Instituto Universitário de Lisboa

Departamento de Ciências e Tecnologias da Informação

Implementação de Zonas de Acesso Proibido para UAVs Usando Spoofing de Sinais GPS

Vasco Rafael Jerónimo Velez

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Engenharia de Telecomunicações e Informática

Orientador:
Professor Doutor Nuno Manuel Branco Souto, Professor Auxiliar,
ISCTE-IUL

Co-Orientador:
Professor Doutor Pedro Joaquim Amaro Sebastião, Professor Auxiliar,
ISCTE-IUL

Outubro, 2018

Agradecimentos

Aos meus orientadores, Professor Nuno Souto, e ao Professor Pedro Sebastião agradeço toda a orientação disponibilizada, assim como o conhecimento partilhado, desde o auxílio aos conselhos que me deram e que foram bastante importantes, de modo a conseguir concluir com sucesso tanto o projeto como a dissertação.

À minha mãe e minha irmã, em especial, que estiveram sempre ao meu lado tanto nos bons e maus momentos, no qual sempre me apoiaram até ao fim.

Aos colegas de investigação e amigos, apesar dos contratempos existentes que existiram.

Ao Professor Francisco Cercas, pela sua disponibilidade e ao seu vasto conhecimento transmitido nesta área.

Ao IT – IUL (Instituto de Telecomunicações), por ter fornecido os equipamentos que foram necessários e cruciais ao desenvolvimento.

A todos os que enumerei o meu sincero “Obrigado” e agradeço a vossa preocupação para comigo.

Resumo

A recente proliferação de veículos aéreos não tripulados (UAV) em aplicações civis levantam sérias preocupações técnicas e sociais, bem como desafios que precisam de ser abordados, tanto em termos de privacidade como segurança pública. Torna-se por isso crucial desenvolver soluções eficazes para a deteção, localização e neutralização de UAVs não autorizados.

Neste trabalho pretendia-se estudar e implementar técnicas eficazes para a restrição do voo de uma ampla variedade de UAVs não-autorizados de forma a que posteriormente essas funções possam ser integradas num sistema sem fios escalável para deteção rápida, localização e neutralização de UAVs.

Uma das técnicas que pode ser utilizada e que foi o foco deste trabalho é o Spoofing de sinais GPS, uma vez que os sistemas de navegação dos UAVs necessitam constantemente da sua utilização para se localizarem e operarem em modo autónomo. Para se implementar esta técnica recorreu-se a plataformas de SDR – Software Defined Radio, que são altamente versáteis e de baixo custo, permitindo a geração de sinais GPS através de software. Deste modo é possível induzir trajetórias alternativas ao percurso inicial do UAV, prevenindo a sua entrada se o mesmo não for autorizado.

Através dos testes efetuados com o sistema de defesa anti-UAV desenvolvido, foi possível observar que os recetores GPS comuns não têm forma de verificar a informação recebida quando é transmitido o GPS contrafeito, estando por isso vulneráveis a ataques de spoofing.

Palavras-Chave: UAV; GPS; Spoofing; SDR.

Abstract

The recent proliferation of Unmanned Aerial Vehicles (UAV) in civilian applications raises serious technical and societal concerns as well as challenges that need to be addressed, in terms of privacy and public safety. Therefore, it becomes crucial to develop effective solutions for the detection, localization and neutralization of unauthorized UAVs.

The main objective of this work was to study and implement effective techniques for restraining unauthorized UAV operations and integrate those functions into a scalable wireless system capable of fast detection, localization and neutralization of a wide scope of UAVs.

One of the techniques that can be used and which was the main focus of this work is GPS spoofing, since the navigation systems of UAVs constantly need their use to locate and operate in autonomous mode. To implement these techniques, it was intended to use SDR - Software Defined Radio platforms, which are highly versatile and low cost, allowing the generation of GPS signals through software. In this way it is possible to induce alternative routes to the initial course of the UAV, preventing its entrance, if it is not authorized.

Through several experimental tests with the developed anti-UAV defense system, it was possible to observe that common GPS receivers have no way of verifying the information received when the GPS counterfeit signal is broadcast, which makes them vulnerable to spoofing attacks.

Keywords: UAV; GPS; Spoofing; SDR.

Índice

Índice de Figuras

Lista de Abreviaturas e Siglas

4G LTE	Fourth-Generation Long Term Evolution
5G	Fifth Generation
6G	Six Generation
API	Application Programing Interface
BPSK	Binary Phase Shift-Keying
C/A	Coarse/Acquisition
CDMA	Collision Division Multiple access
BeiDou 2	Beidou Navigation Satellite System 2
DHL	Dalsey, Hillblom and Lynn
DJI	Dà-Jiāng Innovations
E.U.A.	Estados Unidos da América
FPGA	Field Programmable Gate Array
GALILEO	Sistema de Navegação da União Europeia
GB	Gigabyte
GCS	Ground Control Station
GHz	Gigahertz
GLONASS	Globalnaya Navigatsionnaya Sputnikovaya
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HOW	Handover Word
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
IDE	Integrated Development Environment
IoT	Internet of Things
ISCTE	Instituto Superior das Ciências e Trabalho Empresarial

LGPL	GNU Lesser General Public License
LOS	Line of Sight
M2M	Machine to Machine
MHz	Megahertz
MIT	Massachusetts Institute of Technology
NASA	National Aeronautics and Space Administration
NAVSTAR-GPS	Navigation Satellite Timing and Ranging-GPS
NMA	Navigation Message Authentication
NMEA	National Marine Electronics Association
OSQZSS	Open Source Quasi-Zenith Satellite System
P(Y)	Precision Code
PPS	Precision Positioning Service
PRN	Pseudo Random Noise
RC	Radio Controlled
RFID	Radio Frequency Identification
RGB	Red, Green, Blue
RPA	Remotely Pilot Aircraft
RPAS	Remotely Pilot Aircraft System
SDK	Software Development Kit
SDR	Software Defined Radio
SPS	Standard Positioning Service
STACOM	Satellite Communications
TLM	Telemetry
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UTC	Coordinated Universal Time

WGS-84	World Geodetic System-84
WLAN	Wireless Local Area Network

Capítulo 1 – Introdução

1.1. Motivação e Enquadramento do tema

Os UAVs – Unmanned Aerial Vehicles, mais conhecidos como "*drones*", têm vindo a popularizarem-se em grande escala na nossa sociedade, colocando desafios e problemas relacionados com a segurança pública. A ausência de piloto a bordo, não impede o seu correto funcionamento, podendo ser operado e controlado remotamente [1]. Com o avanço tecnológico e o aparecimento das "Smart Cities" e IoT – Internet of Things, tornar-se-á mais frequente o uso de UAVs, o que desperta mais interesse quanto à aquisição deste tipo de aparelhos. Com redução dos preços de aquisição, perspetiva-se que no futuro, não sejam apenas utilizados pelas populações, mas também por empresas multinacionais de grande dimensão, ideia esta que vem sendo considerada há algum tempo. Os UAVs entram nesse ecossistema, devido às elevadas funcionalidades e modos de operação que oferecem, tais como: - vigilância, - entrega de encomendas, - divertimento, - captura de imagens, entre outros, de modo a facilitar as tarefas humanas, reduzindo assim os custos. Cada vez mais começa-se a introduzir funcionalidades de navegação autónoma nos UAVs, no qual deve-se dar particular atenção na sua segurança, pois essa operação autónoma, pode nem sempre ser devidamente modelada ou desenvolvida, causando assim um possível ataque por parte de falhas (bugs) e/ou de ataques de "*hackers*" [2].

Apesar dos regulamentos atuais colocarem restrições para voo dos veículos aéreos não tripulados (UAVs) em áreas povoadas, a crescente utilização destes veículos em aplicações civis levanta preocupações significativas em termos de privacidade e segurança pública. Existe uma necessidade urgente de desenvolver soluções para a deteção, localização e neutralização de UAVs não autorizados. Entre as abordagens que começaram a surgir, as soluções mais promissoras dependem apenas de contramedidas eletrónicas. No ramo de segurança contra UAVs, as soluções existentes no Mercado podem ser bastante dispendiosas e limitadas em termos de cenários/aplicações no combate aos UAVs. Nos dias de hoje verifica-se cada vez mais a perturbação de espaço(s) cuja intrusão não é autorizada, p.e., aeroportos, bases militares, eventos, etc. Existem falta de meios eficientes e acessíveis no combate a este tipo de intrusos, o que poderá potenciar a desastres [3].

Os UAVs, para usufruírem de navegação correta e fiável, precisam de um recetor de sinal proveniente de GNSSs – Global Navigation Satellite System. Entre outros tipos de GNSS, existe um que é bastante conhecido, denominado por GPS – Global Positioning System, que compreende um espetro de frequências que são emitidas pelo sistema cujo acesso é livre – GPS civil, e outro que contém criptografia na informação recebida no qual é utilizado para operações militares – GPS militar. Para que o sistema de localização do UAV funcione, é preciso que os recetores do mesmo, consigam captar os sinais rádio emitidos pelo GNSS, de modo a que o recetor do UAV consiga calcular a sua posição no espaço tridimensional. Existem várias variantes, podendo ser regionais ou globais. As variantes globais existentes, são: o NAVSTAR-GPS, sendo este o mais conhecido e usado em todo o mundo, com origem nos Estados Unidos da América, tendo sido o primeiro sistema do mundo a ser completamente implementado; o GALILEO, o qual foi concebido pela União Europeia e que ainda está em fase de conclusão, contudo espera-se que seja terminado em 2019, encontrando-se já ativo mas ainda com pouca utilização, devido a ser um dos sistemas mais recente; o GLONASS, sistema desenvolvido pela Rússia, o qual começou a ser desenvolvido na mesma altura que o sistema Americano; por fim o BeiDou 2 ou *Compass*, sistema Chines ainda em fase de conclusão, mas já com usabilidade em regiões da Ásia Central. Estes são os quatro sistemas GPS com acesso global, embora existam outros sistemas, mas são apenas de acesso regional [4], [5].

Sendo os sinais GPS civis livres e não encriptados podem ser facilmente enganados através da capacidade de criar uma situação de spoofing. Esta habilidade de ataque de spoofing consiste em criar um sinal contrafeito igual ao original, mudando também os dados originais, mas, mantendo a mesma autenticidade do sinal verdadeiro, criando assim informação falsa no recetor GPS. Isto torna possível atacar as comunicações GPS do UAV sem prejudicar o voo, alterando apenas a trajetória original para o percurso desejado pelo atacante/defensor, causando a sua possível captura dos sistemas de navegação. Este tipo de vulnerabilidade do sinal GPS afeta grande parte destes recetores, visto que, as comunicações do GNSS civil não incluem encriptação nas informações. Por outro lado, as comunicações do sistema de navegação militar não são vulneráveis a este tipo de ataque, visto que as mesmas são fortemente encriptadas, usando o algoritmo de chave simétrica e, ou assimétrica – pública/privada. Este tipo de

ataque já é conhecido pela comunidade científica há algum tempo, aguardando-se uma solução para o problema [6], [7], [8].

1.2. Objetivos de investigação

O objetivo deste projeto de dissertação, consiste no desenvolvimento de um sistema capaz de capturar os sistemas de navegação do UAV utilizando plataformas SDR (designado de Software Defined Radio). Este tipo de plataformas, permitem utilizar software para implementar a comunicação de ondas rádio, sendo utilizado hardware especializado para tal. Os SDRs podem ser usados para desenvolver qualquer tipo de comunicação Rádio que permaneça dentro da largura de banda do dispositivo, o que os torna bastante versáteis para várias aplicações. No caso do trabalho desta dissertação, a banda de frequências a ser utilizada, situa-se entre os 1400MHz e 1600MHz, onde o sinal GPS é transmitido pelos satélites. Desta maneira, ir-se-á permitir a captura, ou mudança de trajetória do UAV, através da falsificação do sinal GPS – técnica denominada por Spoofing, utilizando antenas diretivas de modo a direcionar a transmissão, na direção do UAV, com a finalidade de desviá-lo, do seu percurso original, impedindo-o de entrar em zonas proibidas.

Seguem-se os principais objetivos definidos para a conclusão da implementação:

- Investigar e estudar meios de gerar artificialmente ondas rádio de sinal GPS, usando plataformas SDR, tais como BladeRF, HackRF, USRP de forma a interferir com os recetores do UAV;

-Desenhar e implementar um sistema capaz de transmitir sinais falsos do sistema NAVSTAR-GPS para induzir o UAV para uma posição falsa utilizando plataformas de SDR, de forma a impedir de entrar numa zona de acesso restrito;

- Implementação de um algoritmo capaz de prever/estimar a trajetória do UAV e delinear uma rota falsa que permita o desvio do mesmo da zona proibida.

1.3. Estrutura e organização da dissertação

O presente estudo está organizado em cinco capítulos que pretendem refletir as diferentes fases até à sua conclusão.

O primeiro capítulo introduz o tema da investigação, assim como a motivação e objetivos da mesma, bem como uma breve descrição da estrutura do trabalho realizado.

O segundo capítulo reflete as especificações tanto dos UAV como do sistema NAVSTAR-GPS, em que são descritas todas as informações teóricas necessárias à conclusão da dissertação.

O terceiro capítulo é dedicado ao spoofing, e seus derivados. Contém desde a sua descrição como as ferramentas utilizadas para realizar com sucesso o spoofing de sinais GPS.

O quarto capítulo apresenta o sistema implementado, e a sua explicação detalhada, além da teoria envolvida na sua realização. Por fim, são demonstrados os resultados obtidos, de acordo com a metodologia que se utilizou.

No quinto e último capítulo apresentam-se as conclusões deste estudo bem como o trabalho futuro.

Capítulo 2 – UAVs e Sistemas GNSS

2.1. Introdução aos UAVs

2.1.1. Conceito básico de UAV

O termo UAV – Unmaned Aerial Vehicle em inglês, descreve um aparelho voador que evita a necessidade de piloto a bordo do mesmo, e que a sua ausência não prejudica o seu funcionamento. Tem vindo a crescer bastante nestes últimos anos, e perspetiva-se que continue assim futuramente. Existem várias formas de descrever este tipo de veículos, os mais conhecidos são: *Drone,* UAV, UAS, RPA ou RPAS. O termo "*Drone*" é o mais conhecido devido à sua grande popularidade pela sociedade e pelos meios de comunicação social, de um sistema de pequeno porte, e que é descrito na figura 1. Na grande maioria são relacionados a multicópteros, no qual são operados pelo controlador terrestre através de um controlador remoto, e que podem ser capazes de suportar ou não, funcionalidades semiautónomas e/ou autónomas. Em todos os casos tem software como base do seu funcionamento e na sua descrição de atuação. O termo UAS – Unmaned Aircraft System, refere-se ao sistema completo, dado que o UAV é referente apenas ao veículo, ainda assim é utilizado maioritariamente em termos militares, como é descrito na figura 2. Este termo descreve o aparelho e o sistema por completo, incluindo a estação de controlo terrestre, o UAV e, os sistemas e meios da operação/comunicação, sistemas estes capazes de serem novamente usados (isto exclui qualquer tipo de mísseis ou tipo de armamento teleguiado). São executados através de componentes eletrónicos e/ou computadores, podendo ser guiados por sistemas autónomos com ou sem a ajuda de um operador. RPA – Remotely Pilot Aircraft, ou RPAS – Remotely Pilot Aircraft System, são descritos como sistemas de controle rádio semelhantes a carros ou helicópteros RC, mas com a distinção de serem direcionados a UAVs sem terem necessidade de câmeras e outro tipo de visualização a bordo. Visto que cada vez existem mais tipos de variantes diferentes de UAVs, são distinguidos pelo seu peso e forma [1], [9].

Figura 1-Um Quadcopter e o comando remoto de um UAV, Fonte: [9] [1]

Figura 2-UAV de calibre militar, Fonte: [9] [2]

São distinguidas três peças fundamentais para a constituição de um sistema UAS, que são: o UAV, o tipo de comunicação, e a GCS (Ground Control Station) – a estação base, em que esta possa ser um operador com controlador remoto, ou a estação de controlo terrestre.

O UAV pode ser composto por vários sistemas que interagem entre si. São constituídos por componentes eletrónicos que fundamentam a base do sistema (placas-mãe, circuitos integrados, controladores, antenas, etc), pelos meios de comunicação (2,4/5 GHz, 4G LTE, 5G, etc), sensores e sistemas de navegação, (tais como altímetros, acelerómetros, GPS, IMU, INS) e sistemas de aviação e controle (motores, flaps, ailerons, estabilizadores, hélices, propulsores).

Uma parte fundamental do UAV são os seus meios de comunicações, de modo a que seja possível que o operador, consiga operá-lo, assim como monitorizar o seu estado e as suas funções autónomas, se este as tiver. O tipo de comunicação entre o operador e o UAV, podem ser de duas formas: LOS (Line of Sight) – linha de vista, tipo este que é o

[1] Imagem retirada do site: https://wiki.ezvid.com/m/drone-vs-uav-what-is-the-difference-_2FJYp_SrUkP-
[2] Imagem retirada do site: https://wiki.ezvid.com/m/drone-vs-uav-what-is-the-difference-_2FJYp_SrUkP-

mais conhecido e utilizado comercialmente; e SATCOM (derivado de Satellite Communications) – comunicação por via satélite, no qual é utilizada apenas a nível governamental e militar. Este último meio de comunicação é dos mais sofisticados que existe, no qual interliga diretamente o UAV à sala de controlo terrestre (*coque pit*). As bandas de frequências dos UAVs comerciais mais usadas e licenciadas, no caso dos LOS, começam nos 2.400-2.4835MHz e nos 5.470MHz-5.725MHz, na europa vão até aos 5.725-5.875MHz no qual não podem exceder 25mW de potência emitida. Estas são as bandas de frequências mais usadas nos UAVs tanto para controlo do aparelho, como para a transmissão de vídeo das câmeras a bordo para o ecrã do controlador. Consequentemente começam a ficar saturadas devido à utilização massiva dos 2,4GHz do Wifi. No entanto pensa-se em criar outro tipo de banda alternativa que não cause interferência com as redes sem fios domésticas e com as comunicações dos UAVs. Por fim ainda em fase de aparecimento, mas com grande força em termos de expansão, começam a existir novas versões de comunicação, tanto via 802.11(WLAN), redes móveis (4G (LTE), 5G/6G) ou integração de comunicações RFID, M2M, que interligam diretamente nos UAVs, no qual são tecnologias já apresentadas e utilizadas em grande variedade de dispositivos móveis, mas emergentes no campo dos UAVs. Este tipo de comunicação está a ser demonstrado e utilizado para operações via remota do aparelho sem que seja necessário algum tipo de visualização física do aparelho (LOS), o que pode facilitar algumas operações, assim como introduzir novas funcionalidades [10], [11], [12].

2.1.2. Principais tipos de UAVs

Existem muitas variantes de modelos, que diferem nas formas e feitios, assim como no peso dos mesmos. No entanto as autoridades reguladoras obrigam a que haja uma classificação do tipo e peso dos UAVs em questão, seguindo-se abaixo os principais tipos de classificação:

- Fixed-wing – UAVs que contêm asas fixas e no qual é acoplado um ou mais motores (propulsores), geralmente atrás do veículo, para dar impulsão e velocidade. Habitualmente é preciso uma pequena pista de modo a que o UAV levante voo, ou então, lançados por um indivíduo. São bastante utilizados em vigilância devido à grande capacidade de gerar elevação e percorrer grandes distâncias.

- MultiRotor – estes são os UAVs mais conhecidos, e são os mais predominantes no mercado. Costumam ter entre 4, 6 ou 8 hélices para lhe darem uma maior estabilidade e agilidade, no qual funcionam exatamente como um helicóptero. Têm tipicamente a forma de quadrado ou de estrela. No entanto não necessitam de pista para levantar voo, ao contrário dos UAVs de asa fixa, são versáteis e podem ser reconfigurados para as tarefas e missões.
- Blimps – são pequenos balões semelhantes a dirigíveis, mas em formato bastante mais pequeno, e são bastante requisitados em zonas de monitorização ambiental, devido ao facto de estes conseguirem ter uma longa duração de autonomia, assim como velocidades bastante reduzidas. Tipicamente contém um gás bastante mais leve que o ar, o que os transforma na ferramenta ideal para quem precisa de um UAV com grande autonomia.
- Outro tipo de aparelhos semelhante a UAVs – existem cada vez mais variantes de aparelhos semelhantes aos UAVs, podendo ter capacidade híbridas, em que conseguem acomodar aptidões tanto para asa-fixa ou com vários rotores semelhantes ao MultiRotor [10] [12] [13] [14].

Além do tipo de veículo existem também variantes de peso. Seguem-se abaixo os principais tipos de classificação por peso dos UAVs:

- Até 2 kg – são considerados micro UAVs. São aparelhos de pequeno porte e são os mais encontrados entre as populações.
- De 2 a 20 kg – UAVs considerados de pequeno porte ou mini UAVs. São utilizados por empresas/profissionais de fotografia e filmagens, devido a terem maior capacidade de transporte de material de vídeo e têm tipicamente alcances até 10 a 25 km.
- De 20 kg até 150 kg – são considerados de UAVs de médio porte, e são bem mais raros de se ver, no entanto são mais utilizados pelas forças governamentais ou por infraestruturas de suporte a tarefas especificas, assim como empresas que necessitem de algumas funcionalidades especiais, tem tipicamente alcances maiores que a categoria anterior e uma altitude maior.
- Mais de 150 kg – UAVs de grande porte. Só são encontrados UAVs deste tipo em uso militar ou de forças especiais. São conhecidos por serem UAVs táticos, para a área de videovigilância, onde são capazes de voar centenas de quilómetros.

Estes são os principais tipos de classificação de UAVs, no entanto não quer dizer que não haja mais categorias, o que de facto existem, mas são de valores superiores, e são maioritariamente utilizados por forças militares e que normalmente estão classificados como confidenciais [10] [12] [13] [14].

2.1.3. Tipos de aplicações para os UAVs

Os UAVs têm várias formas de serem utilizados, para além de divertimento e fotografia, onde são mais conhecidos, e têm vindo a ser explorados novos campos e áreas de tarefas que estes consigam facilmente executar. Nestes últimos anos, os UAVs têm simplificado alguns dos desafios encontrados em certas áreas mais delicadas, tais como vigilância e resgaste em situações complicadas.

Inicialmente os UAVs foram projetados para operações militares e têm sido utilizados já há algum tempo, para operações de vigilância e apoio por parte de agências governamentais e autoridades. No entanto, tinha-se ponderado serem utilizados por parte de empresas e civis, no qual iriam ter grande utilidade, como chegou a acontecer. É possível verificar que esta indústria está cada vez mais a ficar enraizada na nossa sociedade atual e tem-se registado grandes investimentos nesta área, principalmente nos últimos 5 anos.

As aplicações e áreas tipicamente mais conhecidas e utilizadas atualmente podendo ser planeadas para o futuro, são:

- Salvamento e Resgaste
- Vigilância em tempo real
- Operações de reconhecimento
- Monitorização de tráfego
- Inspeção em áreas delicadas
- Agricultura.
- Monitorização ambiental e meteorológica
- Inspeção de linhas de alta tensão e oleodutos
- Monitorização e inspeção de zonas de perigo ambiental ou contaminadas
- Combate a incêndios
- Retransmissão de sinais
- Fotografia e filmagem
- Publicidade

- Entre outros…

Os UAVs começam a ser escolhidos para estas tarefas devido ao facto de serem bastante úteis e eficazes na sua operação e em certas tarefas, podendo executá-las ao mesmo tempo, simplificando trabalho e tempo ao operador. Começam a existir a integração de sistemas autónomos nos UAVs, de modo a executar e concluir tarefas sozinho sem que seja necessária alguma intervenção humana, o que pode acelerar o processo e tempo de execução. Porém estes conceitos e tecnologias ainda são caras e experimentais, mas têm vindo a surgir alguns modelos já com estas funcionalidades. O interesse por parte de grandes corporações na utilização de UAVs para execução de tarefas específicas não é recente, aliás, a gigante Amazon, detém um protótipo em funcionamento para entregar encomendas através de UAVs – PrimeAir (figura 3), e outras empresas de transporte de mercadorias como a DHL, planeiam seguir o mesmo caminho (figura 4). Estas multinacionais estão a projetar a sua utilização em larga escala, devido à sua grande utilidade que os UAVs oferecem, visto que para pequenas distâncias e transporte de pequenas embalagens, são a ferramenta ideal [2], [10], [12], [13], [14].

