Universidade de São Paulo – USP

Escola de Engenharia de São Carlos – EESC
Departamento de Engenharia Elétrica
Trabalho de Conclusão de Curso

IDENTIFICAÇÃO DE ATAQUES A VEÍCULOS AÉREOS NÃO TRIPULADOS VIA RECEPTORES GPS E PROPOSTA DE CONTRAMEDIDAS PARA AUMENTO DA SEGURANÇA DA AERONAVE

Aluno

Amir Nasser Safa Ahmad

Orientadora

Prof. Dra. Kalinka Regina Lucas Jaquie Castelo Branco

São Carlos, 2015

Amir Nasser Safa Ahmad

IDENTIFICAÇÃO DE ATAQUES A VEÍCULOS AÉREOS NÃO TRIPULADOS VIA RECEPTORES GPS E PROPOSTA DE CONTRAMEDIDAS PARA AUMENTO DA SEGURANÇA DA AERONAVE

Trabalho de Conclusão de Curso apresentado à Escola de Engenharia de São Carlos da Universidade de São Paulo como parte dos requisitos para obtenção do título de Engenheiro Eletricista.

Orientador: Prof. Dra. Kalinka Regina Lucas Jaquie Castelo Branco

São Carlos

Safa Ahmad, Amir Nasser
S128i IDENTIFICAÇÃO DE ATAQUES A VEÍCULOS AÉREOS NÃO TRIPULADOS VIA RECEPTORES GPS E PROPOSTA DE CONTRAMEDIDAS PARA AUMENTO DA SEGURANÇA DA AERONAVE / Amir Nasser Safa Ahmad; orientadora Kalinka Regina Lucas Jaquie Castelo Branco. São Carlos, 2016.

Monografia (Graduação em Engenharia Elétrica com ênfase em Eletrônica) -- Escola de Engenharia de São Carlos da Universidade de São Paulo, 2016.

1. SPOOFING. 2. GPS. 3. JAMMING. I. Título.

2015

FOLHA DE APROVAÇÃO

Nome: Amir Nasser Safa Ahmad

Título: "Identificação de ataques a veículos aéreos não tripulados via receptores GPS e proposta de contramedidas para aumento da segurança da aeronave"

Trabalho de Conclusão de Curso defendido e aprovado em 26 / 02 / 2016,

com NOTA 6.0 (seis , zero), pela Comissão Julgadora:

Prof. Associada Kalinka Regina Lucas Jaquie Castelo Branco - (Orientadora - SSC/ICMC/USP)

Prof. Associado Evandro Luis Linhari Rodrigues - (SEL/EESC/USP)

Mestre Daniel Fernando Pigatto - (Doutorando - ICMC/USP)

Coordenador da CoC-Engenharia Elétrica - EESC/USP:
Prof. Dr. José Carlos de Melo Vieira Júnior

AGRADECIMENTOS

Agradeço primeiramente a minha família, pais, irmãos e namorada pelo apoio, incentivo e colaboração durante todas as fases da minha vida, incluindo a acadêmica. Agradeço também aos meus familiares e amigos que contribuíram nessa longa jornada e acompanham até hoje.

À Professora Doutora Kalinka Regina Lucas Jaquie Castelo Branco e ao Doutorando Daniel Fernando Pigatto, pela paciência, atenção e orientação ao decorrer desse projeto.

Ao Departamento de Engenharia de São Carlos e professores, por contribuírem com a minha formação em Engenharia Elétrica.

Resumo

Ahmad A. N. S. (2015). **IDENTIFICAÇÃO DE ATAQUES A VEÍCULOS AÉREOS NÃO TRIPULADOS VIA RECEPTORES GPS E PROPOSTA DE CONTRAMEDIDAS PARA AUMENTO DA SEGURANÇA DA AERONAVE.**

Trabalho de Conclusão de Curso – Escola de Engenharia de São Carlos, 2015.

Palavras-chave: Detecção de Spoofing GPS, Segurança do Sistema GPS, Contramedida para Spoofing GPS

Este trabalho apresenta o funcionamento detalhado do sistema GPS, as vulnerabilidades e as defesas existentes. E a partir de análises e estudos, construir uma possível solução ainda não implementada para o *Spoofing*. Foi implementado um sistema de detecção para o *Spoofing* GPS via software em um *Tablet*, o qual detectou o ataque com eficácia ao obter os dados *spoofados*.

Abstract

This paper presents the detailed operation of the GPS system, vulnerabilities and existing defenses. And from analysis and studies , presenting a possible solution not yet implemented for the Spoofing. A detection system for GPS Spoofing was implemented in software on a Tablet, which detected the attack effectively to get the spoofed data.

Índice de figuras

Sumário

1 INTRODUÇÃO

O Sistema de Posicionamento Global (GPS, Global Positioning System) criado pelos Estados Unidos da América, durante a Guerra Fria, tornou-se funcional em 1995. Porém o seu uso popularizou-se em 2000, quando o governo americano acabou com a degradação proposital do sinal. A partir disso, todos os ramos passaram a usar esse sistema, capaz de fornecer velocidade, localização e tempo, com alta precisão.

Com a revolução tecnológica, os mapas impressos deixaram de ser usados e praticamente a maioria dos veículos tem um sistema de localização, seja para seguir uma rota pré-definida ou um sistema de rastreamento ou monitoramento(caminhões e veículos que carregam cargas de valor).

Apesar de existirem outros provedores de localização, esse é o mais utilizado e estudado. O sistema continua sendo aperfeiçoado para conseguir desempenho e precisão maior, com a inclusão de satélites e novos sinais.

O sistema GPS é baseado no tempo. Os satélites carregam relógios atômicos sincronizados entre si e com os relógios terrestres (bases). Cada desvio de horário ou desvio na órbita do satélite que ocorre é corrigido, ambos são monitorados cuidadosamente. O receptor GPS também tem um relógio que não é sincronizado como os outros, porém é estável. Os satélites GPS continuamente transmitem o horário atual e sua posição. Um receptor GPS monitora simultaneamente múltiplos satélites e resolve equações para determinar a posição exata do receptor e o desvio do verdadeiro horário. No mínimo quatro satélites devem ser “vistos” a fim de computar quatro variáveis (3 coordenadas e o desvio do horário do satélite).

Cada satélite GPS transmite continuamente sinais (frequências portadoras modulada) que inclui:

→ Um código pseudoaleatório (PRN, sequência de 1 e 0) que é conhecido pelo receptor. Por alinhamento na coordenada do tempo, de um código recebido, com um gerado internamente, calcula-se o tempo de chegada (TOA, *time of arrival*) do sinal.

→ A mensagem inclui o horário de transmissão (TOT, t*ime of transmission*) da época do código (na escala de tempo do GPS) e a posição do satélite no momento.

Conceitualmente, o receptor mede os TOAs (de acordo com seu próprio relógio) de quatro sinais de satélite. Utilizando os TOAs e os TOTs, o receptor calcula 4 valores conhecidos como tempo de vôo, que são aproximadamente a distância entre os satélites e os receptores (calcula-se usando a velocidade da luz)[1].

Na prática a posição do receptor (em coordenadas cartesianas tridimensional com a origem no centro da Terra) e a diferença entre os relógios do receptor e do satélite, são computados simultaneamente, usando as equações de navegação.

As soluções das equações são convertidas em latitude, longitude e altura relativos a um modelo da Terra elipsoidal. A altura então pode ser convertida em relação ao nível do mar. Essas coordenadas podem ser mostradas na tela do GPS ou podem ser utilizadas para alguma outra aplicação.

Embora geralmente não seja formado explicitamente no processo de recepção do sinal, o conceito de diferentes tempos de chegada (TDOAs, time differences of arrival) define a geometria medida. Cada TDOA corresponde a um hiperboloide de revolução (multilateração). A linha que conecta 2 satélites forma um eixo da hiperboloide, o receptor é localizado no terceiro ponto onde as 3 hiperboloides se interceptam.

É incorreto dizer que o receptor sempre está na intersecção das três esferas, pois esse ponto é exato, somente se o relógio do receptor encontra-se sincronizado com o do satélite, e para isso seria necessário um relógio atômico em cada receptor, o que elevaria muito o custo do mesmo. Eis a importância do quarto satélite.

A descrição a seguir é a representação de uma situação onde o receptor acabou de ser ligado. Muitos receptores têm um algoritmo de rastreamento chamado de rastreador, que combina conjuntos de diferentes medidas obtidas dos satélites em momentos distintos, aproveitando-se do fato de que cada posição do receptor está próxima da posição seguinte e anterior. Após uma certa quantidade de conjuntos de medidas o rastreador prevê a próxima localização correspondente para o próximo conjunto de medidas dos satélites. Quando as novas medidas são coletadas, o receptor usa um esquema de ponderação para combinar as novas medições

com a previsão.

No geral, um rastreador pode:

→ Refinar a posição do receptor e a precisão do tempo.

→ Rejeitar medições ruins.

→ Estimar a velocidade do receptor e a direção do movimento.

A desvantagem de um rastreador é que a mudança de velocidade ou direção é computada com um pequeno atraso. Os receptores podem utilizar o efeito Doppler dos sinais recebidos para computar a velocidade mais precisamente. Sistemas de navegação mais avançados usam sensores adicionais como compasso e um sistema de navegação inercial (IMU) para complementar o GPS.

Em operações normais de GPS como navegador, são necessários 4 ou mais satélites visíveis para obter um resultado preciso. Porem há aplicações como temporização no tráfego do sinal e a sincronização de estações de celulares, que também utilizam o horário GPS, por ser o mais preciso do mundo.

Embora 4 satélites sejam requeridos para uma operação normal, menos satélites são utilizados em alguns casos. Se uma variável já é conhecida, um receptor pode determinar sua posição usando somente 3 satélites. Por exemplo, uma nave pode conhecer a altura em relação ao nível do mar em que se encontra. Alguns receptores GPS podem usar dados armazenados anteriormente ou de outras fontes, a fim de computar a posição atual, sem ter 4 satélites visíveis no momento.

1.1 MOTIVAÇÃO

A estrutura do sinal transmitido pelo GPS é de conhecimento público e está disponível no site das Forças Aéreas dos Estados Unidos, www.gps.gov, e é assim, para que o receptor consiga interpretá-lo. Porém isso possibilita que alguém emita esses mesmos sinais, fazendo com que receptores alheios utilizem-no para obter uma falsa posição ou informação sobre o tempo. Esse ataque é chamado de *Spoofing*[1].

Em 4 de dezembro de 2011, o RQ-170, um veículo aéreo não tripulado (VANT) americano, foi capturado pelas Forças Aéreas Iranianas próximo a cidade de Kashmar no Irã. O governo iraniano anunciou que um VANT foi aterrissado em segurança, enquanto o governo americano anunciava que o VANT havia sido abatido, e inicialmente negou ser uma nave americana, mas ao constatar que realmente era, pediu-se a devolução da mesma[1].

Fontes próximas ao governo, informavam que o VANT havia sido aterrissado por engenheiros iranianos que bloquearam os sinais GPS, deixando o VANT "cego", e após isso *spoofaram* os sinais falsos, fazendo-o descer.

Mais tarde foi reportado que o Irã havia comprado da Rússia o *Avtobaza*. um sistema terrestre de *jamming* e *spoofing*, ilustrado na imagem seguinte, e este havia sido usado para capturar o VANT.

Figura 1: Avtobaza: estação terrestre russa de jamming e spoofing

Em conhecimento dos fatos anteriores, o trabalho foi desenvolvido a fim de detectar o *spoofing*, tanto em sistemas autônomos quanto para usuários que desconhecem essa vulnerabilidade.

É importante a pesquisa de métodos de detecção de s*poofing*, pois é necessário que os VANTs identifiquem esse tipo de ameaça e tomem contramedidas em defesa própria, impedindo que pessoas má intencionadas consigam aterrissar ou até mesmo roubar o veículo.

1.2 OBJETIVO

O principal objetivo deste trabalho é apresentar a estrutura e o funcionamento do sistema GPS, muito utilizado em diversas áreas, bem como discutir suas vulnerabilidades mais conhecidas. Posteriormente será apresentado um estudo especificamente sobre a simulação de um ataque de *spoofing* de GPS em VANTs, relatando os possíveis impactos deste tipo de ataque, e o desenvolvimento de uma técnica de identificação do ataque via software.

Este trabalho ainda mostra uma solução para o ataque de spoofing de GPS implementada em software, visando impactar o mínimo possível a operação e a aerodinamicidade do VANT, viabilizando a aplicação da solução em sistemas reais.

