MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
GUERRA ELETRÔNICA

1ºTen(QC-CA) LUCAS CAMPESTRINI HARGER

MEDIDAS DE ATAQUE E PROTEÇÃO ELETRÔNICA PARA RECEPTORES NAVSTAR-GPS

Rio de Janeiro
2018

1ºTen(QC-CA) LUCAS CAMPESTRINI HARGER

MEDIDAS DE ATAQUE E PROTEÇÃO ELETRÔNICA PARA RECEPTORES NAVSTAR-GPS

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica

Orientadores:
Capitão de Corveta Alessandro Roberto dos Santos, MSc.
Professor Waldo Araujo Russo Brasil, MSc.

CIAW
Rio de Janeiro
2018

1ºTen(QC-CA) LUCAS CAMPESTRINI HARGER

MEDIDAS DE PROTEÇÃO ELETRÔNICA PARA RECEPTORES NAVSTAR-GPS

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica.

Aprovada em 25/06/2018

Banca Examinadora:

Capitão de Mar e Guerra Gian Karlo Huback Macedo de Almeida, MSc. – CIAW

Capitão de Corveta Alessandro Roberto dos Santos, MSc – CGEM

Capitão-Tenente (EN) Yanes Checcacci Balod, MSc. - CGEM

CIAW
Rio de Janeiro
2018

Dedico este trabalho a todos os profissionais do mar que buscam com afinco construir uma Marinha melhor para o futuro.

AGRADECIMENTOS

Agradeço, sobretudo, a Deus, que sem a fé Nele nada é possível, à minha noiva, pelo apoio incondicional e por sempre me incentivar a fazer o meu melhor, aos meus pais, por serem os responsáveis pela pessoa que me tornei e aos meus irmãos, pelo companheirismo e incentivação. Agradeço também ao meu orientador técnico, pelos importantes ensinamentos e pelo empenho em fazer desta obra, a melhor possível.

“Nesse exato momento há trinta e um satélites ao redor do mundo com nada melhor para fazer que te ajudar a achar o caminho até o mercado”

Ed Burnette

MEDIDAS DE PROTEÇÃO ELETRÔNICA PARA RECEPTORES NAVSTAR-GPS

RESUMO

Os sistemas de posicionamento global já fazem parte do cotidiano da sociedade, e na Marinha do Brasil (MB) não é diferente. O NAVSTAR GPS, ou simplesmente GPS, é o sistema de posicionamento via satélite mais utilizado no mundo e presente em grande parte dos meios navais da MB. O que normalmente se menospreza, são os perigos a que estão sujeitos esses equipamentos. Existem ataques que podem causar indisponibilidade ou um funcionamento incorreto, e é necessário que os militares da Marinha tenham plena ciência desses ataques e possam saber também proteger seus receptores. Sendo assim, a presente obra tem por finalidade a apresentação dos principais ataques a que estão sujeitos os equipamentos GPS, além de propor técnicas que podem mitigar a probabilidade de sucesso desses ataques.

Palavras- chave: GPS, *Jamming*, *Spoofing*, navegação, satélite.

LISTA DE FIGURAS

LISTAS DE SIGLAS E ABREVIATURAS

AGE	Ações de Guerra Eletrônica
AIS	*Automatic Identification System*
A/D	Analógico-digital
C/A	*Course/Acquisition*
CGE	Capacidade de Guerra Eletrônica
CW	*Continuous Wave*
DGPS	*Differential Global Position System*
DMN	Doutrina Militar Naval
DoS	*Denial of Service*
DP	Dispositivo de Privacidade
EEM	Espectro Eletromagnético
EUA	Estados Unidos da América
ESM	*Electronic Support Measures*
FDAF	*Frequency Domain Adaptive Filter*
FFT	*Fast Fourier Transform*
GDOP	*Geometric Dilution of Precision*
GE	Guerra Eletrônica
GPS	*Global Position System*
MAGE	Medidas de Apoio à Guerra Eletrônica
MAE	Medidas de Ataque Eletrônico
MB	Marinha do Brasil
MCS	*Master Control Station*
MGE	Medidas de Guerra Eletrônica
MPE	Medidas de Proteção Eletrônica
NAVSTAR	*Navigation Satellite Time And Ranging*
NB	*Narrow Band*
P	*Precision/Protected*
PPS	*Protected Position Service*
RAIM	*Receiver Autonomous Integrity Monitoring*
SA	*Select Availability*
SPS	*Standard Position Service*
WB	*Wide Band*
WGS84	*World Geodetic System*

SUMÁRIO

1. INTRODUÇÃO

A orientação sempre foi uma necessidade constante do ser humano, sendo os métodos de navegação aprimorados com o passar dos tempos. Com o extenso avançado tecnológico do ultimo século, o ser humano pôde deixar de depender apenas de recursos advindos da natureza, como a observação do céu ou pontos notáveis em terra, para então empregar ferramentas mais sofisticadas, como a navegação baseada em satélites.

Criado e administrado pelo Departamento de Defesa dos Estados Unidos da América (EUA), o GPS (*Global Position System*) foi criado primordialmente para ser empregado em conflitos armados, conferindo elevada precisão às ações militares. Não demorou muito para que fosse identificado e explorado o seu potencial para aplicações civis, como navegação, mapeamentos, topografia, entre outros.

Percebendo a elevada gama de aplicações, algumas nações desenvolveram seus próprios sistemas de navegação via satélite, como é o caso do GALILEO, desenvolvido pela União Européia, e do GLONASS, criado pela Rússia. Não obstante, desenvolver, fabricar e manter uma constelação de satélites é uma tarefa complexa e de custo elevado. No Brasil, por conta de ainda não ter sido desenvolvido um sistema de navegação via satélite, é inevitável a dependência de nações estrangeiras.

1.1. Apresentação do Problema

Dentre os principais sistemas de navegação existentes, a constelação de satélites GPS tem um destaque especial. Presentes em *smartphones*, *tablets*, carros e praticamente todos os equipamentos eletrônicos existentes, o GPS se tornou artigo de necessidade na sociedade, e na MB não é diferente: a grande maioria dos meios navais possui ao menos um equipamento de navegação que utilize o GPS. Em locais longe de costa, onde a navegação radar ou por ponto fixo em terra se torna inviável, a dependência do GPS se faz evidente. Devido à sua precisão e praticidade, esse sistema se torna naturalmente uma das principais ferramentas de navegação dos navios da MB, porém, mesmo sabendo das facilidades que essa tecnologia proporciona, é necessário que sejam evidenciadas suas fragilidades.

1.2. Justificativa e Relevância

Graças à sua precisão e praticidade, o GPS se torna naturalmente uma das principais ferramentas de navegação dos navios da MB. Devido a sua elevada disponibilidade, os usuários desse sistema muitas vezes não se dão conta gama de ataques existentes, que podem levar a inviabilizar o uso do equipamento.

O fator motivacional deste trabalho foi a constatação de um número reduzido de obras sobre o tema no Brasil, principalmente focando nos aspectos relevantes para a Marinha do futuro. A difusão dos conhecimentos que são apresentados neste trabalho entre os oficiais da Marinha é essencial para que uma eventual negação de serviço (DoS – *Denial of Service*) do GPS, por exemplo, não afete o cumprimento das missões.

A MB participa de inúmeros eventos internacionais, onde o GPS acaba sendo a principal ferramenta de navegação nas mais diversas travessias oceânicas. Esse sistema de navegação pode também ser usado para auxiliar nas entradas e saídas de portos e nas mais diferentes manobras, como de atracação e fundeio.

1.3. Objetivos

Os objetivos desta obra foram definidos de forma a incitar a discussão do tema dentro da Marinha do Brasil levando ao desenvolvimento gradual de uma consciência institucional sobre os perigos a que estão sujeitos os receptores GPS.

1.3.1. Objetivo Geral

Como dito anteriormente, as fragilidades do sistema de navegação GPS, que nem sequer é de administração nacional, são reais. Sendo assim, o objetivo principal deste trabalho é apresentar os principais tipos de ataques a que estão sujeitos o GPS e sugerir métodos para proteção contra esses ataques na Marinha do futuro.

1.3.2. Objetivos Específicos e organização do trabalho

Este trabalho de conclusão de curso foi dividido em quatro capítulos, sendo eles: conceitos de guerra eletrônica, o sistema de navegação satelital GPS, ataques a GPS e medidas de proteção eletrônica para GPS.

- Conceitos de Guerra Eletrônica (GE): com o intuito de posicionar o tema dentro da GE, a estrutura básica da GE é abordada e conceitos como Medidas de Ataque Eletrônico (MAE), Medidas de Proteção Eletrônica (MPE) e Medidas de Apoio à Guerra Eletrônica (MAGE) são apresentados de forma breve.
- O sistema de navegação satelital GPS: orbitando ao redor do planeta, existem várias constelações de satélites de navegação. Contudo, uma constelação especifica é de interesse deste trabalho: o GPS. Sendo assim, o objetivo específico deste tópico é apresentar um compilado de informações sobre o GPS, como histórico, organização do sistema e princípio de funcionamento.
- Ataques a GPS: O GPS data da década de 1970 e os tipos de ataques vêm se sofisticando desde então. Antes de apresentar formas de proteger o GPS, é necessário que sejam abordados os principais tipos de ataques existentes, apresentando seus princípios de funcionamento.
- MPE para GPS: Como último tópico, são relacionadas técnicas para prevenir a interrupção ou mau funcionamento deste serviço na marinha do futuro, tendo como objetivo apresentar o princípio de implementação de cada técnica, abrindo espaço para o desenvolvimento de equipamentos de proteção de GPS dentro da MB.

1.4. Metodologia - Classificação

Visando analisar aspetos qualitativos do tema, não é objetivo desta obra levantar dados numéricos que demonstrem a eficácia das soluções para o problema proposto. A pesquisa do presente trabalho pode ser classificada como explicativa e foram utilizadas como referência obras que tem caráter notadamente descritivo.

Ao se apresentar a relação de ataques que afetam o GPS, além de relacionar algumas medidas de proteção eletrônica, pode-se perceber a natureza explicativa da metodologia, quanto aos fins.

