Capítulo 4

Wi-Fi Sensing e CSI aplicados à Cibersegurança: Fundamentos, Aplicações e Prática

Felipe Silveira de Almeida (ITA e Exército Brasileiro), Eduardo Fabrício Gomes Trindade (ITA e e Exército Brasileiro), Gioliano de Oliveira Braga (ITA), Ágney Lopes Roth Ferraz (ITA), Giovani Hoff da Costa (ITA), Gustavo Cavalcanti Morais (ITA), Lourenço Alves Pereira Júnior (ITA)

Abstract

Digital authentication faces increasing challenges due to the limitations of traditional methods, such as passwords and conventional biometrics, in the face of sophisticated attacks like spoofing and relay. In this context, leveraging Channel State Information (CSI) from Wi-Fi networks emerges as a promising solution for secure, non-intrusive authentication. This chapter covers the theoretical foundations of Wi-Fi CSI, describes methods for capturing and preprocessing data, and presents practical demonstrations of authentication and intrusion detection using low-cost devices such as ESP32 and Raspberry Pi. Finally, current challenges and future trends are discussed, highlighting opportunities for developing robust and adaptable CSI-based cybersecurity systems.

Resumo

A autenticação digital enfrenta desafios crescentes devido às limitações de métodos tradicionais, como senhas e biometria convencional, diante de ataques sofisticados como spoofing e relay. Neste contexto, a utilização de Informações do Estado do Canal (Channel State Information – CSI) de redes Wi-Fi emerge como uma solução promissora para autenticação segura e não intrusiva. Este capítulo aborda os fundamentos teóricos do Wi-Fi CSI, detalha métodos de captura e pré-processamento dos dados, e apresenta casos práticos de autenticação e detecção de intrusão usando dispositivos de baixo custo, como ESP32 e Raspberry Pi. Ao final, discutem-se desafios atuais e tendências futuras, destacando oportunidades para o desenvolvimento de sistemas robustos e adaptáveis de cibersegurança baseados em CSI.

4.1. Introdução e Motivação

A infraestrutura Wi-Fi tornou-se onipresente na vida moderna. De residências e escritórios a aeroportos, fábricas e instituições militares, redes sem fio baseadas no padrão IEEE 802.11 passaram de soluções convenientes para componentes críticos de comunicação, controle e automação. Estima-se que, em 2025, mais de 30 bilhões de dispositivos estarão conectados por Wi-Fi em escala global, impulsionando aplicações que vão desde entretenimento doméstico até processos industriais de missão crítica[Cisco 2020]. Essa penetração massiva consolidou o Wi-Fi como infraestrutura de conectividade essencial — mas também como vetor privilegiado de ameaças.

Historicamente, o Wi-Fi foi projetado com foco na mobilidade e facilidade de implantação, o que trouxe implicações de segurança desde sua origem. Apesar da evolução dos protocolos de criptografia (como WPA3), diversos ataques exploram características subjacentes da camada física e do protocolo MAC, contornando os mecanismos tradicionais de defesa. A vulnerabilidade a ataques como *deauthentication*, *evil twin*, jamming seletivo e exploração de *management frames* é explorada por atacantes com conhecimento moderado, armados com ferramentas de baixo custo. Esse cenário impõe novos desafios para pesquisadores e profissionais de cibersegurança: como proteger um canal compartilhado, sem fio, ubíquo e inerentemente exposto?

Nos últimos anos, a comunidade científica passou a enxergar o Wi-Fi sob uma nova ótica: para além de apenas um meio de comunicação, um canal sensível às perturbações do ambiente. Essa mudança paradigmática deu origem ao conceito de *Wi-Fi Sensing*, em que a própria infraestrutura de comunicação é utilizada como sensor passivo de eventos físicos. O princípio é simples e poderoso: ao transmitir sinais OFDM em múltiplas subportadoras, os dispositivos Wi-Fi sofrem influência direta de obstáculos, movimentos e alterações no entorno. Essa influência é captada na forma de variações sutis no *Channel State Information* (CSI), um conjunto de coeficientes complexos que descreve a resposta do canal para cada subportadora e cada par de antenas.

O acesso a dados de CSI em placas comerciais foi inicialmente limitado, mas iniciativas como o Intel 5300 CSI Tool [Halperin et al. 2011], Nexmon [Schulz et al. 2017], ESP32-CSI [Systems 2022], entre outras, abriram caminho para a captura de CSI em tempo real com granularidade suficiente para análise de sinais ambiente. A sensibilidade do CSI é tamanha que pequenas variações são detectáveis e mensuráveis, tais como: o movimento da palma da mão, a respiração de uma pessoa ou a vibração de um objeto. Isso habilita uma nova categoria de aplicações, incluindo monitoramento de sinais vitais[Liu et al. 2015], reconhecimento de gestos[Abdelnasser et al. 2015], detecção de intrusão física[Li et al. 2017] e autenticação por presença[Liu et al. 2014].

A consolidação desta área veio com a criação do grupo de trabalho IEEE 802.11bf, que adiciona formalmente suporte a funcionalidades de *sensing* na pilha Wi-Fi[IEEE 802.11 Working Group 2024]. Essa padronização viabiliza, por exemplo, que um ponto de acesso informe a variação de fase entre subportadoras como parte das medições periódicas de canal, dispensando hacks de firmware e extrações indiretas. O draft atual da 802.11bf ([IEEE 802.11 Working Group 2025]) prevê modos cooperativos de sensoriamento, troca de métricas CSI entre dispositivos e aplicações de detecção baseadas em variações contextuais do ambiente. Com isso, o Wi-Fi passa a ocupar um novo

papel: o de sensor distribuído e não invasivo, presente em praticamente todo ambiente urbano. Essa nova função permite reimaginar soluções de segurança que antes dependiam de sensores dedicados, câmeras ou dispositivos vestíveis. Agora, a própria rede sem fio — já presente e ativa — pode prover indicadores físicos sobre eventos, movimentos e identidades, com latência reduzida e integração direta aos sistemas de autenticação e detecção de anomalias.

No entanto, o uso de Wi-Fi como sensor de cibersegurança ainda enfrenta obstáculos importantes: reprodutibilidade dos experimentos, normalização dos pipelines de coleta, dependência do ambiente físico e escassez de guias sistematizados. A literatura apresenta grande diversidade de abordagens, com métricas heterogêneas, configurações não padronizadas e falta de estudos comparativos. A ausência de benchmarks comuns dificulta a adoção prática e o avanço consolidado da área.

Este capítulo busca preencher essa lacuna ao sistematizar os fundamentos técnicos, os principais trabalhos publicados e as técnicas práticas necessárias para transformar redes Wi-Fi em aliadas da segurança. Partindo da base teórica do CSI, passando por aplicações como autenticação contínua e detecção de intrusão passiva, apresentamos estudos de caso reais validados com ESP32 e Raspberry Pi, cobrindo desde a coleta dos dados até o uso de modelos de aprendizado de máquina. Ao fazer isso, conectamos teoria e prática, contribuindo para uma nova geração de soluções de segurança baseadas na onipresença do Wi-Fi.

4.1.1. Wi-Fi CSI aplicado a Cibersegurança

Apesar do avanço dos mecanismos criptográficos e da adoção de múltiplos fatores de autenticação (MFA), os sistemas atuais ainda enfrentam vulnerabilidades críticas quando confrontados com ataques que manipulam a camada física ou se aproveitam da ausência de autenticação de presença. Operações militares, controle de acesso físico a laboratórios, autenticação em terminais de pagamento ou desbloqueio de recursos estratégicos são exemplos de aplicações sensíveis em que a simples posse de credenciais ou a resposta correta a um desafio (múltiplos fatores) não garantem que o solicitante está, de fato, fisicamente presente no local autorizado.

Dentre os vetores de ataque mais eficazes e difíceis de mitigar, destacam-se os chamados *relay attacks*. Esses ataques interceptam e retransmitem sinais legítimos entre duas partes distantes, de modo que um atacante remoto pode se passar por um usuário autorizado. Tal técnica é particularmente preocupante em sistemas *contactless*, como pagamentos por aproximação, abertura de veículos ou autenticação via NFC. Mesmo com criptografia forte, a temporalidade da comunicação é suficientemente preservada para que o sistema autenticador aceite o atacante como legítimo [Xu et al. 2022, Truong et al. 2020].

Outro problema recorrente é o *spoofing* de dispositivos e identidades em redes Wi-Fi. Com ferramentas como Scapy[1], aireplay-ng[2] e fluxion[3], um atacante pode forjar pacotes de associação, falsificar endereços MAC, replicar características de dispositivos legítimos e induzir pontos de acesso a aceitar conexões maliciosas. Esses ataques ex-

[1] `https://scapy.net/`

[2] `https://www.aircrack-ng.org/doku.php?id=aireplay-ng`

[3] `https://fluxionnetwork.github.io/fluxion/`

ploram falhas na autenticação inicial e na ausência de verificação contextual, o sistema confia na identidade apresentada sem validar características físicas ou comportamentais do emissor. Em particular, ataques de relay em pagamentos sem contato (*contactless*) têm sido uma crescente preocupação devido à simplicidade com que atacantes conseguem retransmitir sinais legítimos remotamente [Xu et al. 2022]. Além disso, a falsificação de identidade em dispositivos IoT, especialmente em ambientes industriais e médicos, gera ameaças críticas e difíceis de mitigar por métodos tradicionais.

Mesmo abordagens avançadas de MFA, que combinam senha com biometria ou tokens físicos, não são à prova de falhas. Biometrias faciais e digitais podem ser clonadas ou contornadas via ataques por apresentação (*presentation attacks*). Tokens físicos podem ser roubados ou replicados. Além disso, muitos desses métodos realizam a autenticação apenas no momento do login, sem manter uma verificação contínua da identidade ao longo da sessão. Isso abre espaço para ataques de sequestro de sessão ou para que um atacante assuma o controle após a autenticação inicial.

Diante desse cenário, trabalhos que representam o estado da arte têm buscado alternativas que incorporem ao processo de autenticação elementos adicionais, difíceis de replicar remotamente e que estejam fortemente ligados ao contexto físico do usuário. É nesse ponto que surge o uso do *Channel State Information* (CSI) como mecanismo capaz de sensoriar o ambiente físico e respectivamente obter padrões e assinaturas que potencialmente enriquecem a identificação de mudanças. Por capturar variações sutis no campo eletromagnético causadas por corpos humanos, objetos, movimentos e posicionamentos espaciais, o CSI oferece uma "assinatura física" que pode ser associada a um usuário ou evento específico. Essa assinatura é difícil de forjar remotamente, pois depende da interação única entre o corpo e o canal de rádio no momento da comunicação.

A ideia central é que o CSI atua como uma fonte de entropia contextual: ao analisar a forma como os sinais Wi-Fi se propagam, atenuam e refletem no ambiente, é possível inferir se o usuário está fisicamente presente e se a configuração espacial corresponde ao padrão esperado. Essa abordagem, por sua própria natureza, amplia as garantias de segurança dos sistemas tradicionais, complementando mecanismos criptográficos e autenticações lógicas com uma verificação baseada em características do mundo físico.

Desse modo, o presente minicurso têm por objetivo sistematizar esse campo emergente. Buscamos proporcionar ao leitor:

- uma visão fundamentada sobre como o Wi-Fi pode ser transformado em sensor de presença e identidade;
- um mapeamento crítico do estado da arte na autenticação baseada em CSI;
- diretrizes práticas de coleta, pré-processamento e modelagem de sinais CSI;
- exemplos reais de autenticação e detecção de intrusão com dispositivos de baixo custo;
- e uma análise sobre trabalhos futuros, com as limitações atuais e os caminhos de pesquisa mais promissores.

Nosso enfoque parte de uma premissa simples: em um mundo cada vez mais vulnerável a ataques remotos e automatizados, proteger apenas as camadas lógicas não é

mais suficiente. A ideia é oferecer uma visão de que a presença física é um recurso de segurança valioso, e o Wi-Fi, com seu alcance e ubiquidade, pode ser um novo ferramental que ajuda a mitigar tais ameaças cibernéticas. Assim, acreditamos que este material contribui para consolidar a área de *Wi-Fi Sensing para Cibersegurança* como linha de pesquisa autônoma, com forte base prática e amplo potencial de impacto. Além disso, esperamos que sirva como porta de entrada acessível para novos pesquisadores, oferecendo não apenas conceitos, mas ferramentas, datasets e orientações para experimentação prática.

Importante mencionar que este estudo se distingue por apresentar demonstrações práticas realizadas com dispositivos acessíveis como ESP32 e Raspberry Pi, ilustrando técnicas viáveis e replicáveis para autenticação e detecção de intrusão com base em características biofísicas extraídas do CSI.

Este capítulo está estruturado em cinco módulos progressivos. A Seção 4.2 apresenta fundamentos teóricos do CSI, ao passo que a Seção 4.3 descreve o estado da arte em autenticação e detecção de intrusão. Do ponto de vista prático, o Seção 4.4 traz um modelo de pipeline de coleta e pré-processamento dos dados oriundos de CSI. Quando observados estudos de caso, as Seções 4.5 e 4.6 demonstrações práticas com dispositivos ESP32 e Raspberry Pi. A Seção 4.7 perspectivas futuras relacionadas ao aprendizado federado e resiliência adversarial. Por fim, na Seção 4.8 conclui-se o capítulo.

4.2. Fundamentos de Wi-Fi Sensing e CSI

O Wi-Fi sensing utiliza sinais sem fio para obter informações sobre o ambiente físico [Ma et al. 2019]. Inicialmente, os sistemas de detecção e localização baseavam-se no RSSI (*Received Signal Strength Indicator*), que mede a potência do sinal recebido. Essa abordagem permitiu técnicas como localização por impressão digital (*fingerprinting*) e monitoramento de presença [Yang et al. 2013, Sen et al. 2012]. No entanto, os pesquisadores apontam que o RSSI apresenta limitações em ambientes complexos devido ao desvanecimento por multipercurso, baixa resolução espacial e instabilidade temporal, fornecendo apenas um valor agregado por pacote.

A introdução do padrão IEEE 802.11n marcou a adoção do *Channel State Information* (CSI — Informação do Estado do Canal), que registra a resposta do canal para cada subportadora em sistemas MIMO-OFDM, fornecendo dados complexos de amplitude e fase [iee 2021]. Os autores em [Ma et al. 2019] destacam que o CSI captura propriedades como atenuação de percurso e atraso de propagação, oferecendo maior precisão em comparação ao RSSI. Essa transição expandiu as aplicações do sensoriamento sem fio, incluindo reconhecimento de atividades humanas, autenticação, localização indoor e segurança de redes [Liu et al. 2020, Tan et al. 2022].

4.2.1. Evolução do Wi-Fi CSI

O CSI é uma métrica fundamental nos sistemas Wi-Fi modernos, caracterizando as propriedades do canal de comunicação sem fio, como espalhamento, desvanecimento e atenuação com base na distância [Ma et al. 2019]. Originalmente, o CSI foi introduzido para otimizar a comunicação, viabilizando a equalização de canal, beamforming e modulação adaptativa, especialmente em sistemas MIMO (Multiple-Input Multiple-Output). Dife-

rentemente do Indicador de Intensidade de Sinal Recebido (RSSI), que mede apenas a potência total do sinal recebido, o CSI fornece informações detalhadas de amplitude e fase por subportadora, capturadas em matrizes de canal complexas [Yang et al. 2013].

Nos primeiros padrões IEEE 802.11 (1997–2003), como o 802.11a/b/g, a estimativa de canal era rudimentar, baseada em RSSI ou em equalizações básicas, sem suporte a MIMO ou beamforming [iee 2021]. O CSI, como é definido hoje, foi formalizado no padrão 802.11n (2009), que introduziu MIMO e beamforming explícito, exigindo medições precisas do canal para calcular matrizes de direcionamento e otimizar taxas de dados [Halperin et al. 2011]. O CSI é estimado pelo receptor utilizando os Long Training Fields (LTFs) no preâmbulo do pacote, com feedback enviado ao transmissor para ajustes, como direcionamento de feixe eletromagnético, o que melhora o alcance, reduz interferência e economiza energia. Padrões subsequentes, como o 802.11ac (2013) e o 802.11ax (2021), aprimoraram o CSI com suporte a MIMO multiusuário (MU-MIMO) e maior largura de banda, enquanto o 802.11bf formaliza seu uso para sensoriamento [iee 2021].

Inicialmente, o acesso ao CSI era interno aos dispositivos, restrito ao firmware para fins de comunicação. A partir de 2011, ferramentas como o Intel 5300 CSI Tool [Halperin et al. 2011] permitiram a extração de CSI em dispositivos comerciais, capturando matrizes para 30 grupos de subportadoras no padrão 802.11n. Essa democratização impulsionou aplicações de sensoriamento, como reconhecimento de gestos [Zheng et al. 2019], autenticação [Wang et al. 2017] e localização indoor [Kotaru et al. 2015], superando as limitações do RSSI, que foi usado nos primeiros estudos de sensoriamento, mas carecia de granularidade [Yang et al. 2013]. Ferramentas posteriores, como o Atheros CSI Tool [Xie et al. 2019], Nexmon [Schulz et al. 2018] e ESP32 CSI Toolkit [Hernandez and Bulut 2020], ampliaram o acesso, viabilizando o uso de sensoriamento em dispositivos de baixo custo, como os utilizados nesta pesquisa.