2 SISTEMA NAVSTAR-GPS

O Sistema Navstar-GPS é um sistema, que por meio de satélites, fornece sua localização em qualquer parte do planeta. Ele foi criado e é controlado pelo Departamento de Defesa dos Estados Unidos da América, e foi projetado para ser usado pelos militares americanos, porém milhões de civis utilizam-no diariamente, tanto para fins pessoais quanto para fins comerciais.

Ele disponibiliza 24 horas por dia, em tempo real, a posição tridimensional e o horário. Qualquer pessoa com um receptor GPS pode acessar o sistema e usá-lo para descobrir suas coordenadas, independente das condições atmosféricas e meteorológicas [2].

O Sistema GPS é dividido em 3 segmentos:

1) O segmento espacial: é composto basicamente pelos satélites;

2) o segmento de controle: é controlado pelos militares dos Estados Unidos;

3) o segmento do usuário: inclui tanto os usuários militares quanto os civis e seus equipamentos.

2.1 SEGMENTO ESPACIAL

O primeiro satélite GPS foi lançado pelas Forças Aéreas dos Estados Unidos no início de 1978. Atualmente, existem 32 satélites orbitando a Terra em uma altitude em torno de 20200 quilômetros [3]. A altitude elevada dos satélites garante que suas órbitas sejam estáveis, precisas e previsíveis, e que os movimentos dos satélites através do espaço não sejam afetados pela resistência atmosférica [4].

Os satélites GPS são alimentados por painéis solares, tendo como fonte secundária baterias de níquel-cádmio. Cada satélite carrega consigo 4 relógios atômicos, e somente um deles está em uso por vez, ou seja, nunca estão sendo usados simultaneamente. Esses relógios atômicos permitem que o GPS seja o sistema que fornece o horário mais preciso do mundo [5].

Inicialmente, existiam 24 satélites orbitando 6 órbitas. Cada órbita tem inclinação de 55 graus em relação a Linha do Equador, isto é, os satélites cruzam a linha do Equador com uma inclinação de 55 graus e cada satélite tem um período orbital de 12 horas siderais, que corresponde a 11 horas e 58 minutos [3], portanto a cada 12 horas cada satélite passa sobre quase o mesmo lugar.

As órbitas foram dispostas de tal maneira que, pelo menos, seis satélites estão sempre na linha de visão de quase toda a superfície da Terra, ele foi projetado para estar completamente operacional mesmo se 2 dos 24 satélites falharem. O resultado disso foi que os satélites não estão igualmente espaçados. Em termos gerais a diferença angular entre os satélites numa mesma órbita é de 30, 105, 120 e 105 graus, que somando resulta em 360 graus [6].

A constelação GPS é uma mistura de satélites novos e antigos, e atualmente conta com 32 satélites, sem incluir os satélites antigos que estão desativados, porém podem ser reativados em caso de falha de algum outro. A adição dos novos satélites aumentou a precisão do sistema com medidas redundantes e as disposições dos satélites deixaram de ser uniformes. Hoje em dia é possível observar de 5 a 9 satélites de qualquer parte do planeta sendo que o mínimo para a obtenção da posição é de 4 satélites [4].

Os dados de navegação transmitidos pelo satélite GPS, codificam uma variedade de

informações incluindo a posição dos satélites, o estado dos relógios internos, e o estado da rede. Estes sinais são transmitidos em duas frequências portadores diferentes que são comuns para todos os satélites da constelação. Duas codificações são usadas: uma pública para navegação e uma criptografada que é usada pelos militares dos Estados Unidos e seus aliados.

2.1.1 FREQUÊNCIAS DOS SATÉLITES

Todos os satélites emitem nas 2 mesmas frequências, 1575,42 MHz (sinal L1) e 1227,6 MHz (sinal L2). A constelação de satélites utiliza a técnica de espalhamento espectral CDMA, onde os dados de navegação são codificados junto com uma sequência pseudoaleatória (Código PRN), que é diferente para cada satélite. O receptor deve saber qual código PRN corresponde a qual satélite para reconstruir os dados transmitidos. O código de curso/aquisição (A/C ou *course/aquisition*), para uso civil, transmite dados a uma velocidade de 1.023.000 bits por segundo, enquanto o código de precisão(P) transmite a uma velocidade 10 vezes maior. A atual frequência interna dos satélites é de 10,22999999543 MHz para compensar os efeitos relativísticos que fazem os observadores na Terra terem uma referência de tempo diferente comparado ao dos transmissores em órbita [7][8].

A portadora L1 é modulada por ambos os códigos C/A e P, enquanto a portadora L2 é somente modulada pelo código P [6]. O código P é criptografado, eis o nome código P(Y), que somente é disponível para quem tem o equipamento com a chave de decriptografia. Ambos os códigos, C/A e P(Y), transmitem a hora exata do dia para o usuário.

O sinal L3 na frequência de 1.381,05 MHz é usado para transmitir dados dos satélites para as estações terrestres. Esses dados são usados pelo Sistema de Detecção de Detonação Nuclear dos Estados Unidos para detectar, localizar e reportar detonações nucleares na atmosfera terrestre e próximas ao espaço [9].

O sinal L4 na frequência de 13.799,14 MHz está sendo estudado para ser usado como correção adicional dos efeitos da ionosfera [5].

O sinal L2C na frequência de 1.227,6 MHz, foi projetado para fins comerciais. Seu nome faz referencia ao sinal L2. Quando combinado L2C com L1 C/A em um receptor de 2

frequências, o L2C possibilitará a correção ionosférica, aumentando a precisão, ou seja, os civis com esse tipo de equipamento, poderão desfrutar da mesma precisão dos militares (ou até melhor). O sinal L2C é transmitido com maior energia, possibilitando que a aquisição dele seja mais fácil, até em locais fechados. É estimado que o sinal L2C gere U$5,8 bilhões até 2030 [5].

O primeiro satélite com o transmissor desse sinal foi lançado em 2005, e a partir dai, todos os satélites transmitem-no. Ele ainda encontra-se pré-operacional e deve ser utilizado pelos usuários por sua conta em risco. O sinal L2C é emitido por 17 satélites atualmente e a previsão é que ele seja emitido por 24 satélites em 2018 [5].

O sinal L5 é o terceiro sinal civil, na frequência de 1.176 MHz, e foi projetado para atender as demandas de transporte de segurança de vida ou outras aplicações de alta performance [10]. Atualmente existem 10 satélites emitindo o sinal L5, e a previsão é que para 2021 existam 24 satélites emitindo o sinal [5]. L5 é emitido numa faixa de rádio exclusiva para serviços de aviação. Ele teve um aumento na energia de transmissão, uma largura de banda maior e a codificação do sinal foi melhorada em relação ao L2 e ao L1 [5].

O futuro da aviação será a combinação do L4 com o L1 C/A para aumentar a precisão (via correção ionosférica) e maior robustez (via redundância de sinal). Será possível um usuário civil utilizar as 3 frequências civis (L1 C/A, L2C e L5) a fim de obter uma posição extremamente precisa, até mesmo em locais fechados [5].

Para os dados de navegação e o código C/A viajarem do satélite até o receptor, eles precisam modular uma frequência portadora. Nesse caso duas derivadas da frequência de 10,230MHz, a L1 (154x10,230MHz = 1.575,420MHz) e L2 (120x10,230MHz= 1.227,600 MHz) [11].

O código C/A é transmitido na frequência L1 a uma taxa de 1,023 MHz usando a modulação em fase (BPSK, *binary phase-shift keying*). O código P(Y) é transmitido em ambas as frequências utilizando a mesma modulação, porém com uma taxa de 10,230 MHz e a onda portadora está em quadratura com a portadora do sinal C/A, ou seja, deslocada de 90 graus.

Um receptor captando mais frequências, além de ser mais resistente a *jamming*, pode capturar dados redundantes, ocasionada pelas várias informações repetidas. Também é possível refinar o processo de localização utilizando a correlação dos sinais, diminuindo o efeito causado pelo atraso na ionosfera.

2.1.2 CÓDIGO DE CURSO/AQUISIÇÃO

Os códigos C/A são pseudoaleatórios (PRN, *pseudo random noise*) com um período contendo 1023 bits transmitidos a 1023 megabits por segundo resultando em um período de 1 milissegundo. Eles são combinados com a mensagem de navegação através de um OU-Exclusivo, e então são usados como sinais moduladores. O fato de serem altamente ortogonais entre si, facilita a identificação de cada satélite [1].

Eles são gerados pela combinação de 2 fluxos de bits, ambos originados por um registrador de deslocamento (LFSR, *linear-feedback shift register*) de 10 bits. Códigos diferentes são obtidos usando atrasos específicos e um dos fluxos de bits.

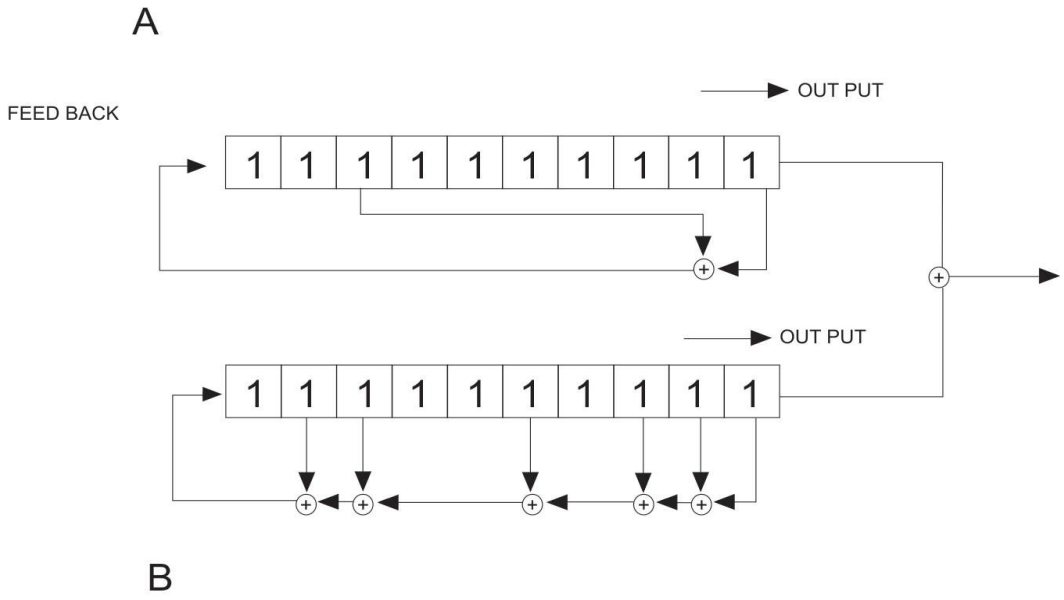

Figura 2: Gerador de PRN no instante t=0 com Di=0.

Cada conjunto de 1023 saídas do circuito acima, corresponde a um código PRN.

$$C/A(t)_i = A(t) + B(t - D_i)$$

Equação 1: Equação geradora do código PRN.

Onde:

C/A(t) é 1 bit do código C/A completo no instante t para um determinado satélite i.

A(t) é a saída do primeiro registrador de deslocamento no instante t, com estado inicial 1111111111 e polinômio gerador sendo:

$$x \rightarrow x^{10} + x^3 + 1$$

Equação 2: Polinômio gerador do registrador de deslocamento A(t).

B(t – Di) é a saída do segundo registrador de deslocamento no instante (t – Di), com o estado inicial 1111111111 e polinômio gerador sendo:

$$x \rightarrow x^{10} + x^9 + x^8 + x^6 + x^3 + x^2 + 1$$

Equação 3: Polinômio gerador do registrador de deslocamento B(t).

Di é um atraso (por um número inteiro de períodos) específico para cada PRN(1 a 32). Seu valor é apresentado no documento de especificação técnica dos satélites GPS [11].

2.1.3 CÓDIGO DE PRECISÃO

O código P é também um PRN, porém nesse caso, o código tem $61871x10^{12}$ bits, ou seja, 720,213 gigabytes, e somente repete-se uma vez por semana (10,23 Megabit por segundo). O código extremamente grande, aumenta o ganho de correlação entre os sinais e elimina algumas ambiguidades de distância. Entretanto, ele é tão longo e complexo que é esperado que um usuário comum não consiga capturar e reproduzir o sinal por si só. É necessário que o receptor utilize primeiramente o código C/A e após obter sua localização aproximada, sincronize com o código P, para refiná-la [1].