Quantos aos meios, a pesquisa deste trabalho de conclusão de curso pode ser classificada como bibliográfica, pois o objetivo principal é a reunião de uma série de trabalhos de notável credibilidade de forma que o objetivo principal seja alcançado.

1.5.Metodologia - Limitações

Devido à limitação de tempo para pesquisas, a proposição de projetos que visam implementar equipamentos de proteção de GPS, por exemplo, não se torna viável. Também por causa a dificuldade supracitada, não foi possível abordar alguns outros tipos de ataques que podem ocorrer no GPS, como os cibernéticos, por exemplo, e ferramentas de navegação alternativas ao GPS.

1.6. Coleta e Tratamento de Dados e Informações

Para a elaboração desta obra, foi realizada uma extensa pesquisa bibliográfica, utilizando-se principalmente de trabalhos, dissertações, teses e artigos disponíveis em meio digital. As informações obtidas foram organizadas de forma a estabelecer uma linha lógica que parte dos conceitos básicos necessários para a ambientação do tema até o tratamento dos tópicos principais que possibilitaram alcançar os objetivos principais.

2. CONCEITOS DE GUERRA ELETRÔNICA

As constelações de satélites de navegação apresentam a grande vantagem de poder fornecer, em tempo real, as coordenadas geográficas de qualquer estação terrena que faz parte de sua área de ação, desde que tenha o equipamento correto para estabelecer o *link* com os satélites. No entanto, esse método de localização necessita utilizar como meio de propagação o espaço livre, fazendo uso do espectro eletromagnético para tráfego de dados.

É nesse cenário que a GE e o GPS se encontram, surgindo a necessidade de que alguns conceitos da GE sejam abordados neste trabalho. Pra tal, foi usada como referência a publicação MB (2017), que trata do tema focando nos aspectos relevantes para a Marinha do Brasil.

2.1. Definição de Guerra Eletrônica

Segundo a Doutrina Militar Naval (DMN), a GE pode ser definida de forma simplificada como um conjunto de ações que visam assegurar a uso do espectro eletromagnético (EEM) pelas forças amigas, ao mesmo tempo em que visa negar seu uso às forças inimigas.

2.2. Capacidade de Guerra Eletrônica (CGE)

Para empreender as ações de GE, é necessário que o poder naval desenvolva uma CGE, que pode ser conceituada como uma reunião de recursos e meios diversos que permitam ao pode naval executar eficazmente ações de GE, beneficiando suas operações.

A CGE é divida em Atividades de GE e Medidas em GE (MGE), sendo que as AGE tem uma função mais de inteligência e apoio, não sendo relevantes para este trabalho. Já os conceitos associados às MGE são de suma importância, pois os ataques a sistema GPS e a prevenção desses ataques constituem claramente MGE. As MGE são dividas em Medidas de Apoio à Guerra Eletrônica (MAGE), Medidas de Ataque Eletrônico (MAE) e Medidas de Proteção Eletrônica (MPE) e são ações caracterizadas por atuarem diretamente em apoio a uma operação militar.

2.2.1. Medidas de Apoio à Guerra Eletrônica (MAGE)

As MAGE, como o próprio nome já diz, visam apoio a GE identificando e localizando as fontes de irradiação eletromagnética, para que uma possível ameaça possa ser rapidamente identificada e outras MGE possam ser empregadas. Na OTAN ela é conhecida como ESM - *Electronic Support Measures*.

2.2.2. Medidas de Ataque Eletrônico (MAE)

As MAE visam negar o uso do EEM por uma força inimiga, além de tentar impedir o funcionamento de equipamentos que utilizam esse espectro. Quando esse conceito é transportado para o GPS, a negação de serviço é um fiel exemplo de MAE. Os diversos ataques a sistemas de posicionamento global, como o *jamming* e o *spoofing*, visam prejudicar a comunicação entre o satélite de navegação e os equipamentos GPS embarcados, negando ou degradando o uso do EEM.

2.2.3. Medidas de Proteção Eletrônica (MPE)

Os meio navais estão sujeito aos mais diversos tipos de ataques eletrônicos, sendo necessário o desenvolvimento de medidas que assegurem o uso do EEM. O conceito de MPE é justamente esse: garantir que equipamentos que utilizam o EEM possam funcionar livremente e sem interferências. As técnicas para prevenir a DoS ,que são abordadas no capitulo 5, são exemplos de MPE.

3. O SISTEMA DE NAVEGAÇÃO SATELITAL GPS

O NAVSTAR GPS (***N**avigation **S**atellite **T**ime and **R**anging **G**lobal **P**osition **S**ystem*), ou simplesmente GPS, representou um marco para a navegação aérea e naval, porém ele não foi o primeiro sistema de navegação satelital. Este capítulo começa com um breve histórico dos satélites de navegação, culminando na criação do GPS, na década de 1970, além de apresentar as características gerais, componentes do sistema, métodos de posicionamento e as fontes de erro.

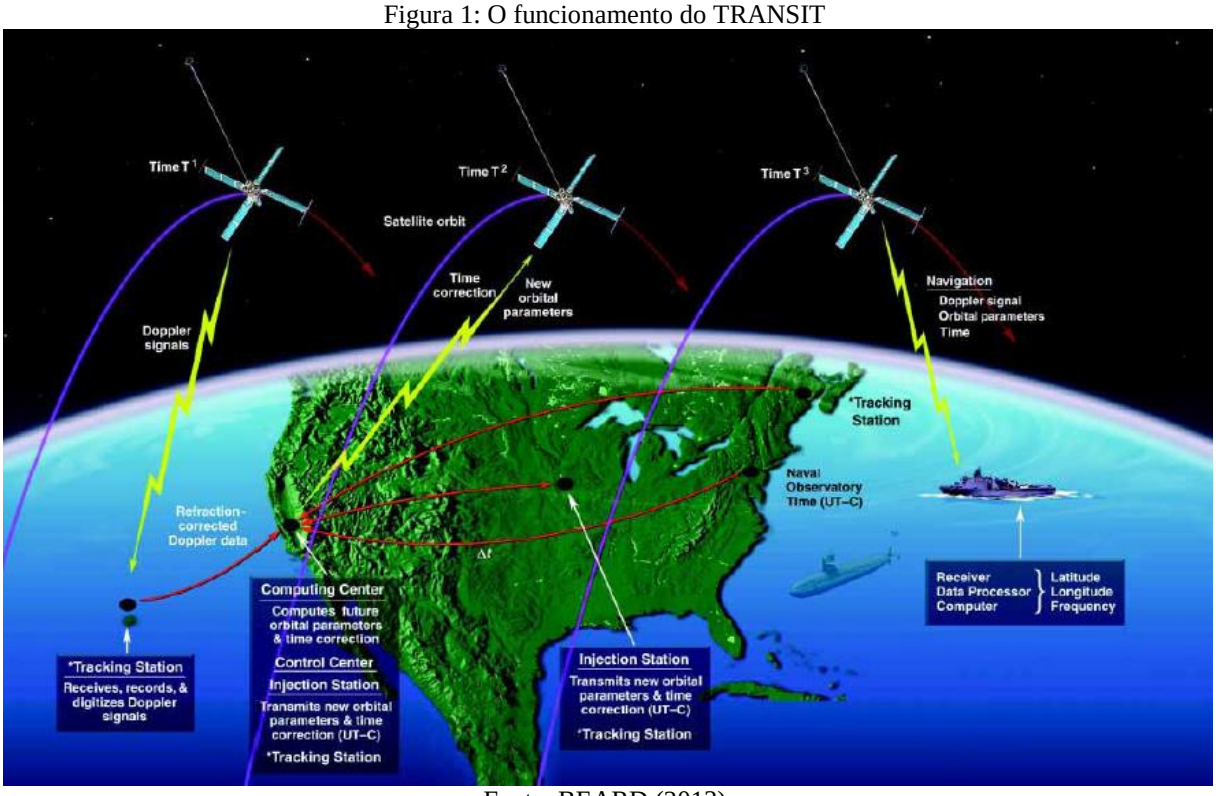
3.1. Breve histórico dos sistemas de navegação satelitais

O princípio da navegação satelital se dá logo após o lançamento do satélite Sputnik, em 1957, quando pesquisadores confirmaram que o efeito Doppler poderia ser usado para cálculo das efemérides (posição) dos satélites, e caso fosse conhecida sua posição, o resultado é a possibilidade da localização de uma estação de terra (AEROSPACE, 2010).

Dois anos após o lançamento do Sputnik, foi iniciado o projeto do TRANSIT, pela J*ohns Hopkins University Applied Physics Laboratory*, com o lançamento do primeiro satélite de baixa altitude (aproximadamente 1075Km) da constelação, dando origem ao primeiro sistema de satélites de navegação, com o objetivo da Marinha dos Estados Unidos localizar e acompanhar seus meios navais (AIAA, 2011).

O TRANSIT tornou-se operacional em 1964, cujo princípio de funcionamento foi por meio do efeito Doppler, podendo funcionar com o mínimo de quatro satélites, chegando ao longo de sua operação a seis satélites. Durante a operação do satélite, os pontos negativos eram o tempo para determinar a localização – cerca de 30 minutos, além do fato de ser apenas 2D. O TRANSIT ficou em operação por 32 anos, sendo descontinuado em 1996 (AEROSPACE, 2010). A Figura 1 mostra o princípio de funcionamento do TRANSIT.

Figura 1: O funcionamento do TRANSIT



Fonte: BEARD (2013)

Outros projetos de relevância são o *Timation*, que demonstrou a viabilidade do uso de *clocks* de alta precisão no espaço, e o programa 612B, que desenvolveu muitas das características usadas pelo GPS (AIAA, 2011).

Foi no ano de 1973 que, em um esforço conjunto entre a Força Aérea dos EUA e a organização de sistema de mísseis, foi criado o programa NAVSTAR GPS. Chefiado pelo então Coronel Brad Parkinson da USAF (*United States Air Force*), esse projeto pioneiro desenvolveu a arquitetura do sistema e os primeiros satélites, além do segmento de controle e dez tipos diferentes de equipamentos para o usuário (AIAA, 2011).