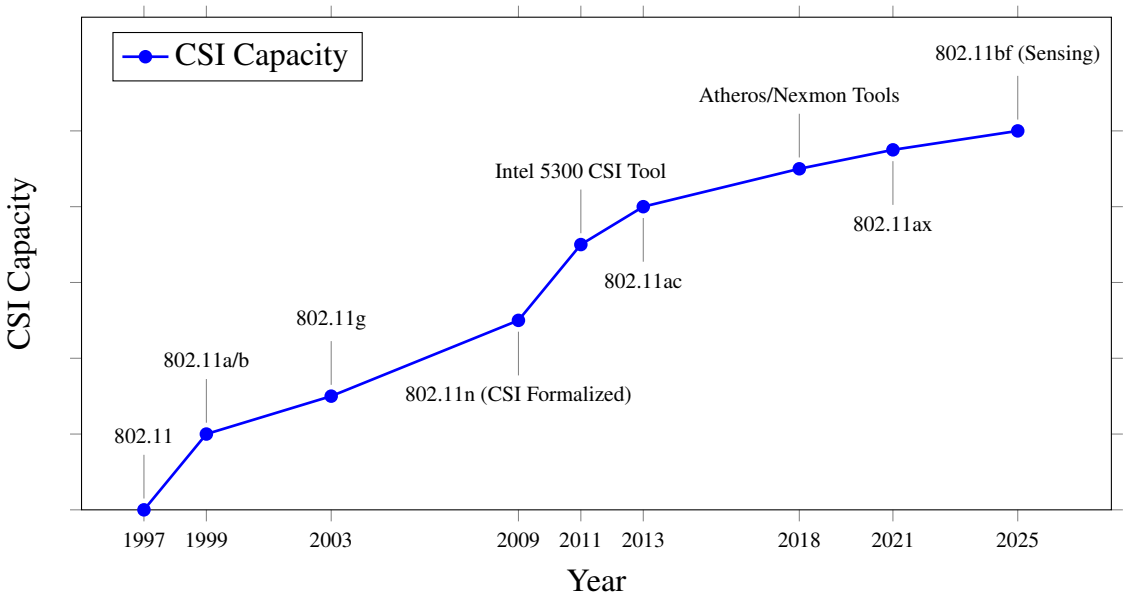


Figura 4.1. Sensoriamento por Wi-Fi [Ma et al. 2019, Halperin et al. 2011].

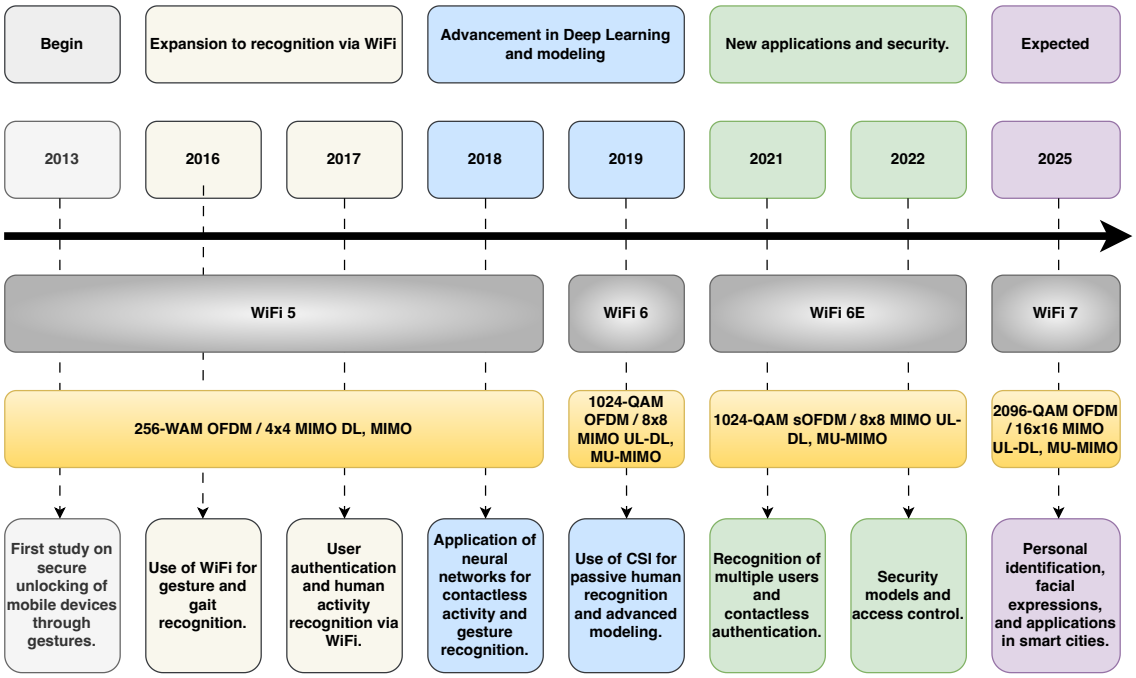


Figura 4.2. Linha do tempo de estudos em Wi-Fi sensing

Esta evolução destaca a transição do CSI de uma ferramenta de comunicação para um recurso de sensoriamento. A Figura 4.1 ilustra essa trajetória, desde a ausência de CSI nos primeiros padrões até sua adoção em aplicações avançadas de sensoriamento.

Como ilustrado na Figura 4.2, essa evolução acompanhou os avanços nos padrões Wi-Fi e no hardware, permitindo maior resolução e sensibilidade. Com a popularização de tecnologias como MIMO e OFDM, o CSI passou a revelar variações eletromagnéticas sutis causadas pela presença física, possibilitando sensoriamento de alta precisão. Um desafio central, no entanto, ainda reside na garantia de identificação resiliente frente ao ruído ambiental, heterogeneidade de dispositivos e posicionamento do usuário — todos fatores que afetam a propagação do sinal. Técnicas robustas de pré-processamento do sinal e de aprendizado de máquina têm emergido como ferramentas essenciais para mitigar esses desafios e ampliar o poder discriminativo dos modelos baseados em CSI.

4.2.2. Arquitetura física do IEEE 802.11

O padrão IEEE 802.11 define uma pilha modular em que a *camada física* (PHY) modula, transmite e recebe sinais de rádio, enquanto a camada *MAC* regula o acesso ao meio compartilhado. A partir do 802.11n, a PHY consolidou duas tecnologias que se tornaram centrais para *Wi-Fi Sensing*: multiplexação por divisão ortogonal de frequência (**OFDM**) e múltiplas antenas em transmissão e recepção (**MIMO**) [Halperin et al. 2011].

- **OFDM** fragmenta cada canal de 20–160 MHz em dezenas ou centenas de subportadoras ortogonais, permitindo que símbolos sejam transmitidos em paralelo com alta imunidade ao efeito *multipath*.
- **MIMO** envia fluxos independentes por múltiplas antenas, explorando a diversidade

espacial para ampliar vazão e robustez.

Cada quadro (*frame*) Wi-Fi inicia-se com campos de treinamento (*Long Training Fields – LTF*). O receptor compara os LTFs recebidos com a sequência conhecida e estima, para cada subportadora k, um ganho complexo $h_k = |h_k|e^{j\angle h_k}$. A coleção desses ganhos para todos os pares de antenas $m \times n$ e para todas as M subportadoras forma a matriz **Channel State Information (CSI)** [Wang and Liu 2019]. Como ilustrado na Figura 4.3, quando empilhamos sucessivas amostras no tempo, obtemos um tensor $H \in \mathbb{C}^{N\times M\times K\times T}$ que descreve, simultaneamente, variações espaciais, espectrais e temporais do canal.

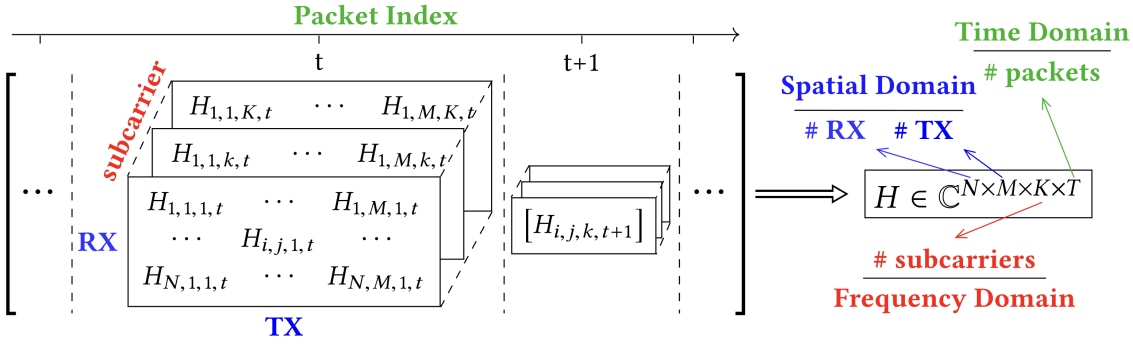


Figura 4.3. Matriz Wi-Fi CSI [Ma et al. 2019].

Comparativo CSI × RSSI × FTM. Enquanto o RSSI condensa todo o canal em um único valor por pacote e o *Fine Timing Measurement* (FTM) (802.11az) oferece apenas atraso temporal, o CSI fornece centenas de graus de liberdade — virtualmente uma "imagem" de alta resolução do ambiente de rádio. Estudos recentes mostram que deslocamentos milimétricos de um corpo humano geram perturbações detectáveis em $|h_k|$ e $\angle h_k$ mesmo através de obstáculos, permitindo monitoramento de sinais vitais, reconhecimento de gestos e autenticação por presença [Wang and Liu 2019].

Relevância para cibersegurança. A granularidade do CSI viabiliza três propriedades desejáveis em sistemas de defesa:

(a) **Autenticação contínua** — perfis biométricos ambientais (ex. geometria da mão) podem ser verificados a cada pacote.
(b) **IDS físico-digital** — alterações abruptas na matriz H denunciam intrusos antes mesmo da associação à rede.
(c) **Resistência a *relay/spoofing*** — replicar remotamente o mesmo padrão de multipercurso é impraticável na ausência física.

Nas subseções seguintes discutiremos o modelo matemático do canal (CFR × CIR), técnicas de normalização e estratégias de engenharia de atributos que convertem o CSI em evidências robustas para aprendizado de máquina e detecção em tempo real.

4.2.3. Modelo de canal e representação em subportadoras

Para compreender o *Channel State Information* é necessário partir do **modelo de canal multipercurso**. No domínio do tempo, o *Channel Impulse Response* (CIR) é expresso

como

$$h(t,\tau) \;=\; \sum_{l=1}^{L} \alpha_l \; \delta(\tau-\tau_l)\; e^{j\phi_l}, \tag{1}$$

onde cada caminho l apresenta atenuação α_l, atraso τ_l e fase ϕ_l em relação ao percurso direto. Aplicando transformada de Fourier em (1), obtém-se a *Channel Frequency Response* (CFR), que descreve o ganho complexo do canal para cada frequência f:

$$H(f,t) \;=\; \sum_{l=1}^{L} \alpha_l \, e^{-j2\pi f \tau_l} \, e^{j\phi_l}. \tag{2}$$

Discretização em OFDM. Em sistemas OFDM, o espectro é dividido em K subportadoras igualmente espaçadas. Avaliando (2) nas frequências discretas $f_k = f_0 + k\Delta f$ ($k = 0,\ldots,K-1$) obtemos o vetor

$$\mathbf{h}(t) = [H(f_0,t), H(f_1,t), \ldots, H(f_{K-1},t)]^{\mathsf{T}},$$

cujos elementos compõem o CSI disponibilizado pelo hardware [Halperin et al. 2011]. O receptor calcula $\mathbf{h}(t)$ a cada pacote, antes da equalização final, e fornece:

(a) **amplitude** $|H(f_k,t)|$, sensível a bloqueios e atenuações;
(b) **fase** $\angle H(f_k,t)$, sensível a deslocamentos de com boa precisão nas aplicações em cibersegurança;
(c) **matriz MIMO** $H_{m,n}(f_k,t)$, quando múltiplas antenas são usadas.

Tensor CSI em $N \times M \times K \times T$. Para um sistema com N antenas receptoras, M transmissoras, K subportadoras e T amostras temporais, empilha-se o CFR em um tensor

$$H \in \mathbb{C}^{N\times M\times K\times T},$$

no qual cada dimensão captura, respectivamente, *diversidade espacial*, *diversidade espectral* e *dinâmica temporal* do canal [Wang and Liu 2019]. Esta representação multi-eixo é a base de técnicas recentes de classificação que tratam o CSI como "imagens" 4-D alimentando redes convolucionais ou modelos híbridos leves.

Resolução temporal e largura de banda. A capacidade de detecção fina depende de dois parâmetros físicos:

- **Largura de banda** (B): quanto maior B, menor o passo Δf entre subportadoras e maior a resolução de atraso $\Delta\tau = 1/B$.
- **Taxa de amostragem de pacotes**: limita a resolução temporal; placas como Intel 5300 capturam $\approx$2,5 k CSI/s, enquanto ESP32 atinge 500–800 CSI/s.

Essas restrições definem o tipo de fenômeno que pode ser capturado. Por exemplo, respiração (0,2–0,5 Hz), gestos (1–5 Hz) ou passos (1–3 Hz) são viáveis com larguras de

Tabela 4.1. Trabalhos sobre aplicações de CSI na literatura.

Referência	Aplicação	Técnicas	Desempenho
[Al-qaness et al. 2016]	Reconhecimento de Atividades	Aprendizado de máquina com janelamento	92%
[Guo and Ho 2022]	Reconhecimento de Atividades	CNN para monitoramento	98,19%
[Wang et al. 2019]	Autenticação e Biometria	ML com atributos tempo-frequência	93%
[Lin et al. 2023]	Autenticação e Biometria	Transfer Learning	97%
[Kotaru et al. 2015]	Localização Indoor	Super-resolução	40 cm
[Zou et al. 2017]	Localização Indoor	Transfer Learning	96%
[Soto et al. 2022]	Monitoramento de Saúde	Análise temporal	95%
[Liu et al. 2018]	Monitoramento de Saúde	ML para sinais vitais	90%
[Gu et al. 2024]	Sensoriamento Ambiental	Análise espectral	83,33%
[Cominelli et al. 2023]	Sensoriamento Ambiental	ML para multipercurso	85%
[Ding et al. 2018]	Detecção de Pessoas	ML com diferença de fase	99,4%
[Wang et al. 2020]	Detecção de Pessoas	Análise de densidade espectral	99%

20–80 MHz; vibrações de alta frequência requerem Wi-Fi 6E/7 com 160 MHz ou 320 MHz.

Implicações para segurança Mudanças inesperadas na distribuição estatística de $\mathbf{h}(t)$ indicam:

(i) **Presença ou ausência** de um corpo humano no local autorizado;
(ii) **Alterações de postura** ou substituição por um impostor;
(iii) **Perturbações externas**, como jamming seletivo ou dispositivos rogue.

Ao modelar a dinâmica de H em janelas curtas (50–200 ms), algoritmos de detecção podem diferenciar assinaturas benignas de atividades maliciosas sem decodificar payloads, fornecendo assim uma camada de defesa independente do protocolo criptográfico.

4.3. Aplicações Wi-Fi CSI em Segurança

A informação de estado do canal (CSI) viabiliza aplicações que exploram variações na propagação do sinal, indo além da comunicação tradicional. Essas variações, causadas por movimentações de pessoas, objetos ou dispositivos no ambiente, são analisadas para inferir padrões em cenários como segurança física, saúde e localização. Ao capturar características detalhadas da propagação do sinal sem fio, o CSI permite diversas aplicações práticas que vão para além da função básica de comunicação. O mapeamento sistemático conduzido nesta pesquisa revela que o Wi-Fi sensing baseado em CSI tem sido amplamente explorado em reconhecimento de atividades humanas, autenticação biométrica, localização indoor, monitoramento de sinais vitais e contagem de pessoas.

A Tabela 4.1 apresenta alguns dos trabalhos identificados na literatura, detalhando autores, aplicações, técnicas e desempenho.

Essas aplicações frequentemente utilizam técnicas de aprendizado de máquina supervisionado, cujo fluxo de trabalho genérico é ilustrado na Figura 4.4, mostrando o processo de coleta de dados, pré-processamento e classificação de eventos, como atividades humanas, a partir de dados rotulados.

