Universidade Federal de Campina Grande

Centro de Engenharia Elétrica e Informática

Programa de Pós-Graduação em Engenharia Elétrica

Localização de *Jammers* em Redes Móveis 5G

Matheus Vilarim Pereira dos Santos

Orientadores: Alexandre Jean René Serres

Edmar Candeia Gurjão

Campina Grande, 2025

Matheus Vilarim Pereira dos Santos

Localização de *Jammers* em Redes Móveis 5G

Dissertação de Mestrado submetida ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande como requisito necessário para obtenção do grau de Mestre em Ciências no domínio da Engenharia Elétrica.

Orientadores: Alexandre Jean René Serres

Edmar Candeia Gurjão

Área de Concentração: Processamento da Informação

Campina Grande, 2025

Matheus Vilarim Pereira dos Santos

Localização de *Jammers em Redes Móveis 5G*

Dissertação Aprovada em: 19 de Fevereiro de 2025

Banca Examinadora:

Alexandre Jean René Serres, D.Sc., UFCG (Orientador)

Edmar Candeia Gurjão, D.Sc., UFCG (Orientador)

Wamberto José Lira de Queiroz, D.Sc., UFCG

Joabson Nogueira de Carvalho, Dr., IFPB

Campina Grande, 2025

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
POS-GRADUACAO EM ENGENHARIA ELETRICA
Rua Aprigio Veloso, 882, - Bairro Universitario, Campina Grande/PB, CEP 58429-900

REGISTRO DE PRESENÇA E ASSINATURAS

1 - ATA DA DEFESA PARA CONCESSÃO DO GRAU DE MESTRE EM ENGENHARIA ELÉTRICA, REALIZADA EM 19 DE FEVEREIRO DE 2025

(Nº 771)

CANDIDATO(A): **MATHEUS VILARIM PEREIRA DOS SANTOS.** COMISSÃO EXAMINADORA: WAMBERTO JOSÉ LIRA DE QUEIROZ , D.Sc., UFCG - Presidente da Comissão e Examinador Interno, ALEXANDRE JEAN RENÉ SERRES, D.Sc., UFCG - Orientador, EDMAR CANDEIA GURJÃO, D.Sc., UFCG - Orientador, JOABSON NOGUEIRA DE CARVALHO, Dr., IFPB - Examinador Externo. TÍTULO DA DISSERTAÇÃO: LOCALIZAÇÃO DE JAMMERS EM REDES MÓVEIS 5G. ÁREA DE CONCENTRAÇÃO: Processamento da Informação. HORA DE INÍCIO: **09h00** – LOCAL: **Sala Virtual, conforme Art. 5º da PORTARIA SEI Nº 01/PRPG/UFCG/GPR, DE 09 DE MAIO DE 2022.** Em sessão pública, após exposição de cerca de 45 minutos, o(a) candidato(a) foi arguido(a) oralmente pelos membros da Comissão Examinadora, tendo demonstrado suficiência de conhecimento e capacidade de sistematização, no tema de sua dissertação, obtendo o conceito APROVADO. Face à aprovação, declara o(a) presidente da Comissão, achar-se o examinado, legalmente habilitado a receber o Grau de Mestre em Engenharia Elétrica, cabendo a Universidade Federal de Campina Grande, como de direito, providenciar a expedição do Diploma, a que o(a) mesmo(a) faz jus. Na forma regulamentar, foi lavrada a presente ata, que é assinada por mim, LEANDRO FERREIRA DE LIMA, e os membros da Comissão Examinadora. Campina Grande, 19 de Fevereiro de 2025.

LEANDRO FERREIRA DE LIMA
Secretário

WAMBERTO JOSÉ LIRA DE QUEIROZ , D.Sc., UFCG
Presidente da Comissão e Examinador Interno

ALEXANDRE JEAN RENÉ SERRES, D.Sc., UFCG
Orientador

EDMAR CANDEIA GURJÃO, D.Sc., UFCG
Orientador

JOABSON NOGUEIRA DE CARVALHO, Dr., IFPB

Examinador Externo

MATHEUS VILARIM PEREIRA DOS SANTOS
Candidato

2 - APROVAÇÃO

2.1. Segue a presente Ata de Defesa de Dissertação de Mestrado da candidato **MATHEUS VILARIM PEREIRA DOS SANTOS,** assinada eletronicamente pela Comissão Examinadora acima identificada.

2.2. No caso de examinadores externos que não possuam credenciamento de usuário externo ativo no SEI, para igual assinatura eletrônica, os examinadores internos signatários **certificam** que os examinadores externos acima identificados participaram da defesa da tese e tomaram conhecimento do teor deste documento.

Documento assinado eletronicamente por **LEANDRO FERREIRA DE LIMA**, **SECRETÁRIO (A)**, em 19/02/2025, às 15:17, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **Matheus Vilarim Pereira dos Santos**, **Usuário Externo**, em 19/02/2025, às 15:26, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **ALEXANDRE JEAN RENE SERRES**, **PROFESSOR(A) DO MAGISTERIO SUPERIOR**, em 19/02/2025, às 15:36, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **EDMAR CANDEIA GURJAO**, **PROFESSOR 3 GRAU**, em 19/02/2025, às 18:46, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

A autenticidade deste documento pode ser conferida no site https://sei.ufcg.edu.br/autenticidade, informando o código verificador **5247920** e o código CRC **D4488ECA**.

Referência: Processo nº 23096.008326/2025-25 SEI nº 5247920

S237l Santos, Matheus Vilarim Pereira dos.
Localização de *Jammers* em redes móveis 5G / Matheus Vilarim Pereira dos Santos. – Campina Grande, 2025.
85 f. : il. color.

Dissertação (Mestrado em Engenharia Elétrica) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, 2024.
"Orientação: Prof. Dr. Alexandre Jean René Serres, Prof. Dr. Edmar Candeia Gurjão".
Referências.

1. Processamento da Informação. 2. Redes Móveis 5G. 3. Bloqueio de Sinais. 4. Localização de *Jammers*. I. Serres, Alexandre Jean René. II. Gurjão, Edmar Candeia. III. Título.

CDU 621.391(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

Agradecimentos

Em primeiro lugar, agradeço ao meu Deus, meu verdadeiro amigo, que me trouxe até aqui e me levará até o fim.

Agradeço à minha esposa e confidente, Maria Luana. Tendo sido meu porto seguro ao longo deste trabalho, me doando cuidado e motivação para que eu pudesse continuar firme todo o tempo. A ela devo cada abraço que procurei nos piores e melhores dias.

Agradeço também aos meus pais, Veridenes e Moisés. Tendo eles trabalhado incansavelmente para que eu chegasse aqui. São a minha fonte de inspiração, carinho e prudência. À minha irmã Mayara, sempre companheira e corajosa. Às minhas avós Josefa e Margarida, mulheres fortes, símbolos de resiliência e amor. Aos meus avôs Carlos e Dezinho, expresso minha gratidão.

Ao professor Edmar Gurjão, agradeço pelos bons conselhos, o empenho para me apresentar oportunidades de crescimento profissional, as colaborações e pelo suporte essencial para que eu pudesse desenvolver este trabalho.

Ao professor Alexandre Serres, pelo suporte e empenho fornecidos, fundamentais para o bom desempenho desta pesquisa. Aos integrantes do laboratório de Radiometria, professora Georgina, professor George Xavier, Joyce, Juliete, Caio, Jéssyca, que foram fonte de apoio e auxílio.

Aos meus colegas do LAPSI e do LABMET, em especial, Fernando e Alisson. Aos técnicos Paulo Márcio e Valber.

Por fim, agradeço à CAPES e à COPELE, pelo provimento da bolsa e do auxílio institucional no âmbito desta dissertação.

"Ó profundidade das riquezas, tanto da sabedoria, como da ciência de Deus! Quão insondáveis são os seus juízos, e quão inescrutáveis os seus caminhos! Por que quem compreendeu o intento do Senhor? Ou quem foi seu conselheiro? Ou quem lhe deu primeiro a Ele, para que lhe seja recompensado? Porque dEle e por Ele, e para Ele, são todas as coisas; glória, pois, a Ele eternamente. Amém."

Paulo de Tarso, Epístola aos Romanos, Capítulo 11:33-36.

Lista de figuras

Lista de tabelas

Resumo

Este trabalho aborda o desafio dos *jammers*, dispositivos eletrônicos destinados a perturbar sinais de rádio frequência, com aplicações que variam desde o bloqueio de sinais em áreas governamentais de segurança até propósitos maliciosos que visam comprometer as comunicações em redes 5G. A pesquisa se concentra na avaliação de métodos para localizar esses dispositivos, utilizando tecnologias presentes no 5G. Exploramos os tipos de *jammers* e os ataques que podem ser realizados, delineando os passos para a localização de uma fonte de rádio frequência passiva. Discutimos técnicas de estimativa de localização com base no tempo, intensidade de sinal e ângulo de chegada, bem como os métodos de localização empregados em redes 5G. Além disso, examinamos o estado da arte em localização de dispositivos *jammers*, identificando avanços e lacunas na literatura. A metodologia envolve o planejamento e a execução de experimentos com um *jammer* apreendido pela Anatel, cujo sinal é capturado e processado para estimar sua localização. Como resultado, utilizando-se da técnica de diferença de tempos de chegada, estimada pelo uso da correlação cruzada dos sinais recebidos filtrados com *wavelets Daubechie*, e da aplicação do método dos mínimos quadrados, obteve-se uma localização com elevada exatidão do *jammer*, sendo o erro médio quadrático observado 0,14 metros.

Palavras-Chave: *Jammers*. Bloqueio de sinais. Localização. 5G.

Abstract

This work addresses the challenge of jammers, electronic devices designed to disrupt radio frequency signals, with applications ranging from blocking signals in government security areas to malicious purposes aimed at compromising communications in 5G networks. The research focuses on evaluating methods for locating these devices, using technologies present in 5G. We explore the types of jammers and the attacks that can be carried out, outlining the steps for locating a passive radio frequency source. We discuss location estimation techniques based on time, signal strength, and angle of arrival, as well as location methods employed in 5G networks. Furthermore, we examine the state of the art in the localization of jammer devices, identifying advances and gaps in the literature. The methodology involves planning and executing experiments with a jammer seized by Anatel, whose signal is captured and processed to estimate its location. As a result, using the time difference of arrival technique, estimated by using the cross-correlation of the received signals filtered with Daubechie wavelets, and applying the least squares method, a highly accurate location of the jammer was obtained, with the mean square error observed being 0.14 meters.

Keywords: Jammers. Blocking signals. Location. 5G.

Lista de abreviaturas e siglas

3GPP	3rd Generation Partnership Project
5GC	5G Core Network
AMF	Access and Mobility Management Function
ANATEL	Agência Nacional de Telecomunicações
ADC	Ângulo de Chegada (Angle of Arrival - AOA)
CJ	Catch the Jammer
LC	Localização por Centroide (Centroid Localization - CL)
SPCU	Separação do Plano de Controle e Usuário (Control and User Plane Separation - CUPS)
CUSUM	Soma Cumulativa (Cumulative Sum - CUSUM)
DIE	Direção da Incerteza do Expoente (Direction of Exponent Uncertainty - DEU)
DL	Downlink
NS	Negação de Serviço (Denial of Service - DoS)
DR	Distance Ratio
DSNR	Distance to Signal Noise Ratio
FEK	Filtro de Kalman Estendido (Extended Kalman Filter - EKF)
eMBB	enhanced Mobile Broadband
FBS	Fibonacci Branch Search
TFF	Transformada Fracionária de Fourier (Fractional Fourier Transform - FRFT)
gNB	gNodeB ou Estação Rádio Base do 5G
GPS	Global Positioning System

GSA	Gravitational Search Algorithm
IMT	International Mobile Telecommunications
ITU	International Telecommunications Union
JRSS	Jammer Received Signal Strength
LBS	Location Based Services
LMF	Location Management Function
CAM	Controle de Acesso ao Meio (Media Access Control - MAC)
MCC	Minimum Circumscribed Circle
MECCL	Minimum Enclosing Circle Center Localization
MERCL	Minimum Enclosing Rectangle Center Localization
MIMO	massive Multiple-Input Multiple-Output
ML	Maximum Likelihood
mMTC	massive Machine-Type Communications
FRV	Funções de Rede Virtualizadas (Network Function Virtualization - NFV)
NRPPa	New Radio Positioning Protocol a
PDCP	Packet Data Convergence Protocol
PDU	Packet Data Unit
PHY	Physical Layer
ECP	Expoente do Caminho de Perdas (Path Loss Exponent - PLE)
PRS	Positioning Reference Signal
RAR	Rede de Acesso por Rádio (Radio Access Network - RAN)
RAT	Radio Access Technologies
RF	Rádio Frequência (Radio Frequency - RF)
IRF	Interferência de Rádio Frequência (Radio Frequency Interference - RFI)

RLC	Radio Link Control
RRC	Radio Resource Control
RSRP	Reference Signal Received Power
ISR	Intensidade do Sinal Recebido (Received Signal Strength - RSS)
RSTD	Reference Signal Time Difference
RTT	Round Trip Time
SBA	Service-Based Architecture
SDAP	Service Data Adaptation Protocol
SDN	Software Defined Networks
SMF	Session Management Function
RSR	Relação Sinal Ruído (Signal-to-Noise Ratio - SNR)
SRS	Sounding Reference Signal
TDOA	Time Difference of Arrival
TOA	Time of Arrival
RT	Relatório Técnico (Technical Report - TR)
TTFF	Time-To-First-Fix
UE	User Equipment
UFCG	Universidade Federal de Campina Grande
UP	Uplink
UPF	User Plane Function
uRLLC	ultra Reliable and Low Latency Communications
VFIL	Virtual Force Iteration Localization
WCL	Weighted Centroid Localization
WSN	Wireless Sensors Network

Sumário

1 Introdução

Os *jammers* são dispositivos eletrônicos construídos com o propósito de causar interferência destrutiva em sinais de rádio. Esses equipamentos podem ser utilizados com propósitos diversos, sejam eles de interesses governamentais, como no bloqueio de sinais de telefonia em perímetros de segurança de penitenciárias, órgãos públicos e isolação de espaços aéreos contra drones. Assim como para propósitos maliciosos, quando atacantes visam indisponibilizar a comunicação por redes sem fio legítimas, sejam elas redes de telefonia móvel de terceira, quarta ou quinta geração, redes Wi-Fi, ou outras que operem nas faixas de rádio frequência.

Os *jammers* podem ser de vários tipos, sendo os principais: constantes - emitem sinais de rádio aleatórios de forma contínua no meio; insidiosos - conhece o protocolo de comunicação utilizado na rede atacada e inunda a interface com transmissões contínuas de pacotes falsos; aleatórios - tem a capacidade de operar como os constantes e insidiosos, porém o faz de forma aleatória; reativos - analisa passivamente a rede alvo e identifica os protocolos utilizados na comunicação, só então quando possui informações suficientes, inicia a transmissão, aderindo às características que sejam mais danosas (PIRAYESH; ZENG, 2022).

A utilização dos *jammers* para emissão de sinais de rádio com o objetivo de perturbar a operação de transceptores, consiste no ataque de *jamming*. Para conseguir maior taxa de sucesso na realização do ataque de *jamming*, o atacante além de selecionar o tipo do dispositivo, pode também aderir a diferentes técnicas de ataque (*spot, sweep e barrage*) e adaptá-las a múltiplos cenários, seja operando de forma fixa, móvel, ou utilizando antenas que concentrem a energia do sinal em uma determinada direção.

As redes 5G são a quinta geração de redes móveis celulares, onde desde sua concepção foram alicerçadas em novas tecnologias que permitem o provimento de banda larga de alta velocidade, conectividade massiva de todas as coisas e comunicações com baixa latência e alta confiabilidade. As principais organizações responsáveis pela padronização e especificação de requisitos do 5G, são o *3rd Generation Partnership Project* (3GPP) e *International Telecommunications Union* (ITU), as quais também definem os aspectos de segurança da rede na elaboração da sua arquitetura. Neste sentido, foram definidos então mecanismos nas funções de rede, escolhidos protocolos, especificados identificadores e interfaces que juntos pudessem, se corretamente configurados, prover confidencialidade, integridade e disponibilidade para rede (PEJANOVIć-DJURIšIć; KUKLINSKI, 2022).

Embora as redes 5G possuam diversos mecanismos de segurança, ataques como *jamming* ainda são um desafio a ser solucionado. De forma geral, os atacantes utilizam o dispositivo *jammer* para indisponibilizar o sinal da rede legítima da operadora e forçar os usuários das regiões atacadas a se conectarem em redes falsas. Dependendo da área impactada, serviços fundamentais para a população podem ser interrompidos, dados pessoais podem ser roubados e informações falsas injetadas na rede. Portanto, faz-se essencial o estudo de técnicas que sejam úteis para solução desse problema.

1.1 Motivação

A Universidade Federal de Campina Grande foi responsável pela condução de um termo de execução descentralizada junto a Agência Nacional de Telecomunicações (Anatel), tendo como parte dos seus objetivos o estudo da segurança cibernética das redes 5G. Foi apresentada como demanda para o pacote de trabalho sobre camada física da rede, o estudo de um dispositivo *jammer* apreendido pela agência. Dada a supracitada provocação, foram conduzidos trabalhos de pesquisa pautados em revisões sistemáticas da literatura que identificaram o problema chave de número seis (*Key Issue #6: Resistance to radio jamming*) da TR 33.809 do 3GPP, que trata sobre o estudo de melhoramento da segurança do 5G contra estações base falsas (3GPP, 2023h). Nela, é apresentada a problemática do *jamming* em redes 5G, são destacadas tecnologias já presentes nas especificações do 5G que permitem que a rede possua maior resiliência, como *beamforming*, duplicação do PDCP PDUs em caso de multi-conectividade e agregação de portadoras. Porém, destacou-se também que essas tecnologias não impedem que seja realizado o ataque de *jamming* e a rede ou equipamento de usuário sofra degradação ou negação do serviço, sendo assim, elas auxiliam na detecção do atacante e uma vez que o ataque encerre a comunicação rapidamente pode ser reestabelecida. Por fim, visto que o atacante pode ser detectado, uma possível solução para o problema é a localização e captura do *jammer*.

O 5G possui capacidade para realizar localização por diferentes técnicas, porém não estão definidas nas especificações técnicas como essas podem ser utilizadas na localização de dispositivos de rádio frequência passivos, como o *jammer*, que não respondem à requisições da rede. Assim, observou-se um momento oportuno para contribuir com o estudo da eficácia de diferentes algorítimos para localização dos *jammers*, usando tecnologias em algum grau já reconhecidas pelo 3GPP.

1.2 Objetivos

Avaliar os métodos de localização de *jammers* com o uso de tecnologias presentes nas redes móveis de quinta geração e, como objetivos específicos:

1. Analisar a especificação de um sistema de localização que seja capaz de localizar o *jammer* em um cenário real;
2. Investigar tecnologias presentes no 5G visando uma estimativa precisa em comparação com as demais técnicas presentes na literatura;
3. Comparar a resposta dos diferentes algoritmos de localização baseados em tempo de chegada, utilizando simulação e testes reais;
4. Analisar as possibilidades para elevar a exatidão da localização.

1.3 Organização

A seção 2 (dois) do presente documento, consiste de uma fundamentação teórica sobre dispositivos *jammers*, onde são apresentados seus tipos quanto ao comportamento, forma e construção. Além disso, também são destacados os ataques de *jamming*, diferentes sistemas e técnicas para estimativa de localização, conceitos sobre a rede 5G e técnicas para localização utilizadas no *New Radio*. A revisão bibliográfica que traça o estado da arte sobre métodos para localização de dispositivos *jammers* já desenvolvidos, está disposta na seção 3 (três). Por conseguinte, na seção 4 (quatro) é caracterizada a metodologia usada na obtenção dos resultados, e na seção 5 (cinco) estão dispostos os resultados. Por fim, na seção 6 (seis), apresentam-se as considerações finais.

2 Fundamentação teórica

2.1 Dispositivos *jammers*

No campo das comunicações sem fio e do processamento de sinais, um *jammer* é um dispositivo usado para interromper ou interferir intencionalmente na transmissão ou recepção de sinais (CAMBRIDGE..., 2023). Os *jammers* podem ser usados para várias finalidades, incluindo o bloqueio do uso de redes sem fio em áreas não autorizadas, interdição do espaço aéreo contra drones, ou ataques maliciosos que visam a interrupção da comunicação em redes móveis celulares. A pesquisa acadêmica nessa área se concentra no desenvolvimento de contramedidas eficazes contra *jammers* e no estudo do impacto do *jamming* nas redes sem fio.

O dispositivo *jammer* é comumente aplicado em ataques de negação de serviço (do inglês, *Denial of Service* - DoS), onde o sinal maliciosamente irradiado na interface aérea causa interferência destrutiva no sinal usado para comunicação entre os transmissores e receptores autênticos. Dessa forma, atacantes em posse desses equipamentos podem desconectar usuários de uma operadora móvel legítima, e forçar sua conexão em uma estação base falsa, possibilitando assim o roubo de dados, ou injeção de pacotes maliciosos na rede.

2.1.1 Tipos de *jammers*

Ao usar o termo *"jammer"*, como já destacado anteriormente estamos nos referindo ao equipamento e aos seus recursos que são utilizados por um atacante para atingir seus objetivos. Um *jammer* pode variar de um simples transmissor a complexas estações de interferência equipadas com ferramentas especializadas. Vários tipos de *jammers* podem ser empregados para atingir as redes móveis celulares. Em (XU et al., 2005), é proposto um conjunto de modelos gerais de *jammers*, incluindo o *jammer* constante, o *deceptive jammer*, o *jammer* aleatório e o *jammer* reativo.

O *jammer* constante emite continuamente sinais de rádio aleatórios no meio sem fio. As mensagens produzidas por esses equipamentos não aderem a nenhum protocolo MAC específico e consistem em bits arbitrários. O objetivo desse tipo de *jammer* é ocupar o canal, interromper a comunicação entre os nós e introduzir interferência nos nós envolvidos em transferências de dados, corrompendo assim seus pacotes.

O *jammer* insidioso possui conhecimento sobre o protocolo usado na rede alvo e emprega uma estratégia de transmissão contínua de pacotes falsificados em uma taxa alta durante um período específico para interromper efetivamente a rede. Esse tipo de *jammer* representa uma ameaça significativa devido à sua capacidade inerente de evitar a detecção, o que o torna excepcionalmente perigoso. Visto que tem o potencial de inundar o Elemento de Processamento (PE) com um fluxo esmagador de dados inúteis ou fabricados, enganando efetivamente o operador da rede. Além de enganar e confundir o operador, também ocupa a largura de banda da qual os nós legítimos dependem para uma comunicação eficiente. No entanto, assim como o *jammer* constante, o *jammer* insidioso é ineficiente em termos de energia.

O *jammer* aleatório opera de maneira semelhante ao *jammer* constante ou ao *jammer* insidioso, mas o faz de forma aleatória. Embora não seja tão eficaz quanto o *jammer* que ele emula (constante ou insidioso), ele oferece maior eficiência energética.

