UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
CURSO DE GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Vinícius Jahn Machado

VULNERABILIDADE DOS SISTEMAS GNSS A ATAQUES DO TIPO SPOOFING

Santa Maria, RS, Brasil

2019

Vinícius Jahn Machado

VULNERABILIDADE DOS SISTEMAS GNSS A ATAQUES DO TIPO SPOOFING

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia Elétrica, da Universidade Federal de Santa Maria (UFSM), como requisito parcial para obtenção do grau de **Engenheiro Eletricista**.

Orientador: Prof. Dr. Marcelo Serrano Zanetti

Santa Maria, RS
2019

Vinícius Jahn Machado

VULNERABILIDADE DOS SISTEMAS GNSS A ATAQUES DO TIPO SPOOFING

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia Elétrica, da Universidade Federal de Santa Maria (UFSM), como requisito parcial para obtenção do grau de **Engenheiro Eletricista**.

Aprovado em 10 de dezembro de 2019:

_____

Marcelo Serrano Zanetti, Dr. Eng. (UFSM)
(Presidente/Orientador)

_____

Bruno Knevitz Hammerschmitt, Me. Eng. (CEESP, UFSM)

_____

Felipe Cirolini Lucchese, Me. Eng. (CEESP, UFSM)

Santa Maria, RS, Brasil
2019

AGRADECIMENTOS

Agradeço à minha família, especialmente aos meus pais Ivanio e Elaine e irmãos Vagner e Stéfani, por todo apoio, suporte, educação e ensinamentos.

Agradeço a Caroline, minha namorada, por todo apoio nos mais diversos momentos vividos durante a graduação, foi um pilar para estar concluindo o curso, por sempre acreditar no meu potencial.

Agradeço à minha segunda família, especialmente a Lisane, Patrícia, Eduardo e Jacob, por todo apoio, suporte e orientações.

De maneira especial, agradeço ao meu orientador, Professor Marcelo, por ter topado estudar um tema pouco abordado e de grande relevância, agradecimento pela amizade e disponibilidade em compartilhar o conhecimento ao orientar este trabalho, além de todo suporte proporcionado, tornando possível a conclusão do mesmo.

A UFSM, pela estrutura disponibilizada, ao Curso de Engenharia Elétrica e a todos professores presentes durante minha trajetória acadêmica, pelo conhecimento transmitido, meu muito obrigado.

Agradeço ainda aos amigos adquiridos nesse período de graduação, pelos bons momentos, apoio e companheirismo demonstrados ao longo do curso.

Aos colegas de apartamento do 1306 e 1207, pelos momentos de alegria e parceria, compartilhados ao longo da graduação.

RESUMO

VULNERABILIDADE DOS SISTEMAS GNSS A ATAQUES DO TIPO SPOOFING

AUTOR: Vinícius Jahn Machado
ORIENTADOR: Marcelo Serrano Zanetti

A vulnerabilidade das constelações GNSS se estendem além de bloqueios e perdas de sinais à ataques falsos, nos quais falsificações de sinais de comunicação são gerados com intuito de manipular a posição, velocidade e informações que um receptor recebe. Considerando que vários sistemas fazem parte da constelação GNSS, se viu necessário realizar um estudo dos sistemas e verificar como cada sistema se porta ao receber um ataque do tipo spoofing. Foi analisado os principais sistemas, GPS, GLONASS, Galileo e Beidou, em relação a frequências de comunicação e seus métodos de evitar um ataque de spoofing. Os dados de alguns sistemas por serem mais utilizados e até mesmo, mais conhecidos, são encontrados em documentos abertos disponíveis na internet, já outros menos conhecidos, são obtidos através de estudos realizados em Universidades. A combinação de estrutura de sinal conhecida e previsibilidade de bits de dados torna os sinais civis do GNSS um alvo fácil para ataques de falsificação. O trabalho faz uma análise sobre as contramedidas de cada sistema, se cada um tem um tipo específico ou se todos utilizam o mesmo padrão de defesa e nisso, uma abordagem sobre algumas contramedidas existentes

Palavras-chave: Spoofing, Anti-spoofing, GNSS.

ABSTRACT

VULNERABILITY OF GNSS SYSTEMS AT SPOOFING ATTACK

AUTHOR: Vinícius Jahn Machado
ADVISOR: Marcelo Serrano Zanetti

The vulnerability of the GNSS constellation extends beyond blocking and signal loss to fake attacks, where communication signal spoofs are generated to manipulate the position, speed, and information a receiver receives. Considering that several systems are part of the GNSS constellation, it was necessary to carry out a study of the systems and verify how each system behaves when receiving a spoofing attack. The main systems, GPS, GLONASS, Galileo and Beidou, were analyzed in relation to communication frequencies and their methods to avoid a spoofing attack. The data from some systems because they are more used and even better known, are found in open documents available on the Internet, while others less known, are obtained through studies conducted at universities. The combination of known signal structure and data bit predictability makes GNSS civil signals an easy target for spoofing attacks. The paper analyzes the countermeasures of each system, whether each one has a specific type or if they all use the same pattern of defense and in that, an approach to some existing countermeasures.

Keywords: Spoofing, Anti-spoofing, GNSS.

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Os receptores GNSS tornaram-se extremamente baratos e compactos nos últimos tempos. E estão sendo muito utilizados em sistemas de rastreamento constante de pessoas, animais, veículos, celulares e muitos outros produtos de consumo. O sistema GNSS é atrativo porque fornece uma localização precisa em qualquer receptor com visão clara do céu com uma precisão que se aproxima de quatro metros. (DOD, 2008) e de tempo de dez nano segundos (Lombardi et al. 2001).

O amplo uso dos sistemas que compõem a constelação GNSS, tanto nos veículos terrestres, como marítimos e aéreos, desperta o interesse de quem pode utilizar essa fragilidade do sistema para algum ato ilícito, como roubo de cargas, sequestros de aviões. Os sistemas de locomoção são dependentes do sistema de posicionamento, e basicamente onde a localização marcar, usuário tende a seguir à risca, sem saber ao certo se a localização é precisa ou não.

Devido a isso, pesquisas relacionadas ao sistema GNSS vem sendo desenvolvidas, com o intuito de aprimorar cada vez mais o sistema e aumentar a segurança de comunicação.

A técnica de spoofing é um aprimoramento do que se chama em redes de computadores de ataque DoS (Denial of service), que consiste em sobrecarregar a rede com mensagens falsas, porém as mensagens falsas emulam mensagens verdadeiras, de tal forma que os dispositivos da rede identifiquem, recebam e decodifiquem as mensagens. Em termos regulatórios, o spoofing não se enquadra na especificação da Anatel de bloqueador, portanto, seria perfeitamente legal utilizar um sistema desse tipo no Brasil.

Realizar um spoofing se torna bastante palpável com o surgimento de soluções baseadas no conceito de Software Defined Radios (SDR), que é um sistema relativamente mais barato, e possibilita qualquer pessoa criar um sistema de spoofing para interferir no recebimento dos dados da constelação GNSS.

Uma das motivações para a elaboração deste trabalho, é o noticiário comentando sobre alguns fatos em que é relatado a perda de sinal repentina ou variando a todo momento, perdendo a precisão dos dados de posicionamento, isto ocorrendo em navios, aeronaves e carros.

Um dos relatos, conforme abordado em (Nakedsecurity, 2017), cita que uma frota de navios que estavam no Mar Negro, tiveram seus sistemas de GPS variando com assiduidade, trazendo leituras erradas para todo o sistema de posicionamento, deixando toda a frota a mercê no meio do Mar Negro.

Uma segunda consideração a respeito da utilização do spoofing é citado em (Defesa.tv.br, 2019), onde o ataque é utilizado como meio de segurança na locomoção do presidente Vladimir Putin, onde é coincidentemente o chefe dos serviços secretos soviéticos e russo (KGB e FSB) e também presidente da Rússia. Há relatos em que todos os sistemas de posicionamento que se aproximavam do presidente, em uma passeata, os sistemas indicavam que a posição do equipamento estava a 65 quilômetros da costa, precisamente no aeroporto de Anapa (Defesa.tv.br, 2019).

Com esses relatos, e vários outros encontrados na internet, teve uma motivação a mais para elaboração deste trabalho, pois percebia que o problema relacionado a ataques de spoofing era reincidente em qualquer parte do mundo, e nesse sentido, procurou-se fazer uma abordagem de como cada sistema de georreferenciamento se portava ao ataque de spoofing e se eles possuem alguma contramedida efetiva para esse tipo de ataque.