As subseções a seguir descrevem seis aplicações com base na literatura, segui-

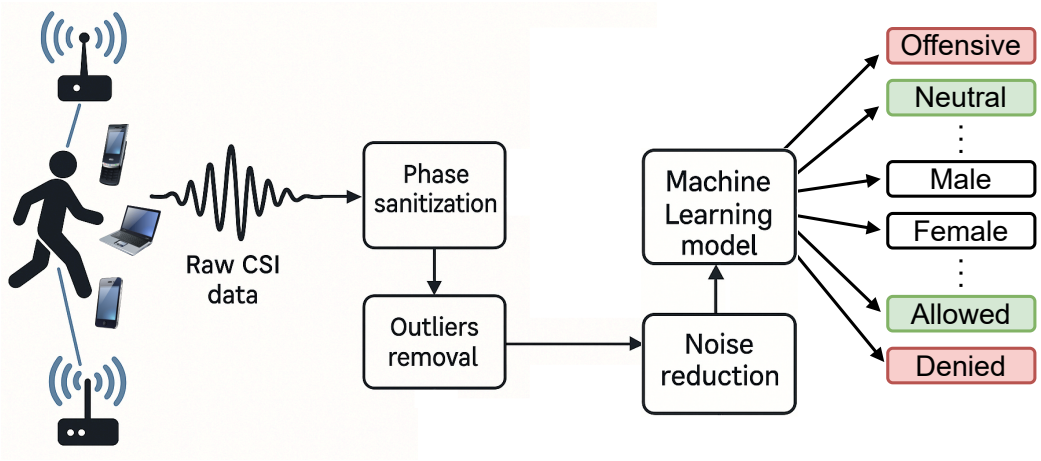


Figura 4.4. Modelo para desenvolvimento classificadores [Abu Ali et al. 2024].

das por uma discussão sobre a originalidade da proposta desta pesquisa, que explora a detecção proativa de dispositivos não autorizados em redes Wi-Fi.

Reconhecimento de Atividades Humanas. O Reconhecimento de Atividades Humanas (HAR — *Human Activity Recognition*) utiliza variações no CSI causadas por movimentos, como caminhar ou gesticular, para inferir ações em ambientes internos. Os autores de [Al-qaness et al. 2016] identificaram seis atividades cotidianas usando um roteador e um laptop, alcançando 92% de acurácia com algoritmos de aprendizado de máquina. Pesquisadores em [Guo and Ho 2022] aplicaram redes neurais convolucionais (CNNs) para monitoramento de quarentena, obtendo 98,19% de acurácia.

A abordagem exige etapas de pré-processamento, como janelamento e filtragem, para mitigar ruídos. Os autores de [Forbes et al. 2020] validaram o uso de hardware acessível, como o ESP32, alcançando 92% de acurácia em 11 classes de atividades. As limitações incluem sensibilidade a mudanças no ambiente e a necessidade de dados rotulados, o que dificulta a escalabilidade em cenários dinâmicos.

Autenticação e Biometria. A autenticação sem contato via CSI identifica usuários com base em características físicas ou comportamentais extraídas das perturbações no canal. Pesquisadores em [Wang et al. 2019] usaram atributos de tempo e frequência para reconhecimento passivo, alcançando 93% de acurácia. Os autores de [Shen et al. 2021] detectaram padrões de digitação em smartphones com 95% de precisão, utilizando análise espectral.

Sistemas baseados em CSI são robustos em ambientes controlados, mas podem exigir calibração para diferentes cenários. Pesquisadores em [Lin et al. 2023] aplicaram *transfer learning*, obtendo 97% de acurácia em múltiplos ambientes. As limitações incluem geralmente a dependência de condições estáveis e a complexidade no treinamento de modelos para novos usuários ou dispositivos.

Localização Indoor. A localização indoor com CSI explora os efeitos de multiper-

curso e variações de fase para atingir precisão inferior a um metro. Os autores de [Kotaru et al. 2015] desenvolveram o SpotFi, combinando algoritmos de super-resolução com CSI, obtendo um erro mediano de 40 cm. Pesquisadores em [Zou et al. 2017] implementaram contagem de pessoas com 96% de acurácia, utilizando *transfer learning*.

A técnica é eficaz em ambientes densos, mas requer múltiplos pontos de acesso. As limitações incluem sensibilidade a obstruções e a necessidade de calibração em cenários dinâmicos, o que aumenta a complexidade computacional em sistemas de baixo custo [Kotaru et al. 2015].

Monitoramento de Saúde. O monitoramento de saúde utiliza o CSI para detectar sinais vitais, como respiração e batimentos cardíacos, ou eventos como quedas, por meio da análise de microvariações no canal. Os autores de [Soto et al. 2022] monitoraram a respiração com 95% de acurácia, utilizando análise temporal e aprendizado de máquina. Pesquisadores em [Liu et al. 2018] detectaram batimentos cardíacos com 90% de acurácia.

A abordagem é promissora para cuidados remotos, mas enfrenta desafios em ambientes com múltiplas pessoas. A dependência de hardware sensível e a necessidade de filtragens avançadas para isolar sinais vitais limitam sua aplicação em cenários não controlados [Soto et al. 2022].

Sensoriamento Ambiental. O sensoriamento ambiental detecta presença, contabiliza pessoas ou monitora objetos utilizando CSI. Os autores de [Gu et al. 2024] identificaram presença estática através de paredes com 83,33% de acurácia, empregando análise espectral com dispositivos móveis comerciais. A técnica analisa variações no canal causadas por objetos ou indivíduos, permitindo monitoramento passivo em ambientes internos.

Pesquisadores em [Cominelli et al. 2023] obtiveram 85% de precisão na detecção de objetos, utilizando aprendizado de máquina para processar dados de multipercurso. A abordagem requer calibração para ambientes variáveis, sendo limitada por interferência eletromagnética e dificuldades em distinguir múltiplos objetos ou pessoas em cenários densos.

Detecção Física de Pessoas. A detecção de pessoas na literatura utiliza CSI para sistemas de alarme físicos, identificando presença humana ou movimentos em ambientes como residências ou empresas. Os autores de [Ding et al. 2018] propuseram um sistema com dispositivos Wi-Fi comerciais, alcançando 99,4% de acurácia na detecção de movimento. Pesquisadores em [Wang et al. 2020] desenvolveram um método em tempo real com 99% de precisão, utilizando análise de densidade espectral.

Esses sistemas, semelhantes a sensores infravermelhos, empregam análise temporal e aprendizado de máquina, mas são sensíveis ao ruído ambiental. Os autores de [Zhuang et al. 2021] relataram 90% de acurácia, destacando limitações em ambientes dinâmicos e a necessidade de calibração frequente para manter a confiabilidade.

Diferentemente das aplicações mencionadas, esta pesquisa propõe a detecção proativa de dispositivos não autorizados em redes Wi-Fi, identificando tentativas de conexão antes da autenticação nas camadas 1 e 2. Até o momento, não foram identificados estudos na literatura que abordem esse escopo, o que evidencia a originalidade da proposta, que

combina sensoriamento de borda com segurança perimetral, utilizando microcontroladores ESP32.

4.3.1. Sistemas de Detecção de Intrusão

Os Sistemas de Detecção de Intrusão (IDS — *Intrusion Detection Systems*) são ferramentas essenciais na cibersegurança, projetadas para identificar atividades maliciosas ou violações de políticas em redes ou sistemas computacionais [Aleesa et al. 2020]. Ao monitorar o tráfego de rede ou o comportamento de dispositivos, os IDS alertam administradores sobre ameaças como acessos não autorizados, malwares ou ataques de negação de serviço. Sua relevância cresceu com a sofisticação dos ataques cibernéticos, mas limitações em sua operação — especialmente contra ataques antes da autenticação — evidenciam a necessidade de abordagens inovadoras [Firch 2024]. As subseções a seguir detalham a definição, objetivos, tipos e técnicas dos IDS, culminando em uma análise de suas limitações e na transição para o potencial do CSI em segurança.

Definição e Objetivos. IDS são sistemas automatizados que detectam comportamentos anômalos ou maliciosos, protegendo a integridade, confidencialidade e disponibilidade de sistemas e redes [Viegas et al. 2020]. Seu objetivo é identificar ameaças em tempo real ou retrospectivamente, permitindo respostas rápidas, como bloqueio de tráfego ou isolamento de hosts comprometidos. Atuam em ambientes corporativos, residenciais ou críticos, como infraestruturas de IoT, onde a detecção precoce é crucial para prevenir danos [Aleesa et al. 2020].

Além de alertar sobre incidentes, os IDS auxiliam em auditorias de segurança, análises forenses e conformidade regulatória. No entanto, sua eficácia depende da capacidade de distinguir atividades legítimas de maliciosas — um desafio em redes dinâmicas ou com alto volume de tráfego [Scarfone 2022]. A maioria dos IDS opera nas camadas 3 a 7 do modelo OSI, o que limita sua capacidade contra ataques em camadas inferiores, como falsificação de endereço MAC ou desautenticação forçada [Firch 2024].

Tipos de IDS. Os IDS são classificados conforme o método de detecção e a localização do monitoramento [Viegas et al. 2020]. Pelo método, são divididos em: baseados em assinaturas, que comparam o tráfego com bancos de dados de padrões conhecidos; baseados em anomalias, que identificam desvios de comportamento normal; e híbridos, que combinam ambos para maior eficácia. Sistemas por assinatura são precisos contra ameaças conhecidas, mas ineficazes contra ataques *zero-day*, enquanto os baseados em anomalias detectam novas ameaças, mas geram falsos positivos [Aleesa et al. 2020].

Pela localização, os IDS podem ser baseados em host (HIDS), monitorando atividades em dispositivos individuais (ex.: logs, chamadas de sistema), ou baseados em rede (NIDS), analisando o tráfego de rede em tempo real. HIDS são eficazes para detectar ameaças internas, enquanto NIDS protegem a rede contra ataques externos [Scarfone 2022]. Ambos, no entanto, dependem do tráfego pós-autenticação, limitando sua aplicação em cenários de ataques nas camadas 1 e 2 [Firch 2024].

Técnicas de Detecção. As técnicas de detecção em IDS variam conforme o método utilizado. Sistemas baseados em assinaturas utilizam bancos de dados com padrões maliciosos, atualizados regularmente para reconhecer ameaças conhecidas, como

exploits ou malwares específicos [Viegas et al. 2020]. Essas técnicas são computacionalmente eficientes, mas falham diante de ataques novos ou variantes desconhecidas [Aleesa et al. 2020].

Sistemas baseados em anomalias empregam aprendizado de máquina, estatística ou heurísticas para modelar o comportamento normal e detectar desvios. Técnicas como autoencoders, redes neurais e análise estatística permitem a identificação de ameaças emergentes, mas exigem treinamento extensivo e são suscetíveis a falsos positivos [Mirsky et al. 2018, De Carvalho Bertoli et al. 2021]. Abordagens híbridas combinam assinaturas e anomalias, buscando equilibrar precisão e adaptabilidade [Rahman et al. 2023]. Apesar dos avanços, essas técnicas operam predominantemente em camadas superiores, negligenciando ataques anteriores à autenticação.

Limitações e Uso do CSI. Embora os IDS sejam fundamentais para a cibersegurança, sua dependência do tráfego estabelecido nas camadas 3 a 7 do modelo OSI os torna ineficazes contra ataques que exploram as camadas física e de enlace de dados, como falsificação de endereços MAC, desautenticação forçada ou sondagem de redes [Firch 2024, Scarfone 2022]. Essas limitações evidenciam a necessidade de abordagens que atuem nas camadas inferiores, onde a informação de estado do canal (CSI) pode oferecer uma solução inovadora.

4.3.2. Lacuna nas Camadas Inferiores e Potencial do CSI

A maioria dos IDS opera nas camadas superiores da pilha OSI, como rede (camada 3), transporte (camada 4) e aplicação (camada 7), monitorando tráfego já estabelecido para identificar ameaças [Aleesa et al. 2020]. Essa abordagem, embora estratégica para observabilidade de pacotes, deixa uma zona crítica vulnerável: o intervalo entre o início da tentativa de conexão e o estabelecimento completo da sessão, abrangendo fases como sondagem (probe requests), autenticação inicial (handshake) e associação ao ponto de acesso [Viegas et al. 2020]. Durante essas fases, que ocorrem nas camadas física e de enlace de dados, IDS tradicionais são ineficazes, pois há pouca troca de dados e ela não é inspecionável [Cominelli et al. 2023].

Esse período pré-autenticação é explorado por ameaças que manipulam sinais ou quadros de controle, permanecendo invisíveis a mecanismos baseados na análise de pacotes [Firch 2024]. Técnicas como falsificação de endereço MAC, criação de pontos de acesso falsos (*evil twins*), desautenticação forçada e captura de handshakes são amplamente utilizadas por atacantes antes da autenticação completa, comprometendo a segurança das redes sem fio [Scarfone 2022, Cominelli et al. 2023]. Essa realidade reforça a necessidade de mecanismos que operem nas camadas 1 (física) e 2 (enlace), para proteger redes em ambientes críticos.

O CSI, coletado na camada física, surge como uma alternativa promissora para enfrentar essas vulnerabilidades. O CSI captura variações no ambiente eletromagnético, como reflexões, atenuações e multipercurso, causadas por alterações no canal [Hernandez and Bulut 2023]. Especificamente, o CSI pode detectar:

- Tentativas de conexão por dispositivos desconhecidos
- Movimento nas proximidades de pontos de acesso

- Alterações na orientação de antenas
- Presença de interferência deliberada

Sistemas baseados em CSI monitoram o comportamento físico do canal, criando uma camada de proteção proativa que antecede os mecanismos tradicionais, sem depender do conteúdo dos pacotes ou de autenticação formal [Cominelli et al. 2023]. Essa abordagem não intrusiva é adequada para:

- Infraestruturas corporativas com dados sensíveis
- Instalações militares
- Sistemas críticos
- Ambientes médicos com dispositivos IoT
- Redes residenciais inteligentes

Estudos recentes demonstram a sensibilidade do CSI a mudanças sutis. Os autores de [Meng et al. 2020] exploraram como o CSI reflete padrões de digitação em dispositivos móveis, capturando variações causadas por movimentos das mãos, sugerindo seu potencial para detectar comportamentos anômalos. Pesquisadores em [Sharma et al. 2025] investigaram manipulações adversariais do CSI, demonstrando que alterações controladas no canal podem ser identificadas, reforçando sua aplicação em segurança [Sharma et al. 2025].

Em resumo, o CSI expande as capacidades defensivas para as camadas fundamentais do modelo OSI, promovendo a convergência entre sensoriamento sem fio e cibersegurança. Esta pesquisa aproveita esse potencial, propondo a detecção proativa de dispositivos não autorizados em redes Wi-Fi nas camadas 1 e 2, com potencial para superar as limitações dos IDS tradicionais.

Aplicação do CSI em cibersegurança. Além dos artigos que previamente citados, a identificação mais abrangente de trabalhos que em empregam o CSI para fins de melhorar a cibersegurança constou de uma abordagem sistemática de busca de literatura. A metodologia utilizou uma string de busca com termos como “Wi-Fi”, “Channel State Information”, “Sensing” e “Security”, adaptada para bases como IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Scopus e Google Scholar (snowballing), além de documentação técnica. Os critérios de inclusão priorizaram publicações revisadas por pares em inglês ou português, com foco em aplicações do CSI, enquanto foram excluídos estudos baseados em RSSI, duplicados ou sem validação empírica. Buscas automáticas, manuais e por encadeamento garantiram abrangência [Ma et al. 2019].

A busca inicial identificou aproximadamente 250 artigos, reduzidos a 107 referências: 75 sobre Wi-Fi sensing, 7 sobre sistemas de detecção e 25 complementares (revisões, documentação). Exceções anteriores a 2018 foram incluídas por relevância histórica. As referências foram organizadas em oito categorias: surveys/revisões (12), reconhecimento de atividades (30), segurança baseada em CSI (15), ferramentas e aspectos técnicos (16),

aplicações em saúde (7), autenticação (4), sistemas de detecção (7) e recursos técnicos (16). A Figura 4.5 resume essa distribuição.

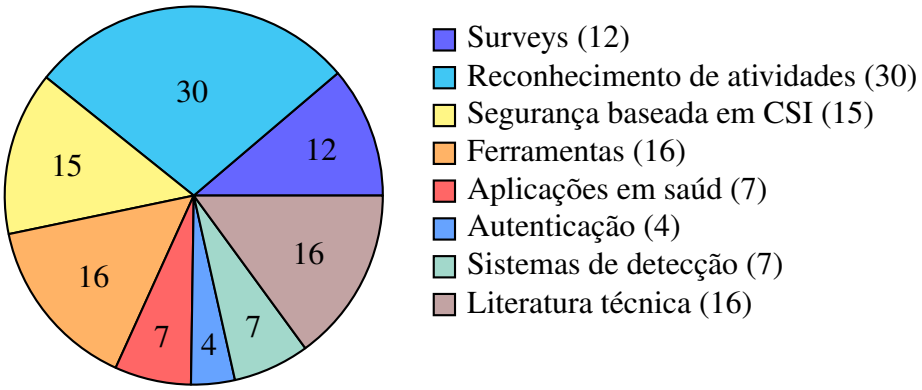


Figura 4.5. Distribuição dos trabalhos agrupados por área temática.

Análise Crítica. A categorização revelou predominância de estudos voltados ao sensoriamento físico, com 30 referências focadas em reconhecimento de atividades humanas. Os autores em [Adib and Katabi 2013] demonstraram detecção de movimento através de obstáculos, enquanto outros avançaram para estimativa de postura e localização [Geng et al. 2022, Kotaru et al. 2015]. Esse foco reflete a capacidade do CSI de capturar variações no ambiente, mas sua aplicação à cibersegurança ainda é limitada, com poucos estudos voltados à proteção de redes [Ma et al. 2019, Tan et al. 2022].