O *jammer* reativo também possui conhecimento dos protocolos de comunicação empregados pela rede de destino. Ele monitora passivamente a rede, aguardando o momento oportuno para lançar um ataque. Ao imitar o comportamento da rede e aderir aos seus protocolos, o *jammer* reativo atinge melhor eficácia quando comparado aos citados anteriormente. Entretanto, essa abordagem não é particularmente eficiente em termos de energia, pois requer uma quantidade significativa de energia para monitorar continuamente a rede.

Pode-se destacar também que além de se diferenciarem quanto ao seu comportamento, os *jammers* variam em sua forma, podendo ser móveis ou estáticos, além de terem diferentes aplicações conforme os tipos de antenas (omnidirecionais e direcionais) utilizadas em sua construção (WANG et al., 2018c). Alguns exemplos podem ser vistos na Figura 1.

Figura 1 – Tipos de dispositivos *jammer*.

(a) *Jammer* móvel omnidirecional

(b) *Jammer* estático omnidirecional

(c) *Jammer* móvel direcional

Fonte: *skylishop.com*.

Os *jammers* móveis são utilizados contra alvos que também possuem mobilidade, geralmente apresentam alcance limitado devido à potência de operação reduzida, consequência da dependência que possui da bateria com dimensões reduzidas para propiciar portabilidade. Já os *jammers* estáticos são utilizados em cenários onde o alvo é uma determinada região de cobertura, normalmente possuindo maior potência de transmissão que visa maior raio de ação, atingindo assim um maior número de alvos. Por fim, o *jammer* direcional tem foco em aplicações contra alvos pontuais distantes, que podem ser atacados por meio de feixes mais estreitos de sinal, evitando que haja interferência em dispositivos circunvizinhos e conseguindo melhor alcance quando comparado as outras opções, sendo essas as razões para serem amplamente utilizados contra drones.

2.1.2 Ataques de *jamming*

Ataques de *jamming* são realizados utilizando o equipamento *jammer*, e consistem da emissão de sinais de rádio com o objetivo de perturbar a operação dos transceptores. A principal distinção entre *jamming* e interferência de radiofrequência (do inglês, *Radio Frequency Interference* - RFI) está em sua intencionalidade. O *jamming* envolve ações deliberadas direcionadas a um alvo específico, enquanto a RFI é uma consequência não intencional que surge quando transmissores próximos operam na mesma frequência, em frequências muito próximas, ou ocorra fenômeno físico que reforce sinais indesejados, como harmônicas que não deveriam ser irradiadas na interface aérea (ADAMY, 2003).

O fator crucial para realizar ataques de *jamming* bem-sucedidos é a relação sinal-ruído (do inglês, *Signal-to-Noise Ratio* - SNR), que pode ser representada como $SNR = P_{signal}/P_{noise}$, em que P_{signal} e P_{noise} denotam as potências do sinal e do ruído respectivamente. O ruído engloba as variações indesejadas e não intencionais do espectro eletromagnético na entrada do receptor. Para que o bloqueio seja considerado eficaz, a SNR precisa ser menor que 1, indicando que a potência do sinal é menor que a potência do ruído (MPITZIOPOULOS et al., 2009). As principais técnicas de *jamming* podem ser listadas como:

- *Spot Jamming*: Conhecido por sua eficácia, esse modelo de ataque gira em torno do conhecimento abrangente do atacante sobre a frequência de rádio precisa da rede alvo. Ao direcionar sua potência de transmissão para a frequência de operação da rede legítima, o invasor interrompe a rede com eficiência usando o mínimo de energia. No entanto, esse método encontra uma vulnerabilidade, pois a rede alvo pode empregar técnicas dinâmicas de evasão de frequência, como navegação de canal ou salto de frequência, mudando rapi-

damente para uma frequência alternativa para evitar as tentativas de interferência. Essa abordagem adaptativa permite que a rede alvo atenue o impacto do bloqueio pontual e mantenha a comunicação ininterrupta;

- *Sweep Jamming*: Caracterizada por sua rápida mudança de frequência, permite que um *jammer* exerça toda a sua potência em uma faixa de frequências. Embora essa abordagem permita o bloqueio de várias frequências de forma rápida e sucessiva, ela não causa impacto simultâneo em todas as frequências, limitando assim sua eficácia geral. No entanto, a varredura realizada por esse modelo de ataque pode levar a uma perda significativa de pacotes e retransmissões, esgotando, consequentemente, recursos valiosos de energia. Essa técnica opera sem conhecimento prévio da frequência-alvo e, em vez disso, são empregadas varreduras periódicas ou aperiódicas no espectro provável, interrompendo temporariamente as redes afetadas. Embora seja menos eficiente e eficaz em comparação com o *spot jamming*, ele têm a capacidade de impedir a liberdade da rede-alvo de alternar entre frequências e exercer restrições em várias redes simultaneamente;

- *Barrage Jamming*: Caracterizado pelo bloqueio simultâneo de uma série de frequências, tem nesse comportamento sua maior vantagem. Essa abordagem diminui efetivamente a relação sinal-ruído (SNR) dos receptores alvo ao utilizar potência suficiente. Entretanto, à medida que a faixa de frequências bloqueadas se expande, a potência de saída do *jammer* é proporcionalmente reduzida. Essa técnica têm a capacidade de cobrir uma largura de banda significativa do espectro de rádio, deixando um espaço mínimo para que a rede-alvo evite a interrupção. Além disso, várias redes podem ser atingidas simultaneamente, ampliando seu impacto. Para manter a densidade espectral de potência necessária para a interferência, os *jammers* utilizados nesse modelo de ataque precisam de alta potência de transmissão.

2.2 Sistemas de localização

Sistemas de localização têm como finalidade a identificação da posição de um objeto em movimento ou estacionário dentro de um sistema de coordenadas. A localização de fontes de RF (*Radio Frequency*) passiva surgiu como um problema crucial que exige atenção considerável nos domínios do processamento de sinais e da comunicação sem fio. Sua importância decorre da ampla gama de aplicações a que serve, atendendo a diversas necessidades, como sistemas de transporte inteligentes, rastreamento de usuários móveis, e sistemas de defesa.

A localização de uma fonte de rádio frequência passiva pode ser dividida em três partes fundamentais: (1) observação do sinal, (2) extração dos parâmetros do sinal relacionados à posição, e (3) estimativa da posição do alvo. Em seguida, são abordadas diferentes técnicas que podem ser empregadas na solução das diferentes partes do problema.

2.2.1 Técnicas para estimativa de localização

As principais técnicas para estimativa de localização de um transmissor passivo, ou seja, que não interaje com os receptores, são baseadas em tempo de chegada (do inglês, *Time of Arrival* - TOA), diferença no tempo de chegada (do inglês, *Time Difference of Arrival* - TDOA), ângulo de chegada (do inglês, *Angle of Arrival* - AOA), intensidade do sinal recebido (do inglês, *Received Signal Strength* - RSS) e parâmetros híbridos (ULUSKAN; FILIK, 2019). Cada uma dessas abordagens podem ser selecionadas de acordo com os cenários e limitações que se apresentam, por exemplo, RSS possui baixa complexidade computacional, porém demonstra maior sensibilidade a alterações no coeficiente de perdas do caminho. Já TDOA e AOA entregam elevada precisão, contudo necessitam de maiores exigências nos requisitos de *hardware* e *software*.

2.2.1.1 Técnica baseada no tempo de chegada

As medições de TOA oferecem um método eficaz para determinar a posição de um dispositivo. Isso se baseia no princípio fundamental de que o tempo que um sinal leva para viajar entre dois pontos com posições distintas, comumente conhecido como tempo de voo, é diretamente proporcional à distância entre ambos, $d = c\tau$, onde τ é o tempo de propagação e c a velocidade da luz no meio. Ao medir com precisão o tempo que o sinal leva para atingir diferentes pontos de referência sincronizados, é possível calcular a posição exata do dispositivo. Para isso, podemos escrever a seguinte equação:

$$t_i = \tau_i + T_{tx}, \tag{2.1}$$

$$t_i - T_{tx} = d_i/c, \tag{2.2}$$

$$t_i - T_{tx} = \frac{\sqrt{(x_i - x)^2 + (y_i - y)^2}}{c}. \tag{2.3}$$

Onde t_i é o tempo de chegada no i-ésimo receptor, τ_i é o tempo de propagação entre o transmissor e o receptor, (x_i, y_i) é a posição bidimensional do i-ésimo receptor, d_i é a distância entre o transmissor e o i-ésimo receptor, e por fim, T_{tx} é o instante em que o sinal foi transmitido.

Observa-se que a Equação 2.3 é não-linear e possui duas variáveis desconhecidas, sendo necessário então um mínimo de três receptores para que se possa garantir uma única solução. Um desafio para o método baseado em TOA é a necessidade de elevado conhecimento sobre o transmissor, dada a dependência de se ter ciência sobre o instante de transmissão do sinal. O que por exemplo, no cenário de localização de *jammers* é na maioria dos casos uma informação pouco provável de se obter.

O tempo de chegada de um sinal pode ser calculado por diferentes algoritmos, destacam-se na literatura técnica:

- **Primeiro Pico**: No processamento de sinais, a identificação do primeiro pico da frente de onda assume um papel de destaque na extração de informações significativas dos sinais. O primeiro pico é definido como o instante temporal inicial em que a amplitude do sinal ultrapassa um limiar previamente definido e atinge um valor máximo local antes de iniciar o decaimento. A seleção cuidadosa do limiar é de suma importância para a eficácia desse método, pois tem o propósito primordial de mitigar a influência do ruído de fundo presente nos sinais. O ruído de fundo, constituído por flutuações aleatórias indesejadas, pode obscurecer a detecção precisa de eventos relevantes, comprometendo a confiabilidade da análise do sinal. Portanto, a determinação precisa do limiar representa um procedimento crítico para discernir picos verdadeiros de interferências de ruído, assegurando assim uma melhor detecção do tempo de chegada do sinal.(GU et al., 2022; ZHANG; KANG, 2020; WANG et al., 2018f; TORRIERI, 1974)

- **Energia Cumulativa**: De forma geral a energia cumulativa de um sinal (x) até a amostra n, é dada por (WANG et al., 2018f; ROBLES; FRESNO; MARTíNEZ-TARIFA, 2015):

$$E_c(n) = \sum_{m=0}^{n} x^2(m). \tag{2.4}$$

Porém, considerando-se que as formas de onda dos sinais obtidos são dadas em termos da tensão ao longo do tempo (KAKEETO et al., 2008), a Equação 2.4 pode ser reescrita como:

$$E_c(t_n) = \sum_{i=1}^{n} [V(t_i)]^2, \tag{2.5}$$

sendo $V(t_i)$ é a tensão no instante de tempo t_i e n é o número de amostras do sinal.

O tempo de chegada do sinal nesse método é descrito como o ponto onde a derivada da curva de energia acumulada é máxima.

2.2.1.2 Técnica baseada na diferença entre tempos de chegada

Dada a Equação 2.1, em um cenário de localização de um transmissor desconhecido e com o qual não se pode trocar informações, torna-se inviável a determinação da sua posição, visto que não se sabe o instante de tempo de transmissão T_{tx}. Desse modo, detaca-se a importância da diferença entre o tempo de chegada em diferentes receptores, por meio da qual se pode eliminar a influência de T_{tx} na estimativa da posição:

$$t_i - t_j = \tau_i + T_{tx} - (\tau_j + T_{tx}) \tag{2.6}$$

$$t_i - t_j = \tau_i - \tau_j \tag{2.7}$$

$$t_i - t_j = \frac{d_i}{c} - \frac{d_j}{c} \tag{2.8}$$

$$t_i - t_j = \frac{\sqrt{(x_i - x)^2 + (y_i - y)^2} - \sqrt{(x_j - x)^2 + (y_j - y)^2}}{c}, \tag{2.9}$$

sendo t_i o tempo de chegada no i-ésimo receptor e t_j é o tempo de chegada no j-ésimo receptor. Sendo então a TDOA calculada pela diferença entre as TOAs obtidas por algum dos algoritmos citados anteriormente ou por correlação cruzada.

O sinal processado para estimativa do tempo de chegada, pode ser o resultado de várias frentes de onda que se formam no ambiente, visto que devido aos obstáculos do percurso presentes no ambiente o sinal pode sofrer difrações e reflexões. A composição dessas múltiplas frentes de onda, se processada de forma inadequada, sucede em um tempo de propagação da onda eletromagnética que não condiz com a menor distância entre o transmissor e receptor. Portanto, para solucionar esse problema, considera-se o princípio de Fermat, por meio do qual se define o tempo de propagação do sinal a partir apenas da primeira frente de onda, que condiz ao caminho mais curto percorrido (FARKAS; KáLY-KULLAI; SIENIUTYCZ, 2005).

Considerando-se a Equação 2.9 para três receptores em posições distintas, pode-se então montar um sistema de equações não-lineares da seguinte forma:

$$((t_1 - t_2).c) = \sqrt{(x_1 - x)^2 + (y_1 - y)^2} - \sqrt{(x_2 - x)^2 + (y_2 - y)^2}, \tag{2.10}$$

$$((t_1 - t_3).c) = \sqrt{(x_1 - x)^2 + (y_1 - y)^2} - \sqrt{(x_3 - x)^2 + (y_3 - y)^2}. \tag{2.11}$$

Poderia ser montada uma terceira equação em função de $(t_2 - t_3)$, a qual não traria nenhuma informação nova, visto que é dependente das outras duas equações. Apesar de na prática normalmente haver apenas uma solução para esse sistema, para garantir a ausência de múltiplas soluções em um sistema de duas equações não-lineares com duas incógnitas, é necessária uma medição adicional. Assim, para se obter a posição do transmissor alvo (x, y), pode-se aplicar por exemplo, uma solução numérica baseada no método de Newton-Raphson ou no método dos Mínimos Quadrados (do inglês, *Least Squares*)(VELEZ-LOPEZ et al., 2019; GRIVA; NASH; SOFER, 2009; LAWSON; HANSON, 1976; BOX; DAVIES; SWANN, 1969).

Para simplificar o cálculo da TDOA utilizando os tempos de chegada obtidos no método da energia cumulativa, pode-se adicionar uma linha com inclinação negativa, por meio da qual se obtém (ROBLES; FRESNO; MARTíNEZ-TARIFA, 2015):

$$E_{neg}(n) = E_c(n) - n\frac{E_N}{N} = \sum_{m=0}^{n}[s^2(m) - n\frac{E_N}{N}], \tag{2.12}$$

sendo E_N a energia total do sinal.

Um método tradicionalmente utilizado para o cálculo da TDOA, é a correlação cruzada entre dois sinais (PALLOTTA; GIUNTA, 2022; JING-GANG et al., 2008; KNAPP; CARTER, 1976):

$$R_{ij} = \sum_{m=-N/2}^{(N/2)-1} s_i(m+1) \cdot s_j(m), \tag{2.13}$$

sendo, s_i e s_j são os sinais respectivamente no i-ésimo e j-ésimo receptor, compostos por N amostras. Assim, a TDOA entre esses dois sinais (τ_{ij}) é dada por:

$$\tau_{ij} = [S_{mx} - (N-1)] \cdot dt, \tag{2.14}$$

em que S_{mx} é a amostra com maior coeficiente de correlação entre os sinais e dt é o tempo entre as amostras.

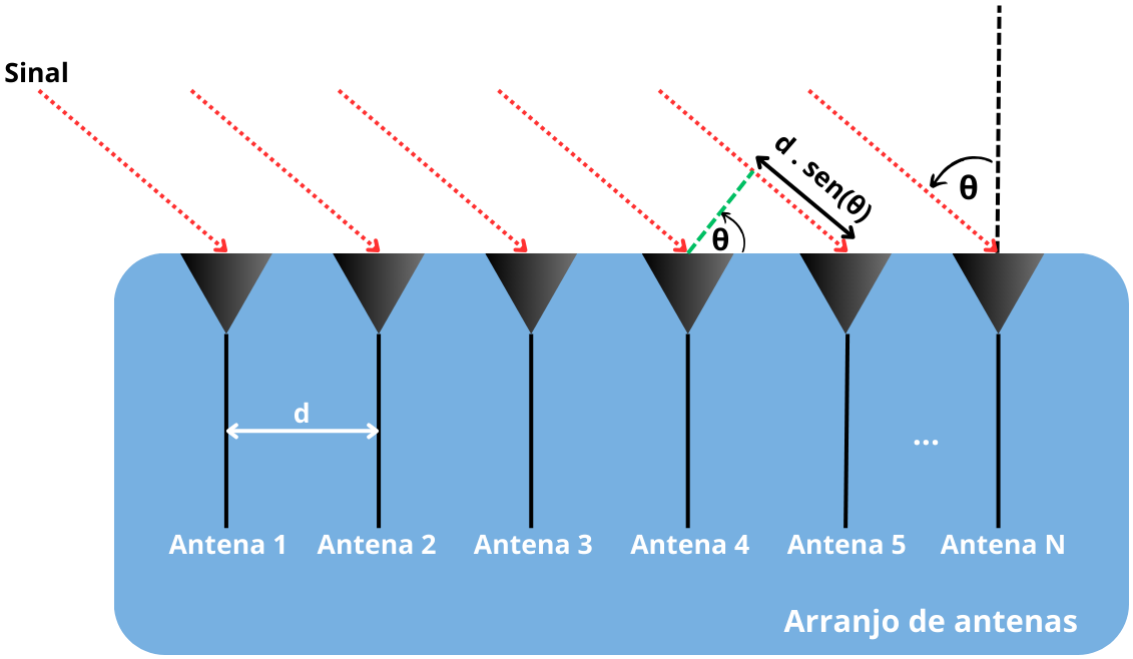
2.2.1.3 Técnica baseada no ângulo de chegada

A técnica baseada no ângulo de chegada (do inglês, *Angle of Arrival* - AOA) consiste na estimativa do ângulo de chegada do sinal, diferenciando-se das demais técnicas que focam na distância relativa entre dois nós. Os métodos para estimar o ângulo de chegada de um sinal

podem ser divididos em duas categorias: (1) tempo real - possuem baixa complexidade e são aplicados onde não há exigência de alta precisão; (2) não tempo real - são altamente complexos e podem ser aplicados a sistemas onde há exigência de alta precisão.

A implementação da técnica de AOA é dependente do uso de dois ou mais receptores com um conjunto de antenas. A estimativa de AOA é computada pela medida da fase relativa entre sinais recebidos nos elementos de antena (WATSON; LLOYD, 2020; FRIEDLANDER, 2009). Na Figura 2, observa-se uma representação que expressa a ideia geral sobre essa metodologia, onde um conjunto de antenas com seus elementos igualmente espaçados por uma distância (d) recebem a incidência de um sinal com angulo de chegada (θ).

Figura 2 – Representação do angulo de chegada de um sinal em um arranjo de antenas.



Fonte: Autoral.

O AOA é usado conjuntamente com TOA ou TDOA para elevar a precisão da localização, ao custo de maior consumo dos recursos computacionais disponíveis. Os algoritmos para estimação do ângulo de chegada de um sinal incluem por exemplo: *maximum likelihood* (ML), MUSIC, *root* MUSIC, DAS e ESPRIT (LINDNER et al., 2015; SHI et al., 2013; ELHAG et al., 2013; GODARA, 1996). A performance de estimação do algoritmo DAS é baixa, também possui sensibilidade alta à SNR, erros de calibração e número de reflexões, porém sua baixa complexidade permite aplicações em sistemas de tempo real. O algoritmo MUSIC calcula um espectro espacial por meio da estimativa do subespaço de ruído e identifica a direção de chegada do sinal com base no pico dominante, sua complexidade algorítmica é alta, porém possui menor sensibilidade aos parâmetros indicados anteriormente quando comparado ao DAS. O *root*

MUSIC compartilha semelhanças com o MUSIC, sendo que a principal diferença é que o AOA é determinado por raízes que estão mais próximas do círculo unitário de um polinômio derivado do subespaço de ruído, possui também melhor eficiência computacional e menor sensibilidade aos parâmetros já citados.

2.2.1.4 Técnica baseada na potência do sinal recebido

A técnica baseada na potência do sinal recebido (do inglês, *Received Signal Strength* - RSS) é a mais simples de todas as abordagens apresentadas para localização de transmissores RF passivos, sendo um dos motivos a independência em relação ao sincronismo dos receptores. Essa técnica aplica algoritmos que consistem na análise da atenuação sofrida por um sinal de rádio durante a sua propagação entre dois nós e sua interação com os objetos do meio. A potência recebida é inversamente proporcional ao quadrado da distância entre os nós, como pode ser visto na Equação 2.15 do modelo de Friis. Portanto, descreve-se com uma extenção dessa equação a potência recebida em um modelo de caminho de perdas log-distante, que pode ser obsevada na Equação 2.16 (HUSSAIN et al., 2022; NIU et al., 2020; ALDOSARI; ZOHDY; OLAWOYIN, 2019b).

$$P_r(d) = P_t \frac{G_r G_t \lambda^2}{(4\pi d)^2 L}. \tag{2.15}$$

$$P_r(d) = P_t + K - 10n \log_{10}(d) + X_\sigma, \tag{2.16}$$

sendo $P_r(d)$ é a potência recebida em uma distância d, P_t é a potência transmitida, G_r e G_t são respectivamente o ganho do receptor e do transmissor, λ é o comprimento de onda, L é o fator de perdas do caminho. Já X_σ é o ruído gassiano com média zero e n é o expoente de perdas do caminho que depende do ambiente de propagação (por exemplo, espaço livre, área urbana ou ambiente fechado) como visto na Tabela 1 (RAPPAPORT, 2001).

Tabela 1 – Expoentes de perdas do caminho.

Ambiente	$\boldsymbol{\eta}$
Espaço livre	2
Área urbana	2,7 à 3,5
Área urbana com sombra	3 à 5
Área interna com linha de visada	1,6 à 1,8
Área interna sem linha de visada	4 à 6
Área fabril sem linha de visada	2 à 3

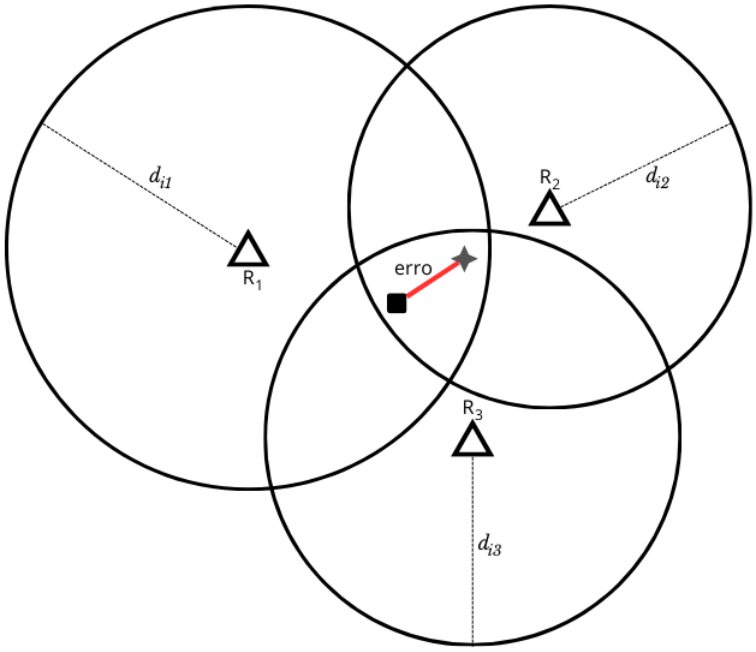
Fonte: Adaptada de Rappaport (2001).