Figura 3-UAV do projeto PrimeAir da Amazon, Fonte: [15][3]

Figura 4-UAV da empresa DHL, Fonte: [16][4]

[3] Imagem retirada do site: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011
[4] Imagem retirada do site: https://www.flexport.com/blog/drone-delivery-economics/

2.2. Sistemas GNSS

2.2.1. Introdução aos sistemas GNSS

Apesar de existirem vários sistemas GNSS globais e regionais, nesta dissertação só se irá discutir o sistema NAVSTAR-GPS, desenvolvido pelos E.U.A., visto que é o único que é amplamente utilizado pelo resto do mundo.

O sistema GPS, mais propriamente o NAVSTAR-GPS, começou a ser desenvolvido em 1973, tendo sido inicialmente planeada a transmissão de dois tipos de códigos/sinais com a mesma funcionalidade, mas com diferentes bandas de frequências: um de nível militar, com precisão e alcance superior, além de forte encriptação, e outro para uso civil, de sinal aberto e livre acesso. Este último, era degradado intencionalmente, para que os recetores não conseguissem obter uma boa aquisição da localização, o qual denominava-se por disponibilidade seletiva ou degradação seletiva. Só mais tarde, mais precisamente nos anos 2000, por ordem presidencial, é que a documentação total das especificações do sinal GPS civil, foi divulgada e aberta ao público (o sinal civil), fazendo com que os recetores de GPS fossem bastante melhorados, dispondo de melhores precisões. Estas informações, podem ser acedidas por qualquer indivíduo, atualmente, no site descrito em [17]. Posteriormente, todos os tipos de recetores GPS passaram a ter uma maior precisão de localização em qualquer parte do mundo, eliminando erros de cálculo de precisão. Assim, passou-se de erros do tamanho de um campo de futebol para apenas alguns metros e/ou centímetros de desvio. A partir dessa data começou a existir um grande aparecimento de aparelhos eletrónicos que utilizam GPS para certo tipo de aplicações que eram úteis em termos civis, tais como sistemas de navegação, e mais tarde a localização nos smartphones, que hoje damos como meios adquiridos [18], [19], [20].

2.2.2. Especificações e funcionamento do sistema NAVSTAR-GPS

O sistema GPS é constituído por uma constelação de satélites os quais orbitam a uma certa velocidade e altitude à volta do planeta Terra, sendo necessários pelo menos 24 satélites para o sistema ser funcional em toda a superfície terrestre. No entanto, existem mais de 24 satélites (aproximadamente 32 no total), em que os restantes, são satélites de backup (alternativos) [21]. Eles estão em funcionamento em conjunto com os satélites iniciais, o que proporciona uma melhor aquisição por parte dos recetores, visto que com este número de satélites, é possível abranger uma maior área de cobertura, o que resulta

num maior um número de satélites visíveis. Apesar da existência de mais satélites dos quais são necessários e que foram originalmente planeados, serve também para caso um dos satélites não esteja em bom estado de funcionamento, possa existir um complementar de forma a que o sistema não fique desfalcado. Esta constelação do sistema GPS está em orbita a uma distância de aproximadamente 20 180 km de altitude, a qual é completa por cada satélite em aproximadamente 11 horas e 58 minutos. Apesar da constante transmissão de ondas rádio que os satélites emitem, nem sempre chegam cem por cento corretamente à superfície terrestre, visto que podem existir perturbações nos sinais rádio à entrada da ionosfera, devido à ionização de plasma, o que afeta os eletrões e provoca refrações e difrações nas ondas eletromagnéticas, afetando assim a informação recebida pelos recetores (figura 5). Isto acontece com menos frequência, quando os satélites estão diretamente verticais em relação ao dispositivo recetor, ou seja, a camada da ionosfera tem pouca influência quando o satélite está diretamente por cima do recetor (ângulos de 90º graus), ao contrário do que, se estiver mais próximo da linha do horizonte. Alguns dos satélites mais recentes possuem recursos já em funcionamento para tentar mitigar este problema. Atualmente já se encontra na versão três do GPS – GPS III. A nova versão que está em desenvolvimento irá contar com bastantes características novas, tais como, novas capacidades de combater ainda mais às perturbações da ionosfera, novas bandas de frequências, tanto comerciais como civis, assim como melhoramentos na integridade, precisão e fiabilidade [20], [21], [22], [23], [24], [25].

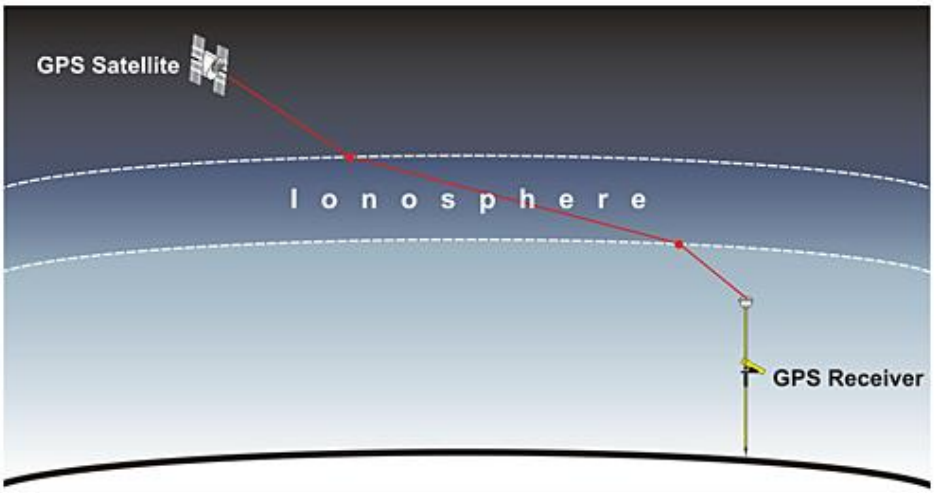


Figura 5-Demonstração da interferência do sinal GPS na ionosfera, Fonte: [24][5]

[5] Imagem retirada do site: https://www.e-education.psu.edu/geog862/book/export/html/1407

Na transmissão de cada satélite, são geradas as informações de data e hora, provenientes de um relógio atómico abordo de cada um. Cada relógio atómico é extremamente preciso e sincronizado em relação aos restantes, no qual determinam o tempo e hora a enviar na mensagem. Existem três tipos de modelos de relógios atómicos que os satélites podem utilizar: de césio, de rubídio, e de hidrogénio, no entanto o sistema NAVSTAR-GPS utiliza dois de césio e dois de rubídio. Inicialmente ponderava-se que os relógios atómicos fossem sincronizados a 10,23MHz, o que impossibilitava o recetor de conseguir calcular a sua localização, visto que eram criados erros de desvio de aproximadamente 11 km, e que resultava num sistema inviável. Isto deve-se à relatividade do tempo em relação à gravidade terrestre no qual é explicado pela teoria da relatividade geral de Einstein. Segundo esta teoria, um relógio na superfície terrestre percorre o tempo mais devagar, do que um outro localizado a uma altitude maior, o que dá a impressão de que, os relógios de cada satélite sofram um atraso de 7 microssegundos por dia, como é possível ver na figura 6. Tendo isso em conta, os engenheiros que planearam e desenvolverem o projeto, tiveram que projetar e calcular uma solução que impedisse que o sistema fosse inexequível, o que resultou na diminuição do relógio de cada satélite em 0.00457Hz, evitando que se formasse um atraso causado pela fraca gravidade do planeta Terra nos satélites, em relação aos recetores. De acordo com teoria de Einstein, os relógios dos satélites percorrem o tempo mais rapidamente do que os relógios terrestres, o que perfaz com que os relógios terrestres sofram na verdade um atraso de 45 microssegundos por dia causando um atraso de 38 microssegundos em relação aos relógios dos satélites. Sendo assim com esta redução da frequência de relógio, os recetores têm a possibilidade de concentrar-se na frequência 10.23MHz sem que haja algum problema com cálculos de relógio que provoquem desvios na localização, visto que é essa frequência que chega à superfície terrestre. Estes valores vão sendo ajustados ao longo dos anos devido à rotação terrestre, no qual os engenheiros da NASA corrigem este tipo de erros que possam surgir de forma a que sistema seja correto e fiável [19], [20], [26], [27], [28].

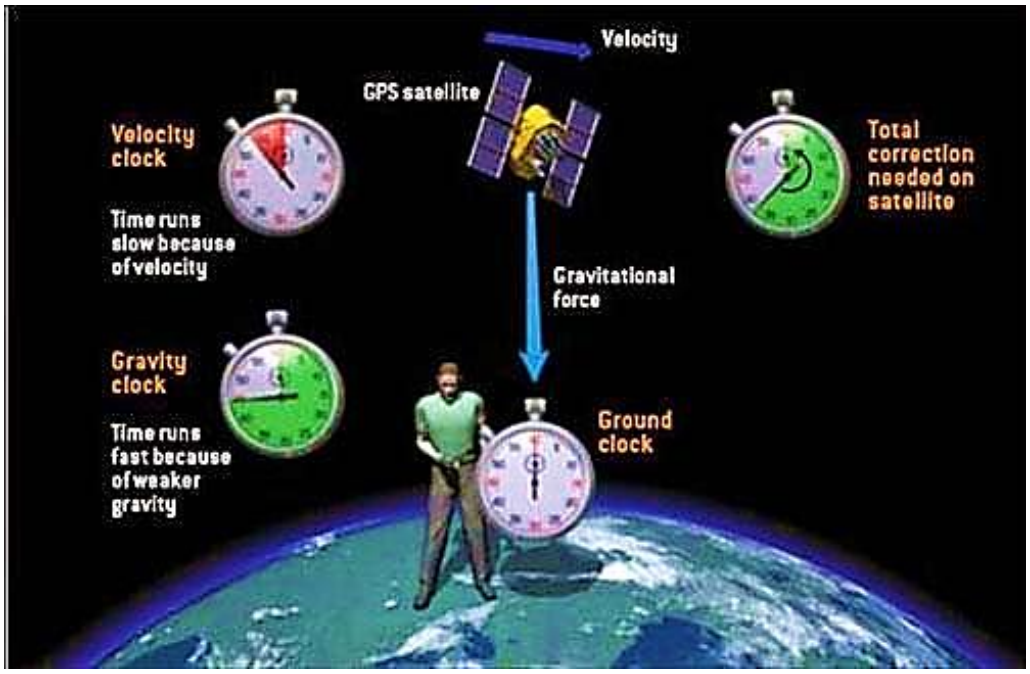


Figura 6-Exemplificação da relatividade do tempo nos relógios dos satélites, Fonte: [29][6]

Cada satélite trabalha com várias bandas de frequências, sendo as principais de 1575.42 MHz, denominada por L1 ou (L1C, nova versão que está a ser projetada para entrar em funcionamento); a L2 a 1227.6MHz, mais utilizada para fins militares devido a sua forte encriptação e L2C para uso civil, mais concretamente para fins comerciais autorizados; e a L5 à frequência de 1116.45MHz, desenhada e implementada para apenas fins civis, mais propriamente para fins comerciais de aviação, com objetivo de criar segurança nos aparelhos, visto que estes requerem constantemente contacto permanente com o sistema GPS. Ainda existem mais duas frequências, mas são para fins nucleares, que são a L3 e a L4, em que utilizam 1381.05MHz e 1379.913MHz respetivamente. Para que o recetor consiga receber os sinais provenientes do sistema GPS, sem que haja interferência eletromagnética, já que os vários satélites transmitem na mesma frequência, utiliza-se a técnica de multiplexagem CDMA (Code Division Multiple Access), o que proporciona a que os recetores consigam receber as ondas rádio sem que exista interferência entre as ondas rádio. Para além disso, a cada satélite é atribuído um código único que se denomina por PRN (Pseudo Random Noise), o que na verdade não é aleatório, mas sim calculado deliberadamente para que as

[6] Imagem retirada do site: http://unbonmotgroundswell.blogspot.com/2014/11/gps-and-relativity.html

mensagens/códigos gerados, não colidam entre si, e cada PRN atribuído a cada satélite, é único [20], [23], [30], [31].

Na banda de frequências L1, são transmitidos dois códigos, o civil C/A (Coarse/Acquisition) e o código P(Y) (Precision code). O primeiro é denominado por SPS (Standard Positioning Service) e é para uso civil. O segundo, denominado por PPS (Precise Positioning Service), e é apenas utilizado por forças militares e/ou governamentais. Apesar de existirem os dois códigos na banda de frequências L1, o código militar P(Y) é modulado em fase e na quadratura em conjunto com o código civil (C/A), como é possível ver na figura 7. Além disso existe a presença de um segundo código militar, o qual se designa por código-M, que foi projetado para ser resiliente a bloqueadores de sinal (jammers) e que está planeado para no futuro, substituir os códigos P(Y). Portanto os códigos M e P(Y), além de devidamente encriptados, são apenas para aparelhos militares, já que são os únicos que conseguem desencriptar os dados da informação. Por sua vez o código C/A não contém sequer algum tipo de criptografia, e a sua documentação é de livre acesso e o sinal de livre uso. O código C/A é transmitido a 1.023 Mega chips por segundo, e os códigos P(Y) e/ou M a 10.23Mcps, dez vezes maiores do que o código civil, sendo ambos posteriormente modulados por modulação BPSK (Binary Phase Shift Keying) na fase da transmissão. Na banda L2, apenas existem códigos P(Y) e M, que são códigos militares os quais têm exatamente as mesmas especificações que foram expressas anteriormente, apenas são gerados por uma portadora diferente, na banda dos 1227.6MHz. No entanto na mesma frequência, existe uma outra banda, a L2C, que além de conter os sinais militares P(Y) e M, contém ainda o sinal C/A, que foi descrito anteriormente. Esta banda de sinal foi projetada para combater as perturbações que eram causadas pela ionosfera, que o sinal L1 sofre. A banda L2C, foi desenvolvida também para fins comerciais autorizados e/ou fins militares, tendo uma maior precisão face ao sinal L1. Por fim a banda de frequências 1176.45MHz, que é destinada ao sinal L5, o qual é um dos mais recentes a ser implementada no sistema GPS (à exceção do L1C que ainda está em fases de testes). Esta foi projetada principalmente para a aviação e aplicações de alta performance, que precisam de um sistema preciso e fiável. Para além de uma maior resiliência a erros de precisão devido às camadas da ionosfera, tem uma maior potência de transmissão [20], [22], [23], [31], [32], [33], [34].

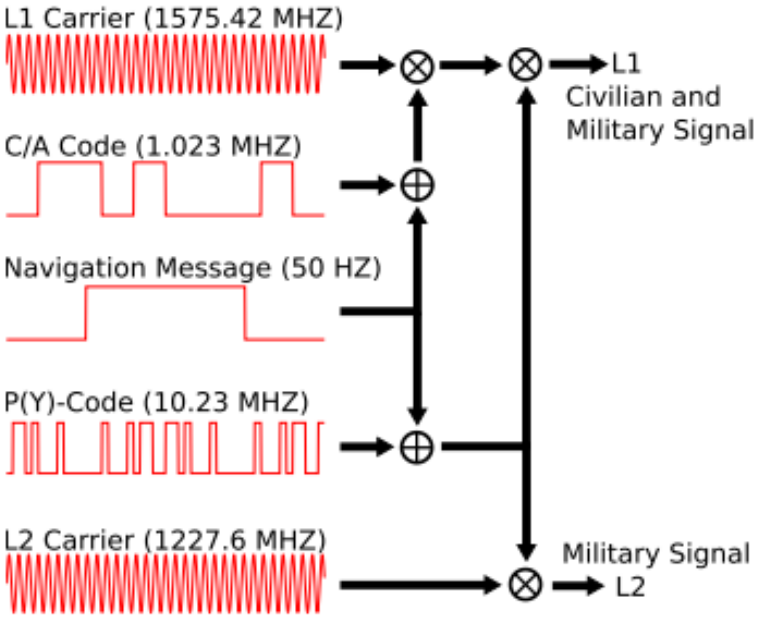


Figura 7-Estrutura do sinal GPS, bandas L1 e L2, Fonte: [22]

Demonstradas as especificações do sistema GPS, é necessário examinar a mensagem gerada por cada satélite, à qual dá-se o nome de Navigation Message (mensagem de navegação), que é possível ver na figura 8. Esta contém as informações necessárias de cada satélite, assim como outras, para que o recetor tenha a capacidade de conseguir calcular a localização mais rapidamente, visto que assim é possível identificar cada satélite. A mensagem de navegação é composta por 25 tramas, em que cada trama contém 1500 bits de informação. Cada trama é dividida em 5 subtramas. Uma subtrama é formada por 300 bits de informação, os quais são divididos em dez palavras (words), no qual cada palavra guarda até 30 bits de informação. Cada subtrama contém parâmetros com informação especifica, e começa sempre com duas palavras específicas: TLM – que é indicado para a telemetria da mensagem; e a HOW – que são para efeitos de handover. Na 1º subtrama – inclui o tempo/horário da semana em segundos, tempo do relógio do satélite, o estado do satélite, número da semana, assim como outros parâmetros de correção; nas 2º e 3º subtramas – contêm os dados da ephemeris, o que são na verdade informações precisas relativas à orbita, velocidade e tempo das rotas de cada satélite, no qual são válidas por várias horas (de 12 a 24 horas); por fim as 4º e 5º subtramas – contêm o almanaque. O almanaque é divido em 25 páginas, que inclui informações sobre os vários satélites em orbita, assim como informações do seu estado, como alguns valores de correção, além do tempo UTC – Universal Time Coordinated.

Nessas 25 páginas do almanaque, são guardadas as informações dos satélites 25 a 31, que são colocados na 4º subtrama, enquanto as informações dos satélites restantes (1 a 24), são dispostas na 5º subtrama. As informações do almanaque que contém partes de informação de outros satélites, servem para que os recetores consigam adquirir mais facilmente o sinal. Para finalizar a mensagem de navegação é transmitida a um débito binário bastante baixo, apenas de 50bps, o que perfaz a soma total da mensagem completa de 37500 bits, e se dividir-se pelo débito binário, dá um total de 750 segundos. A transmissão da mensagem total só é completa em 12,5 minutos, voltando a ser retransmitida novamente outros 12,5 minutos, assim sucessivamente [7], [22], [23], [35].

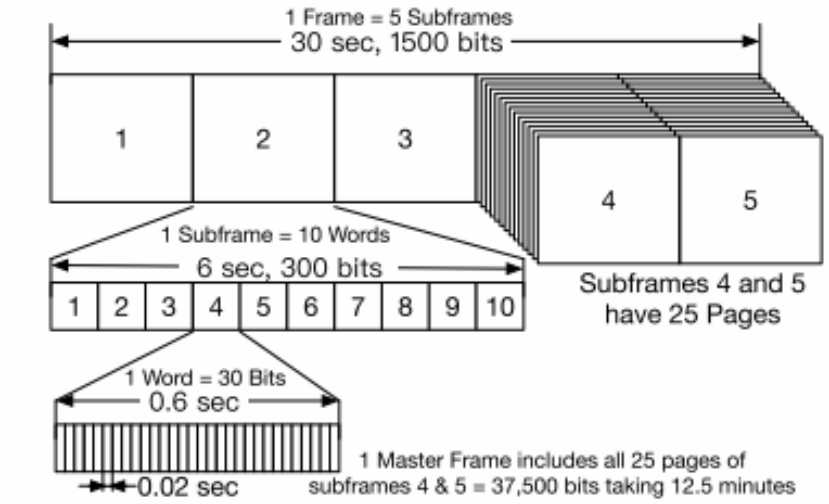


Figura 8-Estrutura da trama do sistema GPS, Fonte: [7]

2.2.3. Trilateração e efeito Doppler

Para que seja possível que os recetores consigam calcular a sua posição na superfície terrestre, são precisas técnicas especializadas, dado que os satélites estão em constante movimento. Para isso utilizam-se fórmulas trigonométricas no recetor, de maneira a que este consiga calcular a sua localização na superfície terrestre. O modelo que é utilizado denomina-se por trilateração, o que é diferente de triangulação. A diferença entre estes dois conceitos, reside em que na trilateração são medidas distâncias com base no tempo de propagação, e na triangulação são medidos ângulos de forma a ser possível calcular o ponto central [36].

A trilateração consiste (figura 9), na aquisição da distância dos satélites através do tempo de propagação da onda eletromagnética, que é transmitida pelo satélite até ao recetor. O recetor calcula a distância do satélite até ao mesmo com a seguinte fórmula,

$$d = c \times t_d \, , \tag{1}$$

em que *d* é a distância, *c* a velocidade da luz no vácuo e t_d é o tempo de propagação entre o satélite e o recetor. O recetor calcula o t_d através da comparação do tempo enviado na mensagem com o tempo recebido pelo recetor, onde é extraída a diferença entre os dois tempos que é posteriormente utilizado na fórmula (1), determinando a distância desde do satélite até ao recetor. Como se pode ver na primeira fase da figura 9, o recetor adquire o tempo transmitido pelo primeiro satélite e determina a respetiva distância, que consiste na esfera verde. Continuamente calcula a distância dos restantes satélites, até ao quarto satélite, utilizando a intersecção nas esferas para determinar a sua posição terrestre. Anteriormente foi referido que era necessário no mínimo quatro satélites para que seja possível a localização. Na figura 9 é demonstrado a sua razão, como os três primeiros determinam o ponto na superfície terrestre, o quarto satélite serve para definir o tempo onde o recetor se localiza [22], [37], [38], [39].

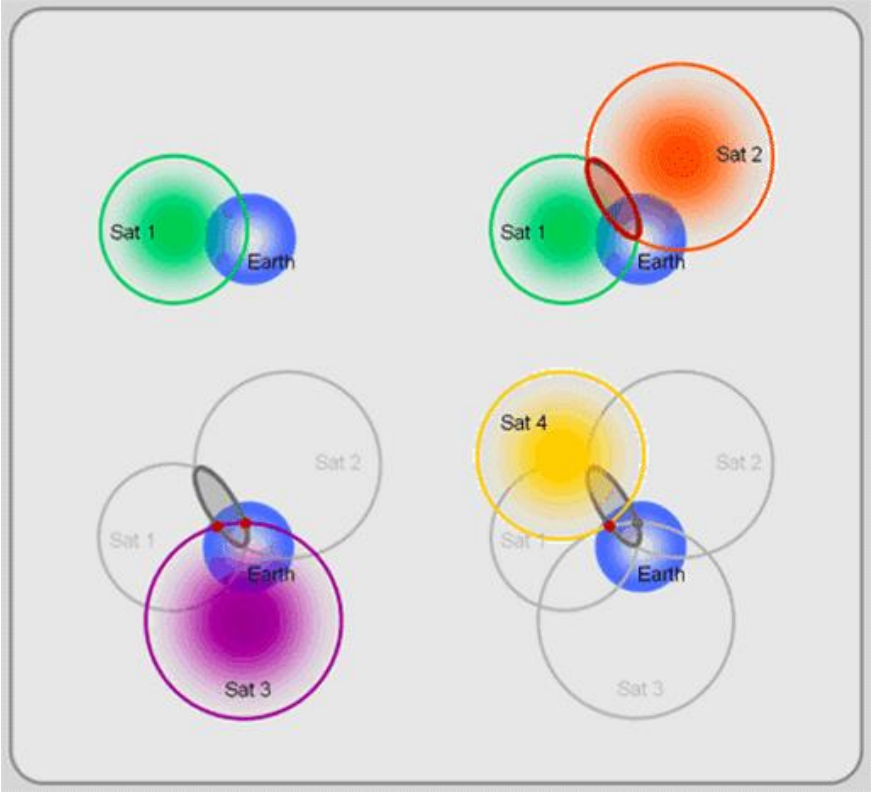


Figura 9-Demonstração da trilateração, Fonte: [40][7]

[7] Imagem retirada do site: https://i2.wp.com/www.techjini.com/wp-content/uploads/2013/04/FVsHS.gif?ssl=1

O efeito doppler ou mais conhecido como desvio de Doppler, é um desafio físico que se enquadra apenas no recetor, devido à constante movimentação dos satélites GPS. O efeito doppler, consiste na expansão ou compressão da onda rádio, consoante a movimentação, o que afeta o formato da onda rádio recebido no recetor, ou melhor, consiste no aumento ou diminuição da frequência entre o emissor e o recetor. Como se verifica na figura 10, o efeito doppler da onda eletromagnética sobre o recetor, quando o satélite se dirige na direção do mesmo, a sua frequência final sofre uma compressão da onda recebida, ou seja, o recetor tem que ajustar o desvio de doppler na frequência recebida, neste caso, decrementando ligeiramente a frequência, de forma a que consiga adquirir as informações corretas do satélite. O mesmo acontece quando o satélite se afasta, em que o recetor tem que ajustar a frequência recebida, de forma a combater o mesmo efeito. Estes ajustes são fundamentais para que seja possível decifrar as informações recebidas da mensagem de navegação, no qual auxiliam o recetor a localizar os restantes satélites [41], [42].

