Dissertação apresentada à Pró-Reitoria de Pós-Graduação do Instituto Tecnológico de Aeronáutica, como parte dos requisitos para obtenção do título de Mestre em Ciências no Programa de Pós-Graduação em Engenharia Eletrônica e Computação, Área de Telecomunicações.

Antônio Pedro Santos Dias de Carvalho

MITIGAÇÃO DE EFEITO *SPOOFING* EM GNSS NA PRÉ-CORRELAÇÃO

Dissertação aprovada em sua versão final pelos abaixo assinados:

Prof. Dr. Felix Dieter Antreich
Orientador

Profa. Dra. Emília Villani
Pró-Reitora de Pós-Graduação

Campo Montenegro
São José dos Campos, SP - Brasil
2023

Dados Internacionais de Catalogação-na-Publicação (CIP)
Divisão de Informação e Documentação

Carvalho, Antônio Pedro Santos Dias
Mitigação de Efeito *Spoofing* em GNSS na pré-correlação/ Antônio Pedro Santos Dias de Carvalho São José dos Campos, 2023.
68f.

Dissertação de mestrado – Programa de Pós-Graduação em Engenharia Eletrônica e Computação, Área de Telecomunicações – Instituto Tecnológico de Aeronáutica, 2023. Orientador: Prof. Felix Dieter Antreich

1. Sistemas de Navegação por satélites. 2. Processamento de sinais. 3. Sistemas de posicionamentos. I. Instituto Tecnológico de Aeronáutica. II. Título

REFERÊNCIA BIBLIOGRÁFICA

SANTOS DIAS DE CARVALHO, Antônio Pedro. **Mitigação de efeito *spoofing* em GNSS na pré-correlação**. 2023. 68 f. Dissertação (Mestrado em Engenharia Eletrônica e Computação) - Instituto Tecnológico de Aeronáutica, São José dos Campos, 2023.

CESSÃO DE DIREITOS

NOME DO AUTOR: Antônio Pedro Santos Dias de Carvalho
TÍTULO DO TRABALHO: Mitigação de Efeito *Spoofing* em GNSS na pré-correlação
TIPO DO TRABALHO / ANO: Dissertação / 2023

_____

Antônio Pedro Santos Dias de Carvalho
Divisão de Engenharia Eletrônica - Laboratório de GPS/GNSS - CTA
CEP: 12228-615, São José dos Campos/SP - 12228-610

MITIGAÇÃO DE EFEITO *SPOOFING* EM GNSS NA PRÉ-CORRELAÇÃO

Antônio Pedro Santos Dias de Carvalho

Composição da Banca Examinadora:

Prof. Dr.	Daniel Basso Ferreira	Presidente	-	ITA
Prof. Dr.	Felix Dieter Antreich	Orientador	-	ITA
Prof. Dr.	Dimas Irion Alves	Membro interno	-	ITA
Prof. Dr.	Marcos Vinício Thomas Heckler	Membro externo	-	Unipampa

ITA

Agradecimentos

Sou muito grato a Deus por sempre ter me dado forças e o equilíbrio que pedi para batalhar por cada conquista que almejei na vida.

Agradeço a minha amada esposa Caroline e a minha filha Giovanna por serem uma grande inspiração para mim.

Agradeço ao meu pai Antônio Ricardo, a meu irmão Paulo Fernando, a minha madrinha Teresa Cristina e aos meus sobrinhos João Pedro e Valentina que sempre me alegraram nesse período difícil.

Agradeço aos brilhantes professores que conheci no ITA que com dedicação souberam transmitir conhecimentos tão importantes. Sobretudo sou grato a meu orientador Felix Dieter Antreich que me ajudou não apenas como orientador ou professor mas como um grande amigo também.

Agradeço aos meus amigos de coração André Luiz A. Silva, Luis Gustavo R. Vito, Françoa Taffarel R. Corrêa, Alessandro Roberto dos Santos, Derek do Espírito Santo Nogueira, Carlos Kleber Arruda, Douglas Lopes da Silva, Hyrllann Almeida de Souza, Martins Francisco F. da Silva, João Clávio S. Filho e Cláudio Bastos pela ajuda verdadeira que prestaram e pelos momentos de camaradagem.

Por último eu não poderia deixar de agradecer a Força Aérea Brasileira, a Marinha do Brasil, ao próprio ITA e ao Centro de Guerra Acústica e Eletrônica da Marinha pela oportunidade de valor inestimável que me foi dada para cursar o Mestrado no ITA.

"A gratidão não é apenas a maior das virtudes, mas a mãe de todas as outras."

Marco Túlio Cícero

Resumo

O GNSS (*Global Navigation Satellite System*) pode ser utilizado em aplicações militares e civis para fornecer posicionamento contínuo, seguro e confiável, velocidade e serviços de medição e cronometragem para usuários que necessitam de serviços de navegação, localização, serviços financeiros e de distribuição de energia. A utilização desse sistema exige estimativa confiável de posição e um grande risco para essa estimativa de posição é a chamada ameaça *spoofing* (falsificação). Um *spoofer* pode fabricar sinais falsos para induzir um receptor GNSS a estimar uma posição errada para seu usuário. Ao contrário do *jamming*, que visa interromper os sinais GNSS, os *spoofer*s são tecnicamente mais elaborados. Ao replicar os sinais GNSS, um *spoofer* pode enganar o receptor fazendo-o pensar que está em outro local naquele momento e diferentemente do *jamming*, o usuário não o detecta facilmente. Muitas pesquisas abordam a detecção e mitigação de *spoofing* considerando várias técnicas e estratégias distintas. Neste trabalho será apresentada uma abordagem de mitigação de *spoofing* na pré-correlação considerando um sistema com vários sensores. Esta abordagem é independente dos sinais GNSS ou constelação considerados, seja considerando serviços abertos ou para militares autorizados. É assumido neste trabalho um receptor integrado solto onde o subsistema *anti-spoofing* está processando sinais do arranjo de antenas e então passa um sinal livre de *spoofing* para o receptor GNSS conectado. Assim, o receptor GNSS é considerado de última geração, sem características específicas. A detecção de *spoofing* na estimativa de direção de chegada (azimute e elevação), a subsequente atenuação do *spoofing* por filtragem espacial e a continuação do serviço dos satélites será discutida. Essa abordagem pode ser considerada uma abordagem adaptativa cega, pois nem as características do sinal nem os DOA's dos sinais são conhecidos antecipadamente pelo receptor. Assume-se um receptor estático com 7 sensores e um atacante/spoofer estático com 1 antena transmissora.

Abstract

GNSS (Global Navigation Satellite System) can be used in both military and civil applications to provide continuous, safe and reliable positioning, speed and measurement and timing services for users who need navigation services location, financial services and energy distribution. Using this system requires reliable position estimation and a major risk to this position estimation is the so-called threat of spoofing. A spoofer can fabricate false signals to trick a GNSS receiver into estimating the wrong position for the user. Unlike jamming, which aims to interrupt GNSS signals, spoofers are technically more elaborate. By replicating GNSS signals, a spoofer can trick the receiver into thinking it is somewhere else at that time and unlike jamming, the user does not easily detect it. Much research addresses spoofing detection and mitigation considering several different techniques and strategies. In this work, we present a pre-correlation spoofing mitigation approach considering a system with several sensors. This approach is independent of the considered GNSS signals or constellation, either considering open or authorized services. In this work, we assume a loose integrated receiver where the anti-spoofing sub-system is processing signals of the antenna array and then passes a spoofing-free signal to the connected GNSS receiver. Thus, the GNSS receiver is considered a state-of-the-art with no specific features. The spoofing detection based on the direction of arrival (azimuth and elevation) estimation, the subsequent spoofing mitigation by spatial filtering and the continued reception and processing of the GPS satellites will be discussed. This approach can be considered a so-called blind adaptive approach, as neither the signal characteristics nor the DOAs of the signals are known by the receiver in advance. A static receiver with 7 sensors and a static attacker/spoofer with 1 receiver antenna is assumed.

Lista de Figuras

Lista de Abreviaturas e Siglas

VANT	Veículo Aéreo não Tripulado
DoD	United States Department of Defense
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
CRPA	Controlled Reception Pattern Antennas
PVT	Posição, velocidade e tempo
SDR	Software defined radio
SNR	Signal to Noise Ratio
SSR	Spoofing to Signal Ratio
L_1	Frequência de 1575,42 MHz
L_2	Frequência de 1227,60 MHz
PRN	Pseudorandom Noise
ITA	Instituto Tecnológico de Aeronáutica
Matlab	Software de computação numérica da empresa MathWorks
SI	Sistema Internacional de Unidades
FFAA	Forças Armadas
RMSE	Root Mean Square Error
NMA	Navigation Message Authentication
SPS	Standard Positioning Service
PPS	Precise Positioning Service
ITU	*International Telecommunication Union*

Sumário

1 Introdução

A distorção e interrupção operacional dos receptores de navegação, em virtude do efeito *spoofing* (falsificação), representam uma séria ameaça para muitas aplicações de GNSS (*Global Navigation Satellite System*), especialmente para aquelas com aspectos críticos de segurança, no setor bélico e nas atividades com grande impacto econômico (MEURER *et al.*, 2016).

Os receptores GNSS, vitais para informação de posicionamento, ainda que bem desenvolvidos, podem ser enganados, sofrendo interferências denominadas *spoofing*. Um *spoofer* transmite réplicas de sinais de satélite para controlar a estimativa de PVT (posição, velocidade e tempo) do receptor da vítima, enganando-a quanto à sua localização (MERWE *et al.*, 2018).

Em contraste com o *jamming* (bloqueio), onde a operação do receptor é significativamente distorcida, um ataque de *spoofing* tem a peculiaridade na qual muitas vezes pode não ser detectado pelo usuário de GNSS, especialmente se a solução de PVT afetada for bem elaborada e lenta. Portanto, a detecção de ataques *spoofing* é um importante campo de pesquisa com fito de mitiga-lo e coibi-lo. O desenvolvimento de contramedidas adequadas é um dos temas abordados pela estratégia de *e-Navigation* lançada pela Organização Marítima Internacional (APPEL *et al.*, 2018) e será também explorado neste trabalho. Além disso, aplicações aeronáuticas têm uma grande demanda por mitigação de *spoofing*, pois cada vez mais são encontradas incidências de *spoofings* (GOWARD, 2022).

A Figura 1.1 mostra o *spoofer* (*Spoof. Source*) fazendo uso do sinal original do GNSS para então enviar um sinal falso de GNSS ao usuário (*True Position*) com informações erradas sobre a localização deste. Como se vê, nesse trabalho todo o sinal de *spoofing* é advindo de uma mesma direção, o que difere do conjunto de sinais transmitidos de cada satélite, que obviamente comporta sinais de direções distintas. Assim, o cálculo PVT do receptor do usuário se baseia numa correlação de sinais mais fortes realizada com os sinais *spoofing* ao invés dos sinais originais de satélites, levando-o a ser iludido quanto à sua localização.

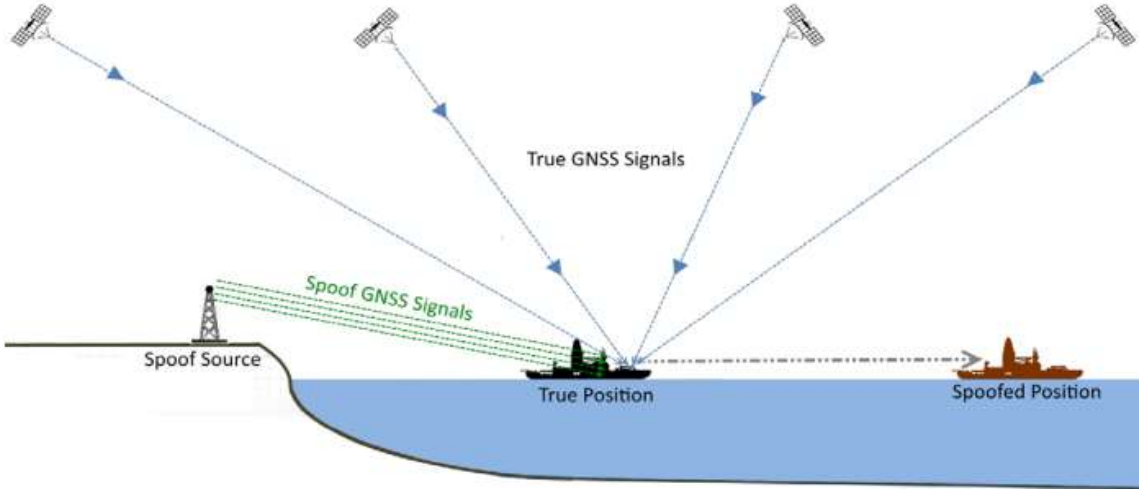

Figura 1.1 Efeito do *spoofing* (MILNE, 2018).

Nas atividades atinentes aos setores bélico/defesa nacional, comercial, de vigilância e de segurança nacional, o assunto abordado é de grande relevância. Pois conforme se implementa na prática o conhecimento de contramedidas de *spoofings*, é possível realizar trajetos e fundear embarcações com menores riscos de abalroamentos ou outras complicações portuárias, evitar dispêndios de munições em áreas não afins e evitar acidentes com VANT's (veículo aéreo não tripulado).

Tal estudo é imprescindível para se ter um sistema de armas avançado, principalmente em um meio não tripulado onde não há envio de informações visuais em tempo real para o navio controlador ou aeronave mãe, o que o aprimora tanto no sentido de seus ataques como de sua própria proteção.

Assim, planeja-se poder detectar um atacante agindo em proveito do efeito *spoofing* para então coibir seus efeitos. Tal detecção, na presente dissertação, se dá através pelo método "direção de chegada" (*DOA - direction of arriving*), no qual se percebe que alguns sinais que a priori seriam de satélites (sinais autênticos), na verdade chegam de uma só direção (do *spoofer*). Então, a mitigação do efeito *spoofing* ocorre gerando-se um nulo espacial em tal direção.

Neste trabalho pretende-se realizar a correlação entre os sinais recebidos de diferentes antenas e, em seguida, realizar a estimativa do DOA para posteriormente ser feita a filtragem para mitigação do *spoofing*. Será também mostrado que os sinais de *spoofing* podem ter potência igual ou mesmo menor que dos sinais originais dos satélites e ainda assim poderem ser mitigados.

1.1 Objetivo

O objetivo é desenvolver uma abordagem para mitigação do efeito *spoofing* que possa ser realizada independentemente do receptor GNSS e que também possa ser aplicada para serviços de militares autorizados. Esta abordagem pode ser chamada de abordagem cega, pois nem as características do sinal nem os DOA's dos sinais são conhecidos antecipadamente pelo receptor. Tal estudo é diferente da maioria das técnicas que podem ser encontradas na literatura, que se baseiam na estimativa DOA pós-correlação e conhecendo as sequências de espalhamento de cada satélite (APPEL *et al*., 2018). A única abordagem encontrada na literatura que também poderia ser aplicada na pré-correlação sem o conhecimento das sequências de espalhamento dos satélites foi apresentada em (BROUMANDAN *et al.*, 2014). No entanto ela não conseguiu estimar os DOAs dos sinais de falsificação e baseou-se no *beamforming* pós-correlação, conhecendo as sequências de espalhamento dos diferentes satélites no receptor GNSS. A abordagem proposta no atual trabalho também deve ser de complexidade razoável. Portanto, o objetivo é realizar a detecção de *spoofing* baseada na estimativa DOA dos sinais de *spoofing*, considerando o chamado ataque de repetição (*replay spoofing attack*) ou ataque de *spoofing meaconing*, onde o *spoofer* recebe os sinais do satélite, amplificando-os e encaminhando-os sem outras alterações adicionais ao receptor GNSS da vítima/usuário.

Assim, desenvolve-se um trabalho de mitigação e de detecção da pré-correlação do *spoofing* GNSS utilizando um arranjo de antenas. No trabalho em tela, um subsistema *anti-spoofing* processa os sinais recebidos da matriz da antena e, após a mitigação, os sinais de *spoofing* passam um sinal GNSS "limpo" para um receptor de última geração. O subsistema proposto também pode facilmente incluir mitigação de bloqueio. Tal Trabalho está bem alinhado com os sistemas atuais para mitigação de interferência militar chamados Antenas Padrão de Recepção Controlada (CRPA – Controlled Reception Pattern Antennas) (EGEA-ROCA *et al.*, 2022).

Neste trabalho, será considerado o GPS (GNSS estadunidense) para a análise do desempenho da abordagem de mitigação e detecção proposta.

1.2 Conteúdo e Organização

O capítulo 1 mostra os princípios de funcionamento do GNSS. De forma resumida demonstra fisicamente como é possível o usuário saber sua própria localização em qualquer parte do globo terrestre e apresenta a utilização do GPS pelas forças armadas brasileiras.

O capítulo 2 apresenta o cenário geográfico/físico no qual os satélites, receptor/vítima e *spoofer* se encontram. Também são mostradas características de um receptor e a modelagem matemática de um sinal complexo em banda base utilizada no receptors.

O capítulo 3 mostra como operam os algoritmos de direção de chegada Conventional Beamformer e Capon para se descobrir a direção (azimute e elevação) do atacante/*spoofer* e os resultados que esses algoritmos conferem após simulação em Matlab.

Por fim o capítulo 4 apresenta o funcionamento do filtro espacial capaz de anular os efeitos do *spoofing* na pré-correlação que ocorre, permitindo que apenas os sinais originais de GPS sejam remanescentes para o receptor. Para aprimoramento do filtro é mostrada a filtragem com a incrementação da matriz de Toeplitz, que consegue ampliar o nulo na direção do *spoofing*. Os resultados de tal filtro são então apresentados.

1.3 Global Positioning System (GPS)

O Sistema de Posicionamento Global, ou GPS, é um sistema de navegação estadunidense de vigilância que utiliza sinais de satélites em órbita e que pertence ao Departamento de Defesa dos EUA (DoD). O GPS opera independentemente de internet ou de recepção telefônica e pode funcionar em qualquer lugar na Terra ou próximo a ela, onde haja uma linha direta de visão dos satélites. Com aplicações militares, civis e comerciais, o GPS é uma ferramenta poderosa para comunicação, navegação, serviços de emergência e muitos outros (GABLE, 2022).

1.4 Princípios de Operação do GPS

O GPS está em operação desde 1995 e tem hoje 31 satélites em órbita, de modo a garantir que em 95% do tempo, 24 destes estejam operacionais (INPE, 2022). Eles orbitam a Terra em um período de 12 horas, aproximadamente 20200 km acima da Terra, e permitem determinar a posição com grande exatidão em qualquer parte do globo, a qualquer hora e com quaisquer condições atmosféricas. Existem seis planos orbitais, igualmente espaçados de 60

graus, cada plano orbital é ocupado por 4 satélites, permitindo, teoricamente, uma visibilidade entre 5 e 8 satélites em qualquer parte do globo terrestre. Cada um dos satélites em órbita transmite a hora certa juntamente com sua posição exata e outras informações. O receptor, por possuir a hora sincronizada com o que é difundido pelo satélite, computa o tempo percorrido entre a transmissão e recepção do sinal e o converte em distância, a chamada pseudo-distância. A posição do receptor (x, y, z), tomando o centro da Terra como origem, é calculada quando quatro satélites estiverem visíveis (CASTRO, 2001).

Embora tenha sido concebido com fins militares (permitir o guiamento preciso de mísseis balísticos), o GPS possuiu, desde a sua gênese, dois níveis de serviço: Um nível com melhor performance, disponível apenas aos utilizadores militares autorizados e denominado Serviço de Posicionamento Preciso (*Precise Positioning Service - PPS*), com erro de poucos metros e grande robustez, de onde se obtém boa proteção contra *spoofings* e transmissão dos sinais cifrados, para evitar utilização não autorizada. E outro nível com performance mais fraca, disponível a todos os utilizadores do GPS e conhecido por Serviço de Posicionamento Padrão (*Standard Positioning Service - SPS*), que permite exatidão na ordem das poucas dezenas de metros (MONTEIRO, 2007).

Os sinais transmitidos pelos satélites são extremamente fracos, sendo designados por ruído pseudoaleatório (*pseudo-random noise*), já que se confundem com o ruído atmosférico de fundo. Tais sinais possuem uma densidade de potência, em vista do receptor, de $P = P_t / (4\pi R^2)$, onde P é a densidade de potência recebida (potência por unidade de área), P_t é a potência total transmitida pela fonte (satélite), R é a distância entre a antena e a fonte do sinal (BALANIS, 2016). Em muitos casos atingem um receptor em Terra, podendo ser medida uma potência de $5x10^{-17}$ W, que é um valor incrivelmente baixo (bilhões de vezes mais fraco que os sinais de televisão). Como medida de comparação, podemos dizer que corresponde à luz que veríamos de uma lâmpada de 25 W se ela estivesse colocada a uma distância igual à altitude dos satélites: 20200 km.

Esses sinais são modulados na banda UHF (*Ultra High Frequency*) do espectro eletromagnético, que corresponde a faixa de 300 MHz a 3000 MHz, conforme padrão da ITU (*International Telecommunication Union*). Este trabalho, considera apenas o sinal L_1 C/A, que possui frequência central L_1 = 1575,42 MHz. Neste sinal, estão presentes a portadora, os dados de navegação modulados em BPSK (*Binary Phase Shift Keying*) e uma sequência pseudoaleatória chamada de código C/A (*Coarse/Acquisition*), responsável pelo espalhamento espectral do sinal numa banda de 2,046 MHz.

O código C/A é uma sequência pseudoaleatória de 1023 chips (cada chip representa um bit, mas possui essa nomenclatura para indicar que não carrega informação) transmitida a uma taxa de chips de 1,023 MHz, de modo que a duração da sequência é de 1 µs (BORRE *et al*., 2007). Essa sequência é única para cada um dos satélites em operação, os quais são identificados por um número PRN (*Pseudo-Random Noise*), que vai de 1 a 32 e que está associado a um código C/A. Devido à propagação do sinal do satélite até o usuário, há um atraso na sequência pseudoaleatória que deve ser determinado pelo receptor do usuário e está relacionado com a medida de pseudo-distância a ser utilizada no cálculo da posição (BORRE *et a*., 2007):.

Uma tabela mostrando a frequência central, nome da banda, largura de banda e outras informações a respeito de cada GNSS pode ser vista na Figura 1.2.

Constellations	Bands	Frequency in MHz				Wavelength (cm)	Minimum Received Power (5º Elev) dBW*	Signals / Comments
		Centre	Bandwidth	Lower	Upper			
GPS	L1	1575.42	±2	1573.42	1577.42	19.0	-163.0(D) / -158.25(P)	L1C GPS III
			±1.023	1574.397	1576.443		-157	L1C/A
			±10.23	1565.19	1585.65		-161.5	L1P(Y)
			±15	1560	1590		-158.0	M Code
	L2	1227.60	±10.23	1217.37	1237.83	24.4	-160.0 (Block II F)	L2P(Y)
			±1.023	1226.577	1228.623		-161.5 (Block II F)	L2C
			±15	1212	1242		-164.0	M Code
	L5	1176.45	±10.23	1166.22	1186.68	25.5	-157.9 (Block II F)	L5I/Q
QZSS	L1	1575.42	±2	1573.42	1577.42	19.0	-163.0(D) / -158.25(P)	L1C D/P
			±1.023	1574.397	1576.443		-158.5	L1C/A
	L6	1278.75	±21.0	1257.75	1299.75	23.4	-156.82	Block II
	L2	1227.60	±1.023	1226.577	1228.623	24.4	-158.5	L2C
	L5	1176.45	±10.23	1166.22	1186.68	25.5	-157	I/Q
GALILEO	E1	1575.42	±12.276	1563.144	1587.696	19.0	-157.25	D/P
	E5a	1176.45	±10.23	1166.22	1186.68	25.5	-155.25	D/P
	E5(altBOC)	1191.795	±25.575	1166.22	1217.37	25.2	-155.25	AltBOC
	E5b	1207.14	±10.23	1196.91	1217.37	24.8	-155.25	D/P
	E6	1278.75	±20.46	1258.29	1299.21	23.4	-155.25	D/P
GLONASS	G1	N/A		1598.0625	1605.37	~18.7	-161.0	FDMA
			±0.5					CA
			±5.0					P
	G1a CDMA	1600.995	±5.0	1595.995	1605.995	18.7	-158.5	L1SC
			±1	1599.995	1601.995			L1OC-D
			±2	1598.995	1602.995			L1OC-P
	G2	N/A		1242.9375	1248.625	~24.0	-167	FDMA
			±0.5					CA
			±5.0					P
	G2a CDMA	1248.06	±7.0	1241.06	1255.06	24.0	-158.5	L2SC
			±1	1247.06	1249.06			L2OC-D
			±2	1246.06	1250.06			L2OC-P
	G3 CDMA	1202.025	±10.23	1191.795	1212.255	24.9	-158.5	L3OC-D / L3OC-P
BEIDOU	B1I	1561.098	±2.046	1559.052	1563.144	19.2	-163	BeiDou(II) OS
	B1	1575.42	±16.368	1559.052	1591.788	19.0	-159(MEO) / -161(IGSO)	BeiDou (III) / B1A-D / B1A-P
	B2a	1176.45	±10.23	1166.22	1186.68	25.5	-163	BeiDou (III) I/Q
	B2/B2b	1207.14	±10.0	1197	1217	24.8	-163	BeiDou (III) Not Published
	B3I	1268.52	±10.23	1258.29	1278.75	23.6	-163	B3C-D / B3C-P
IRNSS/NAVIC	L5	1176.45	±12.0	1164.45	1188.45	25.5	-159.0	SPS
	S	2492.028	±16.0	2476.03	2508.3	12.0	-162.3	SPS
WAAS/EGNOS	L1	1575.42	±1.023	1574.397	1576.443	19.0	-158.5 / -152.5 (Future)	C/A
	L5	1176.45	±10.23	1166.22	1186.68	25.5		L5 I/Q
L-BAND CORRECTIONS	L			1539	1559			
IRIDIUM				1616	1626.5			RHCP
				1621.35	1626.5			Up Load
GLOBALSTAR	L-Band			1610	1618.75			LHCP
	C-Band			6875	7055			
INMARSAT	L-Band			1525	1559			Downlink
				1626.5	1660.5			Uplink
	Extended			1518	1559			Alphasat
				1668	1675			
LIGHTSQUARED/LIGADO				1526	1536			Limits power to 10 W
LTE JAPAN	Band 11			1475.9	1500.9			Down Link
	Band 21			1495.9	1510.9			Down Link
LTE EUROPE	Band 32			1452	1496			Down Link

** Power is received with a 0dB gain antenna*

Figura 1.2 Informações dos GNSS (TALLYSMAN, 2023).