Como exemplo de aplicação do algoritmo de localização baseado em RSS, na Figura 3, pode-se observar três receptores representados por triângulos (R_1, R_2 e R_3). A distância estimada entre o nó do receptor j e o transmissor i é denotada por d_{ij}, e a partir do modelo de caminho de perdas log-distante já apresentado é dada pela Equação 2.17. Além disso, o retângulo na área de interseção das circunferências diz respeito a posição real do transmissor, já a estrela representa a posição estimada com base na distância calculada por cada nó de recepção. Desse modo, o erro de localização é dado pela distância entre a posição real e a posição estimada.

$$d_{ij} = 10^{\frac{P_0 - P_{ij}}{10 \cdot \eta}}, \tag{2.17}$$

sendo P_{ij} é o valor médio da RSS no receptor i devido às transmissões de j, e P_0 é a intensidade do sinal (dBm) de referência no receptor à uma distância de um metro do transmissor.

Figura 3 – Localização por meio de RSS.



Fonte: Autoral.

Uma vez obtidas as distâncias estimadas entre cada receptor e o transmissor, visto que a posição dos receptores é conhecida, pode ser utilizado por exemplo o algoritmo de multilateração para estimar a posição do alvo. A multilateração consiste no cálculo da posição baseado na área de interseção entre círculos com centro nos receptores e raios iguais as distâncias estimadas, para tal se utilizam métodos de otimização para minimizar o erro entre as distâncias estimadas e euclidiana obtidas na posição atual estimada para o transmissor i. Na Equação 2.18 é apresentada a expressão para cálculo da distância euclidiana entre os nós i e j:

$$D_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}. \tag{2.18}$$

Já a função custo da multilateração pode ser definida como:

$$f_{cML} = \sum_{i=1}^{n} \sum_{j=1, j\neq i}^{m+n} |d_{ij} - D_{ij}|. \tag{2.19}$$

Esse método é simples de usar e funciona bem no espaço livre. Entretanto, é sensível à variação do caminho de perdas, por exemplo, efeitos de sinais de múltiplos caminhos, sombreamento (atenuação do sinal devido às obstruções causados por objetos, construções, vegetação) e um alvo com potência de transmissão ajustável, podem adicionar erros na medição da RSS que levam a estimativas de posição imprecisas. Para que essa técnica alcance melhores níveis de precisão, pode-se empregar um número elevado de receptores (PATWARI et al., 2005).

2.2.1.5 Técnica híbrida

Sistemas de localização podem utilizar uma composição de diferentes técnicas de localização, visando assim uma abordagem híbrida que atenda aos critérios apresentados no cenário que se deseja solucionar. Por exemplo, TOA e AOA podem ser aplicadas em conjunto para buscar melhor precisão na posição estimada com o mesmo número de receptores. Já a TDOA pode ser empregada com a RSS, visando melhora da precisão, menor dependência de um número elevado de receptores e da linha de visada. Mais combinações podem ser exploradas, inclusive alterando os algoritmos para estimação dos parâmetros utilizados no processo de localização (ARABSORKHI; ZAYYANI; KORKI, 2023; ZHAO et al., 2020; ZHANG et al., 2017).

2.3 Redes móveis 5G

As redes móveis de quinta geração (5G), conhecidas tecnicamente como IMT-2020, foram pensadas para entregar banda larga aprimorada (eMBB - *enhanced Mobile Broadband*), internet de todas as coisas com conexões massivas (mMTC - *massive Machine-Type Communications*), e comunicações de alta confiabilidade com baixa latência (uRLLC - *ultra Reliable and Low Latency Communications*). O 5G é padronizado por instituições como a União Internacional de Telecomunicações (do inglês, ITU - *International Telecommunication Union*) e o *3rd Generation Partnership Project* (3GPP). A ITU é responsável por coordenar as telecomunicações internacionais e define os requisitos técnicos e espectrais para o 5G. O 3GPP, por sua vez, é uma colaboração entre várias organizações de padronização e desenvolve as especificações

técnicas para o 5G, incluindo os serviços eMBB, mMTC e uRLLC. Essas instituições garantem a interoperabilidade e a compatibilidade das redes e equipamentos 5G em todo o mundo. A Tabela 2, resume alguns dos requisitos de sistema do 5G presentes na especificação técnica TS 22.261 do 3GPP (3GPP, 2023g).

Tabela 2 – Requisitos de sistema do 5G.

Parâmetros	**Requisitos**
Pico da taxa de transferência	DL: 20 Gbps, UL: 10 Gbps
Taxa de transferência experimentada pelo usuário	DL: 100 Mbps, UL: 50 Mbps
Capacidade do tráfego por área	10 Mbps/m^2
Latência	eMBB: 4 ms, URLLC: 1 ms
Densidade de conexões	1 milhão de dispositivos por km^2
Tempo de interrupção da mobilidade	0 ms
Largura de banda mínima	100 MHz

Fonte: Autoral.

Visando atender aos requisitos estabelecidos, o 5G faz uso de tecnologias como a virtualização de funções de rede (do inglês, NFV - *Network Function Virtualization*), que consiste em virtualizar as funções tradicionalmente executadas por hardware em redes de comunicação. Além disso, temos as redes definidas por software (do inglês, SDN - *Software Defined Networks*), que permitem a gestão centralizada e programável das redes, trazendo maior flexibilidade e eficiência. Outra tecnologia importante é o fatiamento de rede (do inglês, *network slicing*), que permite criar fatias virtuais da rede para atender a diferentes requisitos de aplicação. Por fim, temos o MIMO massivo (do inglês, *massive Multiple-Input Multiple-Output*), que utiliza múltiplas antenas para melhorar a capacidade e a eficiência das comunicações sem fio.

O MIMO massivo é uma tecnologia que utiliza arranjos de antenas de grande porte, geralmente com mais que 8 elementos, para permitir múltiplas transmissões e recepções entre os equipamentos de usuário (UE) e a estação rádio base do 5G (gNB). Além disso, esses arranjos de antenas podem ser usados para formar feixes direcionais, conhecidos como *beamforming*, que consistem no controle da magnitude e fase dos sinais aplicados individualmente aos elementos do arranjo, permitindo assim o ajuste na direção em que se propagam as ondas de radiofrequência irradiadas. Essa técnica permite melhorar a capacidade de cobertura, o aproveitamento de recursos de tempo e frequência e a eficiência energética das comunicações sem fio, proporcionando uma experiência de conectividade aprimorada no 5G (KHWANDAH et al., 2021).

A arquitetura geral do 5G pode ser dividida em rede núcleo (5GC) e rede de acesso por rádio (do inglês, RAN - *Radio Access Network*). A seguir são tratadas algumas das principais considerações na arquitetura de projeto do 5G:

- **Arquitetura Baseada em Serviços** (do inglês, SBA - *Service-Based Architecture*): Os elementos da rede são definidos por um conjunto de serviços acessíveis via funções de rede. Cada função de rede é composta por uma implementação e uma interface baseada em serviço, sendo essa última responsável por definir como as funções se comunicam umas com as outras;

- **Virtualização de Rede**: As funções de rede não estão presas a um hardware específico, elas são totalmente implementadas em software e podem ser executadas em hardware de uso geral. A virtualização permite que as funções estejam centralizadas ou distribuídas, além de simplificar a manutenção da rede e possibilitar expansão ou retração rápida e flexível de recursos e serviços na rede;

- **Separação entre Plano de Controle e Plano de Usuário** (do inglês, CUPS - *Control and User Plane Separation*): Permite a centralização do plano de controle e distribuição do plano de usuário. As funções responsáveis pelo plano de usuário podem ser distribuídas em nós mais próximos dos UEs, permitindo que os dados sejam roteados diretamente para os usuários e os serviços que exigem baixa latência sejam atendidos;

- **Fatiamento de rede** (*Network Slicing*): A rede pode ser subdividida em fatias de rede virtuais que operam em paralelo de acordo com requisitos de qualidade de serviço demandados por cada aplicação.

Na RAN do 5G se pode destacar a presença da gNB, a qual é composta por um conjunto de protocolos (SDAP - *Service Data Adaptation Protocol*, RRC - *Radio Resource Control*, PDCP - *Packet Data Convergence Protocol*, RLC - *Radio Link Control*, MAC - *Medium Access Control*, PHY - *Physical Layer*) responsáveis pelo estabelecimento e continuidade da conexão de radiofrequência com os dispositivos móveis, escalonamento de recursos e gerenciamento da mobilidade (3GPP, 2023f). Já a rede núcleo do 5G, comumente tratada como Core 5G, é composta por um conjunto de funções (por exemplo, AMF - *Access and Mobility Management Function*, SMF - *Session Management Function*, UPF - *User Plane Function*) que são responsáveis por gerenciar dentre outras coisas o acesso, mobilidade, sessão, segurança e dados (3GPP, 2023k). Essas funções trabalham em conjunto para garantir a prestação rápida, flexível e segura dos serviços providos pelo 5G.

As funcionalidade do 5G relacionadas à localização e baseadas nas tecnologias do *New Radio*, foram estabelecidas a partir da *Release* 16 do 3GPP. A arquitetura de serviços de localização melhorada definiu métodos que são uma evolução dos sistemas de posicionamento das redes móveis legadas, porém também foram propostas novas técnicas que exploram *Massive MIMO* e *beamforming*. No core 5G, a AMF é responsável pelo início do serviço de localização no plano de controle, onde a requisição desse serviço é direcionada para função de gerenciamento de localização (do inglês, LMF - *Location Management Function*) (3GPP, 2023a).

O 5G também estabelece um conjunto de requisitos para localização em: serviços baseados em posição (do inglês, LBS - *Location Based Services*), indústria, saúde, emergência, missão crítica, veículos terrestres, marítmos e aéreos. A Tabela 3 resume alguns desses requisitos de posicionamento de acordo com os casos de uso (3GPP, 2023g). Os requisitos se concentraram principalmente em dois indicadores de desempenho: a precisão no ajuste da posição e o tempo até o primeiro ajuste (do inglês, TTFF - *time-to-fisrt-fix*), que é o tempo decorrido até que o resultado do posicionamento esteja disponível.

Tabela 3 – Resumo de requisitos de posicionamento em casos de uso no 5G.

Casos de uso	**Tipo de serviço**	**Precisão da posição**	**TTFF**	**Latência**	**Disponibilidade**
Realidade aumentada	LBS	2m	10s	1s	90%
Notificações de anúncio	LBS	3m	-	60s	99%
Pessoas e dispositivos em hospitais	Saúde	0,2m	10s	1s	99%
Veículos em fábricas	Indústria	0,5m	-	20ms	99%
Chamada de emergência	Emergência	50m	30s	60s	95%
Controle e monitoramento de tráfego	Veículos terrestres	1-3m	10s	30ms	95%
Gerenciamento e rastreio de ativo	Veículos marítmos	1-30m	-	-	99%
Controle remoto de drone	Veículos aéreos	0.5m	-	150ms	99%

Fonte: Adaptada da TR 22.872 (3GPP, 2023j).

2.3.1 Técnicas para localização utilizadas no 5G *New Radio*

Os métodos para localização utilizados em redes celulares, podem ser divididos em dependentes de tecnologias de acesso por rádio (*RAT-dependent*) e independentes de tecnologias de acesso por rádio (*RAT-independent*). A diferença entre as duas abordagens consiste em que as *RAT-dependent* fazem uso dos sinais de rádio transmitidos pela rede celular para atingir seus objetivos, já as *RAT-independent* utilizam outros sinais como GPS, Wi-Fi ou Bluetooth para obter as estimativas de posição. O 5G dá suporte a ambos os métodos, assim como propõe novas tecnologias para aprimoramento de técnicas existentes em redes legadas e implementação de novas (3GPP, 2023i).

O 3GPP classifica as técnicas para localização *RAT-dependent* melhoradas ou novas presentes no 5G, em: baseadas no *downlink* (DL-TDOA e DL-AOD), baseadas no *uplink* (UL-TDOA e UL-AOA), e baseadas em *uplink* e *downlink* (multi-RTT) (3GPP, 2023b).

As soluções que se baseiam em *downlink* consistem em medições realizadas pelos UEs de sinais vindos das gNBs para o cálculo da localização. O DL-TDOA (do inglês, *downlink time-difference-of-arrival*) tem como princípio de funcionamento o TDOA já relatado neste trabalho, assim, os UEs calculam a diferença entre os tempos de chegada dos sinais de referência advindos de diferentes estações base. Já no DL-AOD (do inglês, *downlink angle-of-departure*) os UEs medem os sinais vindos de diferentes feixes e enviam um relatório para a rede, com base nessas informações a estação base devolve informações sobre os feixes medidos, como a direção em que cada feixe foi transmitido (BARTOLETTI, 2023).

As soluções baseadas em *uplink* consistem em uma ou mais gNBs realizarem medições para localização baseadas nos sinais de referência enviados pelos UEs. O UL-TDOA (do inglês, *uplink time-difference-of-arrival*) tem como princípio a medição da diferença entre os tempos de chegada dos sinais de *uplink* dos UEs, as informações coletadas são enviadas para a função LMF do 5GC. Já no UL-AOA (do inglês, *uplink angle-of-arrival*) a estação base define de qual direção estão vindo os sinais de *uplink* dos UEs (BARTOLETTI, 2023).

As soluções baseadas em *uplink* e *downlink*, utilizam ambos os sinais para localizar os UEs. O multi-RTT (do inglês, *multiple round trip time*) consiste em multiplas medições do tempo de propagação dos sinais para ir até os UEs e voltar à gNB. Esse método apresenta maior robustez contra erros de sincronização de tempo na rede (BARTOLETTI, 2023).

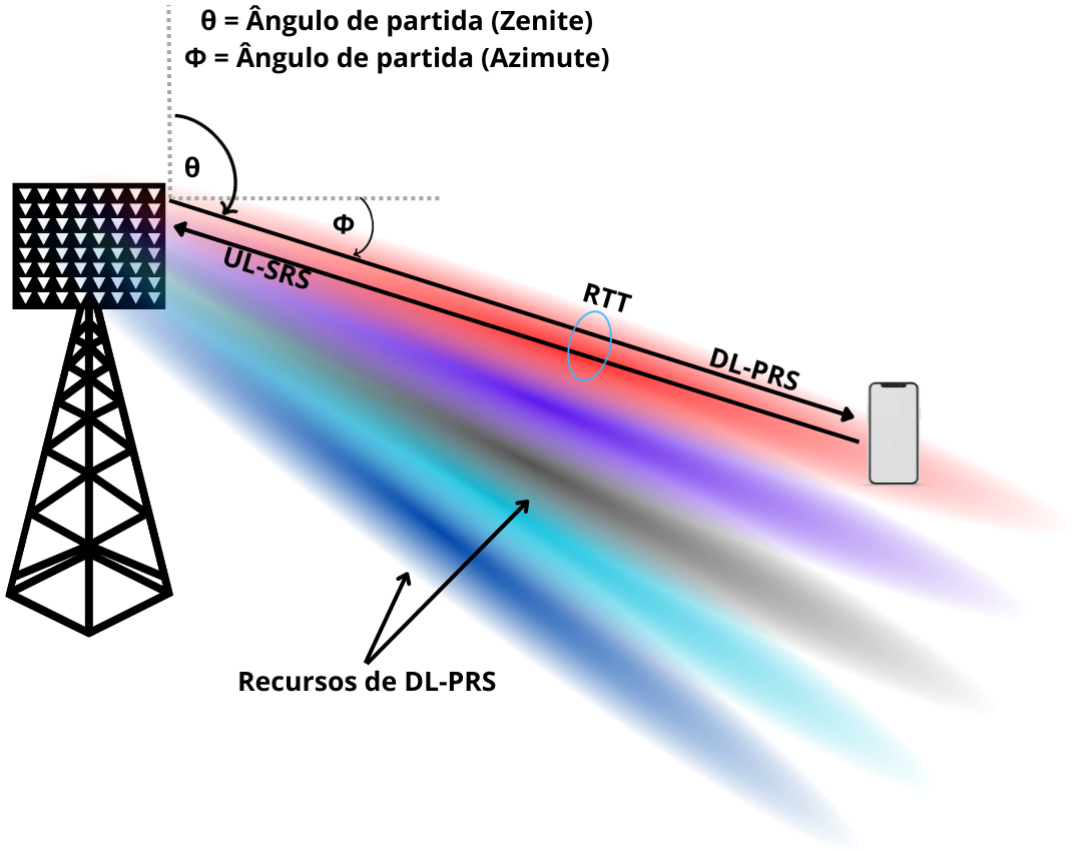
Como relatado nos parágrafos anteriores, as técnicas para localização empregadas no 5G dependem de múltiplos sinais de referência. O *New Radio* dispõe de dois novos sinais de referência, o DL-PRS (do inglês, *downlink positioning reference signal*) e UL-SRS (do inglês,

uplink sounding reference signal). O PRS serve como o principal sinal de referência para métodos de posicionamento baseados em *downlink*, oferecendo altos níveis de precisão, cobertura e atenuação de interferência. Embora outros sinais estejam disponíveis, o PRS é especificamente otimizado para atender a esses requisitos. Para garantir um *design* eficiente do PRS, foi feita uma consideração cuidadosa à sua faixa de atraso de propagação, permitindo a recepção do sinal de estações base vizinhas que podem estar distântes para a estimativa precisa da posição. Isso é obtido com a utilização de toda a largura de banda do 5G e a transmissão do PRS em vários símbolos, os quais podem ser agregados para acumular energia (3GPP, 2023e; 3GPP, 2023d).

Na versão 16 do 3GPP, o SRS foi introduzido para posicionamento na direção do *uplink*. Esse novo sinal aborda dois aspectos específicos do posicionamento. Em primeiro lugar, como o posicionamento envolve medições de várias estações rádio base, o SRS deve ter alcance suficiente para atender a gNB de serviço e as gNBs vizinhas envolvidas no processo de posicionamento. Em segundo lugar, assim como o PRS, o SRS foi projetado para cobrir toda a largura de banda do *New Radio*, com elementos de recursos distribuídos em diferentes símbolos para cobrir todas as subportadoras. Esses aprimoramentos no SRS contribuem para melhorar os recursos de posicionamento nas redes 3GPP (3GPP, 2023e; 3GPP, 2023d). A Figura 4 exemplifica a presença dos sinais de referência em um cenário de conexão. O DL-PRS é empregado para a técnica DL-TDOA, enquanto o UL-SRS é utilizado para a abordagem UL-TDOA. Ambos os sinais desempenham um papel fundamental nas medições multi-RTT e angulares no posicionamento.

A partir dos sinais de referência podem ser calculadas três medidas principais, ângulos de partida e chegada, RSRP (do inglês, *Reference Signal Received Power*) e RSTD (do inglês, *Reference Signal Time Difference*). Assim, como visto na Tabela 4 é possível relacionar cada uma das técnicas de localização usadas no 5G com essas medidas.

Figura 4 – Sinais de referência para localização nas redes 5G.



Fonte: Autoral.

Tabela 4 – Técnicas de localização e medidas correspondentes segundo padrões do 5G.

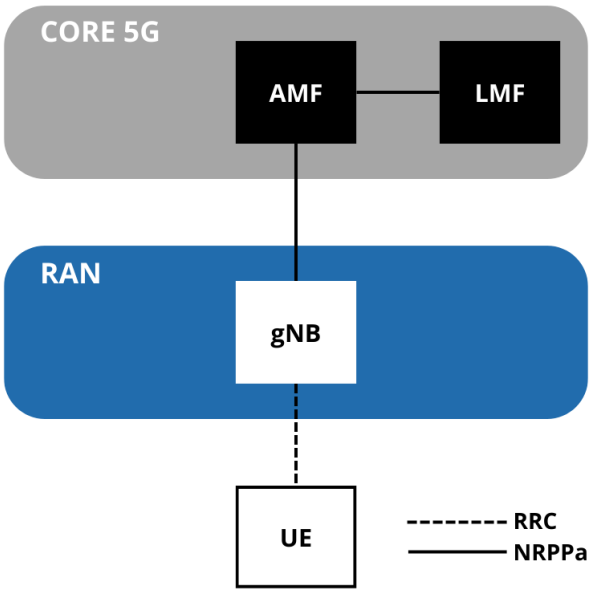
Técnica de localização	**Medida**
DL-TDOA	RSTD, opcional complementar PRS-RSRP
DL-AOD	PRS-RSRP
UL-TDOA	UL-RTOA, opcional complementar SRS-RSRP
UL-AOA	Azimute-AOA, Zenite-AOA, opcional complementar SRS-RSRP
multi-RTT	Diferença de tempo gNB Rx-Tx, UE Rx-Tx, opcional complementar PRS-RSRP, SRS-RSRP, A-AOA, Z-AOA

Fonte: Adaptado de Bartoletti (2023).

É importante também destacar o protocolo que permite toda a troca de informações para localização, sendo utilizado no 5G o NRPPa (do inglês, *New Radio Positioning Protocol a*). Esse protocolo é responsável por cobrir a troca de mensagens entre a RAN e a LMF do

5GC (do inglês, 5G *CORE*), por meio da AMF. A Figura 5 retrata o percurso dos dados do NRPPa na arquitetura de localização do 5G (3GPP, 2023c).

Figura 5 – Protocolo NRPPa na arquitetura do 5G.



Fonte: Autoral.

Portanto, conclui-se que o 5G possui um conjunto aprimorado de técnicas para localização, porém essas no estado atual são incapazes de localizar um dispositivo que não responda aos sinais de referência e protocolos definidos pelo 3GPP. Sendo assim necessárias novas técnicas que utilizem as tecnologias já definidas, entretanto implementando algoritmos capazes de localizar um *jammer*.

3 Estado da arte

Neste capítulo, são apresentadas as abordagens empregadas para localização de dispositivos *jammers*, incluindo as vantagens e desvantagens, focou-se na análise descritiva das soluções propostas de forma a possibilitar a comparação das técnicas em um panorama geral. Também foram apresentados trabalhos sobre detecção de *jammers* e localização em cenários com mobilidade. Ao final de algumas subseções, tem-se uma tabela resumindo as principais contribuições dos trabalhos citados.

3.1 Métodos para localização de dispositivos *jammers*

O bloqueio de sinais por interferência destrutiva, conhecido como *jamming*, é um tipo de ataque de negação de serviço comum nas redes móveis celulares. Essa forma de ataque ocorre quando nós maliciosos deliberadamente interferem na conexão legítima entre os dispositivos móveis e a estação rádio base, resultando na interrupção da conectividade normal. Como resultado, esses ataques têm um impacto significativo no desempenho da capacidade de comunicação dos dispositivos móveis (ALIKH; RAJABZADEH, 2022).