Enquanto os PRNs no código C/A são únicos para cada satélite, o PRN no código P é um pequeno fragmento do Código P Mestre com aproximadamente $2.35x10^{14}$ bits de tamanho (26.716 Terabytes). Cada satélite transmite uma parte conhecida desse código mestre.

Para prevenir que usuários não autorizados utilizem ou possam interferir com o sinal militar através de um processo chamado *spoofing*, criptografou-se o código P. Ele foi modulado com o código W, um código criptográfico especial, e gerou-se o código Y. Desde que os módulos *anti-spoofing* foram ativados, os satélites emitem o código Y, que é conhecido como código P(Y).

2.1.4 MENSAGEM/DADOS DE NAVEGAÇÃO

Além dos códigos PRN dos satélites, um receptor necessita saber informações detalhadas sobre a posição de cada satélite e da constelação. Essas informações estão moduladas em ambos os sinais e são chamadas de dados de navegação.

Os dados de navegação carregam informações que podem ser classificadas em 3 tipos:

- Dados e horário do GPS, mais o estado do satélite e a indicação de confiabilidade do satélite.
- Efemérides: informações orbitais que permite ao receptor calcular a posição do satélite. Cada satélite transmite sua própria efemérides.
- Almanaque: informações e o estado de todos os satélites.

Embora as informações das efemérides sejam altamente detalhadas, elas são válidas apenas por 4 horas, enquanto as informações de almanaque são geralmente válidas por 180 dias. O almanaque auxilia o receptor a determinar quais satélites deve escolher, e após a escolha ser feita, baixa diretamente desse satélite os dados de efemérides dele. A determinação de uma posição não é possível até que o receptor tenha uma cópia completa dos dados de efemérides do satélite. Se o sinal do satélite é perdido enquanto os dados são baixados, eles devem ser baixados novamente, descartando-se os dados incompletos [11].

Os dados de navegação são formados por 1500 bits (1 *frame*). Cada *frame* é formado por 5 *subframe*s de 300 bits, numerados de 1 a 5. Cada *subframe*, contendo 10 palavras de 30 bits, leva 6 segundos para ser transmitido. Logo 30 segundos são necessários para a transmissão de 1 *subframe*. Todo *subframe* tem o horário GPS. O *subframe* 1 contém a data GPS (Número da Semana) e informações para corrigir o horário do receptor para o horário GPS, junto com o estado e a confiabilidade do satélite. Os *subframe*s 2 e 3 juntos contêm os dados de efemérides do satélite. E os *subframe*s 4 e 5 contêm os componentes de almanaque. Porem cada *frame* contém somente 4% dos dados de almanaque (1/25), ou seja, o receptor deve capturar 25 *frame*s completos para ter os dados de almanaque completo. Com a taxa de 50 bits/s são necessários 12,5 minutos para capturar todo o almanaque se utilizando um satélite. Cada 1 das 25 versões dos *subframe*s 4 e 5 são chamados de página e são numeradas de 1 a 25. [11]

Os *frame*s iniciam e terminam, respectivamente no início ou no fim da semana somado de um múltiplo inteiro de 30 segundos. No início/fim da semana o ciclo entre as páginas é reiniciado para a página 1.

Cada *subframe* inicia com a palavra de Telemetria (TLM, telemetry word), que permite ao receptor detectar o início do *subframe* e determinar em qual horário do relógio do receptor o *subframe* inicia. A palavra seguinte é a palavra de *Handover* (HOW, *handover word*), que transmite o Horário GPS (na verdade o horário quando será transmitido o primeiro bit do próximo *subframe*) e identifica o *subframe* como parte do *frame* completo [12]. As outras 8 palavras contêm os dados específicos de cada *subframe*. Cada palavra inclui 6 bits de paridade gerados usando um algoritmo baseado no código de *Hamming*, que leva em conta os 24 bits de não paridade do *frame* e 2 bits da palavra anterior.

Após o *subframe* ter sido lido e interpretado, o horário que o próximo *subframe* será enviado pode ser calculado através da correção de data do relógio e o HOW. O receptor sabe o horário do relógio dele mesmo no qual ele receberá o próximo *frame*, e a partir da detecção da palavra de Telemetria (TLM) ele consegue calcular o tempo de transito da mensagem, ou seja, quanto tempo o sinal levou para percorrer do emissor do satélite até a antena do receptor GPS, podendo-se assim calcular a pseudodistância. O receptor é capaz de calcular a pseudodistância no início de cada *subframe*, isto é, a cada 6 segundos.

2.1.4.1 HORÁRIO GPS

O Horário GPS, expresso com a resolução de 1,5 segundos, é o número da semana e o contador de tempo da semana (TOW, *time of week*) [11]. Seu ponto inicial (Semana 0, TOW 0) é definido sendo 06/01/1980 as 00:00 no fuso horário do Meridiano de Greenwich. O contador TOW é um valor variando de 0 a 403.199 cujo significado é o número de vezes que se passou 1,5 segundos desde o início da Semana GPS. Para representar TOW são necessários 19 bits. O horário GPS é uma escala de tempo contínua que não inclui os segundos bissextos, portanto o início/fim das semanas GPS podem diferir da Coordenada Universal do Tempo (UTC) de um número inteiro de segundos.

Em cada *subframe*, cada Palavra de *Handover* (HOW,) contém o contador TOW. Note que os 2 bits menos significativos podem ser seguramente omitidos, pois um HOW ocorre a cada 6 segundos nos dados de navegação, que é igual ao a resolução de truncamento do TOW [11]. Sendo assim, os 2 últimos bits do TOW podem ser omitidos.

Cada *frame* contém (*subframe* 1) os 10 bits menos significativos que corresponde ao número da semana GPS. Note que um *frame* nunca cruza a fronteira de semana GPS, ou seja, um *frame* está inteiramente dentro da semana. Sabendo que o número de semanas é zerada a cada 1.024 semanas GPS (aproximadamente a cada 19,6 anos), um receptor que calcula as datas do calendário necessita deduzir os bits da semana seguinte ou obtê-los de uma outra fonte. Um possível método é o receptor salvar a data atual em memória quando for desligar, e quando religar,

assumir que o novo número de semana truncada corresponde ao período de 1024 semanas que iniciaram na última data salva. Esse método deduz corretamente o número de semana completo se o receptor for proibido de permanecer mais de 19,6 anos desligado.

2.1.4.2 EFEMÉRIDES

Efemérides fornece a posição natural tanto de objetos astronômicos quanto de objetos artificias, como os satélites GPS, em um determinado período de tempo.

As efemérides transmitida pelos satélites, consistem em dados sobre o estado do satélite e sua localização exata. Esses dados são fornecidos no sistema de coordenadas polar esférica [11].

2.1.4.3 ALMANAQUE

O almanaque é formado por dados sobre a órbita (muito menos detalhadas que as informações de efemérides) e estado de cada satélite da constelação, um modelo ionosférico, e dados para ajustar o horário GPS com padrão (UTC). Cada quadro contém uma parte do almanaque (nos *subframe*s 4 e 5) e o almanaque completo é transmitido por um único satélite em 25 *frame*s (12,5 minutos) [13].

O almanaque é usado para muitas funções. A primeira é auxiliar o receptor a gerar uma lista dos satélites visíveis a partir da posição em que se encontra. Além de disponibilizar parâmetros para a correção do relógio, fornece uma modelagem geral para ionosfera. Ambos dados aumentam precisão da localização.

2.2 SEGMENTO DE CONTROLE

O Segmento de controle é composto por 4 elementos:

→ Uma Estação de Controle Mestre (MCS);

→ Uma Estação de Controle Mestre Reserva;

→ Quatro antenas dedicadas;

→ Seis estações de monitoramento dedicados.

O MCS pode acessar outras antenas de monitoramento das Forças Aéreas dos Estados Unidos e estações de monitoramento da Agência de Inteligência Geo Espacial dos Estados Unidos(NGA). Os satélites são rastreados por antenas das Forças Aéreas dos Estados unidos localizados no Havaí (Atol de Kwajalein), em Diego Garcia, na Ilha da Ascensão, em Colorado (Colorado Springs) e no Cabo Canaveral. Também conta com estações de monitoramento do NGA instalados na Inglaterra, na Argentina, no Equador, no Barém, na Austrália e na cidade de Washington [14].

As informações de rastreamento são enviadas a Estação de Comando das Forças Aéreas (MCS) em Colorado Springs, onde são analisadas. E através das antenas, regularmente atualiza os relógios atômicos abordo dos satélites a fim de sincronizar os nanosegundos de diferença entre eles e ajustar a efemérides do modelo orbital interno de cada satélite. As atualizações são criadas pelo Filtro de Kalman que utiliza informações das estações de monitoramento, informações sobre o clima espacial e outras variáveis [14].

As manobras dos satélites não são previstas pelas normas do GPS, então para alterar a órbita do satélite, ele deve ter o estado alterado para desativado, para que os receptores não utilizem-no. Após a manobra, a nova órbita é rastreada pelos engenheiros, os dados de efemérides são enviados ao satélite, só então é marcado como ativado e pode ser utilizado.

2.2.1 ATUALIZAÇÃO DE DADOS

Os dados dos satélites são geralmente atualizados a cada 24 horas e ficam salvas informações de até 60 dias anteriores caso haja problema na atualização regular. A atualização contém os novos dados de efemérides e de almanaque (esse atualizado menos frequentemente que aquele). O segmento de controle garante que os almanaques serão atualizados a cada 6 dias.

Os satélites emitem a cada 2 horas novos dados de efemérides, que geralmente são validos por 4 horas. O tempo necessário para a aquisição da efeméride é uma parte significante do atraso antes de obter a primeira posição, pois por mais que os receptores tenham se tornado mais eficazes e consigam captar os sinais dos satélites com maior velocidade, os dados de efemérides necessitam de 18 a 36 segundos para serem recebidos, devido a baixa taxa de transmissão.

2.3 SEGMENTO DO USUÁRIO

O segmento do usuário é composto por centenas de milhares de americanos e aliados militares usando o Serviço de Posicionamento Preciso (PPS, *precise positioning service*), e dez milhões de usuários civis, comerciais ou pesquisadores utilizando o Serviço de Posicionamento Padrão (SPS, *standard positioning service*).

Geralmente, os receptores GPS tem uma antena, tunelada com as frequências transmitidas pelos satélites, processador e um relógio altamente estável (frequentemente oscilador de cristal). Eles também podem ter um *display* para informar a localização e a velocidade para o usuário. Um receptor é frequentemente descrito pelo seu número de canais, ou seja, quantos satélites o dispositivo consegue monitorar simultaneamente. Originalmente limitado a 4 ou 5, porém atualmente é possível encontrar receptores que tem entre 12 a 20 canais.

2.3.1 DEMODULAÇÃO E DECODIFICAÇÃO

O receptor GPS recebe o sinal L1 e separa suas componentes: a onda portadora, o código P(Y), o código C/A e a mensagem de navegação. Ele deve calcular o tempo que o sinal levou do satélite até a antena, e para isso, é gerado internamente o código PRN, que é comparado com o recebido, sendo que aquele é defasado no tempo até obter-se a correlação máxima entre os códigos. O tempo observado multiplicado pela velocidade da luz no vácuo, gera a uma medida conhecida como pseudodistância [15].

> "Após retirar do sinal recebido todos os códigos, o receptor reconstrói a onda portadora e pode medir a fase da portadora, que é uma observação muito mais precisa que o tempo de propagação [16]."

Como todos as portadoras estão na mesma frequência, os sinais devem ser separados após a demodulação. Isto é feito se utilizando o PRN que é único pra cada satélite. Os sinais são decodificados após a demodulação, utilizando o PRN correspondente para cada satélite monitorado pelo receptor [16].

Se a informação de almanaque foi adquirida anteriormente, o receptor escolhe os satélites a

monitorar pelos seus PRNs. Se os dados de almanaque não estão na memória, o receptor inicia um modo de busca até encontrar um satélite que seja diretamente visível (não tenha objetos obstruindo a comunicação). Agora o receptor pode adquirir os dados de almanaque e determinar quais satélites ele deve procurar. Como ele detecta o sinal de cada satélite, é possível identificar cada um pelo seu código C/A. Pode haver um atraso maior de 30 segundos antes de ser estimado a primeira posição pois é necessário a leitura dos dados de efemérides dos satélites.

Um receptor GPS processa os sinais recebidos pela sua antena, a fim de determinar a posição velocidade e/ou horário. O sinal na antena é amplificado, após isso ele é demodulado, separando-se os sinais, então é digitalizado.