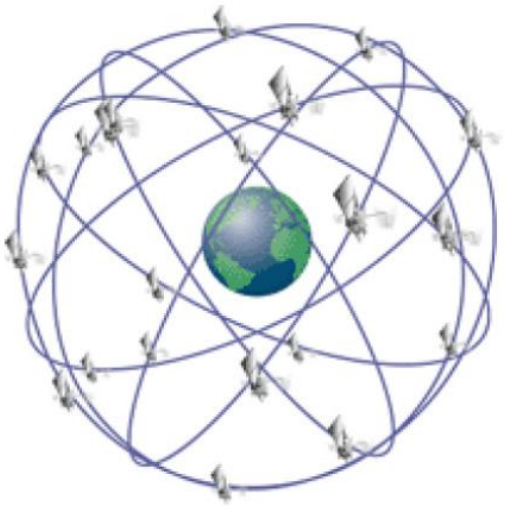
O primeiro protótipo dessa geração experimental de satélites, conhecida como Bloco I, foi lançado em 1978. Entre 1978 e 1985, dez protótipos foram lançados ao espaço com sucesso (AIAA, 2011).

A segunda fase do programa, chamada de Bloco II, começou em 1989 e foi até 1994, sendo desenvolvidos e lançados os primeiros satélites operacionais. Em 1995, os 24 satélites previstos estavam em órbita e o sistema foi declarado plenamente operacional (STURDEVANT, 2007).

3.2. Características gerais

O GPS consiste de um conjunto de 24 satélites, localizados a uma altitude média de 20200 km e distribuídos por seis planos orbitais. Essa constelação completa uma volta em torno da terra a cada 12 horas e foi concebida de forma que, em qualquer ponto do planeta, ao menos quatro satélites estejam disponíveis (RIBEIRO, 2002).

Figura 2: A constelação GPS



Fonte: GOMES (2010)

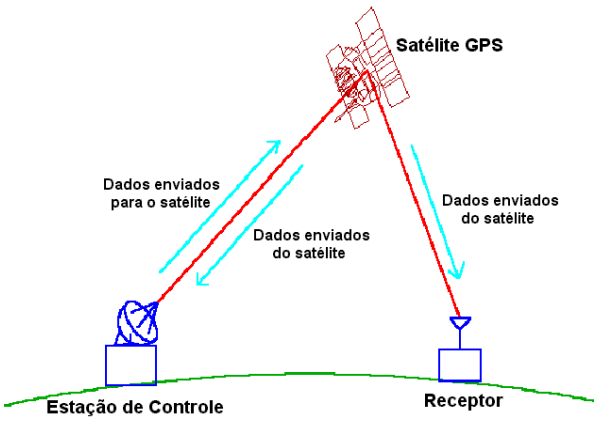
Existem duas bandas de operação, sendo apenas uma disponibilizada para uso civil. As bandas L1 e L2 têm frequência da portadora de 1.575,42 MHz e 1.227,60 MHz, respectivamente. No código disponibilizado a todos os usuários, chamado C/A (*Course Acquisition*), os receptores utilizam apenas a banda L1 e possuem uma precisão inferior ao código de uso exclusivo do governo dos EUA. Conhecido como P (*Precise/Protected*), esse código exclusivo faz uso das duas bandas L1 e L2, emprega criptografia *anti-spoofing* e possui alta precisão (KAPLAN; HEGARTY, 2006).

Até o ano de 2000, o SPS (*Standard Positioning Service*), que é o serviço disponibilizado ao usuário comum, utilizava o código C/A associado ao código SA (*Selective Availability*), fazendo com que a precisão do GPS degradasse de forma expressiva. Após a retirada do código SA, as precisões dos equipamentos foram da ordem de 100 metros para cerca de 15 metros (ALBUQUERQUE; SANTOS, 2003).

3.3. Componentes do Sistema

O GPS pode ser divido em três componentes: espacial, de controle e de usuário. O segmento espacial é formado pelos 24 satélites da constelação, com quatro satélites em cada órbita defasados de 90º entre si, provendo cobertura global, inclusive nos pólos (ALBUQUERQUE; SANTOS, 2003). A Figura 3 mostra as três componentes do GPS.

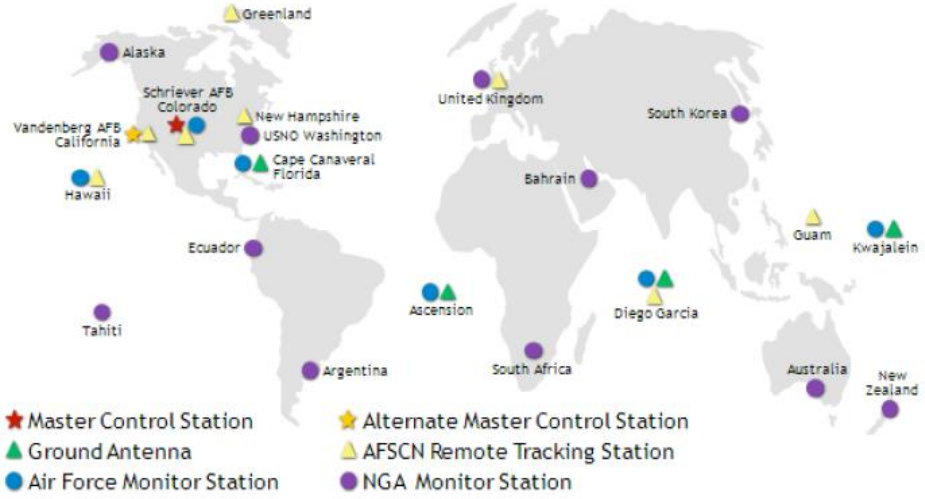
Figura 3: As componentes do GPS



Fonte: ALBUQUERQUE; Santos (2003)

O componente de controle terrestre tem a função de manutenção e controle do serviço. É composto por Estações de Controle Central (MCS - *Master Control Station*), de monitoramento e rádio. As estações de monitoramento ficam em constante acompanhamento dos veículos espaciais e enviam as informações coletadas à MCS. As estações rádio têm a função de enviar aos satélites atualizações do sistema. Já a MCS é capaz de detectar anormalidades na operação do sistema, compilar sinais vindos do espaço referentes ao erro de localização do usuário, elaborar novas predições de órbitas e *clocks* e gerar as atualizações do sistema. Ao todo, esse segmento possui duas MCS, uma principal e uma alternativa, 12 estações rádio e 16 estações de monitoramento. A Figura 4 mostra a localização das estações de controle ao longo do globo (KAPLAN; HEGARTY, 2006).

Figura 4: As estações de controle terrestre



Fonte:WINTERNITZ (2017)

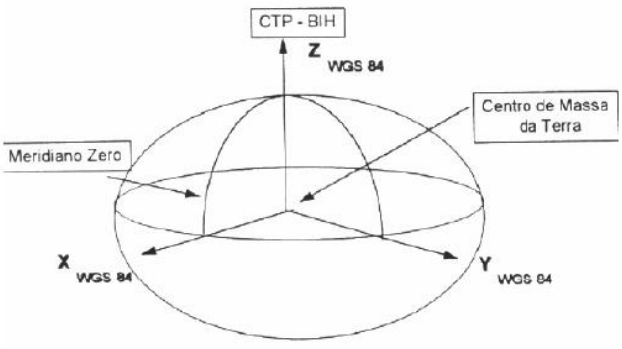
O segmento de usuário é formado por todos os receptores que são capazes de captar os sinais GPS e convertê-los em informações de posição, velocidade e tempo. Os usuários ainda podem ser diferenciados pelo serviço utilizado: SPS, do usuário comum, e o PPS (*Protected Position Service*), somente disponibilizado com a autorização do governo dos EUA. (RIBEIRO, 2002).

3.4. Métodos de Posicionamento

Antes de abordar os métodos de posicionamento, fazem-se necessárias algumas ressalvas em relação ao DATUM (sistema de referência) do GPS, quando se quer determinar a localização de um ponto na superfície terrestre.

Sabemos que o planeta terra não é uma esfera perfeita, pois além de sua superfície possuir muitas irregularidades, a forma geométrica que mais se aproxima do globo é o elipsóide. No caso do GPS, o DATUM mais adotado é o WGS84 (*World Geodetic System* 1984) e pode ser usado para a navegação em todo o mundo (GOMES, 2010). A figura 5 ilustra o globo terrestre considerado por esse DATUM, onde a superfície considerada é totalmente lisa e os raios do elipsóide são 6.378.137 e 6.356.752 metros (ROSA, 2013).

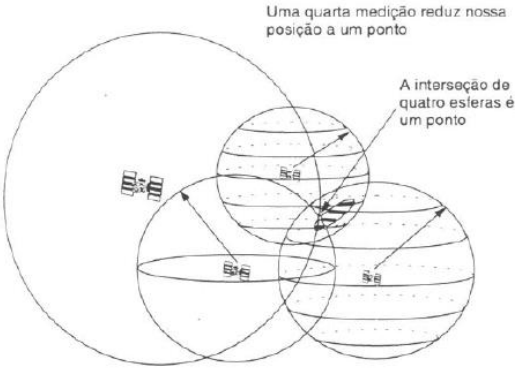
Figura 5: O DATUM WGS84



Fonte: GOMES (2010)

Para a obtenção da posição de um usuário, são necessários três satélites, que juntos são capazes de fornecer as coordenadas X, Y e o tempo T. Esse método é chamado de trilateração e com a ajuda de um quarto satélite, o GPS pode também fornecer a altitude do receptor (KAPLAN; HEGARTY, 2006). Quanto maior o numero de satélites captados pelo usuário, maior a precisão das coordenadas obtidas.

