UNIVERSIDADE FEDERAL DE ITAJUBÁ

PROGRAMA DE PÓS-GRADUAÇÃO
EM ENGENHARIA ELÉTRICA

ANÁLISE DA SEGURANÇA CIBERNÉTICA DE MICRORREDES FRENTE A *REPLAY ATTACKS* UTILIZANDO MARCAS D'ÁGUA COMO TÉCNICA DE DETECÇÃO E PREVENÇÃO

Gustavo Ognibeni Troiano

Agosto de 2025

Itajubá – MG

UNIVERSIDADE FEDERAL DE ITAJUBÁ

PROGRAMA DE PÓS-GRADUAÇÃO
EM ENGENHARIA ELÉTRICA

Gustavo Ognibeni Troiano

ANÁLISE DA SEGURANÇA CIBERNÉTICA DE MICRORREDES FRENTE A *REPLAY ATTACKS* UTILIZANDO MARCAS D'ÁGUA COMO TÉCNICA DE DETECÇÃO E PREVENÇÃO

Dissertação de Mestrado submetida ao Programa de Pós-Graduação em Engenharia Elétrica como parte dos requisitos para a obtenção do Título de Mestre em Engenharia Elétrica.

Área de Concentração: Sistemas Elétricos de Potência
Orientador: Antonio Carlos Zambroni de Souza, Ph.D.
Coorientadora: Cláudia Eliane da Matta, Dra.

Agosto de 2025
Itajubá – MG

Dedico este trabalho ao meu Deus e à minha família.

AGRADECIMENTOS

Agradeço imensamente ao grande professor Antonio Carlos Zambroni de Souza pela orientação e por todo o apoio oferecido durante a elaboração desta dissertação. Serei eternamente grato pela confiança e pelo suporte incondicional prestados ao longo de todas as etapas deste trabalho.

Expresso também enorme gratidão à professora Cláudia Eliane da Matta, pela coorientação e pelos valiosos ensinamentos transmitidos ao longo deste processo.

Estendo meus agradecimentos à professora Eliane Valença Nascimento De Lorenci, cujas sugestões e contribuições foram fundamentais para a concretização desta dissertação.

Finalmente, dedico um agradecimento mais do que especial à minha família e aos muitos amigos que fiz durante o mestrado, pelo apoio constante, pela amizade e por cada momento, bom ou ruim, que compartilhamos.

RESUMO

A modernização dos sistemas elétricos de potência, caracterizada pela inserção cada vez mais intensa de novos equipamentos elétricos, elementos de comunicação, bem como pelo fluxo de energia bidirecional, deu origem ao conceito de redes inteligentes e, por consequência, à uma abordagem particular destas, denominada microrredes. As microrredes são sistemas que podem operar de maneira conectada ou isolada da rede principal, cujo funcionamento é assegurado por tecnologias de comunicação próprias. Estas, de acordo com o meio de transmissão e condições de propagação, estão sujeitas a perdas de informação ou problemas concernentes à segurança dos dados e ciberataques, com estes dois últimos quesitos tendo recebido atenção crescente nos últimos anos. Desta forma, o presente trabalho tem por objetivo verificar o desempenho do sistema de comunicação de uma microrrede no que tange ao tráfego seguro de dados, bem como mecanismos de prevenção e tratamento contra investidas virtuais maliciosas. Para isso, os sinais de controle da rede sob análise foram configurados com marcas d'água aditivas, sendo este mecanismo testado quanto à detecção e proteção contra *replay attacks* inseridos por agentes externos. Os estudos foram conduzidos inicialmente no circuito IEEE 13 Barras com a finalidade de validar a metodologia proposta, enquanto os testes subsequentes utilizaram como base uma modelagem da rede elétrica da Unifei. O sistema IEEE 13 Barras demonstrou comportamento satisfatório nos cenários de simulação implementados, autenticando comandos contendo marcas d'água legítimas e rejeitando aqueles sem autenticação ou com assinaturas inválidas. Para o modelo da microrrede da Unifei foram implementados quatro ambientes de testes distintos, os quais contemplaram diferentes níveis de ruído e atenuação provocados pelo canal de comunicação. Os resultados indicaram que, mesmo sob condições adversas, os sinais foram recuperados com sucesso, apresentando baixas taxas de falhas, sendo o ruído o principal fator de degradação em comparação à atenuação. Adicionalmente, embora tenham sido observados aumento de latência e consumo energético na microrrede, seus impactos na operação do sistema foram bastante reduzidos. Assim, as principais contribuições deste trabalho envolvem a caracterização da resiliência das marcas d'água frente à degradação da comunicação, além da análise dos impactos no desempenho e no consumo de energia da microrrede.

Palavras-Chave: Microrredes, Cibersegurança, *Replay Attack*, Marca D'Água, Simulação.

ABSTRACT

The modernization of electrical power systems, characterized by the increasingly intensive integration of new electrical equipment, communication elements, and bidirectional energy flow, has given rise to the concept of smart grids and, consequently, to a specific approach known as microgrids. Microgrids are systems capable of operating either in connection with or in isolation from the main grid, with their operation supported by dedicated communication technologies. These technologies, depending on the transmission medium and propagation conditions, are subject to information loss or issues related to data security and cyber-attacks, concerns that have received growing attention in recent years. The objective of this study is, therefore, to evaluate the performance of the communication system employed in the microgrid, with a focus on secure data transmission and on the implementation of mechanisms for the prevention and mitigation of malicious cyber-attacks. To this end, the control signals of the analyzed network were configured with additive watermarks, which were tested for their effectiveness in detecting and mitigating replay attacks initiated by external agents. Initial simulations were carried out using the IEEE 13-Bus circuit to validate the proposed methodology, while subsequent tests were based on a model of the power grid of Unifei. The IEEE 13-Bus system exhibited satisfactory performance under the implemented simulation scenarios, successfully authenticating commands containing valid watermarks and rejecting those lacking authentication or containing invalid signatures. Four distinct test environments were implemented for the Unifei microgrid model, incorporating varying levels of noise and attenuation introduced by the communication channel. The results indicated that, even under adverse conditions, the transmitted signals were successfully recovered with low failure rates, with noise being identified as a more significant degradation factor than attenuation. Furthermore, although increased latency and energy consumption were observed during operation, their impact on the performance of the microgrid was minimal. In summary, the main contributions of this work include the characterization of the resilience of watermarking mechanisms under degraded communication conditions, as well as an analysis of the impacts on performance and energy efficiency within the microgrid environment.

Keywords: *Microgrids, Cybersecurity, Replay Attack*, *Watermark*, *Simulation.*

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

1G	Primeira Geração
2G	Segunda Geração
3G	Terceira Geração
4G	Quarta Geração
5G	Quinta Geração
A1	Alimentador 1
A2	Alimentador 2
A3	Alimentador 3
A4	Alimentador 4
A5	Alimentador 5
AAA	Authentication, Authorization, and Accounting
ABB	Asea Brown Boveri
AD	Automação da Distribuição
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
ANEEL	Agência Nacional de Energia Elétrica
AP	Access Point
AWGN	Additive White Gaussian Noise
BAN	Building Area Network
BB	Broadband
BLE	Bluetooth Low Energy
CA	Corrente Alternada
CC	Corrente Contínua
CEMIG	Companhia Energética de Minas Gerais
CHP	Combined Heat and Power
COM	Component Object Model
CRC	Cyclic Redundancy Check
D7AP	DASH7 Alliance Protocol

DASH7	Developers Alliance for Standards Harmonization 7
DEP	Densidade Espectral de Potência
DES	Data Encryption Standard
DLMS	Device Language Message Specification
DLT	Distributed Ledger Technology
DNP3	Distributed Network Protocol 3
DoS	Denial of Service
DDoS	Distributed DoS
DSL	Digital Subscriber Line
EC	Elemento de Comunicação
EC	Extended Coverage
ECC	Elliptic Curve Cryptography
EMS	Energy Management System
FPB	Filtro Passa-Baixas
FRE	Fonte Renovável de Energia
FWaaS	Firewall as a Service
GD	Geração Distribuída
GSM	Global System for Mobile Communications
HAN	Home Area Network
HART	Highway Addressable Remote Transducer
HFC	Hybrid Fiber-Coax
HTTP	Hypertext Transfer Protocol
IAN	Industrial Area Network
IAP	Interoperability Architectural Perspectives
ICMP	Internet Control Message Protocol
IE	Intensivo em Energia
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Eletronic Engineers
IETF	Internet Engineering Task Force
IID	Identically Distributed
IoT	Internet of Things
IP	Intensivo em Potência
IP	Internet Protocol

IPSec	IP Security
ISA	International Society of Automation
ISO	International Organization for Standardization
L2TP	Layer 2 Tunneling Protocol
LAT	Laboratório de Alta Tensão
LDT	Linha de Distribuição Trifásica
LoRa	Long Range
LPWA	Low Power Wide Area
LR	Long Range
LTE	Long Term Evolution
LTE-A	LTE-Advanced
LTE-M	LTE for Machines
LTI	Linear Time Invariant
MAC	Medium Access Control
MD5	Message-Digest Algorithm 5
MGMS	Microgrid Management System
MIMO	Multiple Input Multiple Output
MiWi	Microchip Wireless
MPLS	Multiprotocol Label Switching
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NAN	Neighborhood Area Network
NB	Narrowband
NF	Normalmente Fechado
NR	New Radio
ONS	Operador Nacional do Sistema Elétrico
OpenDSS	Open Distribution System Simulator
OSI	Open Systems Interconnection
PAC	Ponto de Acoplamento Comum
PAN	Personal Area Network
PCH	Pequena Central Hidrelétrica
PFV	Painéis Fotovoltaicos
PHY	Physical
PID	Proporcional-Integral-Derivativo

PLC	Power Line Communication
PLL	Phase-Locked Loop
PPTP	Point-to-Point Tunneling Protocol
PWM	Pulse Width Modulation
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
REN	Resolução Normativa
RSA	Rivest-Shamir-Adleman
RU	Restaurante Universitário
SAE	Sistema de Armazenamento de Energia
SCADA	Supervisory Control and Data Acquisition
SEP	Sistema Elétrico de Potência
SGIRM	Smart Grid Interoperability Reference Model
SGW	Serving Gateway
SHA	Secure Hash Algorithm
SIG	Special Interest Group
SIN	Sistema Interligado Nacional
SNR	Signal-to-Noise Ratio
SQL	Structured Query Language
SSL	Secure Sockets Layer
STA	Station
STP	Shielded Twisted Pair
SYN	Synchronization
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TVWS	Television White Spaces
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UNB	Ultra Narrowband
UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair
VDSL	Very-high-bit-rate Digital Subscriber Line

VE	Veículo Elétrico
VHF	Very High Frequency
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WISA	Wireless Interface for Sensors and Actuators
XSS	Cross-Site Scripting

SUMÁRIO

CAPÍTULO 1 – INTRODUÇÃO

A inserção de novos e diversificados elementos nos sistemas elétricos modernos tem se intensificado cada vez mais nos últimos anos (EPE, 2019). Equipamentos de Geração Distribuída (GD), Fontes Renováveis de Energia (FRE), Veículos Elétricos (VE), Elementos de Comunicação (EC), bem como Sistemas de Armazenamento de Energia (SAE) têm tido suas aplicações difundidas de maneira crescente, alterando o perfil de funcionamento da rede para um fluxo bidirecional, tanto de energia, quanto de informações (Nascimento; Lorenci; Minami, 2022). Desta forma, a operação integrada entre todas essas entidades, deu origem ao conceito de redes inteligentes, as quais possibilitam diferentes configurações operativas do sistema elétrico, melhorando sua resiliência, segurança e eficiência (Ekanayake *et al.*, 2012). Dentro deste contexto, observou-se o surgimento de uma nova abordagem construtiva dos sistemas de energia, denominada microrredes (Roosa, 2020).

Microrredes nada mais são do que sistemas dotados de capacidade de operação autossuficiente, com forte inserção de GD, os quais estão habilitados a funcionar de maneira conectada ou isolada da rede (Delboni *et al.*, 2018). Em uma outra definição, microrredes podem ser consideradas como redes elétricas locais, com limites bem definidos, atuando como uma entidade única e controlável (Hu; Lanzon, 2019). São também entendidas como a integração de diferentes tipos de GD, SAE, sistemas de proteção inteligentes, e cargas que podem operar de forma independente ou colaborativa com os sistemas elétricos tradicionais, bem como com outras microrredes (Sinha; Kanwar, 2023).

Com isso, as microrredes podem ser implementadas em localidades remotas, como ilhas ou regiões de difícil acesso. Ademais, vale ressaltar que as fontes de geração integradas a estes sistemas são, em geral, renováveis, caracterizando-se por seus altos níveis de intermitência (Daza; Sperandio, 2019). Isto faz com que seja necessária a adoção de medidas que permitam o funcionamento destas redes, consoante aos limites pré-estabelecidos, tais como níveis de tensão nas barras, frequência de operação, atuação dos sistemas de proteção, dentre outros (Gimenes *et al.*, 2020).

Todo o equilíbrio operativo das microrredes é garantido por meio da inserção de mecanismos de controle, sendo estes subordinados a uma entidade coordenadora central, que faz parte do Gerenciamento do Sistema de Energia, do inglês *Energy Management System* (EMS) (Schwaegerl; Tao, 2014). Cada parte deste elemento controlador é integrada, uma à outra, através de um sistema de comunicação, estabelecido por meio dos mais diversos tipos de

tecnologias. Tais tecnologias podem ser cabeadas (fibra óptica, par trançado, cabos coaxiais e elétricos) ou sem fio (satélite, rede celular, rádio cognitivo, além de outras.) (Vadana *et al.*, 2020).

Os sistemas de comunicação, de acordo com o meio de transmissão, bem como suas condições de propagação, estão sujeitos a perda de informação, latência, *jitter*[1], além de problemas concernentes à segurança dos dados e cibersegurança (Shun-Ping Chen, 2020). Aspectos relacionados a estes dois últimos quesitos têm adquirido bastante relevância, à medida que o número de equipamentos conectados em rede aumenta consideravelmente ano após ano, sendo estimados mais de 27 bilhões de dispositivos, em nível global, até o ano de 2025 (Sen; Dasgupta, 2023).

Ao longo dos anos, diversos tipos de ataques cibernéticos foram criados por agentes maliciosos, visando o roubo de informações, inserção de dados falsos ou desatualizados, introdução de anomalias ou até mesmo a derrubada de sistemas ciberfísicos inteiros (Du *et al.*, 2023a). Uma das investidas criminosas mais comumente encontradas, especialmente em redes inteligentes e microrredes, são os denominados *replay attacks*, nos quais informações antigas ou incorretas são replicadas pela rede com a finalidade de induzir a operação a erro, visando a obtenção de vantagens econômicas de forma fraudulenta, bem como outros objetivos (Tahoun; Arafa, 2022). Com isso, técnicas de detecção e prevenção desta modalidade de ataque foram desenvolvidas, dentre as quais a inserção de marcas d'água na informação transmitida (Singh; Pati, 2020). Estes sinais são codificados na informação original pelo transmissor, os quais podem ser removidos pelo receptor, permitindo a recuperação correta e atualizada dos dados enviados (Ahmed; Palleti; Mishra, 2022).

1.1 PROBLEMAS DE PESQUISA

Ao longo dos anos, diversas modalidades de ataques cibernéticos foram desenvolvidas, com o objetivo de roubar informações, sabotar sistemas, inviabilizando sua operação de forma temporária ou permanente, além de outras finalidades. *Replay attacks* são investidas extremamente difíceis de se detectar (Naha *et al.*, 2023), uma vez que o atacante do sistema se utiliza de dados operativos antigos, armazenados durante um período específico de funcionamento da rede (Liu; Mo; Johansson, 2021). Com isso torna-se possível induzir sistemas de controle e medição inteiros a erro. Diversas técnicas de deteção deste tipo de ataque foram

[1] O termo *jitter* representa a variação dos atrasos de propagação sofridos pelos dados trafegados através da rede. Em suma, este parâmetro é calculado como o desvio padrão da latência média do sistema (Li, 2007).

já formuladas e testadas (Selin; Preetha Mathew, 2024), apresentando-se eficientes para determinados ambientes de aplicação, e ineficientes em outros. Sendo assim, à medida que novos cenários são implementados, onde tais mecanismos são aplicáveis, testes de validação de seu funcionamento podem ser formulados, tanto para o aprimoramento das técnicas existentes, quanto para o desenvolvimento de outras.

Desta forma, a medida que surgem novas técnicas de detecção e prevenção voltadas a prevenir modalidades específicas de ataques cibernéticos, como seria possível comprovar a eficácia de uma implementação destinada a mitigar um ataque em particular, sem a necessidade de submetê-la a todos os testes referentes ao sistema ciberfísico que visa proteger?

1.2 JUSTIFICATIVA

Ao longo do período compreendido entre 2016 e 2023, investimentos em segurança cibernética saltaram de 83 bilhões para 173,5 bilhões de dólares, refletindo um crescimento médio superior a 10 por cento, a nível global (Dunn Cavelty, 2024). Além disso, o mercado mundial de cibersegurança tem apresentado taxas de crescimento expressivas ao longo dos anos, com previsão de crescimento médio anual de 15 por cento até o ano de 2026 (Xu; Xu, 2022). Em contrapartida, ao mesmo tempo em que os investimentos são feitos, os crimes cibernéticos causam prejuízos enormes, os quais chegam a cifras de trilhões de dólares, no âmbito mundial (Miller; Bossomaier, 2024).

Com relação às redes inteligentes e, consequentemente, às microrredes, o mercado de segurança cibernética tem recebido bastante atenção das concessionárias de energia, dado que o sistema elétrico está cada vez mais automatizado e conectado à internet (Aurangzeb *et al.*, 2024). No ano de 2023, o Departamento de Energia dos Estados Unidos anunciou investimentos da ordem de 70 milhões de dólares na modernização dos sistemas cibernéticos de concessionárias rurais e municipais (Office of Cybersecurity, 2023). Com relação ao Brasil, em um período de dois anos, concessionárias como a Copel Paranaense, Light, Energisa, Enel, além da Eletronuclear, foram vítimas de investidas criminosas através da rede (Lima, 2022). Com isso, a Agência Nacional de Energia Elétrica (ANEEL) e o Operador Nacional do Sistema Elétrico (ONS) publicaram, respectivamente, a Resolução Normativa (REN) N° 964/2021 (ANEEL, 2021) bem como uma Rotina Operacional (ONS, 2022), as quais devem ser adotadas pelas empresas do setor elétrico, com o objetivo de aprimorar o ambiente de segurança da informação relativo ao Sistema Interligado Nacional (SIN).

1.3 OBJETIVOS

Desta forma, esta dissertação tem por objetivo verificar o desempenho do sistema de comunicação de uma microrrede no que tange ao tráfego seguro de dados, bem como mecanismos de prevenção e tratamento contra investidas virtuais maliciosas. Para isso, os sinais de controle da rede sob análise foram configurados com marcas d'água aditivas, sendo este mecanismo testado no que se refere à detecção e proteção contra *replay attacks* inseridos por agentes externos.

Os objetivos específicos deste trabalho são:

- Implementar, em Python, o sistema de controle da microrrede, responsável por gerenciar o sistema elétrico local, desenvolvido no *software Open Distribution System Simulator* (OpenDSS). Em cada barra do circuito, serão incorporados dispositivos capazes de gerar marcas d'água aditivas, as quais são integradas aos sinais de controle emitidos pela microrrede sempre que ocorrer uma anomalia em seu estado operacional.
- Validar a eficácia das marcas d'água quanto à detecção e prevenção de sinais emitidos por agentes maliciosos, visando alterar o estado operativo da rede. É esperado que apenas os elementos de comunicação que gerem a marca d'água correta, tenham seus sinais de comando recebidos e encaminhados pela rede.
- Configurar cenários de operação da microrrede relativos às violações de limites de consumo nas barras, considerando os fluxos de potências ativa e reativa em trechos específicos do sistema. Com isso, os ajustes pertinentes ao modo de operação do circuito só poderão ser validados caso os comandos recebidos e enviados pelo Centro de Controle contenham a marca d'água característica da planta. Além disso, a capacidade de detecção do sistema de segurança será avaliada mesmo na presença de perturbações, tais como ruído e atenuação nos sinais, bem como diante do envio intencional de marcas d'água falsas.

1.4 CONTRIBUIÇÕES

Ao longo dos anos, diversas técnicas de inserção de marcas d'água para o controle de sistemas cibernéticos foram desenvolvidas. Tais métodos têm se mostrado eficazes na detecção e prevenção de *replay attacks*, uma vez que as marcas d'água podem ser inseridas tanto em nível de sinal de controle, quanto diretamente em sensores e atuadores. Com isso, ainda que um

agente externo obtenha êxito ao invadir a rede de comunicação, este poderá ser detectado e neutralizado mediante a atuação do mecanismo supracitado (Patel, 2023).

Esta técnica, entretanto, pode provocar alguns problemas ao sistema no qual é introduzido, sobretudo no que se refere ao surgimento de transientes, perdas do sinal de controle, sobrecarga dos elementos da rede, bem como falsos alarmes de invasão (Patel, 2023). Dentre os diversos métodos existentes, a inserção de marcas d'água multi-senoidais aditivas, a qual foi adotada por este trabalho, se destaca por sua relativa simplicidade de implementação, uma vez que não requer o conhecimento do modelo matemático da planta, sendo necessário apenas que se saiba o valor de sua resposta em frequência (Ghamarilangroudi, 2020).

Desta forma, a contribuição desta dissertação consiste em implementar um ambiente de testes, bem como verificar a eficácia da técnica de inserção de marcas d'água aditivas nos sinais de controle de um modelo de sistema elétrico real, representado pela rede da Unifei, como mecanismo de detecção e prevenção de *replay attacks*. Através da avaliação de sua eficácia, funcionalidade, e maneira com a qual tal implementação afeta o desempenho da comunicação da microrrede, é possível definir potenciais cenários de aplicação, além de eventuais inadequações da técnica em questão. Com isso, pretende-se através do desenvolvimento deste trabalho, abordar temas relacionados à segurança cibernética, tecnologias existentes, possíveis aprimoramentos dos métodos já desenvolvidos, bem como a criação de novos outros.

1.5 MOTIVAÇÕES SOCIOCIENTÍFICAS

As motivações sociocientíficas do presente trabalho se referem a questões concernentes a segurança de informações sensíveis que, quando violadas, têm a capacidade de causar prejuízos inestimáveis a entidades públicas ou privadas, afetando sociedades inteiras, seja em nível local ou, até mesmo, global. Desta forma, o desenvolvimento, bem como o aprimoramento e validação de técnicas de prevenção e detecção de tais investidas são fundamentais para a garantia do bom funcionamento de sistemas críticos, tanto sob a ótica da proteção de dados, quanto do ponto de vista operacional.

No caso de instituições governamentais, ao serem atingidas por ataques cibernéticos, as informações de segurança nacional podem ficar em poder de criminosos ou de nações estrangeiras hostis, expondo potenciais vulnerabilidades de um país frente a ataques externos (Mishra *et al.*, 2022). Além disso, infraestrutura, setores estratégicos, bem como dados sensíveis, quando violados, têm o potencial de afetar a economia, não apenas em escala nacional, mas também mundial (Center for Strategic & International Studies, 2024).

Vale ressaltar que a garantia da continuidade de serviços de infraestrutura crítica, sejam estes de abastecimento de água, hospitais, tráfego, e posicionamento geográfico são fundamentais para o bom funcionamento de uma sociedade, inclusive na preservação de vidas humanas (Toledano, 2024). Além disso, ambientes cibernéticos seguros estimulam inovações através da propriedade intelectual, garantindo-se que estas não serão violadas, tampouco copiadas sem autorização. Assim, investimentos em pesquisa e desenvolvimento acabam por ser fomentados, tanto através do setor público, quanto por entidades privadas (Bani-Meqdad *et al.*, 2024).

Com relação às *smart grids* e microrredes, ataques cibernéticos podem provocar a interrupção massiva de sistemas elétricos inteiros, causando prejuízos à indústria, parada de serviços governamentais, roubo de informações, tanto de concessionárias, quanto de consumidores, perecimento de alimentos nas residências, dentre outros transtornos (Rajkumar *et al.*, 2023). No caso de países com invernos rigorosos, como Estados Unidos, Canadá, diversos países europeus e asiáticos, a falta de energia pode levar à ausência de insumos para a operação dos aquecedores das edificações locais, provocando até mesmo a morte de pessoas (Busby *et al.*, 2021).

1.6 ESTRUTURA DA DISSERTAÇÃO

Este trabalho está estruturado em cinco capítulos. No capítulo 2 é feita a revisão da literatura sobre segurança em microrredes, além de uma abordagem a respeito de suas principais características elétricas, bem como requisitos e tecnologias de comunicação aplicáveis. O capítulo 3 faz uma explanação sobre a metodologia desenvolvida para a implementação dos cenários de simulação. Neste trecho da dissertação são descritos os aspectos construtivos e operativos do sistema IEEE 13 Barras e da microrrede da Unifei, os quais foram modelados e utilizados nos testes, além de toda a configuração inserida nos *softwares* OpenDSS e Python, adotados para simular a rede elétrica e de telecomunicações, respectivamente. No capítulo 4 são demonstrados, analisados e discutidos os cenários de testes implementados nas simulações de *replay attacks* em microrredes, utilizando o esquema de detecção e validação por marcas d'água como estratégia de proteção. Nesta seção é verificada a eficácia do mecanismo implementado quanto à sua capacidade de detectar e validar adequadamente os sinais de controle da rede, sejam legítimos ou falsos, quando transmitidos sob diferentes condições do canal de comunicação. Ainda neste capítulo, são examinadas as latências adicionais introduzidas pela técnica, bem como o impacto no consumo energético dos elementos

monitorados. Por fim, o capítulo 5 apresenta as conclusões finais do texto, além de sugestões para trabalhos futuros.

CAPÍTULO 2 – MICRORREDES

As microrredes podem ser definidas como sistemas elétricos capazes de atuar de forma complementar às redes inteligentes, diferindo-se destas, principalmente, quanto à abrangência geográfica do circuito, capacidade energética, além da possibilidade de operarem conectadas ou isoladas do sistema elétrico principal (Du; Lu; Zhong, 2020). Em contrapartida, assim como as redes inteligentes, as microrredes possuem forte penetração de GD, SAE, bem como fluxo bidirecional de informações e de energia. Todas estas funcionalidades adicionais permitem não somente a inserção de novos componentes no sistema elétrico, mas também sua operação e expansão de forma menos custosa e mais eficiente que os métodos tradicionalmente empregados (Bollen, 2011).

Considerando os Sistemas Elétricos de Potência (SEP), do qual fazem parte as microrredes, estes basicamente dividem-se em três partes principais: geração, transmissão e distribuição. Dentre seus elementos, podem ser encontrados unidades geradoras, subestações de energia, transformadores de potência, bancos de capacitores, dispositivos de proteção, equipamentos de medição, além de diversos tipos de cargas (Kirschen, 2024). Para garantir que todos estes componentes do sistema elétrico possam se comunicar de forma eficiente e, por consequência, operarem de maneira apropriada, as tecnologias de comunicação a serem escolhidas para a transmissão dos dados devem seguir uma série de critérios técnicos. Assim, é necessário que se considere, dentre outros fatores, alcance, latência, capacidade de transmissão e protocolos de comunicação implementados pela tecnologia em questão (Begovic, 2012). Além disso, a comunicação da rede deve ser capaz de distinguir mensagens de alta e baixa prioridade, bem como transportar os diversos formatos de protocolos específicos que caracterizam os sistemas elétricos modernos, como o *Distributed Network Protocol 3* (DNP3), *Device Language Message Specification* (DLMS), MODBUS, *International Electrotechnical Commission 61850* (IEC 61850), etc (Butun; Sari, 2021).

Outro fator de importância a ser considerado em uma microrrede é a segurança relacionada à entrega e envio desses dados aos elementos do sistema elétrico. Uma vez que o fluxo bidirecional de informações é introduzido, processos como autenticação de usuários se fazem necessários, com o objetivo de evitar que a rede seja alvo de intervenções maliciosas, como: *Denial of Service* (DoS), *replay attacks*, *snooping*, acessos não-autorizados, dentre outros (Canaan; Colicchio; Ould Abdeslam, 2020). Assim, a rede deve ser implementada com os protocolos apropriados, de modo que seja capaz de defender-se desses tipos de investida. No

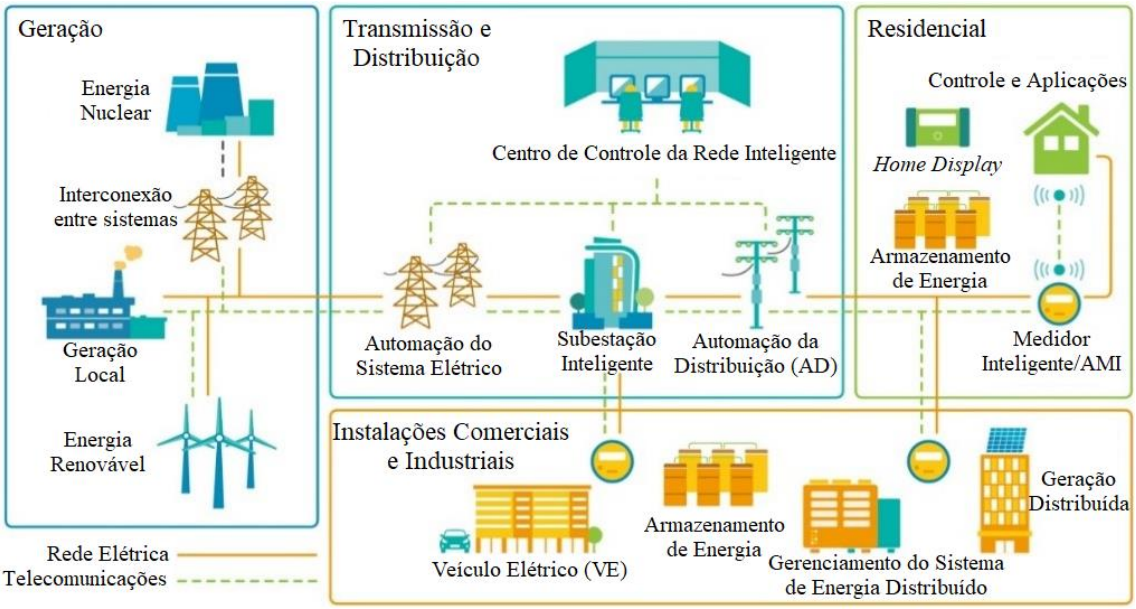
entanto, a introdução de atrasos excessivos de comunicação devido à inserção de tais protocolos é proibitiva, como também o aumento significativo do tamanho das mensagens, devendo ser assegurada, sobretudo, a inteligibilidade dos dados quando chegarem ao seu destino (Dong *et al.*, 2017).

Além de garantir o desempenho da comunicação e da segurança da microrrede, também se faz necessário que todos os seus elementos sejam capazes de desempenhar as funções a que foram designadas de maneira eficiente, independentemente da arquitetura do sistema e das tecnologias adotadas. Novos e antigos dispositivos da rede devem cumprir sua função de forma correta e específica, não interferindo na operação dos demais componentes do sistema elétrico, tais como: infraestrutura avançada de medição, do inglês *Advanced Metering Infrastructure* (AMI), automação da subestação, reguladores de tensão, acionamento da proteção, bem como outras funções da rede (Reddy; Kumar; Chakravarthi, 2022).

Por fim, é imprescindível que a microrrede assegure aos operadores, concessionárias e aos demais participantes do sistema a capacidade de interagir com cada uma de suas funções, de modo a implementar diferentes estratégias de monitoramento e operação, garantindo assim o cumprimento de algum objetivo específico, seja este baseado em modelos de negócio pré-definidos, de caráter técnico ou regulatório, como minimização das perdas elétricas, uso de energias renováveis, resposta à demanda, maximização dos lucros, além de outros (Fadlullah; Kato, 2014).

Com o objetivo de assegurar a operação coordenada de todos os dispositivos e funcionalidades dos sistemas elétricos modernos, foi criado o padrão *Institute of Electrical and Electronics Engineers Standard* 2030.4™-2023 (IEEE Std 2030.4™-2023). Esta norma, também conhecida como *Smart Grid Interoperability Reference Model* (SGIRM), define os requisitos de interoperabilidade entre os subsistemas componentes de uma rede inteligente, tanto para sistemas atuais, quanto futuros (IEEE, 2023). A Figura 1 ilustra a representação completa de uma rede inteligente, considerando seus elementos e respectivas subdivisões.

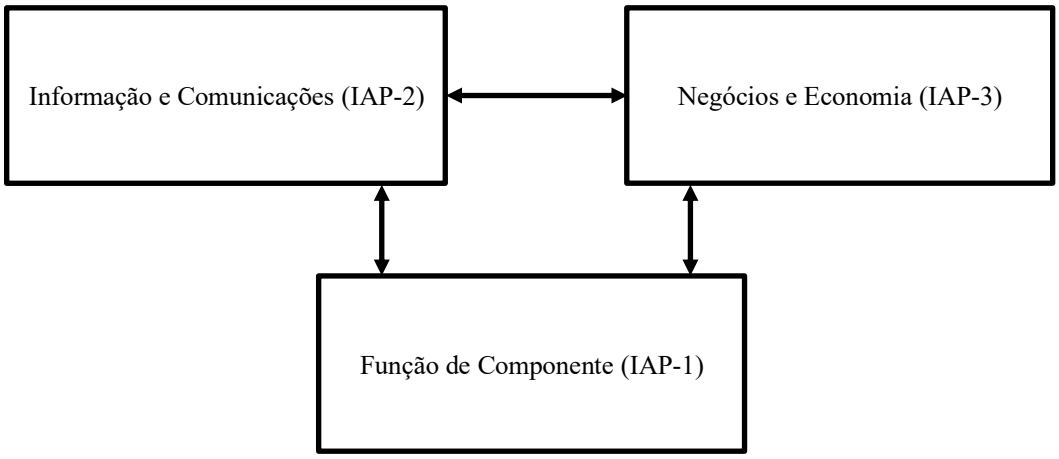
Figura 1 – Representação de uma rede inteligente.



Fonte: (CLP, 2023).

