method is discarded because the extracted ephemeris data of different satellites can not be extracted to the Android Studio platform, this information resides in the data bit layer of the receiver.

3.2.2.27 GPS Clock Consistency Check

This method is discarded because the extracted time of each satellites can not be extracted to the Android Studio platform; this information resides in the data bit layer of the receiver.

3.2.2.28 Detecting False Signals with Automatic Gain Control

This method is discarded because the extracted AGC values can not be extracted to the Android Studio platform, this information resides in the signal processing layer of the receiver.

3.2.2.29 Consistency check of data within the GPS PVT solution

This method requires constant monitoring of the PVT solution values of the GPS of the drone, which are obtained from the MAVLink message GPS_RAW_INT.

To summarize, the selected solutions are: Monitor the relative GPS signal strength, Monitor the signal strength of each received satellite signal, Monitor SV identification codes and number of received signals, Check the time intervals, Consistency Check with Other position technologies, Consistency Check with Other technologies, Consistency Check with other sensors and Consistency check of data within the GPS PVT solution.

3.3 Attack Validation

The validation of the attack conceived by the threat actor is validated in different scenarios based on the schema of section 3.1. The scenarios are defined according to the state of the GPS receiver of the drone which are acquisition and tracking mode.

3.3.1 Attack setup architecture

The attack setup architecture is done with no spoofing RF transmissions. A GPS antenna has been used to receive authentic GPS signals, the received signals are transported through cable to a RF combiner. In this case, the spoofing can take place without faraday cage need because it does not violate radio transmission regulations. It should be considered that multipath propagation can not occur in this setup but this phenomenon happens in real not simulated scenarios.