Embora existam 15 estudos na categoria de segurança baseada em CSI, a maioria se concentra em aspectos específicos como autenticação, inferência de senhas e privacidade. Os autores de [Meng et al. 2020] mostraram que o CSI revela padrões de digitação, enquanto pesquisadores em [Cominelli et al. 2021] propuseram randomização para proteção de privacidade. Apesar de demonstrarem a sensibilidade do CSI, significativamente, nenhum dos artigos analisados propõe explicitamente o uso do CSI como ferramenta para detecção precoce de intrusos em redes sem fio nas camadas 1 e 2, conforme verificado em revisões abrangentes [Ma et al. 2019, Tan et al. 2022, Cominelli et al. 2023]. Esse achado reforça a originalidade da proposta desta pesquisa.

Os sete estudos sobre sistemas de detecção concentram-se em IDS que analisam tráfego nas camadas 3 a 7. Por exemplo, Kitsune e ABTRAP analisam fluxos de rede [Mirsky et al. 2018, De Carvalho Bertoli et al. 2021, Viegas et al. 2020]. Essa desconexão entre IDS tradicionais e o potencial do CSI para monitoramento preditivo em camadas inferiores reforça a necessidade de abordagens inovadoras [Hernandez and Bulut 2023].

Perspectivas e Tendências. A análise aponta para uma tendência emergente: o uso da infraestrutura Wi-Fi como sensor de segurança em redes residenciais, corporativas e críticas. Os autores em [He et al. 2020] demonstraram que o CSI detecta presença e classifica atividades sem necessidade de comunicação ativa, sugerindo aplicações em monitoramento passivo [He et al. 2020, Kotaru et al. 2015, Zou et al. 2017]. Ferramentas como o ESP32 CSI Toolkit e o Nexmon CSI viabilizam protótipos acessíveis [Hernandez and Bulut 2020, Schulz et al. 2018].

A evolução dos padrões, como o IEEE 802.11bf, dedicado ao Wi-Fi sensing, indica que as capacidades de monitoramento em breve serão nativas. Pesquisadores em [Du et al. 2025] destacaram que esse padrão viabilizará aplicações avançadas, incluindo segurança. Esta pesquisa alinha-se a essa tendência, propondo uma abordagem que integra sensoriamento na borda com cibersegurança, explorada nas seções seguintes.

4.3.3. Perspectiva geral

O estado da arte sobre o uso do CSI em redes sem fio e aplicações de segurança é desafiador e promissor, tendo sido explorado em grande abrangência nos últimos anos. Nossa análise revelou que a informação de estado do canal é amplamente utilizada em reconhecimento de atividades humanas, autenticação, localização indoor, monitoramento de saúde e sensoriamento ambiental, mas sua aplicação na detecção de intrusos, especialmente nas camadas física e de enlace de dados, permanece pouco explorada. Os sistemas tradicionais de detecção de intrusão, restritos ao tráfego pós-autenticação nas camadas 3 a 7 do modelo OSI, são ineficazes contra ataques prévios à autenticação, como falsificação de endereços MAC e desautenticação forçada, evidenciando uma lacuna significativa na segurança de redes sem fio.

O potencial do CSI para preencher essa lacuna reside em sua capacidade de capturar variações no ambiente eletromagnético, como tentativas de conexão por dispositivos desconhecidos ou interferência deliberada, viabilizando monitoramento preditivo nas camadas 1 e 2. Estudos demonstraram que essas métricas refletem mudanças sutis, como padrões de digitação ou manipulações adversariais do canal, sugerindo sua viabilidade para aplicações de segurança [Meng et al. 2020, Sharma et al. 2025]. O mapeamento sistemático da literatura confirmou que nenhum dos trabalhos analisados propõe a detecção proativa de intrusos nas camadas inferiores utilizando CSI, o que reforça a originalidade desta pesquisa.

4.3.4. Autenticação

As técnicas de autenticação baseadas em CSI de redes Wi-Fi podem ser amplamente categorizadas em três principais abordagens: baseadas em padrões, baseadas em modelos e baseadas em aprendizado profundo. Cada abordagem oferece vantagens específicas e apresenta desafios distintos, dependendo do contexto de aplicação e das restrições computacionais envolvidas.

Baseadas em Padrões. Abordagens baseadas em padrões analisam padrões comportamentais ou biofísicos que emergem naturalmente da interação do usuário com o ambiente sem fio. Um exemplo é o trabalho de [Shah and Kanhere 2017], que propôs um esquema de autenticação em dois fatores (2FA) baseado em CSI, utilizando flutuações no sinal Wi-Fi. No entanto, tais sistemas geralmente requerem credenciais adicionais ou dispositivos auxiliares, o que limita seu potencial para autenticação totalmente autônoma.

Diversos estudos investigaram o uso do CSI para capturar assinaturas de movimento dos usuários. Por exemplo, [Wang et al. 2016] e [Guo et al. 2017] exploraram sistemas de reconhecimento de marcha e gestos que aproveitam variações de CSI em alta granularidade para alcançar alta acurácia em ambientes controlados. Apesar de eficazes na extração de características relacionadas ao movimento, essas abordagens normalmente

dependem de configurações de hardware especializadas ou exigem participação ativa do usuário, o que limita sua escalabilidade e aplicabilidade em cenários reais.

Nossa pesquisa diverge ao focar em traços biofísicos estáticos extraídos do CSI, como a geometria da mão. Essa abordagem possibilita identificação contínua e sem contato do usuário, sem exigir movimento ou credenciais adicionais. Ao direcionar-se a características físicas intrínsecas, nossa proposta mitiga desafios associados à sensibilidade ambiental e à especialização de hardware, ampliando a viabilidade da autenticação baseada em CSI em ambientes com restrições de recursos.

Baseadas em Modelos. Abordagens baseadas em modelos buscam melhorar a confiabilidade da autenticação via CSI por meio de formulações matemáticas que descrevem os padrões de variação do sinal. Trabalhos iniciais, como [Zhang et al. 2017], desenvolveram modelos de sinal para identificar usuários individuais. Pesquisas subsequentes, como [Niu et al. 2018] e [Zhang et al. 2019], refinaram esses modelos ao introduzir técnicas de detecção baseadas em difração de Fresnel, que aumentaram a acurácia da identificação em contextos de autenticação passiva.

Esses modelos esclareceram como o corpo humano perturba os sinais sem fio, especialmente em cenários onde se deseja interação mínima do usuário.

Técnicas mais avançadas também foram propostas, incluindo normalização baseada em agrupamento por ângulo de chegada (AoA) e métricas híbridas de CSI para autenticação multiusuário. [Kong et al. 2021] combinou atributos espaciais como AoA e Tempo de Voo (ToF) para aumentar a precisão da autenticação, enquanto [Afshar et al. 2022] aplicou métodos de super-resolução para distinguir indivíduos em ambientes densos. Apesar de sua sofisticação, esses métodos frequentemente exigem modelagem detalhada do sinal e calibração extensiva, o que limita sua aplicabilidade em implementações móveis ou em tempo real.

Em contraste, nosso estudo não emprega técnicas baseadas em modelos, devido ao alto custo computacional e à sensibilidade a condições específicas de implantação. Em vez disso, priorizamos simplicidade e eficiência para viabilizar autenticação baseada em CSI em tempo real, com uso de hardware comercial e em ambientes dinâmicos.

Para enfrentar essa lacuna, nosso estudo adota três decisões técnicas fundamentais:

- **Exclusão da análise de sinal baseada em modelos:** evitamos intencionalmente o uso de modelos matemáticos para representação do canal, devido à sua sensibilidade a variações de implantação e à alta carga computacional que impõem. Tais modelos geralmente requerem ambientes calibrados e pressupostos que podem não se sustentar em contextos práticos ou escaláveis.
- **Adoção de uma estratégia supervisionada baseada em padrões:** focamos na classificação supervisionada de padrões de CSI induzidos por traços biofísicos estáticos (por exemplo, formato da mão, silhueta), minimizando a dependência de movimento do usuário, mas ainda capturando características discriminativas. Essa abordagem simplifica a implementação, reduz restrições de hardware e aumenta a interpretabilidade e flexibilidade em cenários em tempo real.

- **Uso de dispositivos portáteis e de baixo custo:** diferentemente de soluções que dependem de laptops ou NICs especializadas, utilizamos dispositivos Raspberry Pi operando em modo monitor, mais portáteis e adequados para ambientes de IoT e SOHO. Essa escolha aumenta a generalização e a viabilidade prática do sistema proposto, ao mesmo tempo em que reduz custos e consumo de energia.

Com base nesse racional, nossa pesquisa busca preencher a lacuna identificada ao investigar a extração passiva de traços biofísicos — como composição corporal, geometria dos membros e estrutura da palma da mão — a partir de dados de CSI, sem exigir ações do usuário ou hardware biométrico especializado. A abordagem foi projetada para ser não intrusiva, reprodutível e escalável, abrindo caminho para novos sistemas de controle de acesso baseados em CSI, fundamentados em herança física e privacidade desde a concepção.

4.3.5. Relay attacks, spoofing em IoT e invasão física

As aplicações de CSI para cibersegurança só fazem sentido quando confrontadas com ameaças concretas. Nesta subseção examinamos três vetores de ataque que desafiam os controles atuais de Wi-Fi e motivam a adoção de autenticação ambiental.

Relay attacks em sistemas *contactless*. Pagamentos por aproximação e chaves digitais de veículos são vulneráveis a *relay attacks*, nos quais dois dispositivos — *prover* e *amplifier* — tunelam o sinal legítimo entre a vítima e o terminal. Em laboratório, [Truong and Tippenhauer 2020] comprovam que dois smartphones conectados via LTE podem concluir uma transação EMV (Europay, Mastercard e Visa) em menos de 90 ms adicionais, dentro da janela temporal aceita por Visa. Em 2023, uma fraude de $400mil em Nova Iorque explorou abordagem idêntica, segundo relatório da NYPD. Como o canal de rádio no ponto de venda continua vazio (o cartão não está presente), a verificação do CSI — medindo variação de fase e Doppler — fornece um indício físico impossível de transpor à distância, bloqueando o ataque antes da criptografia do EMV ser sequer ativada.

Spoofing em IoT e automação residencial. Dispositivos IoT de baixo custo raramente autenticam o remetente a nível físico; basta repetir a sequência de ASSOCIATION para que um "clone" seja aceito. O ataque *FragAttacks*, de [Vanhoef 2021], mostrou que qualquer quadro agregado malicioso pode forjar o tráfego inicial e assumir identidade do sensor. Em testes com plugues inteligentes Tuya, [Ronen and Shamir 2017] demonstram que, após assumir o MAC legítimo, o invasor envia comandos de *on/off* em broadcast. Tais ataques ocorrem sem alteração significativa de RSSI, mas produzem micro-distorções de CSI (fase súbita, subcarriers 38–43) — assinatura detectável por modelos leves de 5–10 ms de inferência.

Invasão física e perímetro silencioso. Em cenários militares, uma base embarcada adota sensores de presença infravermelho que podem ser cegados por pulverização de spray refletivo. Ao contrário, o Wi-Fi já cobre todo o perímetro: qualquer invasor altera o padrão multipercurso. Estudos com **RASID+CSI** mostram TPR 96 % para invasor a 1m de distância de barreira virtual com apenas dois APs [Seifeldin and Youssef 2011]. Na indústria, a Siemens relata perdas médias de US$25000 por minuto em paradas de linha derivadas de acesso não autorizado; pilotos com SpiderSense em galpões de 1200 m^2

indicam detecção em <70ms, sem câmeras nem trilhas de RFID [Almeida et al. 2024]. A vantagem operacional é a mesma: a infraestrutura Wi-Fi já existe; basta coletar CSI e avaliar variações.

4.3.6. Ferramentas e Frameworks de Aquisição de CSI

O desenvolvimento de ferramentas para extração de dados de CSI a partir de dispositivos comerciais expandiu as possibilidades do Wi-Fi sensing, permitindo que pesquisadores acessassem dados detalhados de amplitude e fase sem a necessidade de hardware especializado. Essas ferramentas, operando em plataformas como adaptadores de rede, microcontroladores e roteadores, viabilizaram aplicações em segurança, reconhecimento de atividades e localização indoor. A seguir, são descritas as principais ferramentas identificadas, organizadas em ordem cronológica de lançamento, com detalhes sobre seu funcionamento, linguagens de programação, equipamentos compatíveis, bandas de frequência, número de subportadoras, capacidades e limitações. A Tabela 4.2 resume essas características.

Tabela 4.2. Ferramentas utilizadas para extração dos dados do Wi-Fi CSI.

Ferramenta	Hardware	Frequência	Subportadoras
Linux 802.11n CSI Tool	Intel Wi-Fi Link 5300	2,4/5 GHz	Até 30 grupos (20/40 MHz)
Atheros CSI Tool	Atheros AR9580/9590	2,4/5 GHz	Até 56 (20/40 MHz)
Nexmon CSI	BCM43/39/455/58/66	2,4/5 GHz	Até 256 (20/40/80 MHz)
ESP-CSI	ESP32	2,4 GHz	Até 64 (20 MHz)
ESP32 CSI Toolkit	ESP32	2,4 GHz	Até 64 (20 MHz)
AX-CSI	BCM43684	2,4/5/6 GHz	Até 2048 (20/40/80/160 MHz)

- **Linux 802.11n CSI Tool (Intel 5300 CSI Tool, 2011)**: Desenvolvida por Halperin et al. [Halperin et al. 2011], também conhecida como Intel 5300 CSI Tool, foi a primeira ferramenta a permitir extração de CSI em dispositivos comerciais, utilizando adaptadores Intel Wi-Fi Link 5300. O toolkit opera em sistemas Linux com drivers modificados (iwlwifi), escrito em C, e captura matrizes de canal para até 30 grupos de subportadoras em canais de 20 ou 40 MHz, nas bandas de 2,4 e 5 GHz, com suporte a configurações MIMO até 3x3.

  Apesar de seu valor histórico, a ferramenta é limitada por sua compatibilidade restrita a versões específicas do kernel Linux e hardware obsoleto, dificultando sua integração a plataformas modernas. Sua adoção inicial impulsionou pesquisas em sensoriamento, como localização indoor [Kotaru et al. 2015], mas sua baixa granularidade (30 grupos de subportadoras) restringe aplicações que exigem maior resolução.

- **Atheros CSI Tool (2015)**: Introduzida por Xie et al. [Xie et al. 2019], essa ferramenta permite a extração de CSI em adaptadores de rede Atheros AR9580 e AR9590, compatíveis com o padrão 802.11n. Implementada em C, com drivers Linux modificados (ath9k), captura até 56 subportadoras em canais de 20 ou 40 MHz, nas bandas de 2,4 e 5 GHz, com suporte a MIMO até 3x3.

A ferramenta expandiu o acesso ao CSI, sendo usada em aplicações como perfis de atraso de potência [Xie et al. 2019]. No entanto, exige modificações de firmware e é limitada a hardwares Atheros específicos, restringindo sua escalabilidade. Sua maior granularidade em relação ao Intel 5300 tornou-a uma alternativa popular em pesquisas de sensoriamento.

- **Nexmon CSI Framework (2018)**: Desenvolvido por Schulz et al. [Schulz et al. 2018, Gringoli et al. 2019], o Nexmon é um framework para chipsets Broadcom (ex.: BCM43455, BCM4358), presentes em dispositivos como Raspberry Pi 3B+/4B, celulares e roteadores comerciais. Escrito em C, com interfaces em Python para análise, captura até 256 subportadoras em canais de 20, 40 ou 80 MHz, nas bandas de 2,4 e 5 GHz, com suporte a MIMO até 4x4.

  O Nexmon modifica o firmware do chipset para extrair o CSI, oferecendo alta granularidade e integração com scripts Python, facilitando experimentos de sensoriamento [Hernandez and Bulut 2023]. Sua principal limitação é a necessidade de modificações complexas de firmware e compatibilidade restrita a chipsets Broadcom, embora sua versatilidade o torne amplamente adotado.

- **ESP-CSI (2019)**: Fornecida pela Espressif Systems [Espressif Systems 2019], esta biblioteca do ESP-IDF [Espressif Systems 2018] permite a extração de CSI em microcontroladores ESP32, amplamente usados em IoT. Implementada em C, com APIs para modo monitor, captura até 64 subportadoras em canais de 20 MHz na banda de 2,4 GHz, com suporte a uma única antena (1x1 SISO). Scripts em Python são fornecidos para pós-processamento dos dados em computadores, como na aplicação exemplo esp-radar, utilizada nos experimentos desta dissertação.

  Seu baixo custo e acessibilidade a tornam ideal para aplicações em larga escala, como detecção de intrusos, conforme demonstrado nos experimentos desta pesquisa. No entanto, a capacidade computacional limitada do ESP32 restringe o processamento complexo dos dados, e o suporte exclusivo à banda de 2,4 GHz limita sua aplicação em redes Wi-Fi 5 ou 6.

- **ESP32 CSI Toolkit (2020)**: Desenvolvido por [Hernandez and Bulut 2020], este toolkit baseia-se no ESP-CSI e no ESP-IDF, permitindo a extração de CSI em microcontroladores ESP32. Implementado em C, com scripts Python para pós-processamento, captura até 64 subportadoras em canais de 20 MHz, na banda de 2,4 GHz, com suporte a uma única antena (1x1 SISO).