2. OBJETIVO

O principal objetivo deste trabalho é apresentar os principais sistemas que estão em operação que compõem o Global Navegation Satellite System (GNSS). Após uma apresentação inicial sobre os principais sistemas, será realizada uma comparação entre eles e verificar se todos são susceptíveis a vulnerabilidade relacionada ao ataque do tipo Sspoofing, e se os sistemas utilizam algum padrão de segurança efetivo.

Seguindo que hoje, o spoofing é um tipo de ataque no sinal do receptor que pode causar sérios dados para o usuário, sem que ele perceba, é de relevância trazer uma abordagem do tema sobre os tipos de spoofing e quais as principais técnicas existentes para se proteger dele.

3. METODOLOGIA

3.1 SISTEMA GNSS

GNSS é um termo genérico para Sistema Global de Navegação por Satélite, dois quais existem hoje, apenas dois exemplos completos de sistema, que é o GPS, que é um sistema

controlado pelos Estados Unidos e o GLONASS que é um sistema controlado pela Rússia. Além dos dois sistemas completos, existem outros dois sistemas tornando-se globais, que é o Galileo, que é um sistema Europeu e o sistema chinês, denominado Beidou-2. Cada sistema é mantido por uma organização chamada de "constelação". Os projetos gerais de todas as formas do GNSS são notavelmente semelhantes, todas transmitem três mensagens básicas:

- Um sinal de variação de posição, velocidade e tempo (PVT);
- Dados efêmeros precisos, que especificam a localização exata de cada satélite;
- Um almanaque, que especifica as localizações e órbitas de todos os satélites na constelação, juntamente com informações de saúde e integridade de cada satélite.

O sistema GNSS, permite que os receptores leiam os sinais das quatro principais constelações de satélites, o GPS, GLONASS, Galileo e Beidou, portando, evitando assim certos apagões em terrenos urbanos ou outros com má área de recepção.

Estima-se que até em 2020, cerca de 100 satélites GNSS estarão disponíveis, com previsão de 30 a 40 estarem visíveis a qualquer momento. Todos os tipos de satélites GNSS transmitem em pelo menos duas bandas, um código civil não criptografado, denominado código C/A e um código militar criptografado, chamado P(Y).

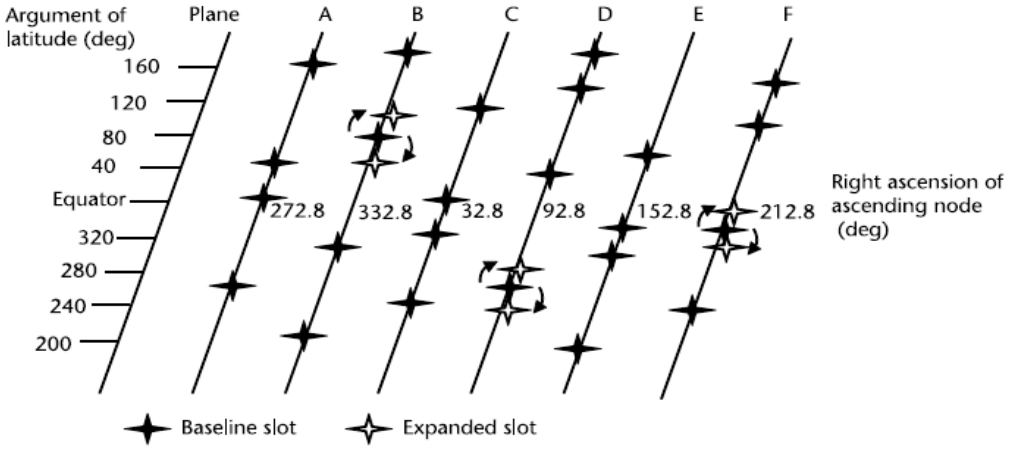
3.2 GPS

O GPS é representado por um sistema espacial de navegação que utiliza de uma rede de no mínimo 24 satélites que orbitam a Terra em posições determinadas. São dispostos de tal maneira de que toda a superfície terrestre esteja visível para no mínimo quatro satélites.

O GPS apesar de ter sistemas concorrentes, é o mais utilizado e o mais estável, pois ele é um aperfeiçoamento do antigo sistema chamado TRANSIT, que se encontrava em operação em 1964 até meados de 1995, quando o GPS se tornou o principal sistema de localização americano (GPS, 2013).

Os satélites desse sistema, orbitam a Terra duas vezes ao dia, transmitindo informações para a terra a uma altitude de aproximadamente 20200 km. Os satélites ficam dispostos em seis planos orbitais igualmente espaçados em torno da Terra, e em cada plano possuindo 4 satélites (GPS, 2013). A partir desse arranjo é assegurado que pelo menos 4 satélites estarão visíveis ao mesmo tempo e em qualquer ponto terrestre, conforme pode ser visto.

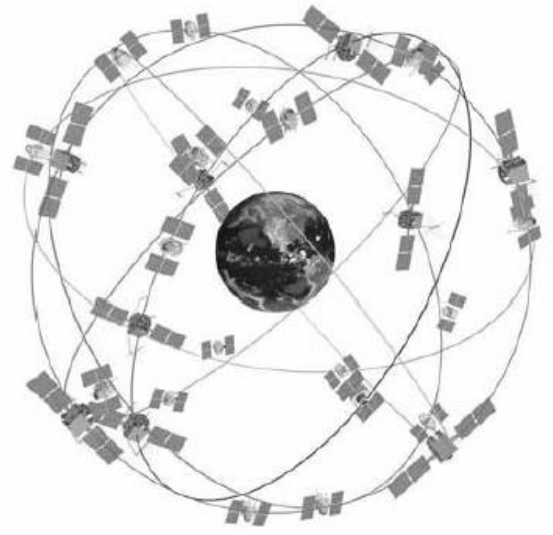
Figura 3.1 – Constelação plana GPS.



Fonte: KAPLAN, 2017.

Com as informações recebidas, os receptores GPS são capazes de realizar uma trilateração, sendo possível calcular a posição exata do usuário. O sistema é um relógio de alta precisão e compara a todo instante o tempo em que um sinal é transmitido com um sinal que é recebido. A diferença desse tempo é utilizada para calcular a distância entre o satélite e o receptor. Quando ao menos 3 satélites são utilizados é possível a obtenção da latitude e da longitude, e a partir de 4 satélites é possível a medida da altitude. Após os cálculos de posicionamento, diversas medidas podem ser feitas, tais como direção, rota, distância de viagem, velocidade do usuário etc.

Figura 3.2 – Constelação GPS.



Fonte: KAPLAN, 2017.

3.2.1 Segmento espacial

Inicialmente existiam 24 satélites orbitando 6 órbitas. Cada órbita com inclinação de 55 graus em relação a linha do Equador, ou seja, 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, portando um satélite passa por Terra duas vezes ao dia.

O sistema foi projetado para que mesmo se 2 dos 24 satélites falhem, o sistema permanece completamente operacional. A diferença angular entre os satélites numa mesma órbita é de 30, 105, 120 e 105 graus, que somando resulta em 360 graus (THOMASSEN, [2017]).

Toda informação do satélite, incluindo sua posição, o estado dos relógios e o estado da rede, são codificados. Geralmente esses sinais são transmitidos em duas frequências portadoras diferentes, uma pública e uma militar.

3.2.2 Segmento de controle

São os centros de controle de terra, que compreende uma estação principal de controle, tendo 12 antenas de controle em 16 locais de monitoramento, conforme Figura 3. Sua principal atividade é o monitoramento das órbitas e a sincronia dos satélites, que também estão sob a jurisdição da força aérea americana.

Figura 3.3 – Distribuição mundial das estações e antenas do sistema GPS.

Fonte: DOD, 2008.

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

O almanaque é formado por dados sobre a órbita e estado de cada satélite da constelação, um modelo ionosférico, e dados para ajustar o horário GPS com padrão (UTC). 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 a precisão da localização.

3.2.3 Segmento de usuário

Corresponde ao aparelho GPS utilizado pelo usuário, com a respectiva antena. Os sinais enviados pelos satélites são decodificados em diferentes canais, passando ao usuário as informações desejadas.

Geralmente, os receptores GPS têm uma antena sincronizada com as frequências transmitidas pelos satélites, processador e um relógio altamente estável. 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.