1.5 Utilização do GPS nas Forças Armadas

O código militar modula L_1 (1.575,42 MHz) e L_2 (1.227,60 MHz). Possui período de 7 dias, o que dificulta a tarefa de sua aquisição. Por essa razão, os receptores que trabalham com o código P utilizam também o código C/A como forma de viabilizar a sincronização no código mais longo. Cada satélite possui um conjunto de códigos específico, por isso diz-se que o sistema emprega CDMA (*Code Division Multiple Access*), ou seja, acesso múltiplo por divisão de códigos (CASTRO, 2001).

As Forças Armadas estadunidenses utilizam o *Precise Positioning Service* (PPS), que é um serviço militar altamente preciso de posicionamento, velocidade e tempo transmitido nas frequências citadas acima. Ambas as frequências contêm um sinal de alcance de código de precisão (P/Y) com uma mensagem de dados de navegação criptografada que é reservada para usuários autorizados (European Space Agency Navipedia, 2020).

No mais atual processo de modernização do GPS, foi introduzido um novo serviço militar, denominado código M, que já é transmitido por mais da metade dos satélites da atual constelação GPS. O sinal de código M é transmitido nas portadoras L_1 e L_2 junto com os sinais de código P/Y atuais.

Envidando esforços para se ter localização precisa e proteção das informações, o Brasil poderá receber essa tecnologia desenvolvida pelos Estados Unidos nos próximos anos. No entanto, é preciso aguardar para ser incluído na lista de países elegíveis para acesso ao GPS militar, do tipo PPS (*Precision Positioning System*).

A Figura 1.3 mostra a utilização do GPS na aeronave Gripen, recém adquirida pela FAB.

Figura 1.3 GPS no console da aeronave Gripen da FAB (Disponível em (SIGAUD, 2017).

2 Modelo do Sistema

Neste capítulo serão apresentados o cenário da constelação de satélites utilizada, o modelo de receptor GPS e o modelo de dados dos sinais recebidos do subsistema *anti-spoofing*.

2.1 Cenário

Para o sistema de coordenadas (x, y, z) adotado neste trabalho, foi considerado o sistema UTM SIRGAS 2000 (equivalente ao sistema WGS-84), também conhecido como Sistema de Referência Geocêntrico para as Américas. O mesmo foi oficializado como o novo referencial geodésico para o Sistema Geodésico Brasileiro (SGB) em fevereiro de 2005, através da resolução 01\2005 do IBGE (GIOVANNI, 2023). A unidade de medida é em metros e a ilustração de seus parâmetros podem ser vistas na Figura 2.1.

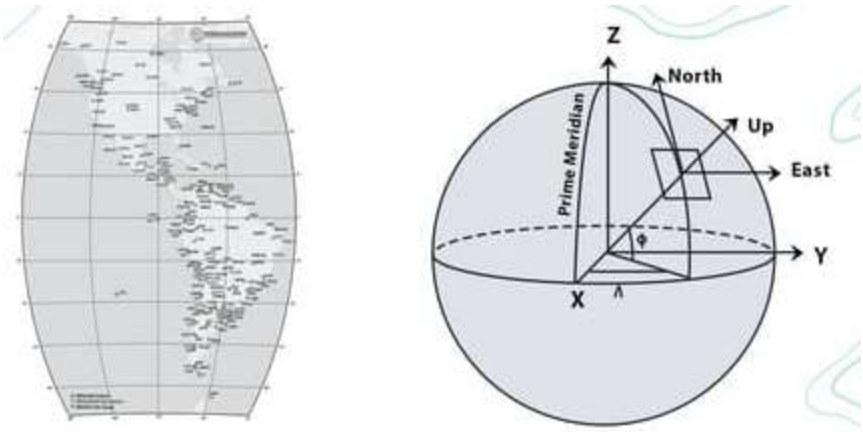

Figura 2.1 Sistema de coordenadas UTM SIRGAS 2000 (MAPPA, 2023).

Considera-se o receptor (usuário/vítima) posicionado nas coordenadas x_r = 4084802,435; y_r = -4209560,399; z_r = -2498053,960.

Os satélites utilizados por este são reconhecidos por seus respectivos números PRN: 13, 21, 19, 17, 12, 15, 25, 01, 24, 10, 32, 23, 14. Eles estão posicionados respectivamente nas seguintes coordenadas:

x_{sat} = [-13241489,5240639 4325256,49343888 -17342302,4016271 -15315976,5314318
7997048,76840368 -2447316,86370926 16831342,0228147 -4363771,71286628
-279461,486419265 20680925,7200179 16298215,6661267 20443120,2330252
-20305081,0300290];

y_{sat} = [22686830,8601624 -15939328,5569623 9105083,47190557 151604,732280984
22825851,7592832 26071295,0492928 20657466,1002167 -14212847,7425504
16346779,9628426 7548148,20556765 -3854630,22289791 16184846,4382148
-7388730,64689610];

z_{sat} = [3216220,32553302 -19984651,2811181 -18146082,3188983 -21271811,3874840
-11385631,8063740 -3496532,69431829 -2056572,08849061 -22292430,5287792
-21133428,1372654 -14939021,8179826 -20459632,6569075 -5247950,20985800
-15482550,7082197];

O atacante (*spoofer*) está posicionado nas coordenadas x_s = 4085802,435; y_s = -4209560,399; z_s = -2498053,960, (elevação de 25º e azimute 120º) estando a 1000 metros do receptor (usuário/vítima).

O diagrama da Figura 2.2 ilustra o azimute e elevação de cada satélite e do atacante *spoofer* com relação ao receptor, ao centro do diagrama. Tal gráfico é chamado de *skyplot*.

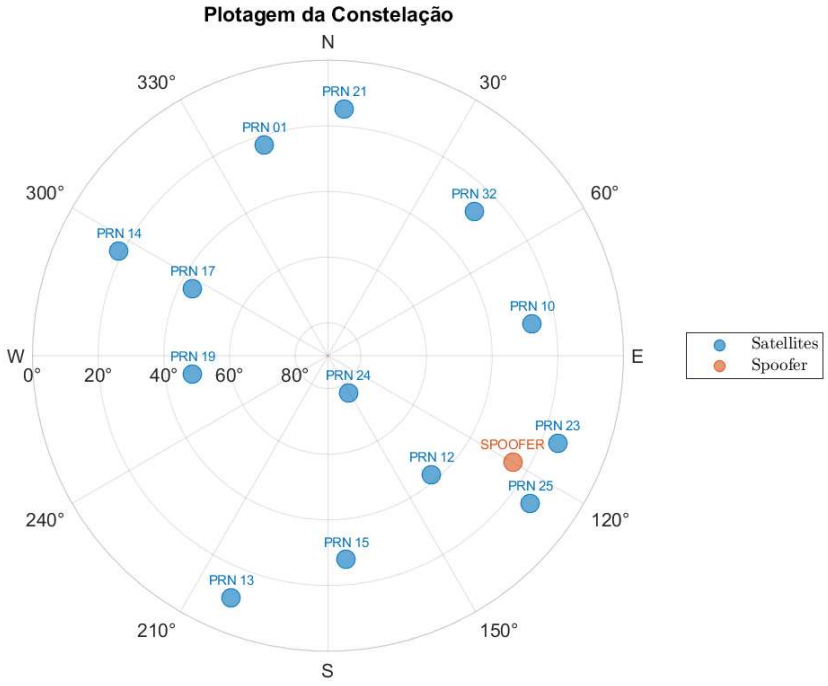

Figura 2.2 Diagrama de azimute e elevação dos satélites e *spoofer*; *skyplot.*

2.2 Modelo do Receptor GPS

De forma resumida, para o cálculo PVT (posição, velocidade, tempo), os receptores GNSS tradicionais realizam primeiramente um processamento analógico para capturar e digitalizar os sinais GNSS. Depois o processamento digital do receptor identifica os diferentes satélites e extrai as informações necessárias para o cálculo PVT. Isso é feito pelos módulos de aquisição e rastreamento do receptor.

Em seguida, o módulo de computação PVT obtém a solução do usuário dada por 4 parâmetros: as coordenadas de posição 3D e tempo GNSS. Para a arquitetura do receptor, pode-se encontrar diferentes alternativas, como arquiteturas baseadas em nuvem, instantâneas e híbridas (EGEA-ROCA *et al.*, 2022). Um diagrama de blocos da arquitetura de um receptor GNSS tradicional pode ser visto na Figura 2.3.

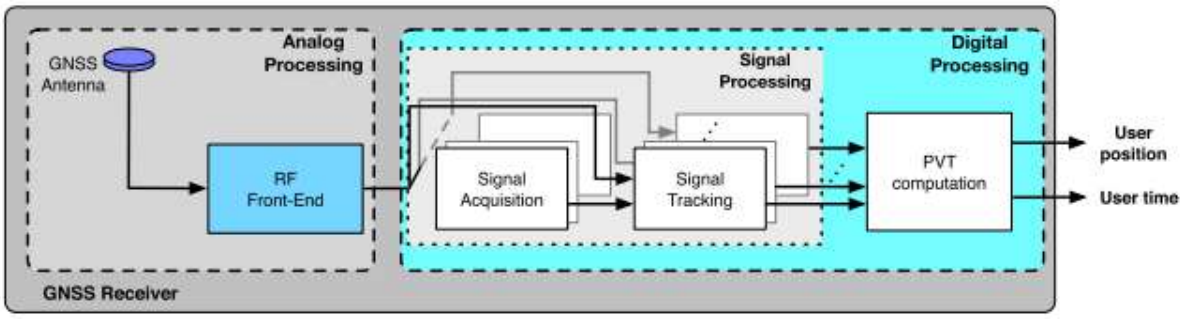

Figura 2.3 Diagrama de blocos da arquitetura de um receptor GNSS tradicional (EGEA-ROCA *et al.*, 2022).

O sistema completo, onde o receptor está enquadrado, pode ser visto na Figura 2.3. O sistema considerado neste trabalho utiliza um arranjo de sensores. O sinal recebido por cada elemento de antena (modelo de sinal vetorial) é convertido para banda base, digitalizado e, em seguida, algoritmos de processamento de sinal são executados para detectar e mitigar o *spoofing*. A necessidade de se converter o sinal para banda base vem do fato de que uma frequência de amostragem para o processamento seria da ordem de 3 GHz. Tal valor está relacionado com a frequência de operação do receptor (1.5 GHz) e a frequência de Nyquist (PROAKIS, 2007), e então 3 GHz seria uma magnitudade muito alta para a operação do processador (vide Figura 2.4). O processamento é realizado fora do receptor, pois o receptor militar é à prova de violação (*tamper proof*). Além disso, pretendemos propor uma arquitetura flexível onde um receptor GPS padrão pode ser facilmente aumentado com mitigação adicional de spoffing usando um arranjo de antenas. A mitigação do *spoofing* é executada por filtragem espacial, que produz um sinal escalar na saída do processador de mitigação de falsificação.

Depois disso, esse sinal escalar é convertido de digital para analógico e novamente para banda passante antes do receptor GNSS de última geração para derivar o PVT.

Este sistema permite detectar e mitigar *spoofing* antes de um receptor de última geração e também pode ser aplicado em situações críticas de segurança militar onde mudanças no receptor GNSS não são possíveis ou os códigos de espalhamento dos satélites não são conhecidos publicamente. Essa arquitetura de sistema também pode incluir mitigação de bloqueio, pois segue uma arquitetura CRPA clássica.

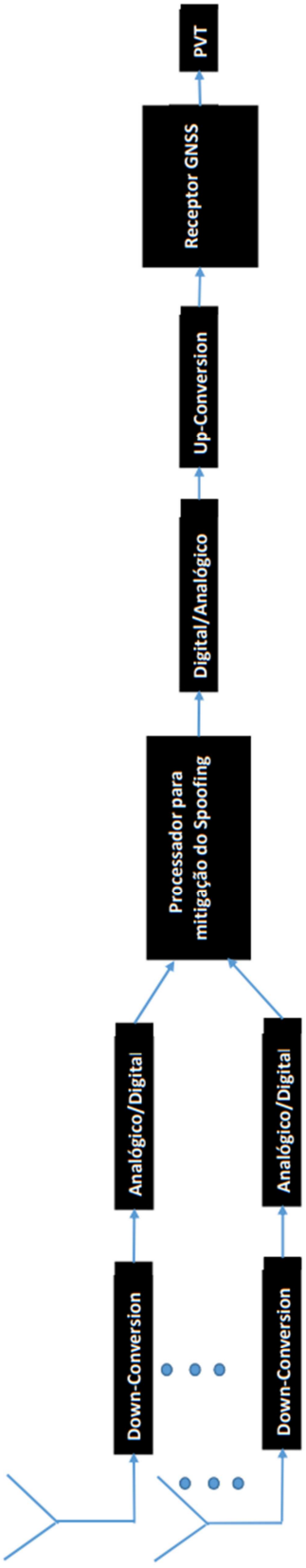

Figura 2.4 Diagrama de Blocos para Mitigação do *spoofing*.

2.3 Geração dos Sinais GPS e Transmissão dos Sinais *Spoofing*

Quando um receptor recebe sinais de pelo menos 4 satélites, ele pode descobrir sua posição 3D no tempo com base em dados de posição de satélite e tempo de GPS usando princípios de trigonometria. A Figura 2.5 mostra a configuração básica usando sinais de GPS para determinar a posição global de um receptor e o tempo do GPS. Suponha que existam três satélites (Satélites 1, 2 e 3) na constelação transmitindo suas coordenadas (x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3) com suas efemérides, e com suas respectivas durações medidas (τ_1, τ_2, τ_3) desde quando o sinal de transmissão é enviado de um satélite até quando é recebido pelo equipamento receptor. Com base nestas informações, pode-se realizar uma trilateração para encontrar as coordenadas (x, y, z) do receptor (CAO, 2020).

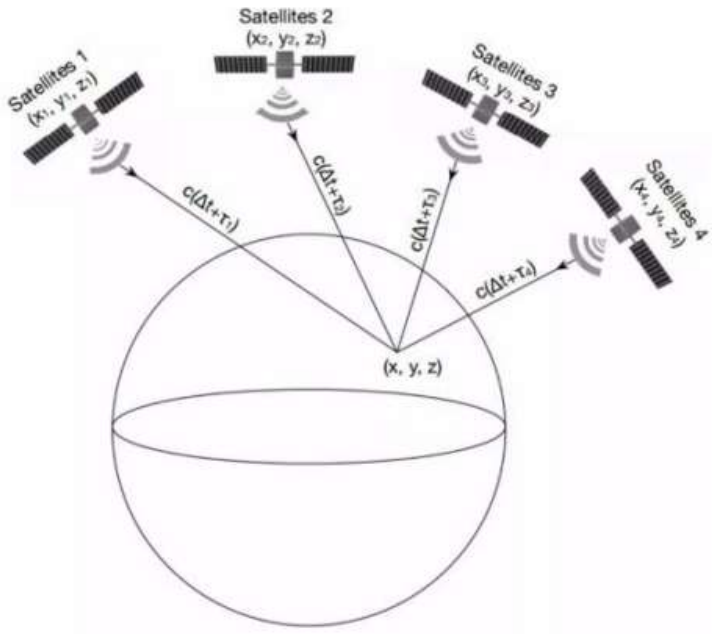

Figura 2.5 Processo de trilateração de sinais GPS (CAO, 2020).

Alguns cálculos explanados nessa sessão foram inseridos na simulação em Matlab. O cálculo do atraso de cada satélite (*delay* ou tempo que o sinal leva do satélite até o receptor), considerando o relógio do receptor sincronizado com os satélites e que não há atrasos ionosféricos, pode ser dado por (ASHBY *et al.*, 1999):

$$\tau_s = \frac{d}{c} \tag{2.1}$$

onde c é a velocidade da luz;
e d é a distância entre o receptor e o satélite e é calculado por:

$$d = \sqrt{|x_{sat} - x_r|^2 + |y_{sat} - y_r|^2 + |z_{sat} - z_r|^2} \tag{2.2}$$

onde x_{sat}, y_{sat}, z_{sat} são as coordenadas (x, y, z) de cada satélite respectivamente e x_r, y_r, z_r são as coordenadas (x, y, z) do receptor respectivamente.

Para o cálculo da frequência Doppler devido ao movimento que cada satélite faz em relação ao receptor, pode-se aplicar por (LI *et al.*, 2011)

$$f_{doppler} = \frac{L_1 V_{LOS}}{c}, \tag{2.3}$$

onde

L_1 = 1575420000 Hz (frequência de operação do satélite) e

V_{sat} = 3872,64 m/s como

$$V_{LOS} = V_{sat} \cos(\theta), \tag{2.4}$$

onde V_{LOS} (*Speed in the line of sight)* é a velocidade projetada na linha de visão do observador e θ é o ângulo ilustrado na figura 2.6, que relaciona o receptor e o satélite.

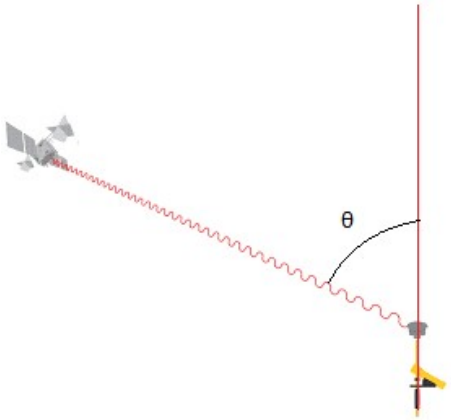

Figura 2.6 Ângulo θ, relacionando receptor e satélite. Adaptado de (SICKLE, 2008).

Em se tratando do *spoofing* de um sinal, inicialmente é realizada uma correlação entre o sinal corrompido e o original. Quando o pico de correlação do sinal corrompido está alinhado com o original, o poder do sinal malicioso é aumentado. Assim, o receptor DLL (*Delay Lock Loop*) centraliza o sinal falso, tomando o "controle" do receptor, podendo gerar qualquer informação PNT (posição, navegação e tempo) pela simples manipulação do sinal gerado e experimentos mostram que é possível e viável de ser implementada (WARNER *et al.*, 2003).

Quanto maior a similaridade entre os sinais, maior será a probabilidade do sinal falso ser aceito como legítimo pelo receptor GPS. Em detalhes esse processo pode ser realizado de diferentes maneiras, utilizando técnicas de processamento de sinal, como a Transformada de Fourier e o algoritmo de correlação cruzada. Além disso, o atacante pode ajustar alguns parâmetros do sinal spoofing, como a amplitude e a frequência, para aumentar a similaridade com o sinal original (GAO, 2014).

Hoje em dia tal tarefa pode ser realizada de forma simples e barata como demonstra (WANG *et al.*, 2015) ao utilizar, por exemplo, o equipamento Hack RF com esse intuito ou outros equipamentos SDR (*software defined radio*) que podem realizar tal tarefa. O HackRF One, da empresa Great Scott Gadgets, é um periférico de rádio definido por software capaz de transmitir ou receber sinais de rádio de 1 MHz a 6 GHz. Projetado para permitir o teste e desenvolvimento de tecnologias de rádio modernas, o HackRF One é uma plataforma de hardware de código aberto que pode ser usada como um periférico USB ou programada para operação autônoma (greatscottgadgets.com).

A Figura 2.7 retrata o passo a passo do processo de correlação em que o spoofer consegue atacar o receptor/vítima. No primeiro gráfico, o falsificador tem potência igual a zero e o receptor vê apenas o sinal verdadeiro. O segundo e o terceiro gráficos mostram o falsificador aumentando sua energia enquanto mantém seu sinal falso em alinhamento com o sinal verdadeira. O atacante é capaz de alcançar esse alinhamento analisando sua própria recepção do sinal original e sabendo o conhecimento da geometria da antena do receptor da vítima. O poder do spoofer no terceiro gráfico é suficiente para obter controle dos 3 pontos vermelhos do DLL do receptor. Na quarta e quinta parcelas, o falsificador inicia e continua um arrasto do pseudoalcance, que é uma falsificação intencional do pseudorange como entendido pela DLL do receptor da vítima.

Como pode ser visto, após a correlação dos sinais, o malicioso se aproveita do receptor da vítima, com uma maior magnitude e se tornando o principal sinal que fornece informações ao receptor (FARIA *et al.*, 2018). O mesmo processo também pode ser visto com outra ilustração em (KYLE *et al.*, 2014). A detecção da correlação de picos também pode ser estudada no domínio da frequência como demonstra (ZHANG, 2014).

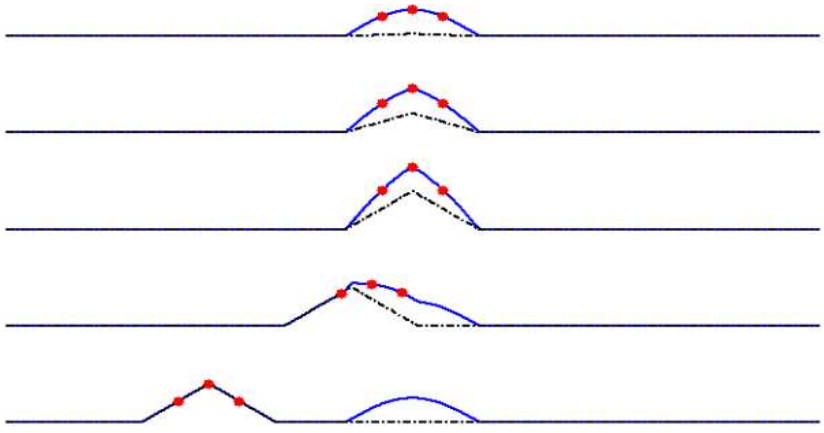

Figura 2.7 Processo de falsificação do sinal GPS (KYLE *et al.*, 2014).

Em linhas gerais, existem quatro principais estratégias para aplicação do *spoofing* (WU *et al.*, 2020):

- Ataque spoofing com réplica/repetição (*Replay spoofing attack* - RSA), que é considerado neste trabalho;
- Ataque spoofing com falsificação (Forgery *spoofing attack* - FSA);
- Ataque spoofing com estimação (*Estimation spoofing attack* - ESA);
- Ataque spoofing avançado (*Advanced spoofing attack* - ASA);

Para cada uma das estratégias citadas, pode-se desenvolver diversas técnicas de ataque citadas em (WU *et al.*, 2020), conforme se vê no fluxograma da Figura 2.8. Cabe ressaltar que as estratégias e técnicas muitas vezes podem ser utilizadas de forma concomitante com fito de efetivar ainda mais o ataque. As estratégias e técnicas costumam ser elencadas quanto aos níveis de dificuldade de implementação, efetividade de ataque, e custo da implementação.