Para um receptor utilizar um satélite, é necessário primeiramente fazer a aquisição do sinal e só então fazer o rastreamento do satélite, enquanto utilizá-lo.

A aquisição do sinal é o processo para determinar a frequência e a fase do código (ambos relativos ao horário do receptor) que vai ser gerado internamente, sem ter conhecimento do sinal recebido. A fase do código deve ser determinada com certa precisão, que varia para diferentes tipos de receptores. Uma precisão da metade do tempo de duração do código PRN(aproximadamente 0,489 microssegundos) é um valor aceitável.

Rastreamento é o processo de ajuste contínuo da frequência e da fase interna a fim de se aproximar ao máximo do sinal recebido.

Um possível procedimento é descrito para aquisição e rastreamento do sinal L1 C/A, no entanto o processo é muito similar para os outros sinais. O procedimento é baseado em computar a correlação dos sinais recebidos com as réplicas geradas localmente e detectar o pico com maior valor e o vale com o menor valor.

A aquisição de um número PRN pode ser conceituado como a procura espacial de um sinal bidimensional, sendo as variáveis: fase do sinal e frequência. Além disso, o receptor pode não conhecer o número PRN que deve procurar, e no caso, uma terceira variável é adicionada: o

número PRN.

A faixa de frequência da busca do sinal é a faixa na qual o sinal pode ser localizado. A frequência portadora tem uma variação de até 5 kHz devido ao efeito Doppler quando o receptor está parado. Se o receptor se move, a variação é maior. O desvio da frequência do código PRN é 1/1540 vezes o desvio da frequência da portadora para o sinal L1,

O código tem o período de 1023 chips que dura exatamente 0,977 microssegundos. O código é altamente autocorrelacionável somente com diferenças com magnitude 1. É típico uma granularidade de 0.5, o que fornece 2046 diferenças de tempo.

É necessário o receptor saber quais dos 32 números PRN corresponde ao sinal que ele recebe no momento para poder fazer a decodificação, eis o motivo dele ser uma variável.

2.4 ERROS

O receptor GPS faz análise de erros. Apesar das correções feitas no relógio, ainda há erros residuais. Como fontes de erro, inclui-se medidas de tempo da chegada do sinal, cálculos numéricos, efeitos atmosféricos (atrasos ionosféricos e troposféricos), dados de efemérides e dados do relógio, sinais multidirecionais, e interferências naturais e artificiais.

Erros artificiais podem resultar de dispositivos de *jamming* ou *spoofing*, que podem ameaçar aeronaves e embarcações.

Atualmente em média, a precisão da pseudodistância medida pelos receptores GPS é de 7,8 metros com um nível de confiança de 95%. A atual precisão depende de fatores fora do controle do governo como efeitos atmosféricos, bloqueio do céu e qualidade do receptor [6].

3 PADRÃO NMEA 0183

Nesse trabalho, serão utilizados os dados obtidos diretamente da camada de aplicação do receptor GPS, que estão no padrão NMEA 0183.

NMEA 0183 é a combinação da especificação elétrica e de dados para comunicação entre eletrônicos marinhos tais como, sonares, anemômetros, bússola giroscópica, autopilotos, receptores GPS e muitos outros tipos de instrumentos. Ele foi criado e é controlado pela Associação Nacional de Eletrônicos Marinhos dos Estados Unidos [17].

O padrão NMEA 0183 usa ASCII simples e protocolo de comunicação serial unidirecional que faz o *broadcast* dos dados para todos. A taxa de transmissão (*baud rate*) é de 4800, e tem as seguintes características:

- Cada mensagem se inicia por um cifrão($).
- Os 2 primeiros caracteres identificam o transmissor, e os 3 seguintes identificam o tipo da mensagem.
- Todos os campos são delimitados por vírgula (,).
- O campo permanecerá em branco se o dado estiver indisponível ou não existir.
- O primeiro caractere que vem logo após o último campo de dados é um asterisco, mas ele só é incluído se um *checksum* for exigido.
- O asterisco é imediatamente seguido pelo *checksum* representado como um número hexadecimal de dois dígitos. O *checksum* é um OU-Exclusivo feito bit a bit do código ASCII de todos os caracteres incluindo o $ e o *.
- A mensagem termina com <CR><LF> (*carriage return* e *line feed*).

Ele é constituído por sentenças, e a primeira palavra contida nele, define a interpretação do resto da sentença. Cada tipo de dado deve ter sua interpretação única e definida pelo padrão NMEA. A sentença GGA por exemplo fornece dados essenciais para fixar um ponto. Outras sentenças podem repetir a mesma informação, porém também fornecerão dados novos. No entanto o dispositivo ou programa que lê os dados pode aguardar os dados que espera e ignorar as outras sentenças que não o interessa.

Existem muitas sentenças no padrão NMEA para todos os tipos de aparelhos que podem ser usados no ambiente marinho. Algumas das sentenças que são aplicadas aos receptores GPS estão listadas abaixo, sabendo-se que todas as sentenças se iniciam por GP [18].

Nmea	Descrição
AAM	Alarme de chegada ao ponto
ALM	Dado de almanaque
APA	Sentença de Auto Piloto A
GGA	Informaçoes sobre o ponto
GLL	Dados de Latitude e Longitude
GRS	GPS Range Residuals
GSA	*DOP* GPS e satélites ativos
GST	GPS Pseudorange Noise Statistics
GSV	Dados detalhados do satélite
TRF	Dado de transição de ponto
VBW	dual Ground / Water Spped
VTG	Vetor de direção do rastreamento e velocidade no solo
XTC	Erro ao traçar a rota
XTE	Medida do erro ao traçar a rota
ZDA	Data e Hora

A seguir alguns exemplos de dados NMEA capturados pelo receptor GPS do *Tablet* utilizado no trabalho.

$PGLOR,0,NEW,PERFIX,1,PER,1000,QOP,-1*1F

$PGLOR,0,RID,BCD,3,19,204,150864*43

$GPGGA,224048.00,,,,,0,00,300.0,,M,,M,,*6D

$PGLOR,1,STA,224048.00,0.000,0.000,-42,98,3000,0,P,F,L,1,C,0,S,0000,0,1,R,33F4*48

$PGLOR,1,SAT*31

$PGLOR,1,SIO,TxERR,0,RxERR,0,TxCNT,76,RxCNT,120,DTMS,999,DTIN,0,0,DTOUT,866,998,HATMD,69*35

$PGLOR,0,HLA,224048.00,L,,Al,,A,,H,,,M,,Ac,0,Gr,0,S,,,Sx,,,T,0,Tr,,Mn,0*0E

$PGLOR,1,PWR,AvgP,30.440001,RFTm,1000,RunT,1000,OscTm,1000,SlpTm,0,MeasTm,1000*1D

$PGLOR,0,PPS,121115,224047.999,,,000.000,0,0,0,*00

$GPGSV,3,1,12,20,58,050,25,12,45,043,27,05,33,120,13,25,88,071,*70

$GPGSV,3,2,12,29,47,192,,21,38,289,,31,22,250,,18,14,344,*78

$GPGSV,3,3,12,15,04,039,,02,04,133,,24,04,007,,26,03,219,*7F

$GLGSV,3,1,09,71,34,085,27,72,21,028,17,75,25,352,13,76,54,286,*62

$GLGSV,3,2,09,86,36,171,,87,26,237,,77,24,221,,70,14,136,*6D

$GLGSV,3,3,09,85,09,123,*58

$GPGSA,A,1,,,,,,,,,,,,,6.0,5.1,3.2*33

$GNGSA,A,1,,,,,,,,,,,,,6.0,5.1,3.2*2D

$GNGSA,A,1,,,,,,,,,,,,,6.0,5.1,3.2*2D

$QZGSA,A,1,,,,,,,,,,,,,6.0,5.1,3.2*2F

4 *JAMMING E SPOOFING*

Jamming é o ato de impedir que o sinal do satélite GPS chegue até o receptor, para que o usuário não consiga obter sua localização, e nenhuma das informações fornecidas pelo sistema GPS.

Spoofing é o ato de enviar dados falsos para um alvo, fingindo ser a fonte oriunda dos dados originais, a fim de se obter alguma vantagem sobre isso. No caso do *Spoofing* GPS, seria o envio de sinais GPS, passando-se pelo satélite, no intuito de fazer o receptor fornecer uma informação incorreta ao usuário, como por exemplo, a posição em que se encontra.

O *Spoofing* é mais perigoso que o *jamming* pois o alvo não consegue detectar o primeiro, e pode continuar navegando através de uma rota não confiável.

Em 2001, o Departamento de Transporte dos Estados Unidos considerou a infraestrutura de transporte americana vulnerável ao *Spoofing* GPS. O aviso, conhecido como aviso *Volpe*, alertou que, “como o GPS está sendo muito usado na infraestrutura civil, ele passou a ser um alvo que esta vulnerável a ataques de pessoas, grupos ou países hostis aos Estados Unidos” [19].

15 anos após o aviso, os receptores GPS civis continuam vulneráveis a essa ameaça. Porém pesquisas para desenvolver contramedidas de *spoofing* vem ocorrendo com mais frequência. O aviso *Volpe* cita um memorando interno da Corporação MITRE, onde o autor Edwin L. Key, examinou o *spoofing* e contramedidas de *spoofing* em detalhe [20]. O memorando recomenda as seguintes técnicas contra o *spoofing*:

1. Diferenciação de Amplitude
2. Diferenciação no tempo de chegada
3. Verificação da unidade de medida de consistência inercial da navegação (IMU).
4. Diferenciação da Polarização
5. Diferenciação no Ângulo de chegada
6 Autenticação criptográfica

As técnicas 1 e 2 podem ser implementadas em software nos receptores GPS, porém as técnicas podem ser efetivas apenas contra os mais simples ataques *spoofing*. Técnicas 3, 4 e 5 podem ser efetivas contra alguns ataques mais sofisticados, mas não todos. Em particular, a diferenciação do ângulo de chegada, que explora a diferença das medidas da fase da portadora a qual utiliza múltiplas antenas, pode ser *spoofado* por um ataque *spoofing* muito sofisticado. As técnicas 3, 4 e 5 necessitam de hardware adicionais ou múltiplas antenas.

Autenticação criptográfica, técnica 6, tem sido estudada com algum detalhe desde o aviso VOLPE [21][22][23]. O pesquisador Logan Scott sugeriu várias formas de autenticação e reforçou seu pensamento em um artigo [24]. Com seu método, os receptores GPS ficariam vulneráveis ao *Spoofing* durante um curto período de tempo que seria entre a recepção e a autenticação das mensagens, que estariam junto aos códigos PRN. Porém para isso, seria necessário uma mudança na estrutura dos sinais, a fim de adicionar as mensagens.

Ou seja, nenhuma das técnicas acima conseguem evitar ou detectar efetivamente um ataque *Spoofing*.

O objetivo desse trabalho é desenvolver uma forma de evitar ou pelo menos detectar o *Spoofing* GPS, desde o ataque mais simples, até o ataque mais robusto. A seguir serão apresentadas algumas formas de *Spoofing* GPS que são utilizadas e estudadas atualmente.

As correlações de tempo, *loops* de rastreamento e as soluções de navegação estão implementadas em software.

Para facilitar a análise do *Spoofing* GPS, esta será dividida em 3: ataques *spoofing* simples, intermediário e sofisticado.

4.1 ATAQUE SIMPLES VIA SIMULADOR DE SINAL

Todos os receptores comerciais civis são vulneráveis ao *spoofing*. Um simples ataque consiste de um amplificador de sinal e uma antena acoplados em um simulador de sinal GPS emitindo os sinais RF na direção do receptor alvo. Um ataque desse tipo com sucesso, foi demonstrado pelos pesquisadores do Laboratório Nacional de Argonne [25].

Embora seja fácil montar um ataque com um simulador de sinais, o custo é alto. Um simulador moderno pode chegar a 400 mil dólares. Simuladores podem ser alugados por 1000 dólares por semana, que fazem-no acessíveis a curto tempo. Outro problema é o tamanho. Muitos simuladores são pesados e grandes. Se usados em um simples ataque – próximo ao receptor da vítima – o mesmo pode ser visto.

Além disso, há a dificuldade de sincronizar a saída do simulador com a atual leitura do sinal GPS no receptor. Um ataque dessincronizado efetivamente age como um sinal de *jamming*, e pode fazer com que o receptor da vítima perca o contato com o satélite e tenha que refazer a aquisição do pacote. Essa requisição repetida pode parecer suspeita, porém é efetiva se não notada, pois após isso, o receptor pode sincronizar-se com o sinal simulado. Porem é necessário que o receptor perca o contato com todos os satélites durante o *jamming* e realize contato diretamente com o sinal simulado [26].