3.3 GLONASS

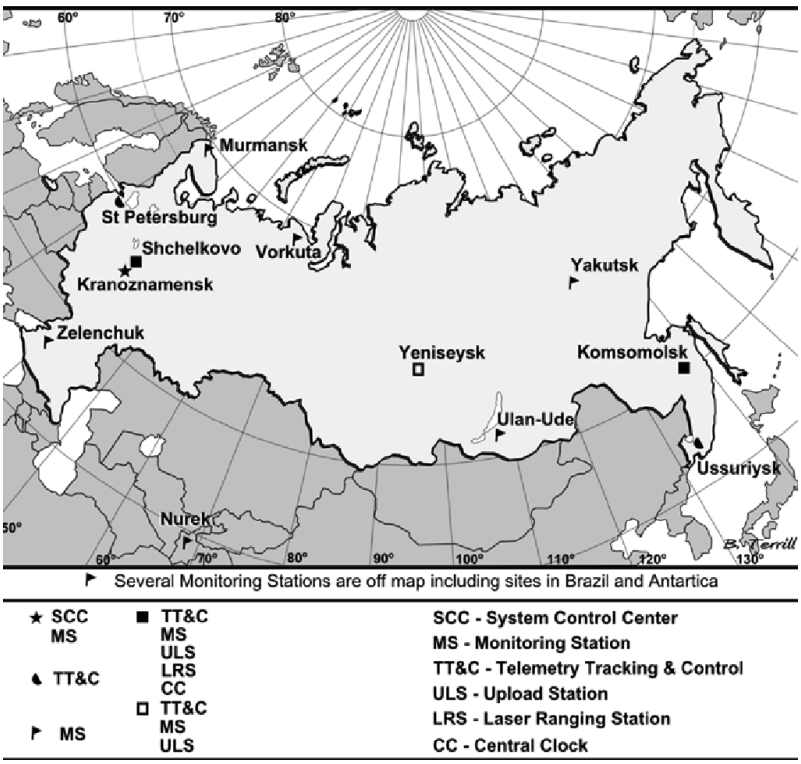
3.3.1 Segmento espacial

O segmento espacial GLONASS consiste nominalmente em 24 satélites ativos, mais 6 reservas. Estão posicionados em uma órbita de 19.100 km com uma inclinação de 64,8°, e um período de revolução de 11 horas e 15 minutos. Os 24 satélites estão uniformemente localizados em três planos orbitais, 120° separados em ascensão reta. Cada plano contém oito satélites, igualmente espaçados com 45° de deslocamento em argumento de latitude. O ciclo de repetição da pista terrestre para o GLONASS é de 8 dias.

3.3.2 Segmento terrestre

O Complexo de Controle Terrestre (GBCC) é responsável para as seguintes funções de medição e previsão de efemérides individuais dos satélites, upload de efemérides previstas, correções do relógio e informações de almanaque. Além disso, é responsável pela sincronização dos relógios de satélite com o tempo do sistema GLONASS e todo o comando, controle, manutenção e rastreamento dos satélites para manter em perfeito uso. O segmento de controle terrestre GLONASS é totalmente instalado em território russo, conforme pode ser visto na Figura 3.4.

Figura 3.4 – Segmento de terra GLONASS.



Fonte: KAPLAN, 2017.

3.4 BEIDOU

O Sistema de Navegação por Satélite BeiDou (BDS) é um sistema global de navegação por satélite independentemente desenvolvido e operado pela China. O BDS foi projetado para ser compatível e interoperável com outras constelações do GNSS (KAPLAN, 2017).

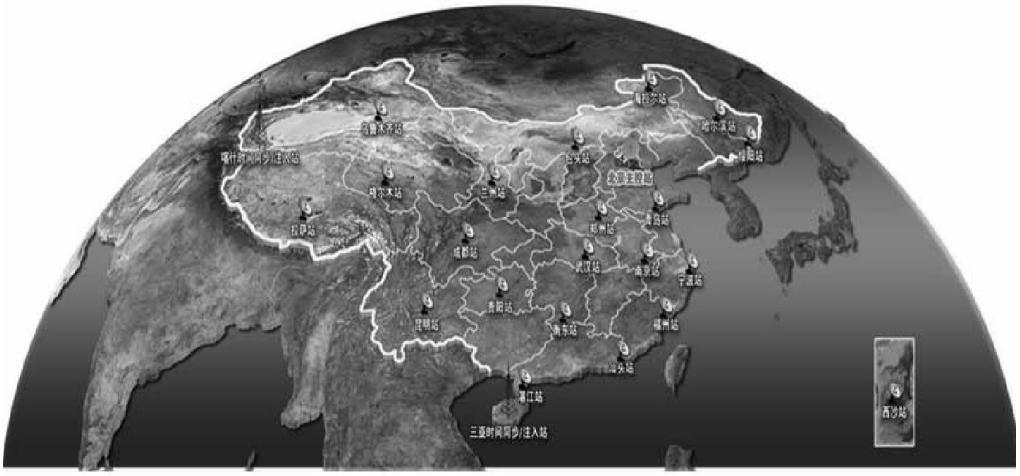
Semelhante ao GPS, GLONASS e Galileo, o BDS é um sistema de navegação baseado em espaço sistema que utiliza o mecanismo de posicionamento de trilateração. O BDS consiste em um segmento espacial, um segmento de controle e um segmento de usuário.

O segmento de controle é uma rede de controle de terra, distribuída com uma estação de controle principal, várias estações de sincronização e upload de informações, além de várias estações de monitoramento. O segmento de usuário do BDS inclui vários BDS de modo de terminal único. O BDS multimodo são compatíveis com outros sistemas GNSS e a principal funcionalidade do BDS é fornecer 24 horas por dia, para qualquer clima, serviço contínuo de posicionamento, navegação e cronometragem (PNT) de alta precisão para usuários.

O BDS junto com GPS, GLONASS e Galileo, foi identificado pelas Nações Unidas (ONU)Comitê Internacional de Sistemas Globais de Navegação por Satélite (ICG) como um dos fornecedores oficiais de GNSS. Com uma infraestrutura nacional crítica de informações espaciais, uma navegação global de satélites de informação é muito importante para defesa nacional, desenvolvimento econômico, e melhora de vida das pessoas. A China atribui grande a importância ao desenvolvimento e suas aplicações do BDS. O desenvolvimento do BDS tem como objetivo construir um sistema de navegação global baseado no desenvolvido de forma independente, aberto e compatível, tecnicamente avançado, estável e confiável para promover a formação da cadeia industrial de navegação por satélite.

Todo o sistema de controle do Beidou, reside na China. Com sua unidade mestre localizada em Beijing. As bases para estações de upload foram escolhidas com base no design da constelação, para que as estações possam rastrear de maneira ideal os satélites. As estações de monitoramento Classe A, ao total de 7, estão bem distribuídas em toda a China e usado para determinação da órbita dos satélites e calibração. As 22 estações de monitoramento de Classe B estão localizadas uniformemente em todo o país e são responsáveis por monitorar a integridade do sistema. A distribuição do segmento de controle é mostrada na Figura 3.5.

Figura 3.5 – Distribuição do segmento de controle BDS.



Fonte: KAPLAN, 2017.

3.5 GALILEO

O sistema Galileo quando totalmente implantado consistirá em 24 satélites operacionais mais seis peças em órbita, posicionadas em três planos circulares da Órbita Média da Terra (MEO) a 23.222 km de altitude acima da Terra e com uma inclinação dos planos orbitais de 56 graus em relação ao Equador.

O sistema GALILEO terá características semelhantes e será totalmente compatível com o GPS e GLONASS, porém totalmente independente. Uma vez terminada a fase de definições do projeto, o cronograma assinala a existência de uma constelação inicial de até 5 satélites em operação.

3.5.1 Segmento espacial

A geometria de referência da constelação do Galileo é o resultado de estudos detalhados para otimizar o número de satélites para a prestação de serviços ao usuário final. O design do sistema resultou inicialmente em uma constelação com 27 satélites operacionais em uma constelação Walker 56º27/3/1", significando 27 satélites em 3 planos, inclinados a 56 graus, e para cada um dos três planos orbitais foi planejado ter um satélite reserva inativo, para se recuperar mais rapidamente das falhas finais do satélite.

3.5.2 Segmento de terra

O segmento de terra do Galileo (GCS), tem como principais funções monitorar e controlar os satélites operacionais por meio de contatos periódicos entre os satélites e as estações de telemetria, rastreamento e controle (TT&C), monitorar e controlar os ativos terrestres e dar suporte de preparação, treinamento e validação de operações.

As operações de plataforma e carga útil e atividades de manutenção, como notas do software de bordo, análise de telemetria e planejamento e execução, manobras de manutenção de órbitas são tarefas essenciais do GCS. A manutenção de geometria de constelação inclui também operações de recuperação, a fim de atender situações de emergência e falhas de satélites com o objetivo de minimizar o tempo quando o satélite não está contribuindo para o funcionamento do serviço.