Para tratar da integração entre os elementos da rede inteligente, foram estabelecidas pelo padrão IEEE Std 2030.4™-2023 as Perspectivas para Interoperabilidade entre Arquiteturas, do inglês *Interoperability Architectural Perspectives* (IAP), para os subsistemas elementares, tratando de questões lógicas e funcionais dos sistemas de potência, de comunicação, tecnologia da informação, além de panoramas econômicos e de negócios (IEEE, 2023). A Figura 2 ilustra a interconexão de cada uma destas perspectivas.

Figura 2 – Interação entre as IAP do modelo SGIRM.



Fonte: (IEEE, 2023).

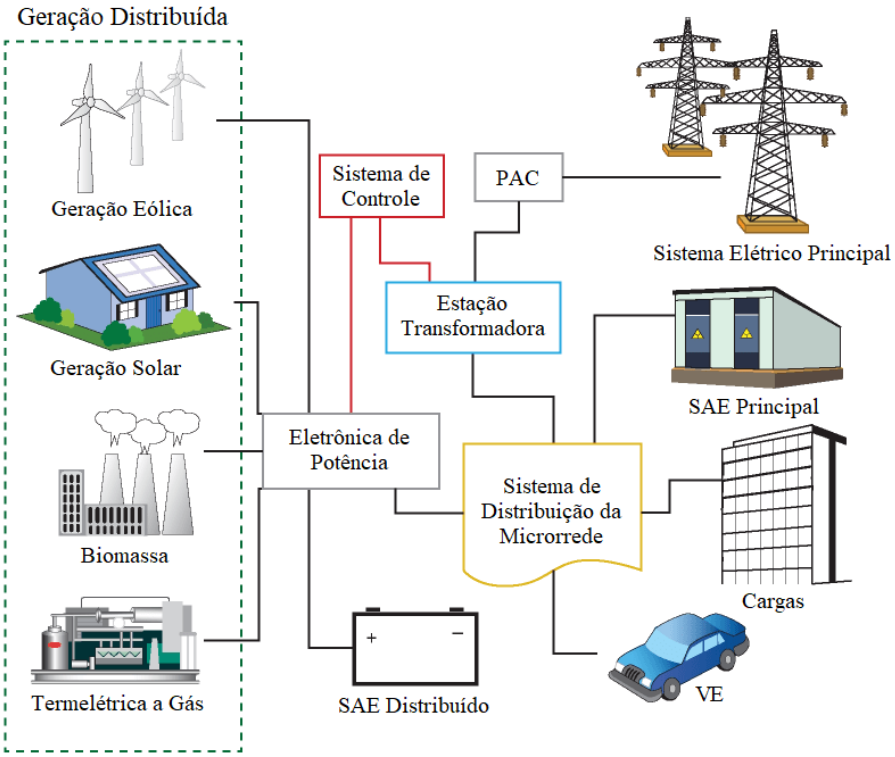
Com relação às subdivisões existentes em uma rede inteligente, serão apresentadas a seguir as arquiteturas básicas de seus componentes e funções (IAP-1), bem como dos seus

sistemas de informação e comunicações (IAP-2). Para isso, considerou-se os principais aspectos construtivos envolvidos, os elementos constituintes dos subsistemas, modos operacionais característicos, bem como a configuração de seus parâmetros essenciais. Uma vez que este trabalho se concentra apenas no aspecto técnico de segurança em microrredes, questões relativas a negócios e economia (IAP-3) não serão exploradas nas seções seguintes.

2.1 MICRORREDES SOB A PERSPECTIVA DOS SEP (IAP-1)

A arquitetura de sistemas de potência de uma rede inteligente abrange os segmentos da geração, transmissão e distribuição de um sistema de energia elétrica. Esta perspectiva pode ser estendida às microrredes, porém em escala reduzida, considerando seus equipamentos, controles e operações, provedores de serviços, consumidores e mercados (Liu *et al.*, 2021). A Figura 3 ilustra a integração de todos estes elementos de uma microrrede, relativos ao funcionamento do sistema de energia.

Figura 3 – Representação elétrica de uma microrrede.



Fonte: (Ebrary.net, 2023).

O barramento no qual cargas e fontes de geração se conectam, podem ser de Corrente Alternada (CA) ou Corrente Contínua (CC). As microrredes CA possuem como vantagens a conversão simplificada e econômica entre níveis de tensão, através de transformadores

eletromagnéticos. Já os sistemas CC necessitam de dispositivos baseados em eletrônica de potência, associados a complexos mecanismos de controle. Em contrapartida, os circuitos CC permitem a integração direta de determinadas fontes de geração, como supercapacitores, células a combustível e elementos fotovoltaicos. Além disso, o diâmetro dos cabos de energia destas redes é reduzido em comparação aos sistemas CA, dada a ausência do efeito pelicular[2]. Vale ressaltar, que as microrredes também podem ser do tipo híbrido, no qual são encontrados barramentos CA e CC, formando subsistemas conectados à rede principal. Uma vez que o presente trabalho trata apenas de sistemas CA, o texto subsequente fará referência somente a este tipo de configuração (Sechilariu; Locment, 2016).

2.1.1 *Elementos de uma microrrede*

Os elementos que constituem uma microrrede, basicamente incluem sistemas de geração distribuída, caracterizados pela forte inserção de fontes energéticas renováveis, dispositivos de armazenamento de energia, equipamentos de proteção, diferentes tipos de cargas, além de elementos conversores baseados em eletrônica de potência (Singh *et al.*, 2020), sendo cada um destes descritos a seguir de forma mais detalhada.

Com relação aos sistemas de geração distribuída, estes podem ser compostos por equipamentos geradores convencionais, como máquinas síncronas ou de indução, bem como por dispositivos baseados em eletrônica de potência, uma vez que a energia gerada por estes não é produzida na mesma frequência de operação da rede. Sob a perspectiva do controle de fluxo energético, tais fontes podem ser classificadas como despacháveis e não despacháveis. Dentre as fontes despacháveis comumente encontradas nas microrredes estão os geradores a diesel, Pequenas Centrais Hidrelétricas (PCH) e *Combined Heat and Power* (CHP). Em contrapartida, considerando as fontes não despacháveis, estão os sistemas fotovoltaicos e a geração eólica (Li; Li; Fengquan, 2015).

Por sua vez, os elementos de armazenamento de energia constituem parte importante das microrredes, dado que auxiliam na operação do sistema através do fornecimento de energia às cargas, quando em operações ilhadas, além de cumprir funções de estabilização de tensão e frequência. Podem ser de dois tipos principais: Intensivos em Energia (IE) e Intensivos em Potência (IP). Os dispositivos IE, basicamente cumprem funções como o gerenciamento da demanda, bem como outras aplicações do EMS. Já os elementos IP atuam durante mudanças

[2] O efeito pelicular é uma tendência que os elétrons possuem de trafegar na superfície dos condutores, à medida que a frequência de operação do circuito aumenta (Fowler, 2013).

abruptas na operação do sistema, e em flutuações de geração e carga. Vale ressaltar também que um único SAE pode cumprir ambas as funções (IE e IP). Os principais tipos de SAE encontrados nas microrredes são as baterias, os supercapacitores, e os *flywheels* (Zheng *et al.*, 2021).

As cargas que compõem as microrredes podem ser de vários tipos, como térmicas, elétricas, dentre outras. Estas, em geral, são inteligentes, as quais permitem a implementação de ações como, por exemplo, resposta em demanda, controles sobre o consumo e conta de energia, sendo classificadas como críticas e não críticas. As primeiras se caracterizam por não permitirem interrupções, ainda que por uma fração de segundo, devendo ser supridas, independentemente do nível de geração disponível e de seu custo. O segundo tipo possibilita o escalonamento da demanda, funcionando em períodos específicos, objetivando a economia de energia. Além disso, algumas cargas possuem operação previsível, tornando possível o gerenciamento e a resposta a demanda (Uddin *et al.*, 2023).

Considerando os sistemas de conversão, estes têm a função de adequar sinais CA para a frequência de operação da rede, ou transformar sinais CC em CA. Tais dispositivos podem ser encontrados em diversos equipamentos de geração distribuída, como turbinas eólicas, painéis fotovoltaicos, baterias e supercapacitores. Estes elementos permitem o controle, por parte da microrrede, da potência ativa, reativa, tensão e frequência (Sun *et al.*, 2022). Os conversores podem ser configurados de duas maneiras distintas: *grid-feeding* ou *grid-forming*, e *grid-following*. Para o primeiro caso, os conversores funcionam como fontes de corrente, estando permanentemente sincronizados com a rede. São implementados principalmente em fontes não despacháveis, as quais requerem a máxima extração de energia gerada. A segunda configuração faz com que os conversores operem como fontes de tensão, sendo sincronizados com o sistema por meio de dispositivos denominados *Phase-Locked Loops* (PLL). Em geral, são aplicados em geradores despacháveis, bem como SAE, produzindo potências ativa e reativa de forma complementar (de Andrade; Castilla; Bonatto, 2020).

Por fim, os sistemas de proteção de uma microrrede precisam ser acionados em duas situações específicas: falta no sistema principal; falta nas instalações da microrrede. No primeiro caso, o elemento de proteção deve atuar no Ponto de Acoplamento Comum (PAC), isolando a microrrede da rede externa. Quando de faltas internas, estas são projetadas para isolar o menor trecho possível do circuito. Para este caso, devido ao elevado número de conversores na rede, métodos tradicionalmente empregados em sistemas de distribuição, como sensibilidade por corrente de curto-circuito, não se mostram eficazes, uma vez que estas correntes possuem

magnitudes em torno de duas vezes a corrente nominal (Zheng *et al.*, 2021). Portanto, os esquemas de proteção das microrredes devem ser implementados de acordo com a topologia do sistema em questão, aplicando novas abordagens desenvolvidas para tal (Andrei *et al.*, 2020).

2.1.2 *Operação e Controle*

A interface entre as microrredes e o restante do sistema elétrico se dá por meio do PAC, nos quais são regulados basicamente os parâmetros de tensão, frequência (sincronização), potência ativa e reativa (controle de despacho). O projeto desta interconexão deve assegurar uma operação segura, confiável e economicamente viável da microrrede. Tais sistemas podem operar de três modos distintos: conectado, isolado, e em transição (Andrade; Castilla; Bonatto, 2020).

Quando conectada ao sistema principal, a microrrede opera importando e exportando energia da rede externa, garantindo o controle e o fluxo de energia e potência. Além disso, são asseguradas funções como serviços ancilares, controle de tensão e frequência, despacho e reservas operacionais, de acordo com as condições de geração e carga. Neste caso, tanto os conversores de fontes despacháveis quanto não despacháveis podem ser configurados como *grid-feeding*, uma vez que os sinais de sincronismo são fornecidos pelo sistema principal (Fusheng; Ruisheng; Fengquan, 2015).

O modo isolado pode ser introduzido na microrrede de forma intencional (manutenções programadas ou baixa qualidade de energia advinda da rede principal), ou não intencional, através de faltas, contingências, ou outros eventos imprevistos. Assim, deve-se garantir o suprimento das cargas críticas do sistema, operação econômica e melhoria da confiabilidade da microrrede. Quando nesta modalidade de funcionamento, ao menos um conversor deve estar configurado como *network-forming*, assegurando as condições de tensão, sincronismo e qualidade de energia do circuito (Haque *et al.*, 2022).

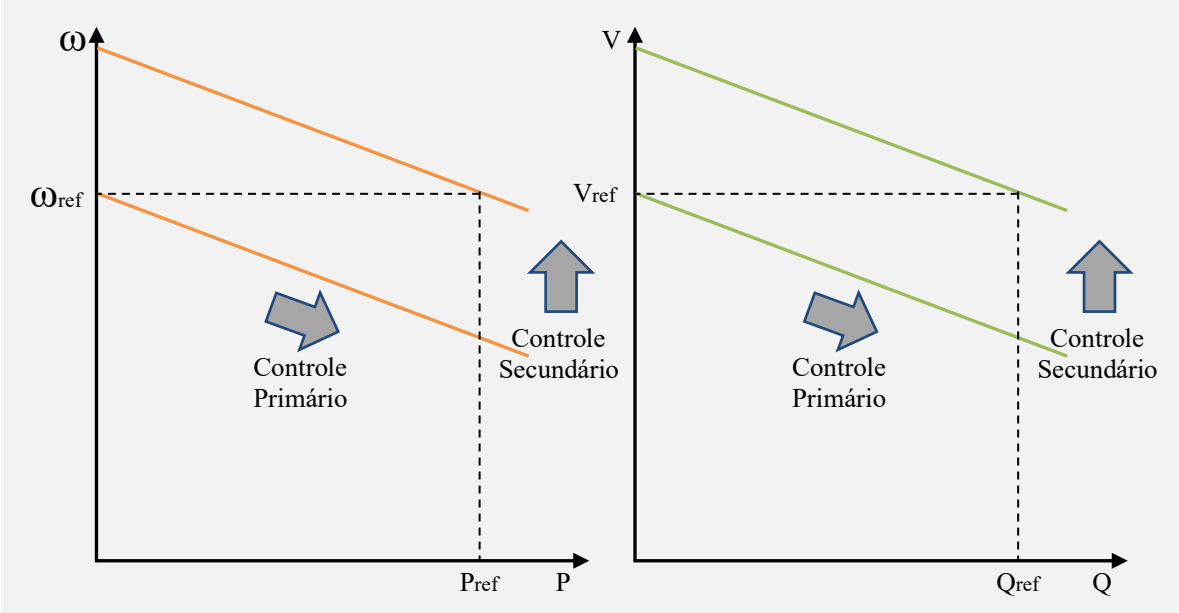
Já no período de transição entre os modos de funcionamento conectado e isolado, a reconexão da microrrede com o sistema principal deve ser feita rapidamente, assegurando o sincronismo de tensão, frequência e fase, além do sequenciamento correto de religamento dos geradores distribuídos, iniciando-se pelas unidades *grid-forming* para restabelecer a referência elétrica e, em seguida, pelas fontes *grid-feeding*, de modo a garantir a estabilidade na recomposição do sistema (Andrade; Castilla; Bonatto, 2020).

Considerando os níveis hierárquicos de controle das microrredes, estas são estruturadas para operarem em três níveis distintos: primário, secundário e terciário. As primeiras camadas

são implementadas diretamente nos dispositivos da rede, possuindo como característica respostas rápidas. Já os estágios superiores funcionam em nível de sistema, atuando de maneira mais lenta. O objetivo desta arquitetura é garantir qualidade de energia, prevenção de distúrbios, estabilidade de tensão e frequência, tudo isso ajustando os fluxos de potência ativa e reativa, filtragem de harmônicos, dentre outros (Mittal *et al.*, 2021).

O controle primário objetiva garantir a estabilidade de tensão e frequência frente a variações bruscas de carga ou geração. Quando da operação em modo ilhado, esse controle assegura a divisão igualitária de carga entre os inversores, adicionando inércia virtual aos mesmos, o que garante a emulação de propriedades físicas dos geradores convencionais. Assim, é possível o estabelecimento do controle de tensão e frequência por meio do método *droop*. Tal método é originário dos sistemas elétricos de grande porte, possibilitando que geradores com grande massa inercial trabalhem em paralelo, dividindo o fornecimento energético e reduzindo suas frequências de operação quando o carregamento da rede aumenta (Li; Nejabatkhah; Tian, 2022). A Figura 4 ilustra o funcionamento do controle *droop*.

Figura 4 – Funcionamento do controle *droop*.



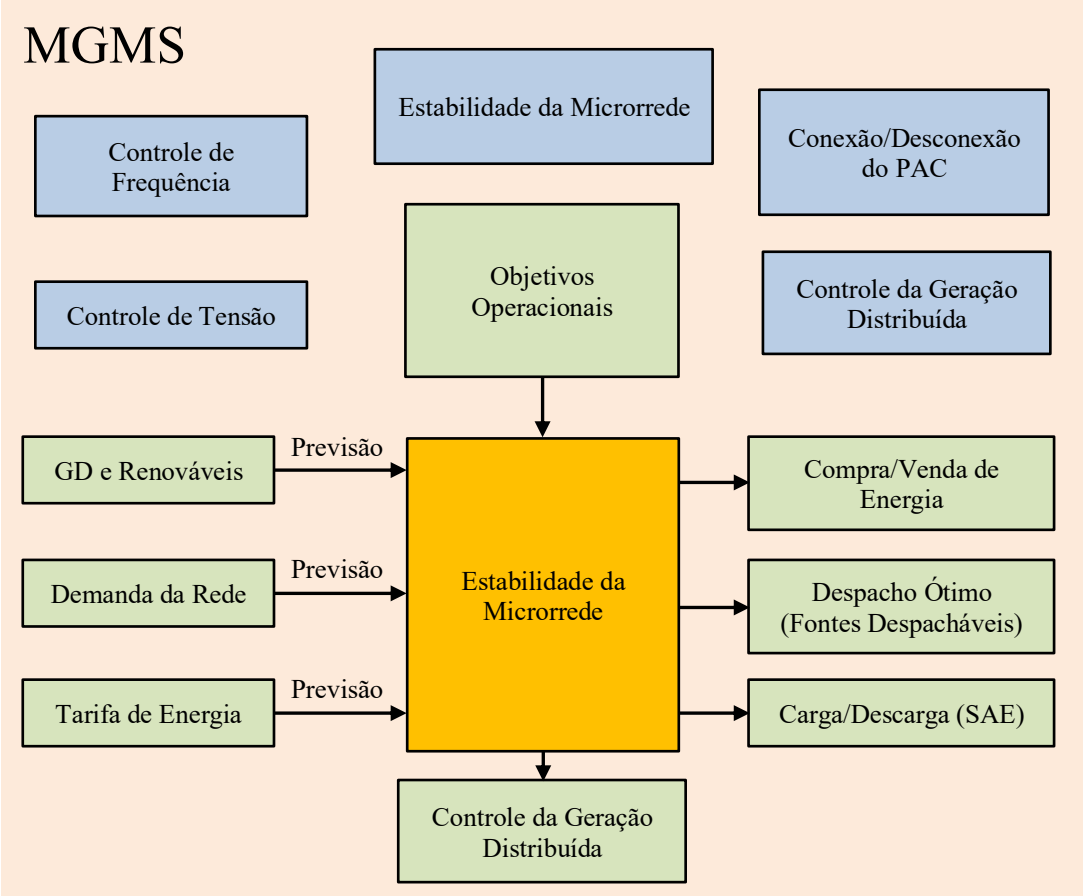
Fonte: (Andrade; Castilla; Bonatto, 2020).

A camada secundária tem a função de mitigar os desvios de tensão e frequência provocados pelo *droop* primário em regime permanente, restaurando seus valores para a referência do sistema, além de realizar a divisão de potência entre os geradores. Sem esse nível de controle, os desvios de tensão e frequência permanecem dependentes da carga, uma vez que

resultam da inércia virtual implementada nos inversores pelo controle primário e da impedância equivalente introduzida pelo método *droop* (Shafiee; Naderi; Bevrani, 2023).

Finalmente, o controle terciário é responsável pelo fluxo global de potência otimizado entre a microrrede e o sistema principal. Tudo isso depende de questões técnicas, econômicas, qualidade de energia (harmônicos), tolerância a faltas devido a flutuações da demanda, desbalanço ou interrupções, preços dinâmicos em períodos de pico de consumo, etc. Esta camada, por vezes, é referida como EMS, aplicada no modo de configuração centralizado da rede, otimizando a operação com o monitoramento de preços em tempo real, decisões automatizadas em custos de geração, previsões de tempo e informações de mercado. Estas funcionalidades e outras adicionais, como suporte de potências ativa e reativa, ilhamento, e serviços ancilares, podem ser providos pelo Sistema de Gerenciamento da Microrrede, do inglês *Microgrid Management System* (MGMS), o qual se comunica com as demais camadas por meio de um controle centralizado (Li *et al.*, 2023). A Figura 5 ilustra o funcionamento da integração entre o EMS e MGMS.

Figura 5 – Interação entre o EMS e MGMS.

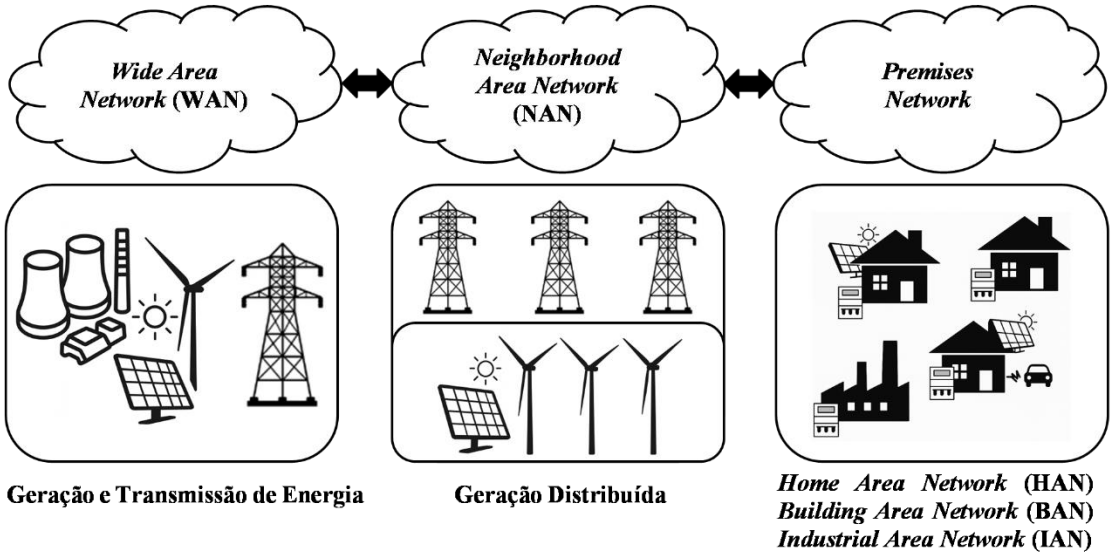


Fonte: (Zheng *et al.*, 2021).

2.2 MICRORREDES SOB A PERSPECTIVA DOS SISTEMAS DE TELECOMUNICAÇÕES (IAP-2)

A arquitetura de comunicação de dados de uma rede inteligente (ou microrrede) pode ser dividida em três segmentos: *Wide Area Network* (WAN), *Neighborhood Area Network* (NAN) e *Premises Network* (Shi; Wong, 2012). Estes trechos são responsáveis pela troca de informações e de mensagens de controle dentro de uma região específica do sistema de distribuição de energia elétrica. Além disso, para cada segmento especificam-se parâmetros como latência, taxas de transmissão, cobertura da rede e aplicações em potencial, os quais são detalhados mais adiante. A Figura 6 ilustra a arquitetura de comunicação de uma rede inteligente e suas respectivas subdivisões.

Figura 6 – Arquitetura de comunicação de uma rede inteligente.



Fonte: (Abrahamsen; Aí; Cheffena, 2021).

Considerando o trecho *Premises Network*, sua abrangência está limitada a apartamentos, casas, residências, conjuntos comerciais e fábricas. Recebe a informação de diversos dispositivos inteligentes, enviando, também, dados para estes mesmos elementos da rede com diferentes objetivos. Este segmento pode ser subdividido em *Home Area Network* (HAN), *Building Area Network* (BAN) e *Industrial Area Network* (IAN). O tráfego gerado por estas redes, pode chegar a centenas de kbps (Altin; Eyimaya, 2023).

O segmento NAN é responsável por fazer a conexão entre as instalações do cliente e o sistema da concessionária de energia elétrica. Sua área de atuação pode chegar a vários quilômetros quadrados, sendo capaz de conter centenas ou até milhares de medidores sob seu

controle. Os medidores, em conjunto, podem enviar até algumas centenas de Mbps, a depender das aplicações em execução. A NAN também é responsável por prover a conexão entre dispositivos de análise dos operadores da rede, como *laptops* e *tablets*, com elementos do sistema de transmissão, distribuição ou da subestação (Belu, 2022).

Já o trecho WAN é capaz de agregar múltiplos segmentos NAN e entregam os dados provenientes destas redes para o Centro de Controle da concessionária. Normalmente estes sistemas cobrem áreas extensas, chegando a abranger milhares de quilômetros quadrados, podendo gerar tráfegos de até centenas de Mbps (Refaat *et al.*, 2021). Assim, o Quadro 1 ilustrado a seguir, apresenta, de forma resumida, os três segmentos da arquitetura de comunicação mencionados, em termos da área de cobertura, taxa de dados requerida, bem como tecnologias de comunicação aplicáveis.

Quadro 1 – Características de comunicação de uma rede inteligente.

Subdivisão	**Cobertura**	**Taxa de dados requerida**	**Tecnologias aplicáveis**
Premises Network	Centenas de m^2	Entre 10 e 100 kbps	IEEE802.15.4 *Wireless Fidelity* (Wi-Fi) *Power Line Communication* (PLC) IEEE802.15.1 *Developers Alliance for Standards Harmonization 7* (DASH7) ZWave *Low Power Wide Area* (LPWA)
NAN	Até alguns milhares de km^2	Até algumas centenas de Mbps, dependendo do tamanho do sistema	Tecnologias Celulares Wi-Fi IEEE802.15.4g (*RF-Mesh*) PLC *Digital Subscriber Line* (DSL) *Cable Modem* Rádio Cognitivo LPWA
WAN	Milhares de km^2	Até algumas centenas de Mbps	Fibra Óptica Tecnologias Celulares *Cable Modem* Rádio Cognitivo Satélite

Fonte: (Ho *et al.*, 2014)–(Adler, 2023).

A seguir será feita uma breve explanação das tecnologias cabeadas e sem fio que podem ser aplicadas às redes inteligentes, atestando suas principais características quanto à capacidade, taxas de dados e cobertura. Como o foco do trabalho é baseado em microrredes, cuja área geográfica não excede ao trecho coberto pelas subdivisões *Premises Network* e NAN, apenas as tecnologias aplicadas a estes segmentos serão explicadas em maiores detalhes.

2.2.1 *Tecnologias Cabeadas*

Dentre os sistemas cabeados aplicáveis às microrredes, as principais tecnologias existentes atualmente são baseadas nos cabos de par trançado, de energia elétrica (PLC), bem como em cabos coaxiais. Existem diversos padrões de comunicação implementados sobre estes meios de transmissão, os quais devem ser selecionados de acordo com os requisitos do sistema de comunicação em questão. A seguir, cada uma destas tecnologias é apresentada de forma detalhada.

Os cabos de par trançado implementam dois padrões de comunicação principais: o DSL e o Ethernet. Os sistemas DSL fornecem tráfego de dados aproveitando a infraestrutura existente das operadoras de telefonia fixa, cuja tecnologia foi desenvolvida com o objetivo de prover altas taxas de transmissão, oferecendo largura de banda dedicada aos usuários. Existem diversas variantes do DSL, estando o *Asymmetric Digital Subscriber Line* (ADSL) e o *Very-high-bit-rate Digital Subscriber Line* (VDSL) entre as mais difundidas, alcançando taxas máximas de 24 Mbps e 300 Mbps, respectivamente (Dulaney, 2017)–(Otung, 2021). No que tange a tecnologia Ethernet, estas utilizam cabos de par trançado com quatro pares, os quais são ativados conforme a taxa de transmissão. Este padrão é definido pela especificação IEEE802.3, sendo cada par disposto desta forma de modo a se evitar o efeito de diafonia[3]. Tais cabos podem ser blindados (*Shielded Twisted Pair*, STP) ou não blindados (*Unshielded Twisted Pair*, UTP), possuindo diversas categorias de uso, que se adaptam aos padrões de transmissão Ethernet (Spurgeon; Zimmerman, 2014). A última especificação da tecnologia é padronizada pela categoria 8, atingindo taxas de até 40 Gbps para distâncias máximas de 30 metros (Docter; Buhagiar, 2022).

O PLC consiste no uso de cabos de energia elétrica para a transmissão de dados. Essa tecnologia já se encontra bastante difundida para fins de telemedição, alarmes, telecomandos e comunicação entre usinas geradoras e subestações de energia. Conforme novos padrões foram sendo desenvolvidos, o PLC passou a ser subdividido em três grandes grupos: *Ultra Narrowband* (UNB), *Narrowband* (NB) e *Broadband* (BB), atingindo taxas de transmissão que variam de 100 bps até a faixa dos Mbps (Kabalci; Kabalci, 2019).

Já os cabos coaxiais constituem sistemas de comunicação que utilizam *modems* para a transmissão de dados. Com isso, deu-se origem à tecnologia *cable modem*, a qual fornece taxas

[3] Diafonia é a interferência indesejada que um circuito causa em elementos vizinhos como efeito do campo magnético, originado pela circulação de corrente (Marin, 2020).

de transmissão capazes de atingir até 10 Gbps no *downlink* e 2 Gbps no *uplink*, dependendo do esquema de modulação utilizado (United States, 2016). Vale ressaltar que uma das principais aplicações da tecnologia *cable modem* é o seu uso em conjunto com fibras ópticas, formando as redes *Hybrid Fiber-Coax* (HFC). Devido à esta integração, a maior parte do percurso de transmissão do sinal é feito via fibra, deixando o sistema imune a interferências eletromagnéticas em uma parte considerável da rede. Além disso, tal configuração permite que a rede tenha ampla cobertura, sendo o sinal convertido de óptico para elétrico quando já próximo das instalações dos usuários (Akujuobi; Sadiku, 2007).

2.2.2 *Tecnologias Sem Fio*

As tecnologias sem fio foram desenvolvidas com o intuito de serem sistemas complementares às redes cabeadas, promovendo, assim, uma maior mobilidade do usuário e flexibilidade na localização e instalação de sua estrutura. Existem inúmeras tecnologias sem fio que são aplicáveis aos sistemas elétricos de potência, sendo caracterizadas, basicamente, por seu alcance e capacidade de transmissão de dados. A seguir, serão apresentadas, de maneira detalhada, as principais tecnologias sem fio com aplicações nos sistemas de comunicação das microrredes. São elas: o padrão IEEE802.15.4, o D7AP, o Z-Wave, o protocolo IEEE802.15.1, os rádios cognitivos, as tecnologias celulares, o Wi-Fi e os sistemas LPWA.

A especificação IEEE802.15.4 define as camadas física, do inglês *Physical* (PHY), e de enlace de dados, do inglês *Medium Access Control* (MAC), de sistemas sem fio aplicados a redes de monitoramento residencial e industrial, usando dispositivos com baixo consumo de energia. Este padrão proporciona alcances típicos entre 10 e 75 m, não sendo capaz de prover comunicação em malha (Zeng; Bao, 2023). Para isso, é necessária a introdução de aplicações específicas para a habilitação desta função. Algumas destas implementações, como o *Microchip Wireless* (MiWi), *Wireless Highway Addressable Remote Transducer* (WirelessHART), *International Society of Automation* 100.11a (ISA100.11a), ZigBee e Thread são usadas para comunicações de curta distância, normalmente voltadas para ambientes internos (Kumari *et al.*, 2022). Outras, como o padrão IEEE802.15.4g, possibilitam a implantação de redes de maior alcance, com milhares de dispositivos (Muñoz *et al.*, 2018). O IEEE802.15.4 opera nas faixas de frequência de 868 MHz, 915 MHz e 2,4 GHz, atingindo taxas que variam de 20 kbps até 250 kbps (Zeng; Bao, 2023).

Considerando o DASH7 *Alliance Protocol* (D7AP), este consiste em um padrão concebido para comunicações entre sensores e atuadores, tendo sido originado através da

especificação *International Organization for Standardization* 18000-7 (ISO 18000-7). Esta tecnologia opera na banda de Sub-1GHz, utilizando canais de comunicação com duas opções de largura de faixa: 25 kHz ou 200 kHz. Trata-se de um protocolo de baixo consumo de energia, com taxas de transmissão máximas de 167 kbps e comunicações multi-saltos, atingindo distâncias de até 2 km. Além disso, pode ser implementado nas topologias estrela ou árvore, sendo composto por três tipos de dispositivos distintos: *gateways*, subcontroladores e *endpoints* (Ghorpade; Zennaro; Chaudhari, 2021).

Com relação ao protocolo Z-Wave, este foi desenvolvido no ano de 2001 pela companhia dinamarquesa Zensys, o qual é mantido atualmente pela Z-Wave *Alliance.* O Z-Wave é uma tecnologia utilizada em sistemas de automação residencial, como controle de iluminação e outros acionamentos. Opera nas faixas de 868 e 915 MHz, com taxas de 100, 40 e 9,6 kbps, alcance máximo de 100 metros, e com baterias que chegam a durar 5 anos[4] (Secgin, 2023).

Já o IEEE802.15.1 é uma especificação de redes *Personal Area Network* (PAN), no qual se baseia o protocolo Bluetooth. Esta tecnologia utiliza a frequência de 2,4 GHz, sendo mantida e atualizada[5] pelo Bluetooth *Special Interest Group* (SIG), cujos padrões devem ser seguidos rigorosamente pelos fabricantes para que possam comercializar seus produtos. O alcance de transmissão varia, conforme a classe do rádio utilizado no dispositivo. Existem duas modalidades desta tecnologia que são o Bluetooth Clássico e o *Bluetooth Low Energy* (BLE). O Bluetooth Clássico atinge taxas de até 3 Mbps. É aplicável em perfis de transmissão contínuos, suportando comunicações de voz e latências de 100 ms. O BLE, também conhecido como *Bluetooth Smart* suporta taxas de até 2 Mbps (Cheruvu *et al.*, 2019), consumindo menos de 50 por cento da energia do padrão clássico. É aplicável em transmissões em rajada, com latências de até 6 ms, não suportando comunicações de voz (Fraccarolli; Quaglia, 2020). Além do Bluetooth, o *Wireless Interface for Sensors and Actuators* (WISA) é um protocolo desenvolvido pela empresa *Asea Brown Boveri* (ABB) em 2003, o qual se baseia na especificação PHY e MAC do padrão IEEE802.15.1, com operação na faixa de 2,4 GHz. Possui

[4] Recentemente foi introduzido no mercado o Z-Wave *Long Range* (LR), o qual encontra-se regulamentado somente nos Estados Unidos. Tal especificação opera apenas na topologia estrela, suportando até 4000 dispositivos por elemento controlador. Além disso, pode atingir até 1,6 km de distância de comunicação, utilizando baterias com capacidade de duração de até 10 anos (Z-Wave Alliance, 2023).