4.2 ATAQUE INTERMEDIÁRIO VIA UM RECEPTOR-SPOOFER PORTÁTIL

Um dos desafios de um ataque *spoofing* é ter conhecimento preciso da posição e velocidade do receptor alvo. Esse conhecimento é necessário para o envio de sinais relativos no lugar dos sinais genuínos. Sem essa precisão de posicionamento, o ataque é facilmente detectado.

Um ataque via *receptor-spoofer*, torna-se difícil pela montagem. Ele pode ser feito pequeno, porém é necessário estar próximo a antena do receptor da vítima. O componente receptor simula o sinal original para estimar sua própria posição, velocidade e tempo. Devido a proximidade, esses dados são aplicados a antena do alvo. Baseado nessa estimativa, o aparelho gera sinais falsos e executa o *spoofing*. O *receptor-spoofer* portátil pode ser posicionado longe do receptor alvo se ele for estático e sua posição em relação aquele for conhecida [26].

Cada canal do receptor alvo está sob controle do *receptor-spoofer*. O pico do sinal falso é alinhado com o pico do sinal genuíno correspondente. A energia do sinal falso é gradualmente elevada. Eventualmente o sinal falso ganha controle no loop de rastreamento que usa a correlação do pico [26].

Como é possível imaginar, não há *receptores-spoofer* portáteis comerciais. E um ataque utilizando-o é muito difícil de se detectar. O *receptor-spoofer* é capaz de sincronizar seu sinal ao tempo GPS e, pela sua proximidade a antena da vítima, alinhar o sinal falso e o original.

Um receptor alvo equipado com um oscilador de referência estável e um IMU sofisticado pode durante muitas horas atuar, sem sofrer o ataque de *Spoofing*. Porém com o tempo, e paciência, o *receptor-spoofer* pode ter acesso indetectável utilizando perturbações no tempo e posição com uma alteração mais detalhada.

Um ataque via *receptor-spoofer* portátil não é fácil de ser executado, por não existir o aparelho. Entretanto, com o acesso a eletrônicos mais baratos, e conhecimento livre na Internet, esse ataque pode em breve se tornar um problema.

4.3 ATAQUE SOFISITICADO VIA MÚLTIPLOS *RECEPTORES-SPOOFER* PORTÁTEIS EM FASE

A técnica de defesa contra *receptores-spoofer* portáteis (diferenciação de ângulo de chegada) pode ser burlada com um ataque coordenado com um *receptor-spoofer* com várias antenas no receptor alvo. Imagine um *receptor-spoofer* do tamanho de um baralho. As antenas de recepção e transmissão estão situadas respectivamente na face de cima e de baixo do aparelho e protegidos para evitar *auto-spoofing*. Agora imagine muitos aparelhos dividindo um oscilador de referência em comum e um canal de comunicação entre eles, com cada aparelho montado para uma antena do receptor alvo. A defesa do ângulo de chegada falha nesse cenário [26].

Naturalmente, este ataque apresenta todos os desafios de montagem de um simples *receptor-spoofer*, com a adição de múltiplos *receptores-spoofer* e a uma complexidade adicional que as perturbações dos sinais vindo devem estar coordenadas em fase.

A única defesa conhecida contra esse tipo de ataque é a autenticação criptográfica.

Em resumo, um ataque via múltiplos *receptores-spoofer* portáteis é mais incomum que um ataque usando um *receptor-spoofer*, mas é impossível de ser detectado com os atuais métodos de defesa.

5 GPS ASSISTIDO

GPS Assistido (A-GPS, *assisted* GPS) é um sistema que acelerou o processo de obtenção do primeiro ponto de localização (TTFF, *time to first fix*) de sistema baseado em satélites de posicionamento GPS. Esse sistema é utilizado em celulares, e seu desenvolvimento foi feito graças a Comissão Federal de Comunicações que exigiu o serviço para atender aos requerimentos do 911 e possibilitar o rastreamento da ligação através da chamada de emergência.

O sistema de GPS assistido é utilizado quando os sinais dos satélites estão muito fracos, estão sofrendo muita interferência ou até sujeitos a muitos obstáculos. E como foi visto, um receptor GPS pode demorar até 12,5 minutos para de obter o primeiro ponto [15].

Um sistema de GPS assistido utiliza dados externos e dependendo do provedor dos dados, esse serviço pode ser cobrado.

Existem 2 tipos de aparelhos que assistem o receptor, o *Mobile Station Based* (MSB) e a *Mobile Station Assisted* (MSA).

A MSB é usada para captar os sinais dos satélites mais rapidamente. Ele fornece os dados orbitais ou almanaques para o receptor GPS, ajudando o receptor na escolha dos satélites.

A MSA é usado para calcular a posição do receptor GPS utilizando informações do mesmo. Geralmente essas estações ficam próximas a torres de celular, com um sinal de satélite bom e sabem as correções dos erros com maior precisão que o receptor. Logo sabendo sua localização, e com maior poder computacional que os receptores, calculam a posição baseada nos dados recebidos do receptor através da rede de dados.

6 FERRAMENTAS UTILIZADAS

O objetivo desse trabalho é elaborar um detector de *spoofing* para um Veiculo Aéreo não Tripulado (VANT). Para isso foi utilizado um software de código aberto, o *GPS Logger* (http://code.mendhak.com/gpslogger/) feito pelo *Mendhak*, no qual foi implementado funções a fim de alcançar o objetivo proposto.

O projeto foi feito em Java utilizando o *API android.location* e testado em um T*ablet Galaxy SII GT-P3110*.

Além disso foi utilizado o aplicativo *Fake GPS Location* para atuar como *Spoofer* do experimento.

6.1 *API ANDROID.LOCATION*

O API utilizado no *GPS Logger* é de fácil uso. Por exemplo, a classe *Location*, fornece a latitude, longitude e o horário GPS por padrão, além disso, há informações opcionais como velocidade e altitude. Ou seja, através do API é possível obter os dados do receptor GPS de uma forma mais limpa e clara, tendo em vista como os dados NMEA são.

Outra classe de extrema importância é a *LocationManager*. Essa classe provê o acesso ao sistema de serviços de localização que fornece a localização geográfica ao aparelho ou se pode iniciar uma aplicação quando o receptor se aproximar de algo definido previamente. Vale lembrar que o sistema pode utilizar outras fontes de dados para calcular sua localização.

A permissão necessária ao aparelho é a *ACCESS_FINE_LOCATION* que possibilita utilizar:

Interfaces:

→ *GpsStatus.Listener*: usado para receber notificacões quando o estado do receptor GPS se alterar.

→ *GpsStatus.NmeaListener*: usado para receber sentenças NMEA do receptor.

→ *LocationListener*: usado para receber notificações do *LocationManager* quando a localização for alterada.

Classes:

→ *Address*: classe representando um endereço, isto é, um conjunto de palavras descrevendo uma localização.

→ *Criteria*: classe representando o critério para a escolha do provedor.

→ *Geocoder*: classe responsável pela geocodificação (processo de transformação de um endereço ou algum outro dado, em coordenadas) e a geocodificação reversa.

→ *GpsSatellite*: classe que representa o estado atual do satélite GPS.

→ *GpsStatus*: classe que representa estado atual do sistema GPS

→ *Location*: classe de dados representando a localização geográfica.

→ *LocationManager*: classe que fornece acesso ao serviço de sistema de localização.

→ *LocationProvider*: superclasse abstrata para os provedores de localização.

A partir dessas classes foi implementada a detecção do *Spoofing*.

6.2 *GPS LOGGER*

O *GpsLogger* é um aplicativo para Android, feito em Java e de código aberto. Ele mostra a localização em tempo real do aparelho, além de salvar esses dados e dados passados em um arquivo no cartão de memória do aparelho. Esse arquivo pode ser salvo nos formatos CSV, KML ou GPX, sendo que esse último é padrão para sistemas de rastreamento. Esses logs podem ser enviados periodicamente durante atividade via FTP, *DropBox*, e-mail ou *Google Docs*, ou via SMS.

É possível salvar dados como velocidade, direção e altitude calculados a partir do sistema GPS, porém esses podem ser obtidos de fonte externa também.

Quando o sistema GPS está desativado no aparelho, ele utiliza as torres de celular para obter uma localização.

Ele pode interagir facilmente com outros aplicativos do celular utilizando condições geradas pelos dados obtidos e disponibilizados no programa.

Ele informa dados como, localização, altitude, direção, latitude, longitude, o número de pontos obtidos, a precisão da localização, o número de satélites vistos e quais estão sendo utilizados para o cálculo da posição. Alguns desses dados só são observados via USB.

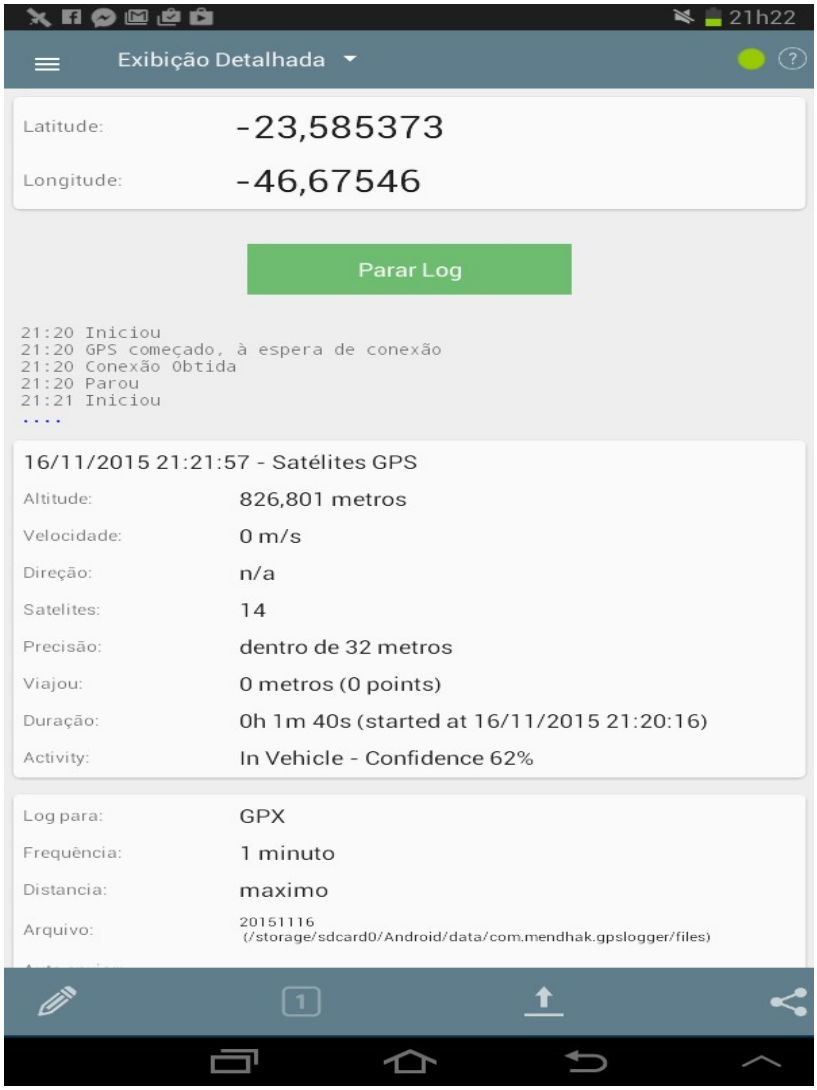

Figura 3: Gps Logger em funcionamento.

6.3 *FAKE GPS LOCATION*

O *Fake GPS Location* é um aplicativo, criado pela empresa Lexa, que altera, via software, as coordenadas atuais do receptor, para coordenadas preestabelecidas

Esse programa será responsável por "*spoofar*" o receptor GPS via software já na camada de aplicação, onde adulterará os dados de localização obtidos.

Figura 4: Tela principal do Fake GPS Location

7 O DECETOR DE *SPOOFING*

O detector de *spoofing* foi criado com a alteração de algumas funções do *GPSLogger* e com a adição de outras.

O sistema calcula se é realmente possível que o receptor esteja naquele ponto, naquele momento, utilizando informações de tempo e localização do instante e anteriores. Utiliza-se também a velocidade atual do dispositivo, que pode ser estimada como uma velocidade média, ou obtida a partir de uma fonte externa. Não é recomendado utilizar a velocidade obtida do sistema GPS, tendo em vista que esta pode ter sido adulterada pelo *Spoofing*.