3.6 CARACTERÍSTICAS DOS SINAIS

A Tabela 3.1 apresenta um resumo de todas as frequências de comunicação dos principais sistemas do GNSS, nela é percebia que apesar de termos quatro diferentes sistemas basicamente implantados, temos uma grande semelhança na parte do uso das frequências, como pode ser visto.

Tabela 3.1 – Comparativo dos principais sistemas GNSS.

Frequências	**GPS**	**GLONASS**	**BEIDOU**	**GALILEO**
F 1	1.575,4Mhz	1.602,4Mhz	1.561,0Mhz	1.575,4Mhz
F 2	1.227,6Mhz	1.246,2Mhz	1.207,1Mhz	1.278,7Mhz
F 3	1.381,0MHz	1.204,7Mhz	1.268,5Mhz	1.191,7Mhz

Fonte: Autor, 2019.

Percebe-se de maneira clara que as frequências variam no geral de 1,2 a 1,6 GHz, como pode ser visto na Tabela 3.1. Para transportar as informações digitais, os segmentos desses sinais básicos são deslocados em fase, como é o caso do GPS e do GLONASS L1. O método usual é o BPSK (“Chaveamento de mudança de fase binária”), que codifica 1 bit por mudança de fase (Betz, 2002). Outras variações são QPSK (“Quadratura em fase”), que usa quatro turnos de fase para codificar 2 bits, conforme é utilizado no Beidou-2, Galileo E1 e projetado para interoperar com o GPS L1.

Em todos os casos, o que é codificado na onda da portadora analógica consiste em uma sequência de números pseudoaleatórios (PRN). O PRN é transmitido em uma ordem de magnitude mais lenta que a portadora, no caso do GPS L1, a 1 megabits por segundo. O comprimento do PRN civil é de 1023 bits, que dura 1 milissegundo, e depois se repete. O código W, usado no GPS L2, tem 6,1871 x 10^{12} bits e leva uma semana para transmitir (KAPLAN, 2017).

Os sinais GPS, Galileo e Beidou-2 são transmitidos usando CDMA (“Divisão de código de acesso múltiplo”), que espalha o sinal em torno de uma frequência nominal. Isso permite que vários sinais, um de cada satélite, são identificados pelos seus códigos PRN e são transmitidos na mesma frequência. O GLONASS por outro lado, utiliza o FDMA, que dedica uma frequência separada para cada satélite da constelação, mas também usa a conexão PRN para codificar o sinal.

3.7 OQUE É O SPOOFING

O spoofing é provisão de sinais do tipo GNSS, transmitidos localmente e codificados para enganar o receptor a pensar que está em algum lugar que na verdade não é.

Um ataque de spoofing de GNSS tenta enganar um receptor transmitindo sinais incorretos, estruturados e assemelhando a um conjunto de sinais originários da constelação GNSS. Esses sinais falsificados podem ser modificados de modo a fazer com que o receptor calcule sua posição para estar em um local incorreto, ou até mesmo localizado onde está, mas com um horário diferente, conforme determinado por quem está realizando o ataque, a Figura 3.6 ilustra como funciona o ataque de spoofing.

Uma forma comum de ataque de spoofing do GNSS, comumente denominado “ataque de fuga”, começa transmitindo os sinais sincronizados com os sinais genuínos observados pelo receptor alvo. Com isso, a potência do spoofing é aumentada gradualmente para que o receptor GNSS da embarcação rastreie os sinais falsos que podem ser manipulados para informar um local diferente do que os indicados pelo sinal genuíno, e sem que o usuário percebesse tal alteração.

Figura 3.3 – Exemplificação Spoofing.

Fonte: INTERTANKO, 2019.

O spoofing é mais perigoso que o jamming pois o alvo normalmente não consegue detecta-lo, e pode continuar navegando através de uma rota não confiável, por isso, se deve dar uma atenção a mais nesse problema.

O spoofing é de certa forma mais sutil que o jamming, e depende da geração de um sinal falso com uma potência elevada, em direção a um receptor. E isso pode ser tratado assim, porque no céu e considerando as condições atmosféricas, a intensidade do sinal pode variar entre -160dbW e -153dbW.

As únicas diferenças detectáveis entre sinais legítimos de satélite e sinais *spoofing* são as discrepâncias no tempo, na direção do sinal, potência, e a relação sinal/ruído.

A maioria dos receptores modernos não estão equipados para detectar essas diferenças, e isso também acarretaria uma elevação do custo de tal receptor. Além disso, por necessidade as antenas receptoras são encontradas em locais em que tenham acesso ao espaço, isso dificulta a distinção de um sinal legítimo de um sinal falsificado, pois o receptor não tem como saber se o sinal vem de um local verídico ou não.

Dado a possibilidade de criar uma situação de spoofing, existem técnicas e tipos específicos para cada situação de ataque. E qualquer tipo de ataque é considerado ilegal na maior parte dos países do mundo.

3.7.1 Tipos de Spoofing

Captura aberta

É conhecido como captura aberta, quando o spoofer não tenta ocultar sua tentativa de burlar o sistema de destino. Consequentemente, o spoofer não precisa alinhar seus sinais simulados com suas contrapartes autênticas na antena no início do ataque, em vez disso, pode simplesmente bloquear as faixas de frequências do alvo, causando com que o receptor alvo perca os sinais e tente readquiri-los, uma espécie de jamming. Após um prelúdio de interferência, o spoofer obterá com sucesso o controle dos loops de rastreamento do receptor de destino se seus sinais simulados chegam com energia suficiente para que excedam confortavelmente a detecção de aquisição do receptor-alvo e os sinais autênticos tem sua potência inferior aos sinais falsificados.

Captura secreta

Na captura secreta, presume-se que o sistema de navegação da aeronave esteja equipado com detecção de falsificação de sinal, medidas essas que o spoofer deve evitar acionar. Conforme abordado na introdução, algumas técnicas de spoofing estão longe de serem implementadas e comercializadas, devido ao seu alto custo e por serem equipamentos pesados para ter seu uso prático para pequenos ARPs. A captura do sistema de navegação será considerada secreta se o spoofer atender a todas as condições de captura aberta e evitar algumas técnicas de detecção, tais como monitoramento de Jamming to noise (J/N) no receptor, monitoramento de desbloqueio de frequência do receptor e teste no estimador do sistema de navegação.

Captura secreta de loops de rastreamento de receptores GNSS

Para fazer a captura secreta dos loops de rastreamento do receptor o spoofer não deve causar desbloqueio de frequência em nenhuma PLL. Para isso, deve garantir que dentro do receptor alvo, todos os sinais de falsificação estão perfeitamente alinhados com seus equivalentes autênticos na fase de código. Uma vez alinhados, os sinais de falsificação podem ser elevados acima da potência dos sinais autênticos para assumir o controle. O alinhamento entre os sinais autênticos requer que todos os atrasos sistemáticos e geométricos e suas taxas de variação no tempo são conhecidos e contabilizados na produção dos sinais de falsificação. Enquanto um spoofer adequadamente projetado é capaz de perfeitamente contabilizar os atrasos devido a interferências e atrasos internos, compensando com precisão os atrasos e taxas geométricas onde requerem conhecimento preciso da posição e da velocidade do spoofer e da

aeronave alvo. Isso torna um spoofing relativamente de difícil implementação, pois qualquer dado incoerente torna o spoofing perceptível.

3.7.2 Classificação do ataque de Spoofing

Os ataques de spoofing podem ser classificados em três tipos: Ataque simples, ataque intermediário e ataque avançado ou ataque sofisticado. A seguir será descrito como funciona cada um deles (HUMPHREYS, 2008).

Ataque simples

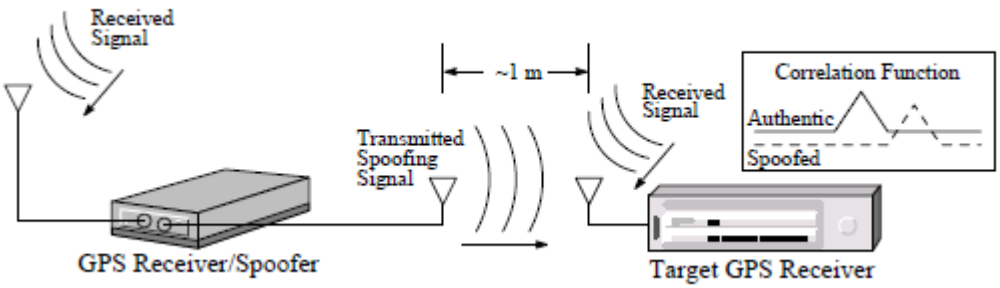
Normalmente esse tipo de ataque age como um *jamming*, congestionando o sinal do receptor, fazendo com que o receptor da vítima perca a comunicação com o satélite e tenha que fazer a reaquisição do pacote. Esse processo, aumenta bastante a chance de o receptor perceber que pode estar recebendo sinais falsos e se tiver alguma alteração repentina na estimativa de tempo do receptor, o receptor vai sinalizar para o usuário que está com possíveis evidências de não estar recebendo sinais originários da constelação GNSS.