Figura 6: Trilateração dos satélites

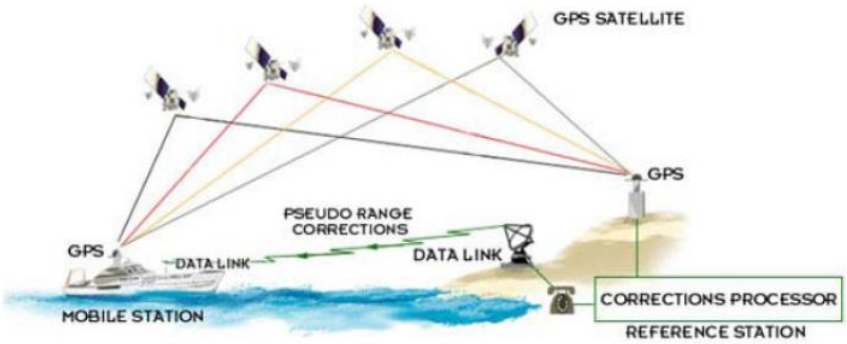


Fonte: MATTOS (2012)

A posição obtida pode ser classificada como absoluta, relativa ou a combinação dessas duas. As medidas absolutas são aquelas obtidas apenas com os satélites da constelação GPS, sem o auxílio de nenhum ponto conhecido. Já na posição relativa, as coordenadas geográficas de um ou mais pontos fixos são conhecidas e a posição é determinada a partir desses pontos. Um exemplo de um equipamento que utiliza tanto a posição absoluta quanto a relativa é o DGPS (GOMES, 2010).

Presente na Marinha do Brasil, o DGPS (*Differential Global Positioning System*) se utiliza de estações fixas em terra para ajustar a posição fornecida pelos satélites, conferindo maior precisão.

Figura 7: O DGPS



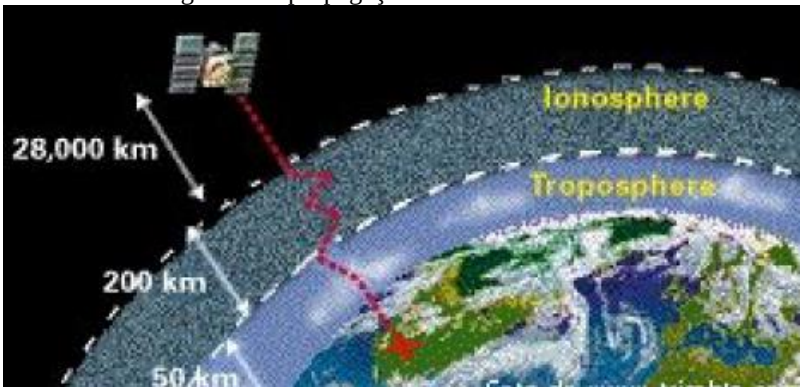
Fonte: GOMES (2010)

3.5. Fontes de Erro

Estando numa órbita de mais de 20.000km, os satélites GPS estão sujeitos a uma série de fatores que contribuem para uma determinação errônea da posição dos usuários. O meio de propagação do sinal, a órbita do satélite, o *clock*, o movimento de rotação terrestre e a geometria são os principais contribuintes de erros.

A atmosfera terrestre é um ambiente bastante heterogêneo e influencia diretamente na operação do GPS. As maiores fontes de erros são a ionosfera e a troposfera, devido às suas características peculiares. A ionosfera é composta por íons carregados, que acabam interagindo com o sinal, alterando o código e a fase do mesmo. Já na troposfera, o maior problema reside na presença de umidade, causando distorções significativas. Caso os efeitos ionosféricos e troposféricos não sejam levados em consideração, erros de mais de 10 metros podem ser observados (RIBEIRO, 2002). Na figura 8, tem-se uma ilustração do efeito dessas camadas atmosféricas na operação do GPS.

Figura 8: A propagação do sinal na atmosfera



Fonte: MATTOS (2012)

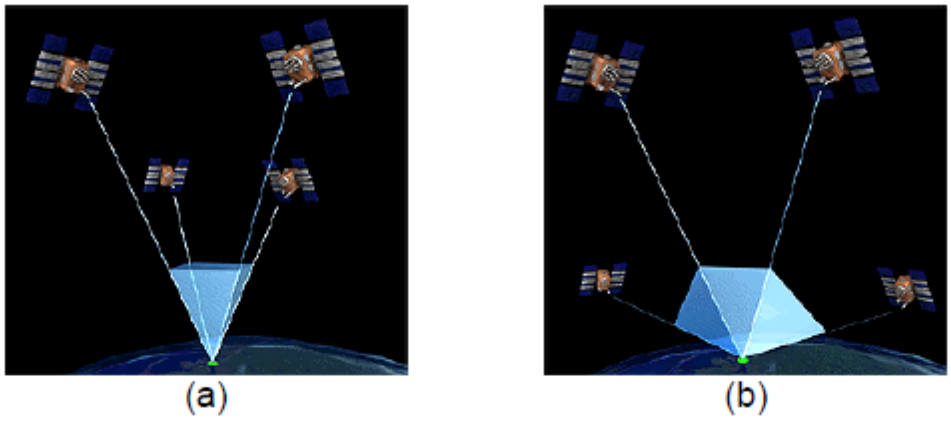
Os satélites GPS foram concebidos para que fiquem numa órbita precisa e previsível por um modelo matemático, fazendo com que as efemérides dos satélites sejam obtidas com a maior precisão possível. No entanto, alguns fenômenos não tão previsíveis acabam interferindo nessa órbita: a influência dos campos gravitacionais terrestre, lunar e solar, o atrito remanescente da atmosfera terrestre e a pressão das radiações solares. É nesse contexto que as estações de monitoramento são essenciais (RIBEIRO, 2002).

Apesar da elevada precisão dos relógios atômicos presentes nos satélites, ainda assim pode-se observar pequenos erros de *clock* devido a manipulações em frequências utilizadas, que tem um impacto expressivo na determinação da posição. Pra se ter uma idéia, um erro de apenas 80ns pode resultar em uma distorção de até 24 metros (KAPLAN; HEGARTY, 2006).

Como os satélites GPS não são geoestacionários, se faz necessária uma constante correção das coordenadas terrestres em virtude da rotação do planeta. Essa correção angular é o produto do tempo de propagação do sinal pela velocidade de rotação da terra (KAPLAN; HEGARTY, 2006).

Como dito anteriormente, são necessários ao menos quatro satélites para o correto funcionamento do sistema, sendo que o posicionamento desses satélites em relação ao usuário influencia diretamente na qualidade das informações do GPS. A chamada GDOP - *Geometric Dilution of Precision*, é definida como o inverso do volume do tetraedro formado pela trilateração dos satélites e dita quão acurada é a posição fornecida (ALBUQUERQUE; SANTOS, 2003). Os valores da GDOP podem variar de um a infinito, sendo normalmente entre dois e três (KAPLAN; HEGARTY, 2006).

Figura 9: Uma GDOP (a) alta (ruim) e uma baixa (boa)



Fonte: ALBUQUERQUE; Santos (2003)

4. ATAQUES A GPS

Na Marinha do Brasil, o GPS se tornou um grande aliado da navegação, sendo utilizado desde em manobras de entrada e saída de porto até nas travessias oceânicas. No entanto, o que muito se menospreza, ou simplesmente se desconhece, dentro do ambiente militar-naval brasileiro é a suscetibilidade do GPS aos mais variados tipos de ataques, que vão desde os menos sofisticados, como o *jamming*, até os mais complexos, como o *spoofing*.

Este capítulo aborda os principais ataques observados, começando com as interferências, que causam a DoS, seguindo do *spoofing*, que pode provocar erros intencionais na posição determinada pelo receptor GPS.

4.1. Interferências

Com a contínua evolução dos ataques a sistema de comunicações em geral, é comum ser observada certa negligência quanto ao tipo mais básico de ataque: as interferências intencionais, comumente conhecidas como *jamming*. No entanto, existem as interferências não intencionais, que também causam transtornos na comunicação entre os satélites e os equipamentos GPS.

4.1.1. Interferências não intencionais

As interferências não intencionais têm a característica marcante de serem mais previsíveis que as intencionais, pois normalmente provêm de outros serviços que se utilizam do espectro eletromagnético e acabam entrando em conflito com os sinais GPS. A dissertação de SOUSA (2005) lista alguns dos principais sinais, cujos harmônicos podem ser danosos, como os sinais de TV, de comunicações em VHF, de FM e radio amadores. A Tabela 1 mostra os harmônicos dos sinais que acabam coincidindo com a banda de operação do sinal L1 do GPS.

Tabela 1: Harmônicos que interferem no sinal GPS.

FONTES PONTENCIAIS DE INTERFERÊNCIA		
Harmônicos	Banda (MHz)	Serviços
L1	1571,42 – 1579,42	GPS (CÓDIGO C/A)
2°	785,71 – 788,71	UHF TV
3°	523,807 – 526,473	UHF TV
4°	392,855 – 394,855	MOBILE / STATION
5°	314,284 – 315,884	MOBILE / STATION
6°	261,903 – 263,237	MOBILE / STATION
7°	224,488 – 225,631	BROADCASTING
8°	196,427 – 197,428	VHF TV
9°	174,602 – 175,491	VHF TV
10°	157,142 – 157,942	VHF MARINE
11°	142,856 – 143,584	VHF MILITARY
12°	130,952 – 131,618	VHF COM
13°	120,878 – 121,494	VHF COM
14°	112,244 – 112,816	VOR/ILS
15°	104,761 – 105,295	FM
16°	98,214 – 98,714	FM

Fonte: SOUSA (2005)

4.1.2. *Jamming*

O *jamming* pode ser definido como o ato de emissão de ondas eletromagnéticas com a finalidade de interromper ou prevenir a transmissão de sinais. O objetivo principal de um *jammer* é causar a DoS, que é quando o receptor não consegue distinguir entre o sinal de ruído e o sinal do transmissor.

No caso do receptor GPS, a demodulação do sinal recebido é feita através de uma comparação do sinal recebido com um sinal gerado por ele próprio, processo chamado de *carrier-tracking loop* (SOUSA, 2005). O sinal recebido pode ser decomposto no sinal proveniente dos satélites (S) somados com sinais ruidosos (N). A divisão entre o sinal S e os sinais N resulta em um termo de grande importância para as comunicações: a relação Sinal-

Ruído (S/N). Com a introdução de sinais ruidosos artificiais, que não são provenientes de características do meio de propagação, das imperfeições dos equipamentos ou de qualquer outro ruído conhecido, ocorrerá uma degradação na S/N, até chegar ao ponto de não ser possível distinguir o sinal dos satélites, do ruído (SOUSA, 2005).