[5] A última atualização do padrão é a Bluetooth 5.3, a qual foi publicada em 13 de julho de 2021. Esta traz melhorias na confiabilidade, eficiência energética e na experiência do usuário, permitindo, dentre outras funcionalidades, que o canal de transmissão seja definido tanto pelo nó central, quanto pelo elemento periférico (Silicon Labs, 2023).

taxas de transmissão de até 1 Mbps, bem como funcionamento em modo determinístico, atingindo dezenas de metros de alcance na comunicação (Berténi, 2012).

Rádios cognitivos são elementos definidos por *software* que usam técnicas de detecção e medição do espectro de frequências em faixa larga. Esta tecnologia permite que os dispositivos tenham seus parâmetros operacionais reconfigurados de acordo com a frequência a ser usada, aproveitando de forma secundária os períodos de ociosidade proporcionados em espectros licenciados de rádio e televisão (Wyglinsky; Nekovee; Hou, 2009). Existem alguns padrões que fazem uso de rádios cognitivos, destacando-se o IEEE802.22, também conhecido como *Television White Spaces* (TVWS) que garante acesso às bandas de *Very High Frequency* (VHF) e *Ultra-high Frequency* (UHF), disponíveis em algumas localidades depois da migração de diversos sistemas para a televisão digital. Possibilita taxas de 1,5 Mbps no *downlink* e 384 kbps no *uplink*, com alcances típicos entre 17 e 30 km, podendo chegar até 100 km, a depender das condições de propagação (Kalidoss; Bhagyaveni; Vishvaksenan, 2022).

As tecnologias celulares foram originalmente desenvolvidas para prover aplicações de voz, mesmo com o usuário em movimento. Com o passar dos anos, essa funcionalidade também foi estendida para serviços de dados. Esses sistemas operam em bandas de frequência licenciadas[6] com taxas de transmissão que variam desde 171,2 kbps (2G) até 20 Gbps (5G). As tecnologias 3G foram as primeiras a fornecer acesso em alta velocidade aos dispositivos móveis, através do mecanismo de comutação de pacotes, juntamente com a parte de comutação de circuitos já existente nos padrões 1G (analógico) e 2G (digital) (Jeszensky, 2004). Os sistemas 4G, em contrapartida, estabelecem uma comunicação inteiramente baseada em comutação de pacotes sobre protocolo de internet, do inglês *Internet Protocol* (IP). Entende-se o *Long Term Evolution* (LTE) como tecnologia celular 4G, sendo este capaz de operar nos modos de duplexação por divisão de frequência (Tipo 1) ou por divisão temporal (Tipo 2), além de implementar a técnica de transmissão denominada *Multiple Input Multiple Output* (MIMO). O LTE-*Advanced* (LTE-A) e o LTE-*Advanced* Pro, configuram evoluções do LTE, os quais são capazes de atingir taxas de transmissão de até 100 Mbps e, no segundo caso, superiores a 1 Gbps (Bruno; Jordan, 2024). Já o sistema 5G, sendo também conhecido como *New Radio* (NR), permite que o usuário atinja taxas de transmissão máximas de 20 Gbps no *downlink*, e de 10 Gbps no *uplink*, com latências que variam de 1 a 4 ms (Atarashi *et al.*, 2020). Essa tecnologia pode operar em duas faixas de frequências distintas: uma delas, compreende o espectro abaixo

[6] As tecnologias 4G e 5G possibilitam também a implementação de redes privadas, bem como a utilização do espectro não licenciado para operação (Holma *et al.*, 2019).

de 6 GHz, nomeada como faixa de Sub-6GHz. A outra, entre 24 GHz e 100 GHz, é conhecida como faixa de ondas milimétricas. A faixa de Sub-6GHz, devido ao seu menor potencial, é usada para cobertura e controle da rede, ao passo que o uso das frequências milimétricas se destina ao tráfego de dados propriamente dito, característica esta que explica as altas taxas de transmissão atingidas pelo sistema (Lau, 2021). Assim como o LTE, o 5G é implementado nos modos de duplexação por divisão frequencial ou temporal (Lin; Lee, 2021).

Baseado na especificação IEEE802.11, o Wi-Fi é um protocolo de redes cuja implantação pode ser realizada de duas formas: (a) modo infraestrutura; (b) modo *ad-hoc*. No modo infraestrutura, todos os nós, do inglês *Station* (STA), se comunicam somente com um único ponto de acesso, do inglês *Access Point* (AP), que coordena toda a comunicação entre eles, além de prover acesso para outras redes. Nessa arquitetura, o alcance da comunicação atinge distâncias máximas de 500 metros, operando nas faixas de frequência de 2,4, 5 e 6 GHz (Morais, 2023). A última especificação do Wi-Fi é o IEEE802.11be[7], o qual atinge taxas de até 46 Gbps (Yarali, 2023). Para o modo *ad-hoc*, cada nó interage diretamente com todos os outros de forma independente, sem a necessidade de um elemento mediador.

Por fim, as tecnologias LPWA foram desenvolvidas com o objetivo de atender os requisitos de comunicação de internet das coisas, do inglês *Internet of Things* (IoT), em que são previstas interconexões dos mais variados tipos de dispositivos através de uma única plataforma(Gu *et al.*, 2020). Tais sistemas, dentre outras características, apresentam um perfil de comunicação representado pela baixa demanda de dados, bem como previsibilidade de tráfego, os quais podem ser emitidos de forma contínua ou em intervalos pré-definidos Muitos destes elementos encontram-se instalados em locais isolados e/ou de difícil acesso, sendo necessária a implementação de interfaces de comunicação com baixo consumo de energia, de maneira que o dispositivo opere sem a necessidade de frequentes trocas de bateria. De igual modo, as redes de comunicação devem possuir cobertura ampla e longos alcances de transmissão (Ouaissa *et al.*, 2024). Dentre as principais tecnologias LPWA existentes estão o LTE *for Machines* (LTE-M), *Narrowband*-IoT (NB-IoT), *Extended Coverage Global System*

[7] Existem outros padrões Wi-Fi os quais foram desenvolvidos para aplicações específicas. O White-Fi, especificado sob a norma IEEE802.11af, aproveita as bandas de televisão ociosas do espectro Sub-1GHz (Agha; Loygue; Pujolle, 2022). Já o Wi-Gig (IEEE802.11ad), foi projetado para transmissão de dados na faixa de 60 GHz, atingindo taxas de até 7 Gbps (Masson; Berbineau, 2017). Por fim, o Wi-Fi HaLow consiste em uma tecnologia cuja operação se dá abaixo de 1 GHz de frequência, suportando até 6000 elementos por AP e alcances máximos de 1 km (Zakariya Saleh, 2023).

for Mobile Communications-IoT (EC-GSM-IoT), Weightless, Sigfox, *Long Range* WAN (LoRaWAN) e INGENU.

2.3 MICRORREDES SOB A PERSPECTIVA DAS TECNOLOGIAS DE INFORMAÇÃO (IAP-2)

A arquitetura de tecnologia de informação de uma microrrede refere-se ao projeto e toda a infraestrutura que habilita a sua operação eficiente, bem como o controle e monitoramento de todos os dispositivos do sistema, por meio da utilização de equipamentos, protocolos de comunicação e elementos de *software* apropriados (Li, 2022). Sendo assim, esta seção tem por objetivo apresentar, em maiores detalhes, as entidades de tecnologia de informação que compõem esta arquitetura, os tipos de ataques cibernéticos mais comuns da atualidade, dando ênfase ao *replay attack*, além das principais técnicas de detecção e prevenção deste tipo de investida, em especial, a inserção de marcas d'água nos sinais trafegados pela rede.

2.3.1 *Entidades de Tecnologias de Informação*

Com relação às entidades de tecnologias de informação das microrredes, estas abrangem elementos responsáveis pelas mais diversas funções desempenhadas pelo sistema, constituindo-se basicamente de dispositivos de *hardware* e *software*, os quais emitem e asseguram que comandos, bem como todas as informações trafegadas cheguem ao destino de forma segura (Li, 2022). Ademais, todo o armazenamento dos dados relativos aos consumidores, registros de acesso, informações mercadológicas e operacionais, devem ser realizados de maneira confiável (Zhang, 2021).

No que tange aos equipamentos de *hardware* existentes nas microrredes, estes constituem-se de medidores, sensores, dispositivos coletores de dados e telemetria, os quais estão relacionados com a produção, consumo de energia, além da estabilidade operativa e informações climáticas (Ayele; Gonzalez; Teeuw, 2024). Outros equipamentos que fazem parte desta arquitetura são roteadores, *switches*, servidores, estações de acesso, dispositivos de armazenamento de informações e *Uninterruptible Power Supplies* (UPS), cuja função é assegurar o funcionamento de toda a infraestrutura de dados, em caso de falta de energia (Hahn, 2017). Para que cada um destes elementos de *hardware* opere de maneira integrada e otimizada, diversas tecnologias foram desenvolvidas, as quais atuam de maneira complementar aos mesmos. Dentre elas estão as *Distributed Ledger Technologies* (DLT); aplicações como as

Virtual Private Networks (VPN), *Multiprotocol Label Switching* (MPLS) e *Virtual Local Area Networks* (VLAN); os servidores *proxy*, *firewalls*, e *Serving Gateways* (SGW); além das técnicas de criptografia, *hashes* e autenticação. Os parágrafos a seguir descrevem cada uma destas tecnologias de maneira detalhada.

As DLT, também conhecidas como *shared ledger* ou somente *distributed ledger* consistem em bases de dados compartilhadas, que são distribuídas entre os participantes de uma rede e espalhadas por múltiplos *sites* e organizações (Bashir, 2020). Com isso, é possível estabelecer mecanismos de confiança em cada uma das transações ocorridas no sistema, por meio das quais são geradas múltiplas cópias, interligadas uma à outra através de um algoritmo criptográfico (Soltani *et al.*, 2022). Existem diversas tecnologias que compõem as DLT, diferindo entre si com relação à estrutura de registros, bem como quanto ao algoritmo de consenso, os quais determinam a forma como os dados, blocos ou qualquer outra informação são armazenados e validados pela DLT (Laufenberg *et al.*, 2020). Dentre as principais variantes existentes, estão o Blockchain, Tangle, Hashgraph, Sidechain, Holochain e Tempo (Radix).

Com relação às VPN, estas são tecnologias as quais permitem que redes privadas sejam estendidas sobre infraestruturas de comunicação públicas através de conexões seguras e criptografadas, assegurando-se que os dados não sejam interceptados nem lidos (Fox; Hao, 2017). A implementação de uma VPN pode ocorrer de três formas distintas: remota, que é quando um dispositivo externo se comunica com uma rede corporativa; *site-to-site*, sendo que a conexão entre duas ou mais redes é estabelecida em localidades diferentes, através de *gateways* e roteadores; ou híbrida, que é a combinação dos modos remoto e *site-to-site* (Naduvath, 2024). São criadas sobre diferentes protocolos, os quais definem regras para o estabelecimento e manutenção de conexões seguras entre cliente e servidor. Dentre as principais tecnologias de VPN consolidadas estão o *Point-to-Point Tunneling Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP), IP *Security* (IPSec), *Secure Sockets Layer/Transport Layer Security* (SSL/TLS) e WireGuard VPN (Easttom II, 2023).

O MPLS é uma técnica capaz de combinar as funções de roteador e *switch* de forma simultânea, operando nas camadas 2 e 3 do modelo *Open Systems Interconnection* (OSI). É padronizado pelo *Internet Engineering Task Force* (IETF), permitindo que protocolos sem conexão, como o IP, ofereçam qualidade de serviço, do inglês *Quality of Service* (QoS), à comunicação. Utiliza-se de rótulos (*labels*), ao invés de tabelas de roteamento para o encaminhamento do tráfego, sendo mais rápido e consumindo menos banda que uma

comunicação IP convencional, promovendo balanceamento de carga entre *links*, *switches* e roteadores da rede (Sharma; Singla, 2015).

A tecnologia VLAN possibilita que uma rede local seja segmentada, de forma lógica, sobre uma infraestrutura física. Com isso, podem agrupar equipamentos pertencentes a um mesmo departamento, tipo de dados, bem como outros critérios. Oferecem segurança ao sistema, performance, controle de *broadcast*, bem como facilidades de gerenciamento e configuração, realizados por *software*. Podem ser implementadas de diversas formas, como em portas de equipamentos de rede, baseadas em *tag* (IEEE802.1q), em arquiteturas privadas, dentre outras, sendo distinguidas por um identificador de VLAN. (Shin, 2017).

Servidores *proxy* são elementos dedicados que agem como equipamentos intermediários entre a internet e o cliente, ou outro servidor. Estes dispositivos têm a função de melhorar a performance da rede, sua segurança, bem como realizar o controle de tráfego. Com isso, torna-se possível a aplicação de filtros de bloqueio a certos tipos de conteúdo, escaneamento de arquivos para verificação de *malwares*, sigilo de endereços IP, dentre outros (Dalela; Dalela, 2023). Existem diversos tipos de *proxies*, sendo os mais comuns o *forward proxy* e o *reverse proxy*, os quais tem a função de proteger clientes e servidores, respectivamente (Danturthi, 2023).

Já os *firewalls* agem como barreiras entre redes internas confiáveis, e ambientes externos desconhecidos, como a internet. Utilizam-se de regras predefinidas para permitir ou bloquear o tráfego de dados, baseadas na origem, destino, protocolo, número de porta lógica ou domínio, bem como com relação ao tipo de informação transmitida (Brooks; Junior, 2022). Podem ser implementados em *hardware*, *software*, combinar ambos, ou serem disponibilizados em nuvem como um serviço de rede, do inglês *Firewall as a Service* (FWaaS) (Kizza, 2024).

Considerando os SGW, estes protegem uma organização contra ameaças de segurança *online*, bem como infecções causadas por *softwares* ou *malwares* iniciados pelo tráfego do usuário. Asseguram a aplicação de políticas de segurança com filtragem de conteúdo baseadas em contexto, implementando a proteção bidirecional contra invasores e acessos externos por parte dos usuários. Possuem foco na camada de aplicação, diferindo-se dos *firewalls* por inspecionar dados com base em protocolos e cabeçalhos, ao invés de pacotes (Naggi; Sales, 2021).

A criptografia de dados é obtida por meio da aplicação de um algoritmo criptográfico em uma mensagem qualquer. Neste processo, também são utilizadas chaves, tanto na cifragem, quanto na decifragem da informação, podendo se apresentar de duas formas distintas: simétrica

e assimétrica (Rubin, 2022). A criptografia simétrica, também conhecida como *single-key* ou *secret-key*, utiliza a mesma chave, tanto na encriptação, quanto na decriptação dos dados. São exemplos de algoritmos simétricos: *Advanced Encryption Standard* (AES), *Data Encryption Standard* (DES), 3DES, Salsa20, Chacha20 e Rivest Cipher 4 (RC4) (Sakkari; Ulla, 2022). Já a criptografia assimétrica utiliza duas chaves para tal, sendo uma pública e a outra, privada, as quais estão ligadas matematicamente entre si. A primeira é compartilhada pelo usuário com os demais participantes da rede, ao passo que a chave privada é armazenada localmente. Dentre alguns exemplos desta técnica de cifragem estão o Rivest-Shamir-Adleman (RSA), *Elliptic Curve Cryptography* (ECC), Diffie-Hellman e ElGamal (Banoth; Regar, 2023).

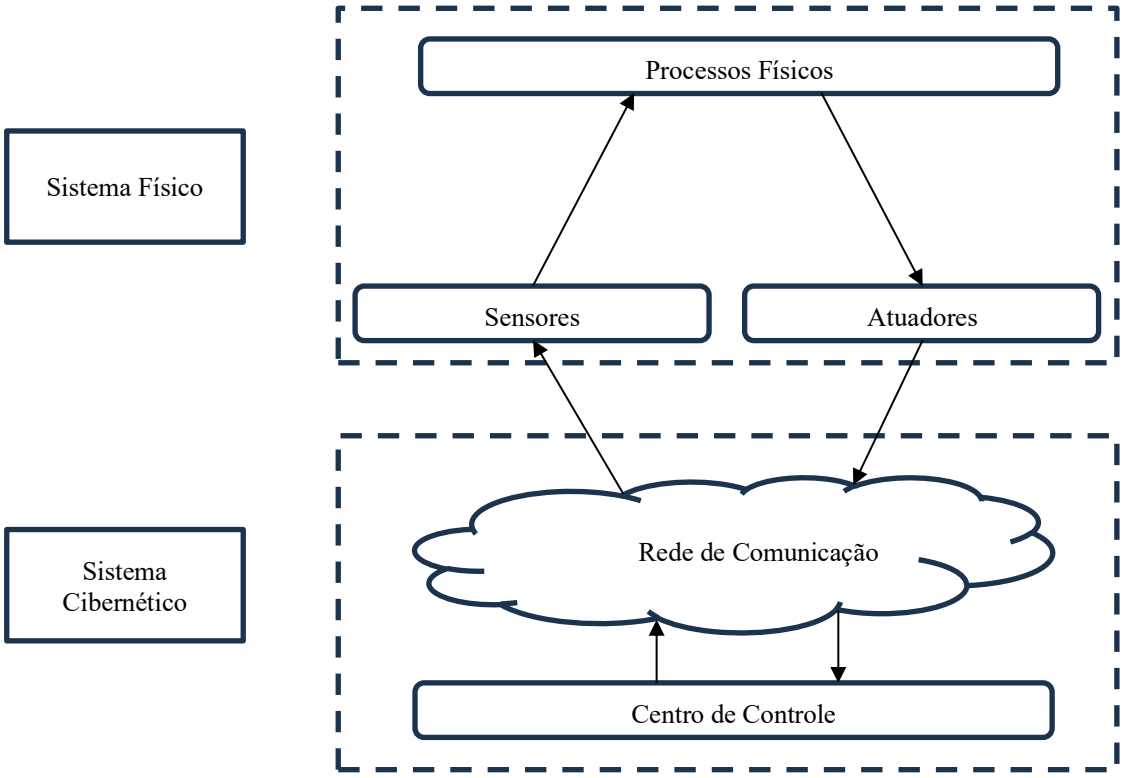
A tecnologia de *hashes* tem a função de assegurar a integridade dos dados a partir de um valor de *hash*, por meio da criptografia dos dados. Ao receberem uma entrada, estes retornam uma *string* de tamanho fixo, denominada valor *hash* ou *digest*. Trata-se de funções de uma única via, não sendo utilizadas para a recuperação da informação original. No entanto, também podem servir como assinaturas digitais da origem dos dados. *Secure Hash Algorithm* (SHA), *Message-Digest Algorithm 5* (MD5) e *Cyclic Redundancy Check* (CRC) são alguns tipos de *hashes* existentes e utilizados atualmente (Prasad; Kaushik, 2019).

Por fim, a autenticação representa o processo realizado entre um usuário que pretende acessar determinada aplicação e um servidor. Sistemas de autenticação são compostos, basicamente, por três etapas distintas e interdependentes, sendo elas a Autenticação, Autorização e Auditoria, do inglês, *Authentication, Authorization and Accounting* (AAA). A primeira representa a validação de uma identificação fornecida pelo cliente. Quando isso ocorre, tal informação é verificada confrontando-a com todo o armazenamento da base de dados do sistema. Havendo correspondência, o usuário é autorizado quanto ao acesso à rede de uma determinada organização. Uma vez que o usuário tenha o seu acesso garantido, suas atividades são registradas em *logs* de autenticação e autorização, gravando estatísticas de sessão e informações de uso, o que caracteriza a última etapa do processo AAA (Tschofenig *et al.*, 2019). Existem diversos protocolos de autenticação que foram desenvolvidos e são implementados atualmente, como o *Remote Authentication Dial-In User Service* (RADIUS), *Microsoft Challenge-Handshake Authentication Protocol* (MS-CHAP), Diameter, Kerberos, além de outros (Feldman; Misenar; Conrad, 2023).

2.3.2 *Sistemas Ciberfísicos, Segurança Cibernética e Ciberataques*

Sistemas ciberfísicos são arquiteturas heterogêneas, as quais integram, de maneira robusta, recursos computacionais, de comunicação, e componentes físicos. Com isso, implementam amplas plataformas de dados interconectadas entre si, formando *loops* de informação entre os ambientes físico e cibernético, sendo estas suportadas por sensores e atuadores, cuja função é o controle de processos do sistema (Tekinerdogan *et al.*, 2021). Desta forma, tais redes convertem grandezas de naturezas diversas, abstraindo suas propriedades físicas, tempos de transição envolvidos, bem como a propagação de informações. Além disso, caracterizam-se por apresentarem trocas constantes de dados, conferindo robustez, confiabilidade e segurança a múltiplos processos simultâneos (Peter, 2023). A Figura 7 ilustra o modelo generalizado de um sistema ciberfísico.

Figura 7 – Modelo generalizado de um sistema ciberfísico.



Fonte: (Duo; Zhou; Abusorrah, 2022).

Vale ressaltar que estes sistemas podem ser autônomos ou comandados por humanos, possuindo aplicações nos setores de agricultura, transporte, construção civil, saúde, bem como no setor elétrico. Ademais, aspectos como a troca constante de dados, bem como a

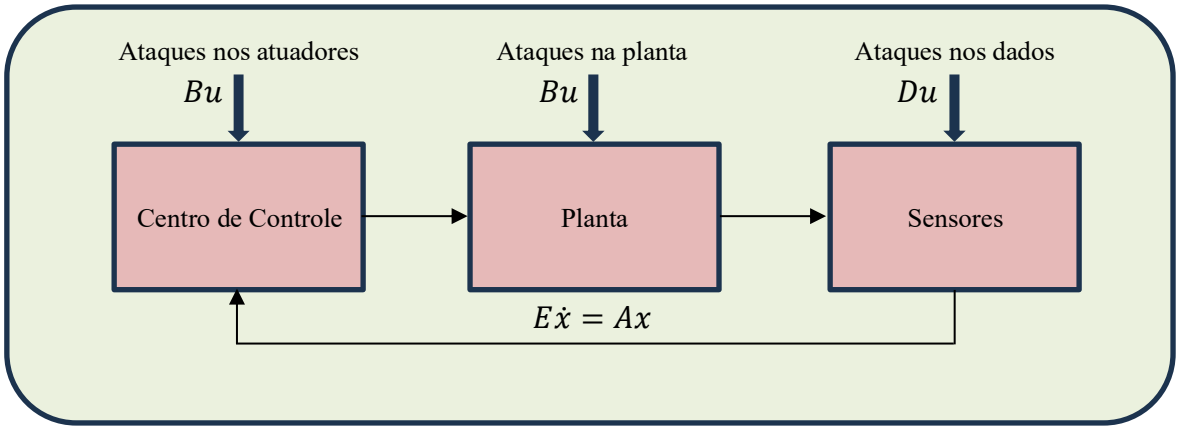
simultaneidade entre processos executados em tempo real, precisam ser assegurados de forma robusta e confiável, garantindo a segurança do fluxo de informações (Peter, 2023).

No que se refere à segurança dos sistemas ciberfísicos, esta consiste em um conceito amplo, o qual abrange várias técnicas e estratégias usadas para combater ameaças, tanto internas quanto externas. Não basta apenas impedir que tais ameaças se concretizem, sendo preciso tomar ações rápidas e que limitem eventuais danos, caso algo ocorra. Além disso, esta abordagem não se restringe apenas à questão tecnológica, envolvendo também políticas de segurança robustas, procedimentos bem definidos, treinamento de funcionários, bem como monitoramento, atualizações e adaptações, por meio de auditorias regulares (Ali *et al.*, 2018).

Considerando o contexto das microrredes, o aspecto relacionado à segurança cibernética é uma das questões fundamentais a serem observadas quando da sua implementação. O fluxo bidirecional de dados na rede, o qual é caracterizado pela participação ativa de diversos agentes no sistema elétrico, faz com que informações privadas, bem como os dispositivos que compõem a microrrede se tornem vulneráveis a ciberataques (Fadlullah; Kato, 2014).

Entende-se por ciberataque qualquer investida criminosa, cujo objetivo seja afetar a integridade, confidencialidade, bem como a disponibilidade de dados ou recursos de uma rede de comunicação, proporcionando, com isso, enormes prejuízos à organização detentora do sistema sob ataque (Hodges; Creese, 2015). Um modelo genérico de ciberataque pode ser definido conforme representado pela Figura 8.

Figura 8 – Modelo genérico de ciberataques.



Fonte: (Pasqualetti; Dorfler; Bullo, 2015).

O ataque a elementos físicos ou cibernéticos pode ser modelado em qualquer parte do sistema. $E\dot{x} = Ax$ representa a dinâmica da rede; Bu define os ataques nos atuadores ou na planta, ao passo que Du são investidas diretas nos dados. Com isso, após o somatório de Du

com Cx, que são as variáveis de estado da rede combinadas com a matriz de saída do sistema, obtém-se como resultado a saída y.

$$E\dot{x} = Ax + Bu \quad (2.1)$$

$$y = Cx + Du \quad (2.2)$$

Ao longo dos anos, diversos tipos de ataques cibernéticos foram desenvolvidos, os quais são caracterizados de acordo com o dano provocado ao sistema, podendo afetar a sua integridade, confidencialidade ou disponibilidade. O Quadro 2 apresenta os principais tipos de ciberataques, de acordo com as classificações supracitadas.

Quadro 2 – Tipos de ciberataques.

Classificação	Ataque	Características
Integridade	*Cross-Site Scripting* (XSS)	Código malicioso injetado e executado em sites seguros, o qual permite o acesso de terceiros a dados sensíveis de uma organização.
	Data Didling	Modificação de informações ou *status* do sistema por pessoas não autorizadas.
	Salami	Execução de pequenos ataques a um sistema, com a finalidade de extrair informações confidenciais sem a percepção dos mecanismos de segurança da rede.
	Session Hijacking	O invasor se torna um participante autorizado do sistema, explorando as vulnerabilidades da rede, bem como de protocolos pouco seguros utilizados na comunicação.
	Injeção *Structured Query Language* (SQL)	Vulnerabilidades do SQL são exploradas pelos criminosos, a fim de acessar a base de dados da organização-alvo. Com isso, executa-se a deleção, modificação ou o roubo de dados.
	Replay	Monitoramento, gravação e substituição de dados atualizados por informações antigas do sistema.
Confidencialidade	Escutas Não Autorizadas	Interceptação de conversas não autorizadas na rede, obtendo-se acesso a informações confidenciais da organização.
	Keylogger	Trata-se de um *software* malicioso instalado sem o conhecimento do cliente, monitorando e acessando as atividades da rede.
	Quebra de Senha	Implementação, por parte do invasor, de ferramentas que, por meio de infinitas combinações de caracteres, visam descobrir senhas de acesso a um sistema.
	Snooping	O criminoso, sem ser notado, visa obter senhas ou qualquer informação confidencial de usuários autorizados. Pode ser realizado de forma física ou virtual.
	Ataque de Engenharia Social	Uso de técnicas de manipulação via internet, cujo objetivo é persuadir o usuário a fornecer dados sigilosos ao invasor, utilizando-se de perfis em redes sociais.

	Análise de Tráfego		O tráfego de dados entre remetente e destinatário é monitorado por um observador externo, o qual obtém informações confidenciais do sistema.
Disponibilidade	DoS e *Distributed* DoS (DDoS)	*Transmission Control Protocol* (TCP) *Synchronization* (SYN)	Consumo excessivo de memória e largura de banda do sistema através do envio de solicitações de acesso ao servidor local, utilizando-se de uma falha no mecanismo *Three-Way Handshake* do protocolo TCP.
		Internet Control Message Protocol (ICMP)	Inundação do tráfego da rede por meio de requisições ICMP.
		Hypertext Transfer Protocol (HTTP)	Através de inúmeras mensagens GET e POST deste protocolo, a camada de aplicação do usuário passa a operar de maneira incorreta.
		User Datagram Protocol (UDP)	Aumento significativo do tráfego da rede, mediante mensagens UDP para endereços IP inexistentes.

Fonte: (Ribas Monteiro; Rodrigues; Zambroni de Souza, 2023).

Além das diversas modalidades de ataques cibernéticos que foram desenvolvidas ao longo dos anos, tais ações podem também ser executadas com o auxílio de *malwares* (junção das palavras inglesas *Malicious Software*), que são códigos ou programas maliciosos projetados para comprometer o funcionamento dos sistemas de dados (Calleja; Tapiador; Caballero, 2019). O Quadro 3 apresenta os tipos de *malwares* mais comumente encontrados na atualidade.

Quadro 3 – Tipos de *malware*.

Malware	**Descrição**
Virus	Trata-se de códigos autorreplicadores, os quais são anexados a outros arquivos ou programas que, quando executados, se espalham infectando a rede. Podem corromper ou destruir dados, diminuir a performance de sistemas, além de afetar o desempenho local.
Worms	São programas autônomos capazes de se multiplicarem sem o auxílio de outros *softwares*. Exploram as vulnerabilidades de uma rede, se propagando rapidamente entre seus domínios. Com isso, provocam o consumo de banda, sobrecarregam sistemas, além de criarem outras ferramentas para ataques futuros.
Ransonware	Tipo de *malware* o qual encripta arquivos de terceiros, impedindo seu acesso pelo sistema. Assim, somente mediante o pagamento de um resgate é que a chave criptográfica é revelada ao proprietário dos dados, permitindo a sua recuperação.
Trojan	Consiste em programas maliciosos que, ao contrário de vírus e *worms*, são estáticos, não se propagando pelo sistema. Entretanto, atuam abrindo portas de comunicação para que agentes externos obtenham acesso à rede, roubando informações, ou perpetrando outras atividades maliciosas.
Spyware	Monitoram e coletam informações sobre as atividades dos usuários, sem o seu consentimento ou conhecimento. Com isso, rastreiam hábitos de pesquisa, registram as teclas digitadas durante o uso do computador, gravando dados sensíveis e enviando-os aos criminosos.
Adware	Não se trata de dados necessariamente maliciosos, porém mostram com frequência anúncios e propagandas, os quais atrapalham a navegação do usuário.

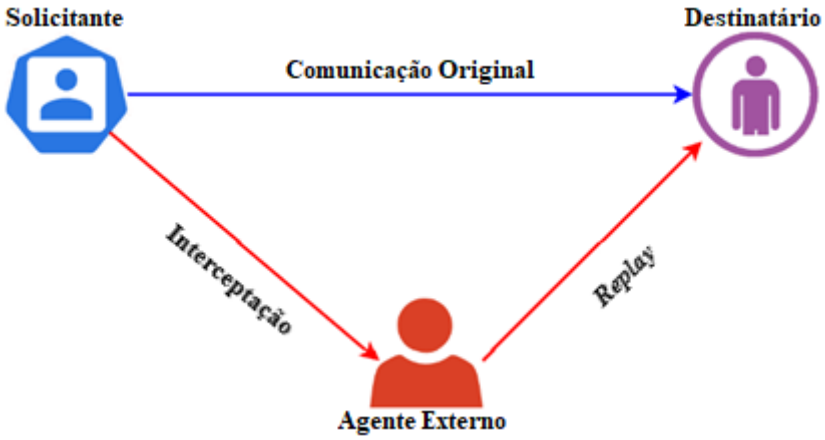
Rootkit	São *softwares* que se instalam no *kernel* do equipamento do usuário, mascarando outras atividades maliciosas correntes na rede. Normalmente são ativados em conjunto com os *trojans*, explorando vulnerabilidades do sistema para a obtenção de acesso ao *kernel*.
Botnet	Trata-se de computadores infectados com *worms* ou *trojans*, passando a ser controlados remotamente por um agente externo. Com isso, torna-se possível a execução de ataques coordenados como o DDoS, envio de *spams*, dentre outros.

Fonte: (Kumar *et al.*, 2023).

2.3.3 *Replay Attacks*

Replay Attacks também conhecidos como *playback attacks* consistem na retransmissão de dados capturados em estágios anteriores da comunicação, visando a obtenção de acesso ao sistema alvo (Stewart; Chapple; Gibson, 2015). Em outras palavras, é a tentativa de restabelecer uma sessão de comunicação sem possuir, necessariamente, as credenciais de acesso de uma rede, replicando-se as informações gravadas de transmissões anteriores, com pequenas diferenças entre endereços IP e *timestamps*. Em geral, esse tipo de investida é realizado contra sistemas que utilizam algoritmos criptográficos sem proteção temporal. Assim, o agente invasor visa interceptar o processo de autenticação de um usuário legítimo, criando outra conexão entre o seu equipamento e o nó de destino da comunicação (Stewart; Tittel; Chapple, 2005). A Figura 9 ilustra, de maneira simplificada, o processo relativo ao *replay attack*. Neste esquema, é possível notar que a comunicação entre o nó solicitante e o destinatário é interceptada pelo agente externo, o qual replica informações antigas ao destino como se fossem atuais, causando problemas no funcionamento do sistema.

Figura 9 – Representação de um *replay attack*.

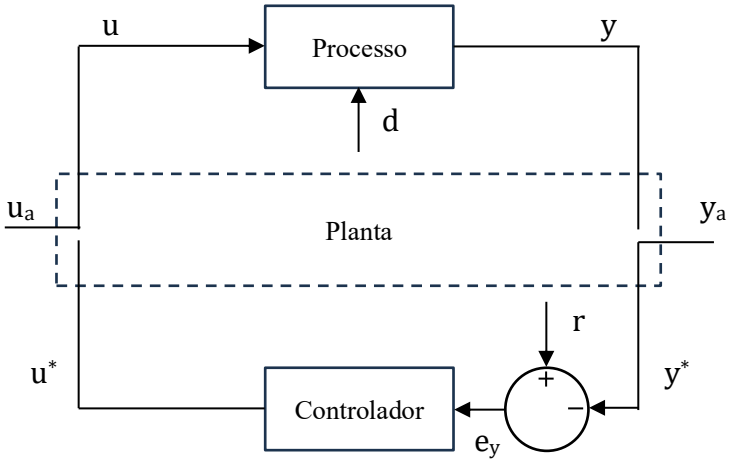


Fonte: (Baeldung, 2024).