Em resumo, a facilidade de montar um ataque via simulador de sinal, torna esse modo de ataque relativamente provável. E infelizmente, embora um ataque via simulador ser de fácil detecção, ainda não temos contramedidas estruturadas para liquidar esse tipo de ataque de spoofing, deixando o sistema vulnerável até mesmo para um ataque considerado simples.

Ataque intermediário

Um dos desafios para realizar um ataque de spoofing bem-sucedido é saber com precisão a posição e velocidade do receptor alvo, pois sem essas informações o ataque pode der facilmente detectado.

Figura 3.7 – Ilustração do ataque de spoofing via receptor portátil.



Fonte: HUMPHREYS, 2008.

Um ataque via receptor portátil, como mostrado na Figura 7, supera algumas dificuldades de construção, pois o receptor spoofer pode ser pequeno o suficiente para ser colocado discretamente próximo da antena do receptor alvo. Tendo o receptor spoofer próximo da antena alvo, o receptor spoofer consegue captar os sinais genuínos e com isso estimar a posição, velocidade e tempo. Após obter a posição, velocidade e tempo, o aparelho então gera os sinais falsos e executa o spoofing.

Ataque sofisticado via múltiplos receptores spoofer portáteis

Esse ataque apresenta os mesmos desafios dos tipos de ataques citados anteriormente e com um acréscimo de múltiplos receptores-spoofer e uma complexidade adicional que as perturbações dos sinais vindas, devem estar coordenadas em fase. A única defesa conhecida contra esse tipo de ataque é a autenticação criptográfica, que é utilizada basicamente por todos os sistemas que fazem parte do GNSS.

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.

3.8 INFLUÊNCIA DO SPOOFING NA POSIÇÃO

Para que seja possível que os receptores consigam calcular a sua posição na superfície terrestre, são precisas técnicas especializadas, dado que os satélites estão em constante movimento. Para isso, utilizam-se fórmulas trigonométricas no receptor, de maneira a que este

consiga calcular a sua localização na superfície terrestre. O modelo que é utilizado denomina-se trilateração, que são medidas de distâncias com base no tempo de propagação.

A trilateração consiste na aquisição da distância dos satélites através do tempo de propagação da onda eletromagnética, que é transmitida pelo satélite até o receptor. E então o receptor calcula a distância do satélite através da seguinte equação.

$$d = c \times t_d$$

Onde d é a distância, c é a velocidade da luz no vácuo e t_d é o tempo de propagação entre o satélite e o receptor. O receptor calcula o t_d através da comparação do tempo enviado na mensagem com o tempo recebido pelo receptor, onde é extraída a diferença entre os dois tempos.

O cálculo de cada posição é obtido com a intersecção das medições realizadas pelos satélites, no caso a trilateração. Com a intersecção de apenas três satélites, é possível calcular uma posição em duas dimensões (Latitude e longitude). Contudo, para que o cálculo dessas posições seja perfeito, não pode existir erros nas medições de tempo efetuadas. Com a intersecção de mais um satélite, já é possível obter a posição a três dimensões (latitude, longitude e altitude).

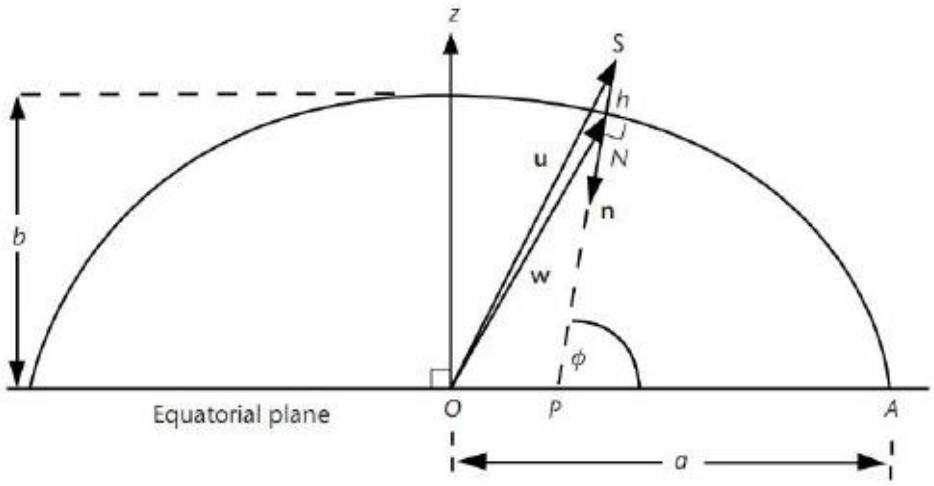
A tarefa fundamental de um sistema GNSS é calcular a posição. Para fazer isso é necessário criar um conjunto de coordenadas com eixos perpendiculares que se cruzam em uma origem que é rigidamente preso a terra. Esses sistemas de coordenadas são chamados de ECEF (Centrado na Terra, Fixo na Terra). Esses sistemas de coordenadas funcionam bem para expressar a posição de um usuário na Terra enquanto ele gira com a própria Terra e a posição de um usuário estacionário na superfície da terra é constante.

O sistema de coordenadas ECEF mais usado é conhecido como WGS 1984, que foi desenvolvido pelo departamento de defesa dos EUA. WGS 84 é um quadro ECEF definido da seguinte forma.

O Sistema ECEF contém sua origem no centro da esfera referente a Terra, com plano x e y localizado sobre o plano equatorial e eixo z sobre o eixo de rotação terrestre com valores positivos direcionados para o norte. Embora o sistema de coordenadas ECEF seja de simples utilização, o planeta Terra não é bem representado por uma esfera e sim através de uma elipsoide de revolução geocêntrica. Assim, foi definido o sistema de referência WGS ("*Word Geodetic System*"), que apresenta os eixos x, y e z dispostos conforme o sistema ECEF, com

semieixo maior *a* contido no plano equatorial e semieixo menor *b* na direção do eixo z, conforme mostra a Figura 3.8.

Figura 3.8 – Modelo elipsoidal terrestre.



Fonte: RODRIGUES, 2011.

A figura ilustra a representação da Terra por meio do modelo elipsoidal com semieixos maior *a* e menor *b,* vetor de posição *u* de um usuário S com altitude *h,* vetor de posição *w* do ponto *N* na superfície e a latitude ϕ referente ao usuário.

Para cálculo, é adotado como padrão para utilização no sistema GPS, os parâmetros definidos pela WGS84. Os principais parâmetros são listados na Tabela 3.2.

Tabela 3.2 – Principais parâmetros do WGS84.

PARÂMETROS	VALORES
Semi-eixo maior	a = 6378137 m
Semi-eixo menor	b = 6356752,31 m
Excentricidade	e = 0,08181918994
Achatamento geométrico	f = 1/298,257223563
Velocidade angular da Terra	We = $7929115*10^{-11}$ rad/s
Constante gravitacional terrestre	μ = $3989005*10^{8}$ m^3/s^2

Fonte: KAPLAN, 2017.

Primeiro calcula-se λ por:

$$\lambda = tan^{-1}\,\frac{Yu}{\mathrm{Xu}}\,, Xu \geq 0$$

$$\lambda = 180° + \ tan^{-1}\,\frac{Yu}{\mathrm{Xu}}\,, Xu < 0\ e\ Yu \geq 0$$

$$\lambda = -180° + \ tan^{-1}\,\frac{Yu}{\mathrm{Xu}}\,, Xu < 0\ e\ Yu < 0$$

Posteriormente pode-se calcular a latitude ϕ e a altura h de diferentes formas. O cálculo das coordenadas geodésias pode ser realizado utilizando o método iterativo de Bowring, demonstrado abaixo.

Inicialmente, calcula-se os valores p e tan u_0:

$$p = \sqrt{x^2 + y^2}$$

$$\tan u_0 = \left(\frac{z}{p}\right)\left(\frac{a}{b}\right)$$

Inicia-se o laço interativo:

$$\cos^2 u = \frac{1}{1 + \tan^2 u_0}$$

$$\sin^2 u = 1 - \cos^2 u$$

$$\tan u = \left(\frac{b}{a}\right)\tan \phi$$

Verifica-se se tan u = tan u. Se for falso, é feito tanu_0 = tan u e continua-se o laço. Se for verdadeiro, é terminada a conversão calculando o valor de N e h conforme mostrado abaixo:

$$N = \frac{a}{\sqrt{1 - e^2\ sin^2\phi}}$$

Para ϕ ≠ ±90°:

$$h = \frac{p}{\cos \phi} - N$$

Ou para ϕ ≠ 0:

$$h = \frac{Z}{\sin \phi} - N + e^2 N$$

Este método iterativo pode ser considerado exato por não exigir mais do que uma iteração e apresenta erros no cálculo de ϕ desconsideráveis para h>= -6300, embora não seja indicado para valores de ϕ próximos de +-90.