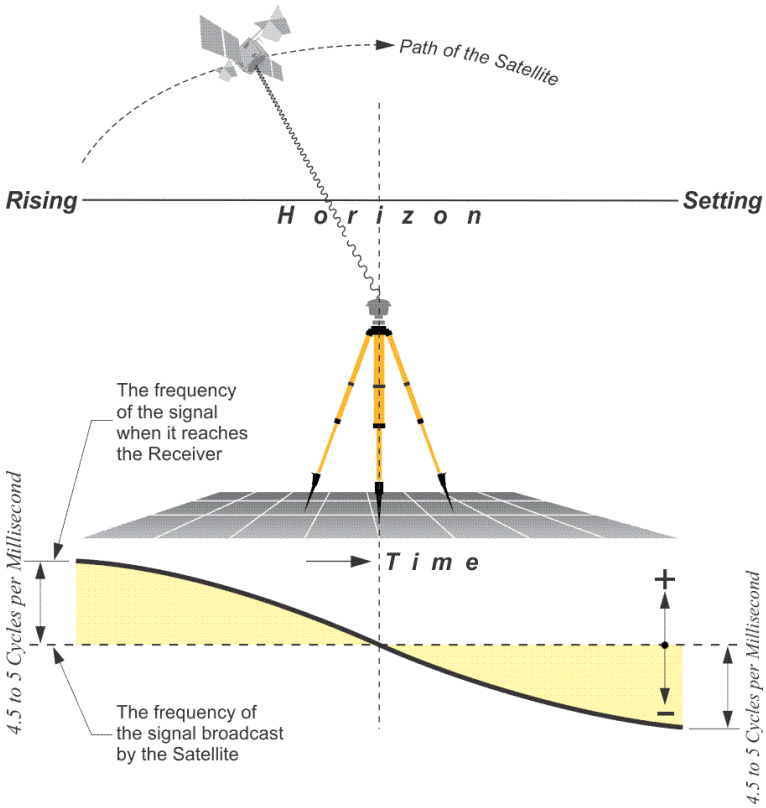


Figura 10-Efeito doppler no recetor, Fonte: [41][8]

[8] Imagem retirada do site: https://www.e-education.psu.edu/geog862/book/export/html/1659

2.2.4. Vulnerabilidade do GPS

O sistema GPS, é utilizado mundialmente, e muitos serviços e aplicações dependem da fiabilidade que o sistema oferece. No entanto a integridade e fiabilidade do sistema GPS pode ser comprometida, principalmente no sinal civil, denotando que este não contém nenhum mecanismo de proteção de informação. Isto quer dizer que é possível falsear a informação e transmiti-la ao recetor sem que este se aperceba, o qual a aceita como sendo original. Esta técnica dá-se o nome de Spoofing, que consiste em falsear a transmissão, isto é, são replicadas as informações contrafeitas de forma propositada, de maneira a que os dispositivos recetores, identifiquem a informação como sendo fidedigna, o que provoca a deturpação dos dados enviados, podendo ser controlado o seu fluxo da comunicação, pelo atacante. O spoofing do sinal GPS, é possível devido à falta de autenticação da mensagem GPS, visto que, não existe qualquer tipo de criptografia ou autenticação nos sinais civis, apenas nos sinais militares, como foi referido anteriormente. Nos sinais militares, isto não é possível devido ao facto de utilizar chaves criptográficas para cifrar a informação. Por outro lado, o sinal civil, devido a ser aberto e de livre utilização, potencia a utilização desta técnica de spoofing, de modo a atacar algum dispositivo recetor, visto que este não tem modo de verificar a autenticidade da informação de forma interna, apenas por meios externos, como por exemplo, outro aparelho, ou a própria rede e/ou a infraestrutura. As informações do sinal GPS podem ser descarregadas, pelo website em [17], o que não impede que qualquer indivíduo consiga visualizar as especificações da mensagem original e replicá-la, com coordenadas diferentes das originais. Este caso do spoofing do sinal GPS, não é recente, como aliás já tem sido alvo de críticas e de diversos tipos de investigação na comunidade científica. Pode-se dizer que além de vários investigadores estudarem este assunto, existe um investigador que alertou e provou os perigos, desta vulnerabilidade. Esse investigador é o professor Todd Humpreys da universidade do Texas, em Austin, no qual além de alertar em vários artigos e relatórios, experimentou esta técnica de spoofing em UAVs, assim como em aparelhos de receção GPS de última geração, ficando mais conhecido, o caso, em que ele e a sua equipa conseguiram ludibriar o sistema de navegação de um iate de luxo, o qual dispunha de tecnologia de ponta, na altura [43].

Além da existência do spoofing, ainda existem técnicas de jamming, que são bloqueadores de sinal que impedem que o recetor receba qualquer tipo de sinal, o que é

mais fácil para o recetor perceber, do que a situações de spoofing, visto que, é mais fácil recriar o sinal do que detetar a sua originalidade. Apesar das vulnerabilidades conhecidas, ambas as técnicas são ilegais na maioria dos países, mas isso não impede a existência de ataques, o que poderá potenciar desastres futuros [18].

2.2.5. Incidentes anteriores

Um dos casos polémicos em 2011, explicado em [44], [45], relata o desaparecimento de um UAV militar Americano, mais concretamente do RQ-170, segundo o qual foi capturado pelas forças Iranianas. Na altura, surgiu a teoria que tinha sido executada através de spoofing do sinal GPS. Para explicar esta teoria, as forças Iranianas, tiveram que usar métodos bastantes complexos e eficientes, além de recursos adicionais, como bloqueadores de alta potência – jammers, e projetaram-nos na direção do UAV, de forma a bloquearem os sinais emitidos pelo sistema de satélite [11], [46]. Apenas ficou recetível o sinal GPS civil, no qual este é aberto, ou seja, as bandas de frequências civis, além de não terem sido bloqueadas, não utilizavam qualquer nível de encriptação. Seguidamente simularam o sinal GPS, com as informações falaciosas, e transmitiram na direção, do UAV, utilizando o spoofing avançado [44]. Deste modo o UAV militar como tinha instruções pré-programadas, para regressar à base, caso perdesse a conexão com o operador, adquiriu o sinal com maior intensidade. Não tendo forma de verificar a origem do sinal, este seguiu as indicações onde estavam a ser projetadas as coordenadas de regresso à base americana, quando na verdade estava a ser manipulado para aterrar num local planeado estrategicamente pelas forças Iranianas. Foi devido a este evento que começaram a surgir mais casos de spoofing em outro tipo de veículos, tais como marítimos e terrestres, sendo assim possível afetar todo o tipo de aparelhos [47].

Com o decorrer da sua investigação, em 2012, [45], conseguiram atacar e manipular um UAV de 80 mil dólares (que naquela época ainda eram emergentes), o qual era utilizado por forças de autoridade para patrulhar. Este veículo que foi testado, era um UAV de alto calibre, e além de ser controlado à distância por operador, estava equipado com um sistema de navegação autónoma. O UAV de testes, estava a ser operado autonomamente, e ele e a sua equipa, conseguiram com sucesso manipular a trajetória do UAV através de spoofing do sinal GPS, e com alguma distância relativamente ao alvo. Para isso desenvolveram equipamento especializado em recriar os sinais GPS, no qual foi desenvolvido por eles e pela resta equipa de investigação da universidade do

Texas. Foi a partir deste marco que se deu mais atenção a casos de spoofing em UAVs, e despertou a atenção da restante comunidade científica, devido ao facto de se estar cada vez mais a implementar sistemas semi e totalmente autónomos, que se baseiam na localização por GPS. Mais tarde, em 2013, [45], ainda testaram o mesmo sistema num iate com tecnologia de ponta em termos de sistemas de navegação, e conseguiram com sucesso também, dissuadir o sistema de navegação por GPS do iate, em que se simulou os sinais contrafeitos de GPS, que por sua vez fez com que o navio fosse desviado da rota atual. Este feito está descrito em [43].

Em 2015, investigadores de uma empresa chinesa de segurança, a Qihoo 360, utilizaram meios e técnicas de spoofing do sinal GPS, para ludibriar a segurança implementada nos UAVs da marca chinesa DJI, no qual conseguiram aterrar um deles dentro do pátio da Casa Branca, nos E.U.A.. Estes investigadores, conseguiram contornar as medidas de segurança que a DJI implementa nos seus UAV, que consistem no bloqueio do dispositivo em certas zonas proibidas, para o seu uso e voo, sendo utilizados sinais GPS para ser monitorizado constantemente o seu percurso. Visto que os investigadores, se aperceberam desta habilidade de recriar os sinais, o que é extramente difícil de ser detetada por estes veículos, decidiram experimentar em vários tipos de UAVs, tanto os da DJI (que é uma empresa de renome, no mundo dos UAVs), como outros. Além da Casa Branca que é uma zona altamente restrita, também invadiram o Aeroporto de Dulles [48].

Mais recentemente, em 2017, vários navios tiveram as suas comunicações e sistemas de navegação GPS, afetados por parte de uma entidade, que fabricou coordenadas contrafeitas, no mar Negro. Grande parte dos países acusam a Rússia de criar uma super-arma de spoofing do sinal GPS, o que pode bem afetar, mais do que apenas os barcos. Vários reportaram que estavam alguns quilómetros afastados do sítio que era esperado estarem. Nunca se chegou a saber quem teria sido a entidade que desenvolveu este ataque [49].

Por fim, o caso da aplicação do Pokémon GO, que consiste num jogo apenas para dispositivos móveis, e que foi desenvolvido pela empresa Niantic, Inc., e utiliza o sistema GPS dos smartphones para interagir com o jogador. O utilizador além de necessitar a localização GPS, tem de procurar os tais objetos virtuais (Pokémons), no qual aparecem no ecrã do smartphone, quando este se encontra fisicamente no local. Para isso, os desenvolvedores desenharam o mapa do jogo em cima do mapa real, o que na verdade tem um funcionamento igual a um sistema de navegação semelhante ao

google maps [50]. No entanto além da febre desta aplicação, iniciou-se uma espécie de desbloqueio dos tais objetos de forma ilícita, que é através do spoofing do sinal GPS, direcionado aos smartphones, o que permite um desbloqueio dos objetos virtuais mais rapidamente. Existem duas maneiras de executar o spoofing, o virtual, em que é feito através de software dentro do dispositivo, ou o real, em que consiste recriar os sinais GPS verdadeiros através de SDR. No primeiro caso apesar de possível e de fácil execução, é difícil executar com sucesso, devido ao próprio jogo conter mecanismos eficazes na verificação deste tipo de fraudulento, o que a companhia considera esta fraude ilegal, e como punição os jogadores são banidos. No segundo caso é mais complicado, como o dispositivo está a receber "supostamente" o sinal GPS original, torna-se bastante complicado de verificar a verdadeira ocorrência. No entanto, ainda assim é possível ser banido, se o jogador fizer o spoofing para um local bastante longe onde se situa. Contudo alguns utilizadores utilizam certas técnicas de spoofing do sinal GPS, sem que seja necessário que estes estejam fisicamente no local, conseguindo obter maiores recompensas pelo jogo, mais facilmente que outros. Apesar disso, não impediu que os jogadores continuassem a fazer a mesma técnica, visto que desta vez nem necessitam de estar presentes no local físico [51].

Capítulo 3 – Spoofing de Sinais GPS

3.1. Introdução ao Spoofing

Como foi mencionado no capítulo anterior, a técnica de spoofing, já é existente no mundo da tecnologia há algum tempo, mais propriamente no domínio das redes sem fios, uma vez que o termo spoofing, deriva desse campo. O seu conceito, consta na replicação das ondas rádio que constituem a informação, neste caso específico é o sinal GPS, de modo a que, os dispositivos recetores não consigam detetar a presença do atacante, visto que este mascara-se como o originador do sinal original. Além de existir variantes de spoofing, torna-se difícil detetar este tipo de ataque, o que faz com que o recetor não tenha maneira de verificar se foi alvo deste tipo de ataque. Existem alguns meios para impedir ataques, como o caso da utilização de criptografia e/ou autenticação nos meios de comunicação, de forma a proteger a informação. Os ataques por spoofing são mais suscetíveis onde a informação é disponível e aberta para o público. Entretanto, estes ataques podem ser utilizados também em comunicações criptografadas onde a informação é protegida, só que o seu sucesso torna-se praticamente impossível, exceto se este conseguir a chave de acesso às comunicações. No entanto, começam a aparecer soluções de autenticação para comunicações civis, como é o caso da faixa L1C e do NMA do sistema Galileo [52], que tentam mitigar este tipo de ataque. Porém isto não previne cem por cento o ataque de spoofing, porque este tipo de mensagem utiliza técnicas e métodos disponíveis publicamente, o que torna o recetor vulnerável.

O GPS militar contém proteções contra este tipo de ataques, inclusive mecanismos de anti-spoofing, o que torna praticamente impossível de simulá-lo. Por outro lado, o sistema civil, não contém qualquer mecanismo de autenticidade (exceto a nova frequência da banda L1C). Nos presentes dias, utilizamos o GPS em numerosas aplicações, tais como localização, sistemas de navegação, etc., no entanto, através de plataformas de SDR, as quais estão cada vez mais acessíveis ao público, tanto em termos de especificações como de custos, é possível recriar as ondas rádio e as mensagens do sinal GPS civil, ainda mais facilmente, visto que grande parte das ferramentas estão disponíveis na Internet, como é explicado em [53] . Existem vários tipos de spoofing, mas no geral, têm todos o mesmo objetivo, que é simular as mensagens futuras emitidas pela constelação de satélites, de forma a que os recetores aceitem as informações como corretas, manipulando a sua posição, velocidade e tempo se necessário.

No caso dos UAVs, tornam-se vulneráveis, tais como os outros tipos de recetores, devido ao facto dos sistemas de navegação, precisarem constantemente dos sistemas GNSS. Esta vulnerabilidade pode ser utilizada tanto para efeitos de ataque, como de defesa, por exemplo um UAV, que esteja a operar em modo de voo autónomo é possível desviá-lo da trajetória atual, desviando-o para uma área proibida (ataque) ou para uma zona segura (defesa) [54].

3.2. Tipos e técnicas de Spoofing e o efeito Doppler

3.2.1. Tipos de técnicas de spoofing

Dado a possibilidade de se criar uma situação de spoofing, existem técnicas e tipos específicos para cada situação de ataque. Qualquer tipo de ataque descrito abaixo, é considerado ilegal na maior parte dos países do mundo. Seguem-se as variantes de ataques de spoofing:

- Meaconing – método de retransmissão do sinal GNSS original, excedendo a potência recebida do mesmo sinal, sobrepondo-se assim à transmissão original, de modo a que o recetor não consiga distinguir o verdadeiro e adquira o sinal com maior potência de receção. Desta forma, as comunicações do recetor sofrem um atraso causado pelo próprio atacante de forma propositada, em que este controla o tamanho do atraso introduzido na retransmissão;
- Spoofing – tipo de ataque que gera e transmite sinais contrafeitos dos sistemas GNSS, em que o seu alvo é um dispositivo recetor, em que este adquire o sinal como sendo o sinal original. Existe a manipulação das mensagens e informação que o atacante pretende enviar, tais como, posição, tempo e velocidade. Existem várias variantes, umas mais simples, e outras mais complexas. Por exemplo, no simplistic spoofing (spoofing simples), são gerados e transmitidos os sinais falsos com mensagens replicadas e manipuladas, no qual o atacante não tem a intenção de visualizar o espectro de emissão, isto é, deste modo o emissor não verifica se há interferência no sinal original, apenas é utilizada uma potencia de emissão maior (requer hardware de baixo custo). No intermediate spoofing (spoofing intermediário), requer que o atacante tente sincronizar o sinal contrafeito com o sinal original, tentando-se sobrepor a sua onda falsa, através da sincronização de fase. Por fim o sophisticated spoofing (spoofing avançado), requer hardware e software de alto custo, no qual seja possível alcançar e monitorizar o sinal

da vítima, em que o atacante, tenha a capacidade de utilizar os métodos anteriormente descritos de forma mais eficaz, com a exceção de controlar a potência emissora, com intuito de aumentar ligeiramente a mais do que o sinal original. Neste tipo de ataque, como o sinal contrafeito tem ligeiramente uma maior potência de receção, o recetor não tem qualquer hipótese de notar algum tipo de diferença, visto que é utilizado o método da sobreposição de onda rádio, além da devida sincronização;

- Estimation and replay – método mais utilizado em comunicações encriptadas, no qual o spoofer (atacante) recebe o sinal e estima a chave de encriptação da informação que nela se encontra, criando um atraso entre o emissor e recetor. Isto dá-se um nome de SCER (Security Code Estimation and Replay), no entanto pode ser utilizada para estimar novos códigos futuros;
- Nulling attack – este ataque é bastante utilizado pelo spoofing avançado, no qual se inibe o sinal recebido no recetor através da destruição da fase de onda, ou seja, é recriada uma onda negativa em relação ao sinal original, de modo com que o sinal original seja anulado por completo [8], [44].

3.2.2. Efeito doppler

O efeito doppler como já foi explicado no capítulo anterior, tem várias vertentes no caso do spoofing. Existem variáveis que são cruciais, tais como, o movimento do dispositivo recetor e o movimento da constelação de satélites em relação à terra, além do movimento entre o atacante e o recetor, se este último existir. No spoofing avançado, requer que o atacante obtenha a constante localização exata do dispositivo recetor, quer este esteja em movimento, ou não, para ser possível recriar os sinais GPS com o desvio de doppler contido no seu ataque, visto que a transmissão gerada pelos satélites sofre um desvio quando chega à superfície terrestre. Assim o dispositivo, não tem qualquer capacidade de observar desvios, quer seja de fase e/ou frequência, o que conclui com sucesso o ataque de spoofing por parte do atacante. É possível observar na figura 11, o constante movimento, além do desvio do movimento do planeta terra, que o atacante tem de ter em conta no seu ataque.

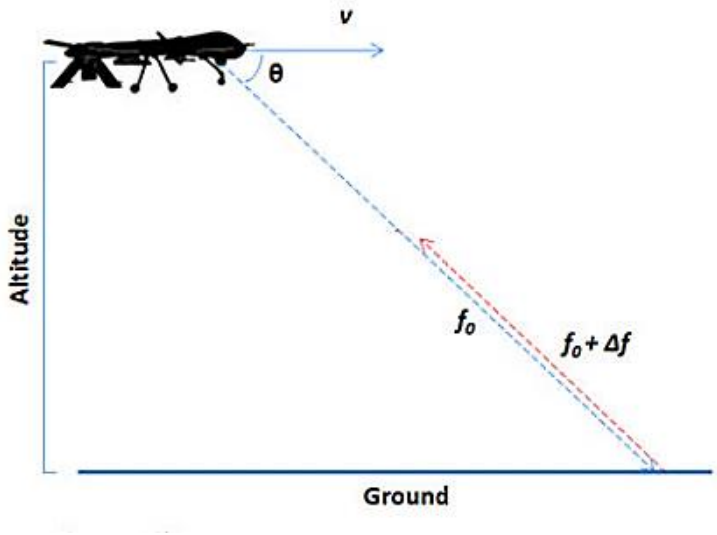


Figura 11-Demonstração de um UAV em movimento, no qual o atacante tem de ter conta os vários desvios possíveis, Fonte: [55]

Isto adiciona um desafio em que o spoofer (atacante), terá de calcular os respetivos desvios, de forma a ter sucesso no seu ataque. No caso do spoofing simples, apenas é preciso ter a noção das ondas recebidas na superfície terrestre, dado que, como foi referido anteriormente, o sinal quando chega à superfície terrestre sofre um desvio de frequência, em relação ao original. Portanto se o atacante não tiver isso em conta e começar a transmitir a constelação com as suas especificações originais, não irá conseguir que o recetor adquira o seu sinal, visto que o recetor contém os desvios predefinidos nos seus cálculos, no qual não baterá certo com os sinais recebidos e descarta o sinal. É possível ver na figura 12, que o recetor tem sempre noção do efeito doppler em relação aos satélites originais. Isto deve-se ao facto de os satélites estarem relativamente longe do recetor final e que o atacante está bastante mais perto da vítima [44], [45], [55].

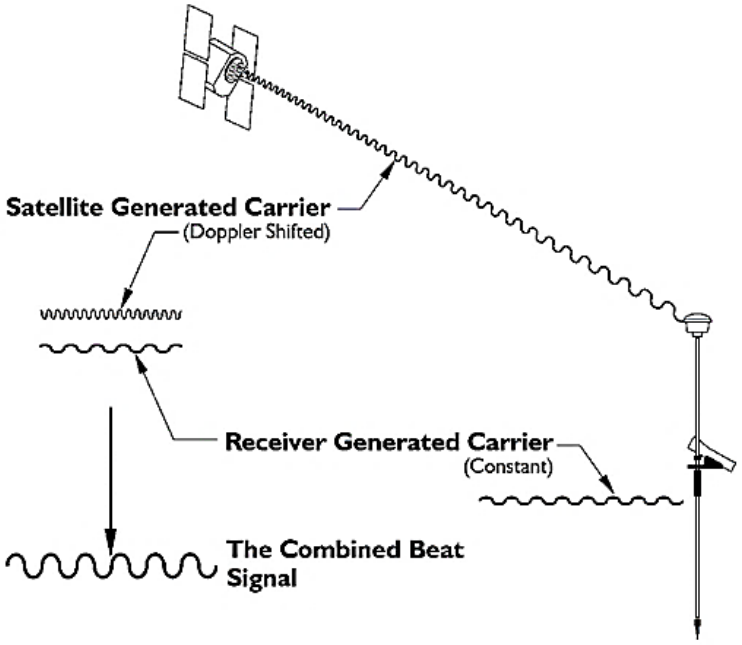


Figura 12-Comparação do espetro de frequências GPS com o Efeito Doppler sobre o Recetor, Fonte: [56][9]

3.3. Simuladores GNSS

3.3.1. Introdução aos simuladores

Para fins desta investigação e do projeto de dissertação, necessitou-se de uma ferramenta que tivesse a capacidade de simular os sinais GPS, com o intuito de poupar tempo e problemas dos desafios anteriormente explicados, dado que desenvolver um sistema de spoofing de raiz, seria bastante complexo e demoroso [45]. Existe um ótimo simulador, que é utilizado para operações que envolvam o sinal GPS, cujo nome é "gps-sdr-sim", e que está disponível no website github [57] através da licença MIT. O seu funcionamento é desenhado para certos tipos de plataformas SDR, as quais são bastante conhecidas, no campo da investigação, por serem bastante versáteis e eficientes em termos de teste e produção de ondas rádio. As plataformas descritas pelo desenvolvedores são: a ADALM-Pluto, a BladeRF, a HackRF, e a USRP, plataformas estas que fazem parte da gama de SDR, mais utilizadas [57].

O(s) criador(es) deste software, tem o nome com a sigla OSQZSS, o que se presume que seja a equipa de engenharia aeroespacial que esteve por detrás do desenvolvimento do programa espacial do Japão – Open Source Quasi-Zenith Satellite System [58]. Não

[9] Imagem retirada site: https://www.e-education.psu.edu/geog862/book/export/html/1659

se sabe ao certo se estes são os verdadeiros desenvolvedores original do projeto espacial, no entanto devido ao nome e à estrutura grande que o código possui, presume-se que seja alguém ligado à área aeroespacial. O simulador em questão, funciona através da linha de comandos do sistema operativo, ou seja, não contém qualquer tipo de interface gráfica. É um software desenhado apenas para recriar situações de simulação do sistema da constelação NAVSTAR-GPS, o que para esta dissertação, era o pretendido.

A BLadeRF, é uma plataforma SDR, da empresa Nuand, tendo sido utilizado o modelo x40, figura 13, que dispõe de especificações essenciais para operações com sistemas GPS, que funciona na banda dos 1575.42MHz. A BladeRF x40, dispõe de uma largura de banda desde os 300MHz, até aos 3,8GHz, o que será mais que suficiente para este projeto. A unidade de processamento desta unidade é uma FPGA, à qual é acoplado a um computador externo, através de USB3.0.