De acordo com Hoehn e Ping Zhang (2016) os *replay attacks* podem ser modelados de forma genérica, conforme ilustrado pela Figura 10. Todo o processo é dividido em duas etapas:

na primeira, que ocorre entre $0 \leq t \leq T$, o invasor coleta os dados transmitidos pela rede. Após esta fase, o agente externo insere as informações gravadas, durante o período $NT \leq t \leq (N + 1)T$, sendo N um número inteiro maior ou igual a um.

Figura 10 – Modelo genérico de *replay attack*.



Fonte: (Hoehn; Ping Zhang, 2016).

- Primeiro estágio ($0 \leq t \leq T$):

$$\begin{bmatrix} u_a(t) \\ y_a(t) \end{bmatrix} = 0 \tag{2.3}$$

$$J(t) = \Gamma^y . y(t) \tag{2.4}$$

- Segundo estágio ($NT \leq t \leq (N + 1)T$):

$$\begin{bmatrix} u_a(t) \\ y_a(t) \end{bmatrix} = \begin{bmatrix} u_a(t) \\ J(t - T) \end{bmatrix} \tag{2.5}$$

$$J(t) = J(t - 1) \tag{2.6}$$

Nas quais:

u e u*: sinais de controle da planta. São iguais quando da operação normal do sistema.

y e y*: sinais resultantes da ação de controle. Iguais caso não haja ação externa na rede.

d: sinal de perturbação desconhecido.

u_a e y_a: sinais injetados pelo invasor.

r: sinal de referência.

e_y: se diferente de zero, aciona o elemento de controle da planta.

J(t): representa os dados de medição gravados pelo agente externo.

Γ^y: matriz binária que determina o modo de gravação das informações coletadas.

Existem duas variantes principais concernentes aos *replay attacks*: uma delas, consiste na captura de novas requisições de um cliente conhecido, ludibriando o servidor; a outra, foca

no processo de negação de serviços de rede, retransmitindo solicitações de conexão e mantendo o servidor ocupado com a criação de novas sessões de comunicação, ao invés do fornecimento de serviços aos clientes. Além da inserção de marcas d'água, os *replay attacks* podem ser evitados por meio de *firmwares* atualizados no servidor, bem como por processos de autenticação única, *timestamps* e períodos de expiração, desafios-resposta, além de sessões sequenciadas (Stewart; Chapple; Gibson, 2015).

2.3.4 *Marcas d'água*

No contexto dos sistemas cibernéticos, marcas d'água são assinaturas inseridas nos sinais de controle da rede, as quais permitem ao nó de destino verificar a autenticidade das informações enviadas por um dispositivo de comunicação pertencente à planta. São particularmente úteis se implementadas como último recurso de proteção em sistemas ciberfísicos, caso agentes externos obtenham sucesso na invasão de algum elemento da rede (Patel, 2023).

Ao longo dos últimos anos, diversas técnicas de detecção de ciberataques baseadas em marcas d'água foram desenvolvidas, sendo o trabalho realizado por Mo e Sinopoli (2009) um dos pioneiros a respeito do tema. Neste artigo, utilizou-se um sistema linear e invariante no tempo, do inglês *Linear Time Invariant* (LTI), controladores gaussianos, além de marcas d'água independentes e identicamente distribuídas, do inglês *Independent and Identically Distributed* (IID), as quais são adicionadas aos sinais de controle da rede. Com isso, receptores χ^2, instalados em cada um dos elementos da planta, estão habilitados a detectarem as marcas d'água dos sinais e atestarem a autenticidade da informação. Em trabalhos subsequentes, os mesmos autores implementaram marcas d'água para sistemas com múltiplas interfaces (Chabukswar; Mo; Sinopoli, 2011), além de outros aprimoramentos, levando em consideração a mesma arquitetura (Mo; Chabukswar; Sinopoli, 2014).

A inserção de marcas d'água pode introduzir diversos problemas à rede, como detecções falsas, diminuição da capacidade de controle da planta, bem como o surgimento de transientes e flutuações de sinais. Com isso, diversas outras técnicas emergiram com o tempo, como em Mo, Weerakkody e Sinopoli (2015), em que foi desenvolvida uma marca d'água gaussiana e estacionária, a qual é utilizada com detectores Neyman-Pearson, visando uma solução de compromisso entre a detecção correta do sinal e a manutenção do controle da rede. Já os autores Weerakkody e Sinopoli (2015) implementaram um método no qual as marcas d'água são alteradas com base nos estados do sistema, sendo estes dependentes do modelo da planta e com

dinâmica linear e variante com o tempo, evitando-se que o invasor se acostume com o sinal de identificação.

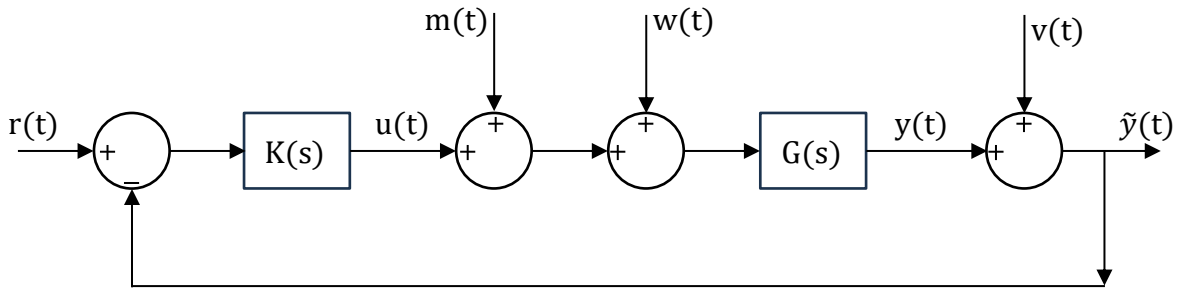
Em outro trabalho, Tang, Alvergue e Gu (2015) realizaram uma implementação baseada no ruído aditivo branco, do inglês *Additive White Gaussian Noise* (AWGN) presentes nos canais de comunicação. Por meio deste, de acordo com a resposta em frequência da rede, é possível estimar seu estado de operação para a detecção do sinal de interesse e, por consequência, da marca d'água. O sistema desenvolvido por Khazraei, Kebriaei e Salmasi (2017) implementou marcas d'água gaussianas IID entre múltiplos agentes, ao invés de aplicá-las individualmente, obtendo-se uma melhor performance no controle da rede.

Em momento posterior, foi desenvolvida a inserção de marcas d'água dinâmicas para sistemas LTI, as quais podem ser aplicadas para a detecção de outros tipos de investida, além dos *replay attacks* (Hespanhol *et al.*, 2017). Neste mesmo período, um sistema baseado em perdas de pacotes e fundamentado em sequências IID de Bernoulli, foi implementado para a construção das marcas d'água (Ozel; Weerakkody; Sinopoli, 2017). Já no ano de 2021, os pesquisadores Ferrari e Teixeira (2021) utilizaram-se de marcas d'água multiplicativas, as quais são aplicadas à cada um dos sensores da rede, permitindo a alternância entre os diversos sinais de identificação do sistema, o que dificulta a detecção por parte de agentes externos.

A implementação realizada por Trapiello e Puig (2022) utiliza-se de filtros de Kalman zonotópicos para a aplicação dos sinais de marcas d'água. Com isso, atingiu-se uma relação de compromisso entre performance, detecção e capacidade de manipulação sobre os sinais de controle da planta. Em outro trabalho, marcas d'água dinâmicas são disparadas por eventos, obtendo-se um desempenho aprimorado, quando da sua aplicação em processos de estimação de estados baseados em eventos da rede (Du *et al.*, 2023b).

Finalmente, o trabalho desenvolvido por Ghamarilangroudi (2020), utilizado como base nesta dissertação, implementou os sinais de marcas d'água inserindo ondas multi-senoidais, de forma aditiva, às informações de controle trafegadas na planta. Embora tal metodologia seja baseada na resposta em frequência do sistema, considerando o espectro usado para a criação da marca d'água, não é necessário o modelamento matemático da rede, bastando apenas que seus operadores conheçam a ordem da sua função de transferência. Além da sua simplicidade, esta técnica tem a vantagem de não inserir transientes aos sinais de operação do sistema, sendo as frequências da marca d'água obtidas de forma experimental. A Figura 11 apresenta o modelo de um sistema linear em malha fechada, operando em regime permanente, do qual são derivados os sinais de autenticação da planta, conforme a sua arquitetura.

Figura 11 – Modelo de um sistema linear operando em regime permanente.



Fonte: (Ghamarilangroudi, 2020).

No qual,

r(t): representa o sinal de referência.

K(s) e G(s): funções de transferência do controlador e da planta, respectivamente.

m(t): marca d'água adicionada ao sinal de controle.

w(t) e v(t): ruídos da planta e do sensor de detecção, respectivamente.

y(t) e $\tilde{y}$(t): sinais de saída da planta, antes e após a inserção do ruído v(t).

u(t): sinal de controle, conforme a diferença entre o sinal de saída e o de referência.

A equação geral do sinal de marca d'água é definida conforme se segue. Esta é determinada de acordo com a ordem do circuito em questão, respeitando-se condições predefinidas quando da aferição dos seus parâmetros numéricos. Com isso, evita-se o surgimento de transientes nos sinais da rede.

$$m(t) = \sum_{i=1}^{n_m} A_i sen(\omega_i t + \varphi_i) \tag{2.7}$$

Na qual,

A_i: amplitude da onda senoidal.

ω_i e φ_i: frequência e fase do sinal, respectivamente.

n_m: número de sinais senoidais gerados, conforme a ordem do sistema.

Em sistemas de primeira ordem, tem-se $n_m = 1$. Além disso, os parâmetros A_1 e ω_1 podem ser escolhidos aleatoriamente. Assim, torna-se possível determinar a fase do sinal, conforme equação a seguir:

$$\varphi_1 + \angle G_{my}(j\omega_1) = 2l\pi \tag{2.8}$$

Nesta equação, l pode assumir qualquer valor inteiro maior ou igual a zero, a critério do operador do sistema. Com isso, uma vez calculada a fase da função de transferência da planta, tem-se o valor de φ_1. Para circuitos de segunda ordem, ω_1 e ω_2 podem ser assumidos

preliminarmente, de maneira aleatória. Outros quatro parâmetros são introduzidos nos cálculos: a_1, a_2, α_1 e α_2, onde:

$$a_1 = A_1|G(j\omega_1)| \tag{2.9}$$

$$a_2 = A_2|G(j\omega_2)| \tag{2.10}$$

$$a_1 = a_2 \tag{2.11}$$

$$\alpha_1 = \frac{\pi}{2}, \alpha_2 = -\frac{\pi}{2} \quad ou \; \alpha_1 = -\frac{\pi}{2}, \alpha_2 = \frac{\pi}{2} \tag{2.12}$$

$$\alpha_1 = \varphi_1 + \angle G_{my}(j\omega_1) \tag{2.13}$$

$$\alpha_2 = \varphi_2 + \angle G_{my}(j\omega_2) \tag{2.14}$$

Assim, uma vez calculados todos os parâmetros, tem-se duas ondas senoidais combinadas, representando o sinal da marca d'água. Da mesma forma que no caso de redes de segunda ordem, para sistemas de terceira ordem também são geradas duas ondas senoidais como marcas d'água, de modo a suprimir a introdução de transientes no circuito. Os parâmetros ω_1 e ω_2 são definidos arbitrariamente, calculando-se os valores conforme se segue:

$$\frac{a_1}{a_2} = \frac{A_1|G(j\omega_1)|}{A_2|G(j\omega_2)|} = \frac{\omega_2}{\omega_1} \tag{2.15}$$

$$\alpha_1 = 0, \alpha_2 = \pi \quad ou \; \alpha_1 = \pi, \alpha_2 = 0 \tag{2.16}$$

Considerando-se uma planta genérica de ordem n, sua função de transferência pode ser assumida como a razão entre dois polinômios:

$$G(s) = \frac{b(s)}{a(s)} = \frac{b_{n-1}s^{n-1} + \cdots + b_1 s + b_0}{s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0} \tag{2.17}$$

O sinal da marca d'água é determinado pela equação a seguir:

$$\frac{p_m(s)}{(s^2 + {\omega_1}^2) \ldots (s^2 + {\omega_{n_m}}^2)} \tag{2.18}$$

$$p_m(s) = c(s).a(s) \tag{2.19}$$

O polinômio c(s) é escolhido, respeitando-se a seguinte condição:

$$grau\, a(s) \leq grau\, p_m(s) \leq 2n_m - 1 \tag{2.20}$$

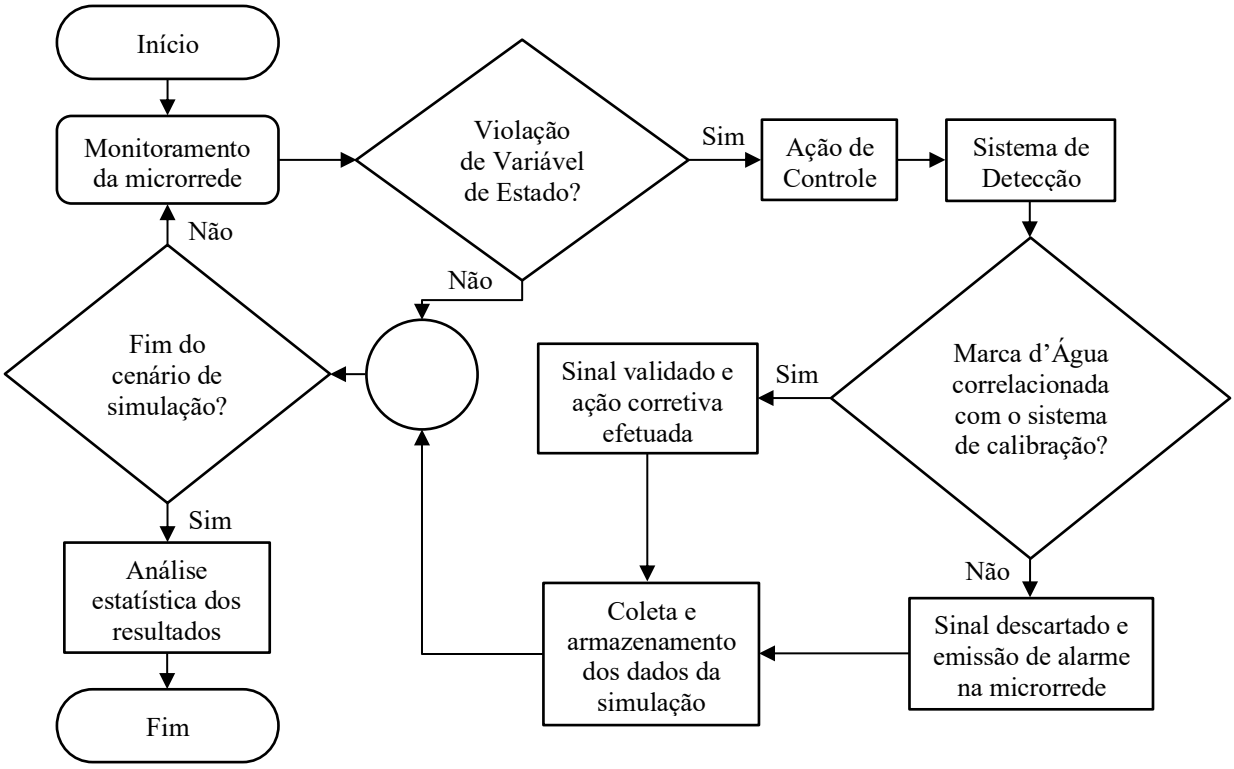
Os valores das frequências angulares podem ser definidos de forma aleatória, sendo o número de senoides da marca d'água determinado pela inequação:

$$n_m \geq \frac{n+1}{2} \tag{2.21}$$

CAPÍTULO 3 – METODOLOGIA

O presente capítulo trata da descrição da metodologia desenvolvida para os testes de detecção das marcas d'água aditivas aos sinais de controle da microrrede. Esta pesquisa, de natureza experimental e aplicada, teve como objetivo investigar a capacidade de identificar e validar comandos emitidos pelo Centro de Controle do modelo computacional de uma microrrede real. O envio desses sinais se dava em resposta à violação de uma variável de estado do sistema, sendo estes codificados com as marcas d'água. Para isso, desenvolveu-se um mecanismo de detecção, o qual permitiu o reconhecimento e a autenticação de comandos legítimos, bem como a rejeição de sinais falsos. Caso a autenticidade do sinal fosse confirmada, uma ação corretiva era executada localmente. Quando da ocorrência de falha, o comando era descartado e um alarme emitido na rede. Esta verificação baseou-se na comparação do sinal recebido com um modelo de calibração que representava o efeito esperado do canal de comunicação sobre as marcas d'água. A eficácia da proposta foi avaliada estatisticamente com base na taxa de autenticações e descartes corretos, conforme meio de propagação considerado, além de avaliar o consumo energético e latência adicional. A Figura 12 ilustra o fluxograma da metodologia desenvolvida.

Figura 12 – Fluxograma da metodologia implementada.



Fonte: Autoria própria (2025).

No decorrer deste capítulo, serão determinados os trechos pelos quais trafegam as informações do sistema, bem como seus pontos de vulnerabilidade a ataques externos, os quais correspondem aos locais estratégicos para a inserção das marcas d'água. Em seguida, serão demonstrados os modelos utilizados para a representação dos elementos de controle da planta, além da ordem dos circuitos em questão. Desta forma, uma vez que tais parâmetros sejam conhecidos, torna-se possível a determinação do número de senoides que integrarão a marca d'água, assim como suas variáveis fundamentais, sendo estas constituídas por valores de amplitude, frequência angular e fase.

Após a demonstração da metodologia de cálculo das marcas d'água, serão apresentados os circuitos elétricos selecionados como elementos controlados da microrrede. Dados relativos ao número de barras, níveis de tensão, transformadores, bem como equipamentos de GD da rede serão explorados em maiores detalhes. Os sistemas utilizados para os testes foram o IEEE 13 Barras, cuja implementação se deu para fins de validação da metodologia, além do circuito elétrico da Unifei, representando um modelo de microrrede real. Vale ressaltar que ambos os sistemas foram modelados por meio do *software* OpenDSS, sendo este uma das ferramentas de simulação adotadas.

Mais adiante, serão descritas as implementações realizadas em Python, as quais representam o sistema de controle da microrrede, responsável pelo gerenciamento dos circuitos elétricos adotados para as simulações. Neste *software* foram implementados, além dos algoritmos de monitoramento das variáveis de estado da rede, os meios de propagação pelos quais trafegam as informações de controle da planta, sendo estes caracterizados por um canal de comunicação simplificado, com ou sem inserção de ruído, bem como por uma modelagem reduzida da tecnologia Ethernet.

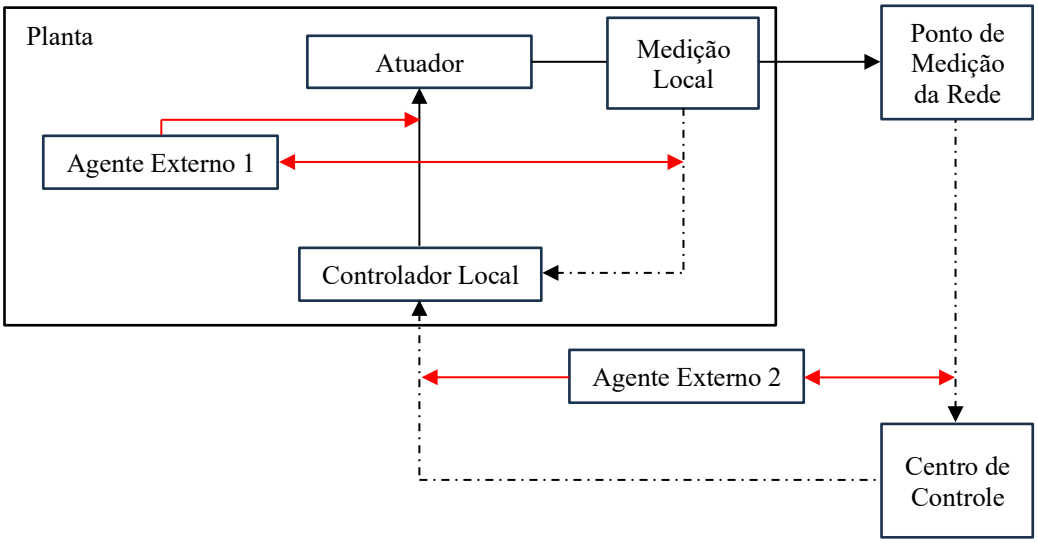
Finalmente, a última seção deste capítulo apresenta a metodologia utilizada para a detecção das marcas d'água inseridas nas informações de controle da microrrede. Para isso, a ferramenta adotada foi o Periodograma, a qual se baseia na densidade espectral de potência do sinal recebido. Neste trecho do trabalho, serão demonstrados o modo de funcionamento desta implementação, além da sua fundamentação teórica.

3.1 PONTOS DE VULNERABILIDADE EM UMA MICRORREDE

Existem dois pontos principais que são vulneráveis a ataques em uma microrrede. Um deles se localiza entre a central de controle do sistema e o elemento de medição do circuito; o outro situa-se entre o elemento sensor e o dispositivo atuador da planta. Para o caso dos *replay*

attacks, ambos os trechos podem ser aproveitados para que o agente externo armazene informações antigas de medição da rede e as reproduza aos elementos de tomada de decisão. A Figura 13 a seguir ilustra tal cenário e como o invasor insere e replica os dados manipulados para os pontos de destino do sistema.

Figura 13 – Pontos de *replay attacks* em uma microrrede.



Fonte: (Patel, 2023).

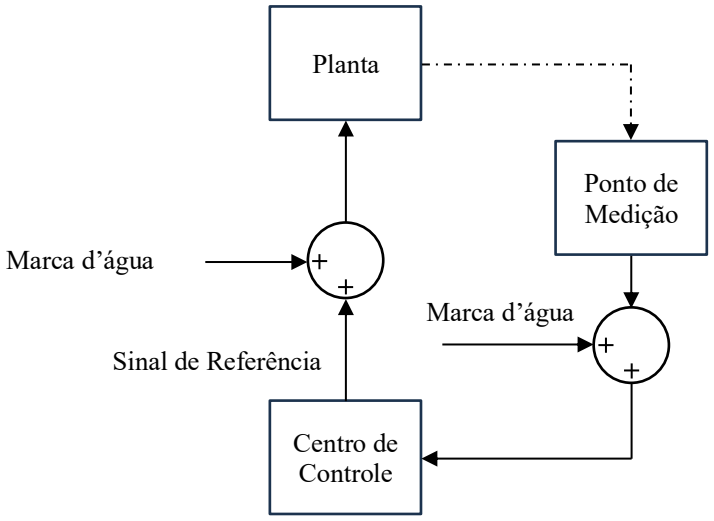
O Centro de Controle é o local responsável pelo gerenciamento de diversos parâmetros do circuito, como níveis de tensão, sinais de potência ativa e reativa dos ramos, frequência, magnitudes de corrente, aberturas angulares das barras, dentre outros. Tais grandezas são enviadas pelo Ponto de Medição da Rede, cuja função é capturar as medidas locais de diferentes elementos do circuito, como barras, dispositivos remotos ou subestações. Caso seja preciso realizar qualquer ação corretiva na planta, o Centro de Controle aciona o Controlador Local, que efetua os ajustes necessários no Atuador até que os níveis da Medição Local correspondam aos estabelecidos pelo sistema de operação.

Considerando um cenário de ataque realizado pelo Agente Externo 1, este grava os dados provenientes da Medição Local, replicando-os para o Atuador como se enviados pelo Controlador Local. Nesta situação, a investida se restringe ao interior da planta, utilizando os meios físicos característicos da rede para o envio das informações. Na hipótese do Agente Externo 2 efetuar o ataque, este registra e reproduz medidas antigas advindas do Ponto de Medição da Rede para o Controlador Local, suprimindo a comunicação por parte do Centro de Controle. Diferentemente do primeiro caso, neste cenário a emissão dos dados se dá por meio

de um canal de transmissão genérico, o qual pode ser estabelecido sobre qualquer tecnologia de comunicação existente, desde que esta seja aplicável ao trecho em questão.

Uma das soluções aplicáveis para resolver este problema, é a introdução dos sinais de marcas d'água aditivas em ambos os trechos da comunicação. Com isso, para que uma informação transmitida seja considerada válida, esta deve conter a assinatura característica, a qual é estabelecida e acordada entre os elementos da rede. A Figura 14 ilustra o modo como o sinal da marca d'água é adicionado aos pontos de vulnerabilidade do sistema.

Figura 14 – Marca d'água adicionada ao sinal de referência.



Fonte: (Patel, 2023).

Vale ressaltar que apenas o sinal trafegado internamente na planta pode afetar o desempenho da microrrede, caso este contenha a marca d'água. Isto porque, conforme mencionado anteriormente, os dados enviados do Controlador Local para o Atuador são transmitidos através do meio físico que constitui a planta. Portanto, a determinação das componentes senoidais da marca d'água deve ser criteriosa, uma vez que tais sinais, quando inseridos no sistema sem prévia verificação, têm o potencial de introduzir instabilidades na microrrede, perdas do sinal de controle, afetação dos níveis de qualidade do sistema, dentre outros fatores.

Entretanto, embora os sinais trafegados entre o Centro de Controle e o Controlador Local não influenciem na operação da microrrede, é recomendável que estes sejam implementados de maneira idêntica aos transmitidos internamente na planta, a fim de que eventuais alterações na composição do sinal, ou ajustes necessários não introduzam complexidade ou confundam o modo operativo dos elementos de controle do sistema.

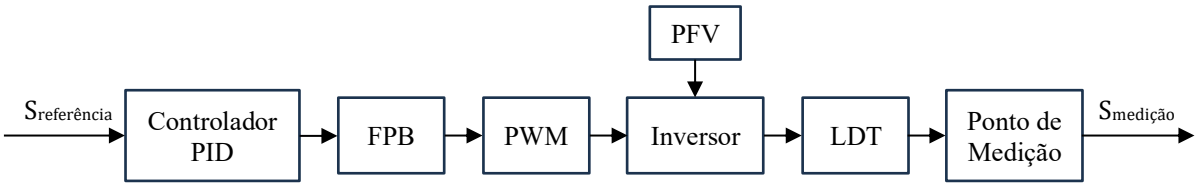
Desta forma, os pontos da microrrede escolhidos para a inserção das marcas d'água, correspondem aos trechos entre o Centro de Controle, o Ponto de Medição e o Controlador Local. Uma vez que o objetivo do presente trabalho é verificar a capacidade de detecção da marca d'água por parte dos elementos da rede, foram modelados e simulados diferentes canais de comunicação, representando o meio de transmissão das informações, bem como um mecanismo receptor baseado na Densidade Espectral de Potência (DEP) dos sinais de entrada para fins de identificação e validação. Com isso, será possível determinar a robustez da metodologia empregada quando submetida a ambientes de propagação distintos, bem como a eficácia da técnica de detecção desenvolvida.

3.2 MODELO UTILIZADO PARA O CÁLCULO DAS MARCAS D'ÁGUA

Para o cálculo do sinal da marca d'água característico de uma microrrede, é necessário conhecer a ordem da função de transferência do circuito, bem como sua resposta em frequência. Uma vez que os sistemas utilizados para os testes não possuem nenhum elemento de controle local, tampouco medidores físicos, adotou-se para cada barra monitorada da rede dois controladores, sendo um destinado a atuar sobre os níveis de potência ativa, e o outro sobre a potência reativa.

Para determinar a função de transferência da microrrede, considerou-se um Controlador Proporcional-Integral-Derivativo (PID) associado a um Inversor e a um Modulador por Largura de Pulso, do inglês, *Pulse Width Modulation* (PWM) (Ghosh; Zare, 2022). Estes blocos controlam os fluxos de potência ativa e reativa em uma Linha de Distribuição Trifásica (LDT) de um metro de comprimento até o Ponto de Medição. O Controlador PID garante resposta rápida, baixo erro em regime permanente e suavização de variações bruscas de carga, o qual é ajustado pelos ganhos proporcional (Kp), integral (Ki) e derivativo (Kd) (Lumkes, 2001). O Inversor é modulado pelo Controlador PID, de modo a regular o fluxo PQ proveniente dos Painéis Fotovoltaicos (PFV). A LDT foi modelada para curtas distâncias, considerando resistência (R) e indutância (L), desprezando-se os efeitos capacitivos. O Inversor, o PWM e o Ponto de Medição foram representados como sistemas de primeira ordem, caracterizados por R e L (Buso; Mattavelli, 2022). Objetivando-se garantir resposta em frequência próxima da unidade, pequenas rotações de fase na faixa de operação das marcas d'água e estabilidade do circuito, foi inserido um Filtro Passa-Baixas (FPB) após o Controlador PID. A Figura 15 ilustra esta composição, além dos sinais de referência ($S_{referência}$) e de medição ($S_{medição}$).

Figura 15 – Modelo utilizado para determinação da função de transferência da planta.



Fonte: Autoria própria (2025).

De acordo com a equação (3.1), tem-se a função de transferência do Controlador PID, considerando seus ganhos K_p, K_i e K_d. Por meio da equação (3.2), é possível determinar a função de transferência proporcionada pelo FPB, por meio de sua resistência (R_{filtro}) e indutância (L_{filtro}) individuais. Para fins de simplificação, a equação (3.3) apresenta a função de transferência unificada do grupo constituído pelo Inversor, PFV, PWM, LDT e Ponto de Medição, com os parâmetros R_{grupo} e L_{grupo} representando os valores acumulados de R e L de cada bloco (Iturra; Thiemann, 2021).

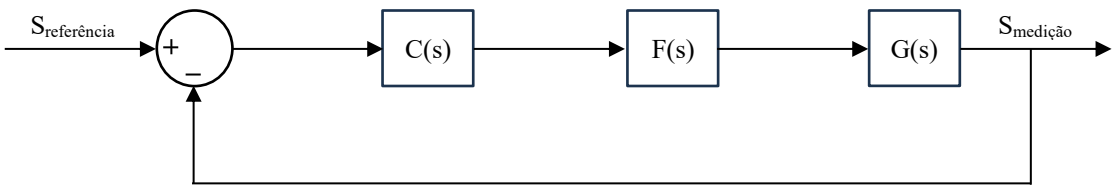
$$C(s) = K_p + \frac{K_i}{s} + K_d s \tag{3.1}$$

$$F(s) = \frac{1}{R_{filtro} + sL_{filtro}} \tag{3.2}$$

$$G(s) = \frac{1}{R_{grupo} + sL_{grupo}} \tag{3.3}$$

O sistema de controle implementado possui um ramo de realimentação negativa, o qual subtrai o sinal medido do nível de referência enviado pelo Centro de Controle da microrrede. O resultado desta operação é inserido na entrada do Controlador PID, que processa a informação e transmite os ajustes necessários aos demais blocos do trecho. A Figura 16 ilustra essa representação, seguida da expressão genérica da função de transferência do sistema.

Figura 16 – Sistema de controle do trecho da microrrede.



Fonte: Autoria própria (2025).

Com isso, por meio da equação (3.4), é possível determinar a expressão geral da função de transferência da rede, a qual pode ser aplicada individualmente para ambas as malhas de controle de potência (ativa e reativa).

$$H(s) = \frac{C(s) * F(s) * G(s)}{1 + C(s) * F(s) * G(s)} \quad (3.4)$$

Os ganhos dos controladores PID foram determinados empiricamente, a fim de que as respostas em frequência de ambos fossem próximas de 0 dB, e com pequenas rotações de fase na faixa de operação das marcas d'água. Com isso, torna-se possível a obtenção das funções de transferência das malhas de controle de potência ativa e reativa. A Tabela 1 mostra os valores definidos para este estudo.

Tabela 1 – Valores dos ganhos do controlador PID.

Ganhos	Potência Ativa	Potência Reativa
K_p	0,50	0,1889
K_i	50,00	0,2000
K_d	0,01	0,0100

Fonte: Autoria própria.

Para o FPB, os valores de resistência e indutância adotados correspondem a 1 Ω e 1 mH (Wentworth, 2008). Já os parâmetros R_{grupo} e L_{grupo} considerados são iguais a 0,01 Ω e 1 mH, respectivamente (Saïd-Romdhane *et al.*, 2016). Finalmente, substituindo-se cada um dos valores apresentados nas equações (3.1)–(3.4), obtém-se, nesta ordem, as funções de transferência de malha fechada do controle da potência ativa, bem como da potência reativa.

$$H_p(s) = \frac{0{,}01s^2 + 0{,}5s + 50}{10^{-6}s^3 + 0{,}01101s^2 + 0{,}51s + 50} \quad (3.5)$$

$$H_Q(s) = \frac{0{,}01s^2 + 0{,}1889s + 0{,}2}{10^{-6}s^3 + 0{,}01101s^2 + 0{,}1989s + 0{,}2} \quad (3.6)$$

Uma vez que ambas as funções de transferência resultantes representam sistemas de terceira ordem, é possível determinar as marcas d'água características de cada uma das malhas de controle. Assim, conforme explicado na seção 2.3.4, estas compõem-se de duas senoides, cujos parâmetros são derivados a partir dos cálculos de magnitude e fase de suas funções de transferência, de acordo com valores de frequência previamente estabelecidos. A equação (3.7) define a expressão geral da marca d'água, tanto do sinal de potência ativa, quanto de potência reativa.