Os *jammers* podem ser distinguidos pela faixa de freqüências utilizada, de banda estreita (NB) ou de banda larga (WB), quando a forma de onda, contínua (CW) ou pulsada e quanto à aplicação, civil ou militar.

4.1.2.1. Quanto à faixa de freqüências e forma de onda

As emissões dos *jammers* podem ser dividas em três categorias: CW, de faixa estreita e de banda larga. As emissões CW, como o próprio nome já diz, são caracterizadas por uma onda ininterrupta com largura de banda bastante estreita, a ponto de ser considerada como de freqüência única. Já os sinais de banda estreita são caracterizados por uma largura de banda de aproximadamente 1,023MHz, mesma largura de banda ocupada pelo código C/A, e usualmente centrado em L1 ou em L2. Nas emissões em banda larga, têm-se também sinais com freqüência central em umas das portadoras do GPS, com a diferença da largura de banda passar a ser de 10,23, coincidindo com a largura de banda do código P (SOUSA, 2005).

4.1.2.2. Quanto à aplicação

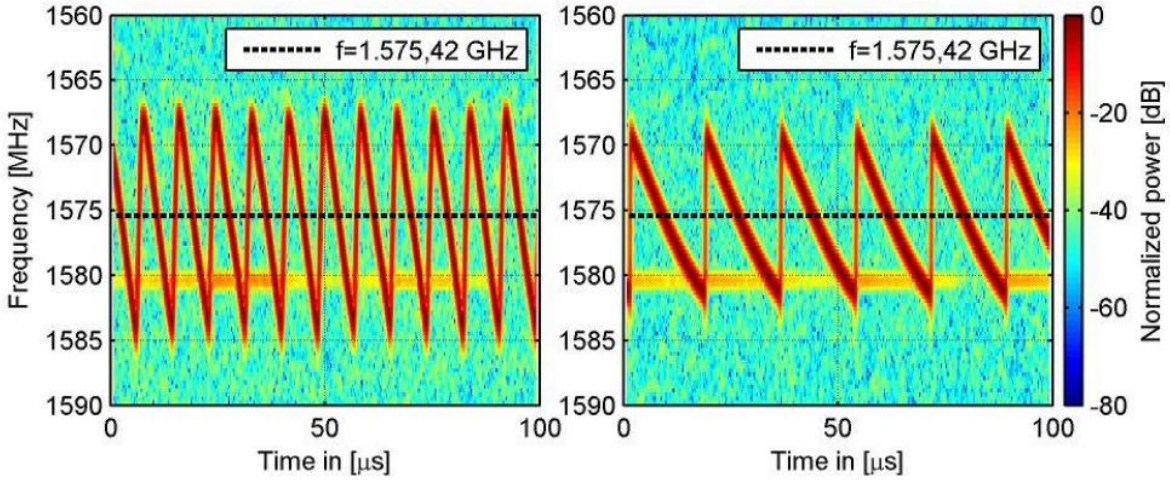
Os ataques aos receptores GPS apresentam notáveis diferenças dependendo como são usados, e por quem. Os bloqueadores GPS de uso civil, também chamado de dispositivos de privacidade (DP), vêm ganhando cadê vez mais popularidade, seja por suas características benéficas no quesito de preservar a privacidade do usuário que não deseja ser localizado, quanto dos incidentes que vem ocorrendo através uso indevido desses aparelhos. Infelizmente, grande parte dos usuários dos DP agem de má fé, utilizando esse aparelho para desabilitar dispositivos de rastreio ou, no caso de embarcações, desabilitar temporariamente o AIS (*Automatic Identification System*) e sair do controle das autoridades marítimas locais.

Figura 10: *Jammers* comerciais

Fonte: BENTO (2018)

Os preços dos DP variam de cerca de 100 reais, para modelos mais simples que podem ser alimentados por acendedores de cigarro automotivos, até algumas centenas de reais, nos modelos mais sofisticados que possuem banda larga e uma variedade de modos de operação. A maioria dos *jammers* comerciais tem como principal característica a transmissão de sinais CW, utilizando a técnica de variação constante de frequência (*chirp*). (RUEGAMER; KOWALEWSKI, 2015).

Figura 11: o "*chirp*" em frequência nos DPs



Fonte: RUEGAMER; Kowalewski (2015)

Já em operações militares, o emprego do *jammer* muda sensivelmente. Como o serviço GPS é utilizado mundialmente, forças oponentes podem utilizá-lo em beneficio próprio. É nesse cenário que o governo americano utiliza o código P: restringe-se o uso do GPS comercial e apenas seus aliados terão direito ao serviço. O que na teoria é excelente, na

pratica o uso de *jammers* em ações militares deve ser utilizado com cautela. Isso se deve ao fato de muitas vezes os próprios militares das forças amigas, em operações disfarçadas, estarem usado o GPS comercial, visto que o GPS militar é bem mais pesado, lento, além de ser pouco intuitivo, sendo impraticável nessas situações (RUEGAMER; KOWALEWSKI, 2015).

4.1.3. Casos reais

Com a recente popularização dos *jammers* ao rendo do mundo, o número de incidentes com esses equipamentos vem aumentando. Em muitos casos, o próprio usuário se utiliza desta ferramenta para beneficio próprio, como desligar o sistema de anti-furto de um carro ou burlar os sistemas de cobrança automática são cada vez mais comuns.

No ambiente naval, foram observados casos de uso de *jammers* para que embarcações não sejam detectadas pelas autoridades portuárias ou para forçar o desligamento do AIS (*Automatic Identification System*), de uso obrigatório nas embarcações civis. O trabalho de COFFED (2014) descreve alguns incidentes envolvendo o uso *jammer* nos EUA.

4.1.3.1. Incidente em San Diego

Em janeiro de 2007, os serviços de GPS foram significativamente interrompidos em toda San Diego, Califórnia (Figura 13). Impactos foram relatados no Centro Médico Naval, onde os pagers de emergência pararam de funcionar, no porto, o sistema de gerenciamento de tráfego aquaviário falhou, o controle de tráfego do aeroporto foi obrigado a usar sistemas de *backup* e o fluxo de aeronaves. Demorou três dias para se encontrar uma explicação para este evento misterioso: dois navios da Marinha estavam nas proximidades do porto de San Diego, realizando exercícios envolvendo *jammers*. Sem querer, eles também bloquearam sinais de GPS através de uma ampla faixa da cidade.

Figura 12: Áreas afetadas pelo exercício

Fonte: COFFED (2014)

4.1.3.2. Incidente no aeroporto de Newark

Em agosto de 2013, a administração federal de aviação multou em Readington, Nova Jersey, um homem em quase US$32.000,00 após concluir que ele interferiu no sistema de rastreamento de aeronaves do Aeroporto Internacional Newark Liberty, usando um dispositivo ilegal de interferência GPS em sua caminhonete para ocultar sua localização de seu empregador. Os sinais que emanaram do veículo bloquearam a recepção dos sinais GPS utilizados pelo sistema de controle do tráfego aéreo. Em outro incidente no final de 2009, engenheiros notaram que os receptores GPS que eram usados para auxiliar a navegação no aeroporto perdiam sinal durante certas horas do dia. A administração federal de aviação nos EUA investigou o problema e depois de dois meses descobriu que um motorista de caminhão local tinha instalado um *jammer* em seu veiculo.

4.2. *Spoofing*

Como foi visto no ultimo tópico, quando um atacante usa um *jammer*, o mesmo intenciona interromper a comunicação entre os satélites e o receptor alvo, e como conseqüência, acaba denunciando seu ataque.

Para empregar o princípio de descrição durante um ataque eletrônico em um sistema de GPS, o *spoofing* torna-se um ataque mais sofisticado e danoso que o *jamming*, gerando uma falsa posição para o usuário (JAFARNIA-JAHROMI et al., 2012).

Devido às recentes inovações tecnológicas nessa área, os *spoofers* modernos que se utilizam da tecnologia de rádios definidos por *software*, estão ficando mais baratos, flexíveis e temidos. Dessa forma, o *spoofing* está ganhando cada vez mais notoriedade justamente pelo fato do alvo muitas vezes não se dar conta que seu equipamento está sendo atacado (JAFARNIA-JAHROMI et al., 2012).

O objetivo principal de um *spoofer* é fazer com que o receptor GPS deixe de acompanhar os sinais emitidos pelos satélites e comece a acompanhar o sinal corrompido. A obra de HUMPHREYS et al. (2008) divide os tipos de ataque em três, de acordo com a complexidade: simples, intermediário e sofisticados.

Figura 13: Ilustração de um Simulador GPS (ataque simples) à esquerda, receptor-*spoofer* (ataque intermediário) no centro e um conjunto de receptores-*spoofers* (ataque sofisticado) à direita

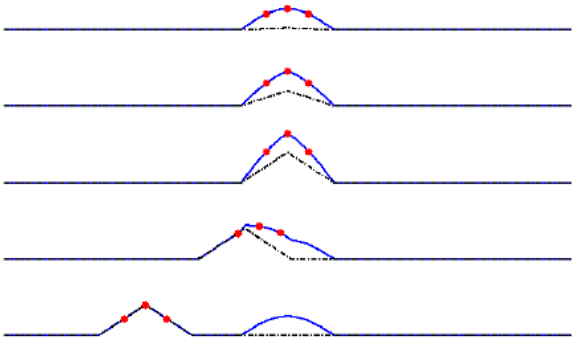
Fonte: HUMPHREYS et al. (2008)

4.2.1. Ataque simples via Simulador GPS

Grande parte dos usuários GPS se utilizam de receptores simples, sem qualquer tipo de defesa contra *jamming* ou *spoofing*. Nesse cenário, o simulador GPS pode ser eficazmente empregado como *spoofer*. Esse equipamento é composto basicamente por um gerador/amplificador de sinais e uma antena, onde os sinais são gerados e posteriormente emitidos contra um alvo (HUMPHREYS et al., 2008).