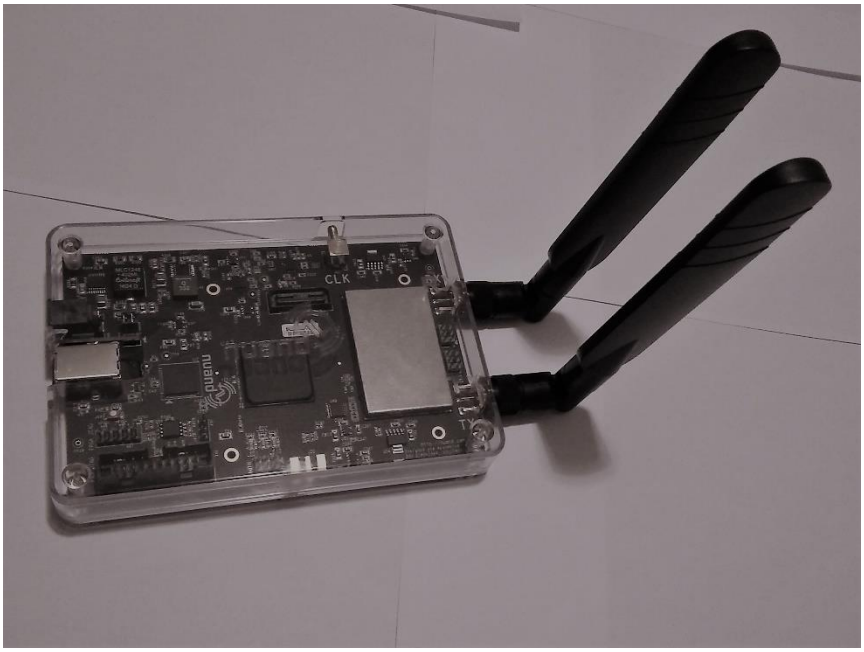


Figura 13-Plataforma SDR utilizada, a BladeRF x40

3.3.2. Simulador gps-sdr-sim

Para utilizar o simulador usou-se uma distribuição Linux, mais concretamente o Ubuntu, no entanto é possível utilizar o simulador em sistemas operativos Windows. Após a instalação, verifica-se que o software necessita primeiro de compilar a informação da localização do local escolhido, e só posteriormente é que é possível gerar os sinais de GPS. Observa-se a compilação de coordenadas estáticas, na figura 14.

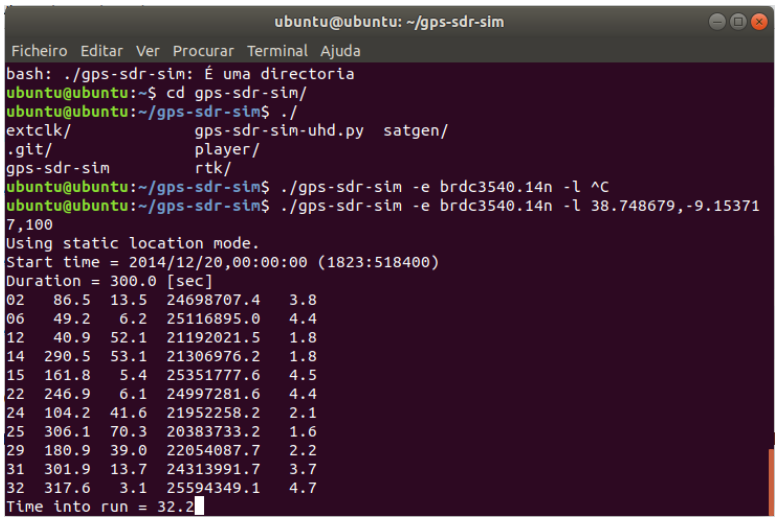


Figura 14-Demonstração do Simulador em execução na compilação das coordenadas

Após concluída a compilação, pode-se executar o comando de transmissão de modo a executar-se o spoofing num local estático, figura 15, onde se vê o software a enviar as informações para BladeRF transmitir.

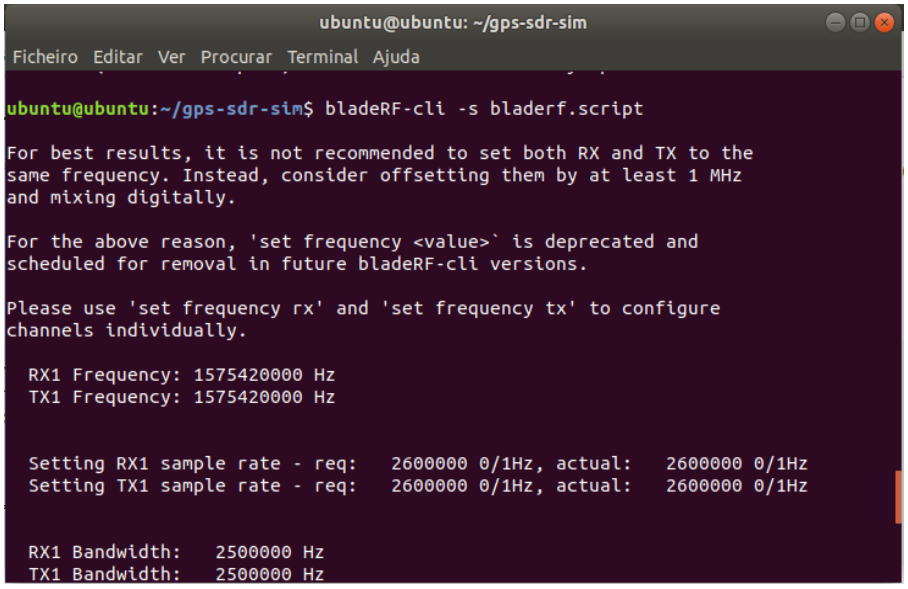


Figura 15-Execução do spoofing através da BladeRF

De maneira a experienciar o spoofing com a utilização do simulador, utilizou-se um dispositivo recetor de GPS, e neste caso escolheu-se um smartphone como alvo. Com o smartphone a receber o sinal GPS original, introduz-se a transmissão do sinal GPS contrafeito de modo a observar-se se é possível manipular a localização real. Como se

pode ver na figura 16, primeiramente o dispositivo adquire com sucesso o GPS original (duas primeiras sequências), e seguidamente após o início da transmissão, observa-se que o recetor além de reconhecer novos satélites, adquire sinais com maior potência, finalizando a sua aquisição da localização, que corresponde a uma localização falsa.

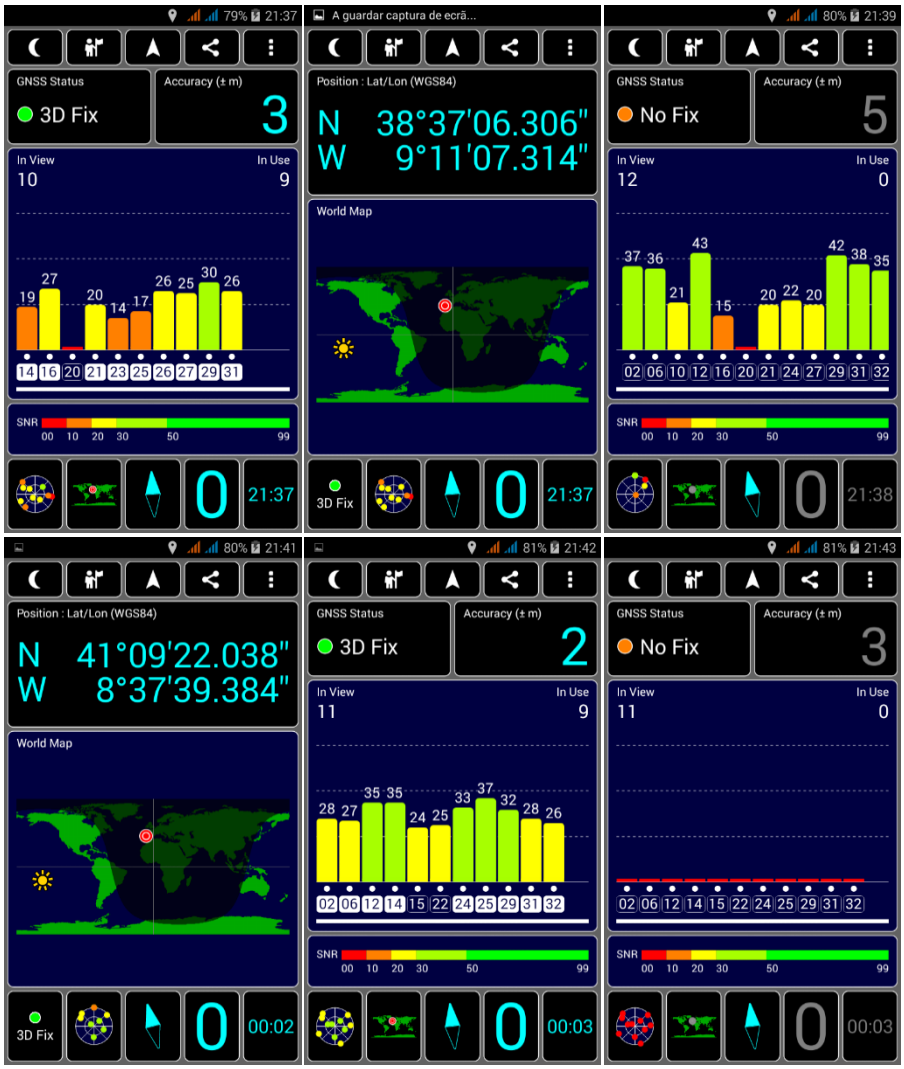


Figura 16-Demonstração da localização contrafeita num smartphone

Apesar disso, para efeitos de desenvolvimento e depois de alguns testes, achou-se que o simulador descrito não era o mais indicado, devido ao facto de se necessitar da compilação e transmissão simultânea, algo que este simulador não permitia. Como se viu nas figuras 14 e 15, era necessário primeiro executar a compilação quer sejam coordenadas geográficas estáticas ou ficheiro com coordenadas, e só posteriormente é que era possível a opção de transmissão. Isto implica que não seja possível, enviar os dados (coordenadas) e transmiti-las ao mesmo tempo, o que compromete o

desenvolvimento do resto do programa. Presenteado o tempo de espera desde a compilação, até a formação da mensagem GPS, foi necessário encontrar outra solução que dispusesse de simulação em tempo real. Essa solução é descrita na próxima secção.

3.3.3. BladeGPS

O software BladeGPS, é uma versão do simulador, gps-sdr-sim, o qual foi apenas desenvolvido para a plataforma BladeRF. Esta versão do simulador, dispõe de características especiais, que não estavam disponíveis anteriormente, figura 17, tais como, a compilação e transmissão, das coordenadas/mensagens, em tempo real. Isto é, apesar de conter a mesma interface, é possível enviar apenas a informação das coordenadas através de um ficheiro NMEA, em que o software, compila e transmite coordenada a coordenada, de forma automatizada, em vez de só se transmitir após a compilação total do ficheiro.

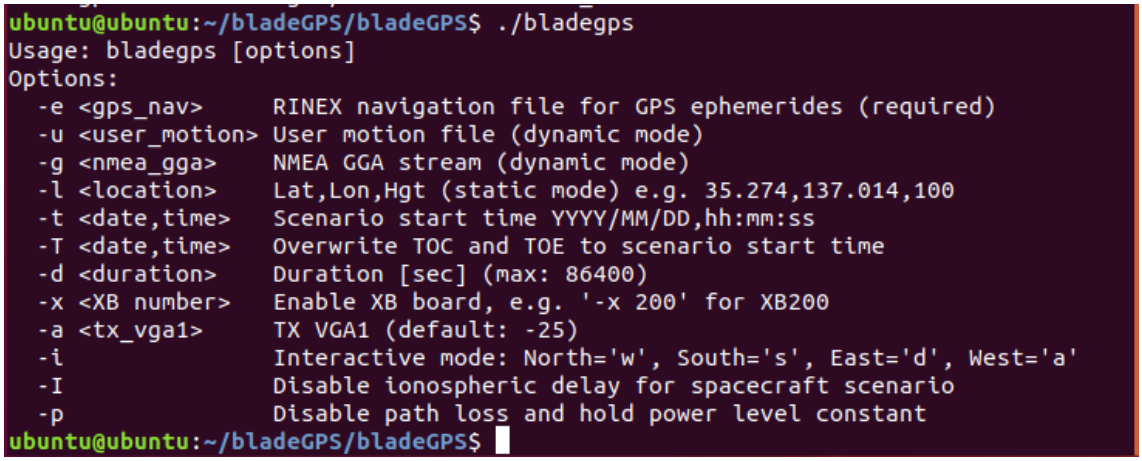


Figura 17-Demonstração do simulador BladeGPS

Os tipos de ficheiros que o programa aceita, podem ser .txt ou .csv, mas necessitam obrigatoriamente de estar organizados com o formato NMEA GGA. A estrutura NMEA, contém vários tipos de formatos, no entanto apenas utiliza-se um tipo, que é o GGA. A sigla NMEA, significa National Marine Electronic Association, e é uma associação internacional que estipulou, formatos de transmissão de informação ainda antes do GPS, ter sido implementado. Este formato é bastante conhecido pelos sistemas GPS, e é considerado um standard universal, o que facilita o desenvolvimento de software que necessite de utilizar coordenadas GPS [59]. O formato NMEA GGA, é descrito por caracteres e coordenadas, os quais começam sempre com o símbolo $ e são sempre

separados por vírgulas. Segue-se uma demonstração de uma coordenada gerada de forma a explicar a sua estrutura [60] [61]:

$GPGGA,151213.069,3747.4664,N,02534.8526,W,1,05,2.87,160.00,M,21.3213,M,,*58

$GPGGA – representa a designação do sistema em uso, neste caso o GPS (se fosse GL, era o sistema Russo, GLONASS);

151213.069 – representa o tempo UTC, no seguinte formato hh:mm:ss.mm;

3747.4664 – representa a latitude em formato de DDMM.MMM;

N – designa o Norte, podendo ser o S de Sul;

02534.8526 – longitude no mesmo formato que a latitude;

W – significado de West ou seja, Oeste, podendo ser E de Est (Este);

1 – significa a fixação do GPS, existindo vários significados que variam consoante a utilização, em que começam no 0 até ao 8;

05 – a quantidade de satélites visíveis;

2.87 – representa a diluição da posição horizontal;

160.00 – representa a altitude;

M – de metros Acima do nível do mar;

21.3213 – a altura em relação ao geoide de acordo com a norma WGS-84;

Espaço vazio;

Espaço vazio;

***58** – consiste no checksum da informação descrita.

Capítulo 4 – Sistema Implementado

4.1. Introdução

O objetivo deste projeto de dissertação é criar um mecanismo de defesa, de forma a impedir a entrada de UAVs, em áreas protegidas, recorrendo a técnicas de spoofing do sinal GPS. Como foi referido anteriormente, os sistemas de navegação do UAV, baseiam-se inteiramente no sistema GPS, o que os torna vulneráveis à manipulação da sua trajetória, como foi demonstrado em [45]. Isto potencia a criação e desenvolvimento de sistemas de defesa, para prevenir potenciais perigos, dado que existe cada vez mais a utilização indevida dos veículos. Além do sistema de spoofing, é necessário a utilização de outros componentes de forma a que o sistema tenha a capacidade de deteção (Radar) e seguimento dos alvos, assim como utilização de técnicas de jamming nas comunicações alvo, de maneira a que o intruso não tenha a capacidade de contra atuar. Apesar destes componentes estarem planeados, não serão abordados neste projeto.

Para efeitos de desenvolvimento, utiliza-se o simulador anteriormente descrito, o BladeGPS, em conjunto com uma interface desenvolvida através do SDK ArcGIS, da empresa Esri, de que é conhecida por sistemas de informação geográfica, e a FrameWork QT, que é uma plataforma baseada em código multiplataforma, no qual contém bibliotecas com diversas finalidades, em que a programação é baseada em C++ e QML. O desenvolvimento deste projeto vem facilitar a visualização, dos acontecimentos para o utilizador final.

O SDK ArcGIS, é um kit de desenvolvimento, da empresa Esri, que é conhecida mundialmente por oferecer serviços de sistemas de informação geográficos, em que, grande parte são relacionados com software de mapas, cartas geográficas, serviços de localização, GPS, etc., o que torna a ferramenta ideal para este projeto. Existem duas versões do SDK, uma totalmente paga, e outra versão gratuita. Ambas têm acesso a todas as características, enquanto não for lançada a versão final do produto, isto é, o desenvolvedor tem acesso total ao software, enquanto não for compilado o programa final, porque cada programa terá que conter uma chave de ativação anual, que funciona como uma marca de água, podendo esta ser renovada se assim o cliente ou desenvolvedor quiser. Na versão gratuita, apenas é necessário a criação de uma conta de desenvolvedor, se este não tiver, a qual dá acesso aos manuais e ao download do SDK, assim como outras funcionalidades que ficam disponíveis, tais como os mapas offline,

em que estes são propriedade da empresa. O SDK tem como alvo várias linguagens de programação, entre as quais a QT, o que auxilia o desenvolvimento do projeto [62].

A framework da QT, é uma das frameworks de desenvolvimento C++, baseada em aspetos gráficos e interfaces, sendo bastante conhecida na área de desenvolvimento de softwares. Além de excelente documentação, contém um IDE – Integrated Development Environment, próprio para a sua linguagem/kit, o QT Creator. Esta framework contém três linguagens de programação, entre as quais o programador, escolherá a que lhe seja mais adequada para o projeto. As três linguagens que podem ser utilizadas em conjunto, são C++, QML e JS (JavaScript), em que a linguagem QML, é proprietária da empresa QT Company, isto é, apenas funciona nesta framework, visto que está interligada com a linguagem C++. O bom desta framework, reside no facto de se conseguir conjugar capacidades de desenvolvimento de linguagens de baixo nível C/C++, com linguagens de alto nível, QML e JS, assim como outro tipo de manipulação de ficheiros, e que dá a possibilidade de interligar as três num só projeto, sem que haja qualquer perda de performance. Uma das razões, de se ter escolhido esta linguagem, deve-se ao facto do simulador ser programado também em linguagem C/C++, o que facilita a sua integração. Esta framework contém duas versões, uma paga e outra gratuita, em que a última versão é open source (código aberto), baseada em licença LGPL v3, que é a versão que foi utilizada neste projeto [63] [64] [65].

O ArcGIS, é posteriormente instalado em conjunto com o QT Creator, estando descrito por completo pelos manuais do ArcGIS, descritos em [66].

Dado as partes reunidas, será apresentado o protótipo de um sistema autónomo de proteção contra UAVs, com foque em não permitir a entrada dos mesmos em espaço aéreo não autorizado.

4.2. Visão geral do Sistema

4.2.1. Desenho do sistema

O sistema, foi desenvolvido através do QT Creator, em linguagens QML/JS e C++, onde a parte gráfica do sistema é desenvolvida em QML, em conjunto com as funções do ArcGIS em JS, e a parte de resolução e manipulação de ficheiros e dados está desenvolvida em C++.

Na aplicação, é demonstrada uma interface com o mapa completo de Portugal, mapa este que é colocado numa diretoria local no computador, e que é acedido com o decorrer da aplicação, quando a sua execução é ativada. O mapa é um ficheiro .mmpk – mobile map package, que é descarregado do website da Esri, sendo apenas acedido com a conta desenvolvedor anteriormente criada. A razão da sua utilização deve-se ao facto de evitar a obrigatoriedade de constante acesso à internet, visto que os ficheiros estão guardados localmente. Este ficheiro .mmpk, funciona como uma base de dados, neste caso do mapa completo de Portugal continental, as ilhas dos Açores e Madeira, assim como o espaço marítimo português. Contém também o mapa, endereços de geolocalização, assim como coordenadas geoespaciais, entre outras informações relativas a mapas. Este ficheiro ocupa 1,4 GB de espaço, sendo um ficheiro bastante completo e algo volumoso [67].

Na interface gráfica é possível ver três tipos de interação possíveis para com o utilizador (figura 18): do lado superior esquerdo, uma pequena janela com informações onde o utilizador pode definir os valores do tamanho da área que quer, assim como o tamanho do radar (visto que o radar, poderá ser anexado no futuro); do lado direito, uma aba que pode ser comprimida ou expandida para uma melhor visualização do mapa, em que serve para fornecer informações e simular aspetos que serão discutidos mais à frente; no canto inferior esquerdo, uma interface de auxílio das coordenadas do local, onde são demonstrados os vários tipos de formato das mesmas, que são apresentadas ao utilizador quando este clica no mapa, além de ser colocada uma pequena cruz vermelha em cima do local escolhido. A aplicação também mostra a atual coordenada desse mesmo ponto, quando introduzidas manualmente na caixa de texto (se estiverem com os formatos corretos). São apresentados quatro tipos diferentes de formatos de coordenadas: a latitude e longitude; graus decimais; graus decimais e minutos; e graus, minutos e segundos, por esta ordem respetivamente.

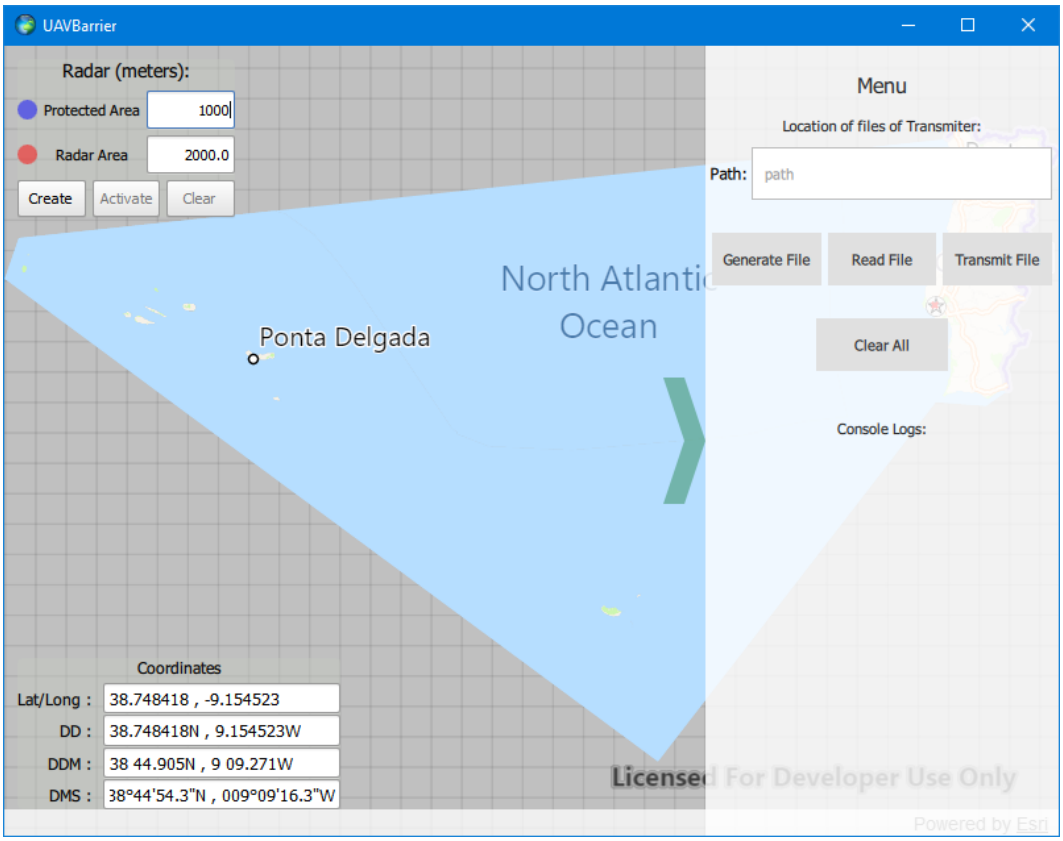


Figura 18-Apresentação da interface de utilizador do sistema implantado

A secção das coordenadas, que está localizada no canto inferior esquerdo, é executada através do CoordinateFormatter, que é uma função disponível no SDK ArcGIS, a qual é executada em QML. Deste modo consegue-se traduzir os pontos clicados no ficheiro .mmpk, que são mostrados na interface, para valores legíveis, neste caso Strings [68]. Esta parte da interface só serve de auxílio à visualização do local no mapa, não tendo qualquer influência no sistema de spoofing.

O funcionamento global do sistema começa com a interação do utilizador, e está descrito no fluxograma da figura 19, em que irá ser explicado cada detalhe do seu funcionamento, assim como os desafios que foram cruciais, de modo a superar problemas e possíveis falhas. A primeira elipse consiste na iteração do utilizador com a interface gráfica, e os quadrados a rosa indicam o resultado das ações do programa. Os losangos a verde designam os algoritmos que operam por detrás do software.