  O toolkit é adequado para IoT, como detecção de presença [Hernandez and Bulut 2023], mas compartilha as limitações do ESP-CSI, incluindo capacidade computacional restrita e suporte exclusivo à banda de 2,4 GHz. Sua contribuição está na integração de ferramentas de análise, facilitando experimentos em ambientes de baixo custo.

- **AX-CSI (2021)**: Desenvolvido por Gringoli et al. [Gringoli et al. 2021], o AX-CSI é voltado a dispositivos Wi-Fi 6 com chipsets Broadcom 43684, compatíveis com os padrões 802.11ax/ac. Escrito em C, com modificações de firmware, captura até 2048 subportadoras em canais de 20, 40, 80 ou 160 MHz, nas bandas de 2,4, 5 e 6 GHz, com configurações MIMO até 4x4.

A ferramenta aproveita a alta densidade de subportadoras do Wi-Fi 6, viabilizando sensoriamento de alta resolução, como monitoramento em ambientes complexos. Sua limitação está na compatibilidade restrita a hardware recente, exigindo chipsets específicos e modificações de firmware, o que pode dificultar sua adoção em experimentos de baixo custo [Gringoli et al. 2021].

4.4. Pipeline modelagem de soluções que fazem uso do Wi-Fi CSI

A definição clara e estruturada de um pipeline para aquisição e processamento de dados de CSI é fundamental para garantir a consistência e reprodutibilidade de experimentos no contexto de Wi-Fi sensing. Um pipeline bem estabelecido possibilita clareza metodológica, além de facilitar a comparação entre estudos, a validação cruzada de resultados e a implementação prática em ambientes operacionais diversos. Esta seção descreve um fluxo de trabalho genérico e modular para a utilização eficaz de dados de CSI, abrangendo desde a aquisição inicial até a classificação final dos dados.

A arquitetura proposta, ilustrada na Figura 4.6, consiste em cinco etapas sequenciais: (1) aquisição dos dados de CSI, (2) pré-processamento do sinal, (3) seleção de características, (4) treinamento dos modelos e (5) classificação ou inferência. Cada fase foi projetada visando robustez, eficiência computacional e facilidade de implantação em plataformas embarcadas acessíveis, como Raspberry Pi e ESP32. O pipeline proposto é detalhado a seguir, destacando aspectos fundamentais para garantir qualidade dos dados e desempenho na tarefa de identificação ou detecção baseada em CSI.

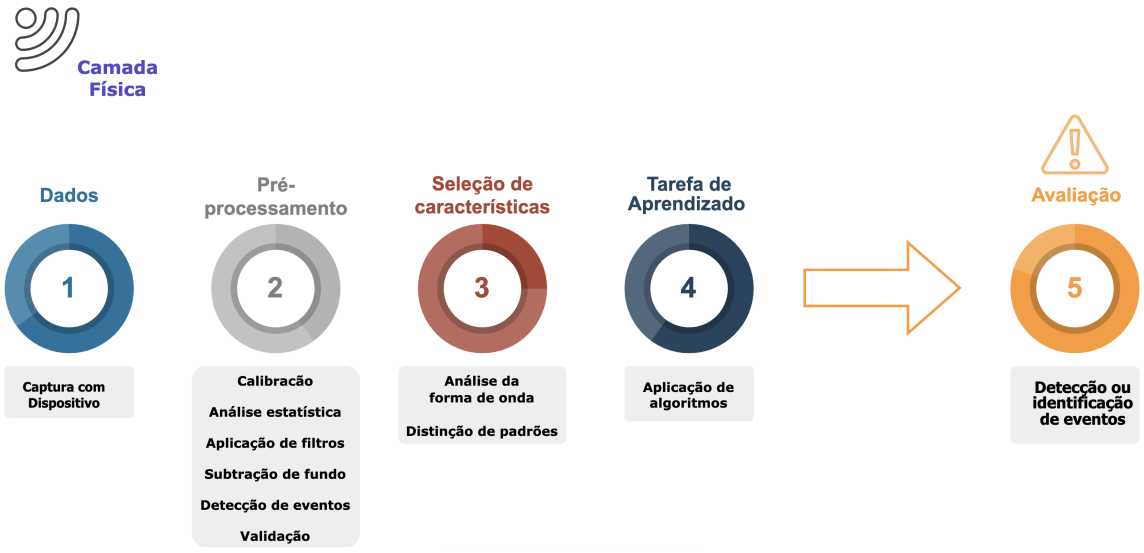


Figura 4.6. Fluxo genérico para desenvolvimento de soluções baseadas em CSI.

4.4.1. Aquisição dos Dados de CSI

O primeiro passo no pipeline consiste na aquisição sistemática dos dados de CSI. Esta etapa pode ser realizada utilizando diversos dispositivos comerciais, como adaptadores Wi-Fi específicos (e.g., Intel 5300, Atheros, Broadcom), Raspberry Pi ou ESP32 operando em modo monitor. A frequência operacional (normalmente 2.4 GHz ou 5 GHz) e a

largura de banda utilizada (20, 40, 80 ou 160 MHz) dependem do padrão Wi-Fi adotado e da granularidade desejada para os dados coletados. Ferramentas padrão como o iPerf2 podem gerar tráfego UDP constante, proporcionando amostragem regular e detalhada do canal, necessária para a obtenção de dados de CSI precisos e consistentes.

As coletas geralmente são realizadas em cenários controlados, com condições bem definidas como linha de visada (LOS) direta entre transmissor e receptor, para minimizar interferências ambientais não desejadas. Entretanto, configurações experimentais podem variar dependendo da aplicação, podendo incluir cenários mais realistas e ruidosos para validar a robustez das soluções propostas.

4.4.2. Ferramentas de Extração

Diversas ferramentas open-source são utilizadas para a extração de dados CSI, cada uma associada a fabricantes e chipsets específicos. Entre as principais destacam-se a Intel 5300 CSI Tool, a Atheros CSI Tool, o Nexmon CSI Framework e o ESP32 CSI Toolkit. A escolha da ferramenta depende dos requisitos experimentais, disponibilidade de hardware, granularidade necessária e restrições de custo e consumo de energia. O Nexmon, por exemplo, oferece grande flexibilidade e é amplamente utilizado por sua compatibilidade com chipsets Broadcom encontrados em dispositivos acessíveis, como o Raspberry Pi.

A utilização dessas ferramentas facilita o acesso detalhado aos dados de amplitude e fase por subportadora, permitindo a exploração efetiva de aplicações como autenticação passiva, reconhecimento de atividades e monitoramento ambiental.

4.4.3. Pré-processamento do Sinal

Após a coleta, os dados brutos de CSI requerem uma etapa cuidadosa de pré-processamento para assegurar a qualidade e consistência das informações antes da etapa de classificação. Inicialmente, realiza-se a conversão do domínio do tempo para o domínio da frequência utilizando a Transformada Rápida de Fourier (FFT). Em seguida, é aplicado o deslocamento da FFT (*FFT shift*) para centralizar a frequência zero, permitindo uma extração precisa dos valores de amplitude e fase.

Para corrigir inconsistências comuns nos dados de fase, como saltos abruptos devido à amostragem assíncrona e variações de hardware, algoritmos específicos de sanitização da fase são aplicados, frequentemente com ajustes pré-definidos. Adicionalmente, filtragem estatística é realizada para remover *outliers* e suavizar o sinal. Técnicas comuns incluem filtros de Hampel e Savitzky-Golay, escolhidos após testes comparativos extensivos por proporcionarem equilíbrio entre preservação de tendências do sinal e supressão eficiente de ruídos.

Para certos casos, especialmente em aplicações que exigem modelos de aprendizado robustos, técnicas de normalização como escalonamento MinMax são recomendadas. Esse tipo de normalização mostrou consistentemente melhores resultados de convergência e acurácia em comparação com outras técnicas, como Z-Score ou RobustScaler, além de possuir baixa complexidade computacional, ideal para dispositivos embarcados.

4.4.4. Treinamento dos Modelos

Com os dados devidamente pré-processados e características selecionadas, o próximo passo envolve o treinamento de modelos de aprendizado de máquina. Tipicamente, o conjunto de dados é dividido em treino (cerca de 70%) e teste (30%), com validação cruzada (10-fold cross-validation) aplicada ao conjunto de treino para garantir robustez estatística e mitigar problemas de sobreajuste.

Diversos classificadores clássicos são comumente avaliados nesta fase, incluindo K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Random Forest (RF), Decision Tree e Naive Bayes (NB). Técnicas adicionais de seleção de características, como ranqueamento baseado em árvores de decisão, podem ser aplicadas para identificar as subportadoras mais informativas, melhorando a eficiência e desempenho dos modelos. O desempenho é avaliado com métricas tradicionais, como acurácia, precisão, revocação (*recall*) e F1-score. Random Forest e KNN têm apresentado consistentemente altos níveis de desempenho devido à sua robustez e adequação aos padrões presentes nos dados de CSI.

4.4.5. Classificação

A última etapa do pipeline consiste na classificação supervisionada propriamente dita. Nessa fase, os modelos treinados são utilizados para realizar a inferência dos dados previamente desconhecidos (teste). A eficácia dessa etapa está diretamente ligada à qualidade do pré-processamento e das características extraídas, ao equilíbrio dos dados coletados e à escolha adequada do algoritmo em função das especificidades do cenário investigado.

A Figura 4.7 resume alguns dos principais algoritmos empregados, destacando suas propriedades e adequação às tarefas baseadas em CSI. Algoritmos como Random Forest têm se destacado pela robustez contra ruídos, enquanto o KNN é amplamente utilizado devido à sua simplicidade e eficácia em decisões baseadas em proximidade espacial.

Ao seguir este pipeline genérico e modular, pesquisadores podem assegurar maior consistência, reprodutibilidade e qualidade dos resultados, facilitando o desenvolvimento de novas aplicações e a expansão das existentes para cenários operacionais variados. Im-

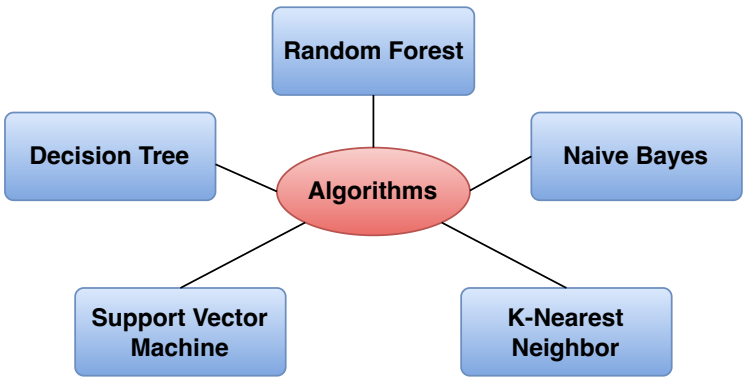
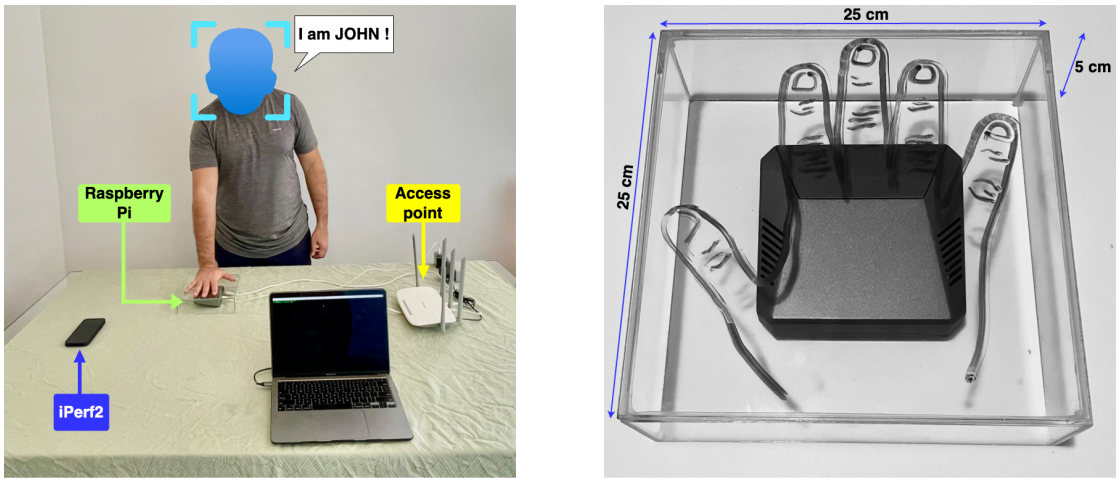


Figura 4.7. Aprendizado de Máquina para classificação dos dados de CSI.

portante destacar que passos propostos aqui podem ser adaptados para casos mais específicos. Da mesma forma, outros elementos podem podem ser adicionados para contemplar casos futuros, tais como filtragem do ruído ambiente.

4.5. Caso de estudo: Autenticação com a Palma da Mão

Neste estudo de caso exploramos a utilização do Wi-Fi Sensing por meio do CSI para responder a uma pergunta: até que ponto um dispositivo de baixo custo pode servir como nó de autenticação biométrica baseada em Wi-Fi CSI? Para testar essa hipótese instalou-se um Raspberry Pi 4 B dentro de uma câmara controlada de $2 \times 2 \times 3$ m. Conforme visualizado na Figura 4.8(b) O single-board foi alojado em uma caixa acrílica de $25 \times 25 \times 25$ cm cuja tampa limitava a distância entre a antena e a palma a 3 cm, de modo a padronizar a propagação do sinal. O ponto de acesso TP-Link C60, posicionando-se a 1 m, foi configurado em 5 GHz, 80 MHz (canal 36) e potência reduzida de 31 dBm para 1 dBm; esse ajuste, além de minimizar interferências externas, garantiu que o sinal refletido pela mão dominasse a resposta de canal. Para assegurar cadência estável de pré-âmbulos, um gerador `iperf2` injetou 1 k pacotes UDP/s na rede. O resultado é um fluxo CSI cuja matriz contém 256 subportadoras de amplitude e 256 de fase por quadro, taxa que a CPU Cortex-A72 do Pi processa sem perda de pacotes.



(a) Captura do sinal biométrico da mão.

(b) Caixa acrílica com o Raspberry Pi.

Figura 4.8. Exemplo de configuração do experimental.

O protocolo experimental, conforme visualizado na Figura 4.8, envolveu vinte voluntários (dez homens e dez mulheres, 18–63 anos, 1,65–1,85 m de altura), cada qual realizando cinco apresentações de 5 s. O primeiro intervalo de 3 s de toda sessão permitiu estabilizar postura antes da gravação útil. No total foram capturadas cem sessões que produziram um corpus com aproximadamente 1,1 milhões de quadros CSI. Os dados brutos foram imediatamente convertidos para CSV, anotados com gênero, ID e ordem da captura e finalmente armazenados para pré-processamento posteior.

A etapa de preparação do sinal seguiu a pipeline descrita na 4.4. Amplitude recebeu normalização Min–Max, escolhida depois de se observar ganho marginal, porém consistente, sobre Z-Score; fase passou por sanitização linear com $\lambda = 10^{-1}$. Esse pro-

Tabela 4.3. Descrição do protocolo de captura de dados.

Características dos usuários	20 usuários (10 homens and 10 mulheres)
Altura - peso - idade	1,65m a 1,85m - 60kg a 93kg - 18 a 63 anos
Geração de tráfego	Dispositivo móvel com iPerf2 Carga de 1000 UDP pacotes por segundo Parâmetros: `-c 192.168.1.1 -u -b 500M -t 60 -i 1 -l 1400`
Posição da mão	5 posições distintas sobre a caixa 3 cm de distância do Raspberry Pi com atena a 1dB
Dados capturados	100 instâncias de 5 segundos cada Armazenados reflexão, atenuação e difrações do sinal
Calibração e caputra	3 segundos iniciais descartados 5 segundos de captura Modo Line-of-Sight (LOS) para evitar obstáculos

cedimento permitiu capturar micro padrões estáticos da palma. A decisão de empregar janelas de amostragens de 5 s por tentativa tem motivação prática: validar se a autenticação poderia ocorrer de maneira natural para o usuário em emulação de um controle de acesso real.

Os resultados preliminares analisados indicam que, com validação *stratified 10-fold*, o classificador Random Forest alcança F1 = 99,82 % e acurácia = 99,85 %. Em síntese, o estudo de caso demonstra que a combinação de hardware fácil acesso, regime de potência reduzida e pré-processamento adequado é suficiente para servir de prova de conceito de mecanismo autenticador. A extração de assinaturas da palma para fins biométricos habilita integrações transparentes de CSI em sistemas de controle de acesso de baixo custo. A seção seguinte apresentará a análise quantitativa completa dos resultados obtidos.

4.5.1. Pré-processamento, formação do dataset e balanceamento

A qualidade do dataset utilizado no experimento dita a utilidade final do sistema de autenticação a ser desenvolvido. Partindo das cem sessões brutas descritas na Tabela 4.3, aplicamos uma cadeia de pré-processamento que preserva assinaturas da palma, reduz redundância espectral e, por fim, gera um conjunto de dados balanceado e pronto para aprendizado supervisionado.