Para que o *anti-spoofer* funcione é necessário que o primeiro ponto seja conhecido e não esteja sendo gerado por um *spoofer*. Logo temos um ponto inicial P0 conhecido e confiável. Após isso o VANT pode ser deixado livre para voo. A partir do momento que se movimentar e calcular um novo ponto P1, o sistema agirá, e calculará a diferença dos tempos dos dois pontos, e a distância absoluta entre eles. Tendo a diferença de tempo entre os pontos e a velocidade do VANT pode-se calcular qual distância foi percorrida nesse período, checando-se assim se o ponto P1 está dentro do alcance possível do veículo aéreo.

A seguir estão descritas as alterações feitas.

7.1 PACOTE ANDROID.WIDGET.TOAST

O pacote é utilizado para o visual do *Anti-spoofer* e é responsável pela exibição das informações de alerta quando o sistema for *spoofado*, além da localização atual *spoofada* e a última localização real.

7.2 SESSION.JAVA

Essa classe é responsável pela sessão atual que está sendo exibida na tela do GPS. Aqui foram adicionadas algumas funções para alterar e atualizar as variáveis da Sessão atual, por exemplo, o horário do último ponto da Sessão atual.

```
public static long getCurrentTime() {
     Location loc = getCurrentLocationInfo();
     return po != null ? loc.getTime() : 0;
}
public static long getPreviousTime() {
     Location loc = getPreviousLocationInfo();
     return loc != null ? loc.getTime() : 0;
}
```

As funções são responsáveis por armazenar o horário do ponto atual e do ponto anterior da Sessão.

7.3 GENERALLOCATIONLISTENER.JAVA

Essa classe é responsável por manipular as informações recebidas dos satélites.

```
case GpsStatus.GPS_EVENT_SATELLITE_STATUS:
         GpsStatus status = loggingService.gpsLocationManager.getGpsStatus(null);
         int maxSatellites = status.getMaxSatellites();
         Iterator<GpsSatellite> it = status.getSatellites().iterator();
         int count = 0;
         while (it.hasNext() && count <= maxSatellites) {
         it.next();
         count++;
         }
```

O código acima, que faz a contagem dos satélites vistos pelo GPS, foi alterado pelo código abaixo.

```
case GpsStatus.GPS_EVENT_SATELLITE_STATUS:
     GpsStatus status = loggingService.gpsLocationManager.getGpsStatus(null);
      int maxSatellites = status.getMaxSatellites();
     float[] Azimuth = new float[maxSatellites];
     float[] Elevation = new float[maxSatellites];
     int[] Prn = new int[maxSatellites];
     float[] Snr = new float[maxSatellites];
     boolean[] InFix = new boolean[maxSatellites];
     Iterator<GpsSatellite> it = status.getSatellites().iterator();
     int count = 0;
     while (it.hasNext() && count <= maxSatellites) {
          GpsSatellite SATS=it.next();
```

```
            count++;
            Azimuth[count]=SATS.getAzimuth();
            Elevation[count]=SATS.getElevation();
            Prn[count]=SATS.getPrn();
            Snr[count]=SATS.getSnr();
            InFix[count]=SATS.usedInFix();
            tracer.debug(String.valueOf(InFix[count]) +"
"+String.valueOf(Azimuth[count])+" "+ String.valueOf(Elevation[count]) +" "+
String.valueOf(Prn[count]) +" "+ String.valueOf(Snr[count]) );
        }
```

Esse trecho envia algumas informações como PRN, azimute, elevação, SNR (taxa sinal-ruido) de cada satélite, e informa se ele está sendo utilizando ou não para o cálculo do ponto atual.

Não é possível escolher qual satélite utilizar para fazer o cálculo, visto que isto é programado no CHIPSET do GPS.

Além disso, foi adicionada uma linha de código, para que todas as sentenças NMEA fossem enviadas via USB. Elas foram mostradas na sessão dos dados NMEA.

```
tracer.debug("\n" + String.valueOf(nmeaSentence) + "\n");
```

7.4 GPSLOGGINGSERVICE.JAVA

Aqui é a classe onde se inicia a classe *LocationManager*, onde é possível escolher a localização via torres de celulares ou GPS. Lembrando que o dispositivo utilizado nesse trabalho não tem acesso a torres de celulares.

Nessa classe foram feitas as maiores alterações e adições.

A função *IsPossibleDistance(loc)*, confere se a posição *loc* está dentro do raio de possíveis posições utilizando a diferença de tempo dessa localização e da anterior e uma velocidade média escolhida.

Abaixo o código:

```
private boolean IsPossibleDistance(Location loc) {
    if (Session.getPreviousLocationInfo() == null) {
        Session.setPreviousLocationInfo(loc);
    }
```

```
    double distance = Utilities.CalculateDistance(
             Session.getPreviousLatitude(),
             Session.getPreviousLongitude(),
             loc.getLatitude(),
             loc.getLongitude());
    double DeltaTime= loc.getTime() - Session.getPreviousTime();
    tracer.info(String.valueOf(loc.getTime()) + " " + Session.getPreviousTime());
    if (distance <= (9*(DeltaTime/1000))) {
         tracer.debug(String.valueOf(distance) + "<= 1000*11*" + DeltaTime);
         return true;
    }

else return false;

}
```

Observa-se que a velocidade aqui escolhida é de 11m/s que corresponde a 39,6 km/h.

O código que obtinha o ponto atual foi alterado para fazer a verificação desse ponto. Abaixo uma parte do código como era inicialmente.

```
tracer.info(SessionLogcatAppender.MARKER_LOCATION,
String.valueOf(loc.getLatitude()) + "," + String.valueOf(loc.getLongitude()));
AdjustAltitude(loc);
ResetCurrentFileName(false);
Session.setLatestTimeStamp(System.currentTimeMillis());
Session.setCurrentLocationInfo(loc);
SetDistanceTraveled(loc);
ShowNotification();
```

Observa-se que ele define as informações atuais de localização da Sessão como as contidas em *loc* (em negrito), sem antes passar por nenhuma verificação. Após a alteração o código ficou dessa forma:

```
if (Session.getPreviousLocationInfo()==null){
    tracer.info("Location to update: " + String.valueOf(loc.getLatitude()) + "," +
String.valueOf(loc.getLongitude()));
    AdjustAltitude(loc);
    tracer.info("Primeira rodada");
    ResetCurrentFileName(false);
    Session.setLatestTimeStamp(System.currentTimeMillis());
    Session.setCurrentLocationInfo(loc);
    SetDistanceTraveled(loc);
    Session.setPreviousLocationInfo(loc);
```

```
}
else {
     if (IsPossibleDistance(loc) == true) {
          tracer.info("Location to update: " + String.valueOf(loc.getLatitude()) +
"," + String.valueOf(loc.getLongitude()));
          AdjustAltitude(loc);
          Session.setPreviousLocationInfo(loc);
          ResetCurrentFileName(false);
          Session.setLatestTimeStamp(System.currentTimeMillis());
          Session.setCurrentLocationInfo(loc);
          SetDistanceTraveled(loc);
     }
     else {
          HackedLoc = loc;
          RealLoc= Session.getPreviousLocationInfo();
          int i=0;
          while(i!=2) {
               tracer.info("Location to update: " + String.valueOf(loc.getLatitude())
+ "," + String.valueOf(loc.getLongitude()) + "FALSE LOCATION! Sppofed GPS
Signals!");
               Toast.makeText(getApplicationContext(), "Your False Location is -
\nLat: " + String.valueOf(HackedLoc.getLatitude()) +
                         "\nLong: " + String.valueOf(HackedLoc.getLongitude()) +
                         "\nYour Last Real Location was -  \nLat:" +
String.valueOf(RealLoc.getLatitude()) +
                         "\nLong" + String.valueOf(RealLoc.getLongitude()),
Toast.LENGTH_LONG).show();
               i++;
          }
          Session.setPreviousLocationInfo(RealLoc);
          AdjustAltitude(Session.getPreviousLocationInfo());
          ResetCurrentFileName(false);
          Session.setLatestTimeStamp(Session.getLatestTimeStamp());
          Session.setCurrentLocationInfo(Session.getPreviousLocationInfo());
          SetDistanceTraveled(Session.getPreviousLocationInfo());
          tracer.info(Session.getPreviousLatitude() + " " +
Session.getPreviousLongitude());
     }
}
ShowNotification();
```

O código acima primeiramente checa se existe informações sobre um ponto anterior, caso não tenha, o primeiro ponto é obtido e essas informações são salvas como sendo do último ponto conhecido e confiável.

Ao buscar um segundo ponto, ele observa que já existe informações anteriores e checa através da função *IsPossibleDistance()* se o veículo pode estar naquele ponto. Se a função retornar *True*, ou seja, o ponto não estiver sendo *spoofado*, as informações atuais são atualizadas e esse ponto é salvo como último ponto conhecido confiável. Caso esse ponto não esteja dentro do limite calculado, essas informações de localização são copiadas para uma variável chamada *Hacked*, e as informações sobre a última localização conhecida é salva em outra variável chamada *RealLoc*.

Após salvas as localizações, o sistema exibe uma mensagem na tela do dispositivo e envia uma mensagem via USB informando que o sistema foi s*poofado*, mostrando a posição *spoofada* e a última posição conhecida.

Após isso é necessário que o VANT execute algum procedimento, visto que as informações sobre a sua posição não são mais confiáveis.

8 MÉTODO

Para fazer o teste do Anti-Spoofer, definiu-se uma rota a ser seguida. A rota escolhida foi o trajeto da Rua Eduardo de Souza Aranha, número 191, do Bairro Vila Nova Conceição, até a Rua Doutor Franco da Rocha, número 669 do Bairro Perdizes, ambos localizados em São Paulo Capital. Abaixo a imagem da rota escolhida em colorido.

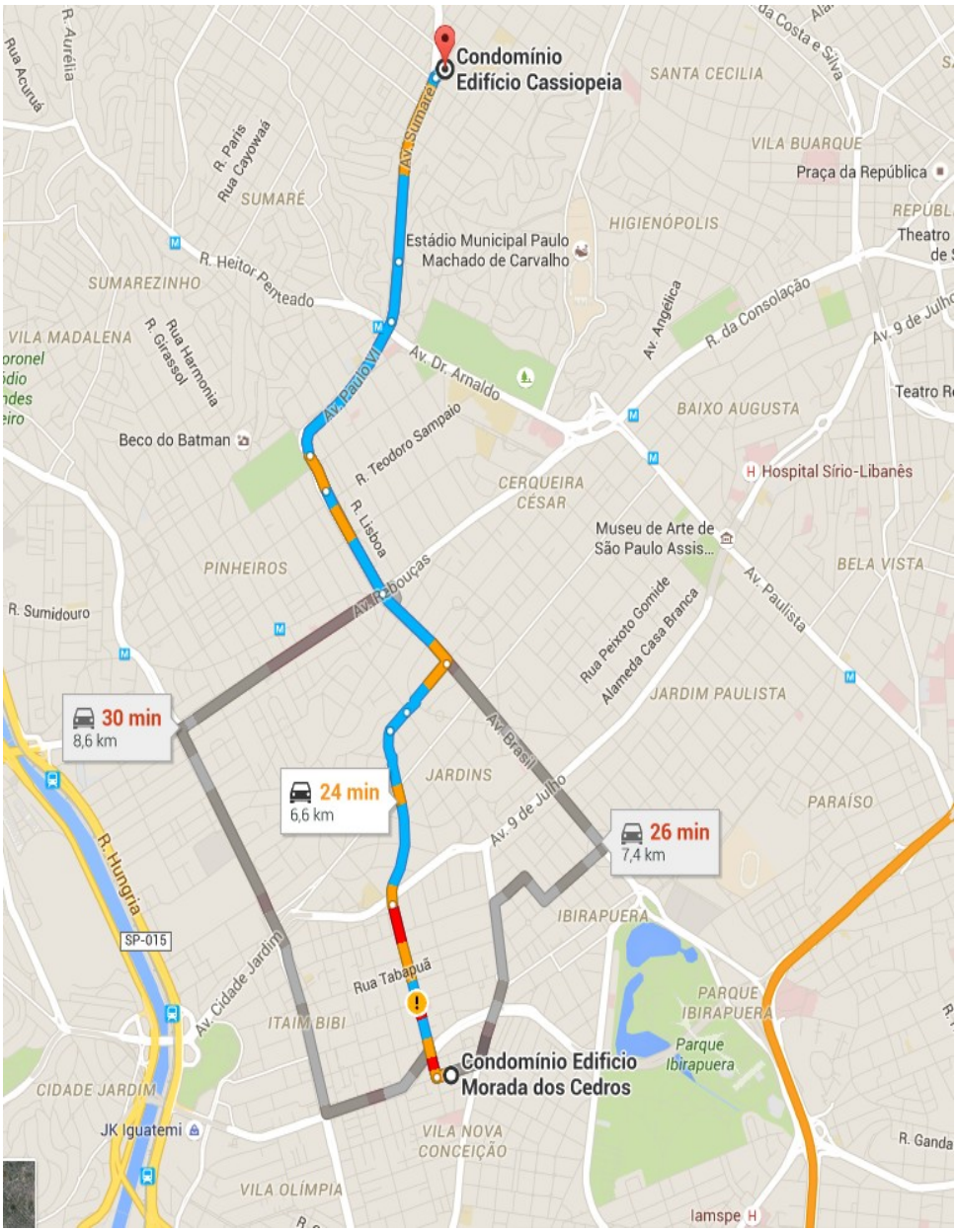

Figura 5: Trajeto colorido correspondente a rota percorrida.