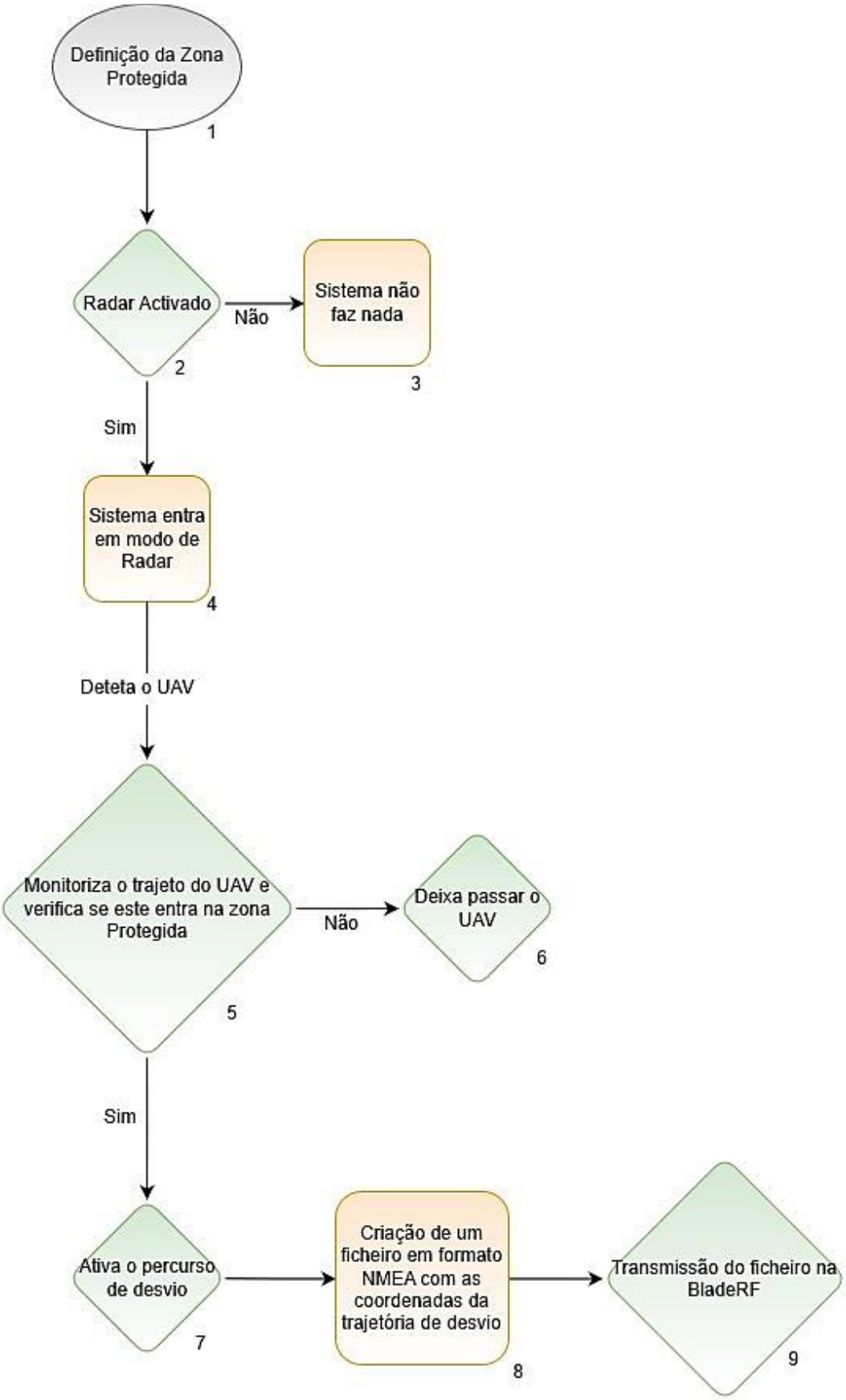


Figura 19-Fluxograma do sistema implementado

4.2.2. Definição da zona protegida

Para dar início ao programa, o utilizador necessita de definir a zona protegida (bloco 1 do fluxograma), para isso é necessário determinar através da introdução dos valores nas caixas de texto da aplicação, o tamanho da área que o radar ocupa e o tamanho da zona a proteger, figura 20. O programa, aceita os valores se estiverem definidos entre 1 até a 10000, em metros, parâmetros estes que podem ser mudados através das variáveis do código. Após serem introduzidos os valores, o utilizador terá seguidamente que clicar no botão "Create" e dirigir-se ao mapa, onde clica uma vez com o ponteiro do rato, e a aplicação recria no mapa os círculos com o raio dos valores anteriormente introduzidos (figura 20).

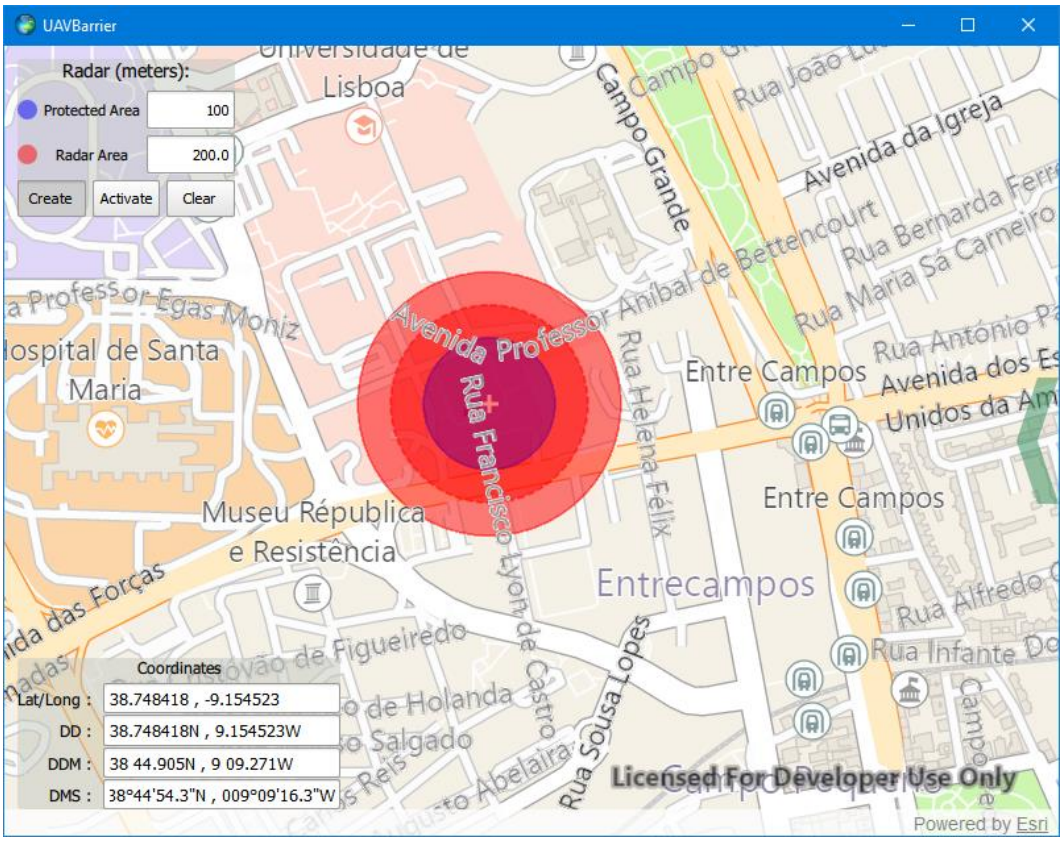


Figura 20-Apresentação da zona protegida e o alcance do radar

Dando o exemplo do ISCTE, coloca-se um raio de 100 e de 200 metros na zona a proteger e no radar, respetivamente, que é centrado no pátio do ISCTE. No entanto é possível verificar que existe uma terceira circunferência, onde este é o ponto de atuação no software (que neste caso está visível para efeitos de demonstração). As cores das circunferências ficam avermelhadas devido às somas RGB dos pixels, uma vez que o

programa desenha três circunferências sobrepostas. O círculo a roxo é designado por zona protegida, como está na legenda no campo superior esquerdo, e as zonas avermelhadas são a área do radar (a circunferência vermelha maior), e a zona de atuação (a circunferência vermelha menor). Os círculos são criados através da função bufferGeodetic da classe GeometryEgine da API do ArcGIS, em que, após estar concluída a criação de cada instância é posteriormente enviada para o GraphicOverlay da aplicação, em que este delineia no mapa [69]. São criadas três instâncias de bufferGeodetic, de forma a perfazer os três círculos definidos pelos valores introduzidos na interface. A razão por apenas estar à vista dois parâmetros, deve-se ao facto círculo intermédio (o círculo do meio, com mais cor a vermelho), ser uma peça intermediária, isto é, ele situa-se a meio da distância entre os restantes círculos. Este círculo intermediário, serve como ponto de atuação caso o UAV transponha essa distância, de modo a impedir que o UAV toque na zona protegida (a zona roxa), prevenindo sempre que este entre sequer para a mesma zona.

4.2.3. Ativação do Radar

Seguidamente após definir a zona a proteger, o sistema necessita da ação do utilizador para prosseguir para o segundo passo, quer dizer, se o mesmo não clicar no botão “Ativar” que fica disponível assim que a área é criada, a aplicação limita-se apenas a traçar na interface a localização do UAV (se assim o utilizador desejar) e não ativa as contramedidas. Dado esse pormenor, se o utilizador prosseguir com a ativação, o software transita para um novo estado, estado esse que fica ativo e à espera que detete algo.

Contudo, apesar de não existir no momento da escrita desta dissertação, algum tipo de hardware que faça de radar, o software está desenhado para ser acoplado a um módulo externo de deteção e seguimento de alvos.

Para se calcular as distâncias entre pontos cartesianos relativos ao UAV e ao ponto central, presume-se a utilização do Teorema de Pitágoras, no entanto, quando se lida com coordenadas geográficas, o mesmo teorema terá de ser complementado com novas fórmulas matemáticas trigonométricas. A razão, deve-se ao facto de as fórmulas com coordenadas geográficas conterem a relação da forma geométrica do planeta Terra, o que com o simples teorema de Pitágoras, tornava-se difícil calcular as verdadeiras

distâncias, porque a superfície terrestre não é plana [70]. Existem vários modelos que tentam aproximar a verdadeira forma geográfica da Terra, sendo os dois mais conhecidos: a esfera perfeita, ou mais conhecida como "Great-Circle"; e o elipsoide, forma esta, que é a que tenta ser a mais aproximada da forma real, figura 21. Este tipo de cálculos e previsões de distâncias, são bem conhecidos nas áreas de aeroespacial, marítima e navegação, visto que sua utilização é uma constante para planear as rotas [71].

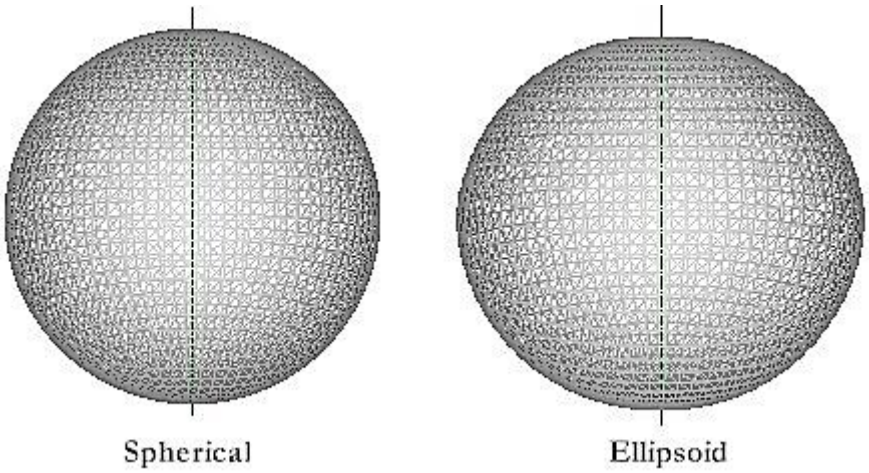


Figura 21-Comparação dos modelos utilizados, Fonte: [71][10]

O modelo da esfera perfeita, utiliza dois tipos de fórmulas, a de "Haversine" e da "Spherical law of cosines". Estas fórmulas, variam na sua precisão e dependem bastante do tipo de processamento em que são inseridas. Por exemplo, a fórmula de Haversine é a mais conhecida, mas tende a ter menos precisão, e requer menos poder de processamento do que de Spherical law of cosines. Entretanto a de Spherical law of cosines, tende a ser mais precisa para pequenas distâncias. Ambos os modelos utilizam o planeta Terra como uma esfera perfeita [72], [73]. Na figura 22, é possível observar as equações de cada um dos teoremas, em que se denota, que o segundo teorema apesar de mais curto é bem mais complexo.

[10] Imagem retirada do site: https://www.codeguru.com/cpp/cpp/algorithms/article.php/c5115/Geographic-Distance-and-Azimute-Calculations.htm

Haversine formula:

$$a = \sin^2(\Delta\varphi/2) + \cos\varphi_1 \cdot \cos\varphi_2 \cdot \sin^2(\Delta\lambda/2)$$
$$c = 2 \cdot \text{atan2}(\sqrt{a}, \sqrt{(1-a)})$$
$$d = R \cdot c$$

Law of cosines:

$$d = \text{acos}(\sin\varphi_1 \cdot \sin\varphi_2 + \cos\varphi_1 \cdot \cos\varphi_2 \cdot \cos\Delta\lambda) \cdot R$$

where φ is latitude, λ is longitude, R is earth's radius (mean radius = 6,371km); note that angles need to be in radians to pass to trig functions!

Figura 22-Fórmulas para calcular distancia entre coordenadas, Fonte: [72][11]

Em relação ao outro modelo, o do elipsoide, são utilizadas as fórmulas de "Vincenty", que é um modelo mais aproximado à escala real [74]. Relativamente a este modelo, é preciso ter a noção que a superfície terrestre não é sempre igual, ao qual dá-se o nome de geoide, como é possível ver na figura 23, o que torna difícil calcular as verdadeiras distâncias à superfície. Este modelo contém alguns parâmetros para suavizar este desafio, sendo utilizado o nível médio de alturas, como se vê a tracejado na mesma figura, em que consiste numa aproximação média relativamente ao nível do mar e terrestre. [75]

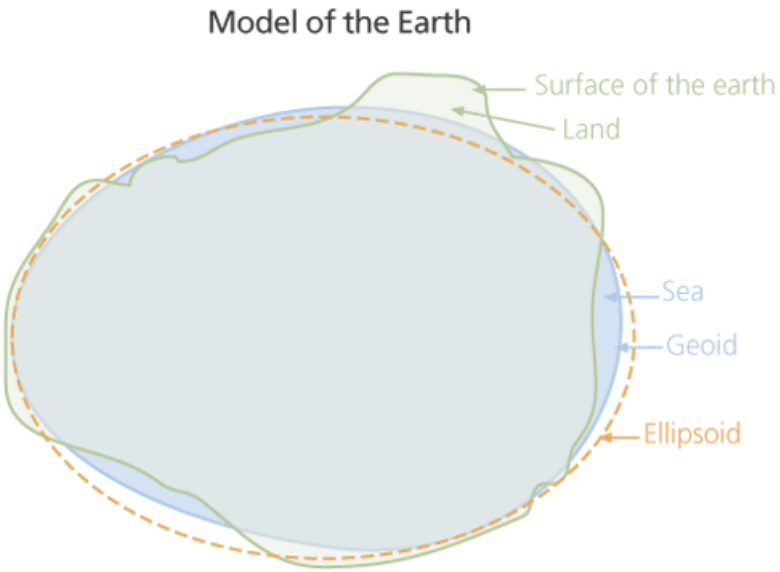


Figura 23-Apresentação do Modelo elipsoide, Fonte: [76][12]

[11] Imagem retirada do site: https://www.movable-type.co.uk/scripts/latlong.html
[12] Imagem retirada do site: http://www.esri.com/news/arcuser/0703/graphics/geoid1_lg.gif

As fórmulas de Vincenty, têm como base o elipsoide terrestre, e tentam solucionar os aspetos referidos anteriormente, o que proporciona a que a nível computacional se obtenha uma precisão, de apenas meio milímetro de erro, o que é espantoso, se considerarmos a dimensão do planeta Terra. No entanto, a nível de processamento, estas fórmulas, requerem bastante poder computacional o que pode levar algum tempo a ser executado. Devido à extensão e ao grande número de equações decidiu-se não se descrever as fórmulas. No entanto, podem ser acedidas a partir de [77] [74]. Na figura 24, observa-se a diferença entre os dois modelos, a tracejado o modelo esférico e a contínua o modelo elíptico, contudo não estão a escala real.

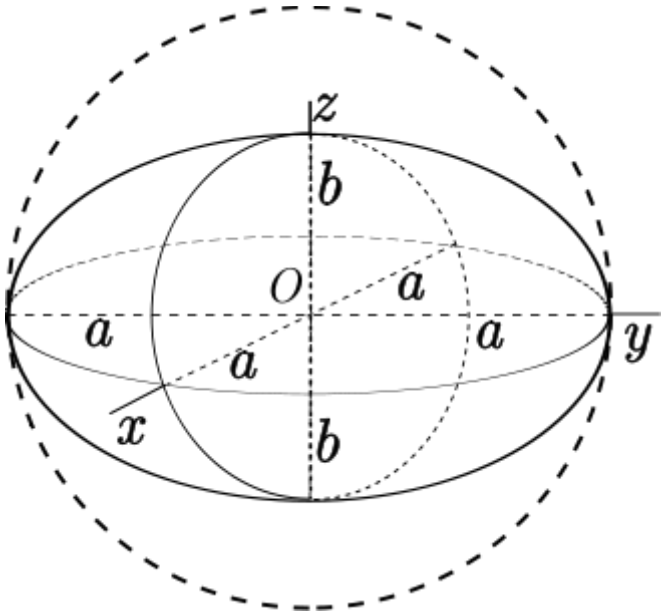


Figura 24-Comparação dos dois modelos da forma terrestre, a tracejado o modelo da forma esférica e a linha continua o do elipsoide, Fonte: [77][13]

Após apresentada a explicação teórica, utiliza-se este conhecimento para determinar as distâncias, entre as coordenadas do UAV e as coordenadas do centro da circunferência. Deste modo, consegue-se verificar se o objeto intruso entra nas áreas pretendidas. Entretanto para se calcular e verificar a distância entre estes dois objetos utiliza-se a função distanceGeodetic, a qual auxilia o cálculo das distâncias, já que, disponibiliza os vários modelos anteriormente referidos. Um dos modelos a utilizar na função é o modelo geodético (GeodeticCurveTypeShapePreserving), que neste caso é utilizado um dos modelos mais aproximado à forma terrestre, de modo a tornar os

[13] Imagem retirada do site: https://community.esri.com/servlet/JiveServlet/showImage/38-57578-376484/327px-Ellipsoid_revolution_oblate_aab_auxiliary_sphere.png

resultados mais realistas. Este modelo rege-se pela norma WGS-84, em que esta norma utiliza como base o modelo das fórmulas de Vincenty. A função além de calcular a distância, calcula também o ângulo das coordenadas (azimute), em que este último será discutido nas secções mais à frente. A razão de não terem sido utilizadas as equações manualmente no programa final, deve-se ao facto de se querer criar uma forma coerente na utilização do SDK, visto que, além das funções e do mapa serem objetos específicos da empresa, achou-se melhor utilizar as próprias ferramentas que a mesma oferece, tornando as operações mais eficientes. Mesmo assim ainda, chegou-se a testar as equações manuais, devidamente programadas, com as funções do SDK, e de facto, após algumas comparações, notou-se que existia uma pequena melhoria de precisão comparativamente à escrita manual. Apesar de ser uma diferença de milésimas, não faria qualquer diferença a sua utilização na aplicação, porque evidentemente que, para cálculos com distâncias de apenas alguns quilómetros ou metros, era irrelevante utilizar qualquer umas das fórmulas.

Voltando ao exemplo do ISCTE, com estas informações, é possível utilizá-las para comparar as distâncias entre o centro da circunferência (ponto central), e a da ocorrência do UAV. Portanto, quando um UAV, tem a sua distância ao ponto central menor que 200 metros, a aplicação transita para o estado seguinte, a monitorização, que é relatada e explicada na secção seguinte. Qualquer outro objeto que esteja localizado a mais que 200 metros, o software deixa de o monitorizar, visto que não é considerado perigo.

4.2.4. Monitorização e verificação da trajetória do UAV

Após ser detetado algum objeto, neste caso um UAV, a aplicação entra no modo de monitorização, como se referiu na secção anterior, o que significa que o UAV situa-se entre o ponto de atuação e o início do radar. Como se pode ver na figura 25, o software tem agora a capacidade de calcular as distâncias entre objetos. Neste exemplo vê-se a distância calculada pelo software do ponto de atuação, onde este começará a agir caso o UAV transponha esta área.

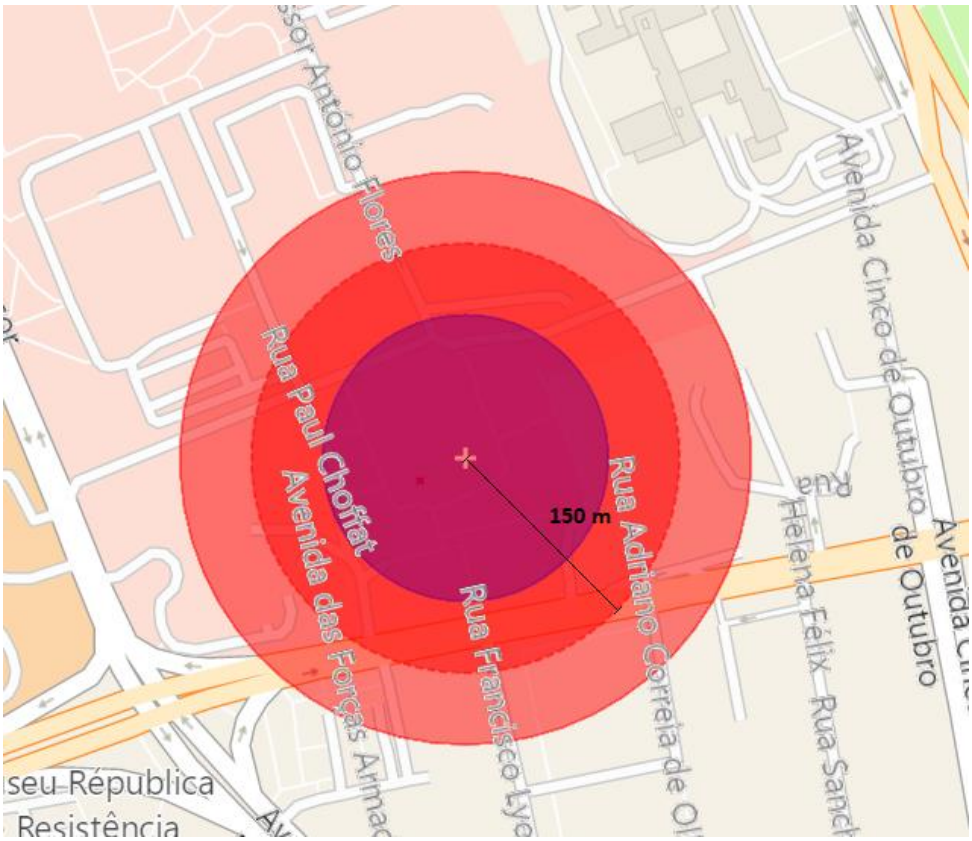


Figura 25-Cálculo da distância de atuação

No software, são desenhadas, virtualmente, retas que perfazem o caminho direto do UAV para posteriormente serem analisadas no ciclo seguinte. Para se ser capaz de estimar a direção do UAV, através das retas, é necessário implementar um algoritmo apropriado para tal. Como inicialmente, não se obtém dois pontos desde a primeira ocorrência de avistamento do UAV, a aplicação necessita de esperar pela segunda, como se pode ver na figura 26. Só a partir dessa ocorrência, é possível traçar uma reta tentando-se prever a trajetória futura.