As ondas geradas pelo simulador possuem as mesmas características dos sinais emitidos pelos satélites, com a diferença de não estarem sincronizados e de possuírem uma potência mais elevada. Como pode ser visto na figura 15, o sinal *spoofer* altera constantemente a fase de seu sinal com o intuito de sobrepor o sinal verdadeiro. Feito isso, o receptor GPS terá boa probabilidade de passar a acompanhar o sinal do *spoofer*, e o ataque será bem sucedido.

Figura 14: Um ataque com simulador visto do receptor GPS. O equipamento deixa de acompanhar o sinal verdadeiro (em azul claro) e passa a acompanhar o sinal corrompido (em azul escuro)



Fonte: Psiaki e Humphreys (2016)

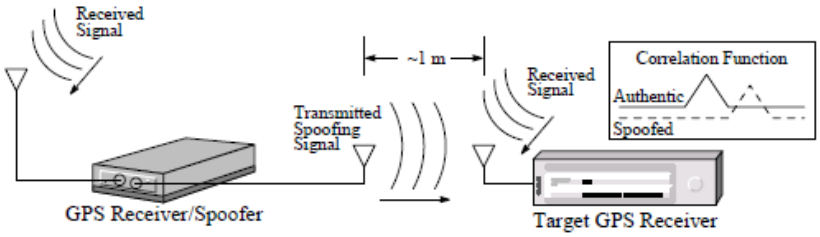
A falta de sincronia é a grande fragilidade deste ataque, pois numa primeira vista os sinais dessincronizados vão atuar "jammeando" ao alvo. Isso pode forçar o receptor a realizar uma reaquisição, parcial ou completa, de sincronismo, sinalizando ao receptor que o mesmo pode estar sendo alvo de um ataque (JAFARNIA-JAHROMI et al., 2012).

Em suma, o simulador pode ser visto como o mais importante devido a sua baixa complexidade de implementação e, por conseqüência, maior probabilidade de incidência. Assim como a relativa simplicidade deste ataque viabiliza seu uso em larga escala, essa mesma característica possibilita que uma serie de técnicas anti-*spoofing* sejam empregadas.

4.2.2. Ataques intermediários via Receptor-*Spoofer* Portátil

O uso de um receptor-*spoofer*, comumente chamado de *meaconer* na literatura estrangeira, fez com que os ataques se tornassem mais inteligentes, eficazes e mais difíceis de serem detectados. O *meaconer* funciona extraindo informações de posição, velocidade e tempo do alvo, gerando assim um sinal mais fidedigno (RUEGAMER; KOWALEWSKI, 2015).

Figura 15: Ataque usando um meaconer



Fonte: HUMPHREYS et al. (2008)

Um ataque com receptor-*spoofer* bem empregado consiste no aumento gradual de potência do equipamento, de modo que sutilmente o receptor algo comece a acompanhar o sinal falso sem levantar suspeitas (RUEGAMER; KOWALEWSKI, 2015). Vale ressaltar que um *meaconer* competente deve ter sua potencia final levemente superior que a potencia usual recebida pelo alvo, do contrario correrá o risco do ataque ser ineficaz e de ser descoberto (JAFARNIA-JAHROMI et al., 2012).

Até o momento, não se tem noticias de um receptor-*spoofer* portátil disponível no comércio, o que torna os ataques desse tipo menos comuns. A dificuldade em alinhar a freqüência e fase da portadora com os sinais verdadeiros e minimizar o efeito de auto-*jamming* são alguns desafios dessa tecnologia (JAFARNIA-JAHROMI et al., 2012).

4.2.3. Ataques sofisticados por múltiplos receptores-*spoofers* casados em fase

O princípio de funcionamento deste ataque é o mesmo do anterior, com a vantagem que é possível simular com maior fidelidade o domínio espacial de sinais, elevando de forma considerável a dificuldade de implementação e a probabilidade de detecção por parte de um receptor convencional (RUEGAMER; KOWALEWSKI, 2015).

Para que funcione, é necessário que se saiba, com a precisão de centímetros, a posição do receptor, de modo que seja possível sincronizar o código e fase da portadora dos sinais falsos com os códigos verdadeiros no receptor. Devido a todos esses requisitos, a região de eficácia desse tipo de ataque é bem mais reduzida, e a sincronização pode ser possível apenas por um período curto de tempo. Há também dificuldades físicas, onde a posição geométrica e movimentação do receptor em relação aos receptores-*spoofers* impossibilitam a aplicação deste método (JAFARNIA-JAHROMI et al., 2012).

4.2.4. Casos reais

Devido ao acesso ainda restrito à *spoofers*, os principais incidentes que têm sido observados ao redor do mundo giram em torno de entidades governamentais com maior capacidade bélica. Os casos relatados a seguir mostram o perigoso potencial deste tipo de ataque, que pode causar sérios transtornos para a navegação aérea e naval, podendo também

ser usado como importante ferramenta em conflitos armados, interferindo na guiagem de mísseis, na operação de drones e no comando e controle de meios.

4.2.4.1. O incidente RQ-170

O uso de veículos aéreos não embarcados pelo governo do EUA vem sendo cada vez mais comuns para as mais diversas ações. CYBER... (2014) relata um caso que ocorreu em 4 de dezembro de 2011, quando um drone modelo RQ-170 pousou indevidamente em solo iraniano. Autoridades do Irã assumiram a responsabilidade de pelo ocorrido, anunciando que assumiram o controle do drone norte-americano com sucesso.

Figura 16: Foto tirada por militares iranianos do drone capturado

Fonte: CYBER... (2014)

O que se sabia das ferramentas de guerra eletrônica do Irã, no que tange o GPS, era que o mesmo possuía a capacidade de jammear receptores, mas nada havia indicado que já se possuía a tecnologia para um *spoofing* sofisticado. Segundo fontes iranianas, o ataque ao RQ-170 se iniciou com *jammers*, para que o drone perdesse contato com a estação de controle norte-americana, seguido do *spoofing*, permitindo que forças iranianas assumissem o controle da navegação do meio.

4.2.4.2. Incidente no Mar Negro

Em 22 de junho de 2017, a Administração Marítima dos EUA fez um relatório de incidente aparentemente sem relevância. O mestre de um navio fora do porto russo de Novorossiysk notou que seu GPS apontava o local errado, indicando que o mesmo estava no Aeroporto Gelendzhik, a mais de 32 quilômetros de distância. Depois de verificar que seu equipamento GPS estava funcionando corretamente, o mestre da embarcação contatou os

navios próximos, sendo o AIS de todos eles apontando para o mesmo aeroporto (SHIPS... 2017).

Esse caso não é o primeiro a ser observado na Rússia, sendo relatado que ataques de *spoofing* estavam causando transtornos no centro de Moscou. O tema só ganhou a atenção devida, quando os usuários do aplicativo PokemonGo – febre entre os anos de 2016 e 2017 – relataram posições equivocadas em seus *smartphones*. O sinal falso aparentou estar centrado no Kremlin, reposicionando muitos usuários do centro de Moscou para as proximidades do Aeroporto de Vnukovo, 32 quilômetros distante. O que se acredita é que a Rússia esteja testando uma nova forma de guerra eletrônica, provavelmente para tentar se proteger de mísseis, bombas e drones guiados via GPS (SHIPS... 2017).

5. MEDIDAS DE PROTEÇÃO ELETRÔNICA PARA GPS

Uma vez apresentadas as ameaças a que estão sujeitos os meios navais, aeronavais e fuzileiros navais da MB que utilizam o GPS, faz-se necessário o emprego de algumas técnicas para que o serviço de localização por satélites não seja interrompido, e as missões assumidas pela MB não sejam prejudicas. O nível de sofisticação necessário para mitigar um ataque é diretamente proporcional à dificuldade de implementação do mesmo, sendo que um ataque efetuado por um conjunto de receptores-*spoofers* é bem mais difícil de ser evitado se for comparado com um *jamming*, por exemplo.

O presente capítulo discorrerá sobre algumas soluções para os ataques citados no capitulo anterior, sendo que as técnicas apresentadas podem ser eficazes ou não a um determinado tipo de ataque, dependendo também de fatores externos como em qual local se está usando o equipamento e como estão posicionados o atacante e o receptor, por exemplo.

5.1. MPE para *Jamming*

Sendo o ataque mais tradicional e popular, o desenvolvimento de técnicas para mitigar os efeitos de interferências intencionais e não intencionais é fundamental para a operação do GPS. Apesar de ilegal em inúmeros países, os relatos do uso de *jammer*s, no âmbito civil e militar, continuam sendo frequentes, podendo-se afirmar ainda hoje as MPE referentes a *jamming* são as mais importantes.

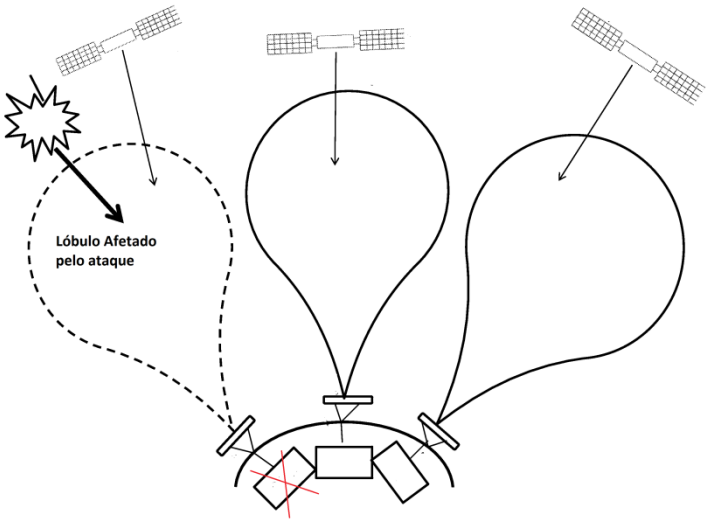
A obra de RUEGAMER; Kowalewski (2015) sugere uma serie de técnicas para proteger os receptores, e são classificas de acordo com o local de atuação dentro do equipamento: antenas, *front-end* e pré/pós correlação do receptor.