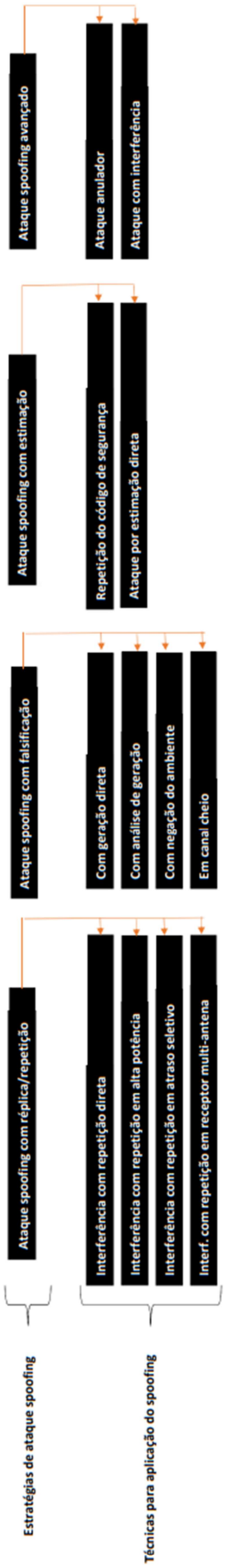

Figura 2.8 Técnicas de ataque *Spoofing*.

E ainda, os ataques *spoofing* podem ser elencados como sugere (HUMPHREYS, 2008), levando em consideração a dificuldade para implementação:

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.

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 ser facilmente detectado. Um ataque via receptor portátil, 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 (com 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 em 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 utilizando um receptor spoofer, mas é quase impossível de ser detectado com os atuais métodos de defesa.

2.4 Modelo de Dados

O modelo de dados para geração dos sinais GPS e utilizado na simulação do spoofing é apresentado nesta sessão. O sinal complexo em banda base de um sinal GPS amostrado e quantizado recebido por um arranjo de antena de m = 1,..., M sensores é dado por

$$\mathbf{x}_m[k] = \sum_{i=1}^{I} a_m(\varphi_i[k], \vartheta_i[k])\sqrt{P_i[k]}\left(\mathbf{c}_i[k;\ \tau_i[k]] \odot \mathbf{d}\left[k;\ \nu_i[k], \phi_{\nu,i}[k]\right]\right) +$$

$$\sum_{q=1}^{Q} a_m(\varphi_q[k], \vartheta_q[k])\sqrt{P_q[k]}\left(\mathbf{c}_q\left[k;\ \tau_q[k]\right] \odot \mathbf{d}\left[k;\ \nu_q[k], \phi_{\nu,q}[k]\right]\right) + \mathbf{n}_m[k]\ , \quad (2.5)$$

onde

$$\mathbf{x}_m[k] = [x_m(kNT_s),\ldots, x_m((kN + n)\,T_s),\ldots, x_m((kN + N - 1)\,T_s)]^T \quad (2.6)$$

$$\mathbf{n}_m[k] = [n_m(kNT_s),\ldots, n_m((kN + n)\,T_s),\ldots, n_m((kN + N - 1)\,T_s)]^T \quad (2.7)$$

$$\mathbf{c}_i[k; \tau_i[k]] = [c_i(\tau_i[k]),\ldots, c_i(nT_s - \tau_i[k]),\ldots, c_i((N-1)T_s - \tau_i[k])]^T \quad (2.8)$$

$$\mathbf{c}_q[k; \tau_q[k]] = [c_q(\tau_q[k]),\ldots, c_q(nT_s - \tau_q[k]),\ldots, c_q((N-1)T_s - \tau_q[k])]^T \quad (3.9)$$

$$\mathbf{d}[k; \nu_i, \phi_{\nu,i}[k]] = [\exp(j\phi_{\nu,i}[k]),\ldots,\exp(j(2\pi\nu_i[k]nTs+\phi_{\nu,i}[k])),\ldots,\exp(j(2\pi\nu_i[k](N-1)T_s+\phi_{\nu,i}[k])]^T \quad (2.10)$$

$$\mathbf{d}[k; \nu_q, \phi_{\nu,q}[k]] = [\exp(j\phi_{\nu,q}[k]),\ldots,\exp(j(2\pi\nu_q[k]nTs+\phi_{\nu,q}[k])),\ldots,\exp(j(2\pi\nu_q[k](N-1)T_s+\phi_{\nu,q}[k])]^T \quad (2.11)$$

sendo:

$\odot$ o produto de Hadamard-Schur (multiplicação elementar);

n = 0, 1,..., N – 1 os instantes de amostragem;

k = 0, 1,..., K − 1 o período;

T_s a duração da amostragem;

i = 1,..., I os sinais de satélites recebidos;

q = 1,..., Q os sinais Q de *spoofing* recebidos;

$c_i(t)$ e $c_q(t)$ as sequências binárias pseudoaleatórias;

τ_i [k] e $\tau_q[k]$ os atrasos de tempo;

$\nu_i[k]$ e $\nu_q[k]$ os desvios Doppler;

$\phi_{\nu,i}[k]$ e $\phi_{\nu,q}[k]$ as fases Doppler;

$a_m(\varphi_i\,[k], \vartheta_i\,[k]) \in \mathbb{C}$ e $a_m(\varphi_q[k], \vartheta_q[k]) \in \mathbb{C}$ o m-ésimo elemento dos vetores de direção da matriz;

$\varphi_i[k] \in [-\pi, \pi]$ e $\varphi_q[k] \in [-\pi, \pi]$ os ângulos de azimute;

$\vartheta_i[k] \in [0, \pi/2]$ e $\vartheta_q[k] \in [0, \pi/2]$ os ângulos de elevação; e

$P_i[k]$ e $P_q[k]$ as potências de sinal.

Assume-se que o *spoofer* está recebendo os mesmos sinais de satélite que o receptor e, portanto, está retransmitindo as mesmas sequências binárias pseudoaleatórias de forma amplificada e direta. Um ataque de *spoofing* comumente pode ser chamado de ataque repetidor ou ataque *meaconing*. Os vetores de direção dos sinais de satélite recebidos são:

$$\mathbf{a}(\varphi_i[k], \vartheta_i[k]) = [a_1(\varphi_i[k], \vartheta_i[k]), \ldots a_m(\varphi_i[k], \vartheta_i[k]), \ldots, a_M(\varphi_i[k], \vartheta_i[k])]^T \quad (2.12)$$

e os vetores de direção dos sinais de *spoofing* recebidos são:

$$\mathbf{a}(\varphi_q[k], \vartheta_q[k]) = [a_1(\varphi_q[k], \vartheta_q[k]), \ldots a_m(\varphi_q[k], \vartheta_q[k]), \ldots, a_M(\varphi_q[k], \vartheta_q[k])]^T . \quad (2.13)$$

Além disso, assumimos

$$||\mathbf{c}_i[k; \tau_i[k]]||_2^2 = ||\mathbf{c}_q[k; \tau_q[k]]||_2^2 = N . \quad (2.14)$$

Quando em geral

$$||\mathbf{c}_i[k; \tau_i[k]]||_2^2 \neq N, \forall \tau_i[k] , \quad (2.15)$$

$$||\mathbf{c}_q[k; \tau_q[k]]||_2^2 \neq N, \forall \tau_q[k] . \quad (2.16)$$

No entanto, em muitos casos, como por exemplo no caso de sequências binárias pseudoaleatórias GPS C/A com largura de banda B ≥ 1,023 MHz, pode-se assumir que

$$||\mathbf{c}_i[k; \tau_i[k]]||_2^2 \approx N, \forall \tau_i[k] , \quad (2.17)$$

$$||\mathbf{c}_q[k; \tau_q[k]]||_2^2 \approx N, \forall \tau_q[k] . \quad (2.18)$$

Como as sequências binárias pseudoaleatórias de todos os GNSS têm boas propriedades de correlação cruzada e de autocorrelação, pode-se assumir que as sequências binárias pseudoaleatórias de diferentes satélites não estão correlacionadas, logo

$$\mathbf{c}_i^T[k; \tau_i[k]]\mathbf{c}_p[k; \tau_p[k]] \approx 0, \text{ para } i \neq p \quad (2.19)$$

e então os sinais de spoofing também são descorrelacionados com

$$\mathbf{c}_q^T[k; \tau_q[k]]\mathbf{c}_p[k; \tau_p[k]] \approx 0, \text{ para } q \neq p . \quad (2.20)$$

Além disso, como assumimos que o transmissor dos sinais de *spoofing* tem uma distância superior a cT_c para o receptor vítima, onde c denota a velocidade da luz e T_c é a duração do chip de sequência binária pseudoaleatória, também podemos assumir que os sinais de satélite e os sinais de *spoofing* com a mesma sequência binária pseudoaleatória i = q são todos descorrelacionados também com

$$\mathbf{c}_i^T[k; \tau_i[k]]\mathbf{c}_q[k; \tau_q[k]] \approx 0, \text{ para } i = q \text{ e } |\tau_i[k] - \tau_q[k]| > Tc. \quad (2.21)$$

O ruído é complexo gaussiano $\mathbb{C}\, N(0, \sigma_n^2)$ com

$$E||\mathbf{n}_m[k]||_2^2 = \sigma_n^2 , \quad (2.22)$$

$$E[\mathbf{n}_m^H[k]\mathbf{n}_p[k]] = 0, \text{ com } m \neq p , \quad (2.23)$$

$$E[\mathbf{n}_m[k]\mathbf{n}_m^H[k]] = \sigma_n^2\mathbf{I}_n . \quad (2.24)$$

onde I_N denota a matriz identidade NxN.

Considera-se neste trabalho uma antena isotrópica, sem as considerações de polarização e acoplamento mútuo entre os sensores, com os 7 sensores localizados conforme a Figura 3.7 e nas seguintes coordenadas cartesianas:

$$\mathbf{p}_1 = [p_{x,1}, p_{y,1}, p_{z,1}]\ T = [0, 0, 0]^T \quad (2.25)$$

$$\mathbf{p}_2 = [p_{x,2}, p_{y,2}, p_{z,2}]\ T = [-\lambda/4, \sqrt{3}\,\lambda/4, 0]^T \quad (2.26)$$

$$\mathbf{p}_3 = [p_{x,3}, p_{y,3}, p_{z,3}]\ T = [\lambda/4, \sqrt{3}\,\lambda/4, 0]^T \quad (2.27)$$

$$\mathbf{p}_4 = [p_{x,4}, p_{y,4}, p_{z,4}]\ T = [\lambda/2, 0, 0]^T \quad (2.28)$$

$$\mathbf{p}_5 = [p_{x,5}, p_{y,5}, p_{z,5}]\ T = [\lambda/4, -\sqrt{3}\,\lambda/4, 0]^T \quad (2.29)$$

$$\mathbf{p}_6 = [p_{x,6}, p_{y,6}, p_{z,6}]\ T = [-\lambda/4, -\sqrt{3}\,\lambda/4, 0]^T \quad (2.30)$$

$$\mathbf{p}_7 = [p_{x,7}, p_{y,7}, p_{z,7}]\ T = [-\lambda/2, 0, 0]^T . \quad (2.31)$$

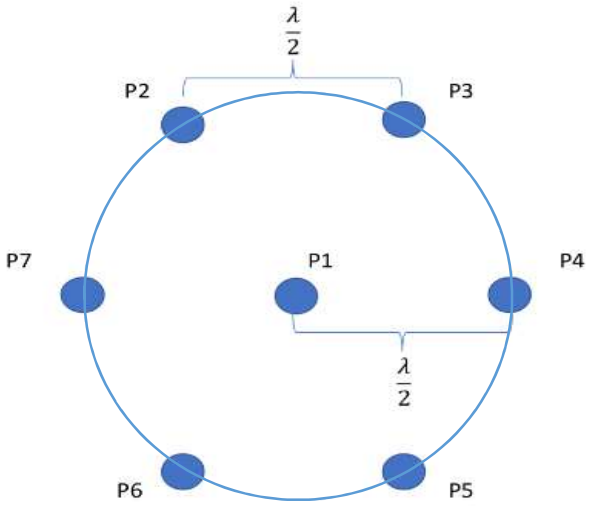

Figura 2.9 Vista superior do arranjo de sensores do receptor/vítima.

Onde λ é o comprimento de onda da portadora L_1 e dos sinais *spoofing*, e c é a velocidade da luz. Pode-se assumir onda distante e banda estreita, e que os vetores direcionais definem que as diferenças de fase relativa podem ser dadas por

$$\mathbf{a}(\varphi[k], \vartheta[k]) = \begin{bmatrix} e^{j\frac{2\pi}{\lambda}\left(u_x[k]p_{x,1} + u_y[k]p_{y,1} + u_z[k]p_{z,1}\right)} \\ e^{j\frac{2\pi}{\lambda}\left(u_x[k]p_{x,2} + u_y[k]p_{y,2} + u_z[k]p_{z,2}\right)} \\ \vdots \\ e^{j\frac{2\pi}{\lambda}\left(u_x[k]p_{x,M} + u_y[k]p_{y,M} + u_z[k]p_{z,M}\right)} \end{bmatrix} \quad (2.32)$$

com

$$\mathbf{u}[k] = \begin{bmatrix} \cos(\varphi[k])\cos(\vartheta[k]) \\ \sin(\varphi[k])\cos(\vartheta[k]) \\ \sin(\vartheta[k]) \end{bmatrix} = \begin{bmatrix} u_x[k] \\ u_y[k] \\ u_z[k] \end{bmatrix} \quad (2.33)$$

O sinal recebido na saída dos sensores da antena podem ser dados pela seguinte notação matricial:

$$\mathbf{X}[k] = \mathbf{A}[k]\boldsymbol{\Gamma}[k](\mathbf{C}[k] \odot \mathbf{D}[k]) + \mathbf{A}_s[k]\boldsymbol{\Gamma}_s[k](\mathbf{C}_s[k] \odot \mathbf{D}_s[k]) + \mathbf{N}[k] \quad (2.34)$$

com

$$\mathbf{X}[k] = [\mathbf{x}_1[k] \ldots \mathbf{x}_m[k] \ldots \mathbf{x}_M[k]]^T \in \mathbb{C}^{M \times N} \quad (2.35)$$

$$\mathbf{A}[k] = [\mathbf{a}(\varphi_1[k], \vartheta_1[k]) \ldots \mathbf{a}(\varphi_i[k], \vartheta_i[k]) \ldots \mathbf{a}(\varphi_I[k], \vartheta_I[k])] \in \mathbb{C}^{M \times I} \quad (2.36)$$

$$\mathbf{A}_s[k] = [\mathbf{a}(\varphi_1[k], \vartheta_1[k]) \ldots \mathbf{a}(\varphi_q[k], \vartheta_q[k]) \ldots \mathbf{a}(\varphi_Q[k], \vartheta_Q[k])] \in \mathbb{C}^{M \times Q} \quad (2.37)$$

$$\boldsymbol{\Gamma}[k] = \text{diag}\{[\sqrt{P_1[k]}, \ldots, \sqrt{P_i[k]}, \ldots, \sqrt{P_I[k]}]^T\} \in \mathbb{R}^{I \times I} \quad (2.38)$$

$$\boldsymbol{\Gamma}_s[k] = \text{diag}\{[\sqrt{P_1[k]}, \ldots, \sqrt{P_q[k]}, \ldots, \sqrt{P_Q[k]}]^T\} \in \mathbb{R}^{Q \times Q} \quad (2.39)$$

$$\mathbf{C}[k] = [\mathbf{c}_1[k; \tau_1[k]] \ldots \mathbf{c}_i[k; \tau_i[k]] \ldots \mathbf{c}_I[k; \tau_I[k]]]^T \in \mathbb{R}^{I \times N} \quad (2.40)$$

$$\mathbf{C}_s[k] = [\mathbf{c}_1[k; \tau_1[k]] \ldots \mathbf{c}_q[k; \tau_q[k]] \ldots \mathbf{c}_Q[k; \tau_Q[k]]]^T \in \mathbb{R}^{Q \times N} \quad (2.41)$$

$$\mathbf{D}[k] = [\mathbf{d}[k; \nu_1, \phi_{v,1}[k]] \ldots \mathbf{d}[k; \nu_i, \phi_{v,i}[k]] \ldots \mathbf{d}[k; \nu_I, \phi_{v,I}[k]]]^T \in \mathbb{C}^{I \times N} \quad (2.42)$$

$$\mathbf{D}_s[k] = [\mathbf{d}[k; \nu_1, \phi_{v,1}[k]] \ldots \mathbf{d}[k; \nu_q, \phi_{v,q}[k]] \ldots \mathbf{d}[k; \nu_Q, \phi_{v,Q}[k]]]^T \in \mathbb{C}^{Q \times N} \quad (2.43)$$

$$\mathbf{N}[k] = [\mathbf{n}_1[k] \ldots \mathbf{n}_m[k] \ldots \mathbf{n}_M[k]]^T \in \mathbb{C}^{M \times N}. \quad (2.44)$$

A matriz de covariância espacial pode ser dada por:

$$\begin{aligned} \mathbf{R}_{xx}[k] &= E[\mathbf{X}[k]\mathbf{X}^H[k]] \in \mathbb{C}^{M \times M} \\ &= \mathbf{R}[k] + \mathbf{R}_s[k] + \mathbf{R}_n[k] \end{aligned} \quad (2.45)$$

onde

$$\begin{aligned} \mathbf{R}[k] &= E[\mathbf{A}[k]\boldsymbol{\Gamma}[k](\mathbf{C}[k] \odot \mathbf{D}[k])(\mathbf{C}[k] \odot \mathbf{D}[k])^H \boldsymbol{\Gamma}^H[k] \mathbf{A}^H[k]] \\ &= E[\mathbf{A}[k]] \boldsymbol{\Gamma}[k] \boldsymbol{\Gamma}^H[k] \mathbf{A}^H[k]], \end{aligned} \quad (2.46)$$

$$\begin{aligned} \mathbf{R}_s[k] &= E[\mathbf{A}_s[k]\boldsymbol{\Gamma}_s[k](\mathbf{C}_s[k] \odot \mathbf{D}_s[k])(\mathbf{C}_s[k] \odot \mathbf{D}_s[k])^H \boldsymbol{\Gamma}_s^H[k] \mathbf{A}_s^H[k]] \\ &= E[\mathbf{A}_s[k] \boldsymbol{\Gamma}_s[k] \boldsymbol{\Gamma}_s^H[k] \mathbf{A}_s^H[k]], \end{aligned} \quad (2.47)$$

$$\mathbf{R}_n[k] = E[\mathbf{N}[k]\mathbf{N}^H[k]] = \sigma_n^2 \mathbf{I}_M. \quad (2.48)$$

Realizando a correlação entre o sinal recebido do sensor m = 1 com os sinais M − 1 recebidos por todos os outros sensores, obtém-se

$$y[k] = \begin{bmatrix} \frac{1}{N} \mathbf{x}_1^H[k]\mathbf{x}_2[k] \\ \vdots \\ \frac{1}{N} \mathbf{x}_1^H[k]\mathbf{x}_m[k] \\ \vdots \\ \frac{1}{N} \mathbf{x}_1^H[k]\mathbf{x}_M[k] \end{bmatrix} \in \mathbb{C}^{M-1 \times 1} \quad . \quad (2.49)$$

Coletando as correlações para k períodos pode-se escrever

$$\mathbf{Y} = [\mathbf{y}[1] \cdots \mathbf{y}[k] \cdots \mathbf{y}[K]]^T \in \mathbb{C}^{M-1 \times K} \quad . \quad (2.50)$$

O sinal após a correlação do sinal do sensor m = 1 com o sensor m = 2,..., M-1 pode ser dado como

$$\frac{1}{N} \mathbf{x}_1^H[k]\mathbf{x}_m[k] = \sum_{i=1}^{I} \underbrace{a_1^*(\varphi_i[k], \vartheta_i[k]) a_m(\varphi_i[k], \vartheta_i[k])}_{\tilde{a}_{m-1}(\varphi_i[k], \vartheta_i[k])} P_i[k] +$$

$$\sum_{i=1}^{I} \underbrace{a_1^*(\varphi_q[k], \vartheta_q[k]) a_m(\varphi_q[k], \vartheta_q[k])}_{\tilde{a}_{m-1}(\varphi_q[k], \vartheta_q[k])} P_q[k] +$$

$$\frac{1}{N}\mathbf{n}_1^H[k]\sum_{i=1}^{I} a_m(\varphi_i[k],\vartheta_i[k])\sqrt{P_i[k]}\,(\mathbf{c}_i[k;\tau_i[k]]\odot\mathbf{d}[k;\nu_i[k],\phi_{v,i}[k]])+$$

$$\frac{1}{N}\sum_{i=1}^{I} a_1^*(\varphi_i[k],\vartheta_i[k])\sqrt{P_i[k]}\,(\mathbf{c}_i[k;\tau_i[k]]\odot\mathbf{d}[k;\nu_i\,[k],\phi_{v,i}[k]])^H\,\mathbf{n}_m[k]+$$

$$\frac{1}{N}\mathbf{n}_1^H[k]\sum_{q=1}^{Q} a_m(\varphi_q[k],\vartheta_q[k])\sqrt{P_q[k]}\,(\mathbf{c}_q[k;\tau_q[k]]\odot\mathbf{d}[k;\nu_q[k],\phi_{v,q}[k]])+$$

$$\frac{1}{N}\sum_{q=1}^{Q} a_1^*(\varphi_q[k],\vartheta_q[k])\sqrt{P_q[k]}(\mathbf{c}_q[k;\tau_q[k]]\odot\mathbf{d}[k;\nu_q[k],\phi_{v,q}[k]])^H\,\mathbf{n}_m[k]+$$

$$\frac{1}{N}\mathbf{n}_1^H[k]\mathbf{n}_m[k]$$

$$=\sum_{i=1}^{I}\tilde{a}_{m-1}(\varphi_i[k],\vartheta_i[k])P_i[k]+\sum_{i=q}^{Q}\tilde{a}_{m-1}(\varphi_q[k],\vartheta_q[k])\,P_q[k]+\tilde{n}_{m-1}[k]. \quad (2.51)$$

Agora, assumindo que as direções de chegada (DOAs) são constantes durante K observações com k =1, …, K e considerando que $a_1(\varphi_i[k],\vartheta_i[k]) = 1$ podemos escrever o sinal de pós-correlação em uma notação matricial

$$\mathbf{Y} = \tilde{\mathbf{A}}\mathbf{P} + \tilde{\mathbf{A}}_s\mathbf{P}_s + \tilde{\mathbf{N}} \quad (2.52)$$

onde

$$\tilde{\mathbf{A}} = [\tilde{\mathbf{a}}(\varphi_1,\vartheta_1)\ldots\ \tilde{\mathbf{a}}(\varphi_i,\vartheta_i)\ldots\ \tilde{\mathbf{a}}(\varphi_I,\vartheta_I)] \in \mathbb{C}^{\,M-1\ x\ I} \quad (2.53)$$

$$\tilde{\mathbf{A}}_s = [\tilde{\mathbf{a}}(\varphi_1,\vartheta_1)\ldots\ \tilde{\mathbf{a}}(\varphi_q,\vartheta_q)\ldots\ \tilde{\mathbf{a}}(\varphi_Q,\vartheta_Q)] \in \mathbb{C}^{\,M-1\ x\ Q} \quad (2.54)$$

$$\tilde{\mathbf{a}} = [\tilde{a}_1(\varphi,\vartheta)\ldots\ \tilde{a}_m(\varphi,\vartheta)\ldots\ \tilde{a}_{M-1}(\varphi,\vartheta)] \in \mathbb{C}^{\,M-1\ x\ 1} \quad (2.55)$$

$$\mathbf{P} = \begin{bmatrix} P_1[1] & \ldots & P_1[k] & \ldots & P_1[K] \\ & & \vdots & & \\ P_i[1] & \ldots & P_i[k] & \ldots & P_i[K] \\ & & \vdots & & \\ P_I[1] & \ldots & P_I[k] & \ldots & P_I[K] \end{bmatrix} \in \mathbb{R}^{I\times K} \quad (2.56)$$

$$\mathbf{P}s = \begin{bmatrix} P_1[1] & \ldots & P_1[k] & \ldots & P_1[K] \\ & & \vdots & & \\ P_q[1] & \ldots & P_q[k] & \ldots & P_q[K] \\ & & \vdots & & \\ P_Q[1] & \ldots & P_Q[k] & \ldots & P_Q[K] \end{bmatrix} \in \mathbb{R}^{Q\times K} \quad (2.57)$$

$$\tilde{\mathbf{N}} = [\tilde{\mathbf{n}}[1]\ldots\tilde{\mathbf{n}}[k]\ldots\tilde{\mathbf{n}}[K]]$$

$$= \begin{bmatrix} \tilde{n}_1[1] & \ldots & \tilde{n}_1[k] & \ldots & \tilde{n}_1[K] \\ & & \vdots & & \\ \tilde{n}_m[1] & \ldots & \tilde{n}_m[k] & \ldots & \tilde{n}_m[K] \\ & & \vdots & & \\ \tilde{n}_{M-1}[1] & \ldots & \tilde{n}_{M-1}[k] & \ldots & \tilde{n}_{M-1}[K] \end{bmatrix} \in \mathbb{C}^{M-1\times K}. \quad (2.58)$$