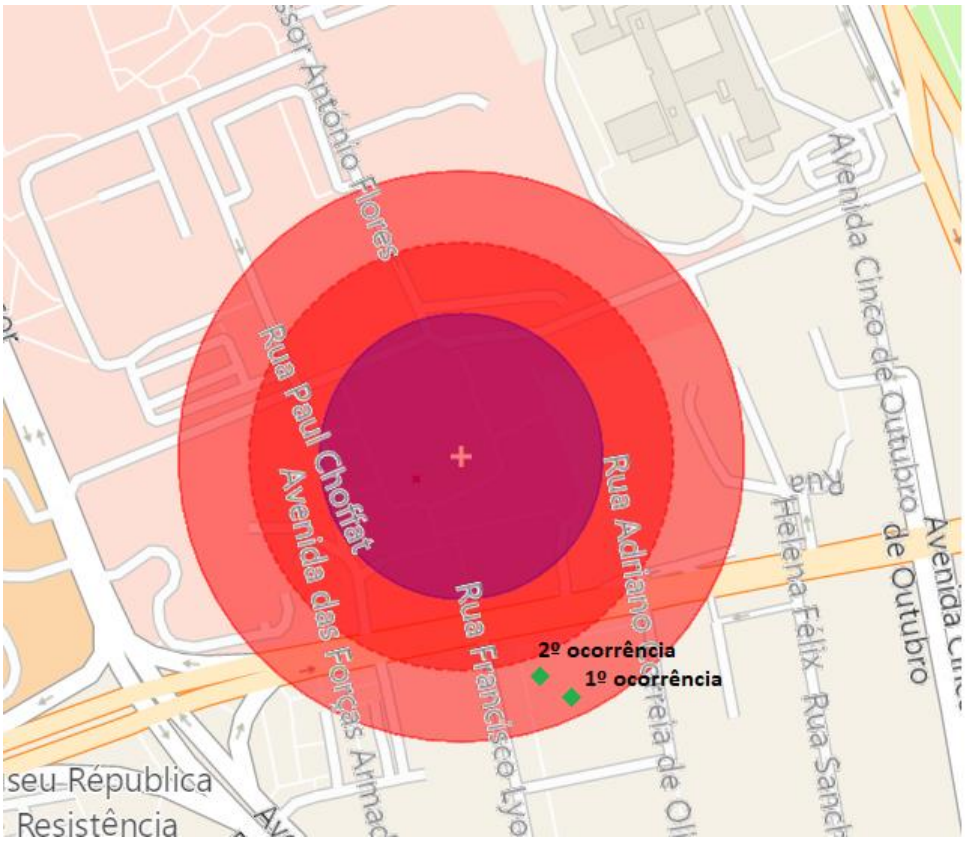


Figura 26-Primeiras ocorrências de UAVs

O modo como o programa calcula a trajetória, é através do azimute, que consiste no ângulo com referência ao polo Norte terrestre e ao polo Sul [78]. Na figura 27 é possível ver como é que os ângulos são calculados, no entanto é preciso salientar que esta imagem é apenas de demonstração e explicação, e não é referente ao exemplo iniciado.

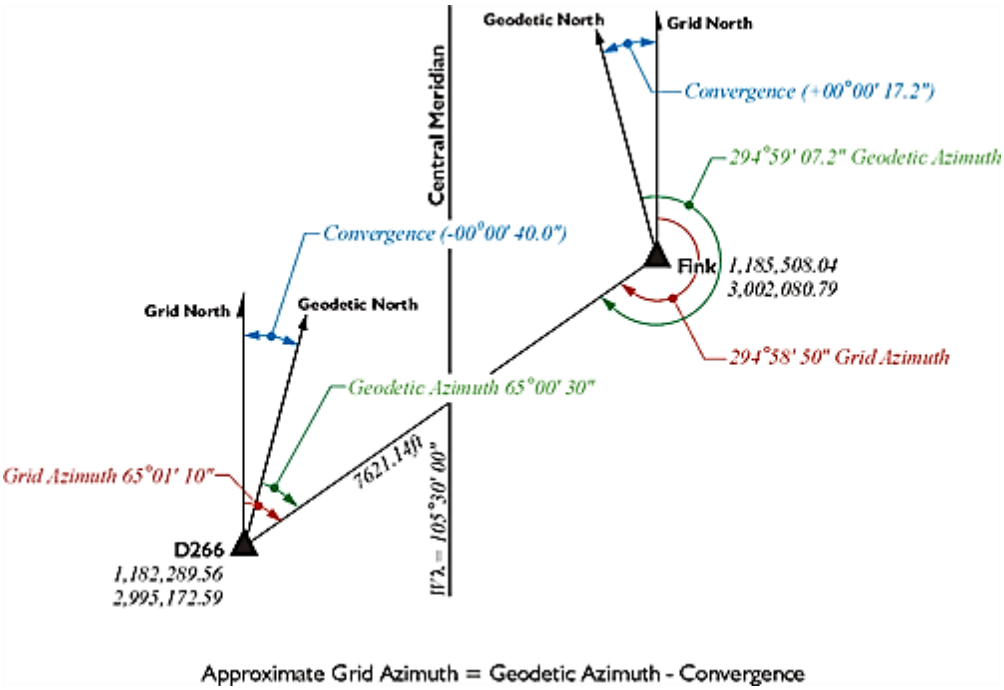


Figura 27-Demonstração e explicação do cálculo do ângulo entre dois pontos, Fonte: [79][14]

É de salientar que o azimute, também tem influência, relativamente à forma terrestre. Isto é, como se pôde observar na figura 27, o ângulo de cada um dos dois pontos, não é igual, isso deve-se ao formato do elipsoide que perfaz a curvatura terrestre. Portanto o azimute dos pontos calculados, terão sempre diferentes resultados, mesmo que sejam em valores de casas infinitesimais. Por isso só o cálculo do azimute de cada ponto não será o suficiente, para superar os desafios. No entanto as fórmulas referidas na secção 4.2.3., também podem ser utilizadas de modo a conseguir-se calcular os ângulos (azimutes) das retas entre os pontos, com base na distância, ou vice-versa, não sendo necessário o cálculo apenas nas coordenadas. Para ser exequível é preciso modificar as equações. Como se pode ver na figura 28, a primeira equação, é utilizada para calcular a distância, com base no azimute das duas coordenadas e a segunda para calcular o ângulo (azimute) com base na distância entre os dois pontos.

[14] Imagem retirada do site: https://www.e-education.psu.edu/geog862/book/export/html/1644

Formula: $\varphi_2 = \text{asin}(\sin\varphi_1 \cdot \cos\delta + \cos\varphi_1 \cdot \sin\delta \cdot \cos\theta)$

$\lambda_2 = \lambda_1 + \text{atan2}(\sin\theta \cdot \sin\delta \cdot \cos\varphi_1, \cos\delta - \sin\varphi_1 \cdot \sin\varphi_2)$

where φ is latitude, λ is longitude, θ is the bearing (clockwise from north), δ is the angular distance d/R*; d being the distance travelled,* R *the earth's radius*

Formula: $\theta = \text{atan2}(\sin\Delta\lambda \cdot \cos\varphi_2 , \cos\varphi_1 \cdot \sin\varphi_2 - \sin\varphi_1 \cdot \cos\varphi_2 \cdot \cos\Delta\lambda)$

where φ_1,λ_1 *is the start point,* φ_2,λ_2 *the end point (*$\Delta\lambda$ *is the difference in longitude)*

Figura 28-Fórmulas para calcular o azimute, Fonte: [72][15]

Mais uma vez por questões de dimensão, as fórmulas de Vincenty, para calcular o azimute estão descritas em [74], sendo utilizadas da mesma forma que as descritas anteriormente. Esta situação é idêntica à das distâncias, ou seja, utiliza-se a mesma função que consegue calcular tanto as distâncias como os azimutes.

Retomando o exemplo inicial, é calculado o azimute das retas traçadas entre a primeira e a segunda ocorrência, de modo a conseguir calcular o ângulo da reta desejada. Posteriormente é utilizado o mesmo ângulo para traçar, uma nova reta, com a mesma distância e ângulo que a primeira. Observe-se na figura 29, as retas traçadas, a azul entre os pontos reais das ocorrências, e a reta branca a da ocorrência simulada, onde se pode apurar que a trajetória do UAV, tem como direção a entrada na zona de atuação.

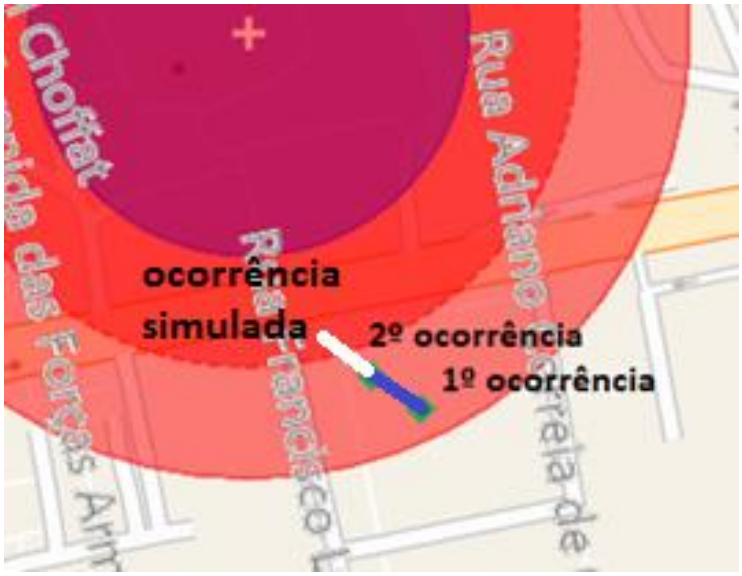


Figura 29-Ampliação do exemplo inicial, e demonstração do cálculo da direção do UAV intruso

[15] Imagem retirada do site: https://www.movable-type.co.uk/scripts/latlong.html

Este ponto final da reta branca, simula uma ocorrência de UAV futuro que é calculado através da função descrita anteriormente, onde se torna possível verificar a trajetória futura do objeto em questão. Portanto, se a ocorrência simulada for menos do que os 150 metros, continuando o exemplo iniciado, o algoritmo ativa o próximo estado. Caso não encontre nenhuma futura ocorrência que indicie que vá para o interior da zona de atuação (menos do que 150 metros), o sistema deixa passar o UAV, p. e., passar pelo radar, mas com direção oposta.

4.2.5. Ativação do percurso de desvio

Dada a deteção na área intermédia, o programa terá que atuar, visto que neste caso dirige-se na direção da zona protegida. A partir deste ponto existem dois tipos de algoritmos, que são utilizados sequencialmente. Primeiramente, é necessário decidir para qual dos lados é que UAV se tem de dirigir, isto é, se é necessário ir para a esquerda da zona protegida ou vice-versa. Isto é crucial para posteriormente realizar-se o spoofing, visto que para se executar esta técnica é essencial ter em conta o movimento do UAV. Seguidamente terá de ser criado o percurso alternativo com base nessa direção.

Continuando a explicação do algoritmo, são executadas várias medições dos ângulos das novas retas, figura 30. Nesta nova situação são necessárias efetuar novas medições de ângulos das retas a amarelo (figura 30) de modo a conseguir-se calcular qual a direção que o UAV deverá ser direcionado.

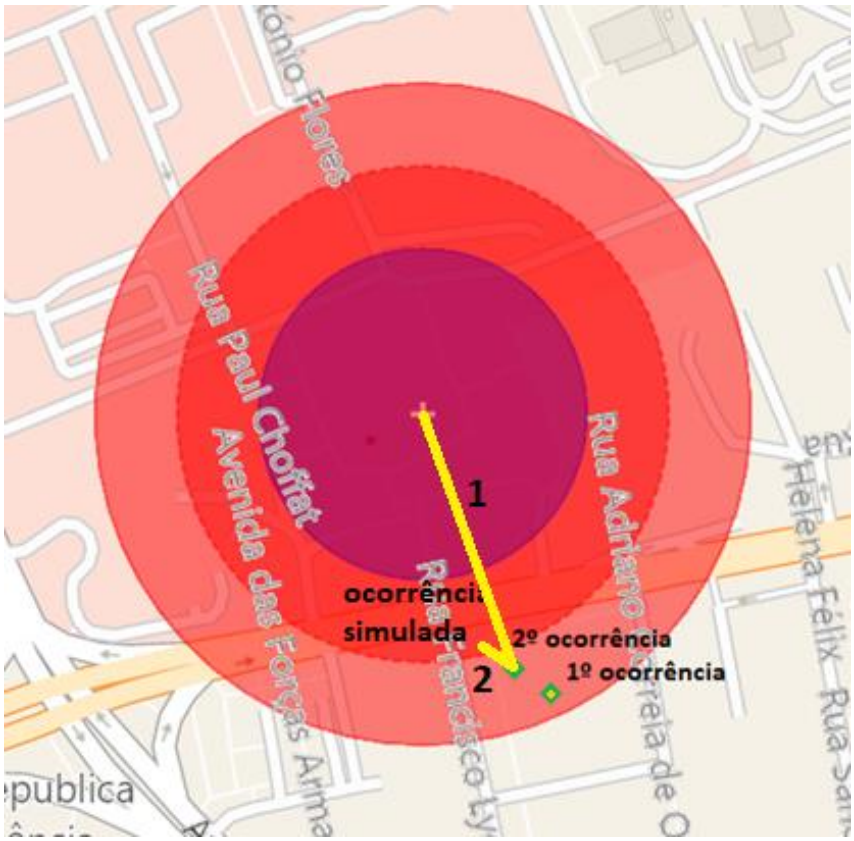


Figura 30-Exemplificação do cálculo da direção do UAV

Como se pôde ver na figura 30, as novas linhas a amarelo são as linhas virtuais que são traçadas pelo programa para determinar o ângulo da direção desejada. Neste caso para nós humanos, é fácil de verificar que, para mudar a trajetória na mesma figura, consiste em desviá-lo para a esquerda. Para isso é preciso um algoritmo que consiga distinguir as direções corretas e verificar se o UAV consiste numa ameaça ou não, para as zonas seguras. O algoritmo desenvolvido, consiste no cálculo dos azimutes das linhas amarelas e verificar qual deles é o maior. Se a primeira reta tiver um maior azimute do que a segunda reta, este terá de ir para direita, caso contrário irá para a esquerda. Veja-se que a direção de referência do azimute é o polo Norte, cujo valor fica nos 0º, enquanto o polo Sul fica nos 180º. Por exemplo, assumindo que os 0º ficam direcionados para a parte de cima da figura 30 e que os 180º na parte inferior da mesma figura, observa-se que ambas as retas estão sensivelmente inclinadas para a esquerda em relação à parte superior. Logo os valores das retas terão que ser ambos negativos, porque, ao estarem desviadas para o lado esquerdo, o valor do angulo é inferior a 0º. A primeira reta tem um valor de -20º sensivelmente, e a segunda reta tem um valor de -35º, portanto com o algoritmo apresentado conclui-se que o UAV terá que ir para a

esquerda, e está correto, porque o azimute da reta um é maior que o da reta dois (-20 > -35). O algoritmo existente parece funcionar independentemente da direção, no entanto existem algumas situações problemáticas que requerem modificações. Para todas as direções que envolvam ângulos desde -179º até a 179º, este algoritmo consegue executar sem problemas, mas, para outro tipo de ângulos diferentes, dará erro. A razão deve-se ao facto da transição dos 180 positivos para os 180 negativos. Observe-se o seguinte exemplo na figura 31, idealizando outra situação com a possível falha.

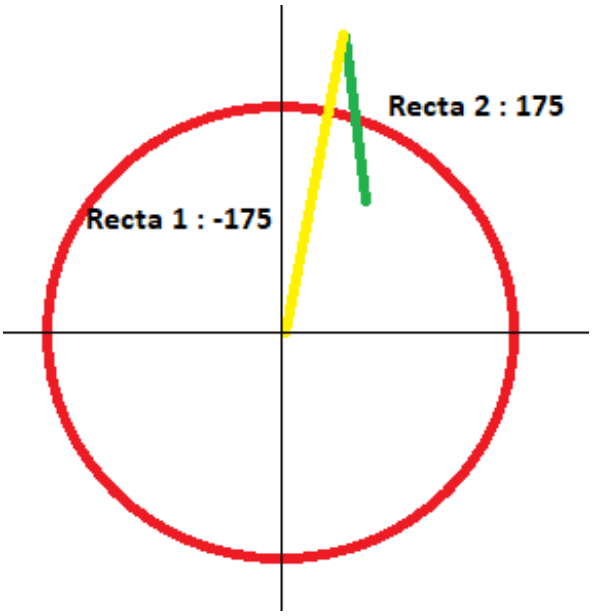


Figura 31-Exemplificação de caso especial que provoque falhas no algoritmo e na mudança de direção

Como se pode verificar, uma reta contém um número negativo e outro positivo. A reta verde seria o percurso do UAV e a reta amarela, a da posição do UAV até ao centro da circunferência. O algoritmo anteriormente mencionado funcionaria da seguinte maneira: como o valor de 175 é maior que o de -175 (175 > -175), o UAV terá que mudar de direção para a direita, o que entra em colapso com o trajeto correto, como se observa na figura 32.

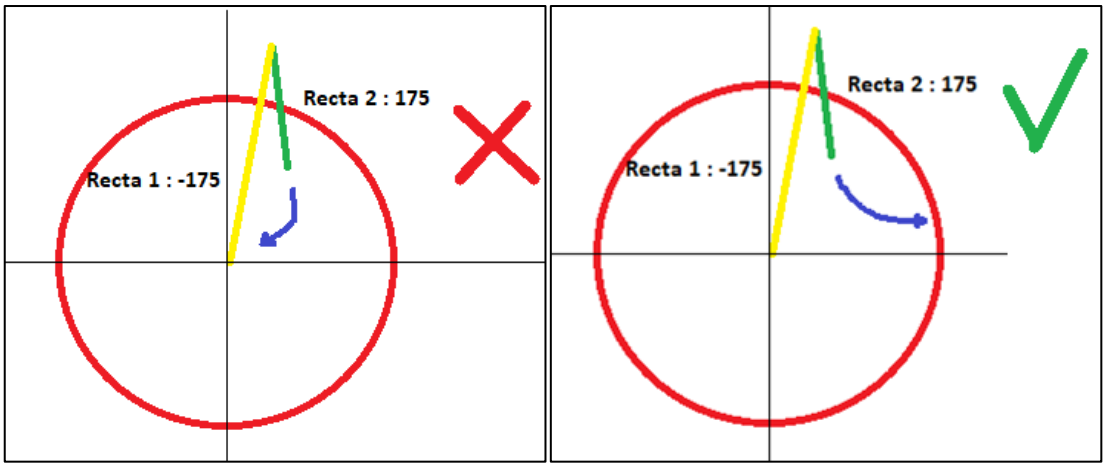


Figura 32-Demonstração de falha no algoritmo da mudança de direção, em que neste caso no lado esquerdo o lado incorreto e do lado direito a direção correta

Como se observa no lado esquerdo da figura 32, segundo o algoritmo sem modificações, o UAV é direcionado para o lado incorreto, quando o correto deveria ser o oposto, como é demonstrado no lado direito da mesma figura, onde o UAV segue para a sua esquerda.

Por isso é que o algoritmo teve que ser modificado, de forma a lidar com estas condições especiais. Denotada esta diferença importante de ângulos, a solução reside na soma ou subtração de 360º, mas apenas a um dos ângulos, solucionando assim o problema. Aplicando a este último exemplo, ter-se-ia que somar mais 360º à reta amarela, perfazendo um total de 185º, obtendo-se assim valores com mesmo sinal. Resolvida a questão testa-se o algoritmo anterior e de facto conclui-se que não existe mais problemas com a direção dos ângulos, a reta amarela é maior do que a reta verde, o que implica que o UAV terá que ir para a esquerda, o que é o pretendido.

Para finalizar, é preciso salientar que, mesmo que se tivesse utilizado uma escala de valores desde 0º até aos 360º e não como se utiliza, dos -180º até aos 180º, o resultado seria idêntico e ter-se-ia exatamente o mesmo problema na transição, como por exemplo o de 356º para 2º.

Continuando o problema inicial do mapa do ISCTE, agora é possível conferir para que lado deve o UAV ser direcionado, neste caso para o lado esquerdo que é para fora da zona roxa (figura 30).

Portanto, agora é preciso delinear, o trajeto, para posteriormente colocar-se no simulador BladeRF, mas este só aceita um ficheiro com o total das coordenadas. Continuando o exemplo inicial da proteção da área do ISCTE, após ser determinada a direção do percurso futuro que o UAV terá de ser desviado, é possível delinear o caminho de desvio, através da utilização das funções anteriores, que é calculado coordenada a coordenada. Para se calcular as coordenadas seguintes é utilizado um certo ângulo e uma distância entre cada uma das coordenadas, que é constante durante todo o percurso, de forma a perfazer uma espécie de semicírculo com a direção desejada. Estes parâmetros podem ser alterados nas variáveis globais do código. Entretanto é necessário salientar outro pormenor importante, que para se calcular o percurso de mudança de direção, é necessário obter-se um ponto máximo para que seja possível calcular o semicírculo, senão o programa começa a entrar em loop infinito. Para prevenir essa situação, adiciona-se um certo valor de graus, quando são conhecidos os ângulos onde estão posicionados o UAV e a próxima coordenada. O método utilizado para exemplificar o que foi descrito, consiste em adicionar ou decrementar, um angulo de 90º, o que limita o ângulo de mudança de direção, como é demonstrado na figura 33.

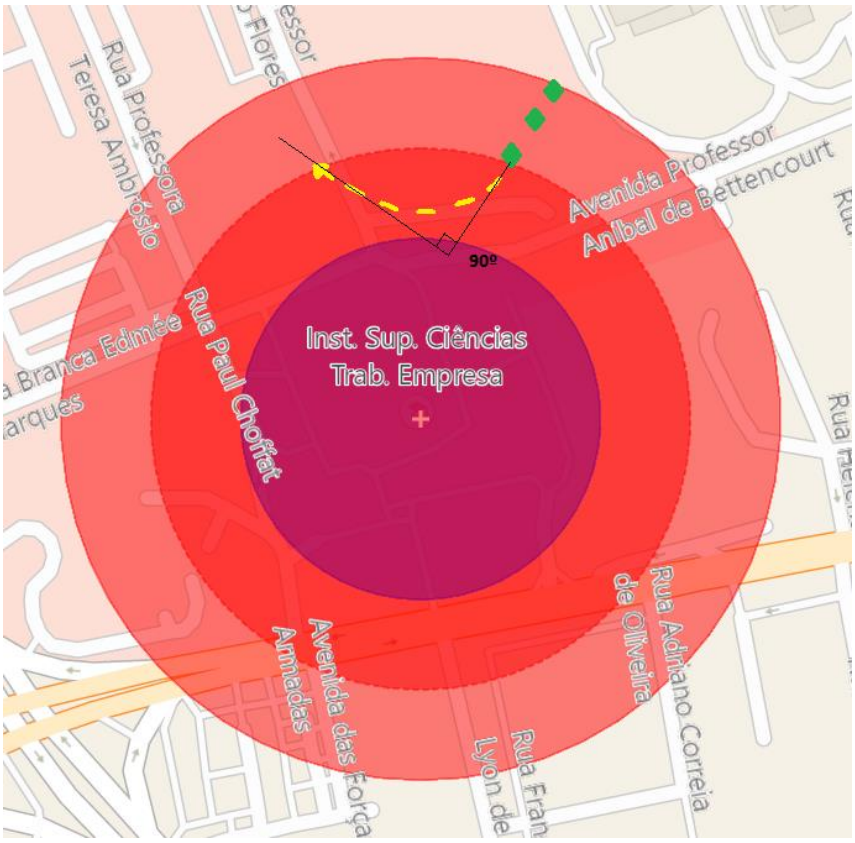


Figura 33-Exemplificação da futura direção recriada para o UAV, com um limite máximo

Para se executar essa tarefa, à medida que são calculadas as coordenadas do percurso alternativo, é sempre verificado se o ângulo em questão da coordenada não transpassa o limite máximo imposto. Caso ultrapasse ou que seja igual, o programa sabe que não necessita de continuar e é parada a iteração, perfazendo assim o percurso alternativo. Para exemplificar, imaginando que a mudança de direção do UAV tenha que ser para o lado direito, como é demonstrado na figura 33, e se obtenha um angulo atual, de -145º, é necessário adicionar um limite máximo de -55º (-145º + 90º), que é visível na seta amarela da mesma figura.

Apesar desse trajeto parecer completo, é necessário criar a sua inversão, visto que para se utilizar o spoofing na direção do UAV, é preciso criar uma espécie U inverso, para que seja possível transmitir essas coordenadas em vez do percurso de desvio. Na figura 34 observa-se essa situação, onde se mostra a amarelo a trajetória desejada e a azul a trajetória a enviar para a BladeRF de forma a fazer spoofing do sinal GPS com sucesso.