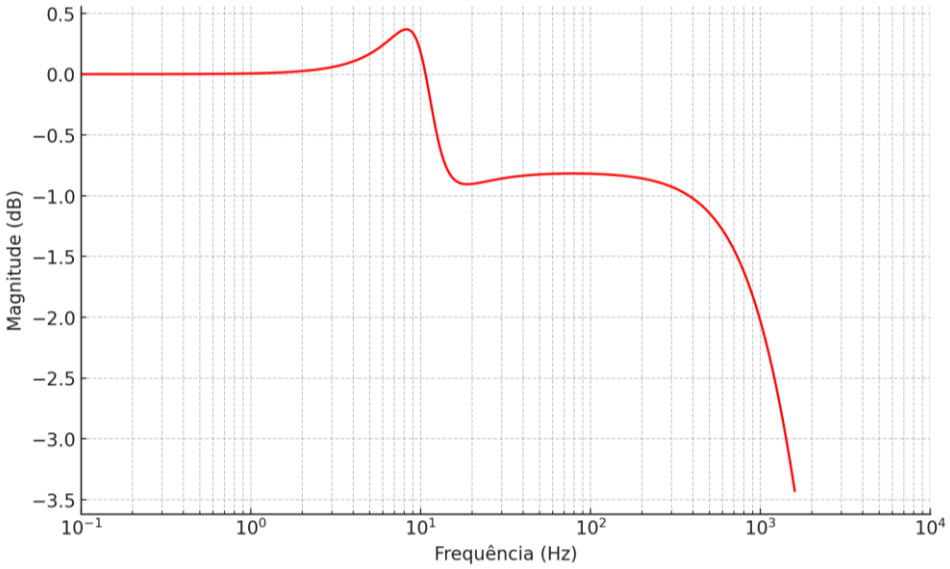
$$M = A_1 sen(\omega_1 t + \phi_1) + A_2 sen(\omega_2 t + \phi_2) \quad (3.7)$$

Após o cálculo das funções de transferência das malhas de controle, faz-se necessário verificar se estas configuram sistemas estáveis ou instáveis, além da análise de suas magnitudes

e rotações de fase na banda de interesse, que é de 0 até 6 Hz. Para isso, foram traçados os diagramas de Bode[8] de cada uma das malhas de controle do trecho monitorado.

O Gráfico 1 apresenta a resposta em magnitude do controle da potência ativa, no qual é possível observar valores próximos de 0 dB na faixa de operação das marcas d'água, isto é, entre 0 e 6 Hz, além de possuir comportamento estável em todo o espectro analisado. O pico na banda de interesse ocorre na frequência de 5,98 Hz, sendo igual a 0,24 dB.

Gráfico 1 – Resposta em magnitude da malha de potência ativa.

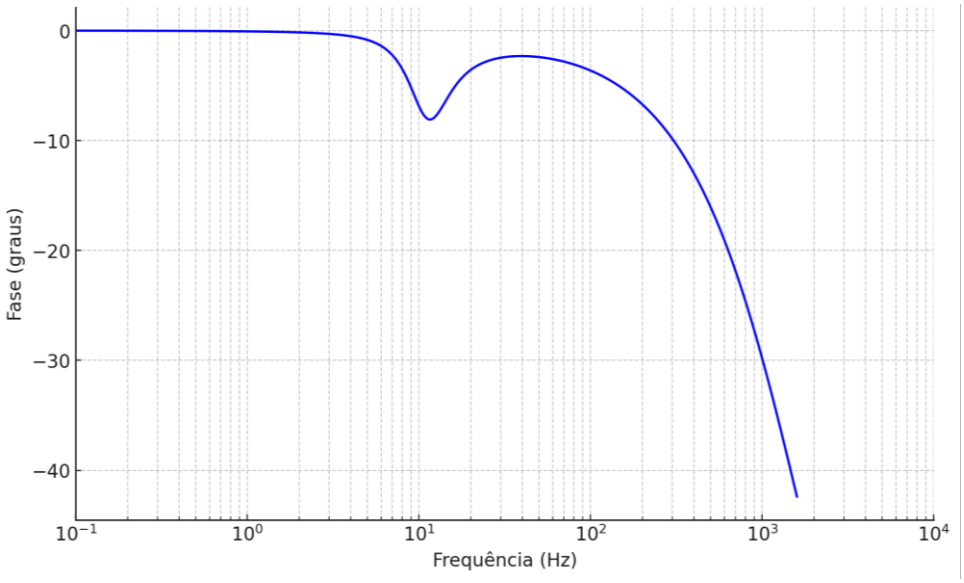


Fonte: Autoria própria (2025).

Por sua vez, a resposta em fase da potência ativa possui rotações em torno de 0° dentro da banda de atuação das marcas d'água, atingindo o desvio máximo de -1,38° na frequência de 5,98 Hz. O Gráfico 2 ilustra o comportamento da fase da função de transferência da potência reativa.

[8] O diagrama (ou gráfico) de Bode representa a resposta em frequência de um sistema linear, mostrando em dois gráficos separados o módulo e a fase em função da frequência, em escala logarítmica (Sadiku; Musa; Alexander, 2013).

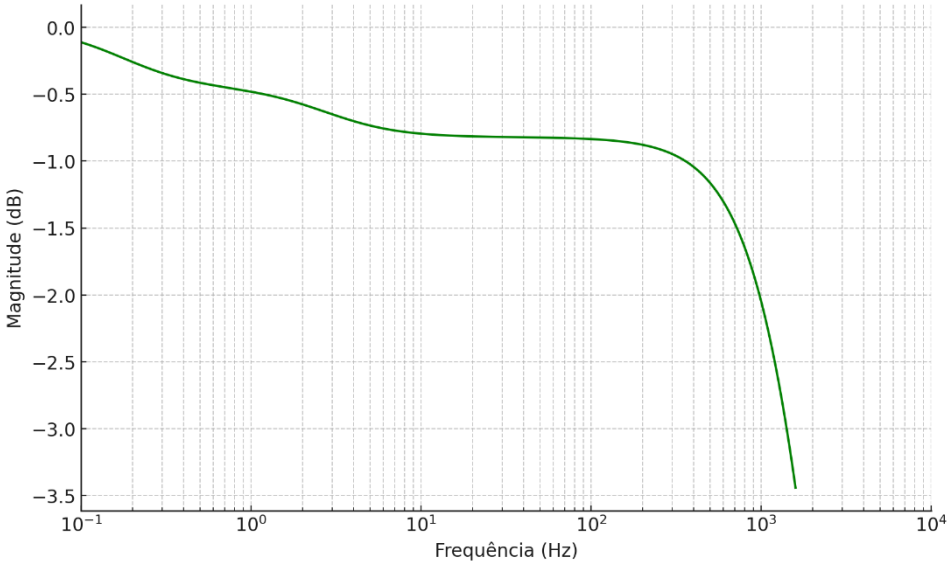
Gráfico 2 – Resposta em fase da malha de potência ativa.



Fonte: Autoria própria (2025).

Considerando a resposta em magnitude da potência reativa, os valores de amplitude mantiveram-se próximos de 0 dB, alcançando o patamar mínimo de -0,76 dB na frequência de 5,98 Hz, levando-se em conta somente a faixa operativa das marcas d'água. O Gráfico 3 apresenta o perfil de magnitude em função da frequência da potência reativa.

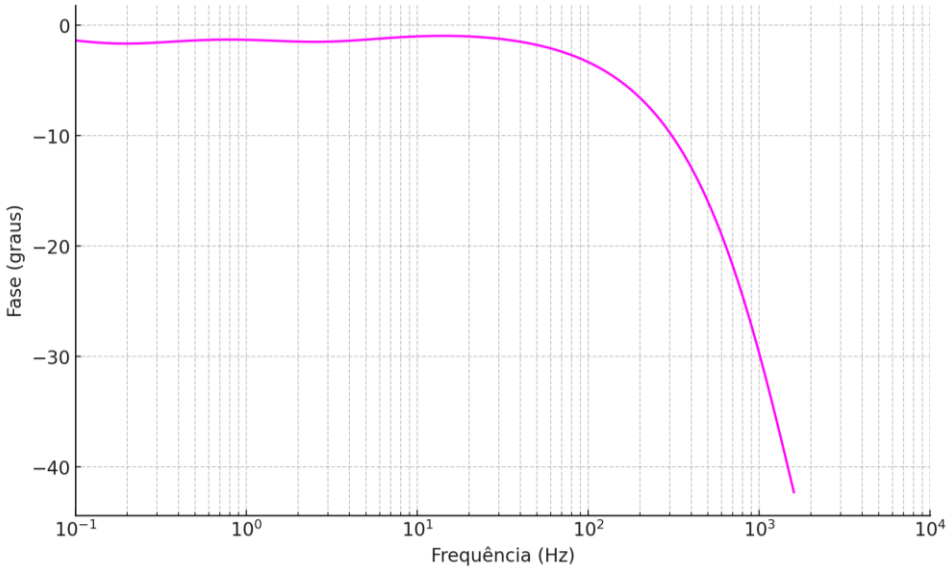
Gráfico 3 – Resposta em magnitude da malha de potência reativa.



Fonte: Autoria própria (2025).

A resposta em fase da potência reativa também apresenta rotações praticamente nulas na banda de operação das marcas d'água, atingindo um desvio máximo de -1,66° em 0,197 Hz. Tal representação pode ser observada por meio do Gráfico 4, no qual se verifica uma reduzida variação angular em toda a faixa de interesse.

Gráfico 4 – Resposta em fase da malha de potência reativa.



Fonte: Autoria própria (2025).

Por fim, com relação ao comportamento, tanto da magnitude quanto do desvio angular de ambas as funções de transferência, observa-se que esses parâmetros se mantêm próximos de zero na faixa entre 0 e 6 Hz, conforme desejado. Com isso, as magnitudes apresentam pequenas variações, mas sem comprometer o funcionamento do sistema. Já as fases permanecem praticamente nulas, com oscilações mínimas, o que assegura a segurança operativa da microrrede.

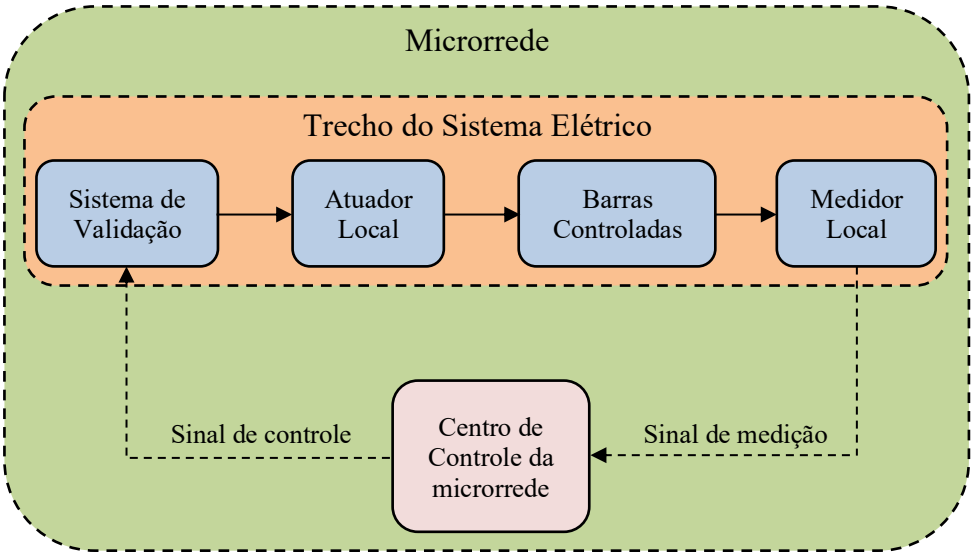
3.3 DESCRIÇÃO DOS MODELOS IMPLEMENTADOS NAS SIMULAÇÕES

Os testes realizados por este trabalho tomam como base os sistemas IEEE 13 Barras, bem como um modelo de circuito elétrico real, representado pela microrrede da Unifei. Ambos foram implementados por meio do *software* OpenDSS, no qual considerou-se os parâmetros das linhas de distribuição, tipos de cargas conectadas, transformadores, GD, SAE, capacitores, chaves seccionadoras, dentre outros elementos. No que tange ao sistema de controle da microrrede, este foi configurado em Python, cuja operação se dá de maneira integrada e sincronizada com o OpenDSS, através da interface *Component Object Model* (COM). Assim, foram modelados nesta linguagem de programação os mecanismos de monitoramento das variáveis de estado dos circuitos, as tecnologias de comunicação utilizadas na transmissão das informações, além das metodologias de inserção e detecção dos sinais de marcas d'água.

A seguir, foram descritos os sistemas elétricos utilizados nas simulações, bem como os cálculos das marcas d'água características de cada um deles, sendo estas determinadas com

base nos valores de referência de potência ativa e reativa das barras dos circuitos. Também foram detalhados o funcionamento do sistema de controle implementado, as tecnologias de comunicação modeladas, bem como o mecanismo de detecção das marcas d'água configurado. A Figura 17 ilustra a integração entre cada um dos elementos constituintes da microrrede.

Figura 17 – Integração dos elementos da microrrede.

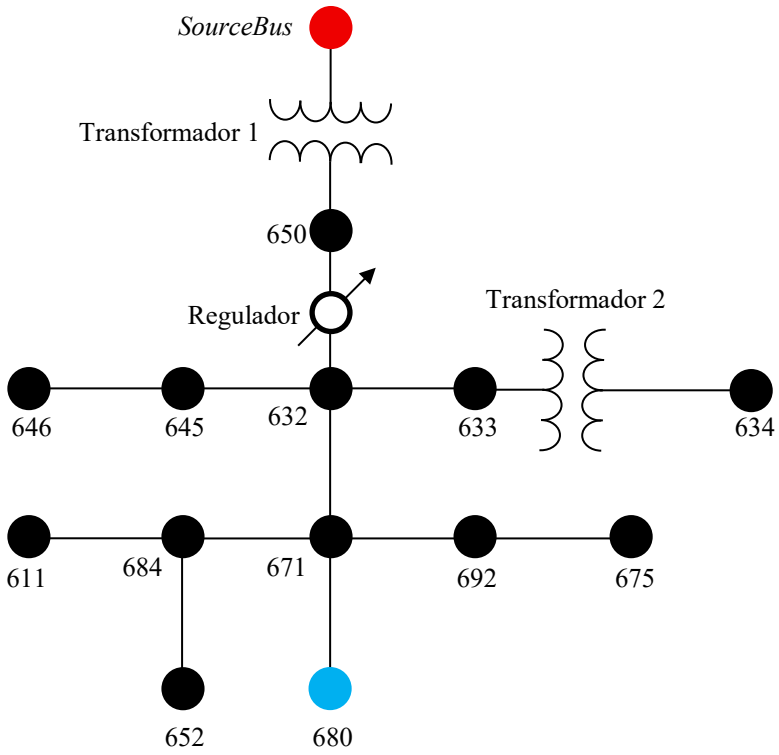


Fonte: Autoria própria (2025).

3.3.1 *Sistema IEEE 13 Barras e cálculo da marca d'água característica*

Para a validação da metodologia do presente trabalho, foi utilizado o sistema IEEE 13 Barras, que se encontra disponível em IEEE (2024). Este circuito é composto por uma subestação, representando o equivalente de Thévenin, que é alimentada por um nível de tensão de 115 kV. Esta variável é convertida para 4,16 kV por meio do Transformador 1, que está inserido entre as barras *SourceBus* e 650 do sistema. Além disso, este elemento conta com três reguladores monofásicos instalados nas três fases do seu terminal secundário, cuja função é manter os níveis de tensão dentro dos limites estabelecidos para o restante da microrrede. A Figura 18 ilustra a disposição dos principais elementos do sistema IEEE 13 Barras, no qual os pontos em vermelho e em azul representam, respectivamente, o Centro de Controle e a barra monitorada do circuito.

Figura 18 – Representação do sistema IEEE 13 Barras.



Fonte: Autoria própria (2025).

A tensão de 4,16 kV é distribuída entre os demais componentes do circuito, com exceção da barra 634, que opera com uma tensão de linha de 480 V. Esta tensão é obtida por meio do Transformador 2, cujo terminal primário está conectado na barra 633. Vale também ressaltar que a barra 692 se encontra ligada ao restante do sistema por uma chave instalada na barra 671, a qual está configurada no modo Normalmente Fechado (NF). Além disso, a rede possui dois capacitores inseridos em diferentes locais, que têm a função de regular os níveis de tensão da microrrede. A Tabela 2 ilustra os transformadores e os capacitores que compõem o sistema IEEE 13 Barras.

Tabela 2 – Transformadores e capacitores do sistema IEEE 13 Barras.

Elemento	**Barra**	**Níveis de Tensão (kV)**	**Conexão**	**Capacidade**
Transformador 1	*SourceBus*/650	115/4,16	Delta/Estrela	5 MVA
Transformador 2	633/634	4,16/0,48	Estrela/Estrela	500 kVA
Capacitor 1	675	4,16	Fase-Fase	600 kvar
Capacitor 2 (Monofásico)	611	2,4	Fase-Neutro	100 kvar

Fonte: Autoria própria.

As onze linhas de distribuição que integram o circuito são parametrizadas por sete *linecodes*, os quais definem diferentes níveis de resistência, indutância e capacitância por unidade de km. Estas foram implementadas nas configurações monofásica, bifásica ou trifásica,

com seus comprimentos estabelecidos originalmente em pés[9]. A Tabela 3 apresenta as características principais das linhas que integram o sistema IEEE 13 Barras.

Tabela 3 – Características das linhas de distribuição do sistema IEEE 13 Barras.

Linha	Barras	Comprimento (m)	Fases	*Linecode*
1	650/632	609,6	3	1
2	632/670	203,3	3	1
3	670/671	406,3	3	1
4	671/680	304,8	3	1
5	632/633	152,4	3	2
6	632/645	152,4	2	3
7	645/646	91,4	2	3
8	692/675	152,4	3	6
9	671/684	91,4	2	4
10	684/611	91,4	1	5
11	684/652	243,8	1	7

Fonte: Autoria própria.

Considerando as cargas do circuito, estas foram implementadas de acordo com os diferentes modelos disponibilizados pelo OpenDSS, por meio das configurações monofásica ou trifásica, nos modos equilibrado ou desequilibrado. O perfil de consumo estabelecido para cada uma das cargas da rede obedece a uma curva distribuída em 24 pontos, representando o período de um dia, cuja demanda de pico ocorre entre as 18 e 23 horas. A Tabela 4 ilustra os parâmetros das cargas que compõem o sistema IEEE 13 Barras.

Tabela 4 – Parâmetros das cargas do sistema IEEE 13 Barras.

Carga	Barra	Potência Ativa (kW)	Potência Reativa (kvar)	Conexão	Configuração
1	671	1155	660	Delta	Trifásica Equilibrada
2	634	400	290	Estrela	Trifásica Desequilibrada
3	645	170	125	Estrela	Monofásica
4	646	230	132	Delta	Monofásica
5	692	170	151	Delta	Monofásica
6	675	843	462	Estrela	Trifásica Desequilibrada
7	611	170	80	Estrela	Monofásica
8	652	128	86	Estrela	Monofásica
9	670	200	116	Estrela	Trifásica Desequilibrada

Fonte: Autoria própria.

O ponto de monitoramento escolhido para os testes foi a barra 680, que está a 121,92 metros do Centro de Controle, localizado na subestação da microrrede. A composição deste trecho foi estabelecida com base no modelo descrito na seção 3.2, sendo representado matematicamente pelas equações (3.5) e (3.6) considerando as malhas das potências ativa e reativa, respectivamente. Além disso, nos terminais da referida barra foi inserida uma carga de 180 kW e 30 kvar, bem como um gerador fotovoltaico de 150 kW, elementos que não fazem parte da configuração original do circuito. Tais valores foram definidos de forma arbitrária, visto que a barra 680, originalmente, não possui qualquer equipamento diretamente conectado.

[9] O comprimento das linhas de transmissão foi convertido de pés para metros para fins de compatibilidade com a modelagem do sistema de controle da microrrede. Vale ressaltar que 1 pé equivale a 0,3048 metros.

Entretanto, o dimensionamento adotado mantém proporcionalidade com as potências observadas nas demais barras, o qual é compatível com o perfil de consumo e geração do sistema. Assim, foi possível reproduzir o modelo apresentado pela Figura 15 na barra 680.

As frequências das marcas d'água, tanto dos sinais de potência ativa, quanto de potência reativa podem ser escolhidas arbitrariamente, desde que seus valores sejam, pelo menos, dez vezes menores que a frequência de operação da rede, que é igual a 60 Hz. Com isso, conforme já mencionado, evita-se a sobrecarga dos elementos do circuito, bem como sua operação em faixas proibidas do espectro, as quais poderiam provocar acionamentos indesejados, introdução de transientes, dentre outros problemas. A seguir é apresentado o processo de cálculo das marcas d'água características da barra 680, cujo primeiro passo define-se pela escolha das frequências angulares dos sinais de potência ativa (ω_p) e reativa (ω_q). Tais valores podem ser adotados de forma arbitrária, desde que estejam situados entre 0 e 6 Hz e que, para uma mesma marca d'água, uma das frequências seja múltipla inteira da outra.

$$\omega_{p1} = 13{,}823\ rad/s \rightarrow\ f = 2{,}2\ Hz$$
$$\omega_{p2} = 27{,}646\ rad/s \rightarrow\ f = 4{,}4\ Hz$$
$$\omega_{q1} = 16{,}3363\ rad/s \rightarrow\ f = 2{,}6\ Hz$$
$$\omega_{q2} = 32{,}6726\ rad/s \rightarrow\ f = 5{,}2\ Hz$$

Após a definição das frequências das marcas d'água, calcula-se o módulo e a fase das respectivas funções de transferência para os valores estabelecidos. É importante assegurar-se de que as respostas em frequência do sistema apresentem módulos próximos à unidade em cada ponto de operação escolhido, o que diminui a atenuação do sinal propagado pela rede. O cálculo do módulo e fase das funções de transferência (3.5) e (3.6), considerando as frequências escolhidas para a marca d'água é dado por:

$$\left|H_p(j\omega_{p1})\right| = 1{,}0035 \qquad \angle H_p(j\omega_{p1}) = -0{,}0033\ rad$$
$$\left|H_p(j\omega_{p2})\right| = 1{,}0149 \qquad \angle H_p(j\omega_{p2}) = -0{,}011\ rad$$
$$\left|H_q(j\omega_{q1})\right| = 0{,}9308 \qquad \angle H_q(j\omega_{q1}) = -0{,}0262\ rad$$
$$\left|H_q(j\omega_{q2})\right| = 0{,}9184 \qquad \angle H_q(j\omega_{q2}) = -0{,}0224\ rad$$

Conforme (2.16), adotando-se $\alpha_1 = 0, \alpha_2 = \pi$, são obtidas as fases das senoides:

$$\phi_{p1} = \alpha_1 - \angle H_p(j\omega_{p1}) = 0{,}0033\ rad$$
$$\phi_{p2} = \alpha_2 - \angle H_p(j\omega_{p2}) = 3{,}1526\ rad$$
$$\phi_{q1} = \alpha_1 - \angle H_q(j\omega_{q1}) = 0{,}0262\ rad$$
$$\phi_{q2} = \alpha_2 - \angle H_q(j\omega_{q2}) = 3{,}1639\ rad$$

Por fim, calcula-se as amplitudes de cada uma das marcas d'água, sendo estas baseadas nos níveis dos sinais de referência das potências ativa e reativa definidos para o trecho. Os valores estabelecidos para esta parte do circuito são, respectivamente, 90 kW e 15 kvar, os quais se relacionam com as amplitudes das senoides conforme a seguir. Cabe destacar que tais grandezas representam 50% da capacidade nominal do trecho monitorado e foram definidas unicamente com a finalidade de provocar violações pontuais durante a operação do sistema.

$$A_{p1} + A_{p2} = 0{,}01 * P_{ref} \tag{3.8}$$

$$A_{q1} + A_{q2} = 0{,}01 * Q_{ref} \tag{3.9}$$

Assim, de acordo com (2.15), para o cálculo das amplitudes do sinal de potência ativa, tem-se:

$$\frac{A_{p1}\left|H_p(j\omega_{p1})\right|}{A_{p2}\left|H_p(j\omega_{p2})\right|} = \frac{\omega_{p2}}{\omega_{p1}} \rightarrow \frac{A_{p1} * 1{,}0035}{A_{p2} * 1{,}0149} = 2 \rightarrow A_{p1} = 2{,}0227 * A_{p2}$$

$$A_{P1} + A_{p2} = 900 \rightarrow 3{,}0227 * A_{P2} = 900$$

$$A_{p1} = 602{,}24$$

$$A_{p2} = 297{,}76$$

De igual modo, seguindo o mesmo método para a potência reativa, calcula-se:

$$\frac{A_{q1}\left|H_q(j\omega_{q1})\right|}{A_{q2}\left|H_q(j\omega_{q2})\right|} = \frac{\omega_{q2}}{\omega_{q1}} \rightarrow \frac{A_{q1} * 0{,}9308}{A_{q2} * 0{,}9184} = 2 \rightarrow A_{q1} = 1{,}9734 * A_{q2}$$

$$A_{q1} + A_{q2} = 150 \rightarrow 2{,}9734 * A_{q2} = 150$$

$$A_{q1} = 99{,}55$$

$$A_{q2} = 50{,}45$$

Finalmente os sinais das marcas d'água da potência ativa e reativa são, respectivamente:

$$M_P = 602{,}24sen(13{,}823t + 0{,}0033) + 297{,}76sen(27{,}646t + 3{,}1526)$$

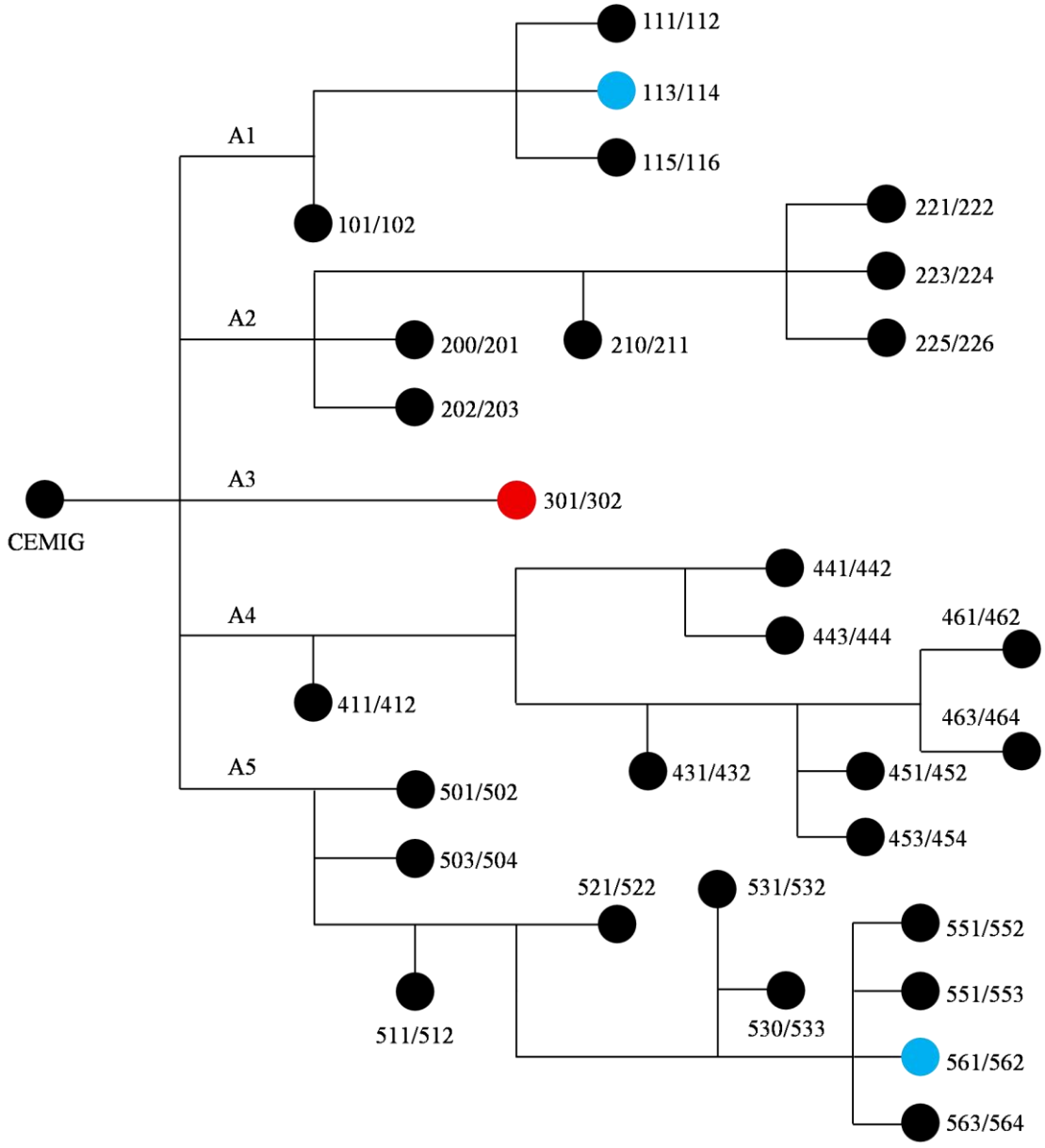
$$M_Q = 99{,}55sen(16{,}3363t + 0{,}0262) + 50{,}45sen(32{,}6726t + 3{,}1639)$$

3.3.2 *Sistema elétrico da Unifei e cálculo da marca d'água característica*

O sistema elétrico da Unifei opera com o nível de tensão de 13,8 kV, fornecido pela Companhia Energética de Minas Gerais (CEMIG). Este circuito é dividido em cinco ramificações, que alimentam 29 blocos, cada uma destas configurada com um perfil de carga próprio, discretizados em 96 aferições, durante um período de 24 horas. Os valores de cada ponto da demanda consistem na interpolação de dados reais, os quais correspondem ao dia 16 de março de 2023, data de registro do maior nível de geração fotovoltaica obtido pela rede. O

pico de consumo do sistema é de aproximadamente 540 kW, sendo este atingido às 14h45min. A Figura 19 ilustra a disposição dos principais elementos do sistema da Unifei, cujos pontos em vermelho e em azul representam, respectivamente, o Centro de Controle e as barras monitoradas do circuito.

Figura 19 – Representação do sistema elétrico da Unifei.



Fonte: Autoria própria (2025).

O sistema é implementado utilizando-se de um único *linecode*, o qual caracteriza as 45 linhas que conectam as 75 barras do circuito. Vale ressaltar que a microrrede da Unifei possui quatro geradores fotovoltaicos, cada um com seu perfil de geração próprio. Além disso, esta

rede conta com um elemento de armazenamento de energia, cuja operação segue uma curva de funcionamento definida a cada 15 minutos. A Tabela 5[10] a seguir ilustra os principais dados dos geradores, bem como do sistema de armazenamento.

Tabela 5 – Geradores e sistema de armazenamento de energia da Unifei.

Elemento	Alimentador	Capacidade	Barra de Conexão	Tensão (kV)
Gerador 1	2	70 kW	222	0,22
Gerador 2	3	300 kW	302	0,22
Gerador 3	4	50 kW	442	0,22
Gerador 4	5	80 kW	564	0,22
Gerador 5	1	100 kW	114	0,22
Gerador 6	5	100 kW	562	0,22
Armazenamento	3	150 kVA	302	0.22

Fonte: Autoria própria.

O Alimentador 1 (A1) é composto por seis linhas de transmissão distribuídas entre 10 barras. Este trecho da rede é constituído por quatro transformadores, cada um alimentando uma única carga. A Tabela 6 apresenta as principais informações dos transformadores, bem como das cargas conectadas à esta ramificação.

Tabela 6 – Transformadores e cargas do Alimentador 1.

Elemento	Barra	Níveis de Tensão (kV)	Conexão	Capacidade (kVA)
Transformador 1	101/102	13,8/0,22	Delta/Estrela	75
Transformador 2	111/112	13,8/0,22	Delta/Estrela	150
Transformador 3	113/114	13,8/0,22	Delta/Estrela	150
Transformador 4	115/116	13,8/0,22	Delta/Estrela	750
Carga 1	102	0,22	Estrela	75
Carga 2	112	0,22	Estrela	150
Carga 3	114	0,22	Estrela	150
Carga 4	116	0,22	Estrela	750

Fonte: Autoria própria.

Com relação ao Alimentador 2 (A2), este é constituído por sete linhas de distribuição, as quais interligam 13 barras. Esta parte do circuito é composta por seis transformadores, e seis cargas distintas, conectadas em 220 V. A Tabela 7 apresenta as principais características dos transformadores e das cargas pertencentes a este trecho da microrrede.

[10] Os Geradores 5 e 6, apresentados na Tabela 5, não pertencem ao circuito original, tendo sido incluídos apenas para fins de compatibilidade com o modelo ilustrado na Figura 15.

Tabela 7 – Transformadores e cargas do Alimentador 2.

Elemento	Barra	Níveis de Tensão (kV)	Conexão	Capacidade (kVA)
Transformador 1	200/201	13,8/0,22	Delta/Estrela	112,5
Transformador 2	202/203	13,8/0,22	Delta/Estrela	150
Transformador 3	210/211	13,8/0,22	Delta/Estrela	300
Transformador 4	221/222	13,8/0,22	Delta/Estrela	150
Transformador 5	223/224	13,8/0,22	Delta/Estrela	300
Transformador 6	225/226	13,8/0,22	Delta/Estrela	150
Carga 1	203	0,22	Estrela	112,5
Carga 2	211	0,22	Estrela	150
Carga 3	222	0,22	Estrela	300
Carga 4	224	0,22	Estrela	150
Carga 5	226	0,22	Estrela	300
Carga 6	302	0,22	Estrela	150

Fonte: Autoria própria.

O Alimentador 3 (A3) é composto por um único transformador, cuja capacidade é de 500 kVA. Este elemento opera com níveis de tensão de 13,8 kV no primário e 220 V no secundário, instalado nas conexões Delta/Estrela. Duas linhas complementam este trecho da rede, as quais suprem uma única carga de 500 kVA. Já o Alimentador 4 (A4), conta com oito transformadores, os quais fornecem energia para oito cargas distintas. Esta ramificação é composta por 15 linhas de distribuição e 23 barras. A Tabela 8 ilustra as principais características dos transformadores do Alimentador 4, bem como de suas cargas.

Tabela 8 – Transformadores e cargas do Alimentador 4.

Elemento	Barra	Níveis de Tensão (kV)	Conexão	Capacidade (kVA)
Transformador 1	411/412	13,8/0,22	Delta/Estrela	150
Transformador 2	431/432	13,8/0,22	Delta/Estrela	112,5
Transformador 3	441/442	13,8/0,22	Delta/Estrela	150
Transformador 4	443/444	13,8/0,22	Delta/Estrela	150
Transformador 5	461/462	13,8/0,22	Delta/Estrela	75
Transformador 6	463/464	13,8/0,22	Delta/Estrela	112,5
Transformador 7	451/452	13,8/0,22	Delta/Estrela	150
Transformador 8	453/454	13,8/0,22	Delta/Estrela	225
Carga 1	412	0,22	Estrela	150
Carga 2	432	0,22	Estrela	112,5
Carga 3	442	0,22	Estrela	150
Carga 4	444	0,22	Estrela	150
Carga 5	462	0,22	Estrela	75
Carga 6	464	0,22	Estrela	112,5
Carga 7	452	0,22	Estrela	150
Carga 8	454	0,22	Estrela	225

Fonte: Autoria própria.