Também é possível calcular diretamente o vetor u = (*Xu, Yu e Zu*) de coordenadas cartesianas a partir de (ϕ, λ, h), através das equações:

$$Xu = \frac{a\cos\lambda}{\sqrt{1+(1-e^2)tan^2\phi}} + h\cos\lambda\, cos\phi$$

$$Yu = \frac{a\sin\lambda}{\sqrt{1+(1-e^2)tan^2\phi}} + h\sin\lambda\, cos\phi$$

$$Zu = \frac{a\,(1-e^2)\sin\phi}{\sqrt{(1-e^2)sin^2\phi}} + h\sin\lambda\, cos\phi$$

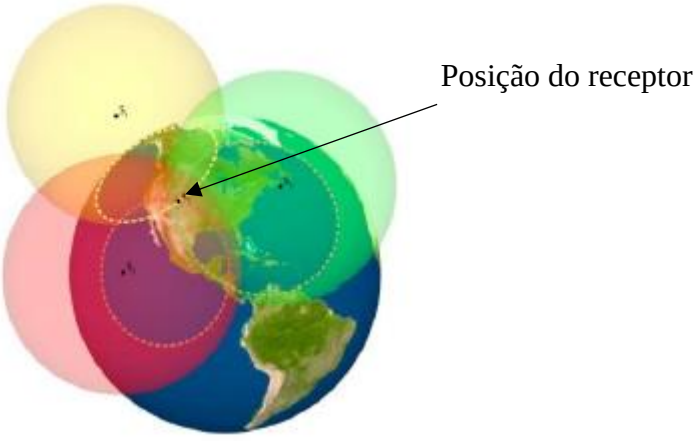
O sistema permite determinar o posicionamento em três dimensões de uma antena receptora que capta sinais de satélites que estão em órbita no planeta Terra. Recebendo esses sinais e determinando o tempo de propagação da antena, do satélite até a antena receptora ($t_u - t_s = \Delta t$), é possível determinar a distância aproximada *d* desses dois pontos. Dessa forma, a pseudodistância é calculada por:

$$d = c(t_u - t_s) = c\Delta t$$

Considerando, a velocidade da luz no vácuo, $c = 3.10^8$m/s

De forma análoga é considerado o caso real de 3 dimensões (x, y, z), as circunferências são consideradas esferas com centro na posição de cada satélite S_i (X_i, Z_i, Y_i) e de raio d_i. A posição do receptor é determinada geometricamente pela intersecção de três esferas de satélites com o planeta Terra, determinando o único ponto possível a_1 que apresenta as distâncias d_i medidas de cada satélite. Conforme mostra a Figura 3.9.

Figura 3.9 – Geometria de posicionamento com três satélites.



Fonte: Autor, 2019.

A determinação do posicionamento do receptor ($X_{u,}Z_u, Y_u$) consiste na resolução do sistema de três equações e três incógnitas:

$$(X_u - X_1)^2 + (Y_u - Y_1)^2 + (Z_u - Z_1)^2 = {d_1}^2$$
$$(X_u - X_2)^2 + (Y_u - Y_2)^2 + (Z_u - Z_2)^2 = {d_2}^2$$
$$(X_u - X_3)^2 + (Y_u - Y_3)^2 + (Z_u - Z_3)^2 = {d_3}^2$$

Essas equações são simplificadas porque a Terra é melhor representada através de uma elipsoide de revolução ao invés de uma esfera. E além disso, é considerado que os relógios dos satélites estão em perfeita sincronia com o relógio do receptor, o que não acontece na realizada devido à baixa precisão dos relógios utilizados no segmento de usuários (comparado aos relógios atômicos dos satélites).

Esse erro de precisão no cálculo pode ser chamado de δt, e a equação anterior 3.19 pode ser reescrita com a nova incógnita, exigindo com que seja observado um quarto satélite.

$$d_1 = \sqrt{(X_u - X_1)^2 + (Y_u - Y_1)^2 + (Z_u - Z_1)^2} - C\delta t$$
$$d_2 = \sqrt{(X_u - X_2)^2 + (Y_u - Y_2)^2 + (Z_u - Z_2)^2} - C\delta t$$
$$d_3 = \sqrt{(X_u - X_3)^2 + (Y_u - Y_3)^2 + (Z_u - Z_3)^2} - C\delta t$$
$$d_4 = \sqrt{(X_u - X_4)^2 + (Y_u - Y_4)^2 + (Z_u - Z_4)^2} - C\delta t$$

Essas equações não lineares podem ser resolvidas utilizando soluções fechadas, métodos interativos a partir da linearização ou filtro de Kalman.

Para considerações, vamos supor que temos (ϕ, λ, h) conhecidos, é possível determinar a posição do receptor usuário para coordenadas cartesianas, se necessário, aplicando as equações 3.13, 3.14 e 3.15.

Um ataque de spoofing na aquisição do posicionamento do satélite, altera principalmente as posições Xu, Yu (ϕ, λ), sem que o usuário perceba tal alteração.

3.9 COMO SE COMPORTA O SISTEMA GNSS AO SPOOFING

Muitas contramedidas já foram propostas para se proteger do spoofing no sistema GNSS, algumas baseadas no processamento de sinais, outras baseando-se na qualidade do sinal e a mais atual e utilizada, a criptografia do sinal. Basicamente todos os sistemas que fazem parte

do GNSS, sofrem pelos mesmos problemas, principalmente por usarem os mesmos tipos de comunicação e frequência, apenas tendo uma alteração do nome.

Em relação ao processamento de sinais, o sinal de RF analógico de entrada da antena é o primeiro sinal amplificado e depois convertido para uma frequência mais baixa e sua potência de sinal ajustada. Após a conversão digital, um código PRN se duplica e é utilizado para separar os sinais de cada satélite. Em várias etapas deste processo, é possível monitorar a aquisição e o rastreamento de sinais para anomalias que podem indicar que um ataque de spoofing está em andamento, porém, esse método que era utilizado, não eliminava efetivamente o spoofing, deixando o sistema ainda vulnerável.

A técnica de monitoramento da qualidade do sinal observa a qualidade e monitora os picos de potência do sinal. Ataques de spoofing em um receptor podem afetar a correlação de saída do monitor, semelhante à dos componentes de caminhos múltiplos. Essa técnica é utilizada aplicando testes de razão de delta para detectar qualquer assimetria anormal, e principalmente os picos de correlação impostos pelo ataque de spoofing.

A técnica da qualidade do sinal, é um método poderoso para detectar o spoofing, especialmente quando utilizadas na linha de ambientes de propagação visual. No entanto, na presenta de múltiplos caminhos a técnica pode não ser capaz de discriminar os sinais de falsificação e os sinais originários, tornando o sistema pouco aplicado.

Em geral, a criptografia tem sido frequentemente a proposta como solução para a ameaça de spoofing no sistema GNSS por ser mais eficiente, de fato. No entanto, para os bilhões de dispositivos comerciais espalhados por todo o mundo, que já usam o sistema civil não criptografado, não é possível adicionar qualquer forma de criptografia a esses protocolos públicos, sendo essa técnica utilizada apenas para comunicações militares.

A única técnica de criptografia atualmente em uso, para os mais diversos sistemas, é a criptografia de código P, usada exclusivamente para aplicações militares, e as aplicações civis ficando vulneráveis a qualquer tipo de ataque de spoofing, por não possuírem contramedidas eficazes.

A criptografia é amplamente utilizada pelos sistemas, no GPS as frequências L1 e L2 são usadas para transmitir dados de navegação totalmente criptografados. Serviços similares a criptografia utilizada nas frequências L1 e L2 também são utilizadas para o sinal VT do GLONASS, no código Q do Beidou nas frequências B1 e B2 e em Galileo na frequência E6. Embora os principais detalhes dessas técnicas de criptografia são de informações secretas e quase nada é conhecido publicamente sobre o GLONASS, Beidou e Galileo, ao longo dos anos surgiram detalhes a respeito do código de criptografia utilizado pelo GPS, o código P(Y).