5.1.1. Técnicas de Antenas

Um equipamento GPS simples é formado de apenas uma antena, o que torna seu padrão de irradiação previsível e propicia a ação de *jammer*s. Para solucionar esse problema, um conjunto de antenas pode ser empregado de forma a alterar esse padrão, fazendo que com o receptor esteja disponível apenas numa determinada direção. Para isso, são empregadas de

duas a sete antenas, que são coordenadas para alterar continuamente o padrão de radiação e reduzir o efeito de um *jammers* numa determinada direção. A figura 17 mostra como um conjunto de três antenas pode ser usado para atenuar um sinal falso.

Figura 17: Um conjunto de antenas

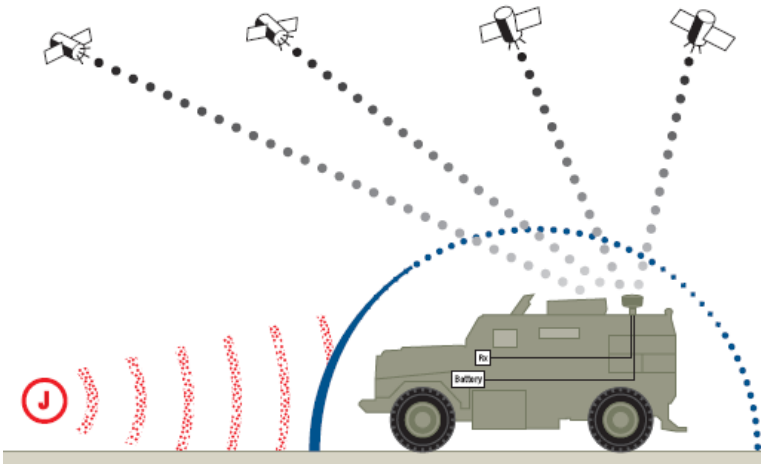


Fonte: o autor

Outra vantagem significativa do conjunto de antenas é a possibilidade de não só mitigar o *jamming*, mas também de melhorar a qualidade dos sinais recebidos. Isso pode ser feito aumentando o ganho em determinadas direções, onde se espera receber sinais do segmento espacial, ao mesmo que tempo que se atenuam os sinais emanados de fontes indesejáveis.

Para que essa técnica seja efetiva, são necessários algoritmos que irão coordenar as antenas, sendo que estes variam de acordo com a aplicação. Quando é desejado um aumento de ganho numa determinada direção, ao passo que se atenuam marcações indesejadas, o algoritmo de formação de feixe é o indicado. Caso o único objetivo seja a supressão de sinais maliciosos assim que são interceptados, opta-se pelo algoritmo de apontamento nulo. Existem ainda algoritmos que são empregados com a única finalidade de detectar a direção de chegada de sinais verdadeiros, bem como de sinais danosos. A figura 18 ilustra o uso do conjunto de antenas de forma a atenuar os sinais advindos da frente do veiculo, ao passo que os sinais dos satélites não sofrem danos.

Figura 18: Conjunto de antenas usados para gerar um apontamento nulo na parte da frente do veículo



Fonte: THIEL e Ammann (2009)

5.1.2. Técnicas de *Front-end*

Um equipamento GPS é composto basicamente por antenas, que captam o sinal e enviam para a unidade de processamento de sinal, composta por conversores analógico-digitais (A/D), amplificadores, filtros, dentre outros. O responsável por conectar a unidade de recepção com as unidades de processamento é chamado de *Front-end*, e através do controle de ganho automático deste componente, pode-se detectar sinais cuja potência está muito acima do esperado para um sinal GPS.

Quando não há a presença de interferência, as amostras do conversor A/D seguem uma distribuição normal, e consequentemente com um simples teste de distribuição normal é possível identificar sinais maliciosos. Detecções de frequência-tempo usando a Transformada de Fourier para tempos curtos e técnicas baseadas em sensibilidade de compressão são outras opções para detectar sinais atípicos.

5.1.3. Técnicas de pré e pós correlação no receptor

Todas as técnicas aplicadas antes do correlator e do *tracking loop* são ditas de pré-correlação. Filtragem, eclipsamento de pulso e apontamento nulo são alguns exemplos dessas técnicas. Se o objetivo for o descarte de sinais que possuem uma potência superior a um dado limiar, pode-se utilizar a técnica de eclipsamento de pulso, onde, além de eliminar sinais de

potencia elevada, também são eliminados sinais cujos períodos são mais curtos que um valor mínimo pré estabelecido.

No caso de *jammers* que se utilizam de sinais CW, tipo mais comum encontrado no comércio, filtros no domínio do tempo, como o rejeita faixa adaptativo, ou filtros no domínio da frequência, como o FDAF (*Frequency Domain Adaptive Filter*) são ferramentas eficazes. No caso da FDAF, os sinais recebidos são vistos no domínio da frequência com o uso da Transformada Rápida de Fourier (FFT – *Fast Fourier Transform*), onde a amplitude de certas frequências está fora do esperado para um sinal GPS e logo os sinais referentes a essas frequências são descartados. A FDAF é bastante eficiente quando se quer evitar fontes não estacionárias, porém é computacionalmente complexo e pode sofrer de um efeito chamado de vazamento de FFT.

Já no caso de técnicas pós-correlatas, é possível o tratamento de cada sinal de forma individual. Como os sinais de *jammers* não são parecidos com os sinais GPS, essas técnicas ficam restritas ao processamento da forma de feixe.

5.2. MPE para *Spoofing*

Levando em consideração os desafios enfrentados pela MB, o conhecimento e implementação de técnicas efetivas contra *jamming* são mandatórias, até porque a facilidade de obtenção de um *jammer* faz com que essa ameaça esteja sempre presente. Já o *spoofing* é uma ameaça silenciosa, que aos poucos está ganhando relevância, sendo importante o conhecimento de como mitigar esse tipo de ataque. A defesa por sinal vestigial, técnicas de antenas e RAIM (*Receiver Autonomous Integrity Monitoring*) são opções que podem ser usadas como medidas de proteção eletrônica em se tratando de *spoofing*.

5.2.1. Defesa por sinal vestigial

O objetivo de um *spoofing* é a supressão completa do sinal original, no entanto isso é bem improvável, e na prática o que se observa é a detecção de aos menos um vestígio

dos sinais oriundos dos satélites e, com a ajuda de técnicas de definição por software, pode-se usar esse fato para proteger o receptor (HUMPHREYS et al., 2008)

Primeiro, o receptor copia os dados de entrada digitalizados do *front-end* no buffer de memória. Em segundo lugar, o receptor seleciona um dos sinais de GPS sendo rastreados e remove a versão regenerada do sinal local, do sinal no buffer. Por fim, o receptor realiza a aquisição para o mesmo sinal que está gravado no buffer (JAFARNIA-JAHROMI et al., 2012). A implementação da detecção de sinal residual aumenta a complexidade de *hardware* e processamento dos receptores porque esta técnica requer canais de rastreamento adicionais para rastrear sinais autênticos e de *spoofing*.

5.2.2. Técnicas de antenas

Assim como no *jamming*, caso seja identificado a direção da interferência, o receptor pode realizar técnicas de antenas para que os ganhos naquela direção sejam atenuados. Para evitar o aumento do custo de *hardware*, é possível empregar um técnica com apenas duas antenas. Este é um método que correlaciona de forma cruzada os sinais recebidos de diferentes antenas e extrai a assinatura espacial dos sinais de *spoofing* com base na sua dominância de potência espacial (RUEGAMER; KOWALEWSKI, 2015).

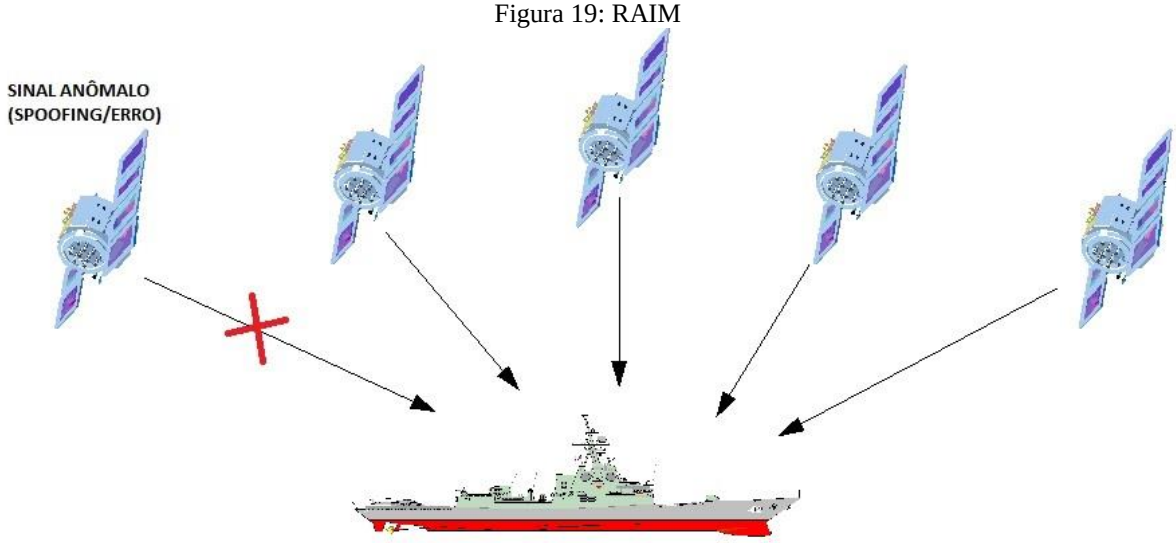
Assumindo que o módulo de *spoofer* transmite vários sinais, cada um com um nível de potência comparável aos autênticos, o vetor de direção correspondente aos sinais de *spoofing* pode ser extraído porque todos os sinais de *spoofing* estão vindo da mesma direção. Este método não precisa de ajustes no ganho ou qualquer outra informação anterior a respeito da orientação do conjunto de antenas e pode ser empregada como um bloco de antenas alinhadas que atenuam os sinais de *spoofing* antes de entrar nos receptores de GPS convencionais (JAFARNIA-JAHROMI et al., 2012).