Considerando o Alimentador 5 (A5), este é composto por 15 linhas de distribuição, as quais estão ligadas a 26 barras. Possui conectados em seu circuito dez transformadores, que suprem a energia demandada por dez cargas. A Tabela 9 apresenta os dados dos transformadores e das cargas pertencentes a esta parte do sistema.

Tabela 9 – Transformadores e cargas do alimentador 5.

Elemento	Barra	Níveis de Tensão (kV)	Conexão	Capacidade (kVA)
Transformador 1	501/502	13,8/0,22	Delta/Estrela	500
Transformador 2	503/504	13,8/0,22	Delta/Estrela	150
Transformador 3	511/512	13,8/0,22	Delta/Estrela	150
Transformador 4	521/522	13,8/0,22	Delta/Estrela	112,5
Transformador 5	531/532	13,8/0,22	Delta/Estrela	225
Transformador 6	530/533	13,8/0,44	Delta/Estrela	225
Transformador 7	551/552	13,8/0,22	Delta/Estrela	112,5
Transformador 8	551/553	13,8/0,22	Delta/Estrela	225
Transformador 9	561/562	13,8/0,22	Delta/Estrela	75
Transformador 10	563/564	13,8/0,22	Delta/Estrela	225
Carga 1	502	0,22	Estrela	500
Carga 2	504	0,22	Estrela	150
Carga 3	512	0,22	Estrela	150
Carga 4	522	0,22	Estrela	112,5
Carga 5	532	0,22	Estrela	225
Carga 6	533	0,44	Estrela	225
Carga 7	552	0,22	Estrela	112,5
Carga 8	553	0,22	Estrela	225
Carga 9	562	0,22	Estrela	75
Carga 10	564	0,22	Estrela	225

Fonte: Autoria própria.

Os pontos de monitoramento desta microrrede foram distribuídos entre o Alimentador 1 (Barra 114) e o Alimentador 5 (Barra 562). O Centro de Controle está localizado no bloco I, que recebe energia diretamente do Alimentador 3. Para cada elemento supervisionado foram testados dois ambientes de comunicação diferentes, sendo estes a transmissão sem protocolo modelado com inserção de ruído AWGN e um modelo simplificado da tecnologia Ethernet.

Assim como no sistema IEEE 13 Barras, as variáveis controladas pela rede são as potências ativa e reativa das barras, as quais são enviadas pelos medidores ao Centro de Controle, que retorna o valor de referência para aquele período específico da operação. Com relação às simulações, foi considerado apenas um valor de referência para cada barra, sendo estes estabelecidos pelo Centro de Controle. Além disso, estas barras estão instaladas a diferentes distâncias do Centro de Controle, fato que influencia na performance do sistema de comunicação adotado. A seguir, são apresentados os cálculos das marcas d'água para cada um dos pontos de monitoramento da rede. Vale ressaltar que este sistema emprega a mesma metodologia de cálculo das marcas d'água utilizadas pelo sistema IEEE 13 Barras. Portanto, estes são apresentados de forma simplificada em seguida.

A função de transferência utilizada para determinação da marca d'água tem o mesmo formato das equações (3.5) e (3.6), tanto para a potência ativa, quanto para a reativa. Porém, os parâmetros foram ajustados com base nos *linecodes* utilizados para caracterização das linhas de distribuição do sistema da Unifei. Estes valores são:

- Barra 114 – Alimentador 1: Esta barra teve sua distância estimada em 90 metros a partir do Centro de Controle. Uma vez que a capacidade total desta carga é de 150 kVA e o fator de potência consta em 0,92, os valores limite de potências ativa e reativa desta barra são, respectivamente 138 kW e 58,5 kvar. No entanto, conforme definidos para o sistema IEEE 13 Barras, os sinais de referência estabelecidos pelo Centro de Controle foram determinados em 50% destes, sendo 69 kW e 29,5 kvar. Além disso, as frequências adotadas para as marcas d'água foram de 2,5 Hz e 5 Hz para a potência ativa, e iguais a 0,7 Hz e 3,5 Hz para a potência reativa. Com isso, obteve-se as seguintes expressões do sinal de autenticação:

$$M_{P114} = 462{,}24sen(15{,}708t + 0{,}004) + 227{,}76sen(31{,}4159t + 3{,}1564)$$
$$M_{Q114} = 244{,}74sen(4{,}3982t + 0{,}0227) + 50{,}26sen(21{,}9911t + 3{,}1669)$$

- Barra 562 – Alimentador 5: Esta barra teve sua distância estimada em 180 metros a partir do Centro de Controle. Uma vez que a capacidade total desta carga é de 75 kVA e o fator de potência consta em 0,92, os valores limite de potências ativa e reativa desta barra são, respectivamente 69 kW e 29,5 kvar. No entanto, conforme definidos para o sistema IEEE 13 Barras, os sinais de referência estabelecidos pelo Centro de Controle foram determinados em 50% destes, sendo 34,5 kW e 14,75 kvar. Além disso, as frequências adotadas para as marcas d'água foram de 1,7 Hz e 3,4 Hz para a potência ativa, e iguais a 1,3 Hz e 3,9 Hz para a potência reativa. Com isso, obteve-se as seguintes expressões:

$$M_{P562} = 230{,}5sen(10{,}6814t + 0{,}0024) + 114{,}5sen(21{,}3628t + 3{,}1482)$$
$$M_{Q562} = 110{,}03sen(8{,}1681t + 0{,}024) + 37{,}47sen(24{,}5044t + 3{,}1662)$$

3.3.3 *Descrição do sistema de controle da microrrede*

O sistema de controle de uma microrrede é responsável pelos processos de monitoramento e verificação das variáveis de estado do circuito, podendo atuar de maneira preventiva e/ou corretiva, caso algum evento inesperado ocorra. A modelagem deste mecanismo foi implementada em Python, cuja captura e análise dos parâmetros controlados é feita a partir da sua integração com o OpenDSS, por meio da interface COM disponível em sistemas operacionais Windows®. O desenvolvimento completo do sistema de controle foi realizado pela criação de cinco classes básicas, as quais estão integradas entre si, sendo algumas

delas acionadas somente em situações de anomalia na operação da microrrede. Estas foram nomeadas como: Principal, Monitoramento, Acionamento, Comunicação e Calibração.

A classe Principal é responsável somente pela inicialização do OpenDSS, na qual o usuário determina o local de registro dos resultados das simulações, bem como o arquivo descritivo do circuito da microrrede. Assim, após analisar o funcionamento da interface COM e confirmar a sua correta inicialização, este trecho do código exibe diversos parâmetros do sistema elétrico, como número de transformadores instalados na rede, capacitores, elementos de armazenamento, geradores distribuídos, informações sobre as barras do sistema, tensões nominais do circuito, além do comprimento das linhas. Uma vez realizadas as verificações necessárias, o usuário poderá selecionar o tipo de simulação que deseja executar, sendo estas instantâneas ou temporais, de acordo com o período estabelecido para os testes. Além disso, é possível escolher as tecnologias de comunicação a serem utilizadas pela microrrede, quais sejam: Transmissão sem Protocolo, Inserção de Ruído, e Meio Cabeado.

Após a definição de todas as configurações da simulação, a classe Monitoramento é acionada, a qual determina, de forma instantânea, ou de acordo com o número de passos previamente estabelecido pelo usuário, os valores de potências ativa e reativa das barras do sistema, sendo estes extraídos diretamente do *software* OpenDSS. Caso a operação da microrrede transcorra normalmente, ou seja, sem qualquer violação dos parâmetros do circuito, o programa permanece executando a classe Monitoramento até o final, exibindo os valores medidos pelo sistema de controle e atestando a operação correta da microrrede.

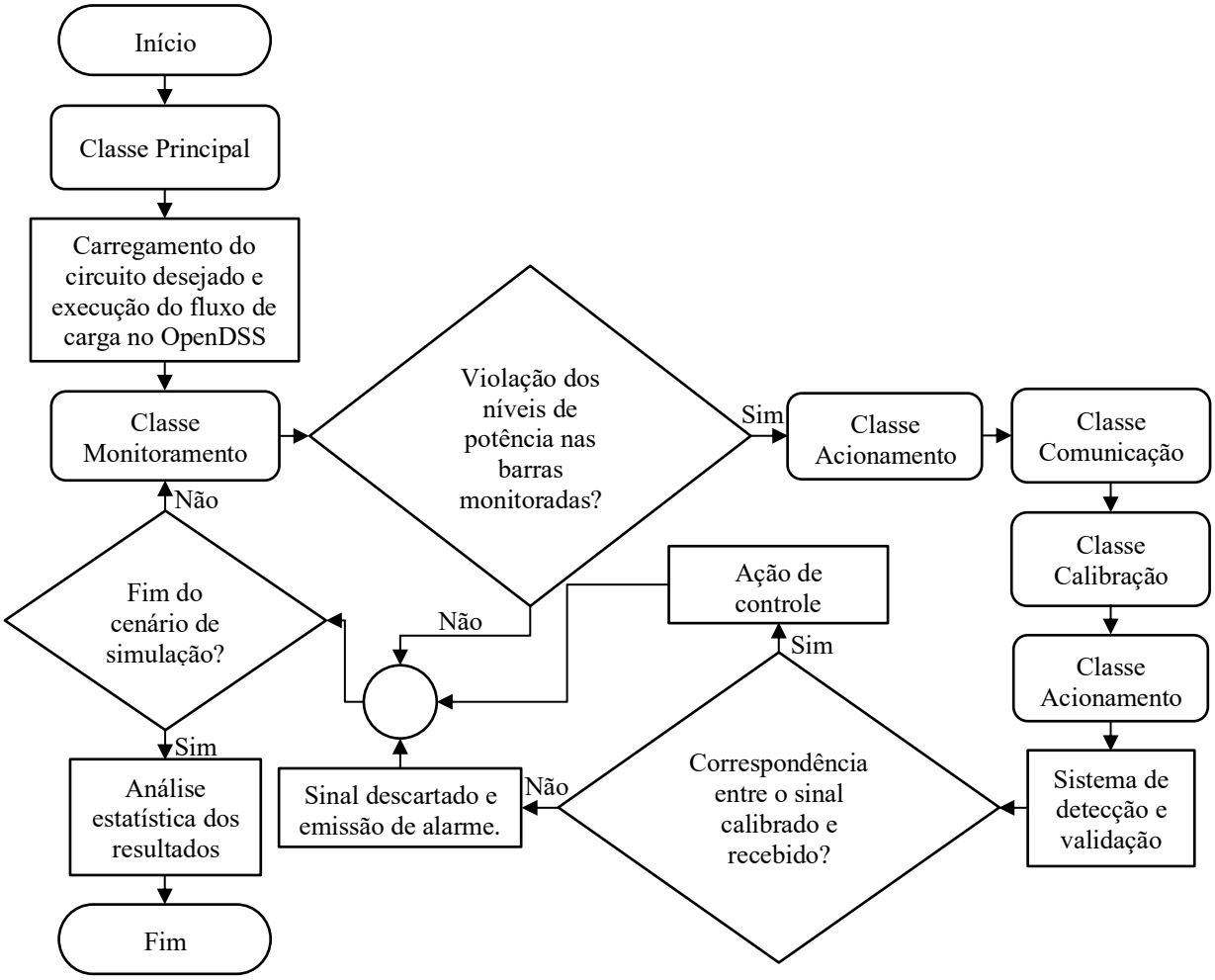
Na hipótese da ocorrência de qualquer violação de potência ativa e/ou reativa em alguma barra do circuito, a classe Acionamento, que representa o envio e o recebimento de comandos por parte da microrrede, é executada. Esta, com base nos valores instantâneos medidos para aquele trecho do sistema, define a ação que deve ser efetuada pelos operadores da rede. Nesta parte do código são inseridas as marcas d'água aditivas às informações de controle, que correspondem aos sinais de medição enviados pela rede. Para este trabalho, ações corretivas são demandadas somente em situações nas quais os limites de potência ativa ou reativa das barras tenham sido extrapolados.

A simulação do meio de propagação pelos quais trafegam os sinais de controle da microrrede é realizada pela classe Comunicação. Nesta foram modelados os canais de transmissão dos dados, de acordo com a tecnologia selecionada pelo usuário. Com isso, a informação trafegada entre os elementos da rede é submetida a um processo de degradação provocado pelo meio de propagação, que são a introdução de latência, atenuação do sinal e

inserção de ruído, os quais são determinados de acordo com a distância entre a origem e o destino da comunicação.

Assim que o sinal é recebido, este é tratado pelo Periodograma, tendo suas DEP calculadas e comparadas com os valores preliminarmente aferidos e armazenados pela classe Calibração, de acordo com o meio de comunicação escolhido. Havendo correspondência entre as componentes espectrais do sinal recebido e aquelas determinadas pelo sistema de calibração, o sinal é validado e a ação corretiva efetuada. Do contrário, os dados são descartados e um alarme é emitido na microrrede. A Figura 20 apresenta o fluxograma ilustrativo do funcionamento do sistema de controle implementado.

Figura 20 – Fluxograma do sistema de controle da microrrede.



Fonte: Autoria própria (2025).

Uma vez que o objetivo deste trabalho é somente verificar a eficácia dos métodos de detecção da marca d'água, apenas o percurso do sinal entre o elemento de medição e o Centro de Controle foi simulado, não sendo considerado o tráfego reverso contendo a ação corretiva

por parte dos operadores da rede. As seções a seguir descrevem em maiores detalhes os meios de propagação modelados em Python, bem como o mecanismo de detecção da marca d'água implementado.

3.3.4 *Modelagem dos meios de propagação utilizados*

Considerando os canais de comunicação modelados nas simulações tem-se a implementação de três funções, as quais podem ser selecionadas quando da inicialização dos testes. Estas são representadas por uma transmissão sem protocolo modelado, uma transmissão sem protocolo com inserção de ruído AWGN, além da tecnologia cabeada Ethernet. Com isso, torna-se possível, por meio de cada cenário testado, verificar os efeitos dos meios de propagação sobre os sinais de controle enviados pela microrrede.

Para o sistema sem tecnologia de comunicação modelada, foi configurado apenas o atraso de propagação provocado nos dados transmitidos, sendo este determinado em função da distância da barra monitorada, a qual é dividida pela velocidade de propagação da luz no vácuo ($C = 3 * 10^8 m/s$). Nesta função, nenhum outro nível de degradação foi inserido na informação de controle, como adição de ruído, dispersão do sinal, múltiplos percursos ou atenuação. Vale ressaltar que este meio de transmissão foi introduzido apenas para fins de validação da metodologia de autenticação adotada, sendo utilizado somente pelo sistema IEEE 13 Barras.

O sistema com inserção de ruído AWGN foi modelado apenas com um valor de relação sinal-ruído, do inglês, *Signal-to-Noise Ratio* (SNR), o qual pode ser configurado pelo usuário, sendo este definido em decibéis (dB). Além disso, assim como na transmissão sem protocolo, um valor de latência é introduzido à comunicação, de acordo com a distância entre transmissor e receptor.

Já o meio cabeado modela a tecnologia Ethernet, com taxa de transmissão igual a 10 Mbps, além da introdução de um fator de atenuação (α) conforme a qualidade do meio de propagação[11]. O sistema também permite a inserção de diferentes níveis de ruído na comunicação, dados em dB. Caso a distância percorrida pelo sinal de comunicação exceda os 100 metros, este é regenerado e transmitido pelo trecho restante.

[11] A fórmula característica para determinação da atenuação provocada ao sinal transmitido é: $Atenuação = 10^{-\alpha * d/10}$, na qual d representa a distância percorrida pela informação (Weik, 2012).

3.3.5 *Mecanismos de detecção implementados*

Para a detecção e validação das marcas d'água aditivas aos sinais de controle da microrrede, foi utilizado o Periodograma, que é uma ferramenta de *software* baseada na estimação da DEP a partir de amostras temporais discretas do sinal de interesse (MathWorks®, 2024). Esta técnica foi inteiramente modelada em Python, constituindo a última etapa do algoritmo implementado.

O processo de análise da informação se dá em duas etapas, que são a aplicação da Transformada de Fourier à entrada passando-a para o domínio da frequência, bem como a determinação do nível de potência das suas componentes espectrais, que ocorre elevando-se o sinal transformado ao quadrado, normalizando-o pelo número de amostras coletadas (Corinthios, 2018). Ambos os cálculos executados pelo Periodograma são apresentados por (3.10) e (3.11), os quais são descritos a seguir:

$$X[k] = \sum_{n=0}^{N-1} x[n] e^{\frac{-j2\pi kn}{N}} \tag{3.10}$$

Na qual,

N: número de amostras do sinal.

n: índices temporais discretos do sinal, variando de 0 até N-1.

k: índices das componentes de frequência dos sinais, variando de 0 até N-1.

x[n]: sinal discretizado no domínio do tempo.

X[k]: Sinal no domínio da frequência, após a aplicação da Transformada de Fourier.

$$P_{xx}(f_k) = \frac{1}{N}|X[k]|^2 \tag{3.11}$$

$$f_k = \frac{k f_s}{N} \tag{3.12}$$

$$-\frac{1}{2\Delta t_s} \leq f_k \leq \frac{1}{2\Delta t_s} \tag{3.13}$$

Nas quais,

f_k: Frequência de interesse.

f_s: Frequência de amostragem.

t_s: Intervalo de amostragem ($1/f_s$).

Assim, de acordo com a equação (3.13), a componente espectral de interesse possui um ciclo temporal pelo menos duas vezes maior que o da frequência de amostragem, obedecendo

ao Teorema de Nyquist[12]. Com isso, garante-se que a integridade das informações do sinal analisado seja preservada ao longo das etapas subsequentes de processamento (Braga, 2019).

Uma das abordagens implementadas no cálculo do Periodograma é o método de Welch. Nessa técnica, longas sequências de dados temporais são subdivididas em segmentos menores e sobrepostos, sobre os quais se aplica uma janela adequada para, em seguida, calcular o Periodograma individual de cada parte. Em seguida, as estimativas obtidas são combinadas por meio de uma média, o que promove a redução da variância na estimativa espectral. Além disso, o método é compatível com diferentes tipos de janelas, permitindo ajustes conforme as características do sinal analisado (Marple Jr., 2019).

Para o enquadramento do sinal, foi adotada a janela de Hamming, uma técnica caracterizada por proporcionar transições mais suaves nas extremidades da sequência temporal. Esta abordagem é eficaz no que se refere à atenuação de efeitos indesejados decorrentes de descontinuidades nas bordas do sinal, tais como o vazamento espectral, o que poderia comprometer a análise correta das DEP (Harris, 1988). É importante destacar que este processo consiste na multiplicação do sinal no tempo por uma função de formato específico, operação que, por sua vez, equivale à convolução no domínio da frequência. A formulação matemática que descreve a janela adotada é apresentada a seguir (Kuo; Lee; Tian, 2006).

$$w[n] = 0{,}54 - 0{,}46 * \cos\left(\frac{2\pi n}{N-1}\right) \tag{3.14}$$

Na qual:

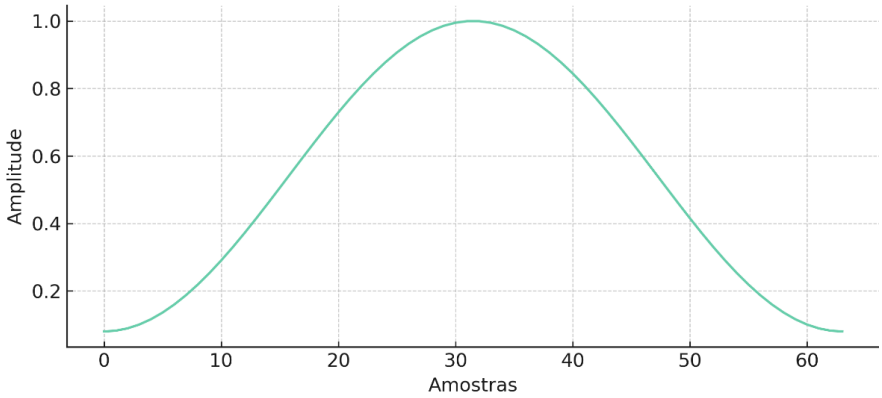
N: Número de pontos da janela.

n: Índice discreto do tempo $0 \leq n \leq N\text{-}1$.

Com isso, no domínio temporal, tem-se uma cossenoide invertida, a qual começa e termina com valores próximos de zero nas extremidades e iguais a um em torno do centro, conforme pode ser visto por meio do Gráfico 5. Tal característica faz com que a janela Hamming reduza significativamente as descontinuidades nas bordas do sinal, atenuando, com maior eficácia, as componentes fora de sua banda principal.

[12] O Teorema de Nyquist estabelece que, para garantir a reconstrução fidedigna de um sinal contínuo a partir de suas amostras, a frequência de amostragem deve ser, no mínimo, o dobro da maior componente presente em seu espectro (Comer, 2016).

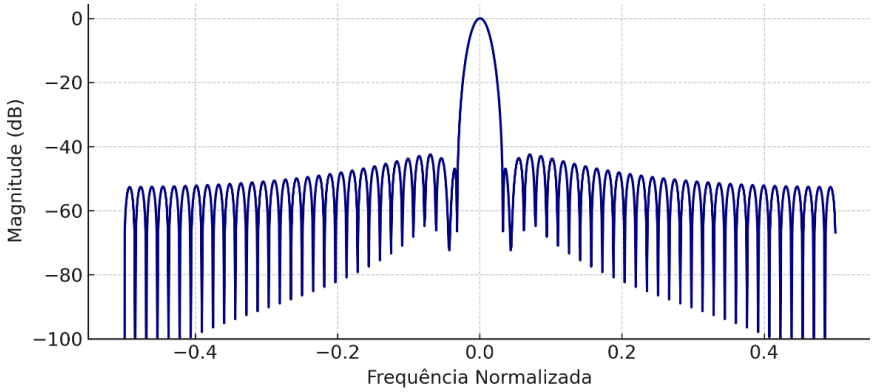
Gráfico 5 – Janela de Hamming no domínio temporal.



Fonte: Autoria própria (2025).

Em contrapartida, ao se analisar a janela de Hamming no domínio da frequência, observa-se que as componentes laterais possuem níveis aproximadamente 40 dB abaixo da amplitude do lobo principal, o que contribui para um baixo vazamento espectral em comparação com a janela retangular padrão, cujas diferenças situam-se acima de 20 dB (SciPy, 2025). No entanto, a largura do lobo principal da janela de Hamming é mais extensa, o que reduz o poder de resolução na estimativa da DEP, tornando mais difícil a distinção entre componentes de frequência próximas (Prabhu, 2018). O Gráfico 6 a seguir ilustra a resposta em frequência desta função de ponderação.

Gráfico 6 – Janela de Hamming no domínio da frequência.



Fonte: Autoria própria (2025).

Baseado no método de Welch e utilizando a janela de Hamming, foi implementado um sistema de calibração para análise espectral. De acordo com o meio de transmissão selecionado pelo usuário, valores previamente calculados por meio do Periodograma de Welch, com janelamento Hamming, são armazenados. Considerando que a frequência de amostragem dos sinais gerados é de 20 kHz e que o cálculo do Periodograma é realizado com uma taxa de 2

kHz, a resolução em frequência resulta em 0,1 Hz. Assim, entre 0 Hz e 6 Hz, o sistema de calibração armazena 61 valores de referência, tanto para a potência ativa quanto para a reativa.

No processo de recepção, o sistema separa as partes do sinal associadas à marca d'água da potência ativa e da reativa. Estas componentes são, então, filtradas por um FPB com frequência de corte em 6 Hz, calculando-se, em seguida, suas respectivas DEP no intervalo de 0 a 6 Hz, para posterior comparação com os valores armazenados durante a calibração. Na hipótese da detecção de uma diferença igual ou superior a 25 dB entre qualquer uma delas e seu valor de referência correspondente, tal frequência é considerada inválida. Caso duas ou mais violações desse tipo ocorram, o sinal completo é descartado e um alarme é emitido na rede. Vale ressaltar que os sinais de potência ativa e reativa são avaliados conjuntamente, ou seja, a invalidação de um implica na rejeição automática do outro. Os limiares de comparação e o número de frequências permitidas com discrepâncias foram definidos empiricamente, com base em testes e observações experimentais.

O próximo capítulo descreve os cenários de simulação adotados, abrangendo tanto o sistema de validação, implementado na rede IEEE 13 Barras, quanto a avaliação do desempenho das marcas d'água durante a operação em um modelo de microrrede real, representado pelo circuito elétrico da Unifei. Em seguida, são apresentados os resultados obtidos sob diferentes condições do canal de comunicação da microrrede, juntamente com suas respectivas análises.

CAPÍTULO 4 – RESULTADOS

O presente capítulo aborda a descrição dos cenários de testes implementados, bem como a apresentação dos resultados e suas respectivas análises. Para tanto, foram utilizados dois sistemas: a rede IEEE 13 Barras, destinada à validação do mecanismo de detecção das marcas d'água, e o circuito elétrico da Unifei, que simula um modelo de microrrede real operada remotamente por um Centro de Controle, o qual, em ambos os sistemas, é responsável pelo monitoramento dos seus níveis de potência ativa e reativa.

A rede IEEE 13 Barras foi empregada exclusivamente para validar o sistema de detecção desenvolvido. Nesse contexto, configuraram-se três cenários distintos: o envio de marcas d'água verdadeiras; a comunicação de sinais de controle desprovidos de qualquer autenticação adicional; e a transmissão de marcas d'água falsas, simulando a ação de um agente externo. O meio de propagação utilizado neste ambiente não possui protocolo modelado, restringindo-se apenas à inserção de um atraso de comunicação nos sinais transmitidos, sem degradações adicionais. Vale destacar que, nesse sistema, apenas uma barra é supervisionada pelo Centro de Controle.

Por sua vez, o modelo de microrrede real, representado pelo circuito elétrico da Unifei, conta com duas barras monitoradas, localizadas a diferentes distâncias do Centro de Controle. Nessa configuração, avaliou-se o desempenho do sistema de detecção, operando sob variadas condições de comunicação, incluindo um modelo sem protocolo com ruído AWGN e um ambiente simplificado baseado na tecnologia Ethernet.

Finalmente, foi realizada a análise do desempenho do sistema de recepção, implementado localmente nas barras sob supervisão. Inicialmente, analisou-se a inserção de latência adicional nos sinais de controle da microrrede e sua viabilidade para aplicações reais. Na sequência, foi examinado o consumo energético extra introduzido pelo sistema de detecção, considerando sua aplicabilidade em soluções IoT de baixo consumo.

4.1 SISTEMA IEEE 13 BARRAS

Para a validação do mecanismo de recepção das marcas d'água, considerou-se apenas um ambiente de propagação, utilizando o sistema IEEE 13 Barras, sem a modelagem de protocolos de comunicação. Nessa configuração, foram analisados apenas os atrasos de transmissão, diretamente proporcionais à distância entre a barra monitorada e o Centro de Controle. O ponto supervisionado foi a barra 680, posicionada a 121,92 metros do Centro de

Controle, localizado na subestação do sistema. Assim, a latência aferida corresponde à razão entre a velocidade da luz no vácuo e a distância mencionada, resultando em aproximadamente 406 nanossegundos.

Para assegurar a eficácia da validação, foram implementados três cenários distintos. O primeiro consistiu no envio da marca d'água legítima, avaliando a capacidade do mecanismo de identificar transmissões autênticas. O segundo abordou a transmissão de dados desprovidos das marcas d'água, com o objetivo de verificar a resposta do sistema na ausência do identificador. Por fim, o terceiro teste simulou a introdução de marcas d'água falsas, tanto para potência ativa quanto reativa, representando uma tentativa de ataque externo. Dessa forma, foi possível analisar a eficiência do receptor na detecção de *replay attacks*.

Conforme já mencionado, na barra monitorada foi instalada uma carga com capacidade total de 180 kW e 30 kvar, a qual foi programada para operar a 50% deste valor. Para cada um dos testes previamente descritos, o circuito foi simulado no modo *snapshot*[13] do OpenDSS, com a rede operando em condição nominal de demanda energética. Desta forma, em todos os cenários implementados, foi gerado o disparo automático de uma ação corretiva por parte do Centro de Controle, permitindo a avaliação completa do desempenho do mecanismo de validação das marcas d'água.

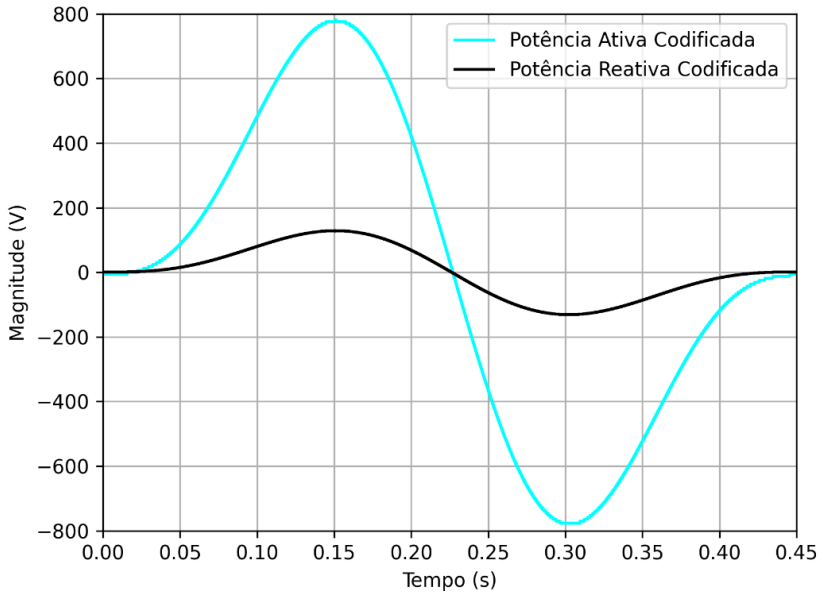
4.1.1 *Sinal de autenticação verdadeiro (Cenário 1)*

Para o Cenário 1, considerando a validação do sistema de detecção, foram adicionadas as marcas d'água autênticas aos sinais de controle da microrrede. Estas foram previamente calculadas na subseção 3.3.1, com suas componentes espectrais aferidas pelo Periodograma e armazenadas pelo sistema de calibração, cujo cálculo também leva em conta as características do ambiente de propagação.

O Gráfico 7 ilustra os sinais de potência ativa e reativa recuperados pelo receptor, os quais correspondem às marcas d'água originais configuradas para autenticação. Observa-se que os sinais recebidos nas barras monitoradas não apresentam nenhum nível de degradação, uma vez que o meio de comunicação é isento de ruído e não introduz atenuação significativa aos dados transmitidos.

[13] O termo *snapshot* se refere a uma execução única e instantânea do fluxo de carga no *software* OpenDSS.

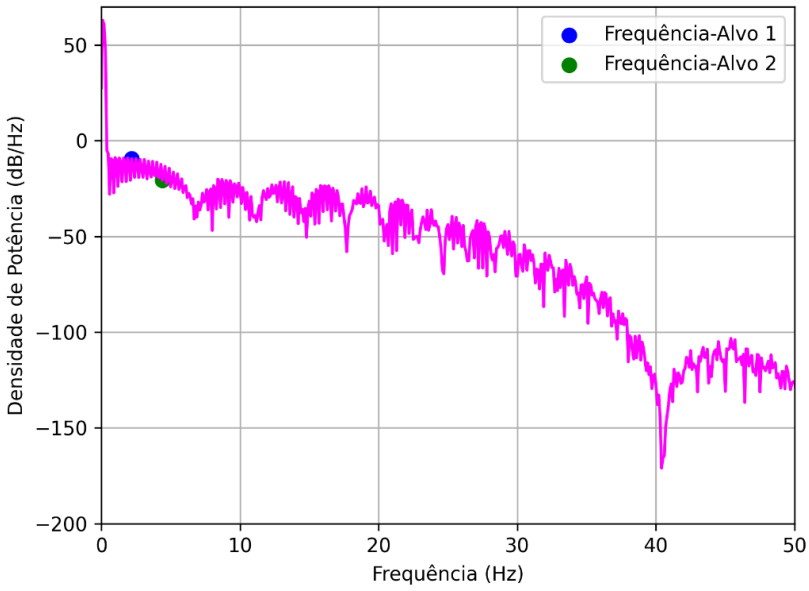
Gráfico 7 – Sinais legítimos de potência ativa e reativa recuperados (Cenário 1).



Fonte: Autoria própria (2025).

O Gráfico 8 apresenta a DEP estimada por meio do Periodograma, no contexto do controle da potência ativa. Embora as frequências centrais da marca d'água estejam em 2,2 Hz e 4,4 Hz, seus níveis de energia, sendo iguais a –9,42 dB/Hz e –20,62 dB/Hz, respectivamente não constam entre os mais elevados do espectro. Os maiores picos da DEP concentram-se nas proximidades de 0 Hz, com valor máximo registrado em 0,1 Hz, atingindo 62,95 dB/Hz.

Gráfico 8 – DEP do sinal legítimo de potência ativa (Cenário 1).

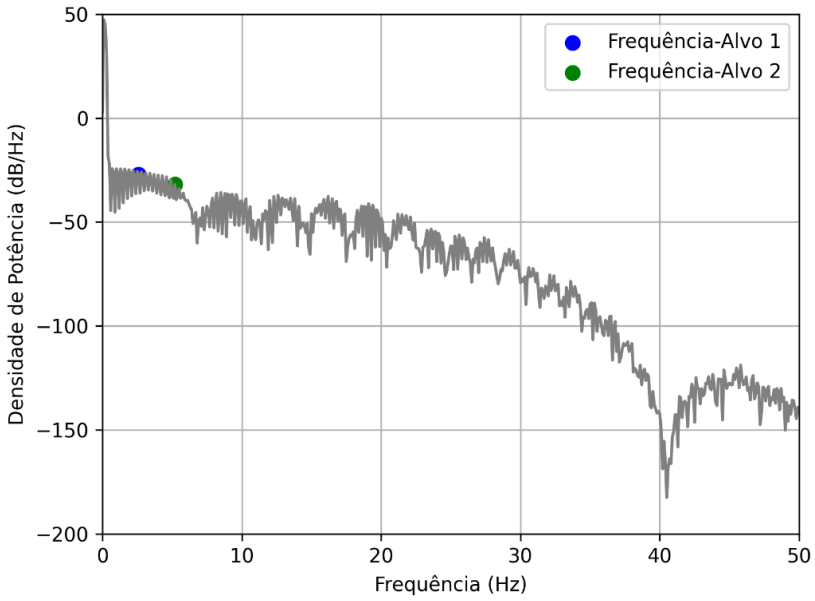


Fonte: Autoria própria (2025).