O objetivo dos atacantes nesses ataques é normalmente desconectar os dispositivos móveis das redes legítimas, interrompendo a comunicação e permitindo que redes falsas possam ser disponibilizadas no local. O bloqueio de sinais é considerado um dos ataques mais perigosos, pois impede o funcionamento adequado dos canais de comunicação sem fio ao introduzir pacotes falsificados e sinais que causam interferência destrutiva, restringindo as frequências de comunicação de rádio nas redes celulares (PIRAYESH; ZENG, 2022).

Quando ocorre o bloqueio de sinais em uma área específica, os dispositivos móveis nessa região são incapazes de executar adequadamente suas funções dependentes de comunicação. Além disso, os equipamentos de usuário podem ser forçados a se conectarem à estações radio base falsas, as quais podem ser disponibilizadas maliciosamente no meio aéreo, visando a captura de dados e injeção de informações falsas nos dispositivos conectados. A menos que o bloqueio de sinais seja acidental, como no caso de um dispositivo móvel danificado, qualquer entidade que esteja gerando o bloqueio de sinais pode representar um perigo para os usuários e para o funcionamento eficiente das redes móveis celulares (IRRAM et al., 2022).

O problema de localização passiva de dispositivos emissores de interferência destrutiva possui aplicações nas áreas de processamento de sinais e comunicações sem fio. A precisão na

localização de fontes de RF é essencial para diversas aplicações, incluindo sistemas de transporte inteligentes, rastreamento de usuários móveis, atividades de resgate e sistemas de defesa. Nesse contexto, diversos parâmetros são utilizados, tais como RSS, AoA, TOA, TDOA e combinações híbridas desses métodos (ULUSKAN; FILIK, 2019).

Embora o uso de TDOA e AOA forneça em geral uma maior precisão, as medições de RSS são preferidas em algumas situações, devido à sua menor complexidade computacional e a pouca necessidade de informações sobre o transmissor. Diversas técnicas têm sido desenvolvidas para solucionar o problema de localização com base em medições de RSS. Essas técnicas incluem: (1) mapeamento (*fingerprinting*), que envolve a construção de um modelo que associa valores específicos de RSS a locais conhecidos; (2) técnicas estatísticas, que fornecem estruturas teóricas para lidar com a presença de ruídos nas medições; (3) soluções baseadas em distância, como a trilateração; e (4) soluções geométricas (ZEKAVAT; BUEHRER, 2012). Por exemplo, como poderá ser observado nos trabalhos apresentados nesta seção, redes de sensores sem fio devido ao seu elevado número de receptores e normalmente baixo poder computacional, possuem alta adesão de técnicas geométricas baseadas em RSS. Já estações rádio base do 5G possuem menor número de receptores distribuídos sobre uma área de influência do *jammer*, porém possuem acesso a elevado poder computacional, propiciando que soluções como TDOA E AOA sejam aplicadas.

O mapeamento de RSS apresenta a desvantagem de exigir um grande volume de dados iniciais para treinar o sistema, porém tem se mostrado eficaz em ambientes internos com relações complexas entre distância e valores de RSS. Já as técnicas estatísticas apresentam a desvantagem de não conseguirem capturar de forma adequada as relações complexas entre distância e RSS, devido às limitações de modelos pré-definidos. Embora as soluções geométricas ofereçam abordagens simplificadas, nem sempre são capazes de fornecer a solução ótima em ambientes ruidosos ou imperfeitos.

Em Uluskan e Filik (2019), é apresenta uma solução geométrica para localização de fontes de RF passivas baseada em RSS quando o expoente de perda de caminho (PLE, do inglês "*Path Loss Exponent*") e a potência de transmissão são desconhecidos. O estudo propõe uma nova solução fechada geométrica chamada Direção da Incerteza do Expoente (DEU) para localização de campo distante. A incerteza no PLE devido a fatores ambientais é um desafio significativo para a localização baseada em RSS. A técnica DEU foi construída após uma investigação dos comportamentos geométricos dos círculos diferenciais de força do sinal recebido, ou seja, o locus da possível localização do emissor quando a potência de transmissão é desconhecida. É mostrado que a incerteza no PLE corresponde a uma incerteza linear para a localização do

emissor no espaço bidimensional. Essa observação crítica cria uma base para o sensor se mover em direção ao emissor sem estimar inicialmente a localização. Além disso, com apenas quatro medições distintas, é possível estimar efetivamente a localização do emissor e o PLE por meio da interseção dos DEUs. Os resultados apresentados no artigo indicam que a interseção dos DEUs atinge o limite inferior de Cramer Rao com um tempo de execução reduzido em comparação com o estimador de mínimos quadrados não lineares (ULUSKAN; FILIK, 2019; PATWARI et al., 2003). O DEU também é proposto como uma ferramenta eficiente de planejamento de rota para sensores móveis, como veículos aéreos não tripulados.

Foi encontrada uma abordagem de localização sem fio que é responsiva ao cenário em que apenas um único receptor está disponível para localizar vários alvos de posição desconhecida. A abordagem DE^2 (estimativa de direção e estimativa de distância) é baseada em restrições de direção e distância entre uma posição desconhecida e o único receptor, que são adequadas para determinar a posição desconhecida. Quando uma pessoa gira em torno de um receptor RF, o corpo humano age como um obstáculo de bloqueio de sinal. Isso faz com que o sinal de um transmissor (posição desconhecida) para o receptor único atenue em um certo escopo. O efeito de bloqueio causado pelo corpo humano pode ser utilizado para obter a restrição de direção entre a posição desconhecida e o receptor. Além disso, uma restrição de distância correspondente também é inferida no RSS rotativo de acordo com o modelo de propagação RF. A abordagem DE^2 reduz o limite do número mínimo de receptores necessários para localização sem muitos esforços de pré-configuração. Para demonstrar a utilidade do DE^2, os autores implementaram-no em redes sem fio com um receptor no mundo real. Os resultados mostram que essas aplicações podem se beneficiar significativamente do DE^2 (REN et al., 2016).

Em Aldosari, Zohdy e Olawoyin (2019b), apresenta-se um método para rastreamento de *jammers* móveis em redes de sensores sem fio (WSNs). O método é baseado no Filtro de Kalman Estendido (EKF), um algoritmo de filtro de estado que pode ser usado para estimar o estado de um sistema dinâmico a partir de dados de medição ruidosos. O método proposto divide o problema de rastreamento do *jammer* em duas partes: Estimação da posição do *jammer* com base nas medições dos nós sensoriais; rastreamento do movimento do *jammer* com base na estimativa de posição.

A posição do *jammer* é estimada usando o EKF, que leva em consideração os dados de medição dos nós sensoriais e um modelo do movimento do *jammer*. O modelo do movimento do *jammer* é baseado na suposição de que o *jammer* se move em uma linha reta com velocidade constante. O movimento do *jammer* é rastreado usando um algoritmo de rastreamento de estado, que leva em consideração a estimativa de posição do *jammer* e o modelo do movimento

do *jammer*. O algoritmo de rastreamento de estado estima a posição do *jammer* no futuro, com base na posição atual do *jammer* e no modelo do movimento do *jammer*. O método proposto foi avaliado em uma simulação de uma WSN com 100 nós sensoriais. Os resultados da simulação mostraram que o método proposto é capaz de rastrear com sucesso *jammers* móveis com alta precisão.

O método proposto tem as seguintes vantagens: é capaz de rastrear *jammers* móveis com alta precisão; é eficiente em termos computacionais; pode ser facilmente implementado em *hardware*; robustez a ruídos nos dados de medição; capacidade de lidar com mudanças na velocidade do *jammer*; capacidade de lidar com *jammers* múltiplos. Também existem algumas desvantagens no método apresentado no artigo. Primeiro, o método é baseado na suposição de que o *jammer* se move em uma linha reta com velocidade constante. Esta suposição pode não ser válida em todos os casos, por exemplo, se o *jammer* estiver mudando de direção ou de velocidade com frequência. Segundo, o método requer um número suficiente de nós sensoriais para fornecer medições precisas da posição do *jammer*. Se o número de nós sensoriais for insuficiente, o método pode não ser capaz de rastrear o *jammer* com precisão. Por fim, se o ruído nos dados de medição for muito alto, o método pode não ser capaz de rastrear o *jammer* com precisão.

O método proposto é uma ferramenta útil para a segurança de WSNs, podendo ser usado para proteger WSNs contra uma variedade de ataques, incluindo ataques de *jammers* móveis. O método é eficiente em termos computacionais e pode ser facilmente implementado em *hardware*.

Visto que os algoritmos tradicionais de localização apresentam falta de precisão em cenários complexos, alguns pesquisadores propuseram técnicas de otimização que podem melhorar a precisão da localização (ex. algoritmos genéticos, algoritmos de pesquisa gravitacional, redes neurais e aprendizado profundo). No entanto, essas técnicas exigem *hardware* adicional para realizar seus cálculos complexos. Por outro lado, algoritmos mais simples, como *Virtual Force Iteration Localization* (VFIL), *Weighted Centroid Localization* (WCL) e *Centroid Localization* (CL), são menos precisos.

Para preencher essa lacuna, observou-se um algoritmo que se propõe a localizar com precisão as coordenadas do *jammer*. O mesmo consiste em três fases: Detectando um ataque de interferência - isso é feito verificando se as intensidades de sinal recebidas (RSS) estão todas abaixo de um limiar; desenhando a região bloqueada - isso é realizado conectando os nós com as menores intensidades de sinal recebidas; localizando o *jammer* - Isso é feito encontrando o nó com a menor intensidade de sinal recebida e utilizando uma técnica chamada *convex-hull*

para calcular o círculo mínimo circunscrito (MCC) de um conjunto de pontos. O algoritmo proposto é leve e não requer nenhum *hardware* adicional. Ele também é mais preciso do que algoritmos mais simples, como VFIL, WCL e CL (ALIKH; RAJABZADEH, 2022).

Em Niu et al. (2020), são analisados métodos de localização de *jammers* em redes de sensores sem fio (WSNs). Como os nós em WSNs são geralmente alimentados por baterias, eles não são geralmente equipados com componentes que podem medir RSSI, TOA, TDOA e AOA dos sinais do *jammer*. Além disso, devido à influência do *jammer*, é quase impossível para os nós localizados na área de *jamming* se comunicarem uns com os outros. Isso significa que os nós bloqueados não podem cooperar uns com os outros para realizar a localização do *jammer*, mesmo que todos os nós estejam equipados com componentes de posicionamento.

Foram propostas uma variedade de métodos para alcançar a localização do *jammer* apenas com base nas informações de localização do nó bloqueado. Métodos típicos incluem *centroid localization* (CL), *weighted centroid localization* (WCL), *minimum enclosing rectangle center localization* (MERCL) e *minimum enclosing circle center localization* (MECCL).

O artigo analisa o princípio de posicionamento e o processo dos métodos relacionados, resume as vantagens e desvantagens dos diferentes métodos e compara a precisão de posicionamento dos diferentes métodos através de experimentos. Os resultados experimentais mostram que o resultado de localização do *jammer* obtido com base no MECCL é mais preciso do que usar CL, WCL, MERCL. E o algoritmo *catch the jammer* (CJ) é melhor que *virtual force iteration localization* (VFIL). Os autores propõem estudar um método de localização aprimorado baseado no MECCL como trabalho futuro.

Alguns métodos propõem a localização de múltiplos *jammers* e se baseiam no algoritmo de busca gravitacional (GSA - do inglês, *Gravitational Search Algorithm*), que é um algoritmo evolutivo de otimização heurística baseado na lei da gravitação universal de Newton e nas interações de massa. Inicialmente, as partículas iniciais são selecionadas aleatoriamente da área bloqueada. Em seguida, a função de aptidão é projetada com base no método de alcance livre. Em cada iteração, a massa e a posição das partículas são atualizadas. Finalmente, a posição da partícula com a massa máxima é considerada como a posição estimada do *jammer* (WEI; WANG, 2021; WANG et al., 2018d). Observou-se uma boa precisão no método, porém ele pode ser lento devido ao grande número de interações para atingir a convergência, é sensível ao ruído e devido a sua complexidade de implementação pode não ser viável para cenários onde os recursos de hardware são escassos.

Foi observado também um método de localização que propõe o cálculo da relação de distância (DR - do inglês, *Distance Ratio*) com base na SNR. O algoritmo, chamado de *Distance*

to Signal Noise Ratio (DSNR), consiste de quatro etapas: capturar a intensidade do sinal do *jammer* (JRSS) e calcular a potência recebida entre o nó de fronteira e seu vizinho, calcular DR, estimar a potência de transmissão do *jammer* e sua localização, e por fim minimizar o erro de localização. Os autores realizaram simulações e demonstraram que a partir do erro médio o DSNR possui melhor performance que o WCL, CL, e FVIL, além de localizar o *jammer* com precisão (ALDOSARI; ZOHDY; OLAWOYIN, 2019a).

Mariappan e Selvakumar (2021) apresentam uma solução de localização *Anti-jammer* com Localizador Estimado Conhecido (KNOWEL). A abordagem consiste de um detector de energia que é usado para definir o limiar de decisão, já em seguida um filtro adaptativo é utilizado para discriminar as diferenças entre o tráfego normal e o de *jammer* reativo, e por fim, o KNOWEL detecta o *jammer* e sua localização exata aprendendo o perfil do atacante. O algoritmo de localização é baseado em CL .

Em Wang et al. (2018e), um esquema de localização e rastreamento de *jammer* móvel é apresentado, o qual contém quatro etapas, ou seja, seleção de nós de monitoramento inicial, determinação de nós cooperativos, localização por trilateração e transferência do grupo de monitoramento. O algoritmo é baseado na intensidade do sinal recebido do *jammer*. Também foi observada técnica que propõe um método de rastreamento de *jammer* móvel baseado em vetor móvel. Nesse método, quando o *jammer* móvel está ativo, a posição inicial do *jammer* pode ser obtida por qualquer algoritmo de localização de *jammer*. Em seguida, um vetor móvel aproximado do *jammer* é calculado a cada momento seguinte (PANG et al., 2017).

Foram observados também métodos para localização de *jammers* que fazem: uso de *tags* de sensores de identificação por radiofrequência (RFID)(HUSSAIN et al., 2022); uso da intensidade do sinal do *jammer* para localizá-lo em redes veiculares (ALMOMANI et al., 2022; HUSSAIN et al., 2023); uso da intensidade do sinal do *jammer* e filtro de Kalman para localizá-lo com o auxílio de drones em cenários de *smart grid* (ZHANG et al., 2019); uso de análise de séries temporais (MLTSA) para algoritmo de localização de *multijammers* (WANG et al., 2018a); uso de uma estrutura algorítmica baseada em fatoração aproximada, filtragem espacial baseada em densidade local e estimativa de máxima verossimilhança (KRISHNAMURTHY; KHORRAMI; KUMAR, 2021; WEI et al., 2018); uso de algorítmo adaptativo que seleciona um dos métodos: localização por centroide (CL), localização por Iteração de Força Virtual (VFIL) ou algoritmo de busca gravitacional aprimorado (IGSA) (WANG et al., 2018c); uso de algoritmos robustos de detecção paralela com base na Curtose e na Transformada Fracionária de Fourier (FRFT)(JAGANNATH; JAGANNATH, 2020); uso de soma cumulativa (CUSUM), que é conhecido por ser ideal para uma formulação de detecção de ponto de alteração estatística

não bayesiana, e realiza a localização usando diferença de tempo de detecção (CHOI et al., 2018); uso da intensidade do sinal recebido e métodos geométricos para localização de *jammers* direcionais (WANG et al., 2018b); uso de sensoriamento compressivo e modelagem do problema de posicionamento como reconstrução de vetor esparso em blocos (YADAV et al., 2023); uso de *Fibonacci Branch Search* (FBS) (YANG et al., 2023).

Tabela 5 – Síntese dos trabalhos encontrados na revisão da literatura

Título	**Autor**	**Ano**	**Técnica**	**Características**	**Sinal**
DE²: localization based on the rotating RSS using a single beacon	Ren et al.	2016	Baseada em RSS. DE² - estimativa de direção e estimativa de distância baseadas na rotação de corpo em torno do receptor.	Único receptor. A estimativa pode ser lenta.	Real.
Tracking the Mobile Jammer Continuously in Time by Using Moving Vector	Pang et al.	2017	Baseada em vetor móvel.	Localiza *jammers* móveis. Necessita de número elevado de receptores.	Simulado.
Mobile jammer localization and tracking in multi-hop wireless network	Wang et al.	2018	Baseada em RSS e trilateração.	Alta precisão. Baixo custo computacional. Necessita de cooperação entre os receptores.	Simulado.
Sequential opening multi-jammers localization in multi-hop wireless network	Wang et al.	2018	Baseada no uso de análise de séries temporais (MLTSA).	Localiza múltiplos *jammers*. Necessita de número elevado de receptores.	Simulado.

Continua na próxima página

Tabela 5 – Continuação

Título	**Autor**	**Ano**	**Técnica**	**Características**	**Sinal**
Collaborative mobile jammer tracking in Multi-Hop Wireless Network	Wei et al.	2018	Estrutura algorítmica baseada em fatoração aproximada,filtragem espacial baseada em densidade local e estimativa de máxima verossimilhança.	Localiza *jammers* móveis. Necessita de número elevado de receptores.	Simulado.
Adaptive jammer localization in wireless networks	Wang et al.	2018	Utiliza algoritmo adaptativo que seleciona um dos métodos: localização por centroide (CL), localização por Iteração de Força Virtual (VFIL) ou algoritmo de busca gravitacional aprimorado (IGSA).	Localiza *jammers* omnidirecionais e direcionais. Necessita de número elevado de receptores e possui elevado custo computacional.	Simulado.

Continua na próxima página

Tabela 5 – Continuação

Título	**Autor**	**Ano**	**Técnica**	**Características**	**Sinal**
CUSUM-based Joint Jammer Detection and Localization	Choi et al.	2018	Utiliza soma cumulativa (CUSUM), que é conhecido por ser ideal para uma formulação de detecção de ponto de alteração estatística não bayesiana, e realiza a localização usando diferença de tempo de detecção.	Detecta e localiza os *jammers*. Necessidade de um centro para fusão dos dados.	Simulado.
Localization of Directional Jammer in Wireless Sensor Networks	Wang et al.	2018	Uso da intensidade do sinal recebido e métodos geométricos.	Localiza *jammers* direcionais. Não apresenta solução para jammers omnidirecionais.	Simulado.
Jammer Localization in Multihop Wireless Networks Based on Gravitational Search	Wang et al.	2018	*Gravitational Search Algorithm* (GSA). Algoritmo evolutivo de otimização heurística baseado na lei da gravitação universal de Newton e nas interações de massa.	Reduz a sensibilidade à distribuição de nós e aos parâmetros do *jammer*. Algoritmo possui elevada complexidade.	Simulado.

Continua na próxima página

Tabela 5 – Continuação

Título	**Autor**	**Ano**	**Técnica**	**Características**	**Sinal**
A geometrical closed form solution for RSS based far-field localization: Direction of Exponent Uncertainty	Seçkin Uluskan & Tansu Filik	2019	Baseada em RSS. Direção da Incerteza do Expoente (DEU) para localização de campo distante.	Útil quando PLE e Ptx são desconhecidos. Único receptor móvel. Solução com elevado custo econômico.	Simulado.
Tracking the Mobile Jammer in Wireless Sensor Networks Using Extended Kalman Filter	Aldosari; Zohdy; Olawoyin	2019	Baseada em RSS. Baseado no Filtro de Kalman Estendido (EKF).	Alta precisão. Baixo custo computacional. Robustez a ruídos. Modelo baseado em movimento retilíneo constante. Requer número elevado de receptores.	Simulado.
JamCatcher: A mobile jammer localization scheme for advanced metering infrastructure in smart grid	Zhang et al.	2019	Uso da intensidade do sinal do *jammer* e filtro de Kalman para localizá-lo com o auxílio de drones em cenários de *smart grid.*	Localiza *jammers* móveis. Algoritmo possui elevada complexidade.	Real e Simulado.

Continua na próxima página

Tabela 5 – Continuação

Título	**Autor**	**Ano**	**Técnica**	**Características**	**Sinal**
Jammer Localization Through Smart Estimation of Jammer's Transmission Power	Aldosari; Zohdy; Olawoyin	2019	Baseada em RSS. Distance to Signal Noise Ratio (DSNR).	Possui melhor precisão e performance que WCL e CL. Requer elevado número de receptores.	Simulado.
Overview of Jammer Localization in Wireless Sensor Networks	Niu et al.	2020	Compara os métodos: Centroid Localization (CL), Weighted Centroid Localization (WCL), Minimum Enclosing Rectangle Center Localization (MERCL) e Minimum Enclosing Circle Center Localization (MECCL).	MECCL é o mais preciso entre os métodos propostos.	Simulado.

Continua na próxima página

Tabela 5 – Continuação

Título	**Autor**	**Ano**	**Técnica**	**Características**	**Sinal**
A Novel Location Pinpointed Anti-Jammer with Knowledged Estimated Localizer for secured Data Transmission in Mobile Wireless Sensor Network	Mariappan; Selvakumar	2021	Baseado em Centroid Localization (CL) e filtro adaptativo. Knowledged Estimated Localizer (KNOWEL).	Robustez a ruídos. Aumenta a segurança na transmissão.	Simulado.
AIGSA-based multi-jammer localization in wireless networks	Wei; Wang	2021	Gravitational Search Algorithm (GSA). Algoritmo evolutivo de otimização heurística baseado na lei da gravitação universal de Newton e nas interações de massa.	Alta precisão. Localiza múltiplos jammers. Pode ser lento devido ao grande número de iterações para atingir a convergência. Alto custo computacional.	Simulado.

Continua na próxima página

Tabela 5 – Continuação

Título	**Autor**	**Ano**	**Técnica**	**Características**	**Sinal**
An approximate factorization approach to multi-jammer location and range estimation from peer-to-peer connectivity measurements	Prashanth Krishnamurthy and Farshad Khorrami and Rahul Kumar	2021	Uso de uma estrutura algorítmica baseada em fatoração aproximada, filtragem espacial baseada em densidade local e estimativa de máxima verossimilhança.	Localização de Jammers em cenários de operações militares. A precisão depende do número de comunicações ponto a ponto entre diferentes dispositivos.	Simulado.
Energy-Harvesting Based Jammer Localization: A Battery-Free Approach in Wireless Sensor Networks	Hussain et al.	2022	Uso de tags de sensores de identificação por radiofrequência (RFID).	Não necessita de bateria nos sensores. A área de ataque precisa estar coberta pelas etiquetas RFID.	Simulado.