Finalmente, pode-se definir a matriz de covariância espacial como:

$$\mathbf{R}_{YY} = E[\mathbf{Y}\mathbf{Y}^H] \in \mathbb{C}^{\,M\text{-}1xM\text{-}1}$$

$$= \tilde{\mathbf{A}}E[\mathbf{P}\mathbf{P}^H]\tilde{\mathbf{A}}^H + \tilde{\mathbf{A}}_s\, E[\mathbf{P}_s\mathbf{P}_s{}^H]\tilde{\mathbf{A}}_s{}^H + E[\tilde{\mathbf{N}}\tilde{\mathbf{N}}^H]\ . \qquad (2.59)$$

Usando (3.51) pode-se escrever:

$$\tilde{\mathbf{n}}[k] = \frac{1}{N}\sum_{i=1}^{I} \tilde{\mathbf{a}}(\varphi_i, \vartheta_i)\sqrt{P_i[k]} + \mathbf{n}_1^H[k](\mathbf{c}_i[k; \tau_i[k]] \odot \mathbf{d}[k; \nu_i[k], \phi_{v,i}[k]]) +$$

$$\frac{1}{N}\sum_{i=1}^{I} \sqrt{P_i[k]}\ \overline{\mathbf{N}}[k](\mathbf{c}_i[k; \tau_i[k]] \odot \mathbf{d}[k; \nu_i[k], \phi_{v,i}[k]])^* +$$

$$\frac{1}{N}\sum_{q=1}^{Q} \tilde{\mathbf{a}}(\varphi_q, \vartheta_q)\sqrt{P_q[k]} + \mathbf{n}_1^H[k](\mathbf{c}_q[k; \tau_q[k]] \odot \mathbf{d}[k; \nu_q[k], \phi_{v,q}[k]]) +$$

$$\frac{1}{N}\sum_{q=1}^{Q} \sqrt{P_q[k]}\ \overline{\mathbf{N}}[k](\mathbf{c}_q[k; \tau_q[k]] \odot \mathbf{d}[k; \nu_q[k], \phi_{v,q}[k]])^* +$$

$$\frac{1}{N}\ \overline{\mathbf{N}}[k]\mathbf{n}_1^*[k] \qquad (2.60)$$

onde

$$\overline{\mathbf{N}}[k] = \left[\mathbf{n}_2[k] \ldots \mathbf{n}_m[k] \ldots \mathbf{n}_{M-1}[k]\right]^T \in \mathbb{C}^{M-1\ x\ N} \qquad . \qquad (2.61)$$

A matriz de covariância do ruído $\tilde{\mathbf{n}}[k]$, com todos os parâmetros constantes, podem ser:

$$\mathbf{R}_{\tilde{n}\tilde{n}} = E[\tilde{N}\tilde{N}^H] = E[\tilde{\mathbf{n}}[k]\tilde{\mathbf{n}}^H[k]] =$$

$$\frac{1}{N^2}\sum_{i=1}^{I} \tilde{\mathbf{a}}(\varphi_i, \vartheta_i)P_i\ (\mathbf{c}_i[k; \tau_i] \odot \mathbf{d}[k; \nu_i, \phi_{v,i}])^H\, E[\mathbf{n}_1[k]\mathbf{n}_1^H[k]](\mathbf{c}_i[k; \tau_i] \odot \mathbf{d}[k; \nu_i, \phi_{v,i}])\tilde{\mathbf{a}}^H(\varphi_i, \vartheta_i) +$$

$$\frac{1}{N^2}\sum_{i=1}^{I} P_i\, E[\overline{\mathbf{N}}[k](\mathbf{c}_i[k; \tau_i] \odot \mathbf{d}[k; \nu_i, \phi_{v,i}])\ (\mathbf{c}_i[k; \tau_i] \odot \mathbf{d}[k; \nu_i, \phi_{v,i}])^T\, \overline{\mathbf{N}}^H[k] +$$

$$\frac{1}{N^2}\sum_{i=q}^{Q} \tilde{a}(\varphi_q, \vartheta_q)P_q + (\mathbf{c}_q[k; \tau_q] \odot \mathbf{d}[k; \nu_q, \phi_{v,q}])^H E[\mathbf{n}_1[k]\mathbf{n}_1^H[k]](\mathbf{c}_q[k; \tau_q] \odot \mathbf{d}[k; \nu_q, \phi_{v,q}])\tilde{\mathbf{a}}^H(\varphi_q, \vartheta_q) +$$

$$\frac{1}{N^2}\sum_{i=q}^{Q} P_q\, E[\overline{\mathbf{N}}[k](\mathbf{c}_q[k; \tau_q] \odot \mathbf{d}[k; \nu_q, \phi_{v,q}])(\mathbf{c}_q[k; \tau_q] \odot \mathbf{d}[k; \nu_q, \phi_{v,q}])^T\, \overline{\mathbf{N}}^H[k] +$$

$$\frac{1}{N^2}E[\overline{\mathbf{N}}[k]\mathbf{n}_1^*[k]\mathbf{n}_1^T[k]\overline{\mathbf{N}}^H[k]] \qquad (2.62)$$

onde

$$E[\overline{\mathbf{N}}[k](\mathbf{c}_{i/q}[k; \tau_{i/q}] \odot \mathbf{d}[k; \nu_{i/q}, \phi_{v,\,i/q}])^*(\mathbf{c}_q[k; \tau_{i/q}] \odot \mathbf{d}[k; \nu_{i/q}, \phi_{v,\,i/q}])^T\, \overline{\mathbf{N}}^H[k]] = \sigma_n^2 N\mathbf{I}_{M-1} \qquad (2.63)$$

E também, considerando [1]$E[\mathbf{a}^T\mathbf{b}^*\mathbf{b}^T\mathbf{a}^*] = E[tr\{\mathbf{a}^*\mathbf{a}^T\mathbf{b}^*\mathbf{b}^T\}] = tr\{E[\mathbf{a}^*\mathbf{a}^T\mathbf{b}^*\mathbf{b}^T]\} = tr\{E[\mathbf{a}\mathbf{a}^H]\ E[\mathbf{b}\mathbf{b}^H]\} = tr\{\sigma_a^2\mathbf{I}_M\sigma_b^2\mathbf{I}_M\} = M\sigma_a^2\sigma_b^2$ com $\mathbf{a}, \mathbf{b} \in \mathbb{C}^{M-1\times 1}$ com média zero multivariada Gaussiana com $\mathcal{CN}\ (0, \sigma_{a/b}^2, \mathbf{I}_M)$ e independente, tem-se:

$$\mathrm{E}[\overline{\mathbf{N}}[k]\mathbf{n}_1^*[k]\mathbf{n}_1^{\mathrm{T}}[k]\overline{\mathbf{N}}^{\mathrm{H}}[k]] =$$

$$\begin{bmatrix} \mathrm{E}\left[\mathbf{n}_2^{\mathrm{T}}[k]\mathbf{n}_1^*[k]\mathbf{n}_1^{\mathrm{T}}[k]\mathbf{n}_2^*[k]\right] & \mathrm{E}\left[\mathbf{n}_2^{\mathrm{T}}[k]\mathbf{n}_1^*[k]\mathbf{n}_1^{\mathrm{T}}[k]\mathbf{n}_3^*[k]\right] & \dots & \mathrm{E}\left[\mathbf{n}_2^{\mathrm{T}}[k]\mathbf{n}_1^*[k]\mathbf{n}_1^{\mathrm{T}}[k]\mathbf{n}_{\mathrm{M}-1}^*[k]\right] \\ \mathrm{E}\left[\mathbf{n}_3^{\mathrm{T}}[k]\mathbf{n}_1^*[k]\mathbf{n}_1^{\mathrm{T}}[k]\mathbf{n}_2^*[k]\right] & \mathrm{E}\left[\mathbf{n}_3^{\mathrm{T}}[k]\mathbf{n}_1^*[k]\mathbf{n}_1^{\mathrm{T}}[k]\mathbf{n}_3^*[k]\right] & \dots & \mathrm{E}\left[\mathbf{n}_3^{\mathrm{T}}[k]\mathbf{n}_1^*[k]\mathbf{n}_1^{\mathrm{T}}[k]\mathbf{n}_{\mathrm{M}-1}^*[k]\right] \\ \vdots & \vdots & & \vdots \\ \mathrm{E}\left[\mathbf{n}_{\mathrm{M}-1}^{\mathrm{T}}[k]\mathbf{n}_1^*[k]\mathbf{n}_1^{\mathrm{T}}[k]\mathbf{n}_2^*[k]\right] & \dots & & \mathrm{E}\left[\mathbf{n}_{\mathrm{M}-1}^{\mathrm{T}}[k]\mathbf{n}_1^*[k]\mathbf{n}_1^{\mathrm{T}}[k]\mathbf{n}_{\mathrm{M}-1}^*[k]\right] \end{bmatrix}$$

$$= \mathrm{E}[\mathbf{n}_2^{\mathrm{T}}[k]\mathbf{n}_1^*[k]] = (\mathrm{M}\text{-}1)\,\sigma_{\mathrm{n}}^4\mathbf{I}_{\mathrm{M}-1} \tag{2.64}$$

bem como

$$(\mathbf{c}_{\mathrm{i/q}}[k;\tau_{\mathrm{i/q}}] \odot \mathbf{d}[k;\nu_{\mathrm{i/q}},\phi_{\nu,\,\mathrm{i/q}}])^{\mathrm{H}}\underbrace{\mathrm{E}[\mathbf{n}_1[k]\mathbf{n}_1^{\mathrm{H}}[k]]}_{=\sigma_{\mathrm{n}}^2\mathbf{I}_{\mathrm{N}}}(\mathbf{c}_{\mathrm{i/q}}[k;\tau_{\mathrm{i/q}}] \odot \mathbf{d}[k;\nu_{\mathrm{i/q}},\phi_{\nu,\,\mathrm{i/q}}]) = \mathrm{N}\sigma_{\mathrm{n}}^2\ . \tag{2.65}$$

Finalmente, tem-se

$$\mathbf{R}_{\tilde{\mathbf{n}}\tilde{\mathbf{n}}} = \sum_{\mathrm{i}=1}^{\mathrm{I}} \frac{\mathrm{P_i}\sigma_{\mathrm{n}}^2}{\mathrm{N}}\tilde{\mathbf{a}}(\varphi_{\mathrm{i}},\vartheta_{\mathrm{i}})\tilde{\mathbf{a}}^{\mathrm{H}}(\varphi_{\mathrm{i}},\vartheta_{\mathrm{i}}) + \sum_{\mathrm{i}=1}^{\mathrm{I}} \frac{\mathrm{P_i}\sigma_{\mathrm{n}}^2}{\mathrm{N}}\mathbf{I}_{\mathrm{M}\text{-}1} +$$

$$\sum_{\mathrm{q}=1}^{\mathrm{Q}} \frac{\mathrm{P_q}\sigma_{\mathrm{n}}^2}{\mathrm{N}}\tilde{\mathbf{a}}(\varphi_{\mathrm{q}},\vartheta_{\mathrm{q}})\tilde{\mathbf{a}}^{\mathrm{H}}(\varphi_{\mathrm{q}},\vartheta_{\mathrm{q}}) + \sum_{\mathrm{q}=1}^{\mathrm{Q}} \frac{\mathrm{P_q}\sigma_{\mathrm{n}}^2}{\mathrm{N}}\mathbf{I}_{\mathrm{M}\text{-}1} +$$

$$\frac{(\mathrm{M}-1)}{\mathrm{N}^2}\,\sigma_{\mathrm{n}}^4\mathbf{I}_{\mathrm{M}\text{-}1}\ . \tag{2.66}$$

Assim, o ruído, após a correlação do sinal recebido pela antena m = 1 com o sinal recebido das outras antenas, ainda é gaussiano, embora colorido espacialmente. A relação sinal-ruído (SNR) antes desta correlação para cada satélite recebido ou sinal de falsificação em cada antena de recepção é dada por

$$\mathrm{SNR_x} = \frac{\mathrm{P_{i/q}}}{\sigma_{\mathrm{n}}^2} \tag{2.67}$$

e é da ordem de -20 a -15 dB. Considerando (2.66), o SNR para cada satélite recebido ou sinal spoofing após a correlação em cada sensor da antena de recepção tem-se

$$\mathrm{SNR_y} = \frac{\mathrm{P_{i/q}^2}}{\frac{\mathrm{P_{i/q}}\sigma_{\mathrm{n}}^2}{\mathrm{N}} + \frac{\mathrm{IP_i}\sigma_{\mathrm{n}}^2}{\mathrm{N}} + \frac{\mathrm{QP_q}\sigma_{\mathrm{n}}^2}{\mathrm{N}} + \frac{\mathrm{M}-1}{\mathrm{N}^2}\sigma_{\mathrm{n}}^4}\quad . \tag{2.68}$$

No caso de $\mathrm{P_i} = \mathrm{P_q} = \mathrm{P}$ e $\mathrm{N} >> \mathrm{M}$ pode-se escrever

$$\mathrm{SNR_y} \approx \frac{P}{\frac{\sigma_{\mathrm{n}}^2}{\mathrm{N}} + \frac{\mathrm{I}\sigma_{\mathrm{n}}^2}{\mathrm{N}} + \frac{\mathrm{Q}\sigma_{\mathrm{n}}^2}{\mathrm{N}}} = \frac{P}{\sigma_{\mathrm{n}}^2}\frac{N}{(1+\mathrm{I}+\mathrm{Q})} = \mathrm{SNR_x}\frac{N}{(1+\mathrm{I}+\mathrm{Q})}\quad . \tag{2.69}$$

No caso de uma largura de banda unilateral dos sinais GNSS, B = 1,023 MHz com N = 2046 e I = Q = 13, o $\mathrm{SNR_y}$ é aumentado em cerca de 19 dB em relação ao $\mathrm{SNR_x}$. Assim, correlacionando os sinais recebidos pelas antenas m = 2, ..., M com o sinal recebido da antena m = 1 tem-se um aumento do SNR efetivo em cada sensor da antena receptora e fornece

condições razoáveis para analisar os DOAs dos sinais recebidos sem conhecimento sobre os sinais em si, apesar de sua largura de banda e frequência da portadora serem necessários.

3 Detecção de Spoofing na operação do GPS

Embora os sinais transmitidos pelos satélites sejam extremamente fracos (na ordem de $5x10^{-17}$ W na recepção) e vulneráveis a interferências não intencionais e sobretudo ao bloqueio deliberado (*jamming/spoofing*), o GPS é o primeiro sistema de radionavegação cujo sinal tem propriedades *anti-jamming/anti-spoofing*. Isso é conseguido espalhando-se os sinais GPS por uma banda de frequências alargada, através de uma técnica denominada espalhamento espectral (*spread spectrum*), que aumenta significativamente a resistência a interferências e *spoofings*, pois este para ser efetivo terá que se espalhar por uma banda de frequências muito larga. De qualquer maneira o sistema não se torna completamente imune, e a interferência ainda é a maior fraqueza do sistema, sobretudo num teatro de operações (MONTEIRO, 2007).

Os ataques *spoofings* podem ser detectados em muitos casos quando não há supressão do sinal de satélite, principalmente se houver aumento repentino de potência recebida pelo receptor dentro de um curto intervalo de tempo, ou uma quantidade de potência maior recebida de uma só direção (WU *et al.*, 2020).

Como mencionado no capítulo anterior, é simulada a estratégia *meaconing* (*replay spoofing attack – RSA*) onde o atacante replica vários sinais originais de satélites para o receptor vítima. Por estar replicando sinais de vários satélites e somando-os, a magnitude de seu sinal é razoavelmente maior que a amplitude de cada onda original dos satélites. Logo, o intuito neste capítulo é saber de que direção (azimute e elevação) um sinal de magnitude maior que os demais é proveniente.

Foi aplicada e simulada em Matlab a técnica de DOA, em um momento utilizando o algoritmo *Conventional beamforming* (CBF) e em outro momento utilizando o algoritmo Capon. O método CBF varre o feixe para avaliar a potência recebida de cada direção e encontrar o sinal direção de chegada de máximo no receptor, que é justamente o *spoofing*. O método Capon utiliza uma matriz de covariância baseada nas amostras do sinal recebido para calcular os coeficientes de um filtro adaptativo. Esses coeficientes são determinados de forma a minimizar a potência do sinal de interferência e maximizar a relação sinal-ruído na direção desejada. Ao ajustar os coeficientes do filtro adaptativo, o método Capon é capaz de suprimir interferências provenientes de outras direções, fornecendo uma estimativa precisa da direção de chegada do sinal desejado (GERSHMAN, 2006). A Figura 3.1 ilustra como funciona de forma resumida o método de DOA.

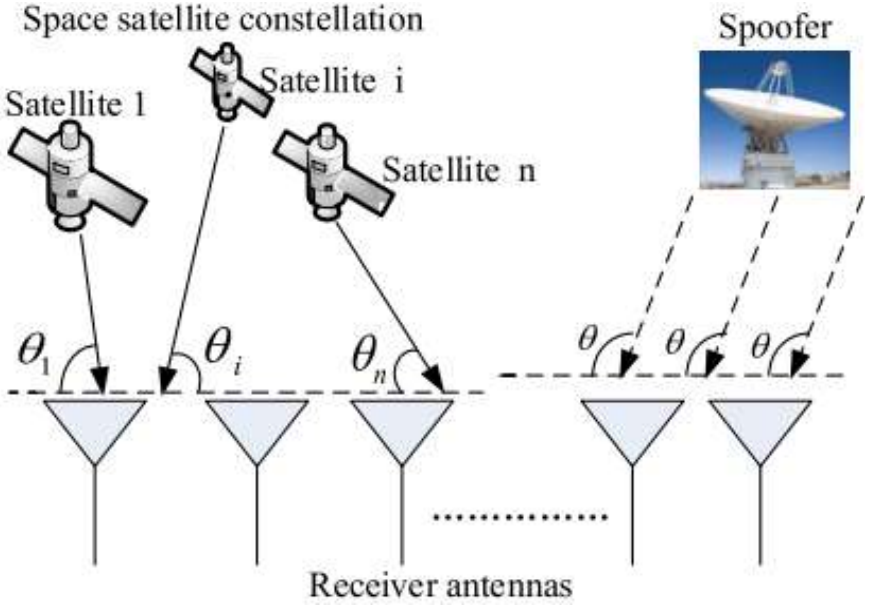

Figura 3.1 Método da Direção de Chegada (DOA) (WU *et al.*, 2020).

3.1 Estimação da Direção de Chegada (DOA)

Neste capítulo, são apresentados os dois algoritmos de estimativa DOA utilizados na simulação em Matlab e os resultados de tal abordagem com relação ao poder dos sinais *spoofing*.

3.1.1 Estimador DOA Conventional Beamformer (CBF)

Um método clássico de localização de direção é o chamado *conventional beamformer* (CBF) que varre o feixe para avaliar a potência recebida em cada direção e encontrar a máxima da direção de chegada na saída de correlação (TREES, 2002)

$$\begin{aligned} V_{CBF}(\varphi, \vartheta) &= E[|\tilde{\mathbf{a}}^H(\varphi, \vartheta)\mathbf{y}[k]|^2] \\ &= \tilde{\mathbf{a}}^H(\varphi, \vartheta)E[\mathbf{y}[k]\mathbf{y}^H[k]]\tilde{\mathbf{a}}(\varphi, \vartheta) \\ &= \tilde{\mathbf{a}}^H(\varphi, \vartheta)\mathbf{R}_{yy}\tilde{\mathbf{a}}(\varphi, \vartheta)\,. \end{aligned} \tag{3.1}$$

Utilizando uma estimativa na matriz de covariância, tem-se

$$\hat{\mathbf{R}}_{yy} = \frac{1}{K}\mathbf{Y}\mathbf{Y}^H\,. \tag{3.2}$$

Pode-se calcular a função de custo por

$$V_{CBF}(\varphi, \vartheta) = \tilde{\mathbf{a}}^H(\varphi, \vartheta)\hat{\mathbf{R}}_{yy}\tilde{\mathbf{a}}(\varphi, \vartheta)\,. \tag{3.3}$$

O CBF representa um caso específico do estimador DOA de máxima verossimilhança (ML) no caso de uma fonte única. Isso é particularmente útil para a presente abordagem, pois considera-se que todos os sinais *spoofing* chegarão do mesmo DOA e, portanto, pode ser

considerado como uma fonte de potência acumulada de diferentes sinais de *spoofing*. O CBF é chamado método de estimativa espectral onde uma função de custo ou espectro deve ser avaliada para todos os possíveis ângulos de azimute e elevação e os picos do espectro então indicam os DOA's dos sinais que atingem o receptor. Consideram-se os sinais spoofing para formar uma fonte poderosa, enquanto os sinais originais dos satélites e o ruído são considerados pelo receptor como ruído. Assim, busca-se apenas o máximo global de $V_{CBF}(\varphi,\vartheta)$ e os respectivos ângulos de azimute e elevação são os DOA's dos sinais de falsificação. Neste sentido, o CBF pode ser considerado um método de baixa complexidade que tem se mostrado muito robusto para modelar incompatibilidades em caso de a resposta da matriz não ser exatamente conhecida ou, caso ocorram grandes erros de medição no modelo disponível, a resposta da matriz deve ser considerada.

3.1.2 Estimador DOA Capon

O estimador Capon pode ser dado por (TREES, 2002)

$$V_{\text{Capon}}(\varphi,\vartheta) = \frac{1}{\tilde{a}^{H}(\varphi,\vartheta)\,\mathbf{R}_{yy}^{-1}\,\tilde{a}(\varphi,\vartheta)} \quad . \tag{3.4}$$

No caso de uma amostra finita a função custo necessária para calcular pode ser dada por:

$$V_{\text{Capon}}(\varphi,\vartheta) = \frac{1}{\tilde{a}^{H}(\varphi,\vartheta)\,\hat{\mathbf{R}}_{yy}^{-1}\,\tilde{a}(\varphi,\vartheta)} \quad . \tag{3.5}$$

O estimador Capon possui as chamadas propriedades de alta resolução, ou seja, pode resolver várias fontes dentro de uma largura de feixe. Os valores dos picos de Capon são aproximadamente proporcionais à potência do sinal. O estimador Capon DOA também é um método de estimativa espectral. Além disso, também podemos aplicar carregamento diagonal para estabilizar o inverso com coeficiente de carregamento $\mu \in R$. Assim, pode-se escrever a função de custo Capon como

$$V_{\text{Capon}}(\varphi,\vartheta) = \frac{1}{\tilde{a}^{H}(\varphi,\vartheta)\,(\hat{R}yy+\mu I_{M-1})^{-1}\,\tilde{a}(\varphi,\vartheta)} \,. \tag{3.6}$$

3.1.3 Resultados das Simulações

Os métodos DOA CFB e Capon foram simulados da seguinte forma: primeiramente o programa realizou uma varredura grosseira a fim de encontrar um valor máximo global correspondendo ao *spoofing*, onde o intervalo espacial da varredura era de 1º. Posteriormente, considerando uma faixa em torno do máximo global, um ajuste fino foi incrementado para se encontrar um máximo mais acurado, considerando nessa etapa uma varredura de 0,01º dentro da tal faixa. O valor baixo de 0,01º (resolução ótima) é de tamanha importância para se evitar erros de discretização, principalmente ao se analisar as Figuras de 3.10 a 3.13. Assim, obtiveram-se as Figuras 3.2 a 3.9. Os gráficos abordados são apresentados com magnitude normalizada, pois não há interesse nos valores das funções de custo de forma absoluta, apenas se necessita apreciar o formato das mesmas para análise dos pontos de máxima. E se trabalhados de forma absoluta, poder-se-ia ter gráficos com dimensões muito exageradas em apenas um dos eixos, o que dificultaria sua visualização.