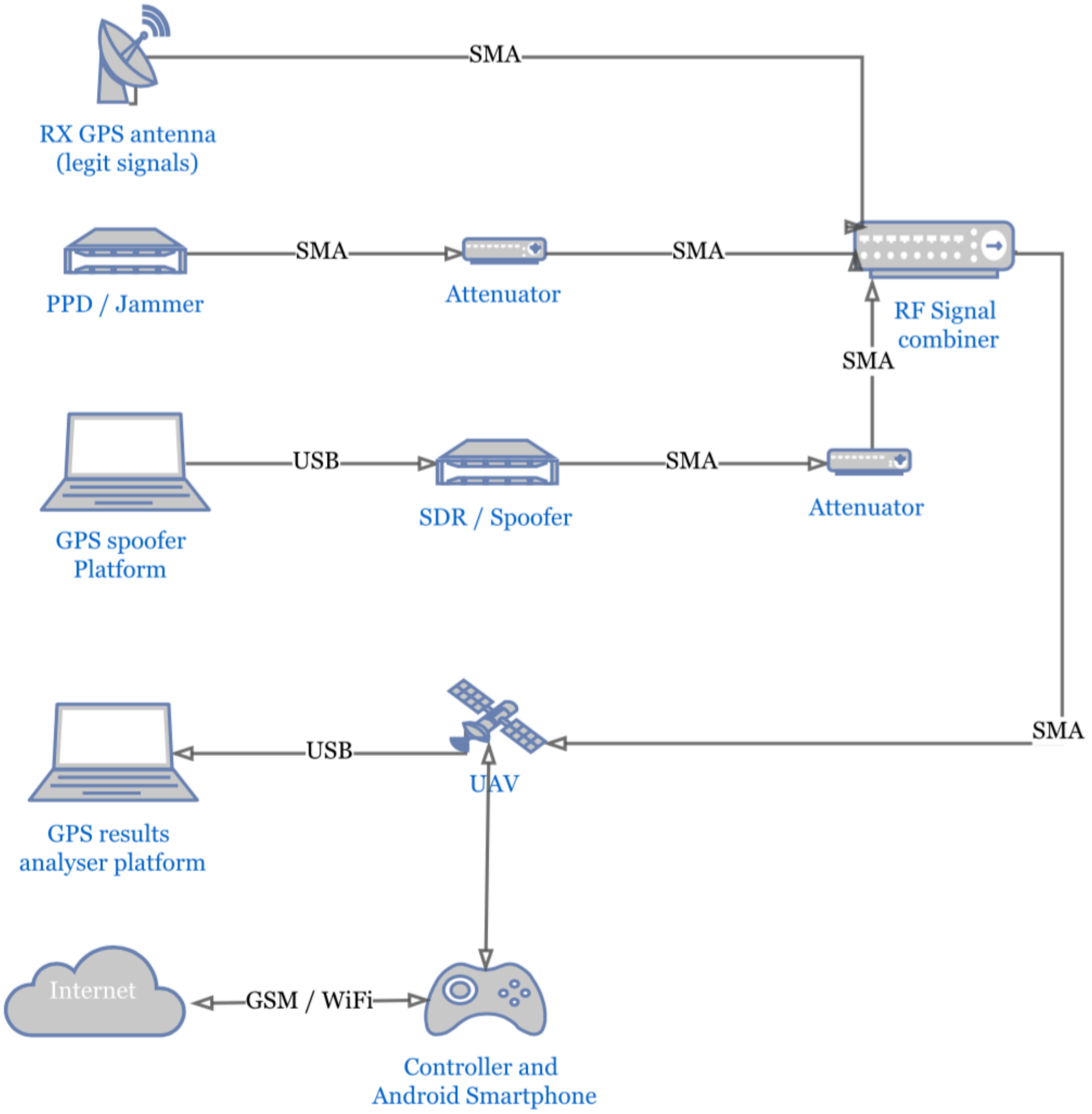


Figure 4. Validation setup architecture

In this setup, no real spoofer transmissions in the Radio Frequency environment takes place; instead, the authentic GPS L1 signal is transported to a RF; then, the legit signal is fed into the to the RF combiner with the GPS spoofing signal and the jamming signal, the outcome of this process is fed into the target receivers. Spoofing and jamming signal power tries to be adjusted by using attenuators.

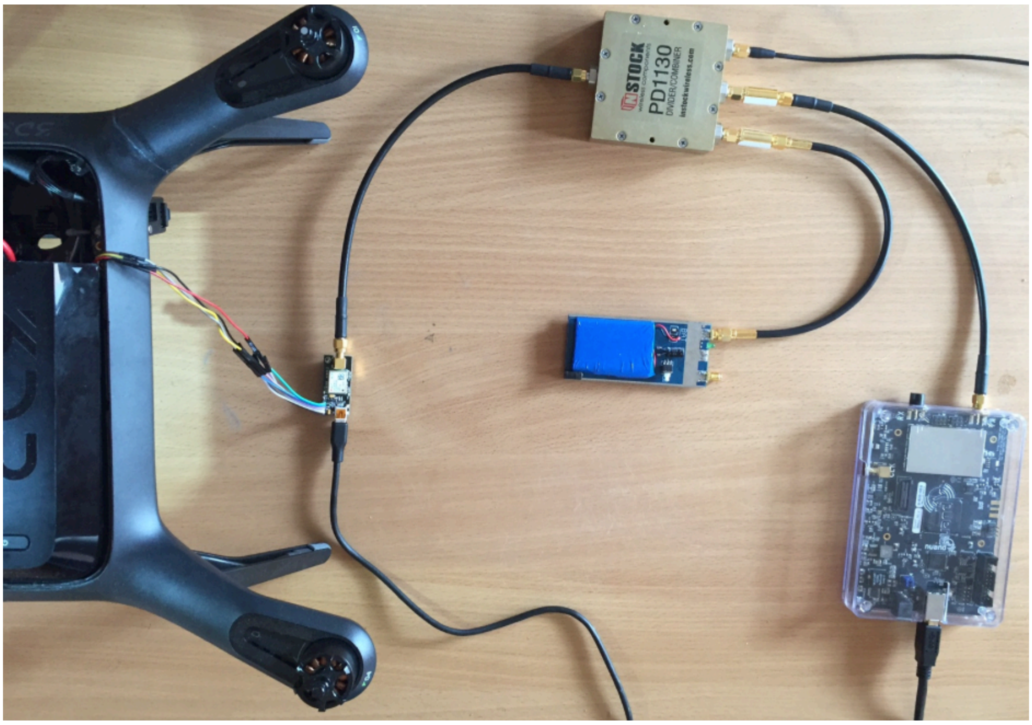


Figure 5. Picture of the architecture setup

3.3.2 Attack during acquisition mode

In acquisition, results can vary depending on the booting mode of the receiver, so that, tests are performed for cold, warm and hot start. Additional tests include the presence of only spoofing signals or the presence of both legit and counterfeit signals when feeding the target receiver.