Continua na próxima página

Tabela 5 – Continuação

Título	**Autor**	**Ano**	**Técnica**	**Características**	**Sinal**
An Efficient Localization and Avoidance Method of Jammers in Vehicular Ad Hoc Networks	Almomani et al.	2022	Usa a intensidade do sinal do *jammer* para estimar apenas a distância entre o jammer e o receptor, enquanto um algoritmo menos complexo é proposto para localizar o jammer e, em seguida, redirecionar os veículos para longe das estradas que o atacante está usando.	Localiza *jammers* em redes veiculares. Foca apenas no cenário de redes veiculares.	Simulado.
Using a lightweight security mechanism to detect and localize jamming attack in wireless sensor networks	Alikh; Rajabzadeh	2022	Baseada em RSS. Utiliza envoltória convexa para calcular o círculo mínimo circunscrito (MCC) de um conjunto de pontos.	Leve e preciso. Requer elevado número de receptores.	Simulado.

Continua na próxima página

Tabela 5 – Continuação

Título	**Autor**	**Ano**	**Técnica**	**Características**	**Sinal**
Jammer Localization in the Internet of Vehicles: Scenarios, Experiments, and Evaluation	Hussain et al.	2023	Baseada em RSS. Desenvolve uma solução que minimiza o erro de localização do *jammer* com base em um conjunto de antenas implantadas no veículo.	Localiza *jammers* em redes veiculares. Necessita de veículos com arranjo de antenas instalado.	Simulado.
Probabilistic Scheme for Intelligent Jammer Localization for Wireless Sensor Networks	Yadav et al.	2023	Baseada na teoria de sensoriamento compressivo, o problema de posicionamento é modelado como um problema de reconstrução de vetor esparso em blocos.	Realiza a estimativa da posição de múltiplas fontes de interferência e melhora a vida útil da rede quando a potência da fonte de interferência é desconhecida e muda.	Simulado.
Jammer Location-Aware Method in Wireless Sensor Networks Based on Fibonacci Branch Search	Yang et al.	2023	Baseada em *Fibonacci Branch Search* (FBS).	Maior precisão e menor sensibilidade à distribuição dos nós e aos parâmetros do jammer, respectivamente.	Simulado.

4 Metodologia

Neste capítulo, descreve-se a metodologia adotada para alcançar os objetivos desta dissertação. A metodologia está organizada em duas categorias: procedimentos práticos, nos quais são detalhados os materiais e métodos utilizados para a medição dos sinais do *jammer*; e procedimentos computacionais, que abordam as técnicas empregadas para a obtenção das diferenças de tempo de chegada dos sinais e a estimação da localização do dispositivo.

Na seção de procedimentos práticos, são apresentadas análises detalhadas dos materiais e métodos empregados na medição dos sinais provenientes do *jammer*. Esta abordagem inclui descrições minuciosas dos instrumentos utilizados, assim como os procedimentos específicos adotados para as medições. A relevância desses procedimentos práticos é destacada no sentido de garantir a obtenção de dados precisos e confiáveis.

Na segunda categoria, os procedimentos computacionais são delineados, apresentando as técnicas utilizadas para calcular as diferenças de tempo de chegada dos sinais e para estimar a localização do dispositivo. São explorados algoritmos e ferramentas computacionais específicas, proporcionando uma visão abrangente do processo analítico adotado. Destaca-se a importância desses procedimentos no contexto da abordagem metodológica, ressaltando sua contribuição para a consecução dos objetivos propostos.

Ao integrar e apresentar em detalhes os procedimentos práticos e computacionais, busca-se estabelecer uma metodologia abrangente que não apenas forneça resultados robustos, mas também assegure a replicabilidade e validade das análises realizadas. Este capítulo visa apresentar a base utilizada para a condução do estudo, fundamentando as escolhas metodológicas e delineando os passos essenciais para alcançar os resultados esperados.

4.1 Procedimentos práticos

Estão descritos neste capítulo os procedimentos práticos que foram empenhados no desenvolvimento desta dissertação.

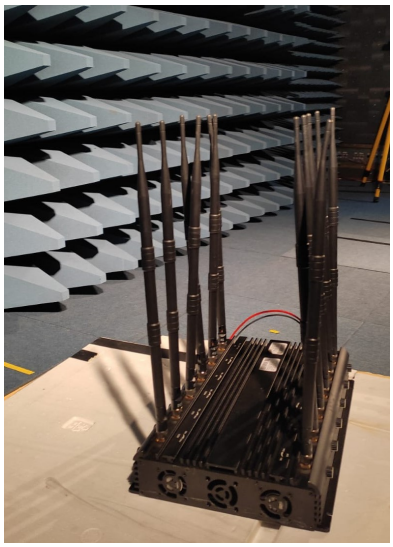
4.1.1 Equipamento *jammer*

Os experimentos para captura do sinal foram realizados com um equipamento *jammer* cedido pela Anatel. O mesmo foi apreendido em uma ação da agência e após todo o trâmite

legal, então direcionado para o presente estudo. Na Figura 6, observa-se o dispositivo, suas antenas omnidirecionais, e indicação das faixas de operação. A intensidade do sinal irradiado em cada faixa pode ser ajustada por meio do uso do potenciômetro correspondente a ela, como destacado na Figura 7.

Figura 6 – Equipamento *jammer* disponibilizado pela Anatel.

(a) Equipamento em ambiente de testes.



Fonte: Autoral.

(b) *Faixas de operação do dispositivo.*

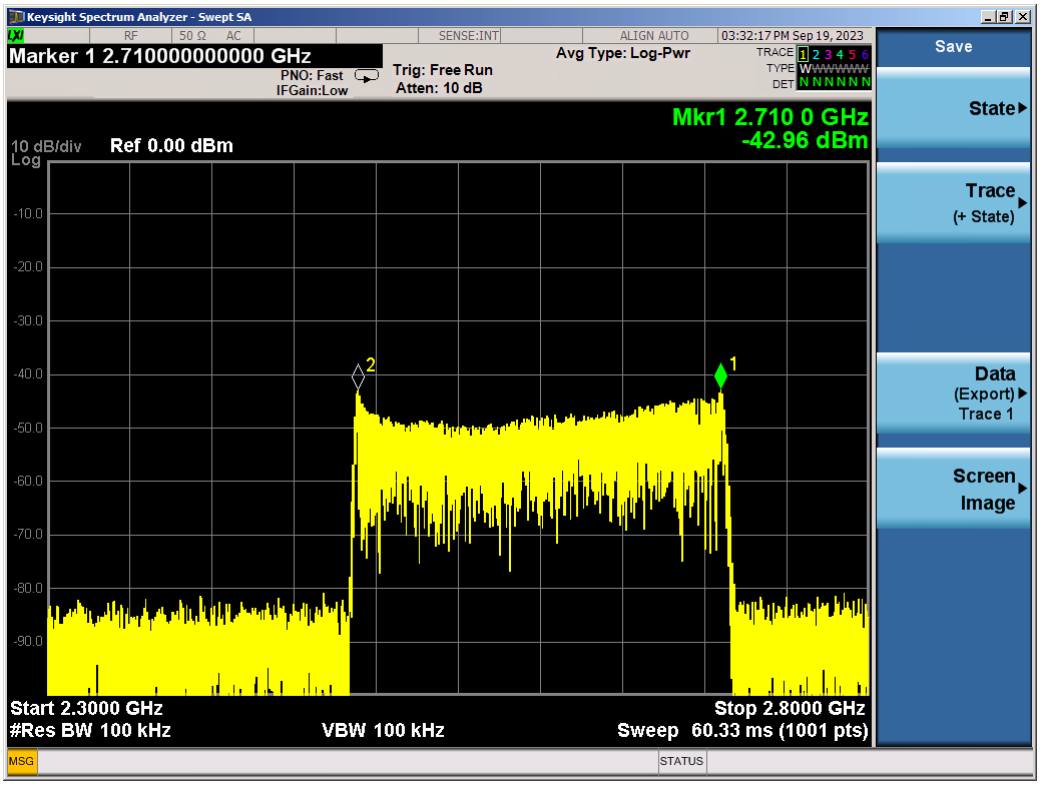
Fonte: Autoral.

Figura 7 – Potenciômetro para ajuste da intensidade do sinal irradiado.

Fonte: Autoral.

Na fase preliminar de estudos com o equipamento, foram realizadas medições em uma câmara semi-anecoica com um analisador de espectro em cada faixa de operação do *jammer*, visando-se compreender as características do sinal irradiado no meio. A Figura 8 é um exemplo de captura realizada, vale salientar que foi utilizado um atenuador de 20 dB na medição, cujo papel fora garantir a preservação da integridade do equipamento de medição, reduzindo o risco de queima desse.

Figura 8 – Captura do analisador de sinais para a faixa 4G do *jammer* com potência máxima.



Fonte: Autoral.

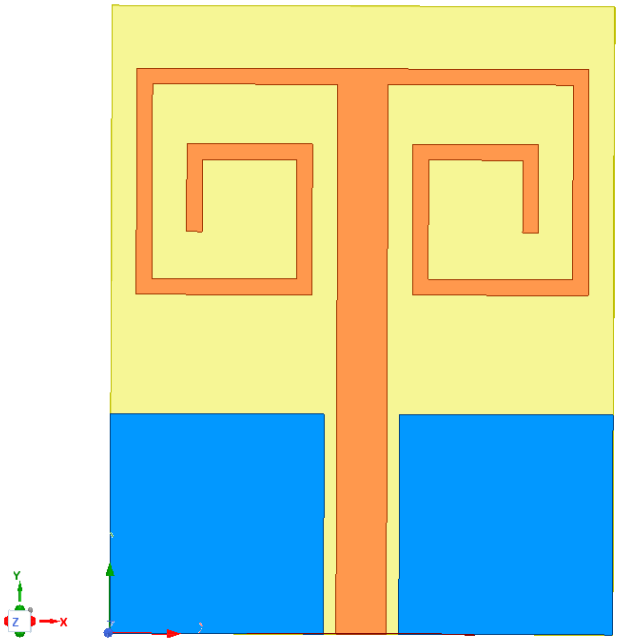
4.1.2 Projeto da antena

Devido à necessidade de quatro antenas com características similares para captura do tempo de chegada do sinal do *jammer*, decidiu-se pelo projeto dessas para a faixa 4G1 (693,78 MHz - 810,64 MHz) do equipamento. Após testes com diferentes geometrias e configurações de antenas, optou-se pelo ajuste do projeto de uma antena coplanar *waveguide* (CPW). Variou-se os parâmetros da antena CPW no ANSYS High-Frequency Structural Simulator (HFSS) e os melhores resultados de simulação obtidos foram os seguintes: faixa de operação em 696–790 MHz com coeficiente de reflexão < -10 dB. A antena, com dimensões do substrato de 50 mm (comprimento) $\times$ 40 mm (largura) x 1,6 mm (altura), e testada em um Agilent Technologies E5071C *Vector Network Analyzer* (VNA), exibiu características de irradiação omnidirecional

em toda a largura de banda de impedância e um coeficiente de reflexão de -35,14 dB a 780,43 MHz. A antena pode ser observada na Figura 9 e o seu S11 na Figura 10.

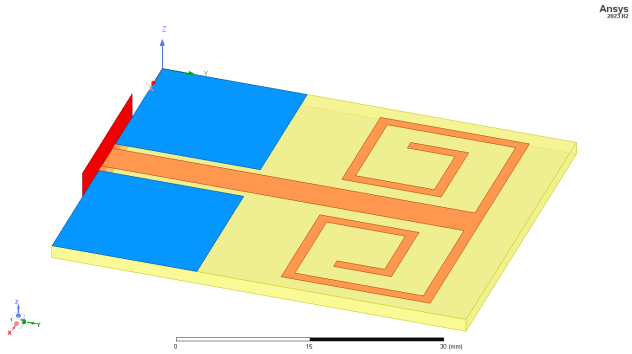
Figura 9 – Antenas para recepção do sinal do *jammer*.

(a) Vista frontal da antena CPW simulada.



Fonte: Autoral.

(b) Antena CPW simulada.

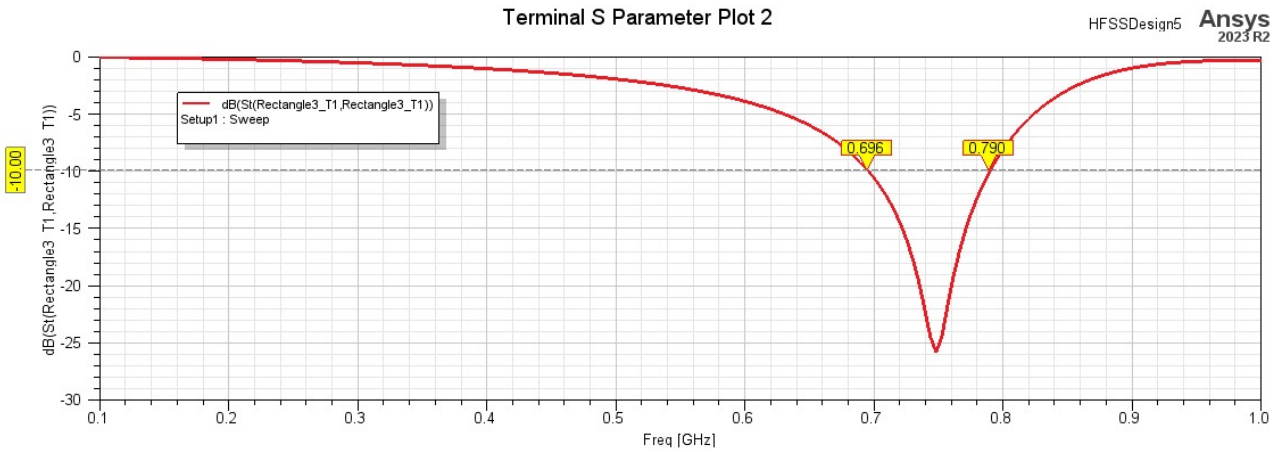


Fonte: Autoral.

4.1.3 Osciloscópio utilizado

Para captura dos sinais que serão utilizados para cálculo da TDOA, foi empregado o osciloscópio da Figura 11 (Tektronix MDO3104), que possui largura de banda de 1 GHz e taxa de amostragem de 5 GSa/s (para um único canal). Foram utilizados três canais para recepção dos sinais das antenas, e fora configurado um limiar de disparo para detecção da chegada

Figura 10 – Coeficiente de reflexão da antena simulada (S11).



Fonte: Autoral.

dos mesmos. Esse último foi ajustado de forma que outros sinais presentes no ambiente não causassem o disparo acidental do gatilho.

O *jammer* operou na faixa de 700 MHz durante os testes, para que, dada a taxa de amostragem supracitada do osciloscópio, pudesse-se satisfazer uma margem bem maior que a exigida pelo teorema de Nyquist-Shannon. Dessa forma, evitando erros na localização provenientes de uma taxa de amostragem insuficiente do osciloscópio.

Figura 11 – Osciloscópio que será utilizado para captura do sinal do *jammer*.

Fonte: Autoral.

4.1.4 Metodologia para localização do *jammer*

Os testes de localização realizados consistiram na verificação da integridade dos cabos, preparação de um arranjo experimental (construção de uma malha de coordenadas, posicionamento dos receptores e do *jammer* na malha, conexão e configuração do osciloscópio), registro das amostras, tratamento dos dados capturados, aplicação do algoritmo de localização e análise dos resultados. A seguir, esses passos serão descritos com maiores detalhes.

4.1.4.1 Verificação da integridade dos cabos

Visando garantir o conhecimento sobre as fontes de possíveis erros no experimento, aplicou-se um procedimento de verificação da integridade dos cabos utilizados no arranjo. A importância de tal procedimento reside no fato de que discrepâncias elevadas na impedância dos cabos ou falhas na integridade física ao longo dos mesmos podem causar resultados incoerentes ou erros elevados na localização.

Para execução do teste foi utilizado o Analisador FieldFox N9918AU da Keysight, em sua função de número 215. Essa corresponde a medidas de TDR (*Time Domain Reflectometry*), que serão utilizadas para caracterizar a integridade e as propriedades dos cabos, incluindo a identificação de falhas, descontinuidades e a medição de impedância (Keysight Technologies, 2024).

Aqui estão os passos básicos para usar o TDR na caracterização de cabos, considerando a resistividade linear (ρ) e a resistência (Ω):

1. Configuração do Equipamento
    - Conectar o cabo ao equipamento de TDR;
    - Certificar-se de que o TDR está calibrado corretamente com uma carga.
2. Envio do Pulso
    - O equipamento de TDR envia um pulso elétrico curto através do cabo.
3. Reflexão do Pulso
    - À medida que o pulso se propaga pelo cabo, qualquer descontinuidade (como uma junção de impedância, falha ou mudança na geometria do cabo) refletirá parte do sinal de volta ao equipamento de TDR.
4. Medição do Tempo de Reflexão

- O TDR mede o tempo que leva para o pulso refletido retornar ao dispositivo. Esse tempo é usado para calcular a localização da descontinuidade no cabo;
- O tempo de ida e volta (t) é relacionado à distância (d) pela fórmula:

$$d = \frac{v \cdot t}{2} \tag{4.1}$$

onde v é a velocidade de propagação do pulso no cabo.

5. Análise das Reflexões Analisando a amplitude e a forma das reflexões, você pode determinar a natureza da descontinuidade. Por exemplo:
   - Uma reflexão positiva pode indicar uma junção de impedância maior;
   - Uma reflexão negativa pode indicar uma junção de impedância menor.
6. Cálculo da Impedância Característica (Z_0)
   - A impedância característica do cabo pode ser determinada pela relação entre a tensão do pulso incidente (V_i) e a tensão do pulso refletido (V_r):

$$Z_0 = Z_{\text{cabo}} \cdot \left(\frac{1+\delta}{1-\delta} \right) \tag{4.2}$$

onde $\delta = \frac{V_r}{V_i}$ é o coeficiente de reflexão.

7. Considerações de Resistividade Linear (ρ) e Resistência (Ω)
   - A resistividade linear do material do cabo (ρ) e a resistência total (Ω) ao longo do comprimento do cabo podem ser usadas para calcular perdas e atenuações ao longo do cabo;
   - A resistividade linear ρ é dada pela fórmula:

$$\rho = \frac{R \cdot A}{L} \tag{4.3}$$

onde R é a resistência medida, A é a área da seção transversal do cabo, e L é o comprimento do cabo.

4.1.4.2 Arranjo experimental

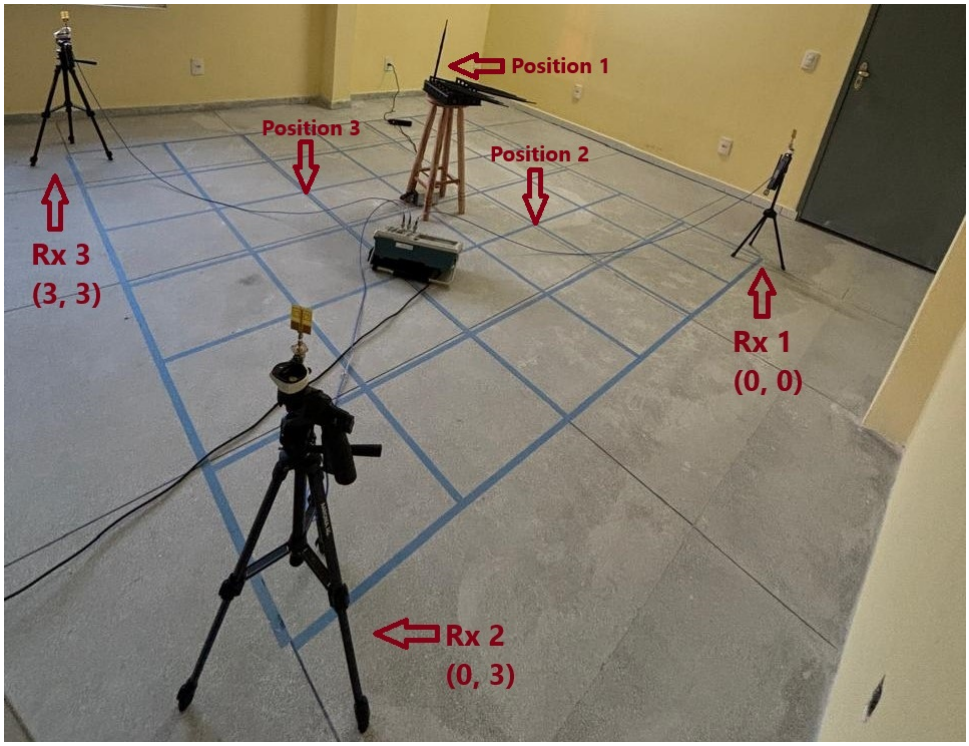
Utilizou-se o maior ambiente interno vazio disponível para montagem de um arranjo. As antenas receptoras foram colocadas nas extremidades da malha quadrada com perímetro de 12 m, foram então utilizados quadrados menores com 50 cm de lado para mapear a localização real do *jammer*. A malha pode ser observado a seguir na Figura 12.

Figura 12 – Malha 3 m por 3 m construída para execução do experimento.

Fonte: Autoral.

O *jammer* foi alocado em 3 posições diferentes da malha. Em cada uma dessas posições foram realizadas três medições simultaneamente dos instantes de chegada do sinal nos receptores. A seguir, pode-se observar na Figura 13 o arranjo completo utilizado para as medições.

Figura 13 – Arranjo experimental utilizado para as medições.



Fonte: Autoral.

A taxa de amostragem máxima de 2,5 GS/s (taxa máxima para captura em canais simultâneos) do osciloscópio configurado (Tektronix MDO3104) em três canais, com 10 M de amostras por captura, foi mais de três vezes a frequência do sinal capturado, o que segundo o teorema de Nyquist, é o suficiente para localizar com precisão o tempo de chegada da primeira frente de onda do sinal do *jammer*. A opção de disparo único foi selecionada, e o nível de tensão foi ajustado para que as transmissões do *jammer* com o potenciômetro em zero não o acionassem - verificado na câmara semi-anecoica. O experimento foi realizado uma vez que um limite estável de 34 mV foi encontrado para garantir que o osciloscópio só acionaria com potência aplicada a uma das bandas do *jammer*.

Com o *jammer* a 1.5 e 1.5 metros (x, y) nas coordenadas, antenas receptoras em (0.0, 0.0), (0.0, 3.0) e (3.0, 3.0), a potência de transmissão foi ajustada para o intervalo proposto, acionando e capturando a frente de onda. Os dados foram salvos em mídia externa para processamento posterior. Este procedimento foi repetido em (1.0, 1.0) e (2.5, 1.5).

4.2 Procedimentos computacionais

Os dados do sinal do *jammer* adquiridos foram processados em um computador para estimativa da localização, o que pode ser sintetizado no fluxograma da Figura 14.

Inicialmente foi realizada a leitura dos dados do sinal do *jammer*. Em seguida, foi aplicado o algoritmos TDOA para localização. Para obtenção da TDOA foram utilizadas as ToAs de cada sinal, que foram calculadas a partir dos algoritmos descritos na Subseção 2.2.1.1, mais especificamente correlação cruzada entre os sinais, e posteriormente aplicadas nas Equações 2.10 e 2.11. Enfim, a localização foi determinada por um método de otimização numérico.