A imagem foi gerada pelo *Google Maps*, e a rota tem em torno de 6,6 quilômetros.

Em alguns momentos aleatórios do trajeto, o *spoofer* será ligado e o ponto a ser *spoofado*, corresponde a localização do Parque Ibirapuera em São Paulo, com as coordenadas 23,5883 Sul e 46,6589 Oeste.

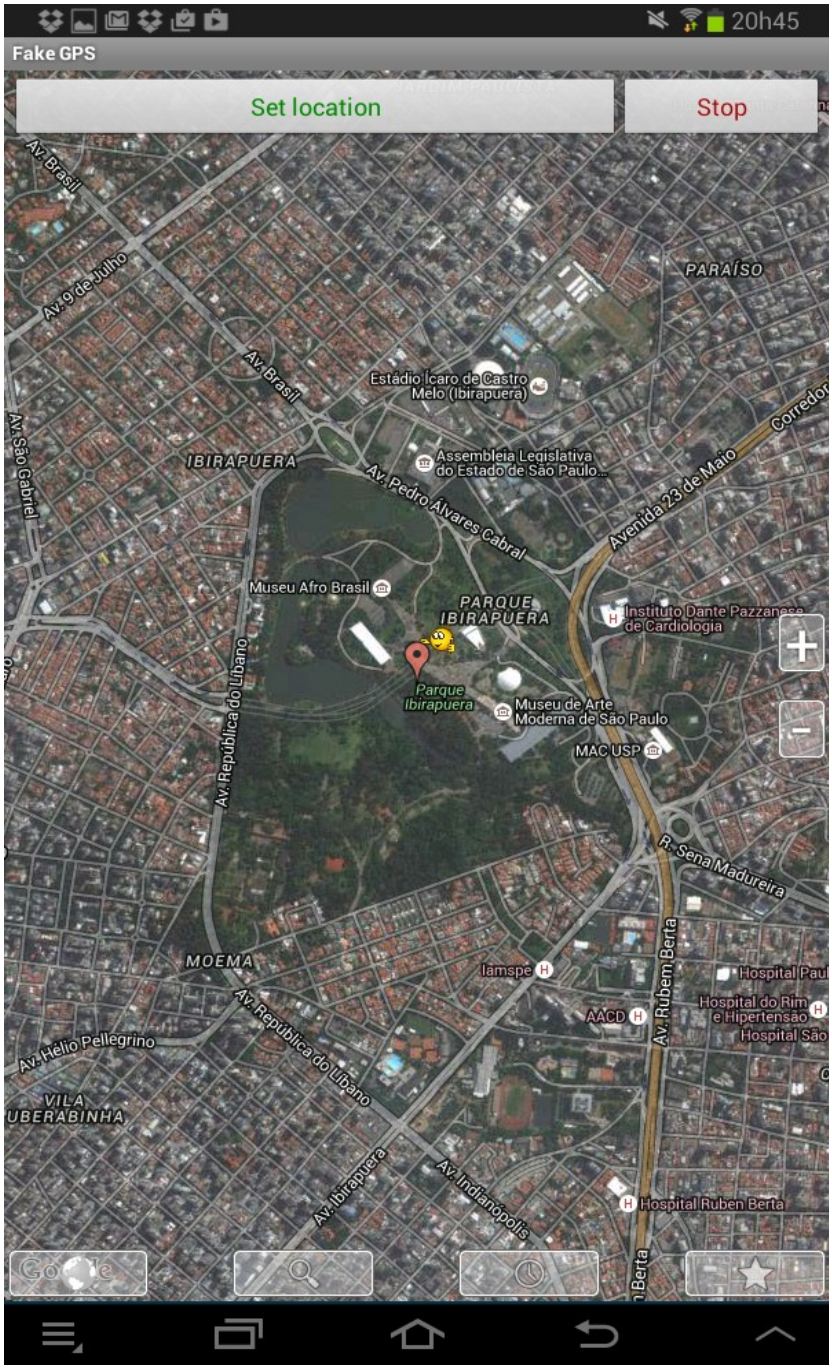

Figura 6: Fake GPS ativado spoofando as coordenadas do Parque Ibirapuera.

Nota-se que o ponto a ser *spoofado* encontra-se em torno de 1 quilômetro do ponto inicial e 5 quilômetros do ponto final.

Ao compilar-se o programa, foi escolhida uma velocidade média de 60 km/h, que corresponde a 16,67 m/s, para ter como base no deslocamento do automóvel pelas ruas. Vale lembrar que nessas vias a velocidade máxima permitida é de 50 km/h, portando está sendo admitido um erro de 20% na precisão do receptor GPS.

9 RESULTADOS

Após o percurso ser percorrido duas vezes, para observação da discretização do sistema (quantidade de pontos por tempo), optou-se pela quantidade de 4 pontos por minuto, ou seja, a cada 15 segundos seria calculada uma nova posição. Isto é, o ponto seguinte deveria estar a uma distância de no máximo 250 metros do ponto atual para ser considerado um ponto válido.

Abaixo os dois mapas mostrando o resultado e os logs dos dois percursos.

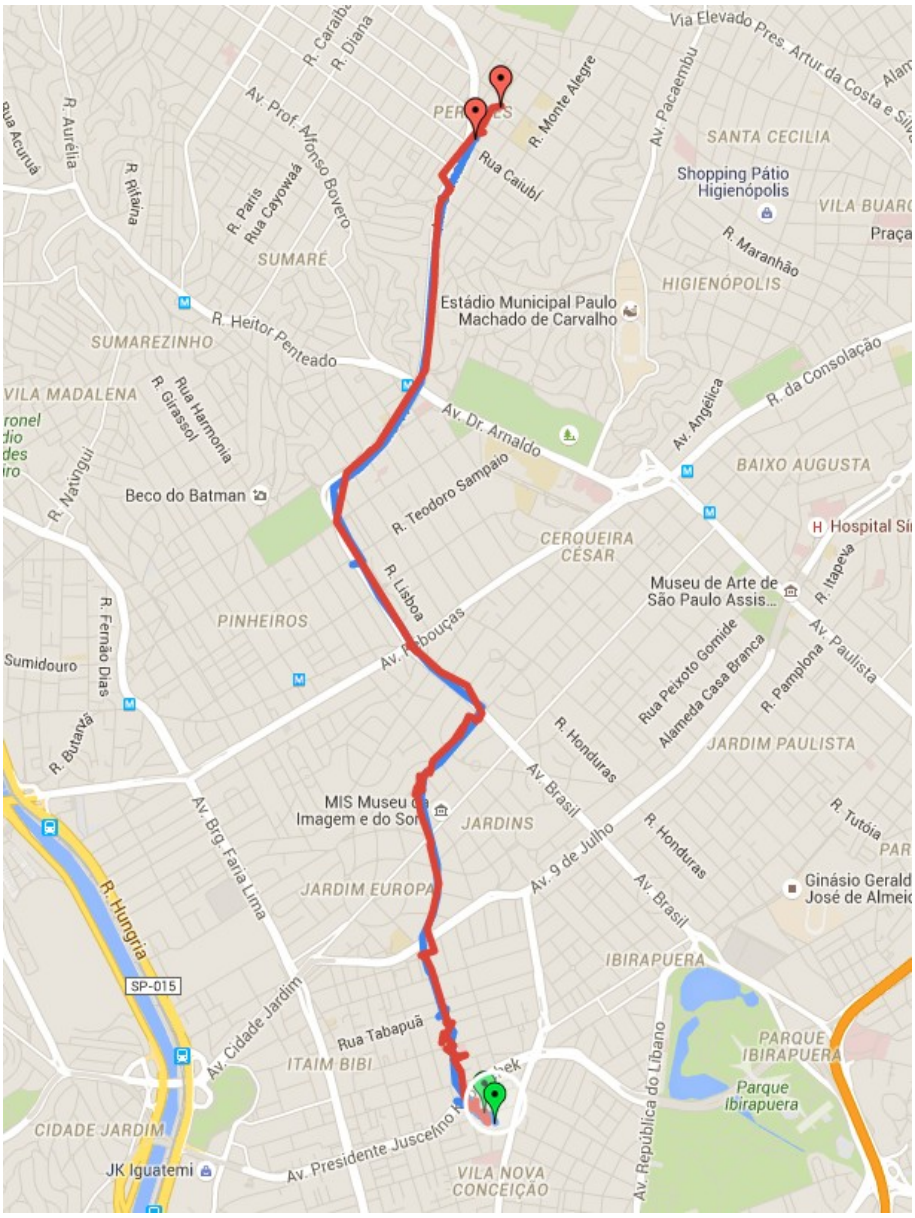

Figura 7: Rota 1 em azul e rota 2 em vermelho; ambas com frequência de atualização 4 pontos/minuto.

Os dados foram extraídos do *debug* do programa e mostram respectivamente, a checagem para saber se é um possível ponto *spoofado* e a atualização dos dados de localização.

IsPossibleDistance:958 - 26.202610852611905<= 1000*16,67*77916.0
OnLocationChanged:845 - Location to update: -23.588439152609322,-46.67278231808028

Também é mostrado os satélites visíveis, e informações sobre os mesmos.

onGpsStatusChanged:142 - true 124.0 62.0 2 33.0
onGpsStatusChanged:142 - true 47.0 20.0 5 25.0
onGpsStatusChanged:142 - true 139.0 25.0 6 26.0
onGpsStatusChanged:142 - true 271.0 27.0 29 15.0
onGpsStatusChanged:142 - true 35.0 58.0 78 19.0
onGpsStatusChanged:142 - false 147.0 11.0 88 8.0
onGpsStatusChanged:155 - 6 satellites

Após constatar que a frequência consegue discretizar bem a rota, foi feito um terceiro percurso, onde o *spoofer* foi configurado para ligar aleatoriamente. E foi obtido um mapa totalmente diferente do atual, com pontos realmente fora da rota.