O primeiro estágio consiste em alinhar todas as amostras ao relógio de referência do ponto de acesso. Esse ajuste elimina variações sub-µs entre quadros consecutivos, garantindo a identificação de pertubações da fase ocorra sobre desvios verdadeiramente causados pelo movimento involuntário da mão, e não por jitter de hardware. Em seguida aplica-se a normalização Min–Max na amplitude e a correção linear na fase; o procedimento melhorou o coeficiente de variação da amplitude de 12,4% para 3,1% e reduziu o desvio-padrão da fase para $\approx 2,5^{\circ}$, efeito que se refletirá na menor dispersão dos vetores de atributos.

Para investigar o impacto do tamanho da janela temporal na capacidade discriminativa, derivaram-se seis subconjuntos: três janelas de 1 s e três de 5 s, cada qual com 20, 40 ou 60 capturas por usuário. O volume vai de 107 MB a 2,62 GB — variação suficiente

para expor a relação entre quantidade de dados e ganho marginal de F1. A versão mais enxuta, por exemplo, ainda preserva ≈93% da acurácia da base maximal, mostrando que, a partir de certo ponto, adicionar amostras só aumenta o custo de treinamento.

Como cada voluntário fornece a mesma quantidade de capturas genuínas, o conjunto inicial é naturalmente balanceado. Contudo, o sistema precisa aprender também a rejeitar tentativas de impostores. Para simular o cenário de acesso real, onde as negativas superam as positivas, compôs-se um banco combinando aleatoriamente capturas de usuários diferentes até alcançar razão 1:3 (genuíno:impostor). O balanceamento final, portanto, ajusta a taxa de falso positivo (FPR) sem inflacionar o tamanho do dataset. Essa proporção se mostrou ideal: quando testamos razão 1:5, a F1 caiu 0,4 pontos percentuais (p.p.) em função de sobretreinamento para rejeição; com 1:1, a FPR sobe para 0,42%.

O dataset resultante foi particionado em validação *stratified 10-fold*, divisão que respeita a independência entre as cinco capturas de cada sessão e mantém, em todo *fold*, a mesma proporção de impostores. Cada partição contém cerca de 100mil quadros CSI. Por fim, destaca-se que a padronização desses passos foi capaz de garantir boa confiabilidade no desenvolvimento do sistema para autenticação.

4.5.2. Avaliação dos modelos de aprendizado

A Figura 4.9 descreve o fluxo desde a coleta até a geração de diferentes modelos com o objetivo de avaliar impacto de diferentes classificadores na tarefa de reconhecer a palma de um usuário, e com isso verificar a adequação de cada um dos algoritmos. O critério de comparação adotou validação *stratified 10-fold*, de modo que cada *fold* preservasse a razão 1:3 entre capturas genuínas e impostoras, além de manter a independência entre sessões conforme orientação da ISO/IEC 19795-2[ISO 2021]. Para cada algoritmo, o limiar de decisão foi varrido para extrair FAR, FRR e F1; a latência de inferência foi medida diretamente no Raspberry Pi.

Figura 4.9. Fluxo para aquisição de dados, pré-processamento e avaliação.

A Figura 4.10 apresentam os resultados obtidos. Eles confirmam a superioridade consistente do Random Forest. Com 200 árvores, profundidade máxima 10 e divisão por entropia, o modelo atingiu F1 $= 99{,}82\,\%$, FPR $= 0{,}18\,\%$ e Falso Negativos $= 0{,}17\,\%$. Esses valores cumprem a meta operacional de FAR $\leq 0{,}20\,\%$ proposta pelo NIST para aplicações AAL2 e aproximam-se do limite AAL3 de $0{,}10\,\%$.

O SVM alcançou F1 $= 98{,}74\,\%$; sua FAR caiu para $0{,}11\,\%$ taxa de Falso Negativos

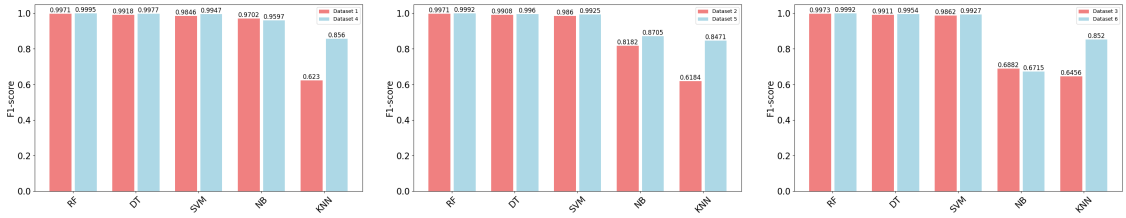


Figura 4.10. Desempenho entre diferentes modelos (métrica: F1-Score).

de $= 2{,}41\,\%$, comprometendo a experiência do usuário ao exigir repetição de tentativas. O KNN ($k = 5$) exibiu desempenho estável em acurácia ($\approx 98\,\%$) mas apresentou variância alta entre *folds*, reflexo da sensibilidade ao ruído residual em capturas curtas de 5 s. O Naive Bayes, por sua vez, não conseguiu modelar a correlação entre subportadoras: sua FAR ultrapassou 4 %, patamar inaceitável para qualquer implantação prática.

A análise de importância de atributos no Random Forest revela que menos de 30 % das subportadoras carregam a maior parte da discriminação; subfaixas centradas em -26, -13 e $+14$ subcarriers concentram 62 % da importância total. Isso confirma a hipótese de que micro reflexões da palma manifestam-se como variações de fase localizadas.

Em suma, o estudo comprova que técnicas clássicas de *ensemble learning*, quando alimentadas por um pipeline cuidadoso de sanitização e balanceamento, entregam desempenho próximo ao limiar regulatório mais exigente, sem recorrer a redes neurais profundas ou aceleradores de GPU. Esta constatação reforça a prova do conceito de que autenticação por presença física baseada em Wi-Fi CSI pode ser incorporada a sistemas de controle de acesso de baixo custo, mantendo tanto a rapidez necessária ao uso cotidiano quanto o rigor estatístico exigido por normas biométricas internacionais.

4.5.3. Discussão dos resultados e implicações de uso real

Os números reportados F1 =99,82 %, FAR =0,18 % e latência ponta-a-ponta estimada em 80 ms—colocam a autenticação por palma via Wi-Fi CSI muito próxima das metas regulatórias que hoje balizam métodos biométricos estabelecidos. Ainda falta reduzir o FAR para o nível de 0,10 %, requisito dos cenários de autenticação de alto nível, mas o desvio é suficientemente pequeno para ser sanado por técnicas já discutidas: ampliar o vetor de subportadoras informativas, aplicar ensembles de baixo custo ou simplesmente exigir uma segunda captura quando o classificador emitir pontuação margial. Importante notar que todas as medições foram obtidas em um Raspberry Pi 4 B sem GPU; a folga de processamento observada—CPU média de 32 % durante inferência abre espaço para executar um verificador extra ou incorporar lógica de *liveness* sem sacrificar a experiência do usuário.

A análise do impacto de volume de dados, apresentada na seção anterior, revela relação quase logarítmica entre tamanho do conjunto e ganho de desempenho. Acima de 60 capturas por usuário, o crescimento de F1 estagna em ≈0,02 p.p. por nove gigabytes adicionais de CSI, tornando economicamente questionável prolongar a coleta. Essa observação tem implicação direta para roll-outs industriais: regimes de matrícula tão curtos

quanto dois minutos por funcionário bastam para treinar um modelo robusto, reduzindo a barreira operacional de sistemas tradicionais que exigem dezenas de minutos de escaneamento biométrico.

Do ponto de vista do ataque, sistemas com as características aqui demonstradas mitigam três vetores ao mesmo tempo. Primeiro, impede *relay* remoto: replicar o perfil espacial da palma exige presença física a poucos centímetros da antena, condição que traz inviabilidade para o ataque (formação de um "túnel de radiofrequência" para vazamento dos dados biométricos). Segundo, frustra spoofing lógico, pois o canal sobre o qual se mede o CSI não pode ser clonado com mera injeção de quadros. Terceiro, adiciona fator contínuo de presença: enquanto o usuário mantém a mão sobre o leitor, o modelo atualiza a confiança em janelas de 200 ms, gerando alarme instantâneo se a palma for retirada ou trocada.

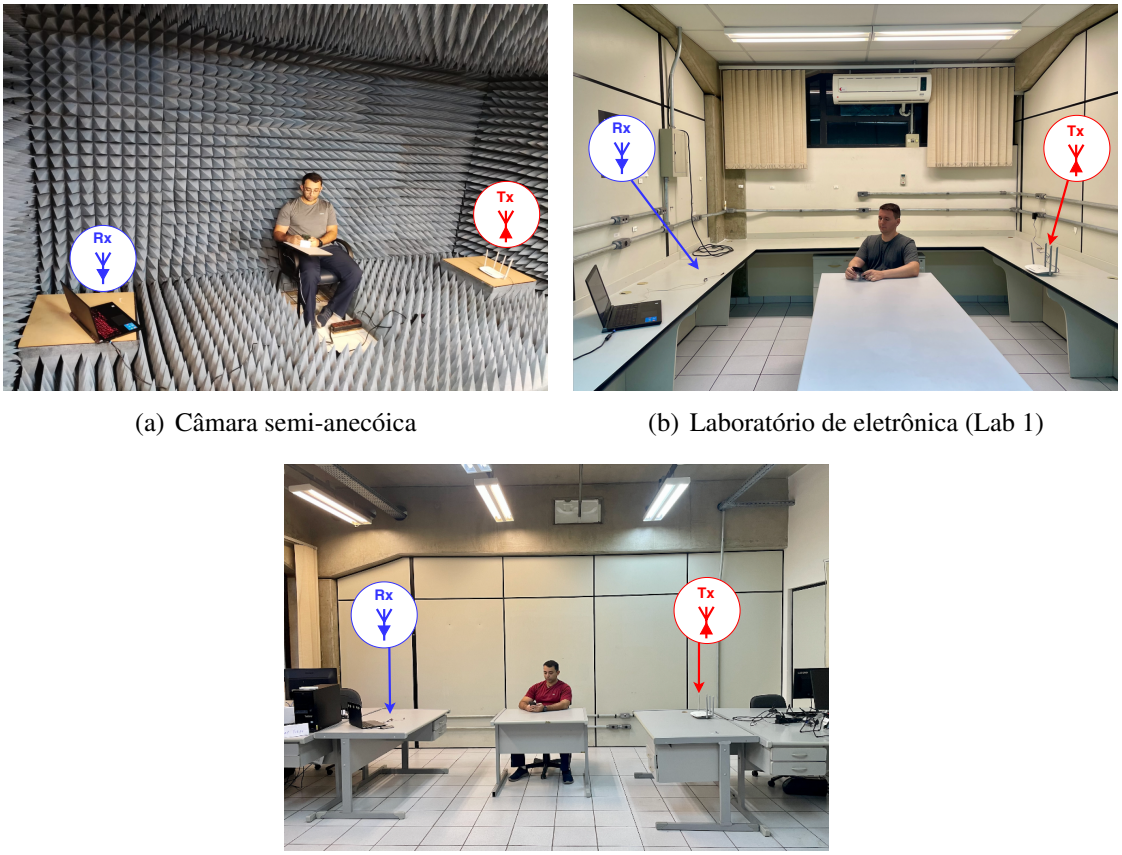
Por outro lado, há limitações que persistem quando considerado o nível de prontidão tecnológico do aparato experimental utilizado neste estudo de caso. A distância adotada de 3 cm entre mão e antena, controlada na Figura 4.8, assegura sinal forte mas não espelha leitores de cartão instalados em catracas, nos quais variações de postura são maiores. Ensaios preliminares com espaçamento de 6 cm deterioraram o desvio-padrão de fase. Também não se avaliou o efeito de agentes externos como luvas, acessórios diversos ou umidade; esses cenários exigirão coletar novas amostras e talvez introduzir fase bidirecional (duas antenas) para recuperar entropia. Por fim, implantação em larga escala exigirá mecanismo de atualização de modelo in-situ.

Em síntese, o presente estudo de caso demonstra, de forma quantificável, que autenticar por presença física usando somente a malha Wi-Fi já instalada é possível. Com ajustes marginais—refino de limiar, captura bilateral ou descarte dinâmico de subportadoras ruidosas—o sistema tende a satisfazer integralmente os requisitos de alto-nível, abrindo caminho para integrações transparentes em catracas, terminais de pagamento e controles de acesso industriais.

4.6. Caso de estudo: Wi-Fi CSI como novo Feature Set para NIDS

O sistema Spider-Sense nasceu da necessidade de detectar tentativas de intrusão ainda na fase de associação Wi-Fi, antes que qualquer pacote de dados seja trocado. Para comprovar sua viabilidade, o estudo descrito em [de Almeida et al. 2024] montou três ambientes contrastantes: uma câmara semianecóica de 20 m^2, o Laboratório 1 de radiofrequência (24 m^2, paredes de drywall) e o Laboratório 2 de pesquisa em redes (36 m^2, estrutura com mesas de escritório e computadores) — Figura 4.11 apresenta fotos sobre estes locais. Em todos os cenários, um ponto de acesso TP-Link C60 operando em 2,4 GHz, 20 MHz e canal 8 gerou pacotes beacon e quadros vazios (*null-data*) a 1 000 pps. O módulo ESP32-WROOM-32E, posicionado a 1,2 m do AP e separado entre si por 180 cm, capturaram CSI em modo *monitor*. Cada sessão de experimento durou 60 s, dos quais os 10 s iniciais serviram para estabilização do ruído de rádio pertencente ao ambiente, seguidos de 40 s de tráfego benigno e, finalmente, 10 s contendo 400 tentativas de força bruta de associação; i.e., quadros `authentication request` enviados com MAC aleatório, replicando o comportamento de *bots* que buscam senha por dicionário.

A escolha do ESP32 decorreu de três fatores práticos. Primeiro, trata-se de hard-



(a) Câmara semi-anecóica (b) Laboratório de eletrônica (Lab 1)

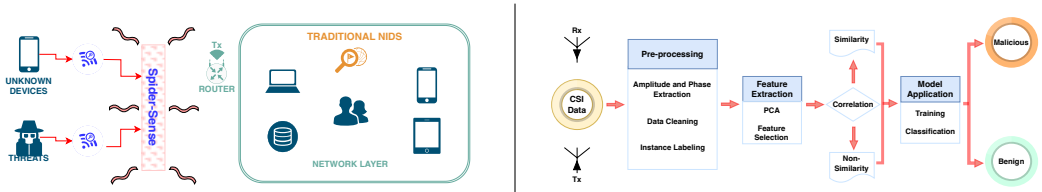
(c) Laboratório de Pesquisas (Lab 2)

Figura 4.11. Ambiente físico para coleta dos dados [de Almeida et al. 2024].

ware amplamente disponível por aproximadamente US$5, o que torna plausível instrumentar ambiente físico com escala sem custo proibitivo. Segundo, o firmware `esp-csi` já expõe 52 subportadoras de amplitude e fase em 20 MHz. Terceiro, a alimentação de 180 mW permite autonomia superior a 12 h com um *power bank* de 10 000 mAh.

Para garantir comparabilidade entre sessões, todos os dispositivos sincronizaram o relógio ao campo TSF dos beacons; o erro acumulado foi menor que ≈20 µs em 45 min, valor suficiente para alinhar as capturas num tensor global $\mathbb{C}^{3\times256\times T}$ sem interpolação. O fluxo CSI bruto de 256 kB/s por receptor foi comprimido com Snappy antes do envio via UDP, reduzindo a banda para 28 kB/s — taxa que não interfere no tráfego de dados do laboratório. Ao final, o dataset resultou em 800.000 instâncias rotuladas (benigno x ataque na razão 1:1; i.e., balanceadas) distribuídas uniformemente pelos três ambientes, volume que equilibra representatividade estatística e tempo de treinamento: o modelo de árvore de decisão escolhido no estudo consome na ordem de 1.4 s para ajustar-se em um notebook Core i7, permitindo re-treino diário sem impactar operações. A Figura 4.12 ilustra o conceito para o desenvolvimento deste estudo de caso.

Essa configuração demonstra que, mesmo em espaços acusticamente tratados ou dominados por estruturas metálicas, o CSI preserva variações sutis produzidas por quadros de gerenciamento forjados. O resultado não depende de amplificadores de potência



(a) Arquitetura. (b) Fluxo para geração do modelo.

Figura 4.12. Detecção antecipada de intrusos com Spider-Sense [de Almeida et al. 2024].

nem de antenas especializadas; basta inserir nós ESP32 nas tomadas existentes para que a malha Wi-Fi ganhe uma "sensibilidade física" adicional, capaz de ir além dos NIDS tradicionais que operam na camada de payload. As seções seguintes descrevem o pipeline de detecção que traduz esses sinais brutos em alertas consumíveis por um centro de operações de segurança.