The tests were done with different spoofed signals PVT, time from future and past (possible by changing the GPS week in the ephemeris file), the position was location was in ranges of few meters to thousands of kilometres of distance, and the velocity have included cero and positive values, additionally, the receiver was power off and power on in every test.

3.3.2.1 Cold start

The GPS receiver has been effectively spoofing when fed only by spoofing signals, when fed with authentic and spoofing signals at the same time, less than thirty seconds of the took the receiver for acquire the position, velocity and time solution provided by the spoofer. Clearly the strongest signal generated by the spoofer have drown the authentic signals. The spoofing detection state flag of the receiver has not been raised and the GPS is the only GNSS tracked or showed. The noise floor value has considerably raised as stated in section 2.2.2.8.

3.3.2.2 Warm start

During the warm start, the GPS receiver was previously tracking legit signals, therefore the warm start is including previous authentic information except the ephemeris data. The receiver started to use the fake PVT solution in less than thirty seconds during all the tests done and spoofing flag not raised either.

3.3.2.3 Hot start

Not data from previous sessions is deleted in a hot start. The spoofer was effective in injecting fake PVT solution into the receiver during all tests, the value of the TTFF between 30 to 40 seconds, in any occasion not indication for spoofing was trigger by the built-in mechanism.

3.3.3 Attack during tracking mode

Simplistic attacks are no effective on tracking devices because the spoofer is not synchronized with the legit signals, therefore the is not possible the lift-off of the correlation peak which is tracked by the DLL and of the GPS receiver, as stated in section 1.2.2 and 2.12.2, unless there is induced a force reacquisition technique. In this section the attacks were conducted expecting the results claimed in theory.

3.3.3.1 Simplistic attack on the receiver in tracking mode

Result are in agreement with the theory, where not in one case the spoofer could be effective. In some cases, in few occasions the built-in spoofing flag was raised intermittently after the attack started. During the attacks the signal of the GPS stellates is visible but not available for use in navigation, only GLONNAS and GALIEO signals remain useful.

3.3.3.2 Force re-acquisition

To induce an acquisition phase for the receiver a jammer was turned on for 20 to 40 seconds. In this case of the force re-acquisition technique, the tests were also ran in the receiver with firmware 2.01, the spoofer could successfully inject the PVT solution in the receiver, it should be noted that in this firmware version the spoofing flag was triggered randomly and not accurately. On the other hand, when the firmware 3.01 was installed the spoofer was only effective when the GPS was the only GNSS enable, in the other cases the spoofing attacks was detected.

3.3.4 Results

The tests have showed that the simplistic attacks performed d by the spoofer are effective every time the receiver is in acquisition phase. During tracking phase, the spoofer was effective for the firmware 2.01 which is the currently installed by default; but not for the firmware 3.01, which showed a solid defence for simplistic attacks when the GPS receiver is in tracking mode.

3.4 Solution Proposal

3.4.1 Data samples recollection

The sample data is recollected from legit and simulated GNSS. It is determined the minimum, maximum, average and standard deviation of the variables required for the spoofing detection selected methods of section 3.2.

3.4.1.1 Spoofer free RF environment

The objective of the dataset recollected is to represent the legit GNSS data obtained by the UAV GPS receiver during ordinary conditions, and not is expected to be used for calculating real and exact 3D position, therefore it is not required to follow a GPS data collection protocol. During the recollection location it was taken into consideration not to be significantly affected by LOS obstacles, weather or other antennas. The samples are taken in an urban environment during scattered cloud conditions.

Table 3.Authentic GNSS data feed sample statics

u-Blox m8n-0-01 Firmware 3.01	Average	Standard Deviation
Multiple GNSS		
SNR of all satellites	27.40	8.77
Number of satellites in view	18.3	4.8
Number of satellites used in PVT	15.4	0.7
GPS		

SNR of all satellites	26.80	10.11
Number of satellites in view	12.5	1.7
GLONNAS		
SNR of all satellites	28.28	7.08
Number of satellites in view	9.5	0.9
Galileo		
SNR of all satellites	25.64	6.16
Number of satellites in view	2.8	1.2

3.4.1.2 Spoofer data feed sample

The input for this dataset is provided by the spoofer used in the project, therefore this information is only of GPS and is not relevant the environment conditions.