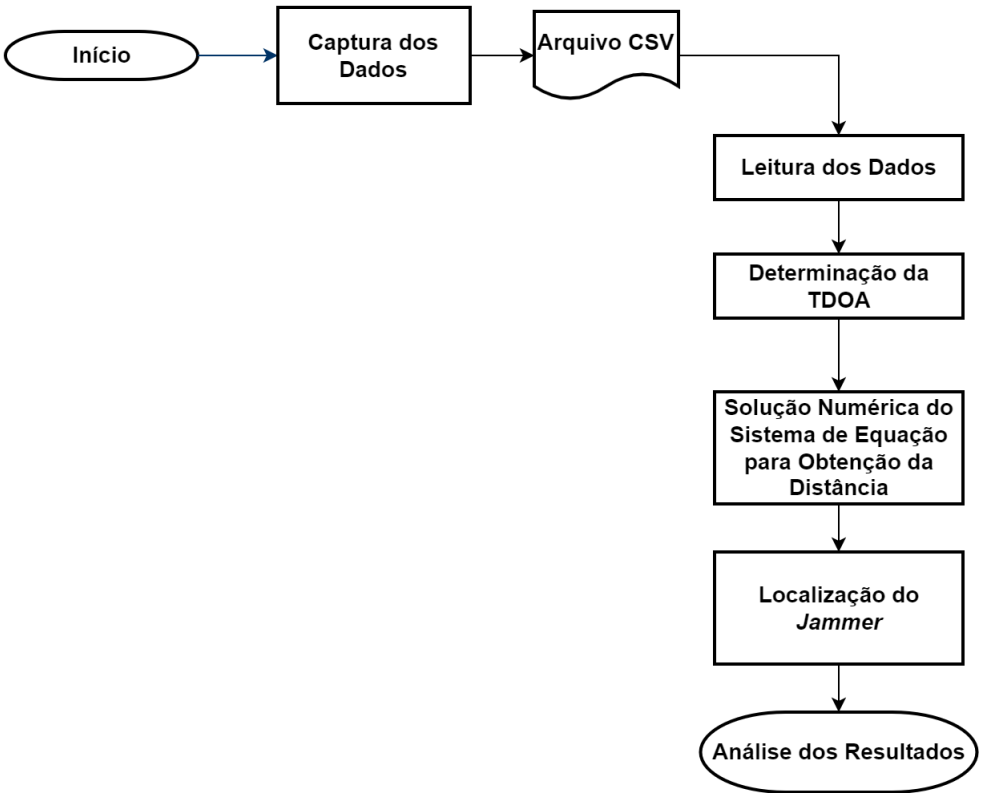
Implementou-se o algoritmo para estimativa da TDOA no MATLAB, o qual carrega, limpa e processa os dados. Um script Python então estima a posição (x, y) com base nos dados processados.

Como já apresentado em seções anteriores, a TDOA entre dois sinais é definida como $\tau_{12} = t_1 - t_2$, onde t_1 e t_2 representam os tempos de chegada da primeira frente de onda do jammer nas antenas 1 e 2, respectivamente. Usando TDOA e o teorema de Pitágoras, a posição 2D (x, y) do *jammer* pode ser estimada com o seguinte sistema de equações:

$$(x - x_1)^2 + (y - y_1)^2 = (v_e t_1)^2, \tag{4.4}$$

$$(x - x_2)^2 + (y - y_2)^2 = (v_e(t_2 + \tau_{12}))^2, \tag{4.5}$$

Figura 14 – Fluxograma dos procedimentos computacionais.



Fonte: Autoral.

$$(x - x_3)^2 + (y - y_3)^2 = (v_e(t_3 + \tau_{13}))^2, \tag{4.6}$$

onde v_e é a velocidade de propagação da onda no meio, t_1 o tempo de chegada da frente de onda inicial no sensor mais próximo do *jammer*, e (x_i, y_i) as coordenadas de cada uma das três antenas posicionadas, com $i = 1, 2, 3$.

O processamento de dados consistiu em a) usar o MATLAB para carregar os dados de tensão de três canais e seus respectivos tempos em variáveis do tipo tabela, que foram então escaneadas para detecção de entradas corrompidas (por exemplo, valores NaN); b) realizar filtragem *wavelet* dos valores processados com um nível de decomposição de 6 usando a *wavelet* Daubechie de ordem 4 (db4), reduzindo efetivamente o ruído nos sinais capturados; c) analisar os sinais filtrados usando um algoritmo de correlação cruzada para avaliar a similaridade como uma função de atraso de tempo. O TDOA entre sinais foi determinado identificando o atraso no qual a função de correlação cruzada atingiu o pico, essencial para estimar atrasos relativos entre sinais em diferentes sensores; d) aplicar as TDOAs τ_{12} e τ_{13} em um algoritmo de mínimos quadrados (MOAYERI, 2023) implementado em python para resolver um sistema de equações. Este método minimiza o erro entre as TDOAs observadas e previstas, permitindo estimar as coordenadas x e y do transmissor. O algoritmo atualiza iterativamente as estimativas de

posição, convergindo para a solução que melhor se ajusta aos dados medidos, fornecendo assim uma localização do *jammer*.

A configuração experimental contemplou a possibilidade de implementar um filtro passa-altas na interface dos canais do osciloscópio, o que potencialmente mitigaria o ruído do sinal adquirido. Contudo, optou-se pelo processamento digital dos sinais capturados sem filtragem analógica prévia. Esta decisão metodológica fundamentou-se em duas considerações principais: 1) restrições orçamentárias associadas à aquisição de filtros analógicos de alta precisão e 2) o potencial exploratório de técnicas de processamento digital, com ênfase na Transformada Wavelet Discreta (TWD), uma abordagem consolidada em diversos contextos de análise de sinais. A TWD constitui uma técnica sofisticada de decomposição de sinais, fundamentada na representação do sinal como uma combinação linear ponderada de funções *wavelets*. O processo de geração dessas funções baseia-se em uma *wavelet* mãe, que é sistematicamente dilatada ou comprimida para produzir um conjunto de bases *wavelets*. Esta metodologia permite a decomposição multiescalar do sinal, mapeando-o em diferentes bandas de frequência e possibilitando uma estimativa aproximada da localização de estruturas espectrais (CHUI, 1992).

A seleção da *wavelet* mãe representa um elemento crítico na análise. O método EBWS (*Energy-Based Wavelet Selection*) emerge como uma abordagem rigorosa, fundamentando a seleção dos filtros de decomposição na distribuição energética entre sub-bandas. O critério de seleção prioriza o filtro que maximiza a energia nos coeficientes de aproximação (LI et al., 2010).

Na investigação específica, os sinais de medição do *jammer*, capturados em uma malha de 3m $\times$ 3m com o equipamento posicionado no centro, foram processados mediante algoritmos em Python implementando o método EBWS. A análise considerou seis níveis de decomposição, revelando as *wavelets* Daubechies de ordens 3 (db3), 4 (db4) e 5 (db5) como as mais adequadas. O princípio fundamental da redução de ruído via *wavelet* reside na capacidade de decomposição do sinal em componentes de diferentes escalas — detalhes e aproximações. A decomposição *wavelet* utiliza bancos de filtros que segregam características médias e variações de alta frequência, gerando coeficientes que representam dinamicamente a estrutura do sinal (NICKOLAS, 2017).

A abordagem de redução de ruído mediante *wavelets* concentra-se no processo de *thresholding*, uma técnica estatística de filtragem. O protocolo metodológico compreende três etapas fundamentais: decomposição do sinal ruidoso mediante filtros *wavelets*, segregando componentes detalhados e grosseiros; aplicação de limiarização (*thresholding*), onde coeficientes de magnitude reduzida — presumivelmente associados a ruído — são definidos como zero; reconstrução do sinal mediante transformada *wavelet* inversa, preservando características espectrais significativas.

A definição do limiar representa um elemento metodológico crítico. Uma estratégia comum envolve estabelecer o limiar em múltiplos do desvio padrão da distribuição dos coeficientes *wavelets*, equilibrando preservação de características espectrais e supressão de ruído.

5 Resultados

Este capítulo apresenta os resultados obtidos na realização do experimento para localização do *jammer*, bem como a análise comparativa desses com técnicas empregadas nos trabalhos identificados durante a revisão da literatura.

5.1 Antena construída

A estrutura da antena CPW simulada foi então construída, utilizando-se da técnica de corrosão com percloreto de ferro e adesivagem sobre uma placa de circuito impresso com substrato de FR4 epoxy e condutor de cobre. O resultado final do processo pode ser visualizado na Figura 15.

A discrepância entre os resultados observados na Figura 16, pode ser justificada pela interferência eletromagnética do ambiente de medição, além disso, o processo de fabricação manual pode resultar em diferenças entre as dimensões exatas utilizadas na simulação e as aproximadas obtidas na construção, pois o percloreto pode penetrar as bordas do adesivo e a *silhuette* possui erro na exatidão no corte do adesivo devido o número de casas decimais considerado, também podem serem consideradas a posição e soldagem do conector na trilha de alimentação, que são simplificados na simulação para apenas uma porta com excitação. O deslocamento observado em relação a faixa de frequência esperada não se confere um grande prejuízo, visto que a aplicação da antena será a captura do tempo de chegada de um sinal e a faixa obtida nas medições contempla metade da faixa de operação 4G1 do *jammer*.

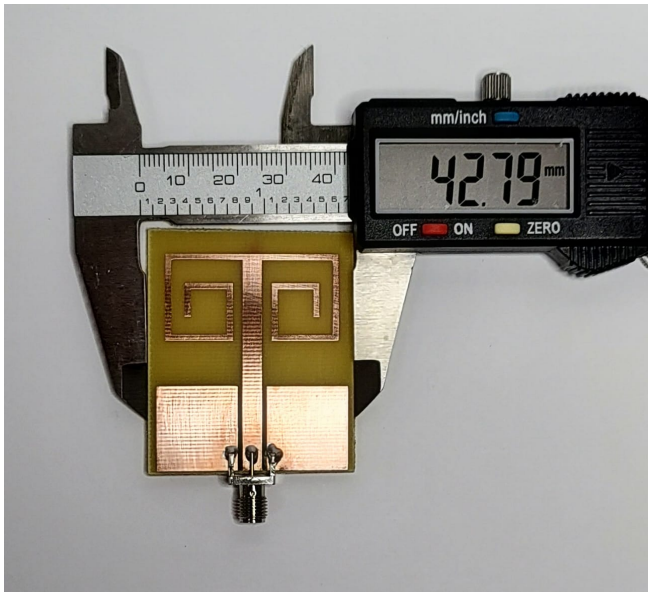
As antenas fabricadas foram então testadas em uma câmara semi-anecoica, onde fazendo uso de um analisador de espectro foi capturado o sinal transmitido pelo *jammer* na faixa de operação proposta, sendo então possível comparar o espectro em frequência do sinal recebido por todas as antenas fabricadas com uma captura de referência realizada com uma corneta.

Os passos realizados para medição foram os seguintes:

- Caracterização da antena do *jammer*;
- Cálculo da menor distância radial para a região de campo distante da antena do *jammer*: $2D^2/\lambda$, onde D é a maior dimensão da antena transmissora e λ o comprimento de onda radiado;

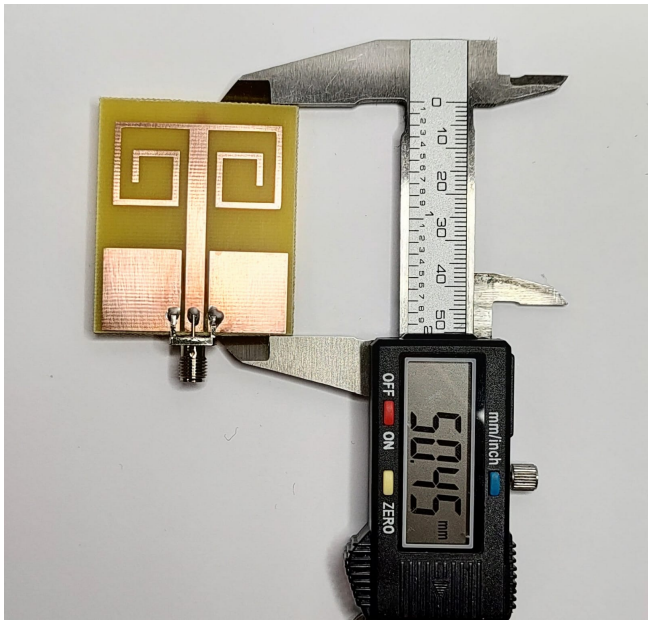
Figura 15 – Antenas construídas para recepção do sinal do *jammer*.

(a) Largura da antena CPW construída.



Fonte: Autoral.

(b) Comprimento da Antena CPW construída.

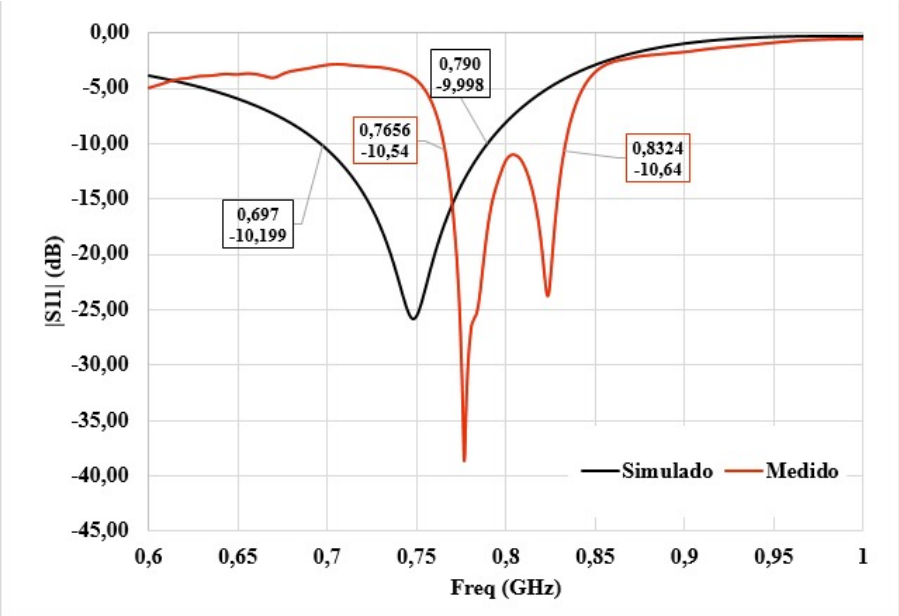


Fonte: Autoral.

- Montagem do arranjo de testes respeitando a distância para o campo distante calculada e mesmo nível de linha de visada para transmissor e receptor;
- Ajuste do analisador de espectro para melhor visualização do sinal capturado;
- Salvamento dos resultados.

Na Figura 17 se pode verificar a antena do *jammer* para a faixa 4G1, aferiu-se o comprimento da mesma em aproximadamente 0,22 metros. Visto que essa antena tem aplicação na

Figura 16 – Comparação entre os resultados simulados e reais da antena construída.



Fonte: Autoral.

frequência de 700 MHz, o que equivale a um λ de aproximadamente 0,3674 metros, resultando em um comprimento da antena de 0,599λ metros. Para o cálculo da menor distância radial para a região de campo distante da antena do *jammer*, tem-se que: $2D^2/\lambda = 2(0{,}22)^2/0{,}3674 = 0{,}2635\ m$. Quando aplicada a mesma fórmula à antena receptora projetada, tem-se: $2D^2/\lambda = 2(0{,}05)^2/0{,}3674 = 0{,}0136\ m$.

A antena do *jammer* foi então acoplada a um VNA, uma ressalva importante é que ao observar os resultados optidos para o S11, deve-se considerar que a impedância da antena é desconhecida. Segue na Figura 18 o resultado capturado. É possível constatar que entre os marcadores 1 e 2 se tem uma faixa entre 717,41 MHz e 744,35 MHz abaixo de -10 dB, da mesma forma entre os marcadores 3 e 4 se tem uma faixa entre 776,37 MHz e 859,72 MHz abaixo de -10 dB, com uma frequência de ressonância de 816,01 MHz a -59,30 dB.

Prosseguindo para realização dos testes, reitera-se que foram utilizadas como referência as medições do sinal 4G1 do jammer realizadas com a corneta da Figura 19, os resultados obtidos para essa podem ser verificados na Figura 20. É importante destacar que nessa faixa a corneta possui um ganho de 9,48 dBi e utilizou-se um atenuador de - 20 dB.

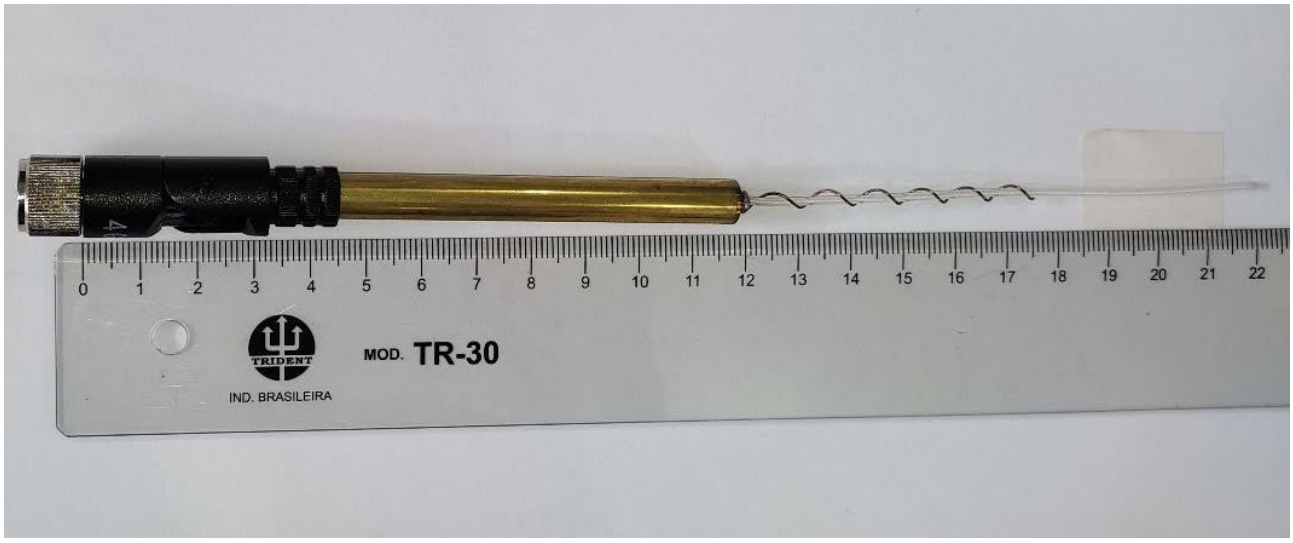
O analisador utilizado (KEYSIGHT MXA Signal Analyzer N9020A) pode ser observado na Figura 21. Já a montagem realizada no interior da câmara pode ser vista nas Figuras 22 e 23.

Figura 17 – Antena do *jammer* para faixa 4G1.

(a) Antena 4G1 do *jammer*.

Fonte: Autoral.

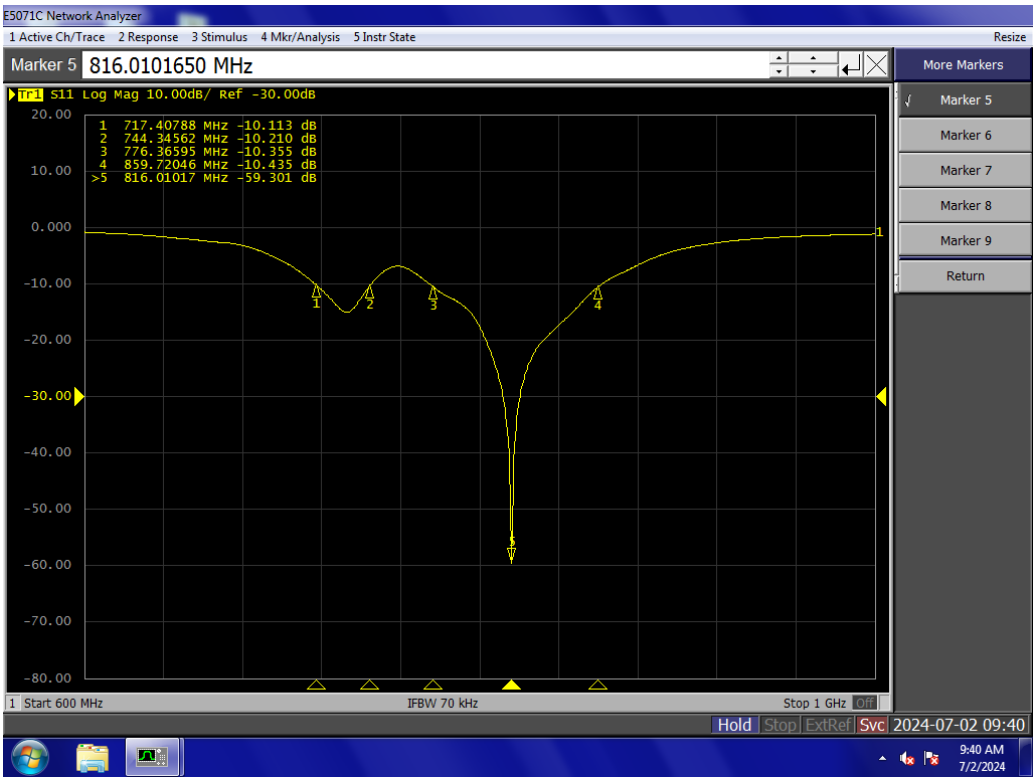
(b) Comprimento da antena 4G1 do *jammer*.



Fonte: Autoral.