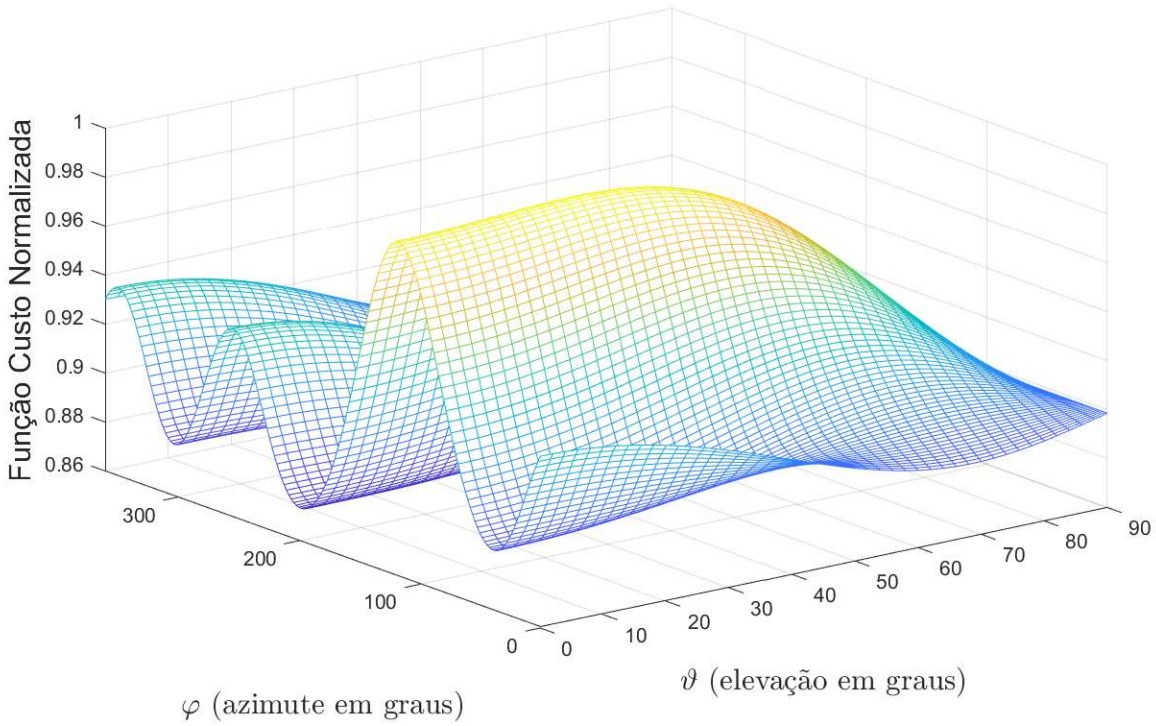

Figura 3.2 Função Custo do método CBF em 3D.

A partir da Figura 3.2, é constatado que existe uma magnitude maior proveniente de uma certa direção (azimute e elevação). Ela é vista de forma mais saliente com a coloração amarela no gráfico, porém pode ser melhor analisada através dos perfis de azimute e elevação nas Figuras de 4.3 a 4.5.

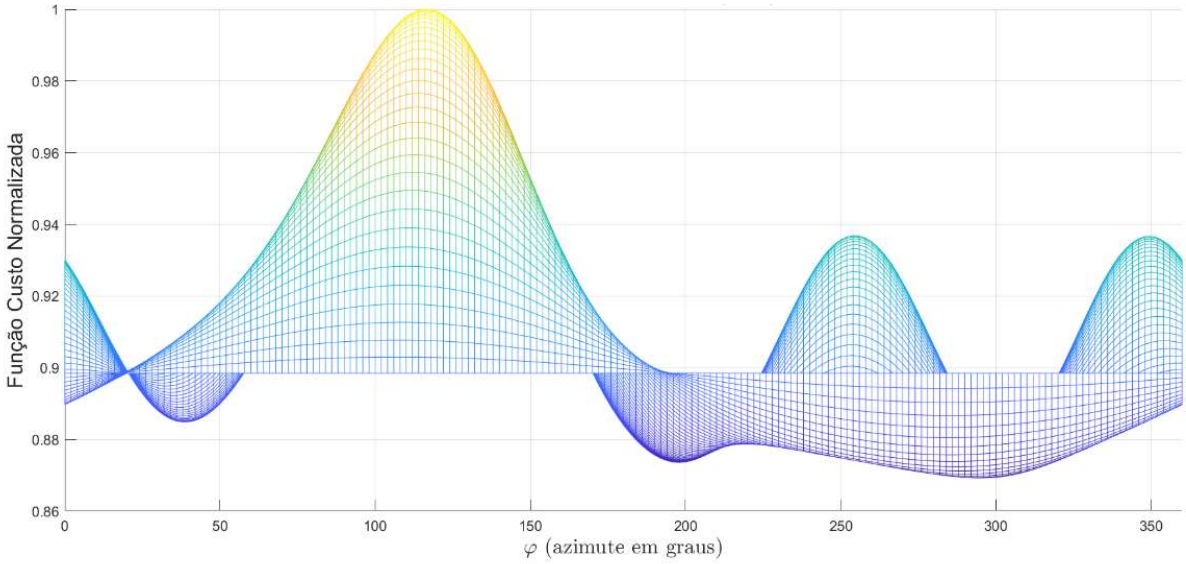

Figura 3.3 Função Custo do método CBF de perfil do azimute.

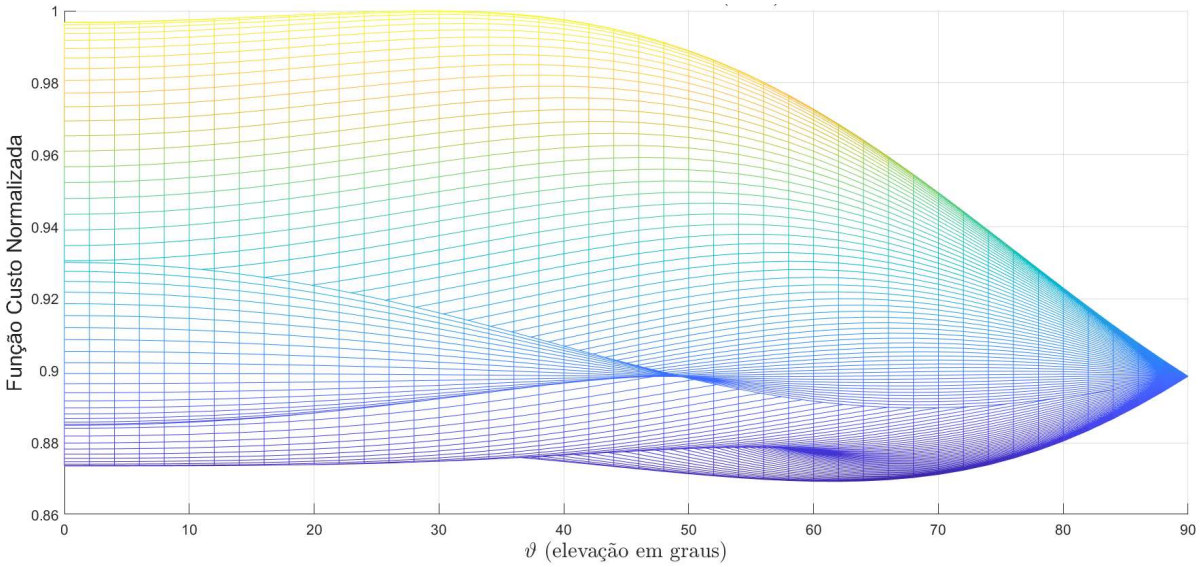

Figura 3.4 Função Custo do método CBF de perfil da elevação.

As Figuras 3.3 e 3.4 possibilitam uma melhor análise da função de custo do estimador CBF e facilmente se observa que os pontos de máximo para azimute e elevação são respectivamente 120º e 25º. Ainda assim, é interessante poder se analisar concomitantemente os máximos de azimute e elevação através da Figura 3.5.

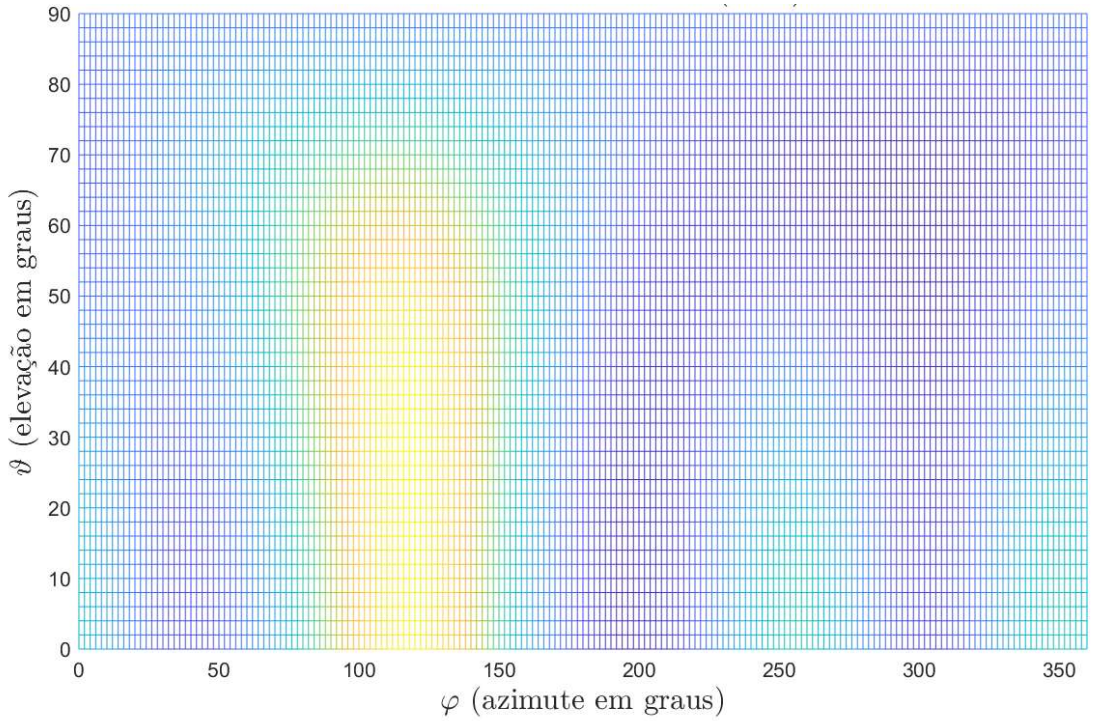

Figura 3.5 Função Custo do método CBF com vista de azimute e elevação.

Da mesma forma como analisados os gráficos para a função de custo do estimador CBF, foram obtidos os mesmos tipos de gráficos para análise com o estimdor Capon, como se vê das Figuras 3.6 a 3.9.

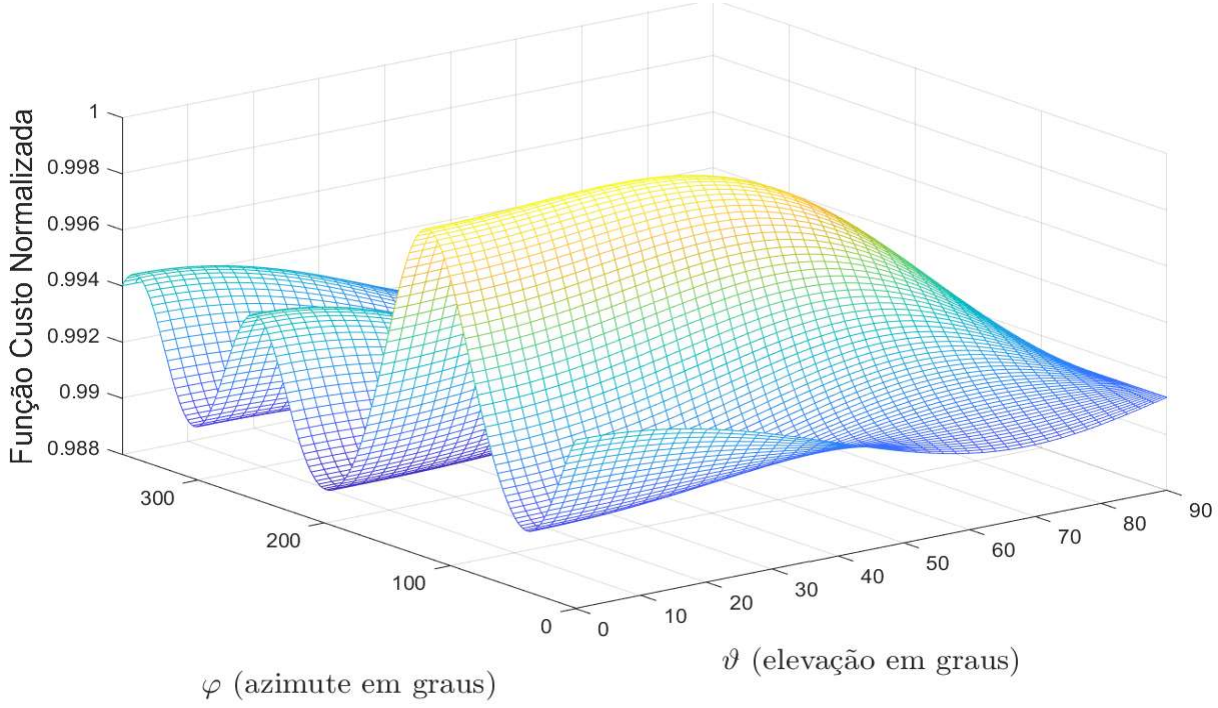

Figura 3.6 Função Custo do método Capon em 3D.

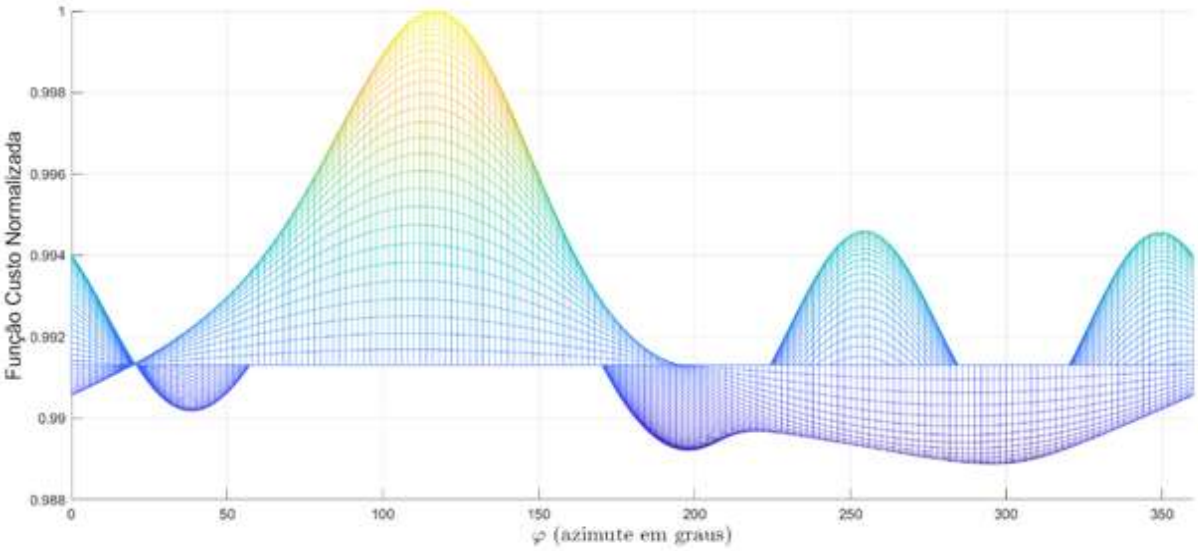

Figura 3.7 Função Custo do método Capon de perfil do azimute.

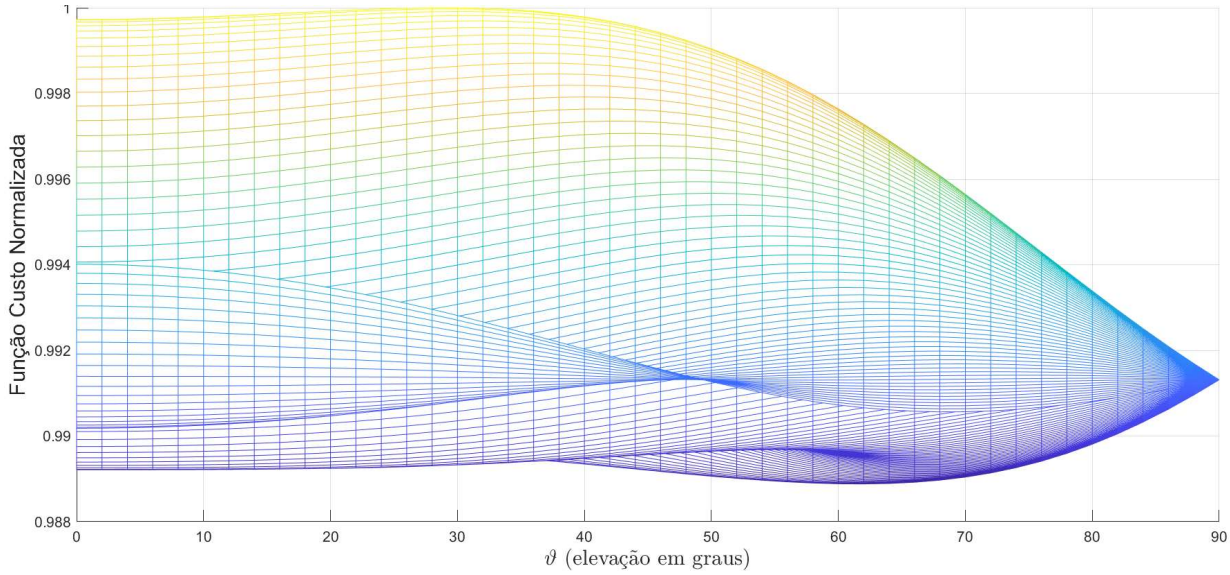

Figura 3.8 Função Custo do método Capon de perfil da elevação.

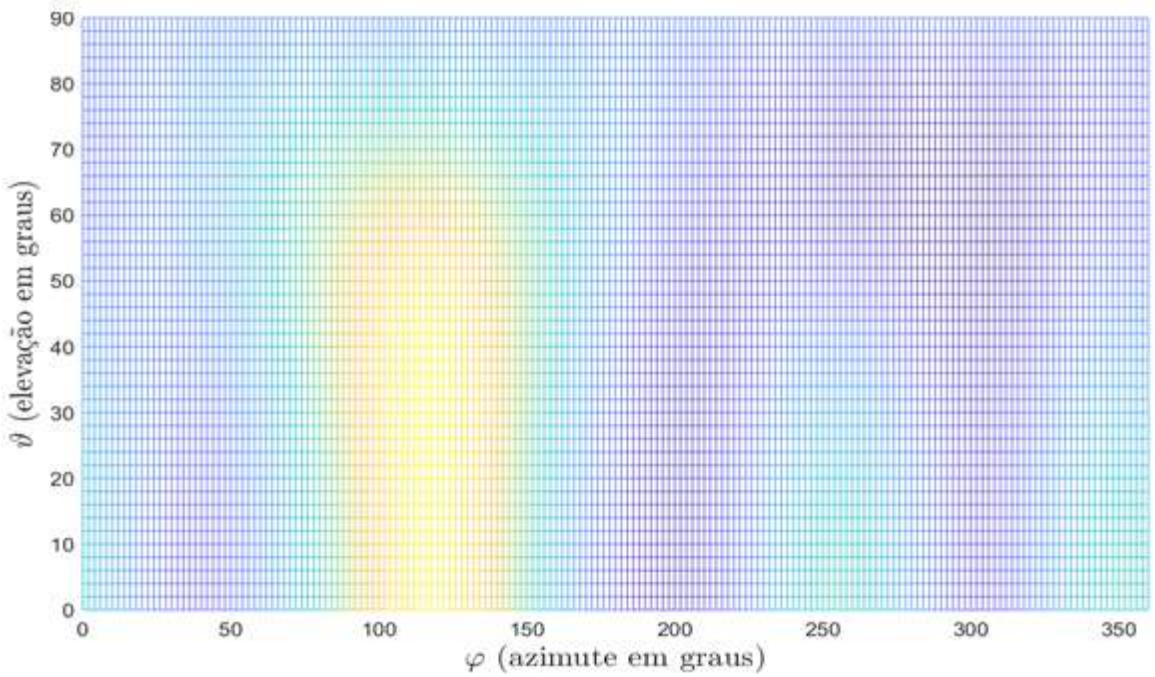

Figura 3.9 Função Custo do método Capon com vista de azimute e elevação.

A partir das Figuras 3.2 a 3.9 pode-se notar que existe um máximo localizado no azimute (120º) e elevação (25º), podendo-se adotar as mesmas considerações tecidas aos gráficos da função de custo do CBF para as figuras da função de custo Capon.

Levando-se em consideração que o sinal que chega no receptor é dotado também de um ruído aleatório, foi realizada uma simulação Monte Carlo com uma frequência de até K = 800 vezes e para se avaliar o erro em azimute e elevação destas estimativas, considerando diferentes níveis de relação *spoofing*-sinal (*spoofing to signal ratio* - SSR) quando utilizados os métodos CBF e Capon.

Os resultados da raiz do erro quadrático médio (*root mean square error* - RMSE) para definir azimute e elevação do *spoofing*, em função do SSR e da frequência gerada nas simulações de Monte Carlo podem ser vistos nas Figuras 3.10 a 3.13. A RMSE é utilizada em virtude das várias simulações de Monte Carlo efetuadas, a fim de se obter justamente uma média dos erros ao tentar encontrar o *spoofing*, considerando todas as simulações, com K variando devido ao ruído aleatório que existe nos sinais.

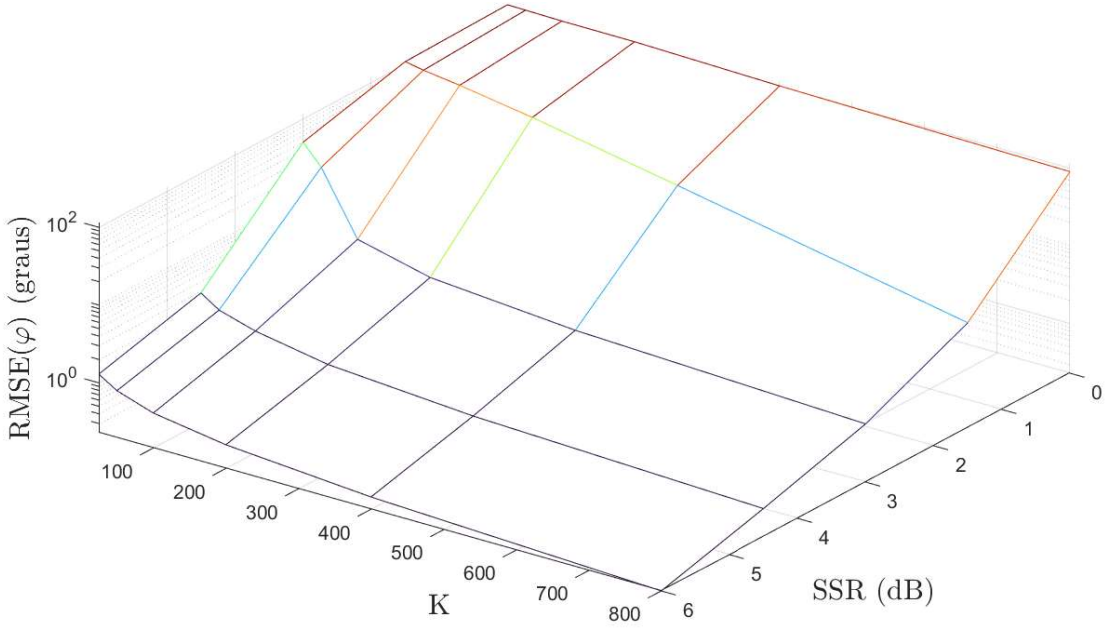

Figura 3.10 RMSE do azimute do spoofing para o método CBF.

Pela figura 3.10 nota-se que, com o estimador CBF, existe um RMSE de aproximadamente 0º para azimute, considerando 800 estimações de K e um SSR de 6 dB, o que representa um erro nulo e um resultado muito bom.

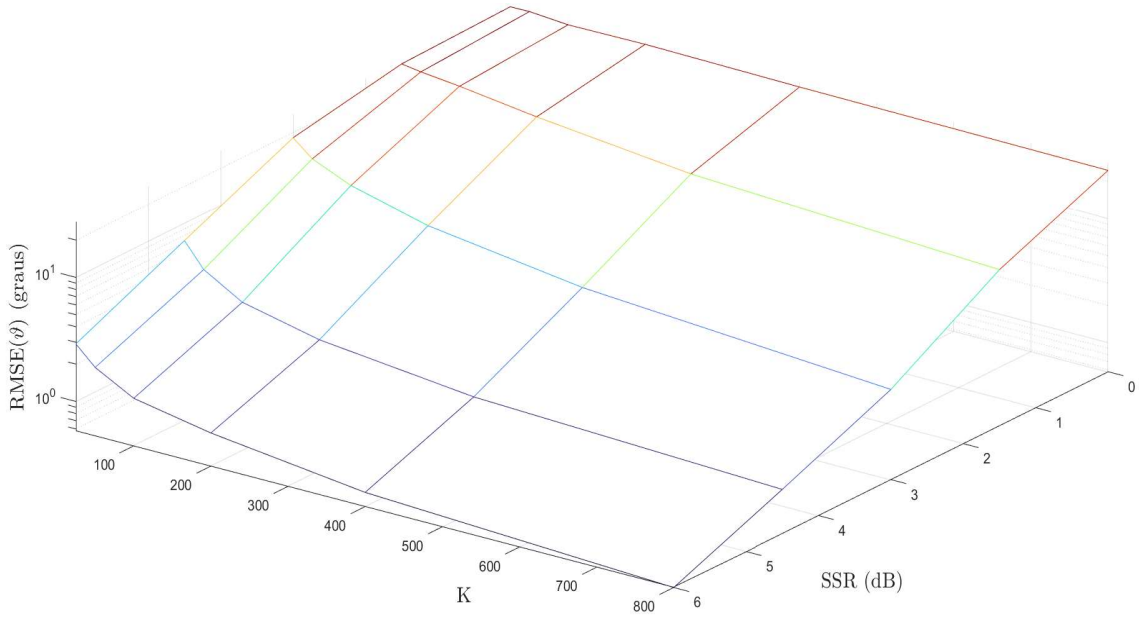

Figura 3.11 RMSE RMSE da elevação do spoofing para o método CBF.