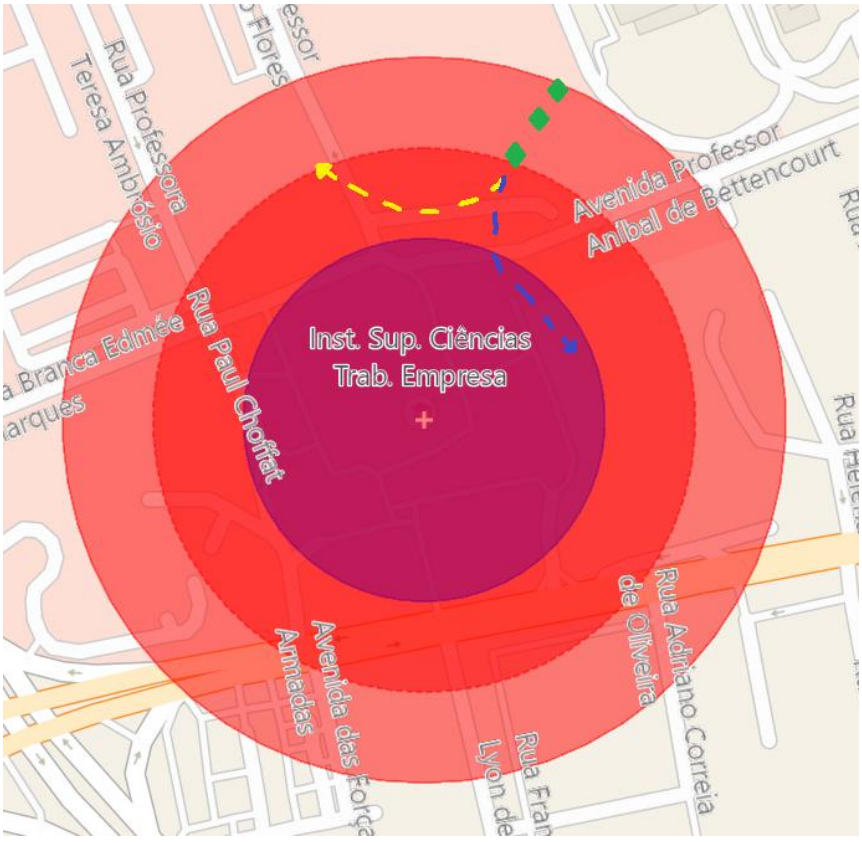


Figura 34-Demonstração das trajetórias, a amarelo o percurso que o UAV terá de ser direcionado e a azul, o percurso a enviar para o simulador

Conhecida a parte algorítmica do programa, falta agora testar tudo o que foi referido anteriormente. Para isso é necessário desenvolver uma parte que simule os efeitos aqui descritos. Essa parte de simulação, é a aba vista inicialmente do lado direito do programa, que serve para simular um percurso de um UAV, assim como guardar os dados dos ficheiros criados, que será explicada seguidamente. Na figura 35, observa-se o programa a executar um percurso aleatório automático, em que a sua execução foi executada com sucesso.

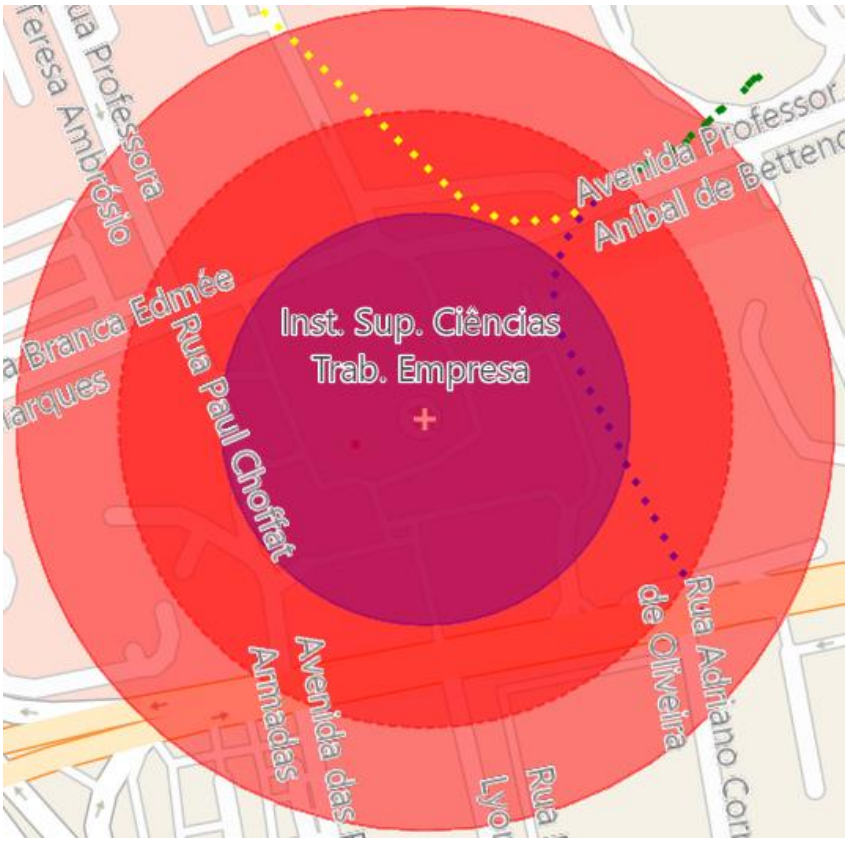


Figura 35-Demonstração do sistema implementado em execução de forma automatizada

Como foi referido no início da secção 4.2. a parte da interface localizada à direita, tem o propósito de criar simulações para que seja possível testar tanto os algoritmos como o funcionamento em conjunto com a plataforma SDR. Para se executar esta simulação, o utilizador, terá de clicar no botão do menu da aba deslizante, em "Generate File", o qual possibilita a criação de um trajeto simulado do UAV, como se pode ver no percurso a verde, na figura 35. Após criado o percurso, é necessário clicar no botão "Transmit File", em que este dá início ao processo de simulação, desde o radar, até à sua deteção e ativação das contramedidas.

4.2.6. Geração do ficheiro NMEA e transmissão

Para finalizar a secção 4.2. falta apenas descrever o envio da trajetória alternativa para a BladeRF. Primeiro necessita-se de transpor os dados em memória para um ficheiro, neste caso em .txt, e escrito em formato NMEA GGA. Por isso a partir daqui, apenas utiliza-se a linguagem C++ para manipular e escrever os ficheiros, e executar o processo do simulador como se irá explicar.

Para transpor os dados utiliza-se o formato que foi explicado, na secção 3.3.2., através da manipulação das Strings, de forma a transformar as coordenadas latitude, longitude, em linhas com a estrutura NMEA GGA, as quais são escritas de forma automática num ficheiro .txt. Depois da conclusão da formatação das coordenadas para formato NMEA GGA, efetua-se o checksum da operação realizada, de forma a tornar os resultados reais, que está descrito em [80].

Após o ficheiro estar concluído o programa executa o simulador, através do início de um processo executado pela linha de comandos do sistema operativo, o qual dá início à transmissão do ficheiro com as coordenadas do percurso alternativo do UAV. Este processo é executado automaticamente pelo programa, através de um QProcess, perfazendo assim a automação completa da aplicação.

4.3. Resultados

Para finalizar o capítulo 4, são apresentados alguns resultados, obtidos através de vários testes realizados ao sistema implementado. Antes de se passar aos resultados, é preciso deixar claro que, para se fazerem testes em UAVs, com este sistema, é necessário realizá-los em locais especiais e ambientes controlados, o que no decorrer desta dissertação não foi possível, devido a não existirem outros componentes do sistema final, nomeadamente as antenas diretivas acopladas diretamente na BladeRF, assim como o respetivo amplificador, e o sistema radar. Com estes entraves em questão optou-se por realizar os testes em dispositivos recetores de GPS, de forma a demonstrar o sistema em pleno funcionamento, porque na realidade os sistemas de receção GPS têm um funcionamento semelhante.

Para começar na figura 36, observa-se a execução da aplicação, de forma automática, em que se verifica através da visualização da consola a negro a execução do simulador, já em fase concluída.

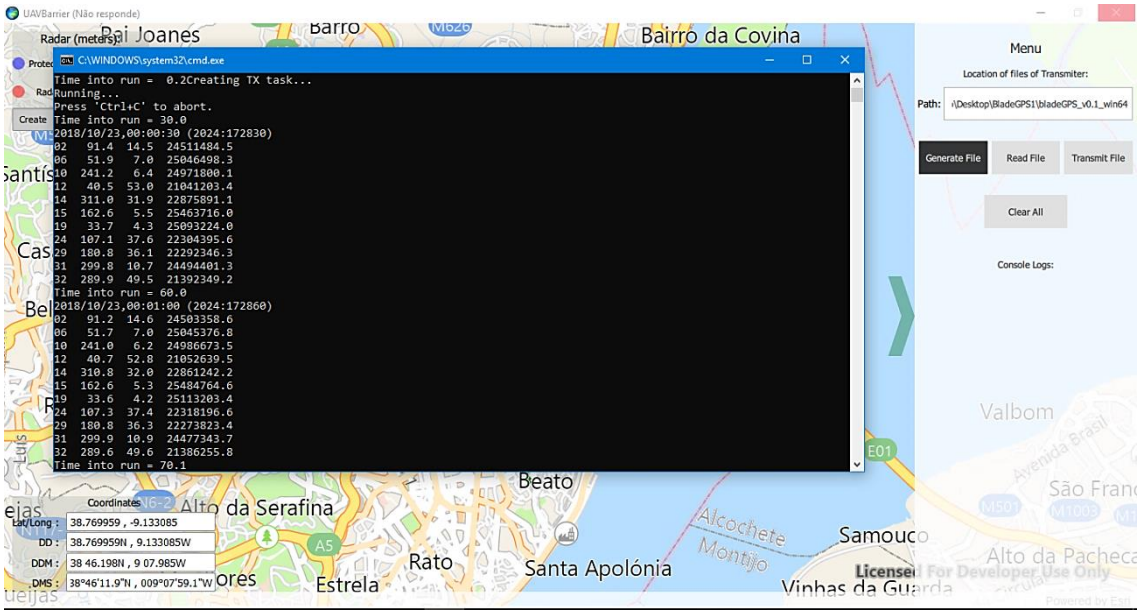


Figura 36-Execução do sistema implementado de forma automatizada

Em termos de recetores, existem dois tipos utilizados: um smartphone, onde se utilizam as aplicações do GPSTest e o google maps, e um recetor de GPS especializado, o u-blox, que consiste num dispositivo próprio para receber sinais de GNSS, sendo utilizado um software especializado, que se denomina por u-center.

Durante a execução do programa, ambos os dispositivos estão a receber a mesma transmissão de forma a tornar os resultados consistentes. Primeiramente apresenta-se a interface u-center na figura 37, onde se exibem os vários módulos das características referentes ao GPS.

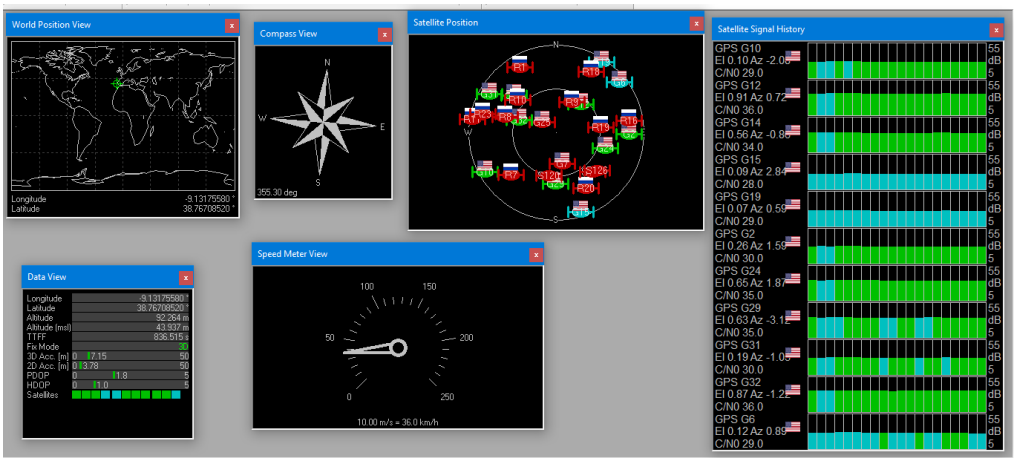


Figura 37-Programa U-blox, onde se visualiza os vários módulos de cada uma das características do GPS

Na figura 38, observa-se de forma ampliada o velocímetro e a bússola do recetor, em que neste caso nota-se que está em movimento, verificando-se que se situa nos 36 km/h.

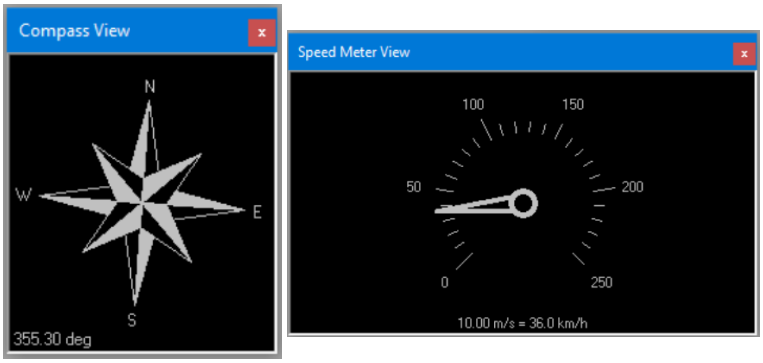


Figura 38-Ampliação dos módulos da figura 37

Na figura 39, verifica-se o mesmo resultado, só com a diferença de se situar noutro dispositivo, neste caso num smartphone. Observe-se que a velocidade acaba por ser quase a mesma, apresentando valores na casa dos 36 e 37 km/h. Os ângulos também apresentam valores bem similares, 355º no u-blox e 352º no smartphone.

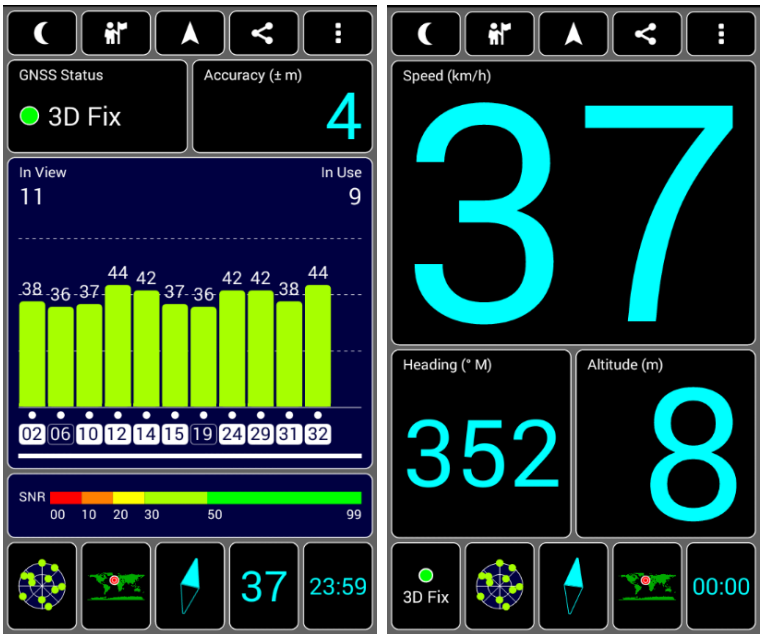


Figura 39-Aplicação GPSTest

Verificaram-se os mesmos dispositivos passados alguns segundos tendo-se constatado que de facto existiu uma mudança na direção em relação à inicial, em que se verifica entre as figuras 38 e 39 com as figuras 40 e 41. Neste caso a velocidade mantém-se praticamente semelhante, mas os ângulos sofreram uma mudança. Entretanto essa mudança é maior no programa do u-blox, devido a ser um objeto estático, enquanto no smartphone existia sempre algum movimento, o que resultou em posições diferentes das iniciais.

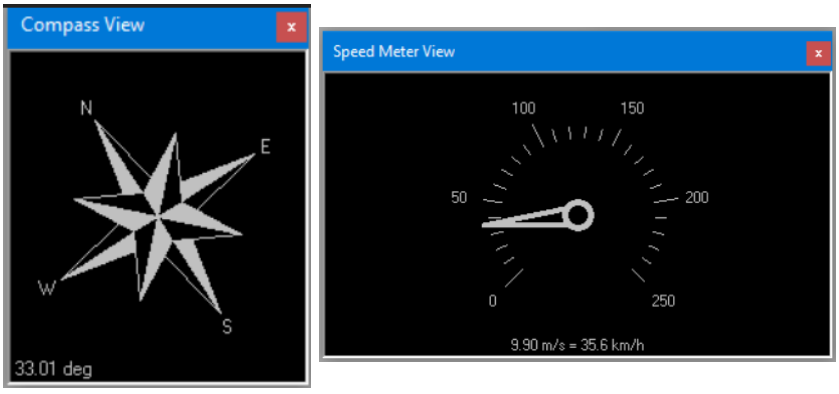


Figura 40-Atualização dos resultados retirados da figura 37

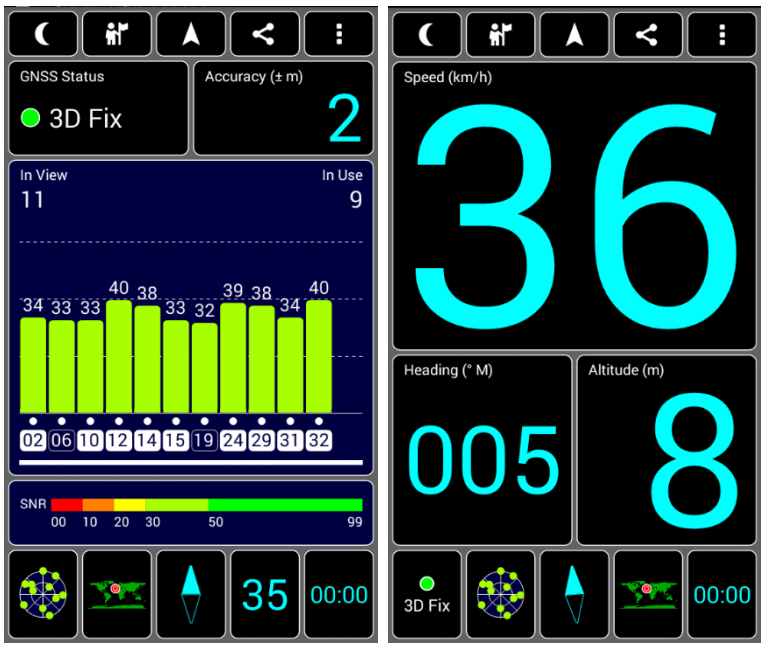


Figura 41-Atualização dos resultados da figura 39

Para finalizar o capítulo 4, apresenta-se o resultado final após a conclusão da transmissão, que é visível na figura 42. Examina-se o resultado descrito a amarelo, que é o pretendido e a roxo o que foi transmitido na bladeRF.

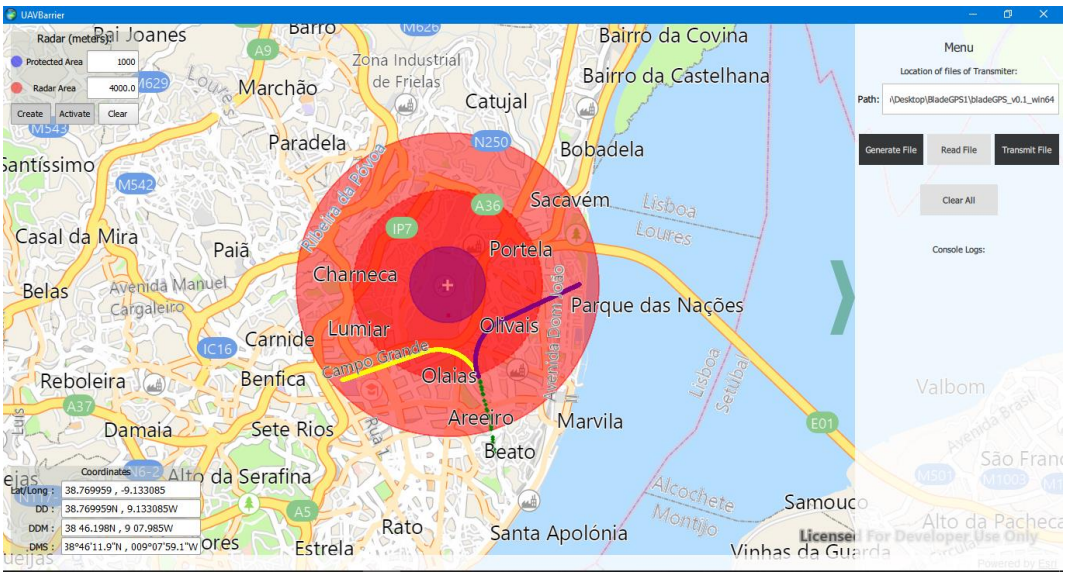


Figura 42-Conclusão da transmissão na aplicação

Na figura 43, observa-se o seguimento de várias imagens que foram captadas ao longo da transmissão, onde se mostra o percurso que supostamente se realizou, mas que na realidade o recetor encontrava-se completamente estático.

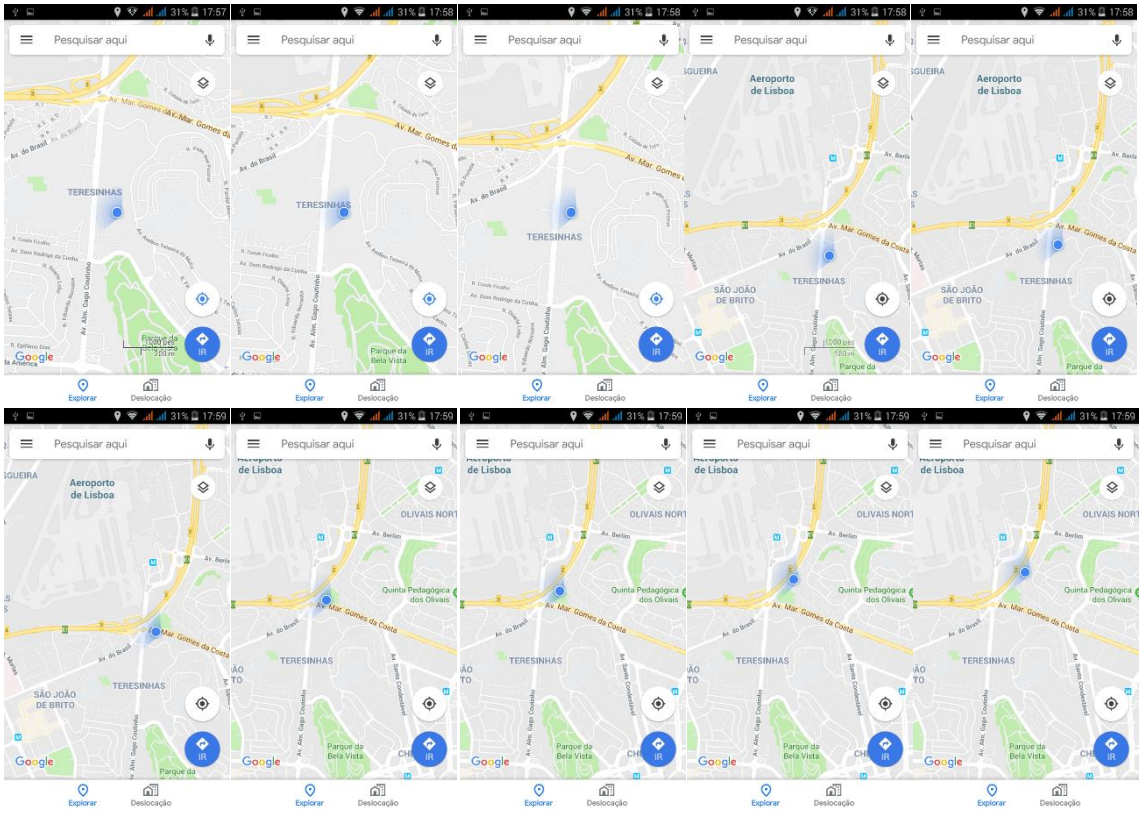


Figura 43-Sequência de imagens de modo a demonstrar-se a localização do smartphone em movimento

Capítulo 5 – Conclusões e Trabalho Futuro

5.1. Principais conclusões

Em relação aos UAVs, e que cada vez mais estão em expansão, aumenta também a sua probabilidade de ataque com estes aparelhos. Consequentemente e crescentemente, os novos aparelhos surgem com capacidades autónomas, o que implica maiores riscos de sofrerem ataques de spoofing. Entretanto mesmo sendo complicado atingir de forma eficaz os UAVs através de spoofing, devido ao facto de existirem bastantes variáveis e parâmetros que são difíceis de modelar, é de salientar, que a probabilidade de os sistemas autónomos sofrerem com esta vulnerabilidade, cresce ainda mais. E devido a isso é necessário criar mais mecanismos de defesa para que se possa evitar estas catástrofes. Por isso é que torna-se necessário, a criação e desenvolvimento de medidas corretas para o combate a este tipo de intrusos e para tal, utiliza-se a contrafação do sinal GPS, para os desviar da trajetória atacante. Para se executar o spoofing, utilizaram-se plataformas SDR, de modo a replicar as ondas rádio do sinal GPS, assim como as suas informações, o que implica a que os recetores adquiram o sinal GPS como sendo fidedigno.