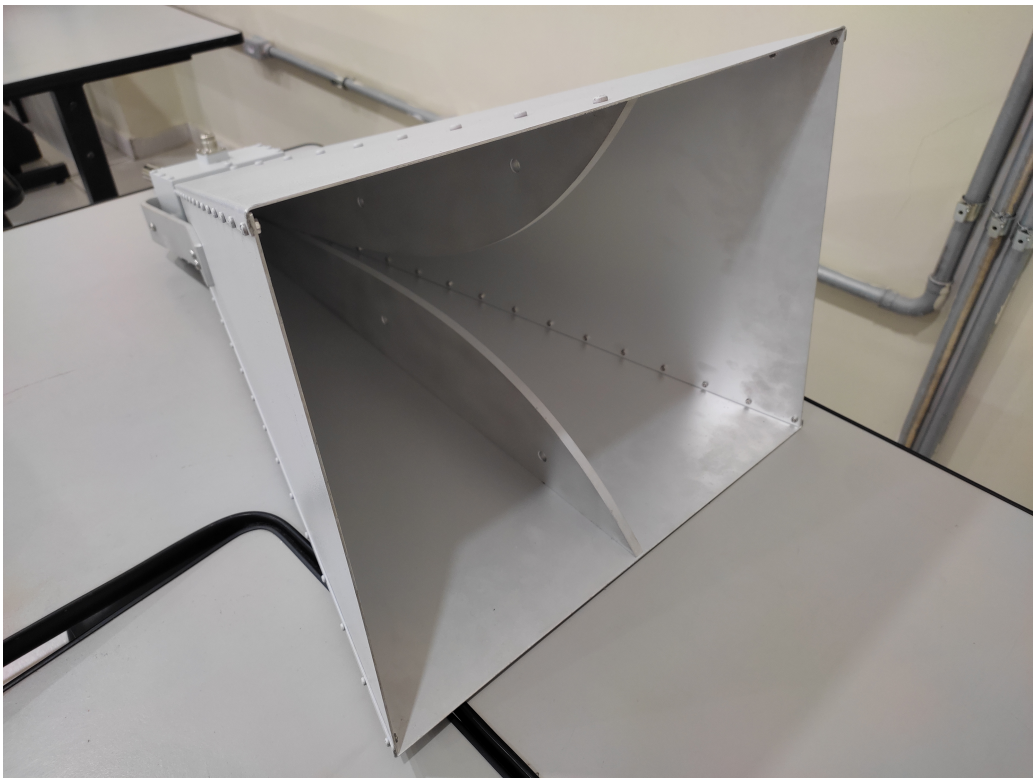
Na Figura 24, pode-se observar o resultado da captura realizada para uma das antenas fabricadas. A partir dos resultados obtidos, foram escolhidas quatro antenas que apresentaram resultados similares para a realização das medições das TDOAs.

Figura 18 – S11 da antena 4G1 do *jammer*.



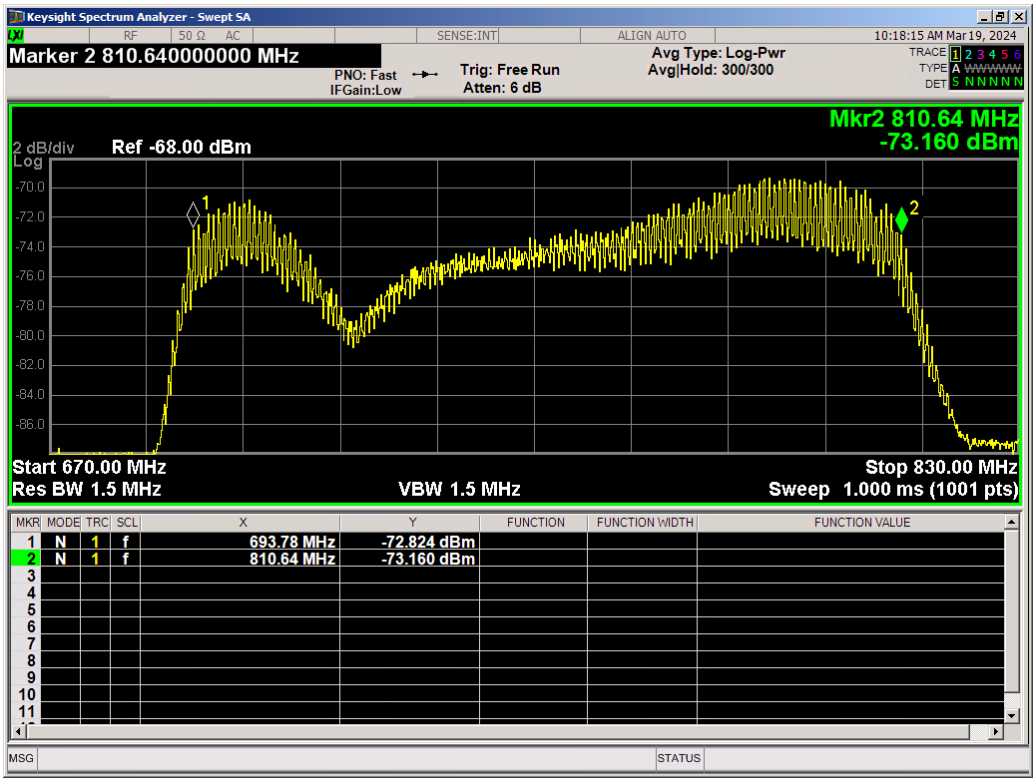
Fonte: Autoral.

Figura 19 – Corneta utilizada como referência para os testes.



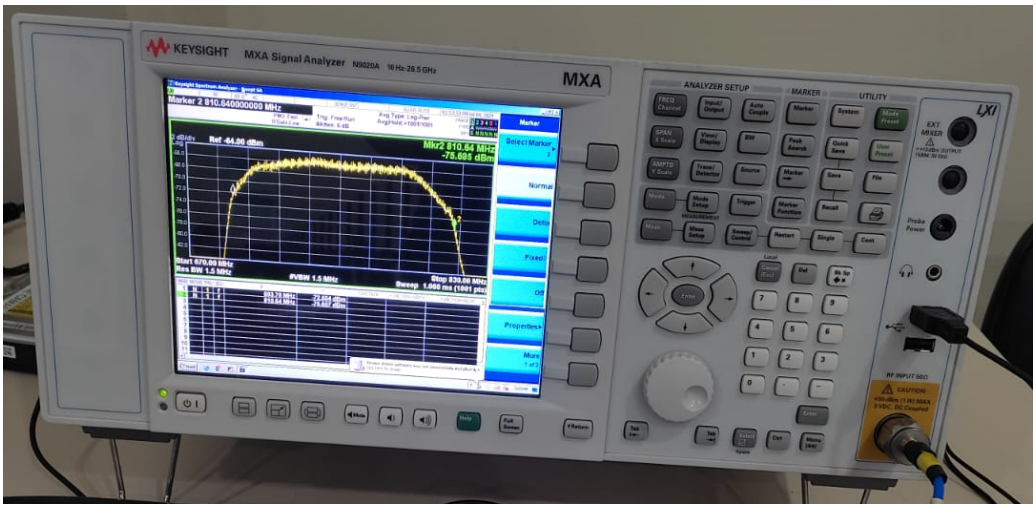
Fonte: Autoral.

Figura 20 – Resultados capturados com a corneta.



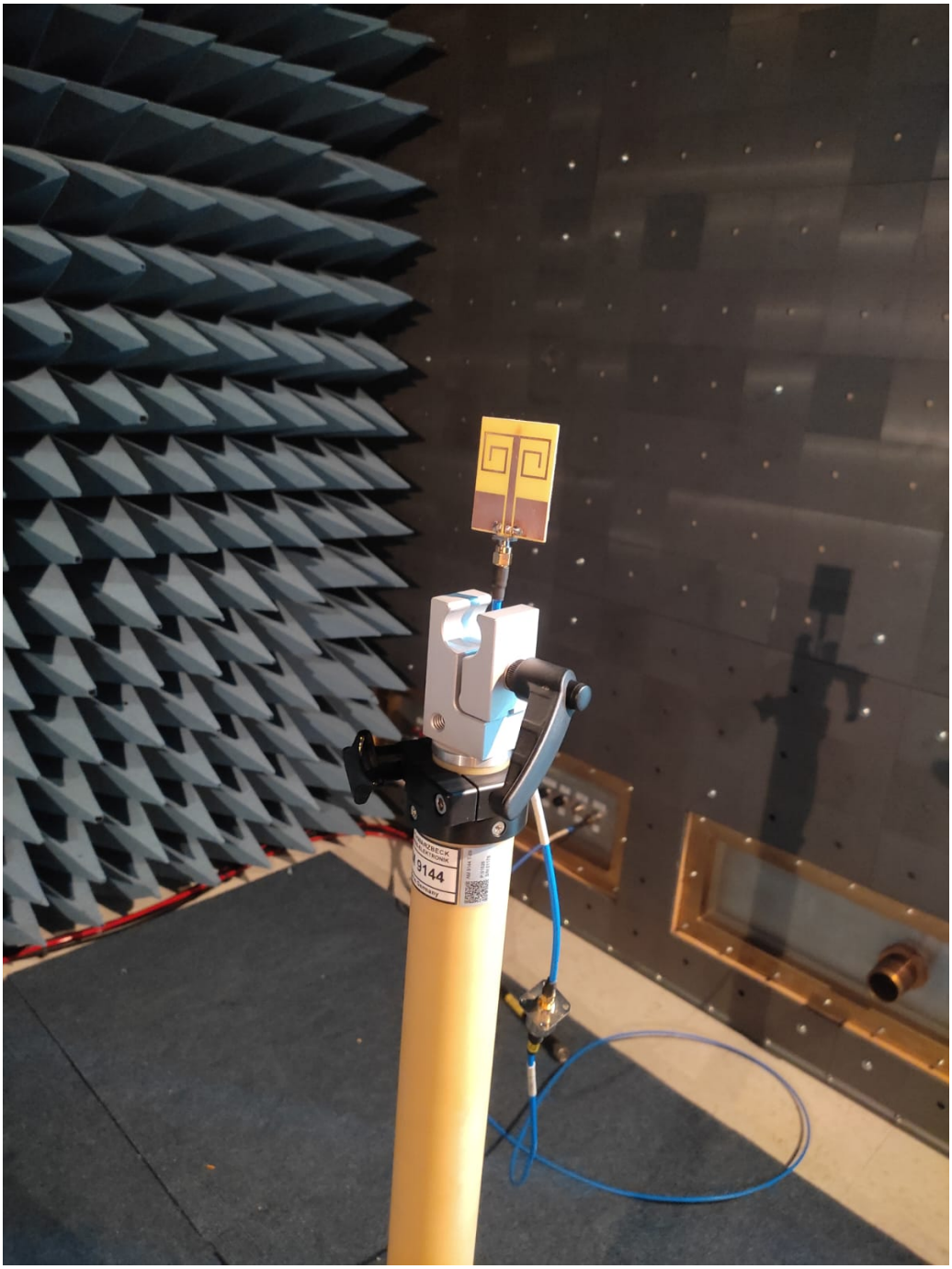
Fonte: Autoral.

Figura 21 – Analisador de sinal utilizado na montagem.



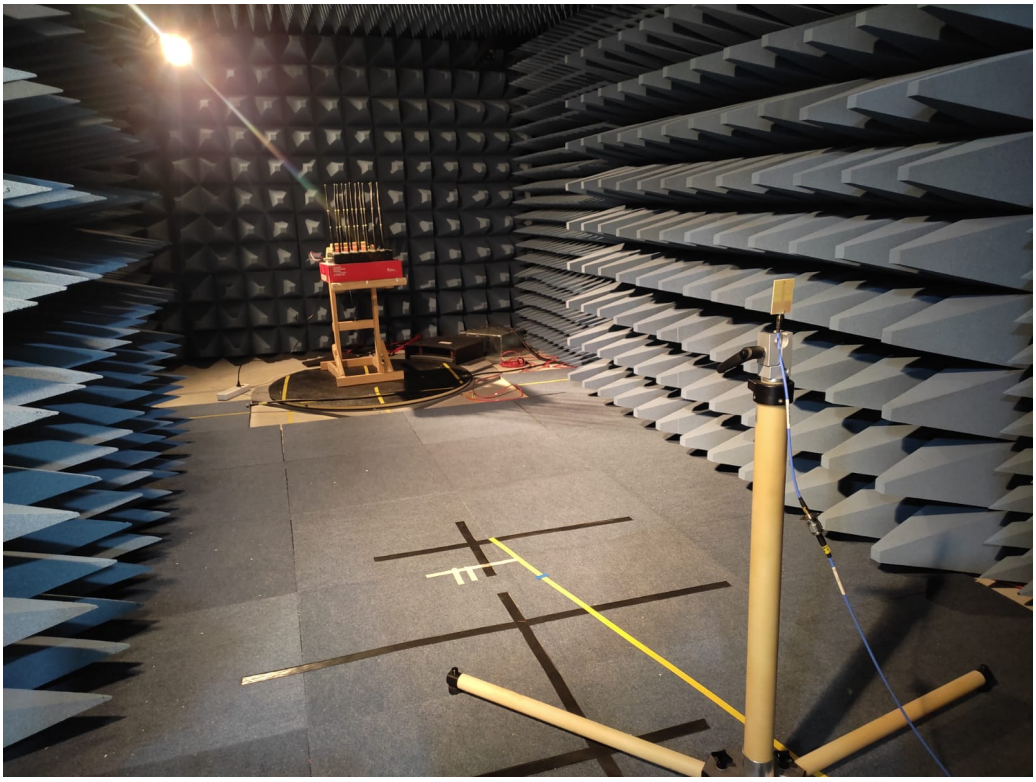
Fonte: Autoral.

Figura 22 – Vista da antena fabricada na montagem realizado no interior da câmara.



Fonte: Autoral.

Figura 23 – Vista geral da montagem.



Fonte: Autoral.

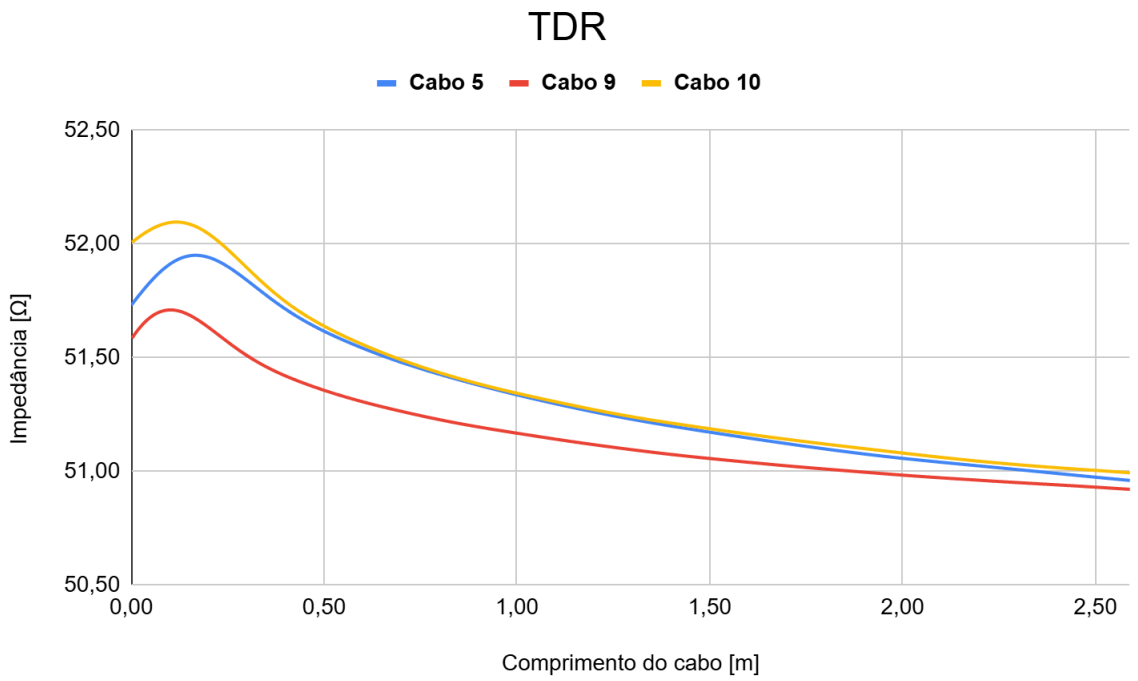
Figura 24 – Resultado obtido na captura do sinal do *jammer* utilizando a antena fabricada.

Fonte: Autoral.

5.2 Análise dos cabos

Cada um dos cabos a serem utilizados foram conectados individualmente no equipamento FieldFox e uma carga de calibração de 50 Ω foi conectada nos terminais da sua outra extremidade, os resultados obtidos podem ser vistos na Figura 25. Onde, pode-se observar pelo método TDR as impedâncias similares entre os três cabos, próximas de 51 Ω. Atribui-se o pico de impedância no inicio dos cabos ao uso de adaptadores para conexão dos mesmos ao analisador. Além disso, não foram verificados quaisquer sinais de descontinuidade ao longo dos cabos.

Figura 25 – Resultados do teste de TDR para os três cabos utilizados no experimento.



Fonte: Autoral.

5.3 Localização do *jammer*

Com as antenas construídas, os cabos com suas integridades atestadas e a partir dos ajustes descritos na metodologia deste trabalho, preparou-se o arranjo de experimentação. Com o *jammer* posicionado na malha de coordenadas, repetiu-se o procedimento de captura do sinal, para tal o dispositivo foi acionado em três posições distintas. Uma das capturas realizadas pelo osciloscópio pode ser vista na Figura 26, essa corresponde à posição (2.5, 1.5) do transmissor. O sinal amarelo corresponde ao capturado pelo Receptor 1, o ciano ao capturado pelo Receptor

Tabela 6 – Resultados de localizações do *Jammer*

Posição 1 (em metros)				
X estimado	**Y estimado**	**X real**	**Y real**	**RMSE**
1.16	1.50	1.50	1.50	0.240
Posição 2 (em metros)				
X estimado	**Y estimado**	**X real**	**Y real**	**RMSE**
0.99	0.89	1.00	1.00	0.078
Posição 3 (em metros)				
X estimado	**Y estimado**	**X real**	**Y real**	**RMSE**
2.58	1.63	2.50	1.50	0.108

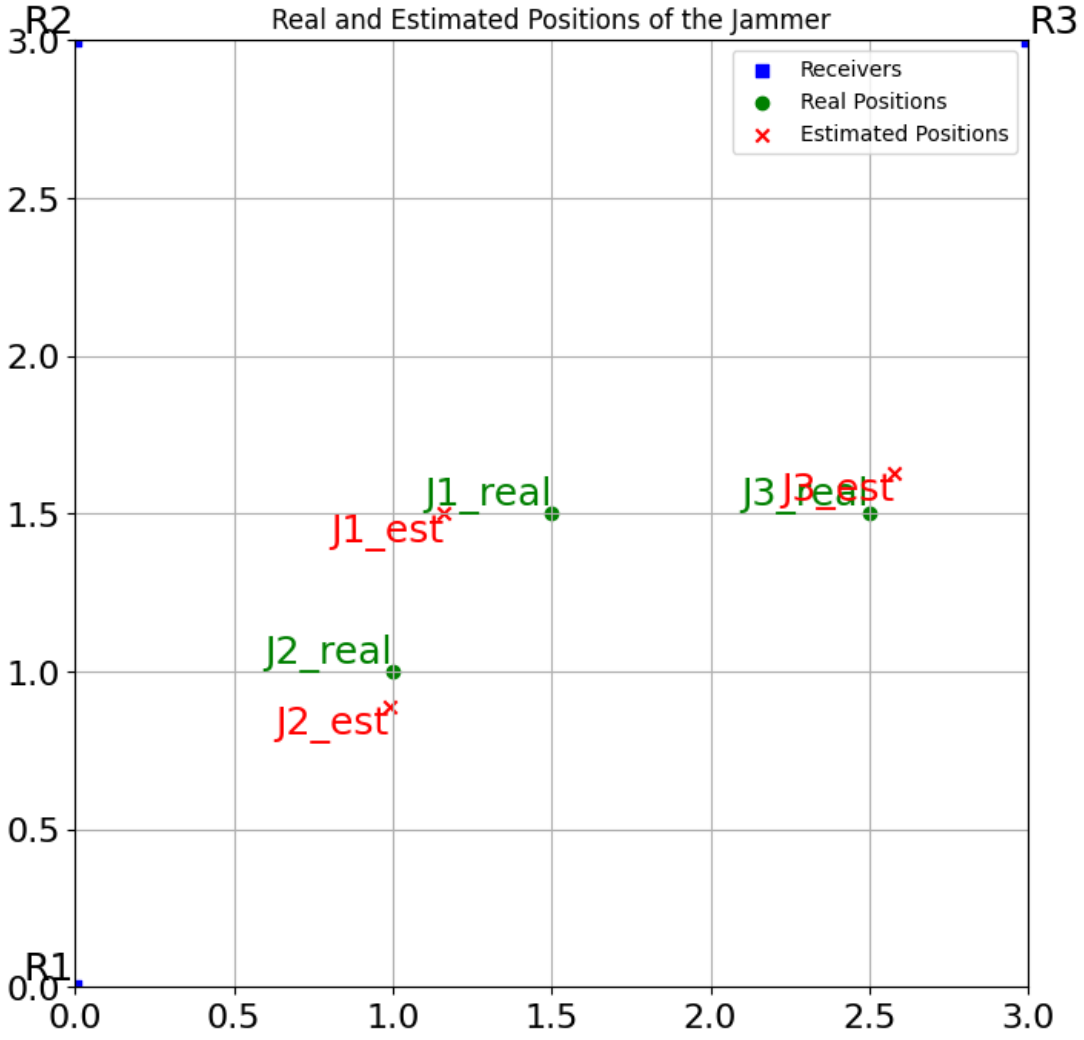
2 e o magenta ao capturado pelo Receptor 3. Como esperado, observa-se que a frente de onda recebida pelo receptor mais próximo está adiantada em relação as outras duas, também é possível notar a proximidade entre os sinais dos receptores que estão a uma mesma distância do transmissor.

Figura 26 – Sinal capturado pelo osciloscópio para posição (1.0, 1.0).

Fonte: Autoral.

Conforme apresentado na Tabela 6, o *jammer* foi localizado com boa exatidão, com todos os Erros Quadráticos Médios (RMSE, do inglês - *Root Mean Square Error*) abaixo de 0,25 metros. Essa exatidão permite que o alvo seja posicionado no ponto mais próximo na grade de coordenadas em cenários práticos. Possíveis fontes de erro incluem atrasos introduzidos pelo osciloscópio, imprecisões na construção da grade e o posicionamento manual dos receptores e do *jammer*. A Figura 27 ilustra as posições reais versus estimadas na grade de coordenadas, onde J1, J2 e J3, representam respectivamente o *jammer* nas posições 1, 2 e 3. Para comparação, o trabalho de Ren et al. (2016), que também envolveu experimentos reais usando a técnica de

Figura 27 – Posições reais e estimadas do *Jammer*.



Fonte: Autoral.

RSS, relatou um erro de localização superior a 0.6 metros para as mesmas distâncias entre receptor e transmissor propostas neste trabalho. Enquanto outros estudos na literatura fornecem resultados baseados em simulação que demonstram efetivamente os métodos propostos, comparar erros de localização é desafiador, pois testes do mundo real introduzem fontes adicionais de erro. Outras técnicas de localização podem ser usadas para reduzir a dependência de um grande número de receptores, mas este estudo considerou a tendência de aumento do número de estações rádio base no 5G, considerando o princípio da sua arquitetura baseada em *small cells*.