Table 4.Spoofer data feed sample statics

u-Blox m8n-0-01 firmware 3.01	Average	Standard Deviation
GPS		
SNR of all satellites	47.47	5.6
Number of satellites in view	8.4	3.5
Number of satellites used in PVT	9	0.8

3.4.2 Threshold definition

Thresholds are defined using previous data samples statistics, the limits in performance of the drone, or the accuracy of the correlated technologies. Those thresholds are an initial reference which can be adjusted later with more profound analysis of input data if more accurate detection spoofing results are desired.

3.4.3 Specification datasheet of the proposed solution

In this section is proposed a group of calculations based on selected detection spoofing methods of section 3.2.2 with a suggested initial threshold definition of section 3.4.1. This approach suggests how to implement a proposed series of monitoring procedures. The alarms mentioned can be a sign or symptom for alerting abnormal behaviour of the receiver and possible spoofing conditions.

The NMEA listener is source of several values which be used to determine if the receiver is under GPS spoofing attack, for example:

- Calculating the average of the values of the SNR parsed from the android Nmea listener, if this value changes 8.77 (threshold) in less than a specific time, an alarm can be triggered in screen: “abrupt changes in absolute signal”. This calculation refers the implementation solution for the Monitor the relative GPS signal strength detection method.
- If the previous calculated average exceeds 35 (threshold: average plus the standard deviation of the SNR of all satellites), an alarm can be triggered announcing “values over normal limits”. This calculation refers the implementation solution for the Monitor the relative GPS signal strength detection method.

- Calculating the average of SNR during a specific time for each satellite ID, if this value changes for 8,77 (threshold) an alarm can be triggered "abrupt satellite signal changes". This calculation refers to the Monitor the signal strength of each received satellite signal detection method.
- If the values of satellites in view and the satellites used to calculate the PVT solution are out of the thresholds limits, alert by announcing "abrupt changes in satellites in view". This calculation refers the implementation solution for the Monitor SV identification codes and number of received signals detection method.
- If the satellites in view value is equal to 0 for more than specific time, an alarm can be triggered in screen: "possible signal interference"

Using other positioning technologies methods by comparing the drone GPS location with android's Wi-Fi, GMS or GPS locations can be a sign of spoofing attacks. These calculations refer the implementation solution for the Consistency Check with Other position technologies detection method.

- If the distance between GPS coordinates of the drone and the location obtained from Wi-Fi changes in more a specific distance (threshold) in less the time taken from the drone to get to this location if flying to maximum speed, trigger alarm "abrupt location changes"
- If the distance between GPS coordinates of the drone and the location obtained from GSM changes in more a specific distance (threshold) in less the time taken from the drone to get to this location if flying to maximum speed, trigger alarm "abrupt location changes"
- If the distance between GPS coordinates of the drone and the location obtained from GPS changes in more a specific distance (threshold) in less the time taken from the drone to get to this location if flying to maximum speed, trigger alarm "abrupt location changes"

Compare the time between the gotten from the GPS of the drone and from a NTP server from internet [1], if the time difference is longer than a specific time (threshold), trigger alarm "abrupt time changes". This calculation refers the implementation solution for the Consistency Check with Other technologies detection method.

If there is difference of altitude between drone barometric altitude and drone GPS altitude for more than a specific distance (threshold) in less than the time taken to the drone to fly in maximum speed to that location, trigger alarm "abrupt altitude changes". This calculation refers the implementation solution for the Consistency Check with other sensors detection method.

Monitor abrupt or erratic changes in altitude, speed, position or coordinates, within some thresholds, in the form a signal quality monitoring solution. This calculation refers the implementation solution for the Consistency check of data within the GPS PVT solution detection method.

[1] http://www.pool.ntp.org/

4 Conclusions

This thesis work demonstrates the security vulnerabilities and risks of flights in GPS navigation based UAVs, and on the other hand, counterattacks the security issues by proposing a theoretical detection solution.

Considering the spoofing threat analysed in this thesis and the tests conducted for the proposed scenario, it can be concluded that currently, the flights of mini and micro GPS navigation based UAVs are susceptible to its prominent GPS spoofing threat vector. The effect of simplistic attack via GPS signal simulator has been exanimated and tested in different case scenario's, and it was shown attack success for some cases, depending on variable receiver, environment and operational conditions. The proposed GPS spoofing detection solution of this work was a theoretical conjugation of multiple GPS detection methods; its design was based on the performance specifications of the mini and micro UAV and limited by the data which could be used at application layer SDK development tool level.