No GPS, a criptografia acontece basicamente multiplicando um código P, por um código W, surgindo assim o código P(Y). Cada um dos 34 códigos W pré-gerados tem 15.345.000 chips. Com isso, esse código leva uma semana para ser transmitido por completo. O código P(Y) criptografado também é transmitido a cerca de 28dB abaixo do nível de ruído térmico típico de um receptor. O código W, é um elemento que varia regularmente, e as informações referentes a esse código fica a poder militar. Essas medidas de criptografia do GPS, são impraticáveis para os receptores civis, pois teria que haver uma alteração no hardware do sistema e com isso o seu custo se elevaria demasiadamente.

No entanto, uma modificação para sinais civis foi proposta por Scott (SCOTT,2003), e outra por Kuhn (KUHN, 2004), em que curtas sequências de códigos de segurança de espectro de dispersão são utilizadas para modificar o sinal de navegação. No entanto, os métodos propostos requerem alteração no protocolo padrão do sinal, tornando esse método impraticável.

Como vimos até agora no decorrer desse trabalho, os diversos sistemas GNSS utilizam praticamente as mesmas frequências. Isso se torna um problema geral pois as mesmas interrupções de sinais que pode acontecer com o GPS, por exemplo, pode também afetar o sistema GLONASS, SATNAV, BEIDOU e GALILEO. Nenhum dos sistemas tem uma forma eficiente de proteger das falsificações de sinais, e também, é muito pouco abordado os métodos existentes, e isso chama atenção devido as incidências desse tipo de problema estar aumentando, e os sistemas GNSS ainda não estarem preparados para combater esse tipo de problema.

Como já citado anteriormente nesse trabalho, diversas são as possibilidades de um dispositivo sofrer um ataque de spoofing, e poucas são as soluções para minimizar esse tipo de ataque. Mesmo tendo diversos problemas de falsificação de sinal, poucas literaturas são encontradas abordando esse tipo de problema e com formas de combater. Partindo disso, será comentado algumas técnicas, ou então, possibilidades de minimizar o problema com o spoofing.

3.10 CONTRAMEDIDAS EXISTENTES

Várias técnicas antispoofing foram propostas em algumas literaturas e geralmente são classificadas em dois tipos, uma quando o receptor consegue apenas identificar que está recebendo sinais falsos e outra que o receptor identifica e tenta eliminar os sinais falsos.

Como o intuito é apresentar soluções para que aumente a segurança do sistema GNSS, será apresentado em sequência as principais técnicas existentes e alguns motivos dos quais elas não estão sendo implantadas em prática.

3.10.1 Detecção de sinal vestigial

Emitir um sinal spoofer para um dispositivo GPS requer conhecimento preciso da posição central da fase da antena da vítima em relação ao centro de fase da antena do spoofer. Segundo (Humphreys, 2008), a técnica de detecção vestigial emprega as seguintes opções definidas por software. Primeiro, o receptor realiza uma cópia da entrada digitalizada do front-end em uma memória buffer. Segundo, o receptor seleciona um dos sinais de GPS rastreados e remove a versão localmente regenerada desse sinal do buffer. Terceiro, o receptor realiza a aquisição pelo mesmo sinal PRN nos dados em buffer.

A implementação da detecção de sinal vestigial aumenta a complexidade de hardware e processamento dos receptores porque essa técnica requer um rastreamento adicional para o canal rastrear os sinais autênticos e os sinais spoofing. No entanto, sinais de spoofing de alta potência e resolução de bits limitada, o vestígio autêntico pode não detectar a presença de um falso sinal, pois pode ter caído no nível de sensibilidade do quantizador do receptor GPS.

3.10.2 Formação de estruturas de multiantena com direção nula

Um receptor de multiantena pode empregar técnicas de processamento para moldar seu feixe. Como tal, depois de detectar a direção do sinal de falsificação, este receptor pode direcionar um valor nulo para a fonte do spoofer e suprimir seu efeito prejudicial (HUMPHREYS, 2011),(ALI-JAFARNIA, 2012).

3.10.3 Monitoramento de integridade de receptor autônomo (RAIM)

Sinais falsos injetam efetivamente pseudoarranjos falsos nas medições do receptor. Essas medições podem ser inconsistentes e consequentemente não levar a uma solução de posição.

A maioria dos receptores GNSS executam o monitoramento da integridades das medições, a fim de detectar e rejeitar medidas discrepantes, e essa técnica é conhecida como monitoramento autônomo da integridade do receptor (KUUSNIEMI, 2007).

Na Tabela 3.7 é apresentado um resumo das três principais técnicas existentes para combater o spoofing e nelas classificadas pelo seu grau de complexidade de implementação e de eficácia

Figura 3.7 – Comparativo das principais técnicas antispoofing existentes para frequência aberta

Antispoofing	Recurso de utilizado	Complexidade	Eficácia	Capacidade de receptor necessário	Cenário geral do spoofing
Detecção sinal vestigial	Sinal autêntico ainda presente e pode ser detectado	Alto	Média	Recebimento múltiplo de canais	Médio
Arranjo de antenas de direção nula	Sinais spoofing chegando da mesma direção	Médio	Alto	Receptor de múltiplas antenas	Alto
RAIM	Resíduos altos de spoofing	Médio	Médio	-	Médio

Fonte: Autor, 2019.

4. RESULTADOS E DISCUSSÃO

Como já citado anteriormente nesse trabalho, diversas são as possibilidades de um dispositivo sofrer um ataque de spoofing, e poucas são as soluções para minimizar esse tipo de ataque. Mesmo tendo diversos problemas de falsificação de sinal, poucas literaturas são encontradas abordando esse tipo de problema e formas de combater.

O estudo realizado mostrou o quão deficiente nosso sistema de georreferenciamento é e pode ser burlado com sistemas simples ou complexos. Uma questão limitante nesse quesito é do investimento, pois um sistema complexo, em que engloba todos os tipos de possíveis soluções para o spoofing se torna inviável por ainda não ter um sistema efetivamente comprovado, e que justifique financeiramente tal investimento para a solução desse problema.

Todos os sistemas da constelação GNSS estudados, se mostraram bastante semelhantes, em todos os aspectos, desde frequência de comunicação até parâmetros para cálculo de posição. Todos realizam o mesmo procedimento para aquisição de dados e para a sua proteção, ambos os sistemas aplicam a questão da criptografia para proteger seus sinais do spoofing, porém, ela é aplicada apenas nas frequências consideradas militares, deixando as frequências abertas vulneráveis para qualquer tipo de interferência.

Por serem todos semelhantes, um ataque de spoofing pode afetar o sistema GPS, o GLONASS, Galileo e Beidou sem dificuldades, pois todos os sistemas tem o mesmo princípio de funcionamento.

Voltado para isso, é de extrema importância e necessidade um estudo aprofundado para criação de um receptor antispoofing para sistemas GNSS, para frequências abertas. A utilização do sistema de posicionamento está cada vez mais comum entre veículos terrestres, aéreas e marítimos, e para esses tipos de locomoções, a confiabilidade do sinal recebido é muito importante, pois um erro de rota pode levar a diversos transtornos.

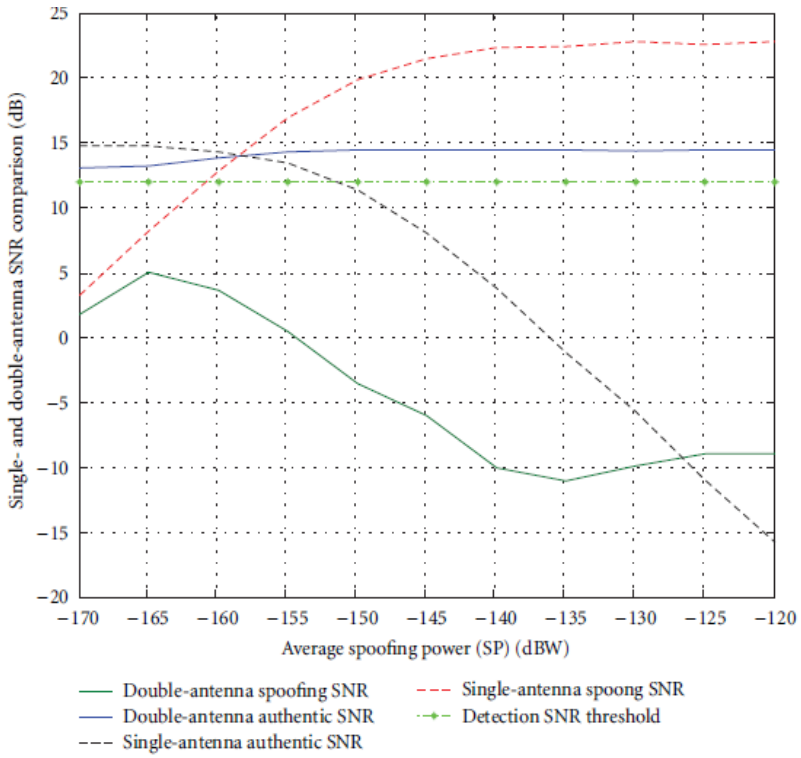
Nesse sentido, uma contramedida abordada por Humpherys e Ledvina, a respeito do receptor com arranjo de antenas, e se mostra com bastante integridade teórica, pois os autores exploram o tema em diversos aspectos, e comprovando que com a utilização do arranjo de antenas, eleva bastante a dificuldade do spoofer em fazer a comunicação com o receptor com sucesso.