Após a implementação do sistema de zonas de acesso proibido a UAVs, foi possível observar-se que a utilização do simulador de sinal GPS, funcionou bastante bem, em conjunto com a parte desenvolvida. Apesar dos desafios encontrados, e com o desenvolvimento dos algoritmos de manipulação de coordenadas e de trajetórias, foi possível a utilização do spoofing do sinal GPS, de forma a conseguir-se criar percursos alternativos, com intuito de desviar os UAV para fora das áreas protegidas. Contudo e com o funcionamento do sistema, constatou-se que os dipositivos recetores de GPS, adquiriam com facilidade o sinal GPS e demonstravam o suposto andamento de acordo com a trajetória simulada.

Sobre o sistema implementado, apesar da inexistência de um módulo de radar e das antenas diretivas, conseguiu-se provar com sucesso que o sistema consegue enganar e repelir os UAVs intrusos das zonas protegidas. Apesar de os testes terem sido efetuados em ambiente controlado em laboratório, ou seja, baseado em apenas simulações, foi possível observar que quando for acoplado a hardware externo, de modo a criar-se um protótipo funcional, o sistema deverá operar como numa medida de defesa eficaz, visto que a automação de grande parte dos UAVs, pode não estar preparada para sofrer

ataques externos, podendo ser utilizado como arma (caso de ataque de spoofing a um UAV autónomo). Apesar disso, este simulador, não serve para realizar ataques, mas sim incentivar a que sejam criadas mais medidas de segurança de forma a evitar desastres futuros.

5.2. Trabalho futuro

Em relação ao sistema, é preciso referir que existem várias formas de o sistema ser melhorado. A principal, consiste no facto de o sistema na versão atual apenas estar a ser executado com uma thread, o que o limita em termos de processamento e de execução. Como se pôde observar, o programa trabalha só com um método de cada vez, ou seja, quando está a transmitir, não consegue atualizar a interface do utilizador. Com este fator em entrave, é possível melhorá-lo e modificar para que o trabalho ao executar o programa seja divido em mais threads, facilitando assim a sua operação e prevenindo que o mesmo sofra bloqueios.

Além da integração de um sistema de Radar, que seja capaz detetar e monitorizar o trajeto do UAV, é possível adicionar técnicas de jamming de forma a bloquear qualquer tipo de comunicações do aparelho, quer sejam elas de controlo ou de sistemas GNSS. Também é possível automatizar ainda mais o sistema de forma a recriar um mecanismo que detete e atue sem necessitar de supervisão humana. Pode-se também atualizar ou criar melhores algoritmos de forma a ser mais eficiente e mecanismos de bloqueio e monitorização em tempo real de forma a que se consiga ter noção se o objeto intruso foi mesmo repelido. Desta forma obtém-se um sistema de defesa completo e que possa ser colocado em áreas críticas.

Visto que o algoritmo é idêntico para qualquer um dos sistemas GNSS, pode ser expandido para outros sistemas globais, como o GLONASS, ou o GALILEO, assim como BEIDU 2, tornando o sistema, globalmente funcional.

Bibliografia

[1] "Drone, UAV, UAS, RPA or RPAS …," [Online]. Available: https://altigator.com/drone-uav-uas-rpa-or-rpas/. [Acedido em Outubro 2018].

[2] F. Mohammed, A. Idries, N. Mohamed, J. Al-Jaroodi e I. Jawhar, "UAVs for smart cities: Opportunities and challenges," em *2014 International Conference on Unmanned Aircraft Systems (ICUAS)*, Orlando, FL, USA, 2014.

[3] D. Eshel e J. M. Doyle, "UAV Killers Gain Role Against Growing Threat," Aviation Week, 18 November 2015. [Online]. Available: http://aviationweek.com/defense/uav-killers-gain-role-against-growing-threat. [Acedido em Setembro 2017].

[4] "Other Global Navigation Satellite Systems (GNSS)," [Online]. Available: https://www.gps.gov/systems/gnss/. [Acedido em Julho 2018].

[5] "The reference for Global Navigation Satellite Systems.," [Online]. Available: https://gssc.esa.int/navipedia/index.php/Main_Page. [Acedido em Julho 2018].

[6] E. Vattapparamban, İ. Güvenç , A. İ. Yurekli, K. Akkaya e S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," em *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Paphos, Cyprus, 2016.

[7] K. Wang , S. Chen e A. Pan , "Time and position spoofing with open source projects," 2015. [Online]. Available: https://www.blackhat.com/docs/eu-15/materials/eu-15-Kang-Is-Your-Timespace-Safe-Time-And-Position-Spoofing-Opensourcely-wp.pdf. [Acedido em Novembro 2017].

[8] D. Margaria, B. Motella , M. Anghileri , J.-J. Floch , I. Fernandez-Hernandez e M. Paonni , "Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives," *IEEE Signal Processing Magazine*, vol. 34, nº 5, pp. 27-37, 2017.

[9] G. &. E. W. Editorial, "Drone Vs. UAV - What Is The Difference?," [Online]. Available: https://wiki.ezvid.com/m/drone-vs-uav-what-is-the-difference-_2FJYp_SrUkP-. [Acedido em Setembro 2018].

[10] S. . G. Gupta, M. M. Ghonge e P. M. Jawandhiya, "Review of Unmanned Aircraft System (UAS)," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 2, nº 4, pp. 1646-1658, 2013.

[11] K. Hartmann e C. Steup, "The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment," em *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, Tallinn, Estonia , 2013.

[12] B. Vergouw, H. Nagel, G. Bondt e B. Custers, "Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments," em *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives*, Springer, 2016, pp. 21-45.

[13] C. Deng, S. Wang, Z. Huang, Z. Tan e J. Liu, "Unmanned aerial vehicles for power line inspection: A cooperative way in platforms and communications," *Journal of Communications*, vol. 9, nº 9, pp. 687-692, 2014.

[14] A. Figueiredo e F. Santos, "Análise de veículos aéreos não," [Online]. Available: http://www.dei.isep.ipp.pt/~ana/ROBOTICA/docs/UAVs_novo.PDF. [Acedido em Setembro 2018].

[15] "Amazon PrimeAir," [Online]. Available: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011. [Acedido em Outubro 2018].

[16] "The Economics of Drone Delivery," [Online]. Available: https://www.flexport.com/blog/drone-delivery-economics/. [Acedido em Outubro 2018].

[17] "Technical Documentation," Space-Based Positioning, Navigation, and Timing, [Online]. Available: https://www.gps.gov/technical/. [Acedido em Outubro 2018].

[18] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," 18 July 2012. [Online]. Available: https://radionavlab.ae.utexas.edu/images/stories/files/papers/Testimony-Humphreys.pdf. [Acedido em Setembro 2018].

[19] O. J. Joensen, "GPS: Global Positioning System," Niels Bohr Institute - University of Copenhagen, [Online]. Available: http://www.nbi.ku.dk/english/www/spinoff/spinoff/gps/. [Acedido em Outubro 2018].

[20] C. Woodford, "Satellite navigation," 2007/2018. [Online]. Available: https://www.explainthatstuff.com/howgpsworks.html. [Acedido em Setembro 2018].

[21] "Space Segment," [Online]. Available: https://www.gps.gov/systems/gps/space/. [Acedido em Setembro 2018].

[22] T. Nighswander, . B. Ledvina, J. Diamond, . R. Brumley e . D. Brumley, "GPS Software Attacks," em *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12*, Raleigh, North Carolina, USA, 2012.

[23] A. E. SÜZER e H. OKTAL, "PRN Code Correlation in GPS Receiver," em *2017 8th International Conference on Recent Advances in Space Technologies (RAST)*, Istanbul, Turkey, 2017.

[24] "Atmospheric Correction," [Online]. Available: https://www.e-education.psu.edu/geog862/book/export/html/1407. [Acedido em Outubro 2018].

[25] "The Ionospheric Effect," [Online]. Available: https://www.e-education.psu.edu/geog862/book/export/html/1596. [Acedido em Outubro 2018].

[26] "The Satellite Clock," [Online]. Available: https://www.e-education.psu.edu/geog862/book/export/html/1596. [Acedido em Outubro 2018].

[27] C. Woodford, "Radio-controlled and atomic clocks," 2009/2018. [Online]. Available: https://www.explainthatstuff.com/howradiocontrolledclockswork.html. [Acedido em Outubro 2018].

[28] D. Dwyer , "How Atomic Clocks Work," [Online]. Available: https://science.howstuffworks.com/atomic-clock2.htm. [Acedido em Outubro 2018].

[29] "GPS and Relativity," 4 November 2014. [Online]. Available: http://unbonmotgroundswell.blogspot.com/2014/11/gps-and-relativity.html. [Acedido em Outubro 2018].

[30] "Pseudorandom Noise Code Assignments," 23 May 2013. [Online]. Available: https://www.losangeles.af.mil/About-Us/Fact-Sheets/Article/343695/pseudorandom-noise-code-assignments/. [Acedido em Outubro 2018].

[31] I. Poole, "GPS Signal," [Online]. Available: https://www.radio-electronics.com/info/satellite/gps/signals.php. [Acedido em Setembro 2018].

[32] "New Civil Signals," Space-Based Positioning, Navigation, and Timing, [Online]. Available: https://www.gps.gov/systems/gps/modernization/civilsignals/. [Acedido em Outubro 2018].

[33] "GPS Signal Plan," [Online]. Available: https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan. [Acedido em Setembro

2018].

[34] "The P and C/A Codes," [Online]. Available: https://www.e-education.psu.edu/geog862/book/export/html/1407. [Acedido em Setembro 2018].

[35] "The Navigation Message," [Online]. Available: https://www.e-education.psu.edu/geog862/book/export/html/1407. [Acedido em Setembro 2018].

[36] "Trilateration vs Triangulation – How GPS Receivers Work," [Online]. Available: https://gisgeography.com/trilateration-triangulation-gps/. [Acedido em Outubro 2018].

[37] "Trilateration," [Online]. Available: https://www.e-education.psu.edu/geog862/book/export/html/1407. [Acedido em Setembro 2018].

[38] M. Brain e T. Harris , "How GPS Receivers Work - 3-D Trilateration," [Online]. Available: https://electronics.howstuffworks.com/gadgets/travel/gps2.htm. [Acedido em Outubro 2018].

[39] "How does GPS work?," [Online]. Available: http://www.physics.org/article-questions.asp?id=55. [Acedido em Outubro 2018].

[40] [Online]. Available: https://i2.wp.com/www.techjini.com/wp-content/uploads/2013/04/FVsHS.gif?ssl=1. [Acedido em Outubro 2018].

[41] "Doppler Shift," [Online]. Available: https://www.e-education.psu.edu/geog862/book/export/html/1659. [Acedido em Setembro 2018].

[42] M. Brain , "How Radar Works - Doppler Shift," [Online]. Available: https://science.howstuffworks.com/radar2.htm. [Acedido em Outubro 2018].

[43] "Spoofing a Superyacht at Sea," 30 July 2013. [Online]. Available: https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea. [Acedido em Setembro 2018].

[44] M. L. Psiaki e T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE* , vol. 104, nº 6, pp. 1258 - 1270, 2016.

[45] D. P. Shepard, J. A. Bhatti, T. E. Humphreys e A. A. Fansler, "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks," em *Preprint of the 2012 ION GNSS Conference*, Nashville, TN, 2012.

[46] K. Hartmann e K. Giles, "UAV exploitation: A new domain for cyber power," em *2016 8th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2016.

[47] M. J. Schwartz, "Iran Hacked GPS Signals To Capture U.S. Drone," DARKReading, 16 12 2011. [Online]. Available: https://www.darkreading.com/attacks-and-breaches/iran-hacked-gps-signals-to-capture-us-drone/d/d-id/1101882. [Acedido em Outubro 2018].

[48] T. Brewster, "Watch GPS Attacks That Can Kill DJI Drones Or Bypass White House Ban," Forbes, 8 August 2015. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2015/08/08/qihoo-hacks-drone-gps/#47db04d92bf5. [Acedido em Outubro 2018].

[49] D. Hambling, "Ships fooled in GPS spoofing attack suggest Russian cyberweapon," NewScientist, 10 August 2017. [Online]. Available: https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/. [Acedido em Outubro 2018].

[50] "Pokémon GO," Google Play, [Online]. Available: https://play.google.com/store/apps/details?id=com.nianticlabs.pokemongo. [Acedido em Outubro 2018].

[51] C. Gartenberg, "This Pokémon Go GPS hack is the most impressive yet," TheVerge,

28 July 2016. [Online]. Available: https://www.theverge.com/circuitbreaker/2016/7/28/12311290/pokemon-go-cheat-gps-signal-spoofing. [Acedido em Outubro 2018].

[52] I. GNSS, "What is navigation message authentication?," 1 January 2018. [Online]. Available: http://insidegnss.com/what-is-navigation-message-authentication/. [Acedido em Setembro 2018].

[53] C. D. Hacker, "GPS Spoofing w/ BladeRF - Software Defined Radio Series #23," Youtube, 11 09 2016. [Online]. Available: https://www.youtube.com/watch?v=VAmbWwAPZZo&t=451s. [Acedido em Novembro 2017].

[54] T. Humphreys, "Statement on the Security Threat Posed By Unmanned Aerial Systems and Possible Countermeasures," 16 March 2015. [Online]. Available: https://docs.house.gov/meetings/HM/HM09/20150318/103136/HHRG-114-HM09-Wstate-HumphreysT-20150318.pdf. [Acedido em Agosto 2018].

[55] M. S. Faughnan, B. J. Hourican, G. C. MacDonald, M. Srivastava, J.-P. A. Wright, Y. Y. Haimes, E. Andrijcic, Z. Guo e J. C. White, "Risk Analysis of Unmanned Aerial Vehicle Hijacking and Methods of its Detection," em *2013 IEEE Systems and Information Engineering Design Symposium*, Charlottesville, VA, USA, 2013.

[56] [Online]. Available: https://www.e-education.psu.edu/geog862/book/export/html/1659. [Acedido em Agosto 2018].

[57] "Software-Defined GPS Signal Simulator," [Online]. Available: https://github.com/osqzss/gps-sdr-sim. [Acedido em Novembro 2017].

[58] "Quasi-Zenith Satelite System (QZSS)," [Online]. Available: http://qzss.go.jp/en/. [Acedido em julho 2018].

[59] "National Marine Eletronics Association," [Online]. Available: https://www.nmea.org/. [Acedido em Agosto 2018].

[60] "NMEA data," [Online]. Available: https://www.gpsinformation.org/dale/nmea.htm#AAM. [Acedido em Agosto 2018].

[61] "GPS - NMEA sentence information," [Online]. Available: http://aprs.gids.nl/nmea/#gga. [Acedido em Agosto 2018].

[62] "ArcGIS Runtime SDKs," Esri, [Online]. Available: https://developers.arcgis.com/arcgis-runtime/. [Acedido em Abril 2018].

[63] "Get Qt," [Online]. Available: https://www.qt.io/download. [Acedido em Junho 2018].

[64] "Language Bindings," [Online]. Available: https://wiki.qt.io/Language_Bindings. [Acedido em Julho 2018].

[65] "About Us," [Online]. Available: https://www.qt.io/company. [Acedido em Julho 2018].

[66] "ArcGIS Runtime SDK for Qt," [Online]. Available: https://developers.arcgis.com/qt/latest/. [Acedido em Julho 2018].

[67] "MobileMapPackage QML Type," [Online]. Available: https://developers.arcgis.com/qt/latest/qml/api-reference/qml-esri-arcgisruntime-mobilemappackage.html. [Acedido em Agosto 2018].

[68] "CoordinateFormatter QML Type," [Online]. Available: https://developers.arcgis.com/qt/latest/qml/api-reference/qml-esri-arcgisruntime-coordinateformatter.html. [Acedido em Julho 2018].

[69] "GeometryEngine QML Type," [Online]. Available:

https://developers.arcgis.com/qt/latest/qml/api-reference/qml-esri-arcgisruntime-geometryengine.html. [Acedido em Julho 2018].

[70] Wabis, "Distances on Globe and Flat Earth," 23 May 2017. [Online]. Available: http://walter.bislins.ch/bloge/index.asp?page=Distances+on+Globe+and+Flat+Earth. [Acedido em Outubro 2018].

[71] A. McGovern, "Geographic-Distance-and-Azimuth-Calculations," 26 March 2003. [Online]. Available: https://www.codeguru.com/cpp/cpp/algorithms/article.php/c5115/Geographic-Distance-and-Azimuth-Calculations.htm. [Acedido em Agosto 2018].

[72] C. Veness, "Calculate distance, bearing and more between Latitude/Longitude points," Movable Type Scripts, [Online]. Available: https://www.movable-type.co.uk/scripts/latlong.html. [Acedido em Agosto 2018].

[73] spk578, "Distance on a sphere: The Haversine Formula," 5 Outubro 2017. [Online]. Available: https://community.esri.com/groups/coordinate-reference-systems/blog/2017/10/05/haversine-formula. [Acedido em Agosto 2018].

[74] C. Veness, "Vincenty solutions of geodesics on the ellipsoid," [Online]. Available: https://www.movable-type.co.uk/scripts/latlong-vincenty.html#datums. [Acedido em Agosto 2018].

[75] W. Fraczek, "Mean Sea Level, GPS, and the Geoid," Esri Applications Prototype Lab, 2013. [Online]. Available: http://www.esri.com/news/arcuser/0703/geoid1of3.html. [Acedido em Julho 2018].

[76] [Online]. Available: http://www.esri.com/news/arcuser/0703/graphics/geoid1_lg.gif. [Acedido em Agosto 2018].

[77] spk578, "https://community.esri.com/groups/coordinate-reference-systems/blog/2017/10/11/vincenty-formula," 2017, 10 Outubro 2017. [Online]. Available: https://community.esri.com/groups/coordinate-reference-systems/blog/2017/10/11/vincenty-formula. [Acedido em Setembro 2018].

[78] "Altitude & Azimuth: The Horizontal Coordinate System," [Online]. Available: https://www.timeanddate.com/astronomy/horizontal-coordinate-system.html. [Acedido em Agosto 2018].

[79] "Grid and Geodetic Azimuths," [Online]. Available: https://www.e-education.psu.edu/geog862/book/export/html/1644. [Acedido em Agosto 2018].

[80] tigoe, 20 November 2007. [Online]. Available: https://www.tigoe.com/pcomp/code/Processing/127/. [Acedido em Agosto 2018].

[81] L. He, . W. Li, C. Guo e R. Niu, "Civilian unmanned aerial vehicle vulnerability to GPS spoofing attacks," em *Proceedings - 2014 7th International Symposium on Computational Intelligence and Design, ISCID 2014*, Hangzhou, China, 2014.

[82] C. Li e X. Wang, "Jamming Research of the UAV GPS / INS Integrated Navigation System Based on Trajectory Cheating," em *2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, Datong, China, 2016.

[83] [Online]. Available: https://community.esri.com/servlet/JiveServlet/showImage/38-57595-375715/Circle-trig6_svg.png. [Acedido em Setembro 2018].

[84] [Online]. Available: https://community.esri.com/servlet/JiveServlet/showImage/38-57578-376484/327px-Ellipsoid_revolution_oblate_aab_auxiliary_sphere.png. [Acedido em Outubro 2018].

Apêndices

Apêndice A – Manual de utilizador

O manual de utilizador, é descrito na legenda seguinte referenciado à imagem da interface.

Legenda:

1 – Distância do raio da zona a proteger, valores possíveis:1-10000

2 – Distância do raio do radar

3 – Botão de criação, para criar tanto a zona protegida como o radar, esta só é criada com sucesso se os valores estiverem corretos, na caixa de texto. Após a criação o botão fica desativado

4 – Botão de Ativação da proteção, fica disponível assim que a utilização do botão criar é concluída. O botão é ativado e desativado alternadamente em relação ao botão de criação.

5 – Botão de remoção, este é utilizado para remover as zonas colocadas no mapa, e faz reset ao sistema, sendo necessário voltar a introduzir os valores.

6 – Janela de coordenadas, nesta janela o utilizador pode colocar as coordenadas manualmente, mas tem que respeitar o formato que está inserido.

7 – Localização dos ficheiros, neste campo é necessário introduzir o caminho onde se irá guardar os ficheiros no sistema de arquivos do aparelho.

8 – Botão de gerar o caminho simulado do UAV.

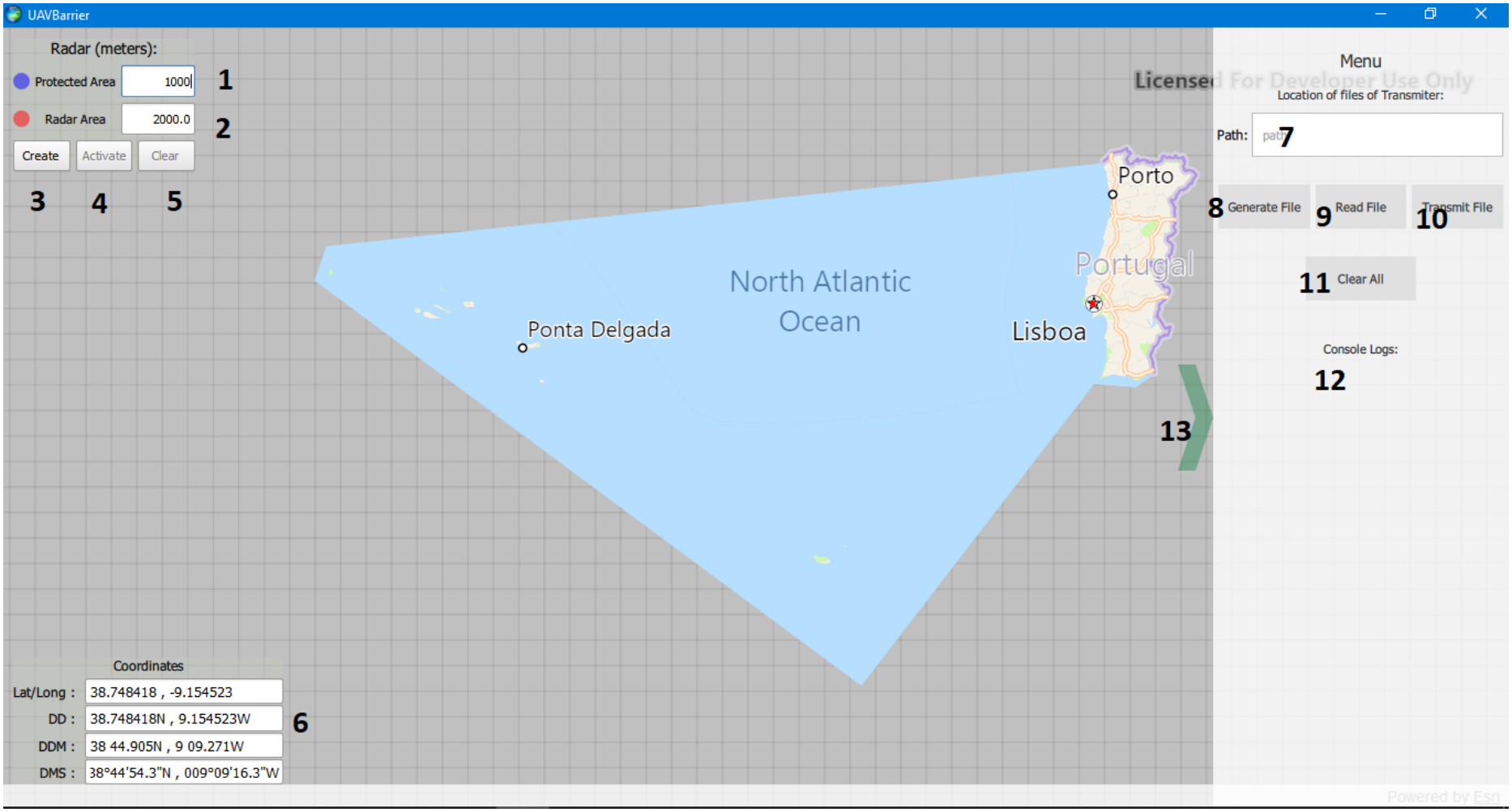
9 – Botão para ler o caminho simulado já existente.

10 – Botão para dar início à transmissão e simulação das contramedidas.

11 – Botão de remover todo o tipo de arquivos.

12 – Consola de registo, é aqui que são descritos os registos relacionados com os botões 7 a 12.

13 – Expandir ou comprimir o menu de simulação.


UAVBarrier
Radar (meters):
Protected Area
1000
1
Radar Area
2000.0
2
Create
Activate
Clear
3
4
5
Coordinates
Lat/Long :
38.748418 , -9.154523
DD :
38.748418N , 9.154523W
DDM :
38 44.905N , 9 09.271W
DMS :
38°44'54.3"N , 009°09'16.3"W
6
North Atlantic Ocean
Ponta Delgada
Porto
Portugal
Lisboa
Menu
Location of files of Transmiter:
Path:
7
8 Generate File
9 Read File
10 Transmit File
11 Clear All
Console Logs:
12
13
Powered by Esri