This chapter provides some concluding remarks as well as recommendations based on the material previously proposed; Section 4.1 discusses the findings on the conducted validation attack on different tests; Section 4.2 provides the conclusions of the GPS spoofing detection methods selection process and solution proposal design; and Section 4.3 gives recommendation and future work suggestions.

4.1 Validation Attack findings and remarks

From the three types od GPS spoofing attacks, the prominent threat vector for micro and mini UAV are the simplistic attacks done via signal simulator spoofer because recent developments have made cheap and without restricted distribution the resources needed to setup such a device. GPS is not authenticated and the there is not strict control on the RF transmission, therefore the GPS navigation based UAV are vulnerable to be fed by counterfeit signalling.

The tests conducted in the thesis scenario demonstrate the spoofer was successful attacking the UAV when the GPS was in acquisition mode, despite the booting mode or if the receiver was simultaneously fed with legit GPS signals. On the other hand, the spoofer was not able to inject the fake PVT solution when the receiver was already tracking authentic GPS satellites, supporting the previous stated claims from previous works; however, using a force requisition technique it possible to conduct a successful spoofing attack depending on the firmware version, it should be noted that the tests were conducted in a recent release of new built-in antispoofing firmware.

4.2 GPS spoofing solution proposal design findings and remarks

Navigation of mini and micro UAVs can be more secure if there is a detection solution for alerting the operator of possible GPS spoofing attacks by reading and analysing abnormal behaviour in the correlated data inputted from different sources of the UAS.

There has not be a completely implanted fool proof solution for the GNSS spoofing threat, however, the conjugation of multiple techniques can reduce false alarm detection probabilities. From various detection techniques founded in the open literature it was selected a subset which had applicability in the scenario of mini and micro UAVs against simplistic GPS spoofing attacks, because the data and hardware requirements of this methods were found in the postulated architecture of UAS and in the environment schema.

There are notorious differences when comparing the data of the authentic and spoofing GPS samples datasets, this results can be used to determine thresholds limits of normal signal behaviour in the proposed software solution.

The proposed detection technique has application flexibility because it was developed and operates in the application layer like other similar open source projects, therefore its nature and concept are extensible to be implemented in other GCS or UAV applications, especially if the communication is also based on the MAVLink protocol Standard, in the same way, the proposed solution implementation does not require to make changes in the architecture or firmware of the GPS receivers.

More methods could have been integrated in the proposed solution of this project but the variables which were needed reside in the other layer of the UAS or the communication message had had to be created in the firmware of the UAV.

4.3 Recommendation and future work

Implement the proposed solution and test the results based on the schema of this work to measure the effectiveness of the solution, additionally, robust work in statistics can be done by gathering, comparing and analysing samples and datasets of authentic GPS signal, counterfeit signals and the result of an implemented solution in order to make accurate thresholds and raise the probability of spoofing detection and decrease the chances of false alarm alters.

5 References

[1] "GPS.gov: Timing applications" in Official U.S. Government information about the Global Positioning System (GPS) and related topics, 2011. [Online]. Available: http://www.gps.gov/applications/timing/. Accessed: May 17, 2016.

[2] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12, 2012.

[3] Humphreys, T. E., "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf, July 2012.

[4] "European Global Navigation Satellite Systems Agency,". [Online]. Available: http://www.gsa.europa.eu/security/prs. Accessed: May 17, 2016.

[5] A. Rawnsley, "Iran's alleged drone hack: Tough, but possible," in Wired.com, WIRED, 2011. [Online]. Available: https://www.wired.com/2011/12/iran-drone-hack-gps/. Accessed: May 17, 2016.

[6] Humphreys, Todd E., Ledvina, Brent M., Psiaki, Mark L., O'Hanlon, Brady W., Kintner, Paul M., Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, GA, September 2008, pp. 2314-2325.

[7] T. Ebinuma, "gps-sim-sdr," in github.com. [Online]. Available: https://github.com/osqzss/gps-sim-sdr. Accessed: May 17, 2016.

[8] Jafarnia, A. "GNSS Signal Authenticity Verification in the Presence of Structural Interference", Department of Geomatics Engineering, University of Calgary, CALGARY, ALBERTA, 2013.