O efeito acima decorre da aplicação de uma janela finita (Hamming), que introduz alargamento espectral do sinal (*spectral leakage*) e distribui parte de sua energia para frequências vizinhas (Xu *et al.*, 2025). Além disso, a utilização do método de Welch, ao realizar a segmentação da marca d'água e determinar as médias entre elas, pode provocar a suavização, bem como a atenuação de picos espectrais (Jwo; Chang; Wu, 2021). Ainda assim, levando-se em conta que o sinal transmitido não sofreu degradações, a DEP obtida é idêntica à armazenada pelo sistema de calibração.

De forma semelhante, o Gráfico 9 apresenta a DEP do sinal de potência reativa. As frequências principais, de 2,6 Hz e 5,2 Hz, também não correspondem aos maiores picos de energia no espectro, pelas mesmas razões apontadas para a marca d'água da potência ativa, tendo seus valores de DEP iguais a –27,18 dB/Hz e –31,92 dB/Hz, nesta ordem. Mais uma vez, a frequência de 0,2 Hz destacou-se com o maior valor dentro da faixa de operação das marcas d'água, registrando 47,36 dB/Hz. Assim como no caso da potência ativa, a ausência de perdas no sinal garante que a DEP calculada coincida com aquela obtida pelo sistema de calibração.

Gráfico 9 – DEP do sinal legítimo de potência reativa (Cenário 1).



Fonte: Autoria própria (2025).

Considerando que não se observou qualquer discrepância entre os sinais recebidos e os calibrados, a autenticação das marcas d'água, tanto para potência ativa quanto para reativa, foi concluída com êxito. Consequentemente, uma ação corretiva foi executada localmente para ajustar os níveis de potência da microrrede, validando o mecanismo desenvolvido para este cenário.

4.1.2 *Sinal sem autenticação (Cenário 2)*

No Cenário 2 em que o sinal foi transmitido ausente da marca d'água, o sistema de detecção rejeitou completamente a tentativa de autenticação, atestando o funcionamento correto do mecanismo implementado. Isso ocorreu, pois o Periodograma, responsável pela análise espectral, estimou tanto a marca d'água da potência ativa quanto da reativa como equivalentes a zero. Com isso, todas as 61 componentes de frequência da informação recebida divergiram em mais de 25 dB, quando comparadas aos valores armazenados pelo sistema de calibração.

É importante ressaltar que, devido à ausência de autenticação nos sinais de controle enviados pelos operadores da microrrede, não foi possível realizar a reconstrução das marcas d'água associadas a essas transmissões. Além disso, a inexistência de informações relevantes inviabilizou a elaboração dos gráficos correspondentes tanto às marcas d'água recuperadas quanto às suas respectivas estimativas de DEP.

4.1.3 *Sinal de autenticação falso (Cenário 3)*

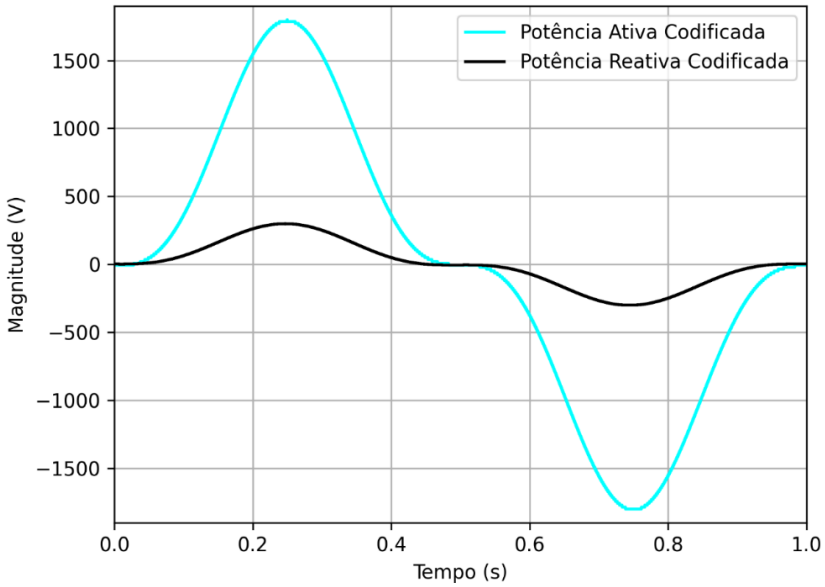
O Cenário 3 consistiu no envio de marcas d'água falsas, com o objetivo de simular uma tentativa de invasão ao sistema por parte de um agente externo. Para a determinação das marcas d'água foram utilizadas as funções de transferência representadas pelas equações (3.5) e (3.6), supondo que o invasor detinha conhecimento prévio da planta. Além disso, os níveis de referência adotados foram de 180 kW, considerando a potência ativa, e de 30 kvar, para a potência reativa. A seguir, são apresentadas as expressões dos sinais de autenticação falsos da microrrede.

$$M_{Pfalso} = 1352sen(6{,}2832t + 0{,}0013) + 448sen(18{,}8496t + 3{,}1469)$$

$$M_{Qfalso} = 223{,}77sen(9{,}4248t + 0{,}0246) + 37{,}47sen(28{,}2743t + 3{,}1652)$$

O Gráfico 10 apresenta os sinais de potência ativa e reativa recuperados pelo receptor. Como não houve degradação durante a transmissão, estes sinais reproduzem, de maneira exata, os comandos emitidos pelo agente malicioso, embora se diferenciem das marcas d'água originais armazenadas no sistema de calibração. Ressalta-se que as frequências associadas à potência ativa são iguais a 1 Hz e 3 Hz, enquanto as relacionadas à potência reativa correspondem a 1,5 Hz e 4,5 Hz.

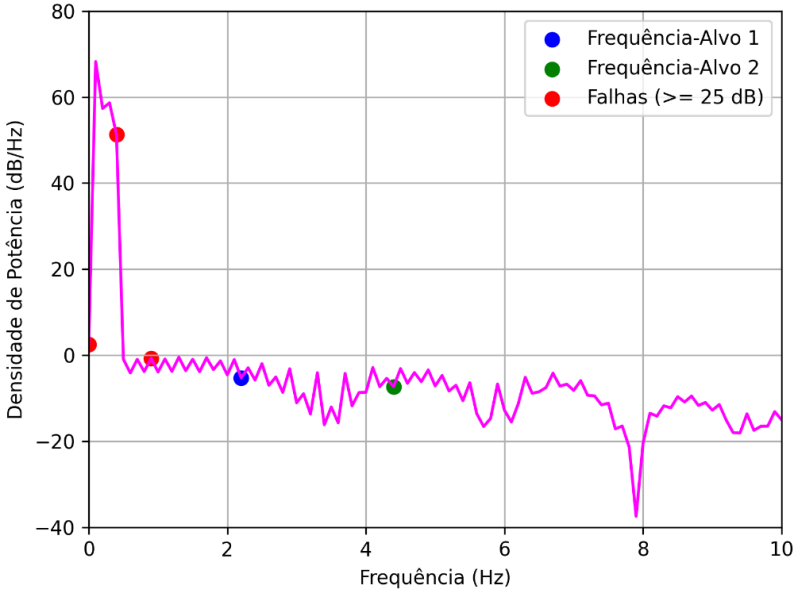
Gráfico 10 – Sinais falsos de potência ativa e reativa recuperados (Cenário 3).



Fonte: Autoria própria (2025).

Considerando a DEP da potência ativa, ilustrada no Gráfico 11, observa-se que algumas componentes espectrais ultrapassaram o limite estabelecido para validação. Os pontos vermelhos no gráfico indicam as frequências que violaram o limiar estabelecido de 25 dB, totalizando três ocorrências. Esta quantidade excedente resultou na invalidação do sinal recebido por parte do sistema de recepção, além da emissão de um alarme na rede. Além disso, as frequências-alvo do sistema, correspondentes a 2,2 Hz e 4,4 Hz, divergiram das DEP estabelecidas pelo sistema de calibração em 4,15 dB e 13,29 dB, respectivamente.

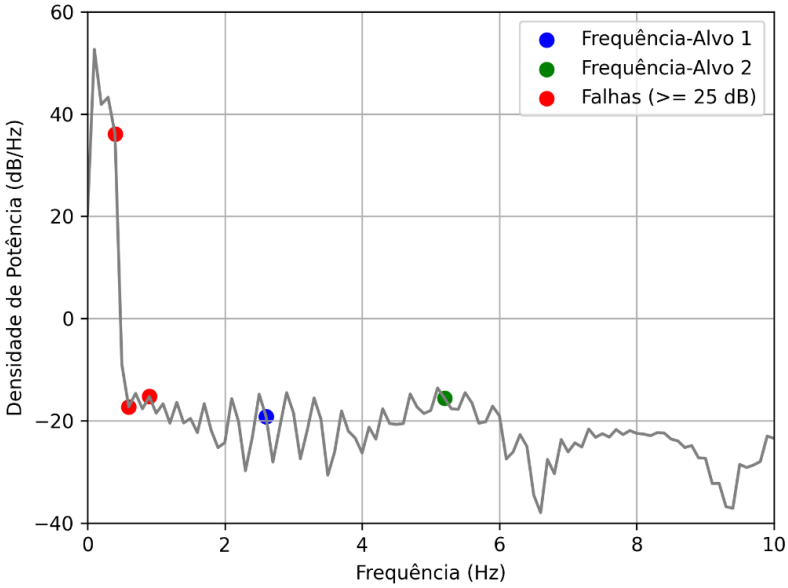
Gráfico 11 – DEP do sinal falso de potência ativa (Cenário 3).



Fonte: Autoria própria (2025).

De modo análogo, o Gráfico 12 apresenta a DEP da potência reativa. Assim como no caso anterior, diversas frequências superaram o limite estabelecido para aceitação, totalizando, também, três ocorrências. A condição de validação define que apenas uma violação é tolerada para que o sinal seja considerado legítimo e possibilite a execução da ação corretiva. Assim como no caso da potência ativa, a ação corretiva foi igualmente descartada, seguida da emissão de um alarme na rede. Ademais, as frequências-alvo do sistema, correspondentes a 2,6 Hz e 5,2 Hz, divergiram das DEP estabelecidas pelo sistema de calibração em 8,01 dB e 16,30 dB, respectivamente.

Gráfico 12 – DEP do sinal falso de potência reativa (Cenário 3).



Fonte: Autoria própria (2025).

Assim, o mecanismo de autenticação comportou-se conforme o esperado nos três cenários analisados, validando os sinais com marcas d'água legítimas e rejeitando tanto aqueles sem autenticação quanto os sinais de controle ilegítimos. Na próxima seção, serão detalhados os testes realizados em um modelo de sistema elétrico real, representado pela rede elétrica da Unifei, bem como os resultados relacionados à capacidade de detecção correta das marcas d'água em ambientes de comunicação sujeitos a ruído e atenuação.

4.2 SISTEMA UNIFEI

O sistema elétrico da Unifei foi adotado como base para os testes considerando inserção de ruído na comunicação, bem como propagação da informação em meio cabeado, objetivando simular a operação e o controle de um modelo de microrrede real. Para isso, o circuito foi

completamente modelado pelo *software* OpenDSS, que permite representar, de maneira satisfatória, todos os seus elementos, incluindo cargas, alimentadores, transformadores e demais componentes. Tal implementação resultou em um ambiente adequado para a simulação do envio de sinais de controle codificados com marcas d'água aditivas, além de possibilitar a análise da eficácia do mecanismo de detecção e validação da autenticidade destes sinais sob variadas condições de propagação do canal de comunicação.

Os sistemas de monitoramento e de comunicação da microrrede foram inteiramente modelados em Python, o qual integra, por meio de múltiplas classes, as funcionalidades de aquisição de dados operacionais, bem como de transmissão de sinais de supervisão e controle. Desta forma, é possível realizar o registro das grandezas elétricas em pontos específicos do circuito, além simular o envio destas informações em uma rede de comunicação. Dois ambientes distintos de propagação foram utilizados para os testes com o sistema da Unifei: um canal de comunicação sem protocolo modelado, sujeito exclusivamente à presença de ruído AWGN, e outro baseado em uma implementação simplificada da tecnologia Ethernet, representando a transmissão da informação em meio cabeado.

As barras analisadas foram a 114, correspondente ao Restaurante Universitário (RU), e a 562, localizada no Laboratório de Alta Tensão (LAT). A barra 114 está conectada ao Alimentador 1 e posicionada a 90 metros do Centro de Controle, situado no Bloco I, cujo fornecimento elétrico provém do Alimentador 3. Por sua vez, a barra 562 pertence ao Alimentador 5 e encontra-se a uma distância de 180 metros desse mesmo ponto de controle. Tal configuração topológica permite investigar a influência da distância física na detecção e validação correta das marcas d'água inseridas nos sinais transmitidos.

Para cada uma das barras foram inseridas oito violações em seus perfis de carga, as quais distribuem-se ao longo de um período simulado de 24 horas, dividido em 96 intervalos de 15 minutos. No caso da barra 114, tais distúrbios ocorreram entre 12h15 e 13h00, e entre 19h00 e 19h45. Para a barra 562, os eventos foram inseridos no intervalo de 14h30 a 16h15. A seguir, apresentam-se os resultados obtidos nas simulações para ambos os ambientes de comunicação, bem como suas respectivas análises.

4.2.1 *Meio de transmissão com inserção de ruído AWGN*

Considerando os testes com inserção de ruído AWGN, foram implementados dois cenários distintos, contemplando níveis de SNR[14] iguais a 15 dB e 5 dB, respectivamente. Com isso, foi possível avaliar os impactos desse tipo de degradação à comunicação, determinando as taxas de detecção e verificação corretas das marcas d'água, bem como os efeitos provocados pela distância de transmissão dos sinais.

No que se refere ao nível de ruído de 15 dB, a Tabela 10 apresenta o resultado das simulações, considerando o número de detecções e validações bem-sucedidas das marcas d'água das potências ativa e reativa, assim como suas respectivas taxas de falhas e erros percentuais, de acordo com a barra supervisionada.

Tabela 10 – Resultado das simulações com inserção de ruído (SNR = 15 dB).

Marca d'Água	Sucesso	Falha	Erro (%)
Potência Ativa – Barra 114	8	0	0
Potência Ativa – Barra 562	6	2	25
Potência Reativa – Barra 114	8	0	0
Potência Reativa – Barra 562	8	0	0

Fonte: Autoria própria.

Para este cenário, ocorreram apenas dois erros na detecção das marcas d'água, ambos relacionados ao sinal de potência ativa da barra 562 (LAT). Uma possível explicação é que essa barra está localizada mais distante do Centro de Controle em comparação à barra 114 (RU), o que a torna mais suscetível à influência do ruído na comunicação. Vale ressaltar que os efeitos da distância na comunicação foram considerados no modelo. No caso das falhas, as componentes de frequência que violaram a diferença de 25 dB foram 2,7 Hz, 3,9 Hz e 4,5 Hz na primeira ocorrência, e 2,7 Hz e 3,9 Hz, na segunda.

O segundo cenário de testes, o qual contempla um nível de ruído equivalente a 5 dB, tem os seus resultados ilustrados pela Tabela 11. Assim como no caso anterior, é possível visualizar a quantidade de detecções e validações corretas das marcas d'água, bem como a ocorrência de falhas e taxa de erros, em porcentagem.

[14] Os níveis de ruído considerados para os testes constituem valores extremos de degradação do meio de propagação, cujos patamares medidos em sistemas reais possuem intensidades menores que aqueles configurados nos cenários de simulação. Entretanto, os níveis de 15 dB e 5 dB foram utilizados para avaliar a robustez da técnica implementada, determinando também como a variação da SNR afeta a capacidade de detecção e validação das marcas d'água.

Tabela 11 – Resultado das simulações com inserção de ruído (SNR = 5 dB).

Marca d'Água	Sucesso	Falha	Erro (%)
Potência Ativa – Barra 114	8	0	0
Potência Ativa – Barra 562	5	3	37,5
Potência Reativa – Barra 114	8	0	0
Potência Reativa – Barra 562	8	0	0

Fonte: Autoria própria.

Novamente as falhas de detecção ficaram localizadas no sinal de potência ativa, sendo registrado um aumento no erro percentual de 25% para 37,5% no envio das marcas d'água. De igual modo, o fato da barra 562 estar mais distante do Centro de Controle, a torna mais exposta a degradações como, por exemplo, a influência do ruído AWGN inserido na comunicação. Além disso, uma vez que a SNR considerada sofreu um acréscimo de 10 dB, a elevação na quantidade de erros de detecção e validação apresenta coerência com a modificação implementada no canal de comunicação. Para este cenário, as frequências divergentes, em 25 dB ou mais, de seus respectivos valores de calibração foram: 0,60 Hz, 2,3 Hz e 3,3 Hz, na primeira ocorrência; 0 Hz e 3,1 Hz, na segunda; 0,6 Hz, 2,1 Hz e 5,4 Hz, no último evento de erro.

Apesar da influência da distância, o caráter aleatório do ruído pode explicar o fato da marca d'água da potência reativa não ter sido afetada por degradação, diferentemente do ocorrido com o sinal de potência ativa. Tal comportamento decorre da natureza estocástica do ruído AWGN, que pode interferir de maneiras distintas em sinais com características similares, atingindo qualquer uma das componentes do espectro de frequências (Hong; Huang; Kuo, 2010).

Além disso, é importante ressaltar que ambas as marcas d'água de um único trecho são autenticadas de forma conjunta. Ou seja, para sinais de mesmo *timestamp*, a invalidação de um deles, automaticamente implica no descarte de toda a ação corretiva para aquele instante. Sendo assim, as falhas ocorridas na barra 562 em ambos os testes, constituem um erro global na atuação de controle de 25% e 37,5%, considerando os níveis de ruído de 15 dB e 5 dB, respectivamente.

4.2.2 *Protocolo de transmissão Ethernet*

Para os testes simulando o envio das informações em meio cabeado, foram configurados dois cenários distintos, considerando graus de atenuação[15] equivalentes a 30 dB/km e 60 dB/km,

[15] Os graus de atenuação adotados para os cenários que simulam a transmissão em meio cabeado são hipotéticos, configurando valores muito acima dos encontrados em ambientes de comunicação reais. No entanto, tais patamares foram adotados, uma vez que o objetivo dos testes é tão somente avaliar a robustez do sinal

respectivamente. O nível de ruído inserido em relação ao sinal de interesse foi de 30 dB e a taxa de transmissão entre os pontos de comunicação iguais a 10 Mbps. Assim, foi possível avaliar os impactos desse tipo de degradação no número de detecções e validações bem-sucedidas do sistema receptor, além da influência da distância na qualidade da rede de comunicação.

Considerando o grau de atenuação igual a 30 dB/km, a Tabela 12 apresenta o resultado das simulações, levando em conta o número de detecções e validações bem-sucedidas das marcas d'água das potências ativa e reativa, assim como suas respectivas taxas de falhas e erros percentuais, de acordo com a barra monitorada.

Tabela 12 – Resultado das simulações em meio cabeado com atenuação (α = 30 dB/km).

Marca d'Água	Sucesso	Falha	Erro (%)
Potência Ativa – Barra 114	8	0	0
Potência Ativa – Barra 562	7	1	12,5
Potência Reativa – Barra 114	7	1	12,5
Potência Reativa – Barra 562	8	0	0

Fonte: Autoria própria.

Neste cenário, dois erros de detecção foram registrados: um deles ocorreu no sinal de potência ativa da barra 562 (LAT); o outro é referente à marca d'água da potência reativa da barra 114 (RU). A atenuação total do trecho entre o Centro de Controle e o LAT é igual a 5,4 dB, a qual corresponde a, aproximadamente, o dobro do valor determinado para o percurso entre o Centro de Controle e o RU, calculado em 2,7 dB. Entretanto, o efeito deste tipo de degradação, somado ao ruído de 30 dB, para ambos os pontos de monitoramento foram iguais. Isso pode ser explicado pela regeneração do sinal destinado à barra 562 após 100 metros, o que, provavelmente, evitou uma maior incidência de falhas na detecção. Para este cenário, as frequências divergentes, em 25 dB ou mais, de seus respectivos valores de calibração foram: 2,7 Hz e 3,2 Hz, na barra 114; 0,5 Hz e 3,3 Hz, considerando a barra 562.

O segundo cenário implementado considera um nível de atenuação igual a 60 dB/km, cujos resultados são ilustrados pela Tabela 13. Assim como nas simulações anteriores, pode-se determinar o número de detecções e validações corretas das marcas d'água, além da ocorrência de falhas e taxa de erros, em valores percentuais.

Tabela 13 – Resultado das simulações em meio cabeado com atenuação (α = 60 dB/km).

Marca d'Água	Sucesso	Falha	Erro (%)
Potência Ativa – Barra 114	7	1	12,5
Potência Ativa – Barra 562	7	1	12,5
Potência Reativa – Barra 114	8	0	0
Potência Reativa – Barra 562	7	1	12,5

Fonte: Autoria própria.

codificado quando submetido a esse tipo de degradação, além de verificar como a variação desse parâmetro afeta a capacidade de detecção correta das marcas d'água.

Os testes realizados com atenuação de 60 dB/km, apresentaram uma falha adicional para o sinal de potência reativa da barra 562. Entretanto, o número de erros considerando os sinais da barra 114 permaneceu o mesmo, ocorrendo uma mudança entre as marcas d'água das potências ativa e reativa. Este aumento é condizente com o acréscimo no grau de atenuação da rede de comunicação, indicando que o declínio na qualidade do meio de propagação afetou diretamente a capacidade de detecção e validação das marcas d'água por parte do sistema de recepção. No que se refere ao fenômeno ocorrido no trecho do RU, uma explicação possível para tal comportamento é que o meio não é totalmente isento de ruído. Assim, devido a seu efeito aleatório, a soma de suas amplitudes com as do sinal de interesse podem ter influenciado na detecção e validação final das marcas d'água. As frequências divergentes para este cenário de simulação foram: 0,7 Hz e 1,4 Hz, na barra 114; 0 Hz e 5,8 Hz, considerando o sinal de potência ativa do LAT; 3,6 Hz e 4,3 Hz, para a potência reativa do LAT.

Destaca-se também o fato de que cada uma das ocorrências de erro foram contabilizadas em instantes diferentes. Assim, uma vez que marcas d'água de mesmo *timestamp* são validadas em conjunto, para o primeiro cenário, o erro global de ambas as barras foi de 12,5%. Já no cenário de maior degradação, o erro global da barra 114 permaneceu igual, ao passo que para o trecho do LAT, este subiu para 25%.

4.3 DESEMPENHO DO SISTEMA DE RECEPÇÃO

Como métricas de desempenho do sistema de detecção e validação das marcas d'água, consideraram-se a latência adicional introduzida no processo de efetivação da ação corretiva, executada localmente nos elementos monitorados da microrrede, e o aumento no consumo energético decorrente do processamento realizado pelo *software* instalado nas barras supervisionadas. Desta forma, foi possível avaliar a performance do sistema com relação aos requisitos necessários para determinadas aplicações em redes inteligentes, bem como ao impacto na autonomia, em caso de utilização de dispositivos IoT alimentados por bateria.

4.3.1 *Introdução de latência*

Considerando a latência adicional introduzida pelo sistema receptor, o tempo médio de processamento necessário para a detecção e validação de ambas as marcas d'água foi de 37 milissegundos. Esse valor demonstra compatibilidade com a maioria das aplicações previstas

em redes inteligentes, cujos requisitos temporais são detalhados no Quadro 4, além de suas respectivas classificações quanto à segurança e confiabilidade.

Quadro 4 – Requisitos de comunicação para aplicações de redes inteligentes.

Aplicação	**Latência máxima**	**Confiabilidade**	**Segurança**
Medição Inteligente	Até 10 segundos	Média	Alta
Resposta à Demanda	1 segundo	Alta	Alta
Conexão e Desconexão	Alguns minutos	Alta	Alta
Comunicação em Subestações	20 milissegundos	Alta	Alta
Supervisory Control and Data Acquisition (SCADA)	Até 200 milissegundos	Alta	Alta
Gerenciamento de Microrredes	1 minuto	Alta	Alta
Otimização da Operação	100 milissegundos	Alta	Alta
Localização, Isolação e Restauração de Faltas	100 milissegundos	Alta	Alta
Vigilância por Vídeo	Alguns segundos	Alta	Alta

Fonte: (Kabalci; Kabalci, 2019).

Com relação aos requisitos expostos pela tabela anterior, constata-se que, para aplicações como controle e ajuste de potências ativa e reativa em SEP, a metodologia proposta é compatível, uma vez que os atrasos máximos admissíveis para esse tipo de operação são da ordem de 100 milissegundos. Em contrapartida, em contextos mais exigentes, como a troca de informações e o envio de comandos em subestações, os requisitos de latência são, obrigatoriamente, inferiores a 20 milissegundos. Nestas condições, o sistema receptor implementado torna-se inadequado para tal.

Ressalta-se ainda que, com exceção da aplicação de Medição Inteligente, cuja robustez de comunicação exigida é considerada média, todas as demais demandam um elevado grau de confiabilidade, a fim de que seja assegurado o bom funcionamento da microrrede. No que se refere à segurança, tal requisito se mostra fundamental em todas as aplicações de redes inteligentes, reforçando a necessidade da implementação de mecanismos que garantam o seu cumprimento de acordo com os patamares estabelecidos.

4.3.2 *Consumo energético adicional*

Para a realização dos testes de consumo energético do mecanismo receptor, foi utilizado um equipamento com sistema Windows® 11 Home Single Language (versão 24H2), equipado

com um processador Intel® Core™ i5-1135G7 de 11ª geração, operando a 1,38 GHz. A fim de garantir que os resultados refletissem apenas o funcionamento da rotina de detecção, todos os processos não essenciais do sistema operacional foram previamente desabilitados.

O mecanismo de detecção desenvolvido gerou um acréscimo de apenas 1,78% na carga de processamento local, resultando em um consumo energético adicional de 9 µWh por acionamento. Assim, considerando uma ativação por hora, o consumo diário estimado é de 216 µWh, totalizando 78,84 mWh ao longo de um ano. Com base em uma bateria hipotética de 1 Wh de capacidade, pode-se estimar a autonomia do sistema sem necessidade de substituição ou recarga. A razão entre a energia disponível e o consumo diário fornece:

$$\frac{1\ Wh}{0{,}07884\ Wh/ano} \approx 12{,}68\ anos$$

Portanto, considerando uma estimativa de autonomia de 12,68 anos, o mecanismo receptor apresenta baixa demanda energética, o que o torna compatível com os requisitos básicos para dispositivos IoT, que frequentemente exigem funcionamento contínuo por mais de uma década sem substituição ou recarga da bateria (Goudos *et al.*, 2019).

Durante a elaboração das simulações, algumas limitações significativas foram identificadas, especialmente no que diz respeito à modelagem do sistema elétrico no ambiente OpenDSS. Embora esta ferramenta seja amplamente utilizada para simulações em sistemas de distribuição, ela não contempla, de maneira exata, todas as particularidades da microrrede da Unifei, como as características dinâmicas específicas dos elementos do circuito, dentre outros aspectos. Além disso, algumas simplificações adotadas na definição dos componentes, das cargas e da demanda energética diária, acabam por comprometer a precisão dos resultados obtidos.

No que se refere ao sistema de comunicação, foram observadas limitações importantes que influenciam diretamente na exatidão dos dados aferidos. O modelo desenvolvido considera apenas uma representação simplificada do ruído, não levando em consideração aspectos como interferência eletromagnética, reflexões no meio físico ou perdas por dispersão. Além disso, o meio cabeado foi representado de maneira genérica, sem incluir a modelagem específica da tecnologia Ethernet, a latência induzida por protocolo, controle de congestionamento, além de fatores como *jitter*, perdas de pacotes e oscilações da taxa de transmissão, cujos efeitos poderiam inviabilizar a implementação da técnica. Outro aspecto restritivo diz respeito à estimativa de consumo energético, baseada em medições indiretas feitas no computador no qual os testes foram realizados, com os demais processos do sistema operacional desativados, o que

não representa a operação de dispositivos reais conectados à rede. Por fim, a utilização de uma bateria hipotética, em substituição a uma célula física com comportamento real, limita a capacidade de avaliação do desempenho energético em regime de operação.

CAPÍTULO 5 – CONCLUSÃO

O presente trabalho abordou a análise da segurança cibernética frente aos *replay attacks*, utilizando, para este fim, marcas d'água aditivas como mecanismo de prevenção e detecção contra esse tipo de investida. Inicialmente, foi apresentada a estrutura das redes inteligentes e microrredes, dando ênfase às suas principais subdivisões. A primeira delas refere-se à arquitetura dos sistemas elétricos de potência, na qual são destacados seus principais elementos constituintes, além das entidades responsáveis pelo controle e operação destes sistemas elétricos.

Os resultados obtidos mostram que o modelo de testes implementado permitiu a verificação do desempenho do sistema de comunicação, bem como do processo de autenticação dos sinais de controle da microrrede, tanto no que se refere à validação da metodologia proposta quanto à resposta dos sinais transmitidos diante da inserção de ruído AWGN e da atenuação imposta pelo meio de propagação. Adicionalmente, foi possível avaliar o consumo de energia e as latências adicionais introduzidas na transmissão em função da atuação do mecanismo de detecção das marcas d'água. Contudo, vale ressaltar que tais estimativas foram alcançadas com base em modelos representativos simplificados, tanto do sistema de controle da microrrede quanto das tecnologias de comunicação utilizadas nas simulações.

No que se refere aos testes de validação realizados com o sistema IEEE 13 Barras, estes indicaram comportamento consistente com a metodologia de detecção e validação de marcas d'água implementada. O sistema autenticou com êxito apenas os sinais legítimos, os quais apresentaram correlação com os valores da DEP registrados pelo sistema de calibração, utilizado como referência na tomada de decisão do receptor. Sinais sem marca d'água, bem como comandos com assinaturas ilegítimas, foram corretamente descartados.

Quanto aos testes realizados com o modelo da microrrede da Unifei, foi possível determinar a influência, tanto do ruído AWGN, quanto da atenuação no desempenho do sistema de detecção. Verificou-se que a intensificação da degradação do sistema, associada a cada parâmetro analisado, contribuiu para a ocorrência de erros nos processos de detecção e validação das marcas d'água. Observou-se, também, que o ruído pode comprometer sinais de maneira diferenciada, mesmo que estes apresentem perfis semelhantes, atingindo quaisquer componentes de seus espectros de frequência devido à sua natureza aleatória.

Com relação à latência e ao consumo energético introduzidos pelo processo de detecção e validação, observou-se impacto adicional mínimo. Dessa forma, a metodologia proposta

mostrou-se adequada para grande parte das aplicações de operação e controle em redes inteligentes e microrredes. Além disso, apresentou compatibilidade com dispositivos IoT, os quais exigem, entre outros requisitos, elevada eficiência energética, com expectativa de operação contínua por até dez anos sem substituição ou recarga da bateria.

Conclui-se, portanto, que a metodologia desenvolvida foi eficaz na avaliação do desempenho de marcas d'água aditivas em ambientes afetados por ruído e atenuação, demonstrando também sua capacidade de detecção por meio da análise da DEP. Essa avaliação foi viabilizada por um sistema de calibração adaptativo, ajustado tanto ao perfil específico da marca d'água quanto às particularidades do meio de comunicação da microrrede. Como trabalhos futuros, recomenda-se a implementação do sistema em microrredes reais, além da modelagem detalhada de outros cenários de propagação e a análise com diferentes tipos de marcas d'água. Sugere-se também a aplicação dos filtros de Kalman na detecção e validação dos sinais codificados, a simulação de outras modalidades de ataques cibernéticos e o estudo do controle de outras grandezas elétricas, como os níveis de tensão e corrente.

REFERÊNCIAS

ABRAHAMSEN, Fredrik Ege; AI, Yun; CHEFFENA, Michael. Communication technologies for smart grid: a comprehensive survey. *Sensors*, Basel, v. 21, n. 23, p. 1–31, 2021.

ADLER, Robertson. *Learn Internet of Things (IoT)*. Wembley, Middlesex, Reino Unido: A G Printing & Publishing Ltd., 2023.

AGHA, Al Khaldoun; LOYGUE, Pauline; PUJOLLE, Guy. *Edge Networking: Internet of Edges*. Hoboken, NJ: Wiley-ISTE, 2022.

AHMED, Chuadhry Mujeeb; PALLETI, Venkata Reddy; MISHRA, Vishrut Kumar. A practical physical watermarking approach to detect replay attacks in a CPS. *Journal of Process Control*, v. 116, p. 136–146, ago. 2022.

AKUJUOBI, Cajetan M.; SADIKU, Matthew N. O. *Introduction to Broadband Communication Systems*. 1. ed. Boca Raton, FL: Chapman and Hall/CRC, 2007.

ALI, Saqib *et al*. *Cyber Security for Cyber Physical Systems*. Cham, Suíça: Springer International Publishing, 2018.

ALTIN, Necmi; EYIMAYA, Süleyman Emre. Advancements in DC Microgrids: Integrating Machine Learning and Communication Technologies for a Decentralized Future. In: APPASANI, Bhargav; BIZON, Nicu (org.). *Smart Grid 3.0: Computational and Communication Technologies*. Cham, Suíça: Springer International Publishing, 2023. p. 357–387.

ANDREI, Horia *et al*. Microgrid Protection. In: KABALCI, Ersan; MAHDAVI TABATABAEI, Naser; BIZON, Nicu (orgs.). *Microgrid Architectures, Control and Protection Methods*. Cham, Suíça: Springer International Publishing, 2020. p. 605–630.

ANEEL. *Resolução Normativa nº 964*, de 14 de dezembro de 2021. Brasil. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-normativa-aneel-n-964-de-14-de-dezembro-%20de-2021-369359262. Acesso em: 5 jun. 2023.