4.6.1. Pipeline de detecção antecipada e assinatura física

Transformar flutuações imperceptíveis de CSI em alarmes acionáveis exige uma sequência de etapas cuidadosamente encadeadas, cada qual desenhada para conservar apenas a parcela do sinal que carrega evidência física de uma tentativa de invasão. O Spider-Sense começa pela mesma sanitização de amplitude e fase já descrita na Seção 4.4, em específico conforme ilustrado na Figura 4.12(b).

O pré-processamento permite realçar os aspectos mais relevantes e descartar quaisquer distorções ou anomalias em potencial. Atualmente, um conjunto específico de técnicas foi identificado como particularmente eficaz para alcançar os objetivos definidos neste estudo. Entre essas técnicas destacam-se: a remoção de *outliers* utilizando o método Hampel, a Calibração de fase, a Aplicação de um Filtro Passa-baixa, a Transformada Discreta de Hilbert, a Transformada Discreta Wavelet, a Técnica de Interpolação, e a Análise de Componentes Principais (PCA). Posteriormente, o estudo apresenta uma discussão sobre o emprego destas técnicas e como análises complementares contribuem para o refino do conjunto de dados coletados neste estudo.

A indicação da presença de seres humanos portando dispositivos com capacidade de conexão a redes Wi-Fi direciona o estudo para técnicas avançadas que facilitam a extração de características específicas. Desse modo, evidenciam-se: a criação de vetores de características por meio da média em subportadoras; a análise da forma da onda; a diferenciação de amplitude de frequência e fase; o emprego de técnicas de *Deep Learning*; e a técnica de *Dynamic Time Warping*. Individualmente, essas técnicas fornecem *insights* relevantes sobre quais atributos são mais significativos para distinguir o que é estático do que tem movimento, contribuindo para o aprimoramento de modelos de aprendizado de máquina. Assim, o trabalho discute a contribuição dessas técnicas para o desenvolvimento de sistemas eficientes de detecção baseados em informações de estado de canal (CSI), avançando na capacidade de monitoramento e segurança.

No sentido de aperfeiçoar a detecção e classificação de seres humanos e dispositivos com capacidade Wi-Fi em ambientes internos, uma gama diversificada de algoritmos e técnicas de análise de sinais tem sido meticulosamente explorada. Cada um destes

algoritmos apresenta uma abordagem única e especializada, proporcionando uma compreensão mais aprofundada e precisa dos dados coletados, refletindo uma sinergia entre inovação tecnológica e aplicabilidade prática. Neste estudo, alinhado com o estado da arte atual e refletindo um compromisso com a precisão e eficácia, as seguintes técnicas foram selecionadas para análise e classificação: passo estimado; SVM; Similaridade baseada em limite; Classificação de Múltiplos Sinais (MUSIC); Similaridade Baseada em Reversão Temporal; Rede Neural Convolucional (CNN); KNN. A Tabela 4.4 reúne as principais técnicas e algoritmos abordados neste estudo.

Tabela 4.4. Principais Técnicas e Algoritmos

Pré-processamento	Extração de características	Classificação
Removedor de Outlier (Hampel)	Seleção de características por média de subportadora	Passo estimado
Calibração de fase	Forma de onda	SVM
Filtro passa-baixa	Análise periódica	Similaridade baseada em limite
Transformada Discreta de Hilbert	Frequência, Amplitude e Diferença de Fase	MUSIC
Transformada Discreta Wavelet	Gingado	Similaridade baseada em tempo reverso
Interpolação	Aprendizado profundo	CNN
Análise da Componente Principal (PCA)	Envolvimento de tempo dinâmico	KNN

4.6.2. Resultados, desempenho e discussão de viabilidade

A robustez do Spider-Sense pode ser avaliada em três dimensões: eficácia de detecção, custo computacional e resiliência a ambientes heterogêneos. Nos 800 000 exemplos balanceados entre tráfego benigno e ataques de força bruta, a árvore J48 treinada com o conjunto reduzido de subportadoras alcançou F1 = 99,95 %, acurácia = 99,96 % e FPR = 0,05 %. Esses valores superam o requisito de FPR $\leq 0,20\,\%$, aproximando-se do limiar de 0,10 % exigido em sistemas biométricos de alto nível. O resultado mais notável, porém, é a uniformidade: em validação *leave-environment-out* a F1 caiu apenas 0,12 pontos percentuais (p.p.) ao migrar da câmara semi-anecóica para o Laboratório 2.

No que tange à latência, o pipeline completo (compreendendo de captura, sanitização, seleção de atributos e inferência) consome 65 ms no cenário controlado e $\approx$78 ms no laboratório (estimativa realizada com base em estudos anteriores [Bertoli et al. 2024]), valores que permanecem abaixo do teto de 100 ms necessário para bloquear a associação antes que o invasor continue o ataque. O consumo de CPU no ESP32 situa-se em 46 % durante picos de 2 000 pacotes por segundo (pps), mantendo margem para criptografar e enviar logs sem degradação da QoS. Em termos energéticos, o nó tem capacidade para operar 12 h com bateria de 10 000 mAh, viabilizando deploy temporário em locais sem estruturada para fornecimento de energia (tomadas).

Como pode ser observado na Tabela 4.5 a maioria dos classificadores obtiveram desempenho ótimo. Uma característica a se observar neste caso é o tempo de construção dos modelos e posteriormente sua capacidade de futuramente serem portados para dispositivos menores e com baixa capacidade computacional. Quando observada a distribuição dos valores constantes no valor amplitude das portadoras (Figura 4.13), a tarefa de distinção entre as ações maliciosas e benígnas se resume a diferenciar entre duas distribuições. Uma delas com tendência a ser uniforme (maliciosas) e outra com *bell-shape* e cauda (benígnas). Uma investigação mais aprofundada nesse sentido pode ser interessante para revelar características das distribuições com confirmação e protocolo estatístico robusto,

algo que está fora do escopo deste estudo de caso.

Tabela 4.5. Desempenho dos classificadores considerados [de Almeida et al. 2024].

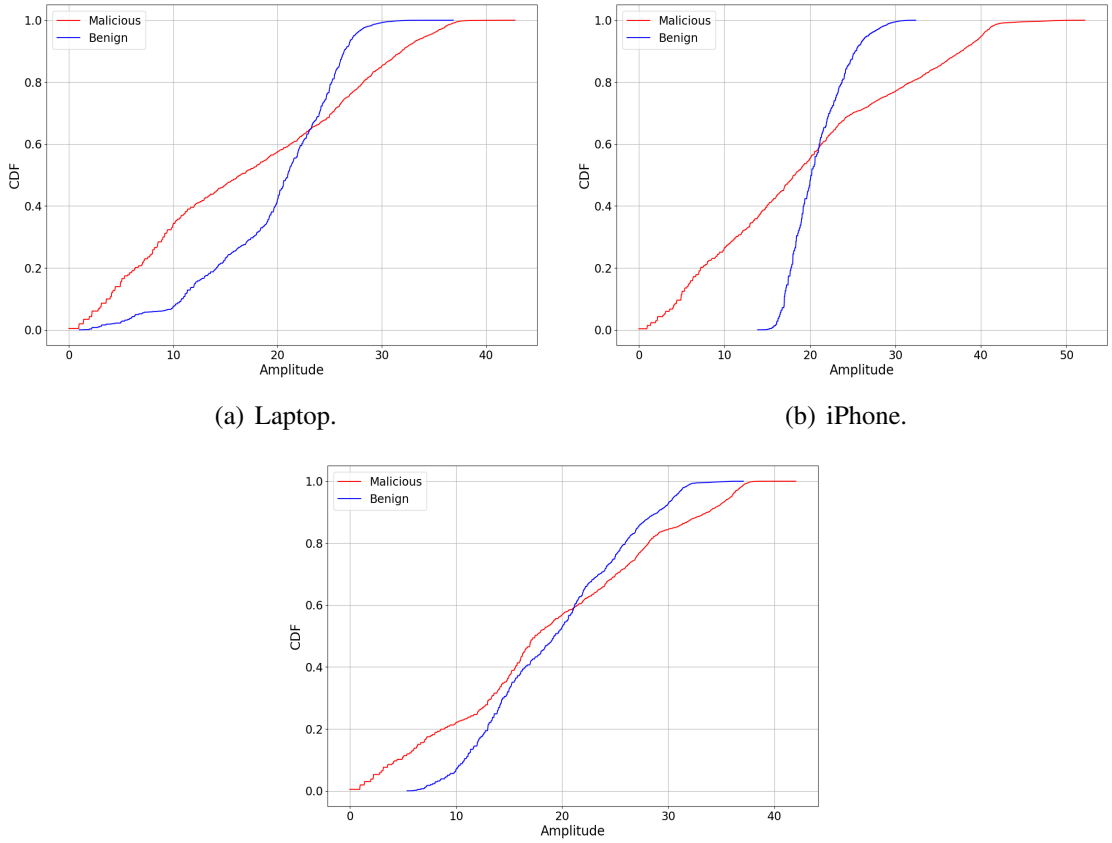
Classificador	Ambiente de teste	Precisão (%)	F1-Score	Construção em (s)
SVM	Câmara semi-anecoica	100,00	1,000	23,35
	Lab 1	99,99	1,000	43,41
	Lab 2	99,98	1,000	116,99
Random Forest	Câmara semi-anecoica	100,00	1,000	9,68
	Lab 1	99,99	1,000	27,31
	Lab 2	99,97	1,000	19,07
KNN	Câmara semi-anecoica	100,00	1,000	0,04
	Lab 1	99,99	1,000	0,03
	Lab 2	99,98	1,000	0,05
Decision Tree	Câmara semi-anecoica	100,00	1,000	1,63
	Lab 1	99,97	1,000	1,93
	Lab 2	99,95	1,000	1,29
Naive Bayes	Câmara semi-anecoica	100,00	1,000	2,91
	Lab 1	96,06	0,921	3,17
	Lab 2	94,76	0,948	2,15

Do ponto de vista operacional, o estudo indica que inserir de dois a três ESP32[2] por sala oferece cobertura angular satisfatória: o que vai permitir uma cobertura maior e potencialmente possibilitar a triangulação e localização física aproximada do atacante. Os presentes resultados demonstram que, diferentemente de NIDS baseados em payload, a distribuição espacial dos sensores melhora a qualidade do "rastro eletromagnético" usado como assinatura física.

Em síntese, os resultados provam o conceito que o Spider-Sense cumpre os limites de latência e precisão para proteção de SSIDs corporativos, sem exigir hardware especializado ou alterações na infraestrutura Wi-Fi. A seção seguinte discute como esses nós podem integrar-se a um centro de operações de segurança, enviando alertas em MQTT ou syslog, e quais extensões são necessárias para cobrir ataques em bandas de 6 GHz [de Almeida et al. 2024].

4.6.3. Integração com SOC e usos industriais

Resultados promissores de laboratório só se convertem em valor quando se encaixam no ecossistema de defesa de uma organização. O Spider-Sense foi projetado para dialogar com um Security Operations Center (SOC) moderno sem exigir alterações na malha Wi-Fi existente. Cada nó ESP32[2] encapsula a decisão da árvore J48 em um registro JSON com cinco campos: timestamp, ID do nó, canal e rótulo (benigno ou ataque). O pacote viaja por MQTT criptografado até um broker local; e finalmente, um conector é usado para preparar os dados para inserção no ambiente SIEM. Toda a conversão leva $\approx$4 ms, de modo que o alarme completo—medido da chegada do quadro `authentication request` ao disparo do evento no dashboard—fica abaixo de 85 ms, ainda dentro do or-



(a) Laptop.

(b) iPhone.

(c) Android.

Figura 4.13. CDFs das amplitudes do dataset [de Almeida et al. 2024].

çamento de 100 ms. Esse valor supera a velocidade de correlação de sondas DPI baseadas em payload, que precisam primeiro decodificar a pilha TLS antes de inferir anomalias.

Por fim, a chegada do IEEE 802.11bf simplificará ainda mais a integração. O draft atual já permite que pontos de acesso publiquem relatórios CSI em moldes similares aos usados pelo Spider-Sense, eliminando a necessidade de firmware customizado. Dessa forma, a viabilidade econômica e técnica do sistema só tende a melhorar, abrindo caminho para que a assinatura física do canal se torne elemento indispensável nos playbooks de resposta a incidentes.

4.7. Tendências Futuras e Fronteiras de Pesquisa

Os estudos de caso de autenticação (Seção4.5) e Spider-Sense (Seção4.6) demonstram que o êxito de um sistema baseado em CSI depende menos do algoritmo escolhido e mais da forma como os dados são obtidos e mantidos ao longo do tempo. Como também apresentado por [Chen et al. 2023], três aprendizados se destacam.

Primeiramente, a coleta deve ser breve e precisa. Sessões prolongadas atingem um ponto assintótico de tal forma que pode-se cessar a coleta naquele instante. Como demonstrado anteriormente, as capturas de 15 s não necessariamente trazem ganho de informação quando comparadas com capturas de menor duração (e.g., 5 s). Em segundo,

a rotulagem exige gatilhos externos. No caso da autenticação, o clique de início de captura, alinhado ao preâmbulo TSF, permite boa precisão. No Spider-Sense, os pacotes de ataque foram rotulados pelo MAC, permitindo casar cada quadro transmitido com o CSI recebido. Ensaios que dispensaram esse sincronismo acumularam desvios de até 600 ms, suficientes para misturar instâncias benignas e maliciosas e prejudicar o desempenho das soluções. A lição operacional é clara: sem rótulo confiável, o modelo aprende a classificar ruído.

Por fim, há uma tendência de presença de *concept drift*. Medições semanais em três salas apontaram degradação total na acurácia do Random Forest quando móveis foram rearranjados ou outras características exógenas (percentual de água no corpo da pessoa). Re-treinar o modelo completo consome 15 s de CPU no Raspberry Pi, mas exige novas amostras rotuladas.

Em conjunto, esses três pontos (coleta adequada, rótulo bem definido e atualização incremental) formam a base de uma implantação sustentável. Sem eles, o desempenho se dilui na variabilidade do ambiente. Ao passo que ao adotar tais cuidados, houve uma efetividade maior dos sistemas analisados e propostos neste minicurso. Um sentido para conseguir o aumento da prontidão tecnológica seria automatizar estes processos e desenvolver sistemas que sejam auto-adaptáveis (não supervisionado, auto-supervisionado, aprendizado por reforço) e consigam filtrar os diferentes ruídos presentes no sistema de modo mais generalizável (e.g., autoencoders).

4.7.1. Limitações atuais e barreiras técnicas

Do ponto de vista de consolidação de mercado, ainda há dificuldades que com a padronização do 802.11bf, apesar de tenderem a melhorar ao longo dos próximos anos. Em especial, atualmente citam-se: heterogeneidade de hardware, lacunas de padronização e desafios de privacidade.

O primeiro obstáculo é a diversidade de chipsets. Estudos concentram-se em um bem conhecido e limitado de hardware, o Intel 5300, o ESP32 e o Raspberry PI. Há implementações específicas com Rádio Definido por Software, o que pode trazer alguma flexibilidade para testes que envolvam Wi-Fi 6 com 512 subportadoras. No entanto, cada geração impõe velocidade de amostragem, quantização e filtros analógicos distintos.

A segunda barreira é o processo de padronização. O draft 802.11bf define a exposição CSI e que pode ser obtido a partir de rádios com frequências mais altas (tais como 6GHz e 60GHz[802.11ad/ay]). Porém, ainda requer a implementação pelos fabricantes para utilização. Nesse sentido, a ausência de uma API comum também também é um fator complicante. Em aplicações militares, por exemplo, processos de auditoria podem exigir a verificação de compliance e averiguação de cumprimento estrito das funcionalidades. Isso permite assegurar que sondas indesejadas sejam postas por meio de ataques em cadeia de distribuição/suprimentos (*supply-chain*).

O terceiro eixo envolve privacidade e regulação. O mesmo sinal que identifica uma intrusão pode revelar batimentos cardíacos ou padrão de respiração. Organizações que coletam CSI em larga escala precisam argumentar que a métrica não constitui dado pessoal sensível. A título de exemplo, a legislação europeia sugere enquadrar tais sinais

como "biometria soft", exigindo consentimento expresso. Já a LGPD brasileira ainda não define categoria específica. Um caminho técnico é executar inferência no próprio ponto de acesso e transmitir apenas hashes e rótulos, mas isso implica colocar modelos nos APs, aumentando custo e exigindo atualizações remotas seguras.

Somam-se ainda problemas operacionais já discutidos: concept drift acelerado por reconfiguração de ambiente e escassez de datasets de longo prazo. Sem bases públicas que cubram seis meses ou mais, permanece incerto se o filtro Hampel ou o re-treino incremental são adequados a cenários de produção onde o ambiente operacional é dinâmico.

Em síntese, a tecnologia atravessou o estágio de prova de conceito. Apesar de se apresentarem como dificuldades, há fortes desafios de pesquisas e oportunidades. No sentido de aumentar o nível de prontidão tecnológica: (i) convergência de medição CSI em 802.11bf, (ii) desenvolvimento de hardware e softwares que sejam mais suscetíveis a regulação e (iii) ferramental de validação cruzada que mantenha desempenho mesmo com hardware heterogêneo. Assim como oportunidades futuras, os protótipos avaliados colocam CSI no patamar de viabilidade técnica, mas o salto para adoção massiva dependerá de uma convergência entre novas tecnologias de rede, técnicas de aprendizado distribuído e modelos de governança de identidade.