[9] U. Hunkeler, J. Colli-Vignarelli, and C. Dehollain,"Effectiveness of GPS-jamming and counter-measures," 2012 International Conference on Localization and GNSS, Jun. 2012.

[10] D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," in ION GNSS Conference Nashville, TN, September 1921, 2012.

[11] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," Proceedings of the 18th ACM conference on Computer and communications security, ETH Zurich - CCS '11, 2011.

[12] UBLOX, "Receiver Description Including Protocol Specification," in U-blox.com. [Online]. Available: https://www.u-blox.com/sites/default/files/products/documents/u-blox8-M8_ReceiverDescrProtSpec_(UBX-13003221)_Public. Accessed: May 17, 2016.

[13] T. Humphreys, "Secure PNT for autonomous systems," in Radionavigation Laboratory of the University of Texas, 2010. [Online]. Available: https://radionavlab.ae.utexas.edu/index.php?option=com_content&view=article&id=351:secure-pnt-for-autonomous-systems&catid=30&Itemid=37. Accessed: May 17, 2016.

[14] GPS World, "Spoofing, detection, and navigation vulnerability," in YouTube, YouTube, 2015. [Online]. Available: https://www.youtube.com/watch?v=qlX-MsYZvoM. Accessed: May 17, 2016.

[15] T. Humphreys and K. Wesson, "unhackable drones the challenges of securely integrating UAV into the national airspace," in Radionavigation Laboratory of the University of Texas, 2013. [Online]. Available: https://radionavlab.ae.utexas.edu/images/stories/files/papers/unhackabledrones_for_distribution.pdf. Accessed: May 17, 2016.

[16] H. Lin and Y. Qing, "Low-cost GPS simulator," in DefCon Communications Inc., 2015. [Online]. Available: https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Lin-Huang-Qing-Yang-GPS-Spoofing.pdf. Accessed: May 17, 2016.

[17] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS Spoofing," Journal of Field Robotics, vol. 31, no. 4, pp. 617–636, Apr. 2014.

[18] O. Petrovsky, "Map in not a territory: How to spoof GPS in a shoestring," in Hewlett Packard Enterprise, 2016. [Online]. Available: http://community.hpe.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/721/1/HPE-SR_WhitePaper_Petrovsky_GPS-Spoof_2016March. Accessed: May 17, 2016.

[19] E. Kaplan and C. Hegarty, Eds., Understanding GPS: Principles and applications. Boston: Artech House Publishers, 2005.

[20] S.-I. Kondo, N. Kubo, and A. Yasuda, "Evaluation of the Pseudorange performance by using software GPS receiver," Journal of Global Positioning Systems, vol. 4, no. 1&2, pp. 215–222, Dec. 2005.

[21] M. Lehtinen, A. Happonen, and J. Ikonen, "Accuracy and time to first fix using consumer-grade GPS receivers," 2008 16th International Conference on Software, Telecommunications and Computer Networks, 2008.

[22] Jafarnia-Jahromi, A., Lin, T., Broumandan, A., Nielsen, J., Lachapelle, G., "Detection and Mitigation of Spoofing Attacks on a Vector Based Tracking GPS Receiver," Proceedings of the 2012 International Technical Meeting of The Institute of Navigation, Newport Beach, CA, January 2012.

[23] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to Spoofing threats and a review of Antispoofing techniques," International Journal of Navigation and Observation, vol. 2012, pp. 1–16, 2012.

[24] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, “Receiver autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil gps spoofer,” in Proceedings of the 2009 International Technical Meeting of The Institute of Navigation, 2009.

[25] M. de Fatima Bento, "Unmanned aerial Vehicles: an Overview," in InsideGNSS, 2008. [Online]. Available: http://www.insidegnss.com/auto/janfeb08-wp.pdf. Accessed: May 17, 2016.

[26] K. Wesson, D. Shepard, and T. Humphreys, “Straight Talk on Anti-Spoofing Securing the Future of PNT,” GPS World, no. January, 2012.

[27] A. RÜGAMER, "Jamming and Spoofing of GNSS Signals, an underestimated risk" 2015. [Online]. Available: https://www.fig.net/resources/proceedings/fig_proceedings/fig2015/papers/ts05g/TS05G_ruegamer_kowalewski_7486.pdf. Accessed: May 17, 2016.

[28] Konovaltsev, Andriy, Caizzone, Stefano, Cuntz, Manuel, Meurer, Michael, "Autonomous Spoofing Detection and Mitigation with a Miniaturized Adaptive Antenna Array," Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014), Tampa, Florida, September 2014.