ATARASHI, Hiroyuki *et al*. 5G Targets and Standardization. In: TOSKALA, Antti; HOLMA, Harri; NAKAMURA, Takehiro (orgs.). *5G Technology 3GPP New Radio*. Hoboken, NJ, EUA: Wiley, 2020. p. 13–26.

AURANGZEB, Muhammad *et al*. Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy preserving storage. *Energy Reports*, v. 11, p. 2493–2515, jun. 2024.

AYELE, Eyuel Debebe; GONZALEZ, Javier Ferreira; TEEUW, Wouter B. Enhancing Cybersecurity in Distributed Microgrids: A Review of Communication Protocols and Standards. *Sensors*, v. 24, n. 3, p. 854, 28 jan. 2024.

BAELDUNG. *What are replay attacks?*. Disponível em: https://www.baeldung.com/cs/replay-attacks. Acesso em: 28 jun. 2024.

BANI-MEQDAD, Mohammad *et al*. Cyber-environment in the human rights system: modern challenges to protect intellectual property law and ensure sustainable development of the region. *International Journal of Sustainable Development & Planning*, v. 19, n. 4, p. 1389–1396, abr. 2024.

BANOTH, Rajkumar; REGAR, Rekha. *Classical and modern cryptography for beginners*. Cham, Suíça: Springer Nature Switzerland, 2023.

BASHIR, Imran. *Mastering blockchain – Third edition: a deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more*. 3. ed. Birmingham, UK: Packt Publishing, 2020.

BEGOVIC, Miroslav M. Power system protection. In: GRIGSBY, Leonard L. (org.). *Power system stability and control*. 3. ed. Boca Raton, FL, EUA: CRC Press, 2012. p. 1–10.

BELU, Radian. *Smart grid fundamentals*. Boca Raton, FL, EUA: CRC Press, 2022.

BERTÉNYI, Tamás. Intelligent small-scale decentralised energy systems. In: GRIMM, Christoph; NEUMANN, Peter; MAHLKNECHT, Stefan (orgs.). *Embedded systems for smart appliances and energy management*. Nova Iorque, NY, EUA: Springer, 2012. p. 23–40.

BOLLEN, Math H. J. *The smart grid: adapting the power system to new challenges*. San Francisco, CA, EUA: Morgan & Claypool Publishers, 2011.

BRAGA, Newton C. *Instrumentação – osciloscópio*. São Paulo: Editora NCB, 2019.

BROOKS, Charles J.; JUNIOR, Phillip A. Craig. *Practical industrial cybersecurity: ICS, Industry 4.0, and IIoT*. Hoboken, NJ, EUA: Wiley, 2022.

BUSBY, Joshua W. *et al*. Cascading risks: understanding the 2021 winter blackout in Texas. *Energy Research & Social Science*, v. 77, p. 102106, jul. 2021.

BUSO, Simone; MATTAVELLI, Paolo. *Digital control in power electronics*. 2. ed. Cham, Suíça: Springer International Publishing, 2022.

BUTUN, Ismail; SARI, Alparslan. Early detection and recovery measures for smart grid cyber-resilience. In: BUTUN, Ismail (org.). *Decision support systems and industrial IoT in smart grid, factories, and cities*. Hershey, PA, EUA: IGI Global, 2021. p. 91–110.

CALLEJA, Alejandro; TAPIADOR, Juan; CABALLERO, Juan. The MalSource Dataset: quantifying complexity and code reuse in malware development. *IEEE Transactions on Information Forensics and Security*, v. 14, n. 12, p. 3175–3190, dez. 2019.

CANAAN, Bushra; COLICCHIO, Bruno; OULD ABDESLAM, Djaffar. Microgrid cyber-security: review and challenges toward resilience. *Applied Sciences*, v. 10, n. 16, p. 5649, 14 ago. 2020.

CENTER FOR STRATEGIC & INTERNATIONAL STUDIES. *Significant cyber incidents since 2006*. Disponível em: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Acesso em: 23 maio 2024.

CHABUKSWAR, Rohan; MO, Yilin; SINOPOLI, Bruno. Detecting integrity attacks on SCADA systems. *IFAC Proceedings Volumes*, v. 44, n. 1, p. 11239–11244, jan. 2011.

CHERUVU, Sunil *et al*. *Demystifying Internet of Things security: successful IoT device/edge and platform security deployment*. 1. ed. New York, NY, EUA: Apress, 2019.

CLP. *Smart grid: what is a smart grid*. Disponível em: https://www.clp.com.hk/en/about-clp/power-transmission-distribution/smart-grid. Acesso em: 7 jul. 2023.

COMER, Douglas E. *Redes de computadores e Internet*. 6. ed. Porto Alegre, RS, Brasil: Bookman Editora, 2016.

CORINTHIOS, Michael. *Signals, systems, transforms, and digital signal processing with MATLAB*. Boca Raton, FL, EUA: CRC Press, 2018.

DALELA, Shruti; DALELA, Mrs. Preeti. *Cyber security & digital awareness*. Birmingham, Reino Unido: Shruti Dalela, 2023.

DANTURTHI, Sarma R. *Database and application security: a practitioner's guide*. Boston, MA, EUA: Addison-Wesley Professional, 2024.

DAZA, Eric Fernando Boeck; SPERANDIO, Maurício. *Sistemas de armazenamento de energia: desafios regulatórios e econômicos para sua inserção em sistemas elétricos de potência*. São Paulo, SP, Brasil: Simplíssimo, 2019.

DE ANDRADE, Flávia; CASTILLA, Miguel; BONATTO, Benedito Donizeti. *Basic tutorial on simulation of microgrids control using MATLAB® & Simulink® software*. Cham, Suíça: Springer International Publishing, 2020.

DELBONI, Luiz F. N. *et al*. Electrical power systems: evolution from traditional configuration to distributed generation and microgrids. In: ZAMBRONI DE SOUZA, Antonio Carlos; CASTILLA, Miguel (orgs.). *Microgrids design and implementation*. Cham, Suíça: Springer International Publishing, 2018. p. 1–25.

DOCTER, Quentin; BUHAGIAR, Jon. *CompTIA A+ complete study guide: Core 1 Exam 220-1101 and Core 2 Exam 220-1102*. 5. ed. Indianapolis, IN, EUA: Pearson IT Certification, 2022.

DONG, Chaoyu *et al*. DC microgrid stability analysis considering time delay in the distributed control. *Energy Procedia*, v. 142, p. 2126–2131, dez. 2017.

DU, Dajun *et al*. A review on cybersecurity analysis, attack detection, and attack defense methods in cyber physical power systems. *Journal of Modern Power Systems and Clean Energy*, v. 11, n. 3, p. 727–743, 2023a.

DU, Dajun *et al*. Attack detection for networked control systems using event triggered dynamic watermarking. *IEEE Transactions on Industrial Informatics*, v. 19, n. 1, p. 351–361, jan. 2023b.

DU, Pengwei; LU, Ning; ZHONG, Haiwang. *Demand response in smart grids*. 1. ed. Cham, Suíça: Springer, 2020.

DULANEY, Emmett. *CompTIA Network+ N10-007 Exam Cram*. Indianapolis, IN, EUA: Pearson IT Certification, 2017.

DUNN CAVELTY, Myriam. *The politics of cyber security*. Nova York, NY, EUA: Routledge, 2024.

DUO, Wenli; ZHOU, MengChu; ABUSORRAH, Abdullah. A survey of cyber attacks on cyber physical systems: recent advances and challenges. *IEEE/CAA Journal of Automatica Sinica*, v. 9, n. 5, p. 784–800, maio 2022.

EASTTOM II, William. *Network defense and countermeasures: principles and practices*. Indianapolis, IN, EUA: Pearson IT Certification, 2023.

EBRARY.NET. *Harmonics in the microgrid and EV charging system*. Disponível em: https://ebrary.net/54783/computer_science/harmonics_microgrid_charging_system. Acesso em: 9 jul. 2023.

EKANAYAKE, J. B. *et al*. *Smart grid: technology and applications*. Hoboken, NJ, EUA: Wiley, 2012.

EPE – EMPRESA DE PESQUISA ENERGÉTICA. *Inserção de novas tecnologias: 1º relatório diagnóstico*. Rio de Janeiro: EPE, 2022.

FADLULLAH, Zubair Md.; KATO, Nei. *Evolution of smart grids*. Cham, Suíça: Springer, 2014.

FELDMAN, Joshua; MISENAR, Seth; CONRAD, Eric. *CISSP® study guide*. Burlington, MA, EUA: Elsevier Science, 2023.

FERRARI, Riccardo M. G.; TEIXEIRA, Andre M. H. A switching multiplicative watermarking scheme for detection of stealthy cyber attacks. *IEEE Transactions on Automatic Control*, v. 66, n. 6, p. 2558–2573, jun. 2021.

FOWLER, Richard. *Fundamentos de eletricidade: corrente alternada e instrumentos de medição*. 7. ed., v. 2. São Paulo, SP, Brasil: McGraw Hill Brasil, 2013.

FOX, Richard; HAO, Wei. *Internet infrastructure: networking, web services, and cloud computing*. Boca Raton, FL, EUA: CRC Press, 2017.

FRACCAROLLI, Enrico; QUAGLIA, Davide. Engineering IoT networks. In: FIROUZI, Farshad; CHAKRABARTY, Krishnendu; NASSIF, Sani (orgs.). *Intelligent Internet of Things: from device to fog and cloud*. Cham, Suíça: Springer, 1. ed., 2020. p. 97–172.

FUSHENG, Li; RUISHENG, Li; FENGQUAN, Zhou. *Microgrid technology and engineering application*. Amsterdam, Países Baixos: Elsevier, 1. ed., 2015.

GHAMARILANGROUDI, Azam. *Detection of replay attack in control systems using multi sine watermarking*. 2020. Dissertação (Mestrado) – Concordia University, Montreal, QC, Canadá, 18 mar. 2020.

GHORPADE, Sheetal N.; ZENNARO, Marco; CHAUDHARI, Bharat S. *Optimal localization of Internet of Things nodes*. Cham, Suíça: Springer, 2021.

GHOSH, Arindam; ZARE, Firuz. *Control of power electronic converters with microgrid applications*. Hoboken, NJ, EUA: Wiley, 2022.

GIMENES, André Luiz Veiga *et al*. *Armazenamento de energia: abordagens sistemáticas referentes aos sistemas elétricos de potência*. Jundiaí, SP, Brasil: Paco Editorial, 2020.

GOUDOS, Sotirios K. *et al*. Communication protocols for the IoT based smart grid. In: ANAGNOSTOS, Dimitrios *et al*. (orgs.). *IoT for smart grids: design challenges and paradigms*. Cham, Suíça: Springer International Publishing, 2019. p. 55–83.

GU, Fei *et al*. Survey of the low power wide area network technologies. *Journal of Network and Computer Applications*, v. 149, p. 102459, jan. 2020.

HAHN, Jeffrey L. Cybersecurity for the smart grid. In: BORLASE, Stuart (org.). *Smart grids: advanced technologies and solutions*. 2. ed. Boca Raton, FL, EUA: CRC Press, 2017.

HAQUE, Ahteshamul *et al*. Centralized intelligent fault localization approach for renewable energy based islanded microgrid systems. In: SHAW, Rabindra Nath *et al*. (orgs.). *Applications of AI and IoT in renewable energy*. Amsterdam, Países Baixos: Elsevier, 2022. p. 129–149.

HARRIS, Frederic J. Multirate FIR filters for interpolating and desampling. In: ELLIOT, Douglas F. (org.). *Handbook of Digital Signal Processing: Engineering Applications*. San Diego, CA, EUA: Academic Press, 1987, p. 173–287.

HESPANHOL, Pedro *et al*. Dynamic watermarking for general LTI systems. In: *Anais IEEE*, dez. 2017.

HO, Quang Dung *et al*. *Wireless communications networks for the smart grid*. Cham, Suíça: Springer, 2014.

HODGES, Duncan; CREESE, Sadie. Understanding cyber attacks. In: GREEN, James A. (org.). *Cyber warfare: a multidisciplinary analysis*. Abingdon, Reino Unido: Taylor & Francis, 1. ed., 2015. p. 33–60.

HOEHN, Andreas; ZHANG, Ping. Detection of replay attacks in cyber physical systems. In: *Anais IEEE*, jul. 2016.

HOLMA, Harri *et al*. Introduction. In: HOLMA, Harri; TOSKALA, Antti; NAKAMURA, Takehiro (orgs.). *5G technology: 3GPP New Radio*. Hoboken, NJ, EUA: Wiley, 1. ed., 2019. p. 1–12.

HONG, Y. W. Peter; HUANG, Wan Jen; KUO, C. C. Jay. *Cooperative communications and networking*. Boston, MA, EUA: Springer US, 2010.

HU, Junyan; LANZON, Alexander. Distributed finite time consensus control for heterogeneous battery energy storage systems in droop controlled microgrids. *IEEE Transactions on Smart Grid*, v. 10, n. 5, p. 4751–4761, set. 2019.

IEEE. *IEEE guide for control and automation installations applied to the electric power infrastructure*. Nova York, NY, EUA: IEEE Standards Association, 2017.

IEEE. *IEEE PES Test Feeder*. Disponível em: https://cmte.ieee.org/pes-testfeeders/resources/. Acesso em: 23 set. 2024.

ITURRA, Rodrigo Guzman; THIEMANN, Peter. Design of current controllers for three phase voltage PWM converters for different modulation methods. In: PINTO, José Gabriel; AFONSO, João L.; MONTEIRO, Vitor (orgs.). *Sustainable energy for smart cities*. Cham, Suíça: Springer International Publishing, 2021. p. 3–14.

JESZENSKY, Paul Jean Etienne. *Sistemas telefônicos*. 1. ed. Barueri, SP, Brasil: Manole, 2004.

JWO, Dah Jing; CHANG, Wei Yeh; WU, I. Hua. Windowing techniques, the Welch method for improvement of power spectrum estimation. *Computers, Materials & Continua*, v. 67, n. 3, p. 3983–4003, 2021.

KABALCI, Ersan; KABALCI, Yasin. *From smart grid to Internet of Energy*. Burlington, MA, EUA: Elsevier Science, 2019.

KALIDOSS, R.; BHAGYAVENI, M. A.; VISHVAKSENAN, K. S. *Cognitive radio – an enabler for Internet of Things*. Hershey, PA, EUA: River Publishers, 2022.

KHAZRAEI, Amir; KEBRIAEI, Hamed; SALMASI, Farzad Rajaei. Replay attack detection in a multi agent system using stability analysis and loss effective watermarking. In: *American Control Conference (ACC)*, 2017, Seattle, WA, EUA. *Anais...* p. 4778–4783, maio 2017.

KIRSCHEN, Daniel S. *Power systems: fundamental concepts and the transition to sustainability*. Hoboken, NJ, EUA: Wiley, 2024.

KIZZA, Joseph Migga. *Guide to computer network security*. Cham, Suíça: Springer International Publishing, 2024.

KUMAR, M. V. Manoj *et al*. Foundation of malware analysis and detection. In: KUMAR, M. V. Manoj *et al*. (orgs.). *Malware analysis and intrusion detection in cyber physical systems*. Hershey, PA, EUA: IGI Global, 2023. p. 22–41.

KUMARI, Dr. G. Vimala *et al*. *Embedded systems and IoT: a theoretical approach*. Chennai, Índia: GCS Publishers, 2022.

KUO, Sen M.; LEE, Bob H.; TIAN, Wenshun. *Real-time digital signal processing: implementations and applications*. 2. ed. Chichester: John Wiley & Sons, 2006.

LAU, John H. *Semiconductor advanced packaging*. Singapore: Springer Nature Singapore, 2021.

LAUFENBERG, Daniel *et al*. Developing a blockchain enabled collaborative intrusion detection system: an exploratory study. In: ARAI, Kohei; BHATIA, Rahul; KAPOOR, Supriya (orgs.). *Advances in information and communication*. Cham, Suíça: Springer International Publishing, 2020. p. 172–183.

LI, Fusheng; LI, Ruisheng; FENGQUAN, Zhou. *Microgrid technology and engineering application*. Amsterdam, Países Baixos: Academic Press, 2015.

LI, Mike Peng. *Jitter, noise, and signal integrity at high speed*. Boston, MA, EUA: Pearson Education, 2007.

LI, Sijia *et al*. Hierarchical control for microgrids: a survey on classical and machine learning based methods. *Sustainability*, v. 15, n. 11, p. 8952, 1 jun. 2023.

LI, Yan. *Cyber physical microgrids*. Cham, Suíça: Springer International Publishing, 2022.

LI, Yunwei Ryan; NEJABATKHAH, Farzam; TIAN, Hao. *Smart hybrid AC/DC microgrids: power management, energy management, and power quality control*. Hoboken, NJ, EUA: Wiley, 2022.

LIMA, Eduardo de Oliveira. *Uma avaliação do cenário da gestão de riscos cibernéticos no setor elétrico brasileiro sob a ótica da rotina operacional do ONS RO CB.BR.01*. 2022. Dissertação (Mestrado em Engenharia Elétrica) – Universidade de Brasília, Brasília, DF, Brasil, 25 nov. 2022.

LIN, Xingqin; LEE, Namyoon. Introduction to 5G and beyond. In: LEE, Namyoon; LIN, Xingqin (orgs.). *5G and beyond: fundamentals*. Cham, Suíça: Springer International Publishing, 2021. p. 1–25.

LIU, Hanxiao; MO, Yilin; JOHANSSON, Karl Henrik. Active detection against replay attack: a survey on watermark design for cyber-physical systems. In: FERRARI, Riccardo M. G.; TEIXEIRA, André M. H. (orgs.). *Safety, security and privacy for cyber-physical systems*. Cham, Suíça: Springer International Publishing, 2021. p. 145–172.

LIU, Yixin *et al*. Application of optimization techniques in the design and operation of microgrids. In: RAHMANI-ANDEBILI, Mehdi (org.). *Design, control, and operation of microgrids in smart grids*. Cham, Suíça: Springer, 2021. p. 49–83.

LUMKES, John H. Jr. *Control strategies for dynamic systems: design and implementation*. Boca Raton, FL, EUA: CRC Press, 2001.

MARIN, Paulo Sérgio. *Cabeamento estruturado – Série Eixos*. São Paulo, SP, Brasil: Saraiva Educação S.A., 2020.

MARPLE JR., S. Lawrence. *Digital spectral analysis*. Mineola, NY, EUA: Dover Publications, 2019.

MASSON, Émilie; BERBINEAU, Marion. *Broadband wireless communications for railway applications*. Cham, Suíça: Springer International Publishing, 2017. v. 82.

MATHWORKS®. *Periodogram*. [S.l.]: The MathWorks, Inc., [s.d.].

MILLER, Seumas; BOSSOMAIER, Terry. *Cybersecurity, ethics, and collective responsibility*. Oxford, Reino Unido: Oxford University Press, Incorporated, 2024.

MISHRA, Alok *et al*. Attributes impacting cybersecurity policy development: an evidence from seven nations. *Computers & Security*, v. 120, p. 102820, set. 2022.

MITTAL, Ayush *et al*. Microgrids, their types, and applications. In: GUERRERO, Josep M.; KANDARI, Ritu (orgs.). *Microgrids: modeling, control, and applications*. 1. ed. Cambridge, MA, EUA: Academic Press, 2021. p. 3–40.

MO, Yilin; CHABUKSWAR, Rohan; SINOPOLI, Bruno. Detecting integrity attacks on SCADA systems. *IEEE Transactions on Control Systems Technology*, v. 22, n. 4, p. 1396–1407, jul. 2014.

MO, Yilin; SINOPOLI, Bruno. Secure control against replay attacks. In: *47th Annual Allerton Conference on Communication, Control, and Computing*, Allerton House, UIUC, Illinois, EUA, 30 set.–2 out. 2009. Anais… IEEE, p. 911–918.

MO, Yilin; WEERAKKODY, Sean; SINOPOLI, Bruno. Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Systems*, v. 35, n. 1, p. 93–109, fev. 2015.

MORAIS, Douglas H. *5G NR, Wi-Fi 6, and Bluetooth LE 5: a primer on smartphone wireless technologies*. Cham, Suíça: Springer Nature Switzerland, 2023.

MUÑOZ, Jonathan *et al*. Evaluation of IEEE802.15.4g for environmental observations. *Sensors*, v. 18, n. 10, p. 3468, 15 out. 2018.

NADUVATH, Avinash. *In zero trust we trust*. Boston, MA, EUA: Pearson Education, 2024.

NAGGI, Rohan; SALES, Ferdinand. *Journey into the world of SASE*. Palo Alto, CA, EUA: VMware, 2021.

NAHA, Arunava *et al*. Sequential detection of replay attacks. *IEEE Transactions on Automatic Control*, v. 68, n. 3, p. 1941–1948, mar. 2023.

NASCIMENTO, Bruno de Nadai; LORENCI, Eliane de; MINAMI, Joseph Schumann. A necessidade de modernização da rede elétrica. In: ZAMBRONI DE SOUZA, Antônio Carlos; BONATTO, Benedito Donizetti; RIBEIRO, Paulo Fernando (orgs.). *Integração de renováveis e redes elétricas inteligentes*. Rio de Janeiro, RJ, Brasil: Interciência, 2022.

OFFICE OF CYBERSECURITY, Energy Security and Emergency Response. *U.S. Department of Energy announces $70 million funding opportunity for rural and municipal utilities to strengthen cybersecurity*. Disponível em: https://www.energy.gov/ceser/articles/us-department-energy-announces-70-million-funding-opportunity-rural-and-municipal. Acesso em: 14 jun. 2024.

ONS – OPERADOR NACIONAL DO SISTEMA ELÉTRICO. *Manual de procedimentos da operação – Módulo 5: Submódulo 5.13 – Rotina operacional*. Rio de Janeiro, RJ, Brasil: ONS, 2022.

OTUNG, Ifiok. *Communication engineering principles*. Hoboken, NJ, EUA: Wiley, 2021.

OUAISSA, Mariyam *et al.* Low power wide area network for large scale IoT: fundamentals, technologies and challenges. In: OUAISSA, Mariyam *et al.* (orgs.). *Low power wide area*

network for large scale Internet of Things: Architectures, communication protocols and recent trends. Boca Raton, FL, EUA: CRC Press, 2024. p. 1–14.

OZEL, Omur; WEERAKKODY, Sean; SINOPOLI, Bruno. Physical watermarking for securing cyber physical systems via packet drop injections. In: *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 8., 2017, Dresden, Alemanha. *Proceedings IEEE*, p. 271–276, out. 2017.

PASQUALETTI, Fabio; DORFLER, Florian; BULLO, Francesco. Control-theoretic methods for cyberphysical security: geometric principles for optimal cross-layer resilient control systems. *IEEE Control Systems*, v. 35, n. 1, p. 110–127, fev. 2015.

PATEL, Harsh Rajnikant. *Replay attack detection in smart grids using switching multi sine watermarking*. 2023. Dissertação (Mestrado) – Concordia University, Montréal, QC, Canadá, set. 2023.

PETER, John Benito Jesudasan. *Cyber physical systems: foundation and its applications*. Chennai, Índia: SK Research Group of Companies, 2023.

PRABHU, K. M. M. *Window functions and their applications in signal processing*. Boca Raton, FL, EUA: CRC Press, 2018.

PRASAD, Ajay; KAUSHIK, Keshav. Message authentication. In: AHMAD, Khaleel *et al.* (orgs.). *Emerging security algorithms and techniques*. Boca Raton, FL, EUA: CRC Press, 2019. p. 225–247.

RAJKUMAR, Vetrivel Subramaniam *et al.* Cyber attacks on power grids: causes and propagation of cascading failures. *IEEE Access*, v. 11, p. 103154–103176, 2023.

REDDY, Gogulamudi Pradeep; KUMAR, Yellapragada Venkata Pavan; CHAKRAVARTHI, Maddikera Kalyan. Communication technologies for interoperable smart microgrids in urban energy community: a broad review of the state of the art, challenges, and research perspectives. *Sensors*, v. 22, n. 15, p. 5881, 6 ago. 2022.

REFAAT, Shady S. *et al. Smart grid and enabling technologies*. Hoboken, NJ, EUA: Wiley, 2021.

RIBAS MONTEIRO, Luiz Fernando; RODRIGUES, Yuri R.; ZAMBRONI DE SOUZA, A. C. Cybersecurity in cyber physical power systems. *Energies*, v. 16, n. 12, p. 4556, 7 jun. 2023.

ROOSA, Stephen A. *Fundamentals of microgrids: development and implementation*. Boca Raton, FL, EUA: CRC Press, 2020.

RUBIN, Frank. *Secret key cryptography: ciphers, from simple to unbreakable*. Shelter Island, NY, EUA: Manning, 2022.

SADIKU, Matthew; MUSA, Sarhan; ALEXANDER, Charles. *Análise de circuitos elétricos com aplicações*. Porto Alegre, RS, Brasil: AMGH, 2013.

SAÏD-ROMDHANE, M. Ben *et al.* Simple and systematic LCL filter design for three phase grid connected power converters. *Mathematics and Computers in Simulation*, v. 130, p. 181–193, dez. 2016.

SAKKARI, Deepak S.; ULLA, Mohammed Mujeer. Review on insight into elliptic curve cryptography. In: ZURADA, Jacek M.; GUNJAN, Vinit Kumar (orgs.). *Modern approaches in machine learning & cognitive science: a walkthrough*. Cham, Suíça: Springer International Publishing, 2022. p. 81–93.

SCHWAEGERL, Christine; TAO, Liang. The microgrids concept. In: HATZIARGYRIOU, Nikos (org.). *Microgrids architectures and control*. Hoboken, NJ, EUA: Wiley-IEEE Press, 2014. p. 1–24.

SCIPY. Boxcar. Disponível em: https://docs.scipy.org/doc/scipy/reference/generated/scipy.signal.boxcar.html. Acesso em: 28 jun. 2024.

SECGIN, Suat. *Evolution of wireless communication ecosystems*. Hoboken, NJ, EUA: Wiley, 2023.

SECHILARIU, Manuela; LOCMENT, Fabrice. *Urban DC microgrid: intelligent control and power flow optimization*. Oxford, Reino Unido: Butterworth-Heinemann, 2016.

SELIN, M.; PREETHA MATHEW, K. Review of spoof detection in automatic speaker verification system. In: *Proceedings of International Conference on Communication Systems and Network Technologies (CSNT)*. [S.l.]: IEEE, p. 317–329, 2019.

SEN, Jaydip; DASGUPTA, Subhasis. *Data privacy preservation on the Internet of Things*. *Journal of Information Security and Applications*, Oxford, Reino Unido, 1 abr. 2023.

SHAFIEE, Qobad; NADERI, Mobin; BEVRANI, Hassan. *Microgrids: dynamic modeling, stability and control*. Hoboken, NJ, EUA: Wiley, 2023.

SHARMA, Divya; SINGLA, Renu. A detail review on Multiprotocol Label Switching (MPLS). *International Journal of Engineering Research and General Science*, v. 3, n. 2, p. 354–361, mar. 2015.

SHI, Wenbo; WONG, Vincent W. S. Introduction to smart grid communications. In: INIEWSKI, Krzysztof; BERGER, Lars T. (orgs.). *Smart grid applications, communications, and security*. Hoboken, NJ, EUA: Wiley, 2012. p. 121–142.

SHIN, Bongsik. *A practical introduction to enterprise network and security management*. Boca Raton, FL, EUA: CRC Press, 2017.

SHUN-PING CHEN. *Fundamentals of information and communication technologies*. Newcastle upon Tyne, Reino Unido: Cambridge Scholars Publishing, 2020.

SILICON LABS. Bluetooth® 5.3 – What's new for IoT device makers and application developers? Disponível em: https://community.silabs.com/s/share/a5U1M000000koJ8UAI/bluetooth-53-whats-new-for-iot-device-makers-and-application-developers?language=en_US. Acesso em: 5 dez. 2023.

SINGH, Arvind R. *et al.* Microgrid system. In: RAY, Papia; BISWAL, Monalisa (orgs.). *Microgrid: operation, control, monitoring and protection*. Cham, Suíça: Springer, 2020. p. 1–25.

SINGH, Madhusudan; PATI, Debadatta. Countermeasures to replay attacks: a review. *IETE Technical Review*, v. 37, n. 6, p. 599–614, 1 nov. 2020.

SINHA, Rishi Ratan; KANWAR, Neeraj. Hybrid microgrids: architecture, modeling, limitations, and solutions. In: MWASILU, F.; JUSTO, J. J.; BANSAL, Ramesh C. (orgs.). *Modeling and control dynamics in microgrid systems with renewable energy resources*. Cambridge, MA, EUA: Elsevier, 2023.

SOLTANI, Reza *et al.* Distributed ledger technologies and their applications: a review. *Applied Sciences*, v. 12, n. 15, p. 7898, 6 ago. 2022.

SPURGEON, Charles; ZIMMERMAN, Joann. *Ethernet: the definitive guide: designing and managing local area networks*. 2. ed. Sebastopol, CA, EUA: O'Reilly Media, 2014.

STEWART, James M.; TITTEL, Ed.; CHAPPLE, Mike. *CISSP Certified Information Systems Security Professional Study Guide*. 3. ed. Indianapolis, IN, EUA: Sybex, 2005.

STEWART, James Michael; CHAPPLE, Mike; GIBSON, Darril. *CISSP Certified Information Systems Security Professional Study Guide Edition*. Hoboken, NJ, EUA: John Wiley & Sons, 2015.

SUN, Yao *et al. Series-parallel converter-based microgrids*. Cham, Suíça: Springer International Publishing, 2022.

TAHOUN, A. H.; ARAFA, M. Secure control design for nonlinear cyber–physical systems under DoS, replay, and deception cyber-attacks with multiple transmission channels. *ISA Transactions*, v. 128, p. 294–308, set. 2022.

TANG, Bixiang; ALVERGUE, Luis D.; GU, Guoxiang. Secure networked control systems against replay attacks without injecting authentication noise. In: IEEE. *Proceedings of the American Control Conference*, Chicago, IL, EUA, jul. 2015.

TEKINERDOGAN, Bedir *et al.* A feature-based ontology for cyber-physical systems. In: TEKINERDOGAN, Bedir *et al.* (orgs.). *Multi-paradigm modelling approaches for cyber-physical systems*. Cambridge, MA, EUA: Elsevier, 2021.

TOLEDANO, Soledad Antelada. *Critical infrastructure security: cybersecurity lessons learned from real-world breaches*. Birmingham, Reino Unido: Packt Publishing, 2024.

TRAPIELLO, Carlos; PUIG, Vicenc. A zonotopic-based watermarking design to detect replay attacks. *IEEE/CAA Journal of Automatica Sinica*, v. 9, n. 11, p. 1924–1938, nov. 2022.

TSCHOFENIG, Hannes *et al. Diameter new generation AAA protocol – design, practice, and applications*. Hoboken, NJ, EUA: Wiley, 2019.

UDDIN, Moslem *et al.* Microgrids: a review, outstanding issues and future trends. *Energy Strategy Reviews*, v. 49, p. 101127, set. 2023.

UNITED STATES. *FCC record: a comprehensive compilation of decisions, reports, public notices and other documents of the Federal Communications Commission of the United States*. Issue 6. Washington, DC, EUA: Federal Communications Commission, 2016. v. 31.

VADANA, D. Prasanna *et al.* Introduction. In: SASI, K. Kottayil (org.). *Smart microgrids*. 1. ed. Boca Raton, FL, EUA: CRC Press, 2020. p. 1–20.

WEERAKKODY, Sean; SINOPOLI, Bruno. Detecting integrity attacks on control systems using a moving target approach. In: IEEE. *Proceedings of the 54th IEEE Conference on Decision and Control (CDC)*. Osaka, Japão, dez. 2015.

WEIK, Martin. *Fiber optics standard dictionary*. New York, NY, EUA: Springer, 2012.

WENTWORTH, Stuart M. *Eletromagnetismo aplicado: abordagem antecipada das linhas de transmissão*. 1. ed. Porto Alegre, RS, Brasil: Bookman, 2008.

WYGLINSKY, Alexander M.; NEKOVEE, Maziar; HOU, Y. Thomas. When radio meets software. In: WYGLINSKY, Alexander M.; NEKOVEE, Maziar; HOU, Y. Thomas (orgs.). *Cognitive radio communications and networks: principles and practice*. 1. ed. Burlington, MA, EUA: Academic Press, 2009. p. 1–12.

XU, Fei; XU, Jing. Economic perspective of cybersecurity: principles and strategies. In: SU, Chunhua; SAKURAI, Kouichi (orgs.). *Science of cyber security – SciSec 2022 Workshops AI-CryptoSec, TA-BC-NFT, and MathSci-Qsafe 2022, Matsue, Japan, August 10–12, 2022, revised selected papers*. Singapore: Springer Nature Singapore, 2022. p. 119–130.

XU, Feifan *et al.* Enhancing accuracy of alignment measurement in lithography using two-dimensional desirable sidelobe convolution window. *Measurement*, v. 242, p. 116196, jan. 2025.

YARALI, Abdulrahman. *From 5G to 6G: technologies, architecture, AI, and security*. Hoboken, NJ, EUA: Wiley, 2023.

ZAKARIYA SALEH, Zahraa. A review of emerging low power networks in Internet of Medical Things (IoMT). In: RABIE, Khaled *et al.* (orgs.). *IoT as a service: 8th EAI International Conference, IoTaaS 2022, Virtual Event, November 17–18, 2022, Proceedings*. Cham, Suíça: Springer Nature Switzerland, 2023. p. 23–37.

ZENG, Xianwu; BAO, Shuping. *Key technologies of Internet of Things and smart grid*. Singapore: Springer Nature Singapore, 2023.

ZHANG, Peng. *Networked microgrids*. Cambridge, Reino Unido: Cambridge University Press, 2021.

ZHENG, Dehua *et al. Microgrid protection and control*. Amsterdam, Países Baixos: Elsevier Science, 2021.

Z-WAVE ALLIANCE. *What is Z-Wave Long Range and how does it differ from Z-Wave?*. Disponível em: https://z-wavealliance.org/what-is-z-wave-long-range-and-how-does-it-differ-from-z-wave/. Acesso em: 21 jul. 2023.