Com base na Tabela 7, observa-se que o método proposto por (SANTOS; SERRES; GURJãO, 2024), utilizando a técnica TDOA em um cenário real, apresentou o menor erro médio, de 0,14 metros, superando tanto abordagens simuladas, como a IGSA (WANG et al., 2018d) e o MCC (ALIKH; RAJABZADEH, 2022), que obtiveram erros de 0,33 e 0,34 metros,

Tabela 7 – Análise comparativa do erro de localização

Autor	Técnica	Cenário	Erro médio até 3 metros
Ren et al. (2016)	DE2	Real	0.60
Wang et al. (2018d)	IGSA	Simulado	0.33
Aldosari, Zohdy e Olawoyin (2019a)	RSS (DSNR, CL, WCL, VFIL)	Simulado	>0.60
Alikh e Rajabzadeh (2022)	MCC	Simulado	0.34
Santos, Serres e Gurjão (2024)	TDOA	Real	0.14

respectivamente, quanto métodos reais, como o DE2 (REN et al., 2016), com erro de 0,60 metros. Adicionalmente, os métodos RSS analisados em (ALDOSARI; ZOHDY; OLAWOYIN, 2019a) apresentaram um desempenho inferior, com erros superiores a 0,60 metros. Esses resultados destacam a eficácia do TDOA na redução do erro de localização em aplicações práticas, como a detecção de *Jammers* em redes 5G. É importante ressaltar que, mesmo em um cenário real, onde há fontes adicionais de erros, como interferências e multipercurso, o método proposto ainda superou significativamente os resultados obtidos em cenários simulados, evidenciando sua robustez e aplicabilidade em condições reais.

Tais resultados demonstram a viabilidade dessa abordagem para localizar *jammers* usando TDOA. Assim, sugerem-se análises adicionais para avaliar com maior profundidade a robustez dessa metodologia em cenários mais críticos (mudanças na topografia que atrapalhem a linha de visada e adição de elementos do ambiente urbano como prédios, vegetação, pessoas e veículos), arranjos experimentais com maiores dimensões, em diferentes ambientes, bem como a inclusão de obstáculos metálicos entre as antenas receptoras e o dispositivo transmissor.

Mediante a construção da antena proposta, obteve-se um ganho realizado máximo de -8,35 dBi nos receptores, o que se mostrou suficiente para detecção do sinal em uma malha de coordenadas reduzidas e colaborou para a preservação da integridade dos canais do osciloscópio. Uma das medições apresentou erro maior que as demais, outros testes também foram realizados, porém um fator de interferência que adiciona variação no erro observado na localização é a presença de uma pessoa dentro da malha de coordenadas, necessária para o acionamento do *jammer*, tal fator ainda não pôde ser completamente contornado pelo algoritmo proposto, em contrapartida adiciona um elemento real de interferência ao experimento.

Em relação às técnicas de processamento de sinais, nota-se que a correlação cruzada e o uso da *wavelet* Daubechies 4 com seis níveis de decomposição, proporcionaram a localização da posição do *jammer*. Vale destacar que ao longo da pesquisa foram experimentados outros algoritmos para estimativa da TDOA, como, por exemplo, o da energia cumulativa, que possui bom desempenho na localização de descargas parciais, mas foi ineficaz no presente cenário, o

que se atribui à natureza e comportamento completamente distintos dos sinais detectados (um impulsivo e outro oscilatório).

6 Considerações finais

Nesta dissertação foi apresentada a aplicação do método TDOA presente nas redes 5G para localização de *jammers* no cenário de ataques às redes móveis celulares.

No presente trabalho, constatou-se que com a aplicação da técnica proposta e o uso de processamento de sinais, pôde-se localizar o equipamento *jammer* com medições reais do seu sinal. Também é importante destacar que com o mínimo de três receptores para que o sistema de equações possua solução, pôde-se obter resultados com erro médio de 0,14 metros, o que é melhor que a maior parte dos algoritmos aplicados em cenários simulados e reais propostos na revisão da literatura do presente trabalho.

Mediante o apresentado, as tecnologias de localização presentes no 5G são capazes de estimar com precisão a posição de equipamentos ativos, ou seja, que respondem às mensagens dos protocolos empregados para tal, e de equipamentos passivos como o *jammer*, que não se comunicam com a rede.

Por conseguinte, destaca-se que o método TDOA apresenta maior robustez frente aos efeitos de reflexões e refrações ambientais em comparação aos métodos baseados na intensidade do sinal recebido. No entanto, tais efeitos indesejados ainda exercem um impacto significativo na precisão das posições estimadas com TDOA. Portanto, investigações mais aprofundadas são necessárias, considerando diferentes tipos de obstáculos na malha de coordenadas e explorando a aplicação de métodos híbridos, como a combinação de TDOA com AOA, para aumentar a imunidade dos resultados a esses efeitos.

Adicionalmente, como resultado da aplicação da metodologia proposta neste trabalho, e diante da dificuldade de acesso a equipamentos especializados e da consequente escassez de dados reais sobre sinais provenientes de *jammers*, foi gerado um banco de dados contendo medições desses sinais. Esse recurso contribui para a aceleração de novas pesquisas na área, fomentando avanços sobre a temática.

6.1 Publicação

Os resultados obtidos nesta pesquisa foram divulgados em publicação de artigo realizada em evento científico internacional, conforme a seguir:

- VILARIM, MATHEUS; SERRES, AJR; CANDEIA GURJÃO, EDMAR. Jammer Localization Using Time Difference of Arrival Algorithm in 5G Mobile Networks. *1st IEEE Latin American Conference on Antennas & Propagation*, 2024.

6.2 Trabalhos futuros

Propõe-se como continuação da pesquisa desenvolvida nesta dissertação:

- **Melhoria do arranho experimental**: Os experimentos realizados neste trabalho apresentaram bons resultados, porém a metodologia aplicada pode ser enriquecida com a consideração de ambientes com diferentes níveis de ruído, uma malha de coordenadas maior e a inclusão de diferentes tipos de obstáculos presentes no ambiente urbano para avaliar os erros de localização;

- **Medições em ambiente aberto:** Obter licença da Anatel para realização de testes em ambientes abertos, realizando-se assim medições que possam atestar a validade da abordagem proposta em ambiente urbano livre;

- **Usar estações rádio base reais para realizar a localização:** conseguir aplicar os procedimentos propostos neste trabalho em gNodeBs reais seria fundamental para entender os desafios práticos e possíveis melhorias que poderiam ser propostas para arquitetura do 5G e além;

- **Construir outros tipos de *jammers* utilizando Radio Definido por Software:** a abordagem proposta pode ser avaliada na localização de outros tipos de *jammers*, podendo esses serem fabricados como o uso de Radio Definido por Software.

REFERÊNCIAS

3GPP. *5G System (5GS) Location Services (LCS); Stage 2*. [S.l.], 2023. Disponível em: <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3577>>. Acesso em: 06.11.2023.

3GPP. *NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN*. [S.l.], 2023. Disponível em: <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3310>>. Acesso em: 08.11.2023.

3GPP. *NG-RAN; NR Positioning Protocol A (NRPPa)*. [S.l.], 2023. Disponível em: <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3256>>. Acesso em: 09.11.2023.

3GPP. *NR; Layer 2 measurements*. [S.l.], 2023. Disponível em: <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3671>>. Acesso em: 31.10.2023.

3GPP. *NR; Physical channels and modulation*. [S.l.], 2023. Disponível em: <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3213>>. Acesso em: 31.10.2023.

3GPP. *NR; Physical layer; General description*. [S.l.], 2023. Disponível em: <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3211>>. Acesso em: 06.11.2023.

3GPP. *Service requirements for the 5G system*. [S.l.], 2023. Disponível em: <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107>>. Acesso em: 31.10.2023.

3GPP. *Study on 5G security enhancements against False Base Stations (FBS)*. [S.l.], 2023. Disponível em: <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539>>. Acesso em: 30.11.2023.

3GPP. *Study on NR positioning support*. [S.l.], 2023. Disponível em: <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3501>>. Acesso em: 08.11.2023.

3GPP. *Study on positioning use cases*. [S.l.], 2023. Disponível em: <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3280>>. Acesso em: 07.11.2023.

3GPP. *System architecture for the 5G System (5GS)*. [S.l.], 2023. Disponível em: <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>>. Acesso em: 06.11.2023.

ADAMY, D. [S.l.: s.n.], 2003.

ALDOSARI, W.; ZOHDY, M.; OLAWOYIN, R. Jammer localization through smart estimation of jammer's transmission power. In: *2019 IEEE National Aerospace and Electronics Conference (NAECON)*. [S.l.: s.n.], 2019. p. 430–436.

ALDOSARI, W.; ZOHDY, M.; OLAWOYIN, R. Tracking the mobile jammer in wireless sensor networks using extended kalman filter. In: *2019 IEEE 10th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*. [S.l.: s.n.], 2019. p. 0207–0212.

ALIKH, N.; RAJABZADEH, A. Using a lightweight security mechanism to detect and localize jamming attack in wireless sensor networks. *Optik*, v. 271, p. 170099, 2022. ISSN 0030-4026. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0030402622013572>.

ALMOMANI, I. et al. An efficient localization and avoidance method of jammers in vehicular ad hoc networks. *IEEE Access*, v. 10, p. 131640–131655, 2022.

ARABSORKHI, M.; ZAYYANI, H.; KORKI, M. 3-d hybrid rss-aoa passive source localization with unknown path loss exponent. *IEEE Sensors Letters*, v. 7, n. 6, p. 1–4, 2023.

BARTOLETTI, N. B.-M. S. *Positioning and Location-Based Analytics in 5G and Beyond*. Wiley, 2023. ISBN 9781119911432. Disponível em: <http://gen.lib.rus.ec/book/index.php?md5=62236756EDC40E485B2B65E834078930>.

BOX, M. J.; DAVIES, D.; SWANN, W. H. Non-linear optimization techniques;. In: . [s.n.], 1969. Disponível em: <https://api.semanticscholar.org/CorpusID:118115316>.

CAMBRIDGE English Dictionary. Cambridge University Press, 2023. Disponível em: <https://dictionary.cambridge.org/>.

CHOI, J. et al. Cusum-based joint jammer detection and localization. In: *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. [S.l.: s.n.], 2018. p. 1–5.

CHUI, C. Wavelet analysis and its applications. In: CHUI, C. K. (Ed.). *Wavelets*. San Diego: Academic Press, 1992, (Wavelet Analysis and Its Applications, v. 2). p. 725. Disponível em: <https://www.sciencedirect.com/science/article/pii/B9780121745905500290>.

ELHAG, N. A. A. et al. Angle of arrival estimation in smart antenna using music method for wideband wireless communication. In: *2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE)*. [S.l.: s.n.], 2013. p. 69–73.

FARKAS, H.; KáLY-KULLAI, K.; SIENIUTYCZ, S. Chapter 17 - the fermat principle and chemical waves. In: SIENIUTYCZ, S.; FARKAS, H. (Ed.). *Variational and Extremum Principles in Macroscopic Systems*. Oxford: Elsevier, 2005. p. 355–373. ISBN 978-0-08-044488-8. Disponível em: <https://www.sciencedirect.com/science/article/pii/B9780080444888500205>.

FRIEDLANDER, B. Chapter 1 - wireless direction-finding fundamentals. In: TUNCER, T. E.; FRIEDLANDER, B. (Ed.). *Classical and Modern Direction-of-Arrival Estimation*. Boston: Academic Press, 2009. p. 1–51. ISBN 978-0-12-374524-8. Disponível em: <https://www.sciencedirect.com/science/article/pii/B9780123745248000015>.

GODARA, L. Limitations and capabilities of directions-of-arrival estimation techniques using an array of antennas: a mobile communications perspective. In: *Proceedings of International Symposium on Phased Array Systems and Technology*. [S.l.: s.n.], 1996. p. 327–333.

GRIVA, I.; NASH, S.; SOFER, A. *Linear and Nonlinear Optimization: Second Edition*. Society for Industrial and Applied Mathematics (SIAM, 3600 Market Street, Floor 6, Philadelphia, PA 19104), 2009. (Other Titles in Applied Mathematics). ISBN 9780898717730. Disponível em: <https://books.google.com.br/books?id=uOJ-Vg1BnKgC>.

GU, H. et al. High resolution time of arrival estimation algorithm for b5g indoor positioning. *Physical Communication*, v. 50, p. 101494, 2022. ISSN 1874-4907. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1874490721002299>.

HUSSAIN, A. et al. Jammer localization in the internet of vehicles: Scenarios, experiments, and evaluation. In: . New York, NY, USA: Association for Computing Machinery, 2023. (IoT '22), p. 73–80. ISBN 9781450396653. Disponível em: <https://doi.org/10.1145/3567445.3567463>.

HUSSAIN, A. et al. Energy-harvesting based jammer localization: A battery-free approach in wireless sensor networks. In: *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*. [S.l.: s.n.], 2022. p. 6212–6217.

IRRAM, F. et al. Physical layer security for beyond 5g/6g networks: Emerging technologies and future directions. *J. Netw. Comput. Appl.*, Academic Press Ltd., GBR, v. 206, n. C, oct 2022. ISSN 1084-8045. Disponível em: <https://doi.org/10.1016/j.jnca.2022.103431>.

JAGANNATH, A.; JAGANNATH, J. Jam-guard: Low-cost, hand-held device for first responders to detect and localize jammers. In: *2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS)*. [S.l.: s.n.], 2020. p. 1–7.

JING-GANG, Y. et al. Study of time delay of uhf signal arrival in location partial discharge. In: *2008 International Conference on Condition Monitoring and Diagnosis*. [S.l.: s.n.], 2008. p. 1088–1092.

KAKEETO, P. et al. Experimental investigation of positional accuracy for uhf partial discharge location. In: *2008 International Conference on Condition Monitoring and Diagnosis*. [S.l.: s.n.], 2008. p. 1070–1073.

Keysight Technologies. *A-Series N991xA/2xA/3xA/5xA/6xA User's Guide (Unabridged)*. [S.l.], 2024. Disponível em: <https://www.keysight.com/br/pt/assets/9921-01766/user-manuals/Users-Guide-A-Series-N991xA-2xA-3xA-5xA-6xA-Unabridged.pdf>.

KHWANDAH, S. A. et al. Massive mimo systems for 5g communications. *Wireless Personal Communications*, v. 120, n. 3, p. 2101–2115, out. 2021. ISSN 0929-6212, 1572-834X. Disponível em: <https://link.springer.com/10.1007/s11277-021-08550-9>.

KNAPP, C.; CARTER, G. The generalized correlation method for estimation of time delay. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, v. 24, n. 4, p. 320–327, 1976.

KRISHNAMURTHY, P.; KHORRAMI, F.; KUMAR, R. An approximate factorization approach to multi-jammer location and range estimation from peer-to-peer connectivity measurements. *Computer Networks*, v. 196, p. 108268, 2021. ISSN 1389-1286. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128621002942>.

LAWSON, C. L.; HANSON, R. J. Solving least squares problems. In: *Classics in applied mathematics*. [s.n.], 1976. Disponível em: <https://api.semanticscholar.org/CorpusID:122862057>.

LI, J. et al. Scale dependent wavelet selection for de-noising of partial discharge detection. *IEEE Transactions on Dielectrics and Electrical Insulation*, v. 17, n. 6, p. 1705–1714, 2010.

LINDNER, T. et al. A practical evaluation of joint angle and delay estimation. In: *2015 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. [S.l.: s.n.], 2015. p. 1–4.

MARIAPPAN, S. M.; SELVAKUMAR, S. A novel location pinpointed anti-jammer with knowledged estimated localizer for secured data transmission in mobile wireless sensor network. *Wireless Personal Communications*, v. 118, n. 4, p. 2073–2094, Jun 2021. ISSN 0929-6212, 1572-834X. Disponível em: <https://link.springer.com/10.1007/s11277-020-07885-z>.

MOAYERI, N. Cooperative localization using received signal strength and least squares estimation methods. In: *2023 13th International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. [S.l.: s.n.], 2023. p. 1–6.

MPITZIOPOULOS, A. et al. A survey on jamming attacks and countermeasures in wsns. *IEEE Communications Surveys Tutorials*, v. 11, n. 4, p. 42–56, 2009.

NICKOLAS, P. *Wavelets: A Student Guide*. [S.l.]: Cambridge University Press, 2017. (Australian Mathematical Society Lecture Series).

NIU, Z. et al. Overview of jammer localization in wireless sensor networks. In: *2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*. [S.l.: s.n.], 2020. v. 9, p. 9–13.

PALLOTTA, L.; GIUNTA, G. Accurate delay estimation for multisensor passive locating systems exploiting the cross-correlation between signals cross-correlations. *IEEE Transactions on Aerospace and Electronic Systems*, v. 58, n. 3, p. 2568–2576, 2022.

PANG, L. et al. Tracking the mobile jammer continuously in time by using moving vector. In: *2017 10th International Symposium on Computational Intelligence and Design (ISCID)*. [S.l.: s.n.], 2017. v. 1, p. 43–48.

PATWARI, N. et al. Locating the nodes: cooperative localization in wireless sensor networks. *IEEE Signal Processing Magazine*, v. 22, n. 4, p. 54–69, 2005.

PATWARI, N. et al. Relative location estimation in wireless sensor networks. *IEEE Transactions on Signal Processing*, v. 51, n. 8, p. 2137–2148, 2003.

PEJANOVIć-DJURIšIć, M.; KUKLINSKI, S. 5g security landscape: Concept and remaining challenges. In: *2022 30th Telecommunications Forum (TELFOR)*. [S.l.: s.n.], 2022. p. 1–4.

PIRAYESH, H.; ZENG, H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys Tutorials*, v. 24, n. 2, p. 767–809, 2022.

RAPPAPORT, T. *Wireless Communications: Principles and Practice*. 2nd. ed. USA: Prentice Hall PTR, 2001. ISBN 0130422320.

REN, L. et al. De2: localization based on the rotating rss using a single beacon. *Wireless Networks*, v. 22, n. 2, p. 703–721, Feb 2016. ISSN 1572-8196. Disponível em: <https://doi.org/10.1007/s11276-015-0998-9>.

ROBLES, G.; FRESNO, J.; MARTíNEZ-TARIFA, J. Separation of radio-frequency sources and localization of partial discharges in noisy environments. *Sensors*, v. 15, n. 5, p. 9882–9898, 2015.

SANTOS, M. V. P.; SERRES, A. J. R.; GURJãO, E. C. Jammer localization using time difference of arrival algorithm in 5g mobile networks. In: *1st IEEE Latin American Conference on Antennas Propagation (LACAP 2024)*. [S.l.: s.n.], 2024. p. 1–2.

SHI, W. et al. Joint direction-of-departure and direction-of-arrival estimation in mimo array. In: *2013 IEEE International Conference of IEEE Region 10 (TENCON 2013)*. [S.l.: s.n.], 2013. p. 1–4.

TORRIERI, D. J. Arrival time estimation by adaptive thresholding. *IEEE Transactions on Aerospace and Electronic Systems*, AES-10, n. 2, p. 178–184, 1974.

ULUSKAN, S.; FILIK, T. A geometrical closed form solution for rss based far-field localization: Direction of exponent uncertainty. *Wireless Networks*, v. 25, n. 1, p. 215–227, Jan 2019. ISSN 1572-8196. Disponível em: <https://doi.org/10.1007/s11276-017-1553-7>.

VELEZ-LOPEZ, G. C. et al. A tool to solve nonlinear algebraic equations systems. In: *2019 16th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE)*. [S.l.: s.n.], 2019. p. 1–4.

WANG, T. et al. Sequential opening multi-jammers localisation in multi-hop wireless network. *IET Information Security*, John Wiley & Sons, Inc., USA, v. 12, n. 5, p. 445–454, sep 2018. Disponível em: <https://doi.org/10.1049/iet-ifs.2017.0346>.

WANG, T. et al. Localization of directional jammer in wireless sensor networks. In: *2018 International Conference on Robots Intelligent System (ICRIS)*. [S.l.: s.n.], 2018. p. 198–202.

WANG, T. et al. Adaptive jammer localization in wireless networks. *Computer Networks*, v. 141, p. 17–30, 2018. ISSN 1389-1286. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128618301920>.

WANG, T. et al. Jammer localization in multihop wireless networks based on gravitational search. *Sec. and Commun. Netw.*, John Wiley & Sons, Inc., USA, v. 2018, jan 2018. ISSN 1939-0114. Disponível em: <https://doi.org/10.1155/2018/7670939>.

WANG, T. et al. Mobile jammer localization and tracking in multi-hop wireless network. *Journal of Ambient Intelligence and Humanized Computing*, Feb 2018. ISSN 1868-5137, 1868-5145. Disponível em: <http://link.springer.com/10.1007/s12652-018-0708-4>.

WANG, Y.-B. et al. Arrival time estimation methodology for partial discharge acoustic signals in power transformers based on a double-threshold technique. *Measurement Science and Technology*, IOP Publishing, v. 30, n. 2, p. 025001, dec 2018. Disponível em: <https://dx.doi.org/10.1088/1361-6501/aaf554>.

WATSON, R. J.; LLOYD, E. M. The accuracy of a low-power approach for jammer angle-of-arrival estimation. In: *2020 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting*. [S.l.: s.n.], 2020. p. 1669–1670.

WEI, X.; WANG, T. Aigsa-based multi-jammer localization in wireless networks. *Applied Soft Computing*, v. 103, p. 107131, 2021. ISSN 1568-4946. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1568494621000545>.

WEI, X. et al. Collaborative mobile jammer tracking in multi-hop wireless network. *Future Generation Computer Systems*, v. 78, p. 1027–1039, 2018. ISSN 0167-739X. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X16306951>.

XU, W. et al. The feasibility of launching and detecting jamming attacks in wireless networks. In: *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. New York, NY, USA: Association for Computing Machinery, 2005. (MobiHoc '05), p. 46–57. ISBN 1595930043. Disponível em: <https://doi.org/10.1145/1062689.1062697>.

YADAV, A. P. et al. Probabilistic scheme for intelligent jammer localization for wireless sensor networks. In: BALAS, V. E.; SEMWAL, V. B.; KHANDARE, A. (Ed.). *Intelligent Computing and Networking*. Singapore: Springer Nature Singapore, 2023. p. 453–463.

YANG, F. et al. Jammer location-aware method in wireless sensor networks based on fibonacci branch search. *Journal of Sensors*, Hindawi, v. 2023, p. 2261730, May 2023. ISSN 1687-725X. Disponível em: <https://doi.org/10.1155/2023/2261730>.

ZEKAVAT, S. A.; BUEHRER, M. *Handbook of position location: theory, practice and advances*. Oxford: Wiley-Blackwell, 2012. (IEEE series on digital mobile communication). ISBN 9781118104750.

ZHANG, T. et al. Jamcatcher: A mobile jammer localization scheme for advanced metering infrastructure in smart grid. *Sensors*, v. 19, p. 909, 02 2019.

ZHANG, Z.; KANG, S. Time of arrival estimation based on clustering for positioning in ofdm system. *IET Communications*, v. 14, n. 15, p. 2584–2591, 2020. Disponível em: <https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-com.2019.0943>.

ZHANG, Z. et al. A shadowing loss compensation method for hybrid rss-based indoor localization. In: *2017 4th International Conference on Information Science and Control Engineering (ICISCE)*. [S.l.: s.n.], 2017. p. 1381–1385.

ZHAO, Z. et al. Receiver placement in passive radar through gdop coverage ratio with tdoa-aoa hybrid localization. In: *IET International Radar Conference (IET IRC 2020)*. [S.l.: s.n.], 2020. v. 2020, p. 476–480.