5.2.3. RAIM

Sinais de *Spoofing* efetivamente injetam pseudodistâncias falsas nas medições do receptor. Estas medições podem não ser consistentes e, consequentemente, não levam a uma solução de posição razoável. Existem receptores GPS que realizam a monitoração da

integridade das medições, a fim de detectar e rejeitar as medições falsas ou erros; essa técnica é conhecida como monitoramento da integridade autônoma do receptor ou RAIM (JAFARNIA-JAHROMI et al., 2012). Na figura 19 é ilustrado como o receptor GPS descartaria um sinal destoante tendo a disponibilidade de cinco satélites.

Figura 19: RAIM



Fonte: o autor

As técnicas de RAIM podem ser empregadas como técnicas úteis de *antispoofing* no nível da solução de posição. No entanto, esses métodos são eficazes somente nos casos em que apenas uma ou duas fontes de *spoofing* estão presentes entre várias fontes autênticas, caso contrário, as medidas falsificadas ficam em maioria e a técnica de RAIM poderá ter efeito inverso (JAFARNIA-JAHROMI et al., 2012).

6. CONCLUSÃO

Com base no que foi abordado neste trabalho, é possível ter uma dimensão da problemática que gira em torno dos ataques ao GPS, sendo que a MB não pode desconsiderar os risco inerentes à uma eventual indisponibilidade desse equipamento.

Feita a ambientação e justificativa do porque este tema está sendo tratado dentro de um trabalho de conclusão de curso em GE, o capitulo três se fez essencial, pois sem saber como funciona o sistema GPS fica notadamente mais complexa a compreensão dos ataques apresentados no capitulo quatro.

Através do relato de casos reais, pôde-se perceber a importância de conhecer como funciona cada tipo de ataque, para que, caso ocorra algum dos tipos de ataques citados, este possa ser percebido e, numa situação ideal, possa também ser efetivamente combatido.

Por fim, pôde-se afirmar que os principais ataques a GPS foram apresentados de uma forma intuitiva e direta, bem como as técnicas que podem ser implementadas para proteger o GPS, fazendo com que o objetivo principal desta obra fosse satisfatoriamente alcançado.

6.1.Considerações finais

Conforme mencionado na introdução, não foi possível abordar outros tipos de ataques, a citar principalmente o cibernético, sendo importante salientar que esta obra não esgota todas as possibilidades de ataques existentes. Também vale ressaltar que existem MPE que não foram mencionadas por se considerar suficientes as medidas elencadas, e a inclusão de mais medidas afetaria a compreensão e aplicação deste trabalho.

6.2.Sugestões para trabalhos futuros

O que se espera é que, após a publicação deste trabalho, possam ser iniciadas linhas de pesquisa que terão como objetivo o desenvolvimento de equipamentos de MPE acoplados ao GPS nos meios navais da MB. A partir deste trabalho introdutório, sugere-se para trabalhos futuros a abordagem específica de cada tipo de receptor GPS, apresentando os

ataques mais eficazes dado o equipamento em uso e consequentemente sugerindo a melhor forma de protegê-lo.

REFERÊNCIAS

AIAA - AMERICAN INSTITUTE OF AERONAUTICS AND ASTRONAUTICS. **History of the GPS Program.** 2011. Disponível em: <https://www.aiaa.org/uploadedFiles/About_AIAA/Press_Room/Videos/IAF-60th-Anniv-GPS-Nomination.pdf>. Acesso em: 17 mar. 2018.

AEROSPACE. **TRANSIT:** THE GPS FOREFATHER. 2010. Disponível em: <http://www.aerospace.org/crosslinkmag/spring-2010/transit-the-gps-forefather/>. Acesso em: 18 mar. 2018.

ALBUQUERQUE, P. C. G.; SANTOS, C. C. GPS PARA INICIANTES. In: MINI CURSO - XI SIMPÓSIO BRASILEIRO DE SENSORIAMENTO. 2003, Belo Horizonte. **Anais... .** Belo Horizonte: Instituto Nacional de Pesquisas Espaciais, 2003. p. 1 - 46. Disponível em: <http://mtcm12.sid.inpe.br/col/sid.inpe.br/jeferson/2003/06.02.09.16/doc/publicacao.pdf>. Acesso em: 17 fev. 2018.

BEARD, R. **GPS, The Early Years, A Naval Perspective.** Washington, D.c.: U. S. Naval Research Laboratory, 2013. 17 slides, color. Disponível em: <ftp://tycho.usno.navy.mil/pub/TimeAndNavigation/GPS_Navy_Perspective_Ron.Beard.pdf>. Acesso em: 18 mar. 2018.

BENTO, C. N. S. **VULNERABILIDADES DA NAVEGAÇÃO POR SATÉLITES.** Disponível em: <http://www.e-nav.net/VULNERABILIDADES DA NAVEGAÇÃO POR SATÉLITES.pdf>. Acesso em: 09 abr. 2018.

COFFED, J. The Threat of GPS Jamming. **Exelis**, [s. L.], p.1-16, jan. 2014. Disponível em: <http://gpsworld.com/wp-content/uploads/2014/02/ThreatOfGPSJamming_FEB14.pdf>. Acesso em: 22 abr. 2018.

CYBER in the Sky – RQ-170 Incident. 2014. Disponível em: <https://blog.sensecy.com/2014/02/27/cyber-in-the-sky-rq-170-incident/>. Acesso em: 24 abr. 2018.

GOMES, T. S. **Fundamentos de GPS:** Conceitos, Operação e Configuração. Brasília: Secretaria Especial de Agricultura Famliar, 2010. Disponível em: <http://www.mda.gov.br/sitemda/sites/sitemda/files/user_arquivos_383/Apostila de GPS - Curso Sig@livre Sistêmico.pdf>. Acesso em: 20 mar. 2018.

HUMPHREYS, T. E. et al. Assessing the spoofng threat: development of a portable gps civilian spoofer. **Proceedings Of The 21st International Technical Meeting Of The Satellite Division Of The Institute Of Navigation (ion Gnss '08)**, Savannah, Ga, Usa, p.2314-2325, set. 2008. Disponível em: <https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf>. Acesso em: 14 abr. 2018.

JAFARNIA-JAHROMI, Ali et al. GPS Vulnerability to *Spoofing* Threats and a Review of Anti*spoofing* Techniques. **International Journal Of Navigation And Observation**, [s.l.], v. 2012, p.1-16, 2012. Hindawi Limited.

KAPLAN, E. D.; HEGARTY, C. J. **Understanding GPS:** Principles and Applications. 2. ed. Norwood, Ma: Artech House, 2006.

MATTOS, T. S. **Sistema de Posicionamento por Satélite.** [s. L.]: Sulgas, 2012. 43 slides, color. Disponível em: <http://sulgas.usuarios.rdc.puc-rio.br/Empreendimento/GPS_1C.pdf>. Acesso em: 21 fev. 2018.

MB: Marinha do Brasil. EMA-305 – Doutrina Militar Naval. Rio de Janeiro, 2017.
PSIAKI, M. L.; HUMPHREYS, T. E. GNSS *Spoofing* and Detection. **Proceedings Of The Ieee**, [s.l.], v. 104, n. 6, p.1258-1270, jun. 2016. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/jproc.2016.2526658.

RIBEIRO, M. J.O. Sistemas de Navegação. **SIAUT**, Cidade do Porto, p.1-11, nov. 2002. Disponível em: <http://ave.dee.isep.ipp.pt/~mjf/act_lect/SIAUT/Trabalhos 2007-08/Trabalhos/SIAUT_Navegacao.pdf>. Acesso em: 21 fev. 2018.

ROSA, R. **INTRODUÇÃO AO GEOPROCESSAMENTO.** Uberlândia: Universidade Federal de Uberlândia, 2013. Disponível em:

<http://professor.ufabc.edu.br/~flavia.feitosa/cursos/geo2016/AULA5-ELEMENTOSMAPA/Apostila_Geop_rrosa.pdf>. Acesso em: 22 mar. 2018.

RUEGAMER, A.; KOWALEWSKI, D. Jamming and *Spoofing* of GNSS Signals – An Underestimated Risk?! In: WISDOM OF THE AGES TO THE CHALLENGES OF THE MODERN WORLD, 7486., 2015, Sofia, Bulgaria. **Anais... .** Sofia, Bulgaria: Navxperience Gmbh, 2015. p. 1 - 21. Disponível em: <https://www.fig.net/resources/proceedings/fig_proceedings/fig2015/papers/ts05g/TS05G_ruegamer_kowalewski_7486.pdf>. Acesso em: 09 abr. 2018.

SHIPS fooled in GPS spoofng attack suggest Russian cyberweapon. 2017. Disponível em: <https://www.newscientist.com/article/2143499-ships-fooled-in-gps-*spoofing*-attack-suggest-russian-cyberweapon/>. Acesso em: 24 abr. 2018.

SOUSA, C. R. M. **Interferidores de GPS:** análise do sistema e de potenciais fontes de interferência. 2005. 90 f. Dissertação (Mestrado em Ciências de Engenharia Elétrica) - Instituto Militar de Engenharia, Rio de Janeiro, 2005.

STURDEVANT, R. W. NAVSTAR, the Global Positioning System: A Sampling of Its Military, Civil, and Commercial Impact. In: DICK, Steven J.. **Societal Impact of SPACEFLIGHT.** Washington: Government Printing Office, 2007. p. 332-351. Disponível em: <https://history.nasa.gov/sp4801-chapter17.pdf>. Acesso em: 19 mar. 2018.

THIEL, A.; AMMANN, M. **Anti-Jamming techniques in u-blox GPS receivers.** 2009. Disponível em: <https://www.u-blox.com/sites/default/files/products/documents/u-blox-AntiJamming_WhitePaper_(GPS-X-09008).pdf>. Acesso em: 27 abr. 2018.

WINTERNITZ, L. **Introduction to GPS and other Global Navigation Satellite Systems.** Boulder Co: Nasa, 2017. Disponível em: <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20170004590.pdf>. Acesso em: 20 mar. 2018.