Na linha de estudo de Humpherys, Ali-Jafarnia traz um método que utiliza um arranjo de antenas com direção nula. O método emprega técnicas de processamento para moldar o feixe do sinal, e direciona um valor nulo para a fonte do spoofer. Que, em consequência disso, tem por objetivo eliminar os sinais de falsificação.

Assim, conciliando as teorias dos autores Humpherys e Ali-Jafarnia, com uma avaliação da potência espacial recebida, após correlacionar os diferentes sinais, mostra-se promissora para a identificação e eliminação do spoofing. Supondo que vários sinais PRN sejam transmitidos pelo módulo spoofer, na qual cada sinal PRN está tendo um nível de potência comparável ao dos sinais autênticos, podemos eliminar os sinais falsos, devido que todos serem provenientes da mesma direção, e com isso, um vetor nulo de direção pode ser extraído correspondente aos sinais de falsificação.

A Figura 3.10 mostra a SNR média dos dados autênticos e os sinais de spoofing, em função do spoofing médio de entrada para receptores de antena única e para uma antena dupla, em teste realizado por Ali-Jafarnia (ALI-JAFARNIA, 2012) Para o caso de receptor de antena única, o SNR autêntico diminui conforme aumenta potência do spoofing. No entanto, observa-se que após a combinação adequada dos sinais de ambas as antenas, o SNR autêntico permanece constante, enquanto o SNR spoofado é sempre muito abaixo do limite de detecção para diferentes entradas de potência do spoofing, dificultando assim, do receptor “aceitar” os sinais spoofados.

Figura 4.1 – SNR médio dos sinais spoofing e sinais autênticos em relação a potência média de falsificação.



Fonte: ALI-JAFARNIA, 2012.

5. CONCLUSÃO

É perceptível que a utilização de drones e ARPs em nosso dia-a-dia vem se tornando cada vez mais comum, devido ao fácil acesso a esses tipos de equipamentos para as mais diversas aplicações. Neste sentido, foi de relevância estudar um tema, em que possui pouca literatura e a maior parte da sociedade, não tem noção a respeito do tema, e com isso, sem ideia do quão periculoso pode ser o spoofing.

E é preocupante todos os tipos de sistemas da constelação GNSS, não possuir contramedida para sinais abertos, deixando vulnerável todo sistema. Supondo que o spoofing pode alterar rotas de qualquer meio, tanto aéreo, marítimo e terrestre sem que o usuário perceba tal alteração, como abordado no decorrer desse trabalho.

O desenvolvimento de contramedidas se aproxima de uma conclusão, há anos Universidade Americanas vem se especializando, e algumas soluções encontradas, tal como a criptografia do sinal, ainda não se tornou aplicável pelo alto custo devido a manutenção em todo o sistema de satélites.

Conforme abordado no trabalho, uma medida de mitigação do *spoofing* merece atenção, que é a técnica citada que utiliza um arranjo de antenas com direção nula. Esse método mostra-se promissor para implementação prática, e melhorado ainda se aliar a ele uma outra medida de detecção do spoofing, principalmente relacionada aos picos de potência elevadas no sinal autêntico, fica como uma possível abordagem para trabalhos futuros, implementar em prática esses dois métodos simultâneos.

O estudo realizado foi de grande importância, pois teve objetivo de mostrar o que é esse problema e o que os atuais sistemas usam para se prevenir dele. Embora toda a abordagem realizada sendo teórica, acredito que aplicando os métodos citados em conjunto com outra medida de identificação, o problema possa ser solucionado.

A elaboração do presente trabalho passou por diversas dificuldades, principalmente pelo desconhecimento do tema, mas em cima disso, aumentou-se a curiosidade para aprender sobre ele a ponto de deixar registrado em forma de trabalho de conclusão de curso um estudo inicial sobre o spoofing.

6. REFERÊNCIAS BIBLIOGRÁFICAS

AGENCIA NACIONAL DE Telecomunicações (ANATEL). Resolução nº 308, de 11 de setembro de 2002: Aprova a Norma de Uso do Bloqueador de Sinais de Radiocomunicações. Último acesso em 25 de agosto de 2019 e disponível em: http://www.anatel.gov.br/legislacao/resolucoes/2002/257-resolucao-308

DOD. 2008. Global Positioning System Standard Positioning Service Performance Standard 4th Edition. Technical Report. U.S. Department of Defense. http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf. Acesso em: 15 de novembro de 2019.

DEFESA.TV.BR. Sua revista eletrônica: " Rússia estaria gerando sinais de GPS falsos para confundir navegação". Acesso em 06 de dezembro de 2019.: https://www.defesa.tv.br/russia-estaria-gerando-sinais-de-gps-falsos-para-confundir-navegacao-de-navios/

ESTUDO SOBRE A INDUSTRIA BRASILEIRA E EUROPEIA DE VEÍCULOS AÉREOS NÃO TRI-PULADOS. Ministério da Industria, Comércio, Exterior e Serviços. Ministry of Industry, Commerce, Foreign and Services.. Acesso em 15 de setembro de 2019. Disponível em: http://www.mdic.gov.br/images/publicacao_DRONES-20161130-20012017-web.pdf

EUROPEAN COMMISSION, "Communication from the Commission—Galileo—Involving Europe in a New Generation of Satellite Navigation Services," COM(1999)54.

E. D. KAPLAN AND C. J. HEGARTY, Understanding GPS Principles and Applications, Artech House, Boston, Mass, USA, 3nd edition, 2017.

FORCA AEREA DOS ESTADOS UNIDOS. GPS Interface Specification (GPS-IS-200H). Forca Aerea dos Estados Unidos, p. 15-26, 2013

H. KUUSNIEMI, A. WIESER, G. Lachapelle, and J. Takala, "User-level reliability monitoring in urban personal satellitenavigation," IEEE Transactions on Aerospace and Electronic Systems, vol. 43, no. 4, pp. 1305–1318, 2007.

HUMPHREYS, T. E.; LEDVINA, B. M. “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer”. Journal of Field Robotics, 31(4): 617–636, 2014.

INTERTANKO. “ Jamming and Spoofing of Global Navigation Satellite System (GNSS)”, 2019.

JOHN BETZ. 2002. Binary Offset Carrier Modulations for Radionavigation. Journal of the Institute of Navigation 48, 4 (2002), 227–246s.

LOGAN SCOTT. 2003. Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems. In Proceedings of the Institute of Navigation GPS/GNSS Conference. ION, Portland, OR, 1543–1552.

MICHAEL A. LOMBARDI, Lisa M. Nelson, Andrew N. Novick, and Victor S. Zhang. 2001. Time and Frequency Measurements Using the Global Positioning System. The International Journal of Metrology 8, 3 (Jul.- Sept. 2001), 26–33.

MACIEL DE SÁ, E.; ZUPAK, G. “Força nacional procura drone que sobrevoou Maracanã na abertura”. Globo. 2016. Acesso em 10 de setembro de 2019. Disponível (online) em: http://globoesporte.globo.com/olimpiadas/noticia/2016/08/forca-nacional-procura-drone-que-sobrevoou-maracana-na-abertura.html

MARCUS G. KUHN. 2004. An Asymmetric Security Mechanism for Navigation Signals. LNCSS 3200 (2004), 239–252.

NAKEDSECURITY, suspeita de spoofing em massa do GPS dos navios do Mar Negro. Acesso em 10 de outubro de 2019. https://nakedsecurity.sophos.com/pt/2017/09/26/suspected-mass-spoofing-of-ships-gps-in-the-black-sea/

T. E.HUMPHREYS, B.M. LEDVINA,M. L. PSIAKI, B.W. O’Hanlon, and P.M. Kintner, “Assessing the spoofing threat: development of a portable gps civilian spoofer,” in Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS ’08), pp. 2314–2325, Savannah, Ga, USA, September 2008

THOMASSEN K. How GPS Works. Disponivel em: http://www.avionicswest.com. Acesso 25 de julho de 2019.