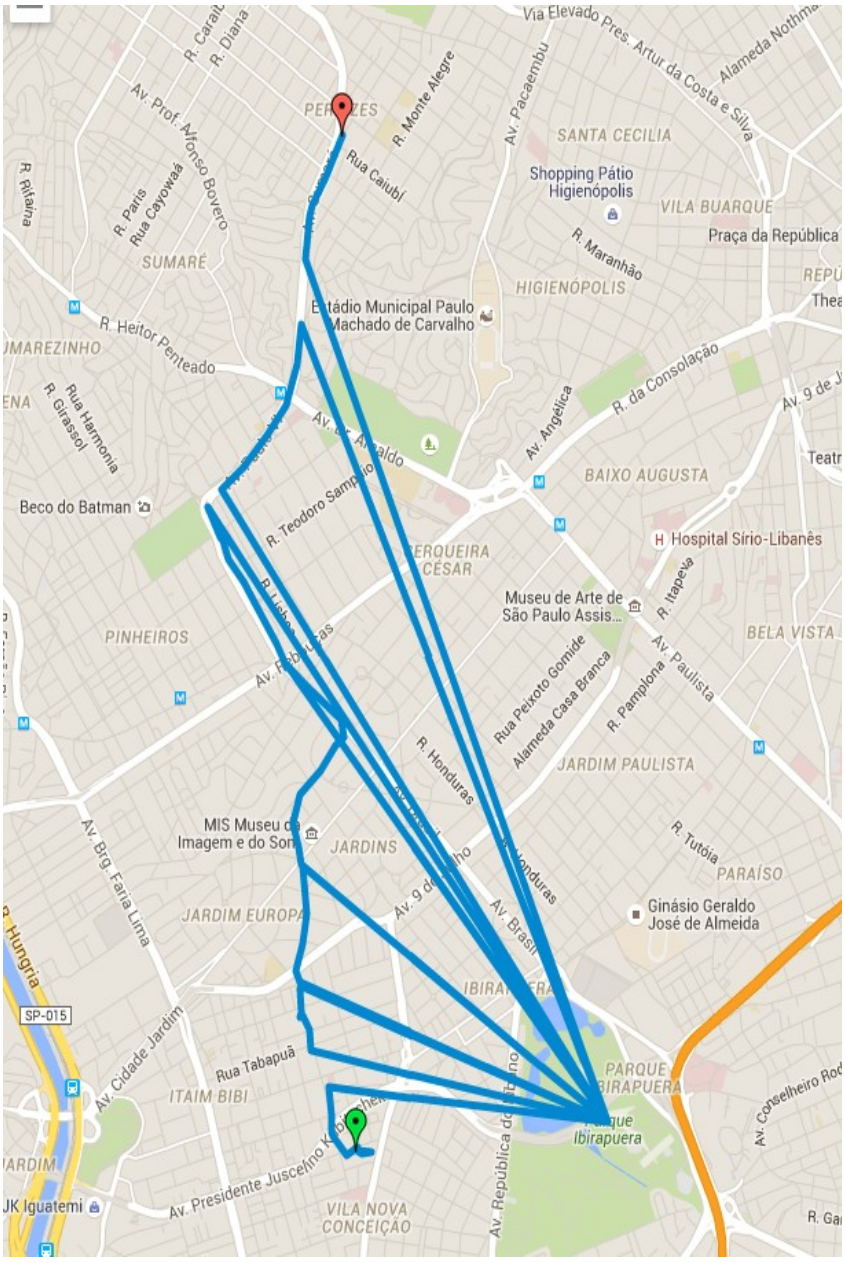

Figura 8: Mesma Rota de 1 e 2 com o spoofer ligado em momentos aleatórios.

Porém nos momentos em que o GPS mostrava o ponto s*poofado*, ele informava que o ponto era duvidoso na tela do *Tablet*, e também via USB. Seria recomendado que nesse momento, houvesse alguma contramedida para que o veículo não seguisse por um caminho incorreto.

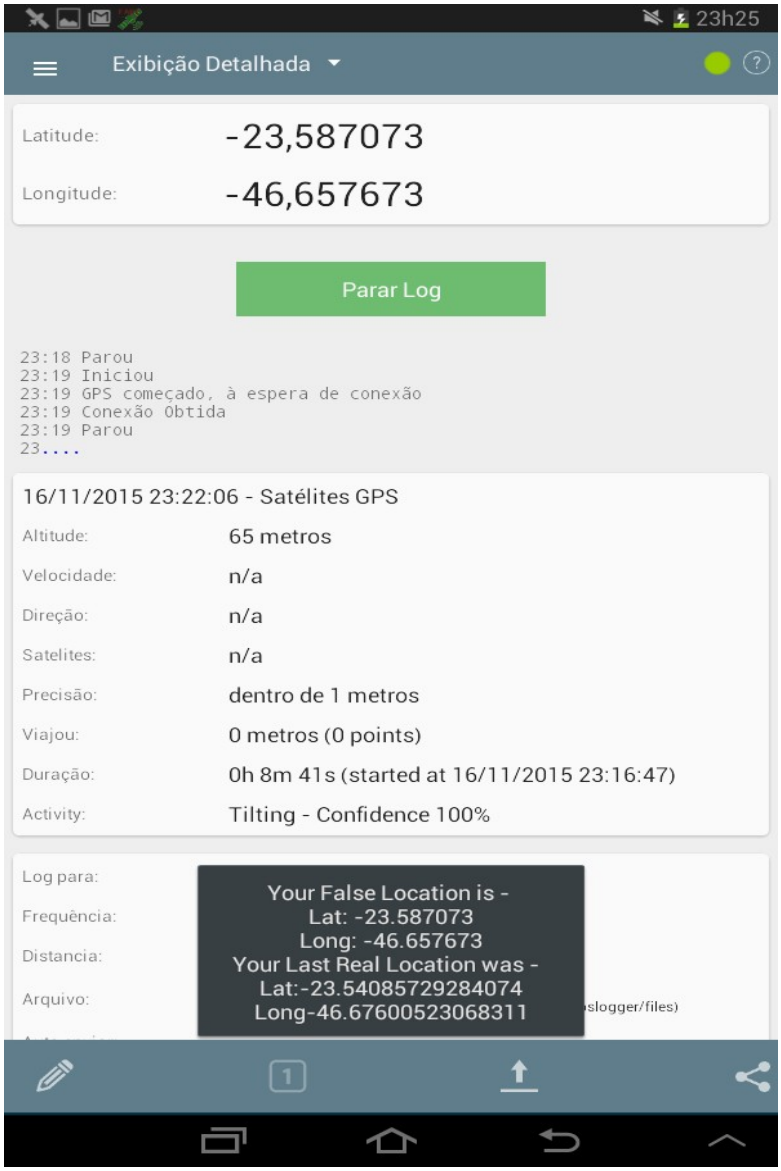

Figura 9: Sistema anti-spoofing informando no display que o receptor está sofrendo spoofing.

E extraindo os dados do *debug* é possível ver o aviso de que a localização é incorreta.

OnLocationChanged:858 - Location to update: -23.586362,-46.658099 FALSE LOCATION! Spoofed GPS Signals!

Como demonstrado, o *spoofing* para esse caso foi detectado, dependendo agora somente da contramedida tomada pelo VANT. Em vista que o sinal está em *broadcast*, é muito difícil evitá-lo.

10 CONCLUSÃO

Tendo o conhecimento que atualmente são conhecidas três formas de *spoofing*, e sendo que, a segunda e terceira só existem na teoria (*receptores-spoofer*). Pode-se dizer que a questão do *Spoofing* foi resolvida temporariamente com esse trabalho.

Vale lembrar que seria um ótimo estudo o uso de um sistema IMU para aumentar a detecção obtendo-se um sistema mais robusto e torná-lo como proteção para o segundo tipo de *Spoofing*.

Uma solução de contramedida ao detectar o *spoofing* seria a troca do provedor, como por exemplo, o uso do GPS Assistido, obtendo a localização pelas torres de celular. Pressupondo que nenhuma dessas torres estivessem sofrendo *spoofing*, o GPS-A informaria a posição correta e o VANT poderia se guiar temporariamente por este. Para isso seria necessário um dispositivo com acesso a rede de dados.

Como falado anteriormente, apenas a criptografia consegue evitar o terceiro tipo de *Spoofing*. Para futuros trabalhos, recomenda-se o desenvolvimento e estudo do *receptor-spoofer* para entender mais a fundo seu funcionamento, a fim de se criar defesas alternativas.

11 BIBLIOGRAFIA

[1] bbc.com. Researchers use spoofing to 'hack' into a flying drone, Disponível em: http://www.bbc.com/news/technology-18643134. Acesso em: 15 de setembro de 2015.

[2] Baroni, L. ALGORITMOS DE NAVEGAÇÃO EM TEMPO REAL PARA UM SISTEMA GPS DE POSICIONAMENTO RELATIVO DE PRECISÃO. INEP, p. 10-20, 2009.

[3] Flandern, T. V. What the Global Positioning System Tells Us about Relativity Disponível em: http://www.metaresearch.org/cosmology/gps-relativity.asp. Acesso em: 20 de outubro de 2015 .

[4] Cooksey, D. Understanding the Global Positioning System (GPS), Disponível em: http://www.montana.edu/gps/understd.html. Acesso em: 15 de setembro de 2015.

[5] Força aérea dos EUA. Informações oficiais sobre o GPS, Disponível em: http://www.gps.gov/. Acesso em: 9 de outubro de 2015.

[6] Thomassen K. How GPS Works. Disponível em: http://www.avionicswest.com. Acesso em: 10 de agosto de 2015 .

[7] Misra, P.; Enge, P. Global Positioning System. Signals, Measurements and Performance. Ganga-Jamuna Press, p.115, 2006.

[8] Borre, K.; Akos, M.; Bertelsen, N.; Rinder, P.; Jensen, S. H. A Software-Defined GPS and Galileo Receiver. A single-Frequency Approach Springer, p.18, 2007.

[9] Força Aérea dos Estados Unidos United States Nuclear Detonation Detection System (USNDS) (U), Disponível em: . Acesso em: 12 de novembro de 2015.

[10] Base das forças Aérea de Los Angeles. Air Force Successfully Transmits an L5 Signal From GPS IIR-20(M) Satellite. Disponível em: http://www.losangeles.af.mil/news/story.asp?storyID=123144001. Acesso em: 8 de agosto de 2015.

[11] Força Aérea dos Estados Unidos. GPS Interface Specification (GPS-IS-200H). Força Aérea dos Estados Unidos, p. 15-26, 2013

[12] Centro de Navegação do Departamento de Segurança dos Estados Unidos. Navstar Gps User Equipment Introduction. Disponível em http://www.navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf. Acesso em: 25 de outubro de 2015.

[13] Base das forças Aérea de Los Angeles. Navstar GPS Space Segment/Navigation User Interfaces. Disponível em: http://www.losangeles.af.mil/shared/media/document/AFD-070803-059.pdf. Acesso em: 28 de outubro de 2015.

[14] Departamento de Defesa e Departamento de Transporte dos Estados Unidos. USNO

NAVSTAR Global Positioning System. Disponível em: http://tycho.usno.navy.mil/gps.html. Acesso em: 21 de outubro de 2015.

[15] Centro de Navegação do Departamento de Segurança dos Estados Unidos.. GPS NANUS, ALMANACS, & OPS ADVISORIES. Disponível em http://www.navcen.uscg.gov/?pageName=gpsAlmanacs. Acesso em: 5 de novembro de 2015.

[16] Rodrigues, D. D. Rede geodésica de precisão no Estado de Minas Gerais: avaliação de diferentes estratégias de processamento e ajustamento. Tese de Doutorado da USP, Cap. 3. Disponível em: http://www.teses.usp.br/teses/disponiveis/3/3138/tde-06122002-115813/publico/04capitulo03.pdf. Acesso em: 12 de novembro de 2015.

[17] Bennett, P. The NMEA FAQ. Disponível em: http://www.kh-gps.de/nmea.faq. Acesso em: 9 de novembro de 2015.

[18] Associação dos Eletrônicos Marinhos dos Estados Unidos. NMEA Standard. Disponível em: http://www.nmea.org/content/nmea_standards/nmea_0183_v_410.asp. Acesso em: 10 de novembro de 2015.

[19] John, A. Vulnerability assessment of the transportation infrastructurerelying on the Global Positioning System. Volpe National Transportation Systems Center, p. 25-30, 2001.

[20] Key, E. L. Techniques to Counter GPS Spoofing. Corporação Mitre, 1995.

[21] Scott, L. Anti-spoofing and authenticated signal architecturesfor civil navigation systems Instituto de Navegação de Portland, Oregon, p.1542-1552, 2003.

[22] Hein, G.; Kneissi, F.; Avila-Rodriguez, J. A.; Wallner, S. Authenticating GNSS: Proofs against spoofs, Part 1. Revista InsideGnss, p.58-63, 2007.

[23] Hein, G., Kneissi, F., Avila-Rodriguez, J.-A., and Wallner, S. Authenticating GNSS: Proofs against spoofs, Part 2. Revista Inside Gnss p.71-78, 2007.

[24] Stansell, T. Location Assurance Commentary. GPS World,Vol. 18, No. 7, p. 19, 2007.

[25] Warner, J. S. and Johnston, R. G. A simple demonstration that the Global Positioning System (GPS) Is Vulnerable to Spoofing. Jornal da Administração de Segurança dos Estados Unidos, 2003.

[26] Humphreys , T. E.; Ledvina, B. M.; Psiaki, M. L.; O'Hanlon, B. W.; Kintner, P. M. Assessing the Spoofing Threat:Development of a Portable GPS Civilian Spoofer gps.mae.cornell.edu, p. 1-3, 2008. Disponível em: http://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf. Acesso em: 4 de novembro de 2015.