Pela figura 3.11 nota-se que, com o estimador CBF, existe um RMSE de aproximadamente 0,5º para elevação, considerando 800 estimações de K e um SSR de 6 dB, o que representa um erro nulo e um resultado muito bom.

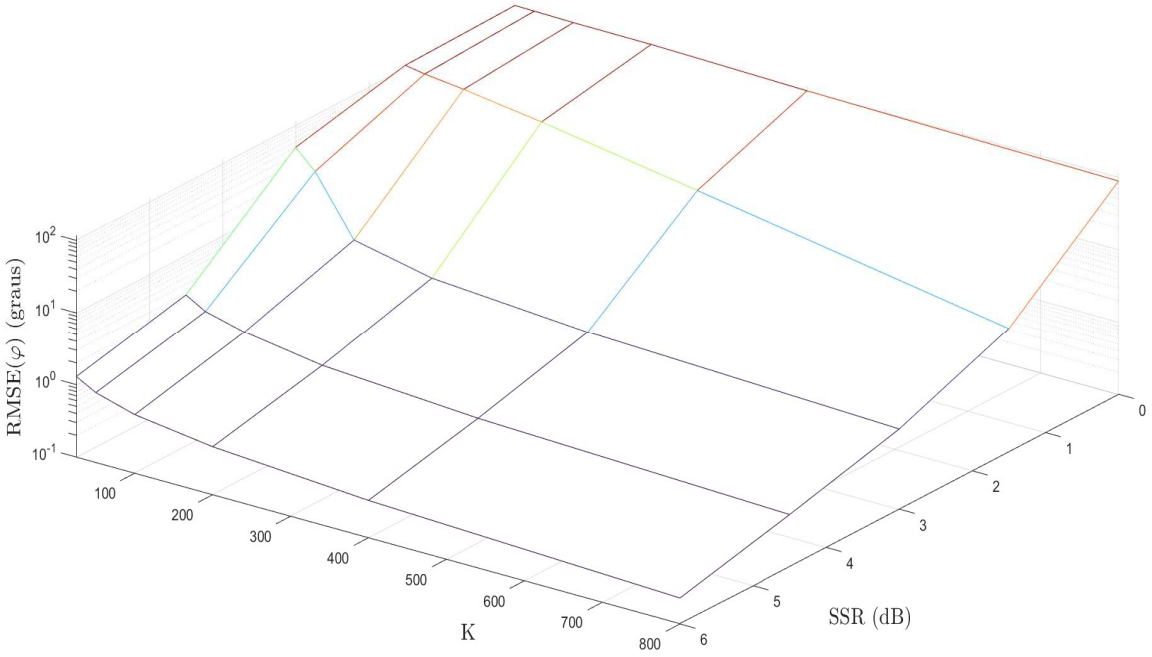

Figura 3.12 RMSE do azimute do spoofing para o método Capon.

Pela figura 3.12 nota-se que, com o estimador Capon, existe um RMSE de aproximadamente 0,5º para azimute, considerando 800 estimações de K e um SSR de 6 dB, o que representa um erro nulo e um resultado muito bom.

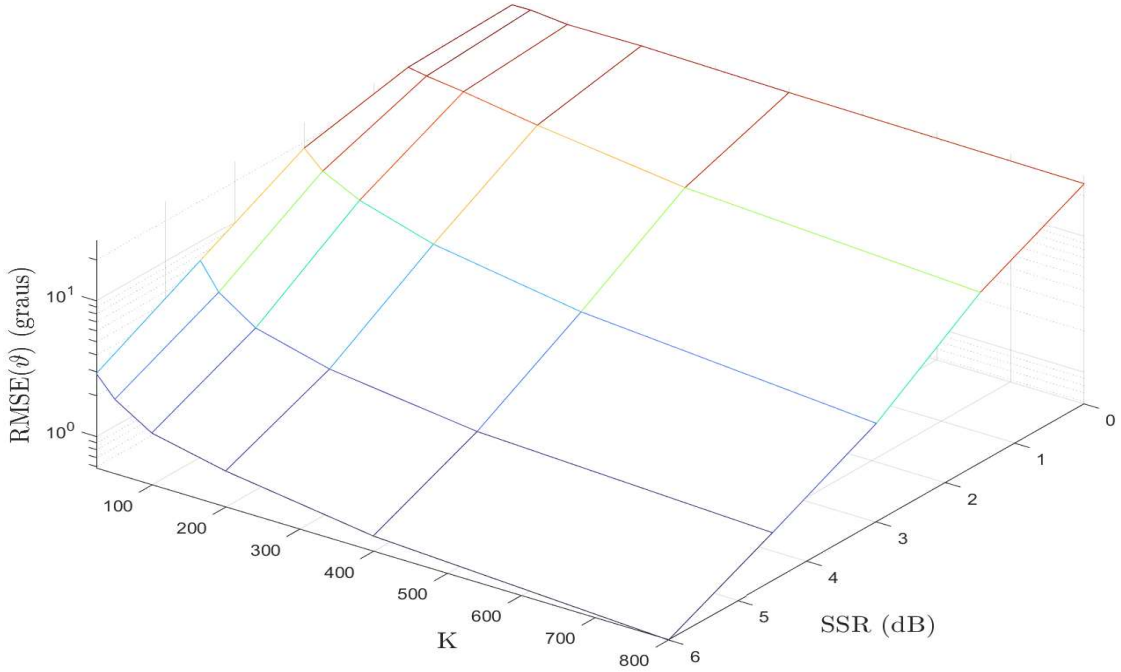

Figura 3.13 RMSE da elevação do spoofing para o método Capon.

Pela figura 3.13 nota-se que, com o estimador Capon, existe um RMSE de aproximadamente 0,5º para elevação, considerando 800 estimações de K e um SSR de 6 dB, o que representa um erro nulo e um resultado muito bom.

Ao analisar os gráficos das Figuras 3.10 a 3.13 percebe-se que realmente quanto maior o valor de SSR, menor tende a ser o erro para o azimute e elevação encontrados. Isso ocorre porque quando se tem um *spoofing* maior em comparação ao sinal original, torna-se mais fácil a percepção do *spoofing*. Ressalta-se que embora isso represente uma facilidade para a vítima em detectar o *spoofing*, quanto maior o *spoofing*, maior é o poder que o atacante tem para conseguir "sequestrar" o sinal original. Observação: O atacante deve também ter o cuidado de não elevar muito a potência para que o ataque não passe a ser um *jamming,* com a vítima percebendo mais facilmente que está sofrendo um ataque (SYAM, 2022).

Os estimadores DOA CBF e Capon alcançam resultados muito semelhantes para o caso em tela. O estimador DOA Capon é considerado um método de alta resolução e tem, no caso de várias frentes de onda correlacionadas estarem presentes, melhores capacidades de resolução do que o CBF. No entanto, para o presente trabalho está sendo considerado que todos os sinais *spoofing* estão chegando da mesma direção e que os sinais de satélite são praticamente descorrelacionados com os sinais *spoofing*. Assim, o CBF é preferido por ser menos complexo, já que nenhuma inversão de matriz precisa ser executada.

4 Mitigação do Spoofing na Operação do GPS

Da mesma forma que têm sido desenvolvidos equipamentos para impedir a utilização do GPS num teatro de operações, os estadunidenses têm desenvolvido medidas para lidar com essa ameaça. São conhecidas duas formas em geral que permitem aumentar muito significativamente a resistência aos ataques em GPS: utilização de antenas especiais (CRPA) que rejeitam os sinais de *jamming/spoofings* e emprego de filtros espaciais nos receptores GPS, tanto militares como civis.

As antenas usadas para mitigar o *jamming* e *spoofing* têm a capacidade de reduzir o ganho na direção desses emissores atacantes, sendo bastante eficazes perante ataques de pontos fixos. Estas antenas são adequadas para aviões e navios, mas não para projéteis, onde é mais aconselhável usar filtros.

No tocante a estes, existem vários tipos de filtros para rejeitar sinais indesejados de *jamming/spoofings* (filtros de frequência, filtros temporais e filtros espaciais), mas os mais usados nos projéteis são os filtros temporais. Estes filtros manipulam as características do sinal no domínio do tempo, conseguindo rejeitar sinais de banda estreita e, mesmo, sinais ágeis em frequência. Este método permite rejeitar parcialmente sinais de *jammings/spoofing* na mesma frequência do GPS, considerando converter os sinais para o domínio do tempo e trabalhar nesse domínio (MONTEIRO, 2007).

Em se tratando dos filtros de forma mais detalhada as tecnologias para se contrapor aos *spoofings* (contramedidas *anti-spoofing*) são dividias em (WU *et al.*, 2020).:

- Tecnologia *anti-spoofing* à nível de sinais
- Tecnologia *anti-spoofing* à nível de dados

Na tecnologia *Signal-level anti-spoofing* estão incutidos dois tipos principais de métodos para resistir a *spoofings*. O primeiro consiste em adicionar recursos de hardware, como arranjos de antenas, multicorrelacionador, sensores de interferência *anti-spoofing* para análise de ângulo de chegada, o que é considerado por (APPEL *et al.*, 2018) como uma medida avançada de proteção.

O segundo consiste em identificar e descobrir o sinal de *spoofing*, bem como seus parâmetros, como a potência do sinal e a relação portadora-ruído do sinal recebido, entre outros. Para cada um desses métodos existem diversas tecnologias que podem ser implementadas.

Na tecnologia *Data-level anti-spoofing*, os dois tipos principais para se contrapor ao *spoofing* são a tecnologia *non-navigation message encryption* (NON-NMET) e a tecnologia *navigation message encryption* (NMET). No tipo NMET, o satélite gera instruções de autenticação por meio de um algoritmo de criptografia. O receptor decriptografa as informações de autenticação usando uma chave. Ao analisar o sinal decriptografado o receptor pode confirmar a autenticidade/integridade da mensagem. Quando as informações de navegação não podem ser autenticadas com sucesso, o receptor pode tratar as informações como informações falsas e excluí-las. Na atualidade, tanto os meios simétricos e assimétricos de criptografia são utilizados para implementação do NMA (*navigation message authentication*). No outro tipo (NON-NMET) não há criptografia. Ainda, para esses dois tipos existem várias tecnologias para mitigar ou coibir os efeitos *spoofings*. A Figura 4.1 detalha um fluxograma com as estratégias, métodos e tecnologias *anti-spoofing* mencionadas em (WU *et al.*, 2020).

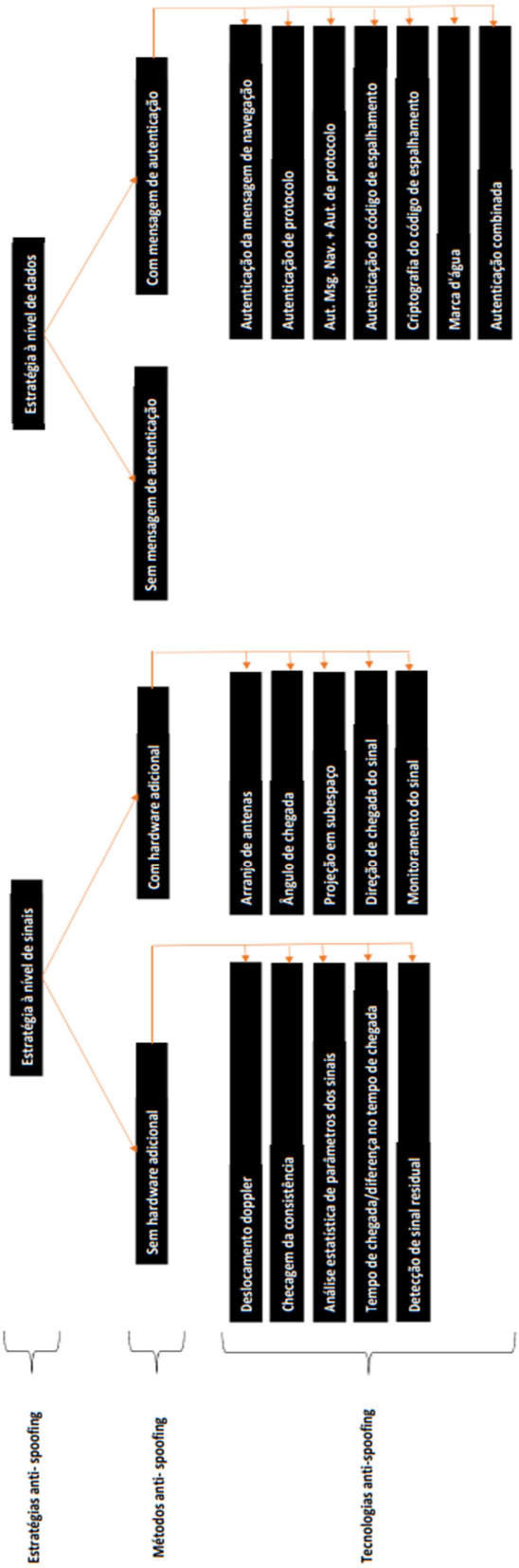

Figura 4.1 Estratégias, Métodos e Tecnologias *anti-spoofing*.

As estratégias, tipos e métodos *anti-spoofings* costumam ser elencadas quanto aos níveis de dificuldade de implementação, grau do efeito na defesa, custo da implementação, e restrições técnicas na implementação (WU *et al.*, 2020).

Segundo (BROUMANDAN *et al.*, 2017), um receptor equipado com um arranjo de antenas pode empregar técnicas de filtragem espacial para moldar seu padrão de feixe de recepção. Esse tipo de receptor pode direcionar um nulo para a fonte de falsificação e suprimir seu efeito destrutivo. A geração de um nulo espacial usando arranjo de antenas é uma das contramedidas mais poderosas contra *spoofings*, além de descartar outros tipos de interferências também (BROUMANDAN *et al.*, 2012). E ainda, John Fischer, diretor técnico da Spectracom, em Rochester, diz que antenas eletricamente direcionáveis são a melhor aposta para combater interferências. Elas também são conhecidas como CRPAs ou antenas “inteligentes”.

Essa técnica se baseia principalmente no fato de que um *spoofer* transmite vários sinais de ruído pseudoaleatório (PRN) de uma mesma antena ou de um mesmo local, enquanto os sinais autênticos do GPS são transmitidos de diferentes satélites e direções diferentes. (DANESHMAND *et al.*, 2017). E ainda, o método de detecção de *spoofing* baseado em arranjos de antenas utiliza técnicas de filtragem espacial para formar um feixe de sinal recebido. Este método fornece um ganho para um ângulo específico e atenua um setor espacial específico. É um método *anti-spoofing* prático e eficaz em cenários de *spoofing* estático e dinâmico. O método é baseado na suposição de que os sinais de *spoofing* que chegam ao arranjo de antenas são todos de uma mesma direção (com amplitudes somadas), mas os sinais de satélite reais que chegam o arranjo de antenas têm características espaciais de diferentes direções.

Para a mitigação dos sinais *spoofing* neste trabalho é introduzido um filtro espacial ou *beamformer* tal que a saída do bloco “processador para mitigação do *spoofing*”, da Figura 2.4, forneça um sinal "limpo" para receptor GNSS padrão de única antena sem quaisquer contramedidas específicas para *spoofing*/falsificação. O beamformer $\mathbf{w} \in \mathbb{C}^{M-1x1}$ irá filtrar o sinal em banda base recebido pelas antenas m = 1, 2, 3, 4, ... M antes da correlação. O sinal de saída do *beamformer* é:

$$\mathbf{z}^{T}[k] = \mathbf{w}^{H}\mathbf{X}[k], \tag{4.1}$$

Nessa parte será utilizado o DOA estimado dos sinais de falsificação para mitigá-los espacialmente e serão configuradas restrições para o padrão de feixe do *beamformer* para amplificar os sinais de satélite para processamento a posteriori. Tentar-se-á alcançar uma resposta desejada sobre uma região específica definida por ângulos de azimute φ e elevação ϑ. A matriz de covariância de uma fonte distribuída pode ser dada como

$$\mathbf{Q} = \int_{\varphi_l}^{\varphi_u} \int_{\vartheta_l}^{\vartheta_u} \tilde{\mathbf{a}}(\varphi,\vartheta)\tilde{\mathbf{a}}^H(\varphi,\vartheta)\mathrm{d}\varphi\mathrm{d}\vartheta \in \mathbb{C}^{M\,x\,M} \tag{4.2}$$

onde o limite superior para os ângulos de azimute e elevação é dado por φ_u e ϑ_u e os respectivos limites inferiores são dados por φ_l e ϑ_l. Usando a matriz Q pode-se direcionar a potência máxima do beamformer para a região definida ao se resolver o problema

$$\max_{\mathbf{w}} \mathbf{w}^H \mathbf{Q}\mathbf{w} \tag{4.3}$$

sujeito a

$$\left|\left|\mathbf{w}\right|\right|_2^2 = 1\ . \tag{4.4}$$

Além disso, deseja-se anular (suprimir) os sinais *spoofing*. Assim, pode-se introduzir a restrição linear adicional

$$\mathbf{w}^H\tilde{\mathbf{a}}(\varphi_s,\vartheta_s) = 0 \tag{4.5}$$

onde φ_s e ϑ_s são o azimute e o ângulo de elevação dos sinais *spoofing*. Assume-se que todos os sinais *spoofing* chegam de um mesmo DOA. O problema dado em (5.3), (5.4) e (5.5) pode ser resolvido por um problema de autovalor incluindo uma restrição nula linear. Para resolver o problema de maximização (5.3) sujeito a (5.4) pode-se usar a técnica de multiplicadores de Lagrange. Então, obtém-se a função lagrangiana correspondente

$$\mathcal{L}(\lambda, \mathbf{w}) = \mathbf{w}^H\mathbf{Q}\mathbf{w} - \varrho(\mathbf{w}^H\mathbf{w} - 1) - \varrho^*(\mathbf{w}^H\mathbf{w} - 1) \tag{4.6}$$

com o multiplicador de Lagrange $\varrho \in \mathbb{C}$. Agora pode-se resolver o problema duplo

$$\max_{\varrho}\max_{\mathbf{w}}\ \mathcal{L}(\varrho,\mathbf{w})\ . \tag{4.7}$$

Primeiro toma-se a derivada com relação a $\mathbf{w}^*$

$$\frac{\partial\mathcal{L}(\varrho,\mathbf{w})}{\partial\mathbf{w}^*} = \mathbf{Q}\mathbf{w} - \varrho\mathbf{w} - \varrho^*\mathbf{w} = 0 \tag{4.8}$$

e assim tem-se

$$\mathbf{Q}\mathbf{w} = 2\mathrm{Re}\{\varrho\}\mathbf{w} = \lambda\mathbf{w}\ . \tag{4.9}$$

Este é um problema de autovalor e, portanto, o $w^\star$ que maximiza (5.3) sujeito a (5.4) é dado pelo autovetor $u^\star$ relacionado com o autovalor dominante $\lambda^\star$ da autodecomposição

$$\mathbf{Q} = \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^H\ . \tag{4.10}$$

Onde $\boldsymbol{\Lambda} = \mathrm{diag}\{[\lambda_1,\lambda_2,...,\lambda_M]^T\} \in \mathbb{R}^{M\,x\,M}$ contém os autovalores e $\mathbf{U} = [\mathbf{u}_1\mathbf{u}_2\ ...\ \mathbf{u}_M] \in \mathbb{C}^{M\,x\,M}$ é uma matriz unitária contendo os autovetores relatados. Em geral pode-se estabelecer que

$$0 \le \mathbf{w}^H\mathbf{Q}\mathbf{w} \le \lambda^\star \tag{4.11}$$

e

$$(\mathbf{w}^\star)^H\mathbf{Q}\mathbf{w}^\star = \lambda^\star\ . \tag{4.12}$$

De uma forma geral, o problema de autovalor também pode ter uma ou até várias restrições lineares. No caso deste trabalho, introduziu-se a restrição nula (5.5). Então o resultado do problema de autovalor pode ser dado como (GOLUB, 1973)

$$\mathbf{G}^{H}\mathbf{Q}\mathbf{G} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^{H} \tag{4.13}$$

onde a matriz de projeção é

$$\mathbf{G} = \mathbf{I}_{M} - \mathbf{a}(\varphi_s, \vartheta_s)(\mathbf{a}^{H}(\varphi_s, \vartheta_s)\mathbf{a}(\varphi_s, \vartheta_s))^{-1}\mathbf{a}^{H}(\varphi_s, \vartheta_s) \tag{4.14}$$

and $\mathbf{V} = [\mathbf{v}_1, \mathbf{v}_2 \cdots \mathbf{v}_M] \in \mathbb{C}^{M \times M}$ é uma matriz unitária contendo os autovetores relacionados. Aqui, w* que maximiza (5.3) sujeito a (5.4) e (5.5) é equivalente a $\mathbf{G}\mathbf{v}^\star$, onde $\mathbf{v}^\star$ é o autovetor relacionado com o autovalor dominante $\lambda^\star$.

Na prática, é muito útil ampliar o nulo na direção dos sinais *spoofing* tanto quanto possível devido a possíveis erros na estimativa DOA dos sinais *spoofing*. Para ampliar nulos em uma determinada área, pode-se introduzir uma matriz de Toeplitz (TREES, 2002). Fisicamente, a matriz de Toeplitz é aplicada a um sinal de entrada para criar um novo sinal de saída. A matriz é multiplicada pelo vetor do sinal de entrada para produzir o vetor do sinal de saída. Cada elemento do vetor de saída é uma combinação linear dos elementos do vetor de entrada, ponderados pelos elementos correspondentes da matriz de Toeplitz. Esses pesos podem ser projetados de tal forma que amplifiquem ou anulem determinadas partes do sinal dentro de uma determinada área (MOON, 2000). A matriz de Toeplitz pode ser representada pela

$$[\mathbf{T}]_{i,j} = \mathrm{sinc}(|i - j|\alpha) \in \mathbb{R}^{M \times M} \tag{4.15}$$

onde $[\mathbf{T}]_{i,j}$ denota o i, jésimo elemento da matriz $\mathbf{T}$ e $\alpha \in \mathbb{R}$ é um parâmetro de projeto. Assim, o considerado problema de autovalor pode ser dado por

$$(\mathbf{G}^{H}\mathbf{Q}\mathbf{G} \odot \mathbf{T}) = \tilde{\mathbf{V}}\mathbf{\Lambda}\tilde{\mathbf{V}}^{H} \tag{4.16}$$

where $\tilde{\mathbf{V}} = [\tilde{\mathbf{v}}_1\ \tilde{\mathbf{v}}_2\ \ldots\ \tilde{\mathbf{v}}_M] \in \mathbb{C}^{M \times M}$ é uma matriz unitária contendo os autovetores relacionados. Assim, $\mathbf{w}^\star$ que maximiza (5.3) sujeito a (5.4) e (5.5) com ampliação do nulo de acordo com $\mathbf{T}$ é equivalente a $\mathbf{G}\tilde{\mathbf{v}}^\star$, onde $\tilde{\mathbf{v}}^\star$ é o autovetor relacionado ao autovalor dominante $\lambda^\star$. As Figuras de 5.2 a 5.11 mostram que o filtro espacial simulado realmente apresentou bons resultados, incutindo ganhos muito negativos para os sinais com azimute e elevação semelhantes ao azimute e elevação do *spoofing*, incluindo-o também. Para os ângulos da região que define a matriz $\mathbf{Q}$ foram utilizados $\varphi_l = 0°, \varphi_u = 360°$, $\vartheta_l = 20°$ e $\vartheta_u = 70°$. As Figuras de 4.2 a 4.5 mostram a resposta do filtro espacial sem utilizar a matriz de Toeplitz $\mathbf{T}$, onde os triângulos em azul denotam os sinais de satélites. Pode-se notar que o nulo na direção dos sinais *spoofing* com $\varphi_s = 120°$ e $\vartheta_s = 25°$ é muito estreito e um possível erro na estimativa DOA dos sinais spoofing já resultaria em uma atenuação muito menor dos sinais *spoofing*. Além disso, observa-

se que o filtro também cria uma atenuação mais forte para sinais com diferença de 180° no azimute, o que infelizmente atenua fortemente alguns dos sinais do satélite. Aplicando a matriz Toeplitz **T** com $\alpha = 1$ pode-se conseguir ampliar o nulo na direção dos sinais *spoofing* e também suprimir uma forte atenuação para sinais com uma diferença de 180° no azimute. A resposta do filtro espacial incorporando a matriz Toeplitz **T** está representada nas Figuras de 4.6 a 4.9.