[29] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver," GPS Solutions, vol. 19, no. 3, pp. 475–487, Sep. 2014.

[30] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, “A low-complexity GPS anti-spoofing method using a multi-antenna array,” in Proc. ION GNSS 2012, 2012, pp. 1233–1243.

[31] A. Jafarnia Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements," International Journal of Satellite Communications and Networking, vol. 30, no. 4, pp. 181–191, Jun. 2012.

[32] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014, May 2014.

[33] J. Warner and R. Johnston, "GPS Spoofing Countermeasures," in Los Alamos National Laboratory, 2003. [Online]. Available: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-6163. Accessed: May 17, 2016.

[34] C. E. McDowell, “GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling—US Patent 7250903 B1,” 2007.

[35] L. Scott, “Anti-spoofing and authenticated signal architectures for civil navigation systems,” in Proceedings of the ION GNSS Meeting, (Portland, Oregon), pp. 1542–1552, Institute of Navigation, 2003.

[36] Kyle Wesson, “Straight Talk on Anti-Spoofing Securing the Future of PNT”, GPS World, 2012.

[37] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," J Inst Navig, vol. 59, no. 3, pp. 177–193, Sep. 2012

[38] Wen, Hengqing, Huang, Peter Yih-Ru, Dyer, John, Archinal, Andy, Fagan, John, "Countermeasures for GPS Signal Spoofing," Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005), Long Beach, CA, September 2005, pp. 1285-1290.

[39] U-Blox, "NEO7 Receiver Description Including Protocol Specification," 2016. [Online]. Available: https://www.u-blox.com/sites/default/files/products/documents/NEO-7_DataSheet_(UBX-13003830).pdf.

[40] U-Blox, "M8 Receiver Description Including Protocol Specification," 2016. [Online]. Available: https://www.u-blox.com/sites/default/files/products/documents/u-blox8-M8_ReceiverDescrProtSpec_(UBX-13003221)_Public.pdf. Accessed: May 17, 2016.

[41] T. Humphreys, "Lost in space: How secure is the future of mobile positioning?" in IEEE CTN CosMoc Technology News, 2016. [Online]. Available: http://www.comsoc.org/ctn/lost-space-how-secure-future-mobile-positioning. Accessed: May 17, 2016.

[42] "NMEA Reference Manual," 2005. [Online]. Available: https://www.sparkfun.com/datasheets/GPS/NMEA%20Reference%20Manual1.pdf. Accessed: May 17, 2016.

6 Appendix

6.1 License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Santiago Andres Sarmiento Bernal**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

Detection solution analysis for simplistic spoofing attacks in commercial mini and micro UAVs,

supervised by Supervised by Olaf Manuel Maennel and Raimundas Matulevičius,

2. I am aware of the fact that the author retains these rights.
3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **05.05.2016**

Table of abbreviations and terms

AGC	Automatic Gain Control
AOA	Angle of Arrival
BLOS	Beyond Line of Sight
CAF	Cross Ambiguity Function
CDMA	Code Division Multiple Access
DME	Distance Measurement Equipment
DLL	Delay Lock Loops
DOA	Direction of Arrival
EGNOS	European Geostationary Navigation Overlay Service
GALILEO	European Global Satellite Navigation System
GCS	Ground Control Station
GIS	Geographic Information System
GNSS	Global Navigation Satellite System
GLONASS	Globalnaya Navigazionnaya Sputnikovaya Sistema
GPS	Global Position System
IS	Interface Specification
ISR	Intelligence Surveillance Reconnaissance
LOS	Line of Sight
MTOW	Maximum Take-off Weight
NTP	Network Time Protocol
PLL	Phase Lock Loops
PPD	Personal Privacy Devices
PPS	Precise Positioning System
PRN	Pseudo Random Number
PRS	Public Regulated Service
PVT	Position Velocity Time
RAIM	Receiver Autonomous Integrity Monitoring
RF	Radio Frequency
SDK	Software Development Kit
SR	Short Range
SQM	Signal Quality Monitoring
SV	Space Vehicle
TOA	Time of Arrival
TTFF	Time to First Fix

UAV	Unmanned Aerial Vehicle
UAS	Unmanned Aerial System
VOR	VHF Omnidirectional Range