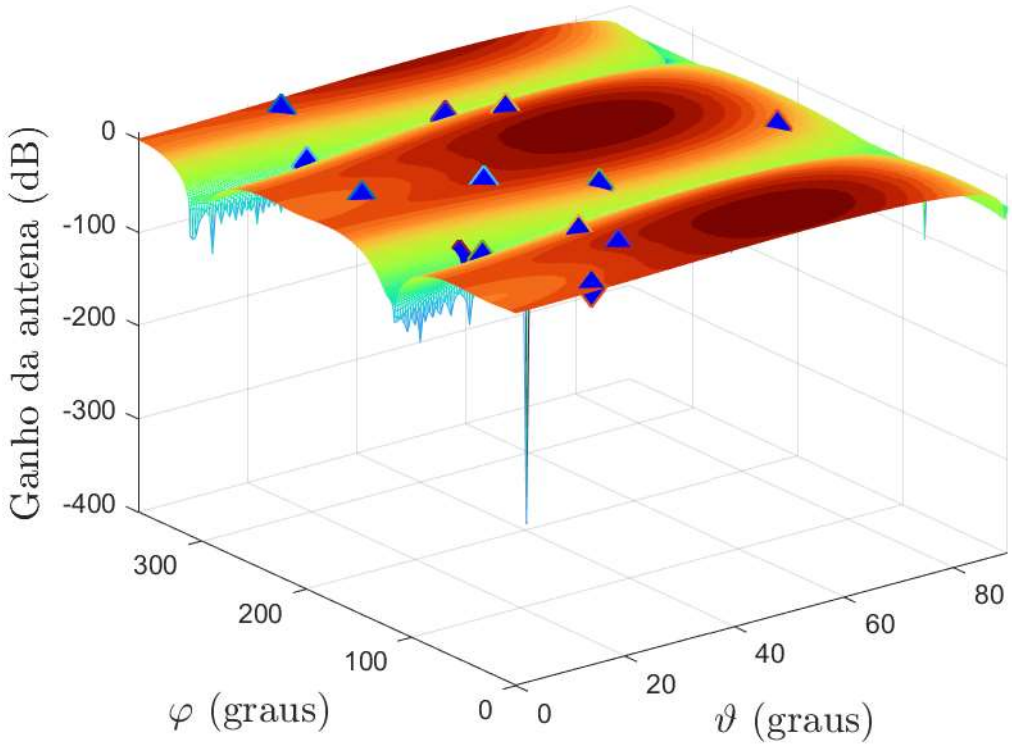

Figura 4.2 Resposta do beamformer sem a matriz de Toeplitz, em 3D.

Nota-se uma atenuação saliente denotada pelas regiões em amarelo e azul. Percebe-se ainda que tal atenuação impacta alguns satélites também. Mas uma análise mais aprimorada pode ser realizada ao se observar tal figura pelos perfis de azimute e elevação, o que é mostrado respectivamente nas Figuras 4.3 e 4.4. Também é interessante analisar a Figura 4.2 em uma vista de cima, resultando na Figura 4.3.

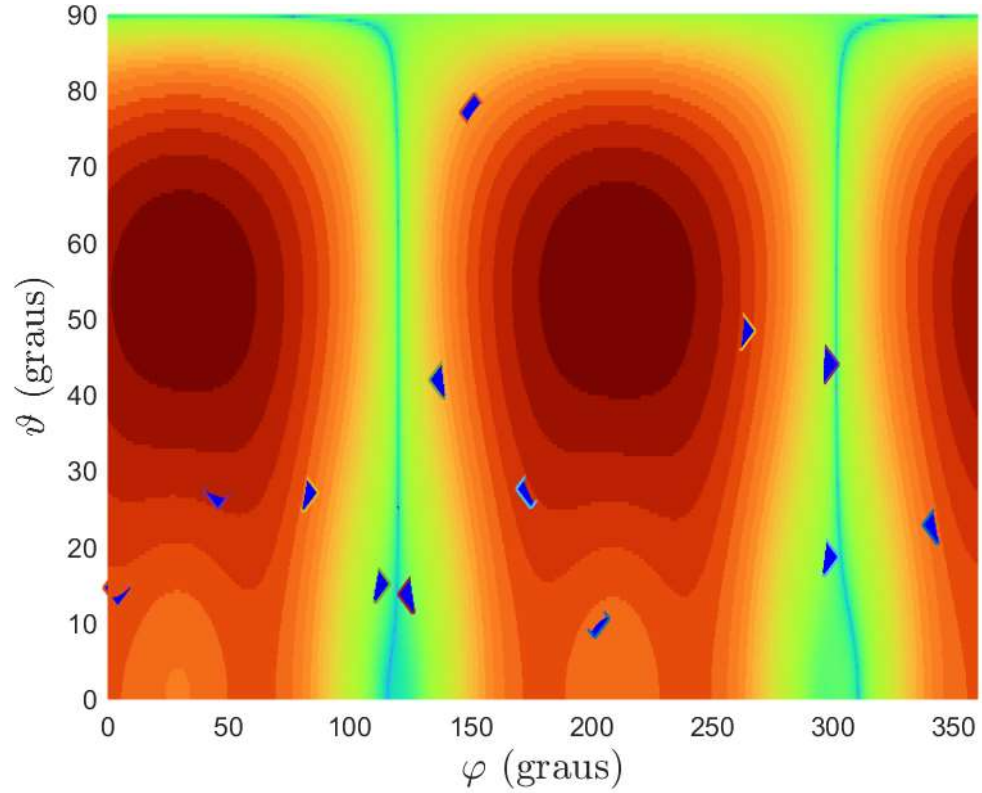

Figura 4.3 Resposta do beamformer sem a matriz de Toeplitz, em vista de azimute e elevação.

A Figura 4.3 mostra claramente que além de atenuado o sinal spoofing azimute 120º elevação de 25º) houve também uma atenuação considerável a 7 satélites, que são alguns triângulos azuis em regiões amarelas e azul.

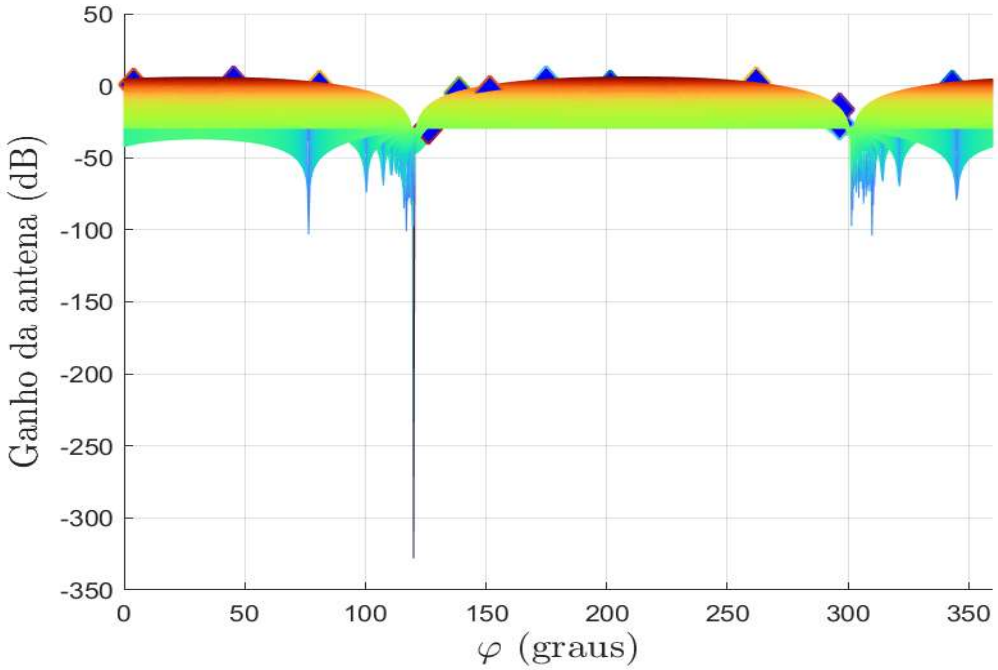

Figura 4.4 Resposta do beamformer sem a matriz de Toeplitz, de perfil do azimute.

Pela Figura 4.4, em perfil de azimute, pode-se perceber, felizmente, a forte atenuação do spoofing, que atinge um ganho de -320 dB, porém existindo outras atenuações indesejáveis.

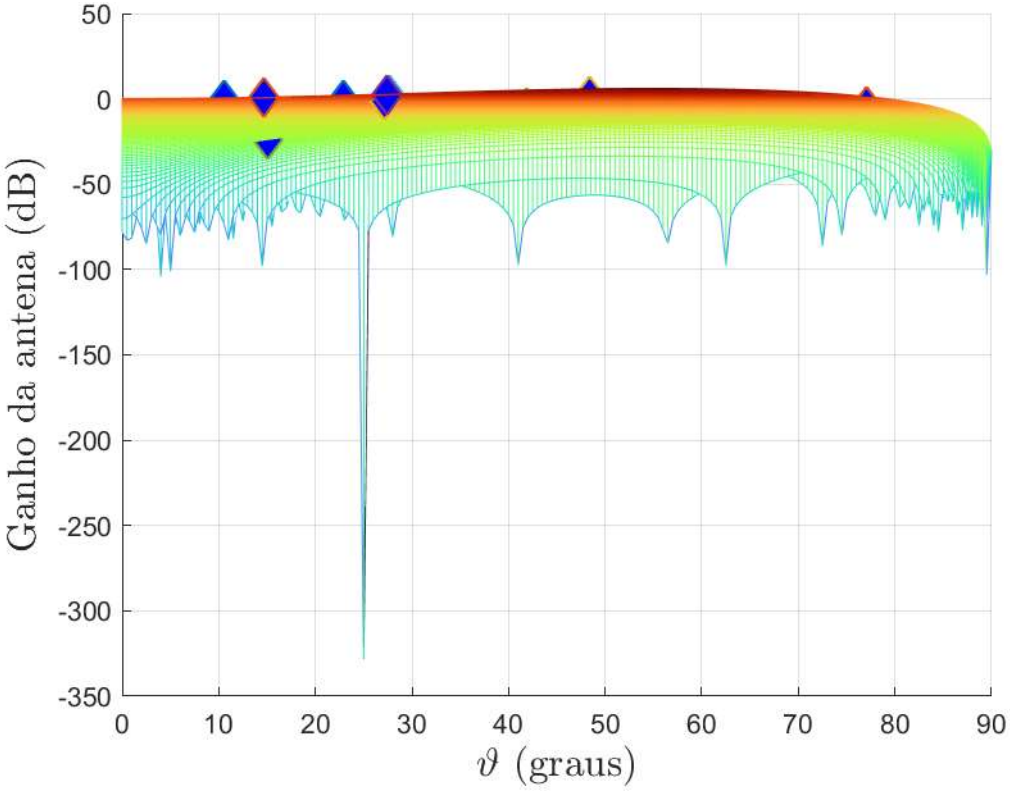

Figura 4.5 Resposta do beamformer sem a matriz de Toeplitz, de perfil da elevação.

Do mesmo modo, mas em perfil de elevação, a Figura 4.5 retrata, felizmente, a forte atenuação do spoofing, que atinge um ganho de -320 dB, porém existindo outras atenuações indesejáveis.

Com as mesmas vistas das Figuras 4.2 a 4.5, são mostradas agora as Figuras de 4.6 a 4.9, onde há uma menor supressão de sinal das áreas em amarelo e azul, a excetuar o próprio sinal spoofing, causada pela técnica com a matriz de Toeplitz implementada.

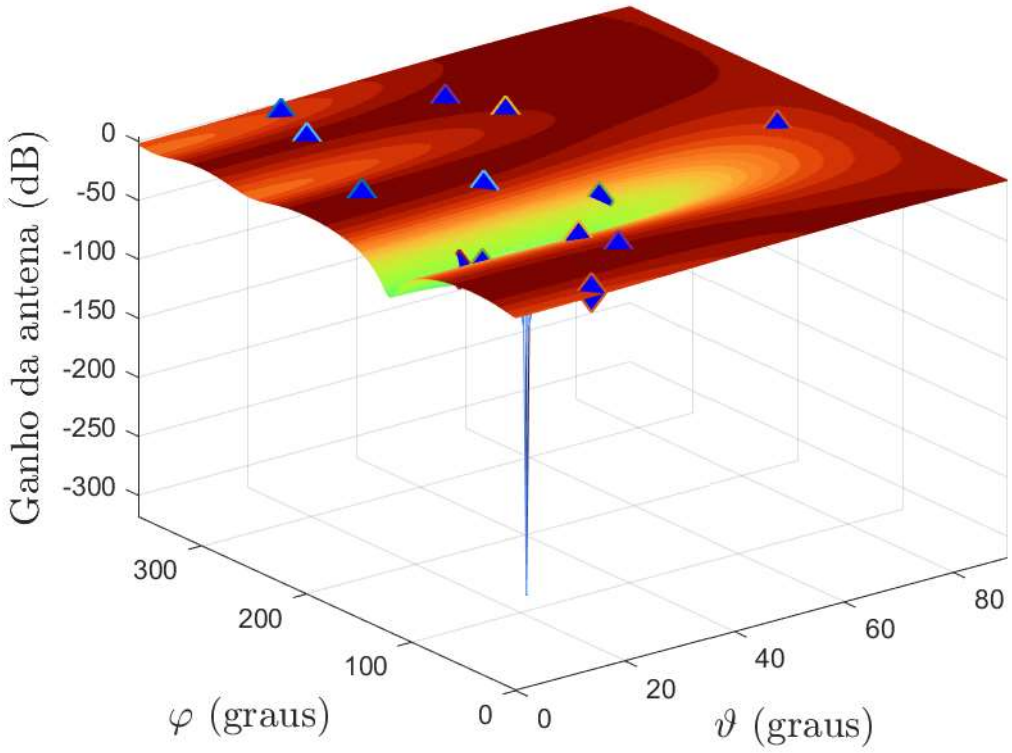

Figura 4.6 Resposta do beamformer com a matriz de Toeplitz, em 3D.

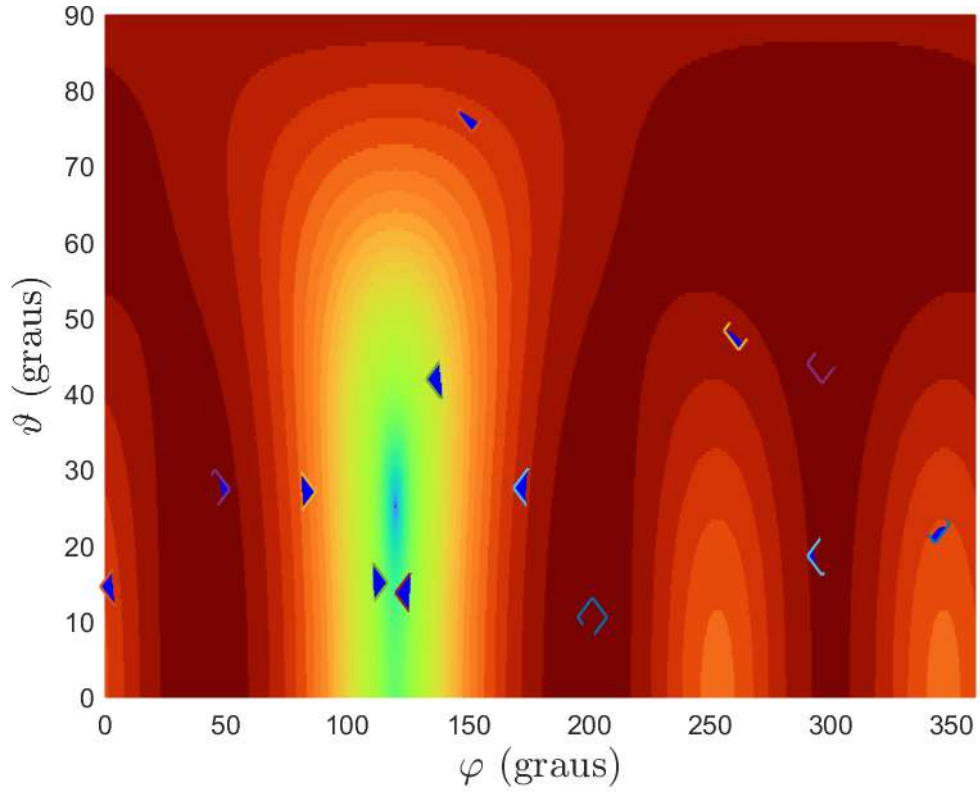

Figura 4.7 Resposta do beamformer com a matriz de Toeplitz, em vista de azimute e elevação.

Olhando pela perspectiva da Figura 4.7, evidenciou-se o sinal spoofing ainda com uma forte atenuação e apenas 4 satélites que ainda continuam de certa forma tendo seus sinais atenuados.

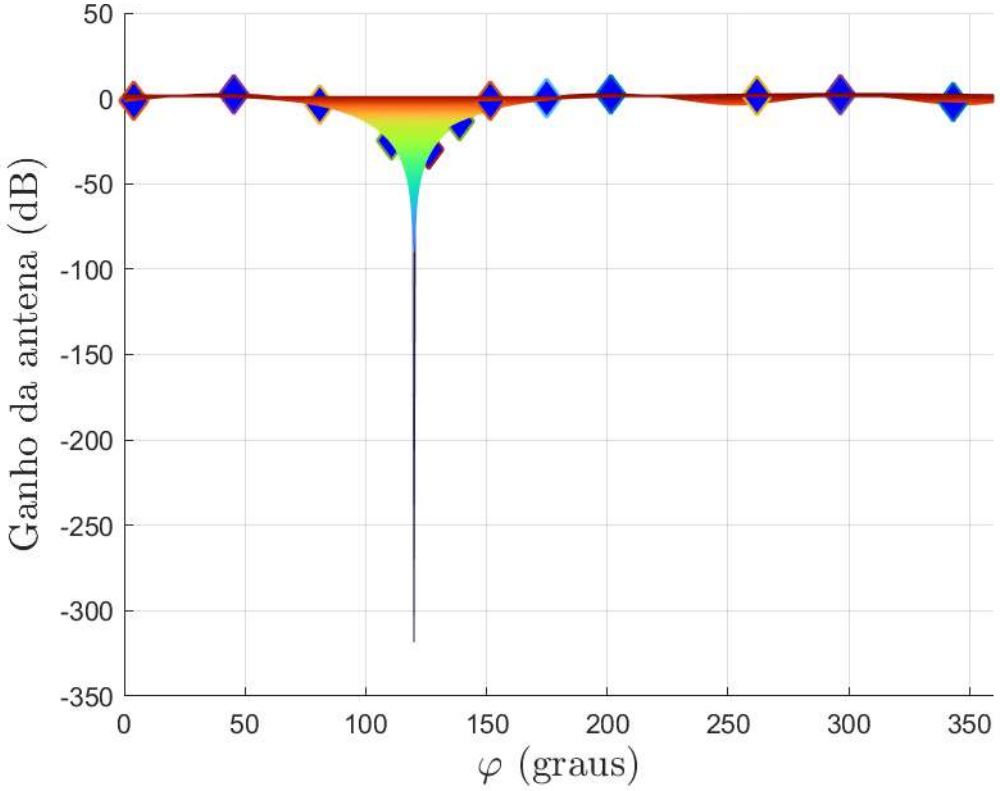

Figura 4.8 Resposta do beamformer com a matriz de Toeplitz, de perfil da azimute.

Pela Figura 4.8, em perfil de azimute, pode-se perceber, felizmente, a forte atenuação do spoofing, que ainda atinge um ganho de -320 dB, e com outras atenuações, dessa vez atingindo apenas 4 sinais de satélites.

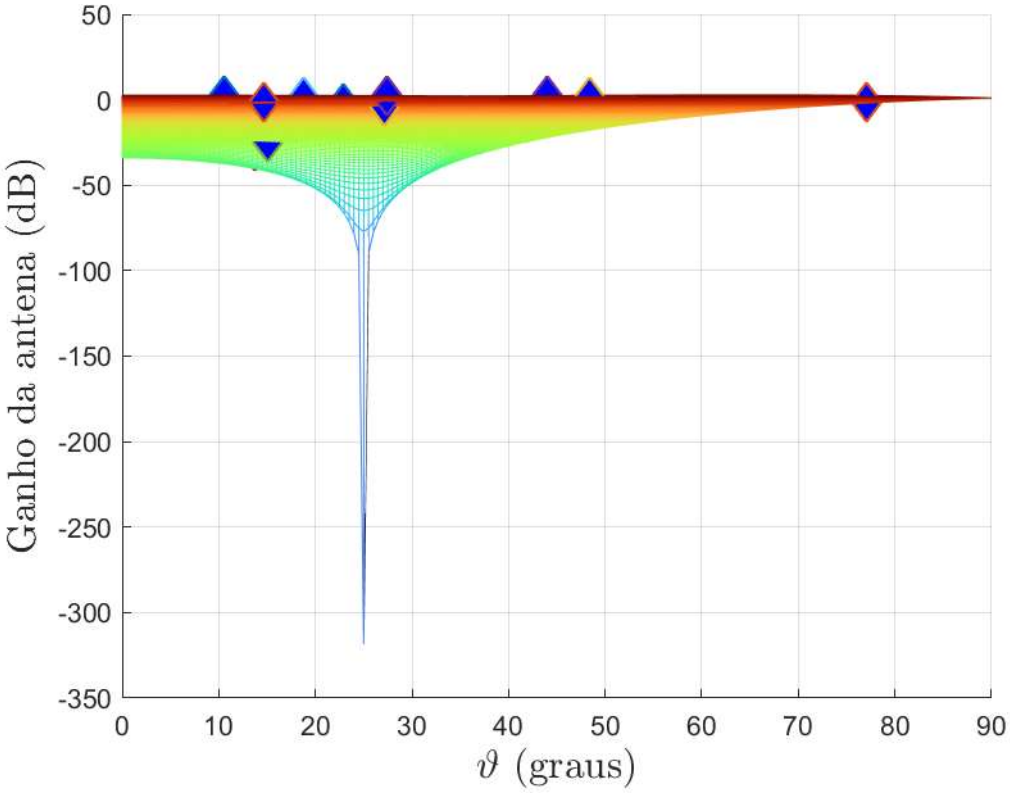

Figura 4.9 Resposta do beamformer com a matriz de Toeplitz, de perfil da elevação.

Pela Figura 4.9, em perfil de elevação, pode-se perceber, felizmente, a forte atenuação do spoofing, que ainda atinge um ganho de -320 dB, e com outras atenuações, dessa vez atingindo apenas 4 sinais de satélites.

As Figuras 4.10 e 4.11 mostram o ganho do arranjo em relação aos diferentes sinais de satélite. Pode-se observar que os sinais dos satélites com PRN25 e PRN23 são fortemente atenuados, pois estão chegando com o DOA próximo ao DOA dos sinais *spoofing*. Muitos dos diferentes PRNs recebem um pequeno ganho ou uma pequena perda tolerável no ganho da matriz, obtendo assim um bom desempenho, considerando que a matriz de antenas possui apenas sete antenas e, portanto, apenas 6 graus de liberdade podem ser usados para moldar a resposta do filtro espacial, além de introduzir o nulo na direção dos sinais de falsificação. O uso da matriz Toeplitz **T** alcança uma mudança significativa no ganho de matriz para os satélites que chegam com uma diferença de 180° no azimute em relação aos sinais de falsificação. Os PRNs 14 e 17 sofrem uma grande perda sem usar a matriz Toeplitz **T** e recebem até mesmo um pequeno ganho de array ao aplicar a matriz Toeplitz **T**.

Em geral, o projeto do filtro tem limitações devido aos graus de liberdade limitados e uma série de sinais que precisam ser amplificados sendo mais que o dobro dos graus de liberdade disponíveis. Assim, o projeto de filtro espacial para tal problema, e mesmo sem

informações sobre os DOA's dos sinais de satélite só pode alcançar ganhos limitados. Observação: Sinais de satélite com atenuação entre 5 a 8 dB começam a entrar numa faixa de não operacionalidade em vista do receptor/usuário.

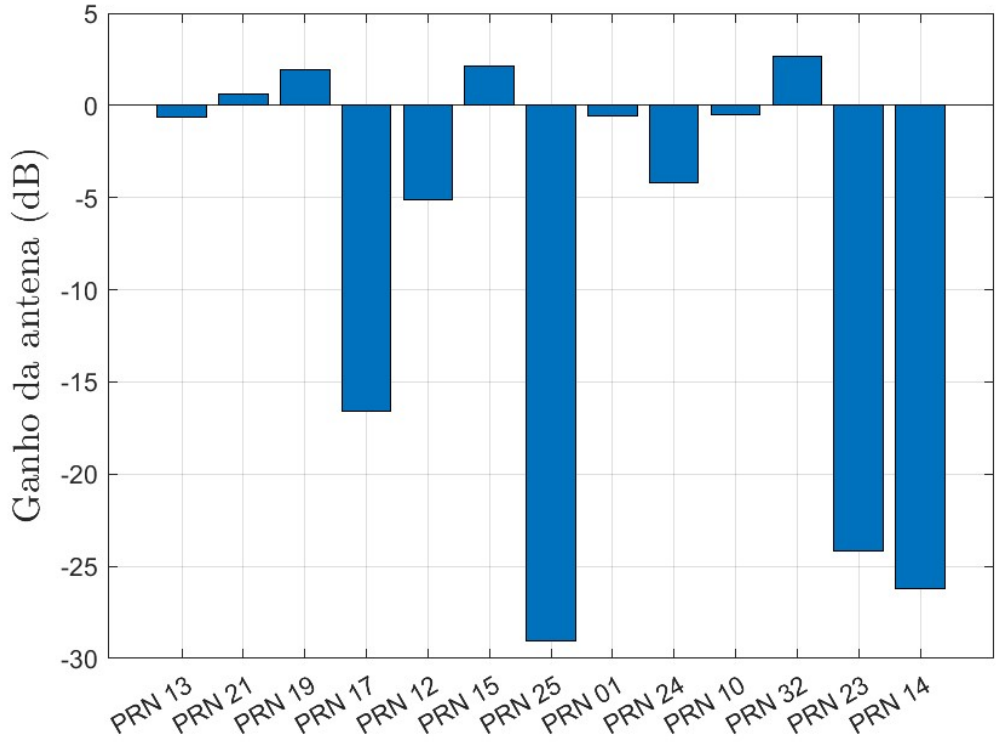

Figura 4.10 Ganho do sinal de cada satélite na recepção, sem a matriz de Toeplitz.

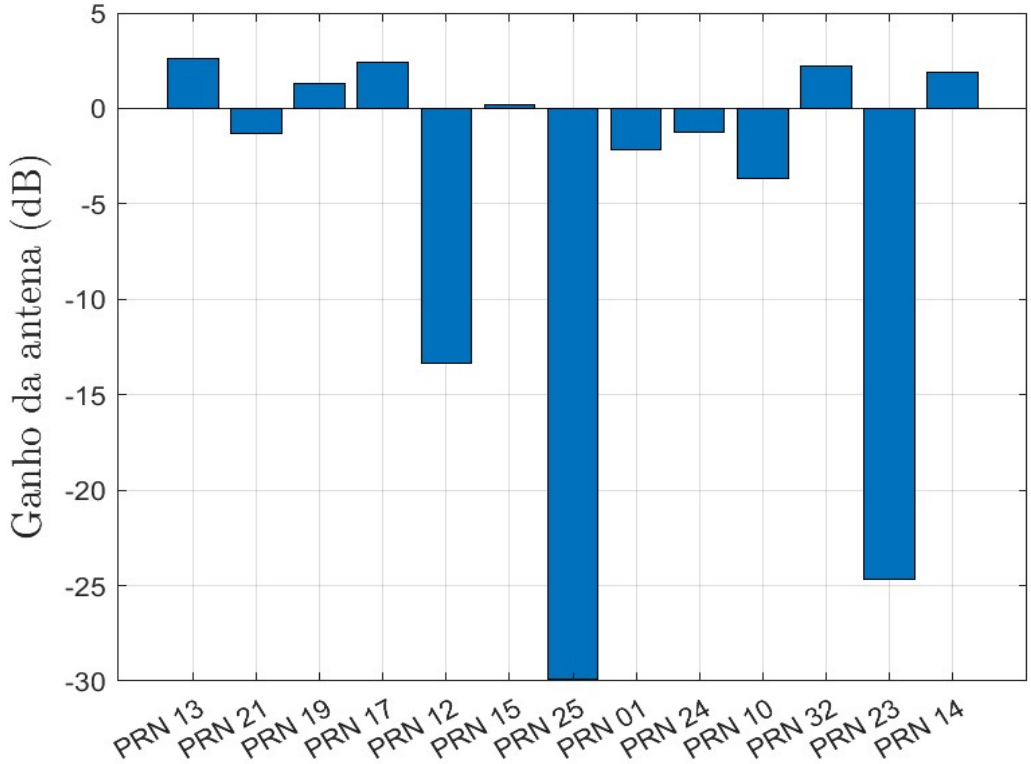

Figura 4.11 Ganho do sinal de cada satélite na recepção, com a matriz de Toeplitz.

5 Conclusão e Considerações Finais

A partir das técnicas apresentadas, o usuário que deseja se contrapor a um ataque *spoofing* deve estimar primeiramente a qual tipo de ameaça ele pode ser submetido (a tecnologia/estratégia empregada nela), para então pensar em uma forma de coibi-la. Deve-se ter em mente as suas restrições operativas bem como as deficiências das técnicas que pretende utilizar. Além disso, cabe realizar uma análise econômica das estratégias, técnicas e tecnologias pretendidas para se opor ao efeito *spoofing* com eficiência, sempre lembrando que tais contraposições podem muitas vezes ser conjuntas ou combinadas.

Este trabalho simulou, através do programa Matlab, a detecção do efeito *spoofing* e a contramedida para mitigação do efeito. Esses processos geraram gráficos que detalham como o processo opera à nível de sinais.

A detecção simulada considerou uma antena de receptor GPS com 7 sensores (1 ao centro e 6 em formato circular) capaz de perceber que havia um sinal de grande magnitude proveniente de uma única direção do espaço, com a utilização da técnica “direção de chegada”, implementada pelos algoritmos CBF (*Conventional beamforming*) e Capon. A partir disso foi evidente que um *spoofer* atuava concentrando a emissão de vários sinais GPS falsificados de um único ponto (azimute e uma elevação) de emissão.

Posteriormente, na mitigação do *spoofing*, um filtro espacial simulado em Matlab operou de forma a reduzir o ganho de quaisquer sinais provenientes de tal direção, remanescendo somente as outras emissões, provenientes dos satélites de GPS. Dessa forma, o usuário pôde usufruir apenas de informações advindas originalmente dos satélites GPS e assume-se que passa a ter a informação correta a respeito de sua localização.

À luz do artigo (WU, 2020), que analisa os métodos de ataque, detecção e mitigação de spoofings com respeito ao nível de dificuldade de implementação, grau de efetividade e custo; pode-se dizer que os métodos envolvidos no presente trabalho apresentam um nível de dificuldade alto de implementação, grau de efetividade alto, e custo médio.

Um usuário portando o conjunto mostrado na Figura 2.4 para servir de exemplo para este trabalho pode ser um automóvel civil ou um veículo de combate, ou mesmo um navio em alto mar, onde não há pontos de referência (principalmente não havendo estrelas em visada), ou mesmo uma aeronave em situação semelhante à do navio, ou mesmo um veículo autônomo que se baseia apenas em sua localização por GNSS, sem se atentar aos aspectos visuais.

Apesar do grande esforço atinente ao desenvolvimento de antenas, filtros e circuitos *anti-jamming/anti-spoofing*, a melhor solução para manter a operacionalidade no ambiente saturado e hostil em um teatro de operações ainda consiste num sistema integrado que combine um receptor GPS e um sistema de navegação inercial. A combinação desses dois sistemas é efetuada de tal forma que quando o GPS puder fornecer informação de confiança, a plataforma utiliza a solução de navegação determinada pelo receptor GPS, e quando este estiver sob ataque, a navegação ficará a cargo do sistema de navegação inercial.

Atentas a essa realidade, as Forças Armadas estadunidenses têm equipado os seus mísseis e projéteis com sistemas integrados (GPS mais sistema inercial de navegação). Por exemplo, os mísseis Tomahawk possuem, além do guiamento por GPS, um sistema inercial complementar. Outros mísseis que ainda não dispõem dessa capacidade serão convertidos (MONTEIRO, 2007). Sugerem-se as leituras de (SILVA, 2020), que aborda a utilização de sistema de navegação inercial em ambientes com interferências e de (GREWAL, 2007) que trata de sistema de navegação inercial.

Como sugestão para trabalhos futuros, em um contexto operacional, sugere-se a implementação de uma doutrina ao usuário do Sistema GPS. Pois além de muitas vezes eficaz e com menos dispêndio financeiro, mais vale se precaver do que remediar as consequências de um ataque *spoofing*. Algumas literaturas indicam práticas a serem efetuadas antes e também durante o teatro de operações, pois coíbem até mesmo o início da correlação do sinal no receptor com um sinal *spoofing* desde que operado o método *anti-spoofing* corretamente pelo usuário do GPS.

Também, ainda em um contexto operacional, é interessante resumir por questões de ergonomia do meio (navios, lanchas, carros de combate, aeronaves, drones, etc.) que tipo de contramedidas de *spoofings* adotar, tendo em vista questões técnicas e econômicas. O trabalho *in locu* utilizou uma contramedida com arranjos de antenas que pode muitas vezes se tornar caro e não exequível para certos usuários como explica (BROUMANDAN, 2014).

Ainda, cabe um estudo mais sofisticado no qual o atacante tenha disponível para si meios em diferentes locais de onde enviar os sinais falsificados de GPS, como cita (TIPPENHAUER *et al.*, 2011), e com magnitude bem inferior ao de um sinal original de GPS. Assim, a dificuldade estaria além de se analisar o limiar entre sinais ou de analisar direção de chegada de sinais para detecção de *spoofing*. Com isso, deve-se adotar procedimentos mais sofisticados explanados por exemplo em (WU *et al.*, 2020). Adicionalmente, cabe também uma etapa mais aprofundada com o receptor e o atacante em situação dinâmica, e com isso algumas

peculiaridades passam a vigorar, como mostra (YUAN, 2018). Cabem também as considerações das correções ionosféricas e troposféricas apresentadas em (SILVA *et al.*, 2021).

Referências

AKOS, D. M. **A Software Radio Approach to Global Navigation Satellite System Receiver Design**. 1997. 140p. Thesis (PhD. in Electrical Engineering and Computer Science) - Ohio University, Ohio, 1997.

APPEL, M.; ILIOPOULOS, A.; FOHLMEISTER,, F.; MARCOS E. P.; CUNTZ, M.; KONOVALTSEV, A.; ANTREICH, F.; MEURER, M. Experimental validation of GNSS repeater detection based on antenna arrays for maritime applications. **CEAS Space Journal**, p. 7-19, 2018.

ASHBY, N.; WEISS, M. A. **Global Positioning System receivers and relativity**. NIST, 1999.

BALANIS, C. A. **Antenna Theory: Analysis and Design.** John Wiley & Sons, 2016.

BROUMANDAN, A.; CURRAN, J. T. GNSS spoofing detection in covered spoofing attack using antenna array. INTERNATIONAL TECHNICAL SYMPOSIUM ON NAVIGATION AND TIMING (ITSNT), 2017. **Proceedings** […]. p. 1-9, 2017.

BROUMANDAN, A.; JAFARNIA-JAHROMI, A.; DEHGHANIAN, V.; NIELSEN, J. GNSS spoofing detection in handheld receivers based on signal spatial correlation. 2012 IEEE/ION POSITION, LOCATION AND NAVIGATION SYMPOSIUM, Myrtle Beach, 2012. **Proceedings** […]. p. 479-487, 2012.

BROUMANDAN, A.; JAFARNIA-JAHROMI, A.; LACHAPELLE, G. Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. **Gps Solutions**, v. 19, n. 3, p. 475-487, 2015.

CAO, J., **Practical gps spoofing attacks on consumer drones**. 2020. 228 p. Thesis (PhD. in Electrical Engineering and Computer Science) - University of Hawai'i at Manoa, 2020.

CASTRO, D. R. S. C., Emprego Militar do Sistema de Posicionamento Global (GPS). **Revista Spectrum**, v. 4, Nov. 2001.

DANESHMAND, S.; JAHROMI, A.; BROUMANDON, A.; LACHAPELLE, G. A low-complexity GPS anti-spoofing method using a multi-antenna array. 25TH INTERNATIONAL TECHNICAL MEETING OF THE SATELLITE DIVISION OF THE INSTITUTE OF NAVIGATION (ION GNSS 2012), 2012. **Proceedings** […]. p. 1233-1243, 2012.

DANESHMAND, S.; JAHROMI, A.; BROUMANDAN, A.; LACHAPELLE, G. A GNSS structural interference mitigation technique using antenna array processing. IEEE SENSOR ARRAY AND MULTICHANNEL SIGNAL PROCESSING WORKSHOP (SAM), 2014, Coruna. **Proceedings** […]. p. 109-112, 2014.

EGEA-ROCA, D., ARIZABALETA-DIEZ, M., PANY, T., ANTREICH, F., LÓPEZ-SALCEDO, J. A., PAONNI, M., & SECO-GRANADOS, G. GNSS user technology: State-of-the-art and future trends. **Future Navigation and Timing Evolved Signals-2**, v. 10, p. 39939-39968, 2022.

EUROPEAN SPACE AGENCY NAVIPEDIA. **GPS Services**. 2020. Disponível em: https://gssc.esa.int/navipedia/index.php/GPS_Services. Acesso em: 05 Ago. 2022.

FARIA, L. A.; ROSO, N. A.; SILVESTRE, C. A. M. Susceptibility of GPS-Dependent Complex Systems to Spoofing. **Journal of Aerospace Technology,** Instituto Tecnológico de Aeronáutica, São José dos Campos, v. 10, 2018.

GABLE, N. **GPS Products**. Baesystems. Disponível em: www.baesystems.com/en-us/product/gps-products. Acesso em: 02 Fev. 2022.

GAO, G. X.; HU, Y., **GNSS spoofing and detection**. John Wiley & Sons, 2014.

GERSHMAN, A. B.; SIDIROPULOS, N. D. Adaptive Arrays. **Signal Processing Magazine**, IEEE, vol. 23, no. 5, pp. 14-35, Sep. 2006

GIOVANINI, A. **UTM Sirgas 2000**. Disponível em: https://adenilsongiovanini.com.br/blog/utm-sirgas-2000-converter-coordenadas/. Acesso em: 04 Jan. 2023.

GOLUB, G. **Some Modified Matrix Eigenvalue Problems**. Society for Industrial and Applied Mathematics, vol. 15, no. 2, 1973.

GOWARD, D. **Ukraine attacks changed russian gps jamming.** GPSWorld, 2022. Disponível em: https://www.gpsworld.com/ukraine-attacks-changed-russian-gps-jamming/. Acesso em: 02 Abr. 2023.

GREWAL, M. S.; WEILL, L. R.; ANDREWS, A. P. **Global positioning systems, inertial navigation, and integration**. John Wiley & Sons, 2007.

HUMPHREYS, T. E. *et al*. "Assessing the spoofing threat: development of a portable gps civilian spoofer." 21ST INTERNATIONAL TECHNICAL MEETING OF THE SATELLITE DIVISION OF THE INSTITUTE OF NAVIGATION (ION GNSS '08), 2008, Savannah. **Proceedings** [...]. pp. 2314–2325, 2008.

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS. **Principais produtos e serviços do INPE**. Disponível em: http://www.inpe.br/faq/index.php?pai=4#:~:text=Uma%20constela%C3%A7%C3%A3o%20de%2024%20sat%C3%A9lites,para%20Sistema%20de%20Posicionamento%20Global. Acesso em: 01 Abr. 2022.

KAPLAN, E. D.; HEGARTY, J. H. **Understanding GPS: Principles and Applications**. 2d Ed, Artech house, 2017.

KYLE, D. W.; GROSS, J. N.; HUMPHREYS, T. E.; AND EVANS, B. L. GNSS Signal Authentication Via Power and Distortion Monitoring. **IEEE Transactions on Aerospace and Electronic Systems**, p. 739-754, 2018.

KYLE, D. W.; HUMPHREYS, T. E.; BHATTI, J. A.; PSIAKI, M. L.; O'HANLON, B. W.; POWELL, S. P.; Schofield A. GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase. 27TH INTERNATIONAL TECHNICAL MEETING OF THE SATELLITE DIVISION OF THE INSTITUTE OF NAVIGATION (ION GNSS+ 2014), **Proceedings** […]. 2014, p. 2776-2800.

LI, P. *et al*. High dynamic signal pulling with biased Doppler aiding from INS. INTERNATIONAL CONFERENCE ON ELECTRICAL AND CONTROL ENGINEERING, **Proceedings** […]. p. 676-679, 2011.

MAPPA. **Sirgas 2000 e WGS84. 2023**. Disponível em: https://mappa.ag/blog/sirgas-2000-e-wgs84-o-que-sao/. Acesso em: 04 Mai. 2023.

MERWE, J. R.; ZUBIZARRETA, X., Lukcin I.; Rugamer A. and Fraunhofer W. F. CLASSIFICATION OF SPOOFING ATTACK TYPES. EUROPEAN NAVIGATION CONFERENCE (ENC), **Proceedings** […]. p. 91-99, 2018.

MEURER, M.; KONOVALTSEV, A.; APPEL, M.; AND CUNTZ, M. Direction-of-Arrival Assisted Sequential Spoofing Detection and Mitigation. 2016 International Technical Meeting (ION ITM), Monterey, **Proceedings** […]. p. 25-28, 2016.

MILNE, E. GNSS: **Mitigating the Threats of Interference, Jamming & Spoofing**. Veripos, 2018. Disponível em: https://veripos.com. Acessado em: 04 Abr. 2022.

MONTEIRO, L. N. C. S. O GPS da Guerra. **Revista Militar**, 2007. Disponível em: www.revistamilitar.pt/artigo/197. Acesso em: 09 Jul. 2022.

MOON, T. K.; STIRLING, W. C. **Mathematical Methods and Algorithms for Signal Processing**. Prentice Hall, 2000.

PROAKIS, J. G. **Digital signal processing: principles, algorithms, and applications.** Pearson Education India, 2007.

PSIAKI, M. L.; AND HUMPHREYS, T. E. GNSS Spoofing and Detection. **Proceedings of the IEEE**, v. 104, n. 6, p. 1258-1270, 2016.

SICKLE, JAN. **GPS for land surveyors**. CRC Press, 2008.

SIGAUD, R. **GPS militar confere precisão e confiabilidade às missões aéreas**. Força Aérea Brasileira, 2017. Disponível em: https://www.fab.mil.br/noticias/mostra/29351/TECNOLOGIA%20%E2%80%93%20GPS%20milit. Acesso em: 09 Ago. 2022.

SILVA, A. L. A. *et al*. Evaluation of the dusk and early nighttime Total Electron Content modeling over the eastern Brazilian region during a solar maximum period. **Advances in Space Research**, v. 67, n. 5, p. 1580-1598, 2021.

SILVA, D. L. **Machine Learning Approach for a Soft-Kill Counter-UAV System Design in an Electronic Warfare and GNSS Spoofing Enviroment**. 2020, 107f. Dissertação (Mestrado em Engenharia Eletrônica e Computação - Instituto Tecnológico de Aeronáutica, São José dos Campos, 2020.

SYAM, W. **Meaconing: the most common type of GNSS spoofing interference attacks**. Wasyresearch , 2022. Disponível em: https://www.wasyresearch.com/meaconing-the-most-common-type-of-gnss-spoofing-interference-attacks/. Acesso em: 01 Mar. 2023.

TALLYSMAN. **GNSS Constellations, Radio Frequencies and Signals**. 2023. Disponível em: https://www.tallysman.com/gnss-constellations-radio-frequencies-and-signals/. Acesso em: 03 Mai. 2023.

TIPPENHAUER, N. O.; PÖPPER, C.; RASMUSSEN, K. B.; CAPKUN, S. On the Requirements for Successful GPS Spoofing Attack. 18TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY. **Proceedings** […]. p. 75-86, 2011.

TREES, H. L. **Optimum Array Processing, Detection, Estimation and Modulation Theory**. Part IV. John Wiley & Sons, 2002.

TSUI, J. B. **Fundamentals of Global Positioning System Receivers**, 2d Ed. John Wiley & Sons, 2005.

WANG, K.; CHEN, S.; PAN, A. Time and Position Spoofing with Open Source Projects. **Black Hat Europe**, v. 148, p. 1-8, 2015.

WARNER, J.S.; JOHNSTON, R.G. GPS spoofing countermeasures. **Homeland Security Journal**, v. 25, n. 2, p. 19-27, 2003.

WU, Z., ZHANG, Y.; YANG, Y.; LIANG, C., AND LIU, R. **Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey**. Joint Foundation of the National Natural Science Committee of China and the Civil Aviation Administration of China, p. 165444-165496, 2020.

XIAO, Y. *et al*. MVDR Algorithm Based on Estimated Diagonal Loading for Beamforming. **Mathematical Problems in Engineering**, v. 2017, 2017.

YUAN, D.; LI, H.; WANG, F.; AND LU, M. A GNSS acquisition method with the capability of spoofing detection and mitigation. **Chin. J. Electron**, vol. 27, no. 1, p. 213-222, 2018.

ZAHAROV, V.; TEIXEIRA, M. SMI-MVDR Beamformer Implementations for Large Antenna Array and Small Sample Size. **IEEE Transactions on Circuits and Systems**, v. 55, n. 10, p. 3317-3327, 2008.

ZHANG, Z.; ZHAN, X., XU, H. **Development and Validation of A Low-cost GPS Spoofing Simulator**. School of Aeronautics and Astronautics, Shanghai Jiao Tong University, 2014.

FOLHA DE REGISTRO DO DOCUMENTO

1. CLASSIFICAÇÃO/TIPO	2. DATA	3. REGISTRO N°	4. N° DE PÁGINAS
DM	23 de maio de 2023	DCTA/ITA/DM-026/2023	68

5. TÍTULO E SUBTÍTULO:
Mitigação de Efeito *Spoofing* em GNSS na Pré-correlação

6. AUTOR(ES):

Antônio Pedro Santos Dias de Carvalho

7. INSTITUIÇÃO(ÕES)/ÓRGÃO(S) INTERNO(S)/DIVISÃO(ÕES):

Instituto Tecnológico de Aeronáutica - ITA

8. PALAVRAS-CHAVE SUGERIDAS PELO AUTOR:

1. Spoofing. 2. Mitigação. 3. Pré-correlação.

9.PALAVRAS-CHAVE RESULTANTES DE INDEXAÇÃO:

Sistemas de Navegação por satélites; Processamento de sinais; Sistemas de posicionamentos; Antenas; Receptores; Telecomunicações; Engenharia Eletrônica.

10. APRESENTAÇÃO: **X Nacional Internacional**

ITA, São José dos Campos. Curso de Mestrado. Programa de Pós-Graduação em Nome do Programa de Engenharia de Computação e Eletrônica. Área de Telecomunicações. Orientador: Prof. Dr. Felix Dieter Antreich_ Defesa em 02/05/2023. Publicada em 2023.

11. RESUMO:

O GNSS (*Global Navigation Satellite System*) pode ser utilizado em aplicações militares e civis para fornecer posicionamento contínuo, seguro e confiável, velocidade e serviços de medição e cronometragem para usuários que necessitam de serviços de navegação, localização, serviços financeiros e de distribuição de energia. Ao replicar os sinais GNSS, um *spoofer* pode enganar o receptor fazendo-o pensar que está em outro local naquele momento e diferentemente do *jamming*, o usuário não o detecta facilmente. Muitas pesquisas abordam a detecção e mitigação de *spoofing* considerando várias técnicas e estratégias distintas. Neste trabalho será apresentada uma abordagem de mitigação de *spoofing* na pré-correlação considerando um sistema com vários sensores. É assumido um receptor integrado solto onde o subsistema *anti-spoofing* está processando sinais do arranjo de antenas e então passa um sinal livre de *spoofing* para o receptor GNSS conectado. Assim, o receptor GNSS é considerado como de última geração, sem características específicas. A detecção de *spoofing* com base na estimativa de direção de chegada (DOA) e a subsequente mitigação de *spoofing* por filtragem espacial será discutida. Essa abordagem pode ser considerada uma abordagem adaptativa cega, pois nem as características do sinal nem os DOA's dos sinais são conhecidos antecipadamente pelo receptor.

12. GRAU DE SIGILO:

(X) OSTENSIVO ( ) RESERVADO ( ) SECRETO