A chegada do Wi-Fi 7 (IEEE 802.11be) multiplicará por quatro a largura de banda espectral e aumentará para 4096 o número de subportadoras capturáveis em modo sensing. Esse salto se traduz em vetor de atributos quase dezesseis vezes maior que o usado pelo ESP32 atual, abrindo margem para distinguir uma gama maior de eventos, como respiração de duas pessoas lado a lado. Contudo, processar tal volume em tempo real exigirá chipsets com unidades MAC/PHY dedicadas a exportar CSI sem obstruir a pilha de dados.

Ao mesmo tempo, a dispersão de pontos de captura demanda *Edge AI*. Executar inferência no ponto de acesso elimina salto de rede e garante que dados brutos de canal não saiam do domínio físico, mitigando riscos de privacidade. O Random Forest de 16 kB cabe na RAM de um AP Wi-Fi 6 de classe corporativa, mas redes neurais leves (TinyML) podem explorar as não linearidades extras do Wi-Fi 7 sem exceder 100 ms.

Aprendizado federado (FL) surge como estratégia para treinar esses modelos sem centralizar CSI sensível. Cada nó coleta, ajusta gradientes locais e envia apenas atualizações criptografadas para o agregador. Nesse sentido, uma lacuna a ser explorada envolve a utilização de múltiplos pontos de coleta (por exemplo, dez Raspberry Pi) em ambiente FL para reduzir o concept drift em um ambiente ou tipo de aplicação em específico. Como a integração com o ambiente físico pode trazer diferenciações na taxa com que os eventos de atualização ocorrem, o tipo de eventos que disparam mudanças e estratégias diferenciadas para agregação dos modelos.

4.8. Considerações Finais

Este capítulo apresentou uma visão abrangente sobre a autenticação baseada em informações da camada física, com foco no uso do Channel State Information (CSI) extraído de dispositivos Wi-Fi comerciais. Foram discutidas as limitações dos métodos tradicionais diante de ataques sofisticados como revezamento e spoofing, apresentando o CSI como

alternativa viável para incorporar consciência ambiental no processo de autenticação. A partir da análise de duas implementações distintas, conduzidas em contextos acadêmico e operacional, foi possível validar o potencial dessa abordagem em cenários com restrições reais de hardware, mobilidade e interferência. A combinação de pré-processamento adequado, extração eficiente de características e uso de modelos leves permitiu alcançar resultados competitivos mesmo sem infraestrutura especializada.

Em suma, dentro do contexto de cibersegurança a assinatura física do canal Wi-Fi não substitui criptografia nem autenticação tradicional; ela adiciona uma camada invisível que dificulta ataques de *relay*, *spoofing* e intrusão silenciosa. Oportunidades futuras que contemplem novas tecnologias e abordagens inovadoras tais como Wi-Fi 7, Edge AI e aprendizado federado possuem o potencial de se transformar em tendência para utilização em cibersegurança. Isso fortalecerá toda gama de dispositivos que instrumentam o mundo físico como é o caso da Internet das Coisas.

Referências

[iee 2021] (2021). Ieee standard for information technology–telecommunications and information exchange between systems - local and metropolitan area networks–specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*, pages 1–4379.

[ISO 2021] (2021). ISO/IEC 19795-2: 2021 Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation.

[Abdelnasser et al. 2015] Abdelnasser, H., Youssef, M., and Harras, K. A. (2015). Wigest: A ubiquitous wifi-based gesture recognition system. In *2015 IEEE Conference on Computer Communications (INFOCOM)*, pages 1472–1480.

[Abu Ali et al. 2024] Abu Ali, N. A., Rehman, M., Mumtaz, S., Khan, M. B., Hayajneh, M., Ullah, F., and Shah, R. A. (2024). Contactless diseases diagnoses using wireless communication sensing: Methods and challenges survey. *ACM Comput. Surv.*, 56(9).

[Adib and Katabi 2013] Adib, F. and Katabi, D. (2013). See through walls with wifi! In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, SIGCOMM '13, page 75–86, New York, NY, USA. Association for Computing Machinery.

[Afshar et al. 2022] Afshar, A., Vakili, V. T., and Daei, S. (2022). Active user detection and channel estimation for spatial-based random access in crowded massive mimo systems via blind super-resolution. *IEEE Signal Processing Letters*, 29:1072–1076.

[Al-qaness et al. 2016] Al-qaness, M. A. A., Li, F., Ma, X., Zhang, Y., and Liu, G. (2016). Device-free indoor activity recognition system. *Applied Sciences*, 6(11).

[Aleesa et al. 2020] Aleesa, A. M., Zaidan, B. B., Zaidan, A. A., and Sahar, N. M. (2020). Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions. *Neural Computing and Applications*, 32(14):9827–9858.

[Almeida et al. 2024] Almeida, F. S., Trindade, E. F. G., Pettersson, M., Machado, R., and Jr., L. A. P. (2024). Spidersense: Early intruder detection in wi-fi networks using channel state information. In *Proc. IEEE Global Communications Conference (GLOBECOM)*, pages 1–6.

[Bertoli et al. 2024] Bertoli, G. d. C., Fernandes, G. V. C., Monici, P. H. B., Guibo, C. H. d. A., Santos, A. L. d., and Pereira Júnior, L. A. (2024). Design and implementation of intelligent packet filtering in iot microcontroller-based devices. *Journal of Internet Services and Applications*, 15(1):289–301.

[Chen et al. 2023] Chen, C., Zhou, G., and Lin, Y. (2023). Cross-domain wifi sensing with channel state information: A survey. *ACM Comput. Surv.*, 55(11).

[Cisco 2020] Cisco (2020). Cisco Annual Internet Report (2018–2023). White Paper.

[Cominelli et al. 2023] Cominelli, M., Gringoli, F., and Restuccia, F. (2023). Exposing the csi: A systematic investigation of csi-based wi-fi sensing capabilities and limitations. In *2023 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 81–90.

[Cominelli et al. 2021] Cominelli, M., Kosterhon, F., Gringoli, F., Lo Cigno, R., and Asadi, A. (2021). Ieee 802.11 csi randomization to preserve location privacy: An empirical evaluation in different scenarios. *Computer Networks*, 191:107970.

[de Almeida et al. 2024] de Almeida, F. S., Trindade, E. F. G., Pettersson, M. I., Machado, R., and Júnior, L. A. P. (2024). Spider-sense: Wi-fi csi as a sixth sense for early detection in network intrusion detection systems. In *GLOBECOM 2024 - 2024 IEEE Global Communications Conference*, pages 2437–2442.

[De Carvalho Bertoli et al. 2021] De Carvalho Bertoli, G., Pereira Júnior, L. A., Saotome, O., Dos Santos, A. L., Verri, F. A. N., Marcondes, C. A. C., Barbieri, S., Rodrigues, M. S., and Parente De Oliveira, J. M. (2021). An end-to-end framework for machine learning-based network intrusion detection system. *IEEE Access*, 9:106790–106805.

[Ding et al. 2018] Ding, E., Li, X., Zhao, T., Zhang, L., and Hu, Y. (2018). A robust passive intrusion detection system with commodity wifi devices. *Journal of Sensors*, 2018(1):8243905.

[Du et al. 2025] Du, R., Hua, H., Xie, H., Song, X., Lyu, Z., Hu, M., Narengerile, Xin, Y., McCann, S., Montemurro, M., Han, T. X., and Xu, J. (2025). An overview on ieee 802.11bf: Wlan sensing. *IEEE Communications Surveys& Tutorials*, 27(1):184–217.

[Espressif Systems 2018] Espressif Systems (2018). Csi documentation – esp-idf programming guide. `https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-guides/wifi.html#wi-fi-csi`. Acessado em 2024-01-20.

[Espressif Systems 2019] Espressif Systems (2019). esp-csi: Channel state information extraction for esp32. `https://github.com/espressif/esp-csi`. Acessado em 2024-01-20.

[Firch 2024] Firch, J. (2024). Wireless network attacks: Learn the common types of wireless attacks. `https://purplesec.us/learn/wireless-network-attack/`. Acessado em 2024-03-22.

[Forbes et al. 2020] Forbes, G., Massie, S., and Craw, S. (2020). Wifi-based human activity recognition using raspberry pi. In *2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI)*, pages 722–730.

[Geng et al. 2022] Geng, J., Huang, D., and la Torre, F. D. (2022). Densepose from wifi.

[Gringoli et al. 2021] Gringoli, F., Cominelli, M., Blanco, A., and Widmer, J. (2021). Ax-csi: Enabling csi extraction on commercial 802.11ax wi-fi platforms. In *Proceedings of the 15th ACM Workshop on Wireless Network Testbeds, Experimental Evaluation & CHaracterization*, WiNTECH '21, page 46–53, New York, NY, USA. Association for Computing Machinery.

[Gringoli et al. 2019] Gringoli, F., Schulz, M., Link, J., and Hollick, M. (2019). Free your csi: A channel state information extraction platform for modern wi-fi chipsets. In *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*, WiNTECH '19, page 21–28, New York, NY, USA. Association for Computing Machinery.

[Gu et al. 2024] Gu, Y., Chen, J., He, K., Wu, C., Zhao, Z., and Du, R. (2024). WiFiLeaks: Exposing Stationary Human Presence Through a Wall With Commodity Mobile Devices . *IEEE Transactions on Mobile Computing*, 23(06):6997–7011.

[Guo and Ho 2022] Guo, J. and Ho, I. W.-H. (2022). Csi-based efficient self-quarantine monitoring system using branchy convolution neural network. In *2022 IEEE 8th World Forum on Internet of Things (WF-IoT)*, pages 1–6.

[Guo et al. 2017] Guo, L., Wang, L., Liu, J., Zhou, W., Liu, B. L. T., Li, G., and Li, C. (2017). A novel benchmark on human activity recognition using wifi signals. In *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–6.

[Halperin et al. 2011] Halperin, D., Hu, W., Sheth, A., Wetherall, D., Anderson, T., and Padmanabhan, V. (2011). Tool release: Gathering 802.11n traces with channel state information. In *Proc. ACM SIGCOMM*. `http://dhalperi.github.io/linux-80211n-csitool/`.

[He et al. 2020] He, Y., Chen, Y., Hu, Y., and Zeng, B. (2020). Wifi vision: Sensing, recognition, and detection with commodity mimo-ofdm wifi. *IEEE Internet of Things Journal*, 7(9):8296–8317.

[Hernandez and Bulut 2020] Hernandez, S. M. and Bulut, E. (2020). Lightweight and standalone iot based wifi sensing for active repositioning and mobility. In *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, pages 277–286.

[Hernandez and Bulut 2023] Hernandez, S. M. and Bulut, E. (2023). Wifi sensing on the edge: Signal processing techniques and challenges for real-world systems. *IEEE Communications Surveys& Tutorials*, 25(1):46–76.

[IEEE 802.11 Working Group 2024] IEEE 802.11 Working Group (2024). IEEE Draft Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment: WLAN Sensing. `https://mentor.ieee.org/802.11/dcn/21/11-21-0915-12-0sensing-802-11bf-draft-specification.docx`. Draft Specification IEEE 802.11bf, v12.0, March 2024.

[IEEE 802.11 Working Group 2025] IEEE 802.11 Working Group (2025). Ieee p802.11bf/d1.4: Wireless lan sensing amendment (draft). Available from IEEE Standards Association.

[Kong et al. 2021] Kong, H., Lu, L., Yu, J., Chen, Y., Xu, X., Tang, F., and Chen, Y.-C. (2021). Multiauth: Enable multi-user authentication with single commodity wifi device. In *Proceedings of the Twenty-Second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, MobiHoc '21, pages 31–40, New York, NY, USA. Association for Computing Machinery.

[Kotaru et al. 2015] Kotaru, M., Joshi, K., Bharadia, D., and Katti, S. (2015). Spotfi: Decimeter level localization using wifi. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, page 269–282, New York, NY, USA. Association for Computing Machinery.

[Li et al. 2017] Li, S., Li, X., Niu, K., Wang, H., Zhang, Y., and Zhang, D. (2017). Ar-alarm: An adaptive and robust intrusion detection system leveraging csi from commodity wi-fi. In Mokhtari, M., Abdulrazak, B., and Aloulou, H., editors, *Enhanced Quality of Life and Smart Living*, pages 211–223, Cham. Springer International Publishing.

[Lin et al. 2023] Lin, C., Wang, P., Ji, C., Obaidat, M. S., Wang, L., Wu, G., and Zhang, Q. (2023). A contactless authentication system based on wifi csi. *ACM Trans. Sen. Netw.*, 19(2).

[Liu et al. 2014] Liu, H., Wang, Y., Liu, J., Yang, J., and Chen, Y. (2014). Practical user authentication leveraging channel state information (csi). In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '14, page 389–400, New York, NY, USA. Association for Computing Machinery.

[Liu et al. 2018] Liu, J., Chen, Y., Wang, Y., Chen, X., Cheng, J., and Yang, J. (2018). Monitoring vital signs and postures during sleep using wifi signals. *IEEE Internet of Things Journal*, 5(3):2071–2084.

[Liu et al. 2020] Liu, J., Liu, H., Chen, Y., Wang, Y., and Wang, C. (2020). Wireless sensing for human activity: A survey. *IEEE Communications Surveys& Tutorials*, 22(3):1629–1645.

[Liu et al. 2015] Liu, J., Wang, Y., Chen, Y., Yang, J., Chen, X., and Cheng, J. (2015). Tracking vital signs during sleep leveraging off-the-shelf wifi. In *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '15, page 267–276, New York, NY, USA. Association for Computing Machinery.

[Ma et al. 2019] Ma, Y., Zhou, G., and Wang, S. (2019). Wifi sensing with channel state information: A survey. *ACM Comput. Surv.*, 52(3):46.

[Meng et al. 2020] Meng, Y., Li, J., Zhu, H., Liang, X., Liu, Y., and Ruan, N. (2020). Revealing your mobile password via wifi signals: Attacks and countermeasures. *IEEE Transactions on Mobile Computing*, 19(2):432–449.

[Mirsky et al. 2018] Mirsky, Y., Doitshman, T., Elovici, Y., and Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. *Network and Distributed System Security Symposium (NDSS)*.

[Niu et al. 2018] Niu, K., Zhang, F., Chang, Z., and Zhang, D. (2018). A fresnel diffraction model based human respiration detection system using cots wi-fi devices. In *Proceedings of the 2018 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '18. Association for Computing Machinery.

[Rahman et al. 2023] Rahman, M. A., Shahriar, H., Clincy, V., Hossain, M. F., and Rahman, M. (2023). A quantum generative adversarial network-based intrusion detection system. In *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 1810–1815.

[Ronen and Shamir 2017] Ronen, E. and Shamir, A. (2017). Extended functionality attacks on iot devices: The case of smart lights. *Proceedings of the IEEE*, 105(8):1495–1510.

[Scarfone 2022] Scarfone, K. (2022). A list of wireless network attacks. `https://www.techtarget.com/searchsecurity/feature/A-list-of-wireless-network-attacks`. Acessado em 2023-08-19.

[Schulz et al. 2017] Schulz, M., Wegemer, D., and Hollick, M. (2017). Nexmon: The c-based firmware patching framework. `https://seemoo.de/nexmon/`.

[Schulz et al. 2018] Schulz, M., Wegemer, D., and Hollick, M. (2018). The nexmon firmware analysis and modification framework: Empowering researchers to enhance wi-fi devices. *Computer Communications*, 129:269–285.

[Seifeldin and Youssef 2011] Seifeldin, M. A. and Youssef, M. (2011). RASID: A robust wlan device-free passive motion detection system. In *Proc. IEEE Int. Conf. on Pervasive Computing and Communications (PerCom)*, pages 180–189.

[Sen et al. 2012] Sen, S., Radunovic, B., Choudhury, R. R., and Minka, T. (2012). You are facing the mona lisa: spot localization using phy layer information. In *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, MobiSys '12, page 183–196, New York, NY, USA. Association for Computing Machinery.

[Shah and Kanhere 2017] Shah, S. W. and Kanhere, S. S. (2017). Wi-auth: Wifi based second factor user authentication. In *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, MobiQuitous 2017, pages 393–402, New York, NY, USA. Association for Computing Machinery.

[Sharma et al. 2025] Sharma, A., Mishra, D., Jha, S., and Seneviratne, A. (2025). Wispoof: Generating adversarial wireless signals to deceive wi-fi sensing systems. *Journal of Information Security and Applications*, 91:104052.

[Shen et al. 2021] Shen, X., Ni, Z., Liu, L., Yang, J., and Ahmed, K. (2021). Wipass: 1d-cnn-based smartphone keystroke recognition using wifi signals. *Pervasive and Mobile Computing*, 73:101393.

[Soto et al. 2022] Soto, J. C., Galdino, I., Caballero, E., Ferreira, V., Muchaluat-Saade, D., and Albuquerque, C. (2022). A survey on vital signs monitoring based on wi-fi csi data. *Computer Communications*, 195:99–110.

[Systems 2022] Systems, E. (2022). ESP32 CSI Tool. `https://github.com/espressif/esp32-csi-tool`.

[Tan et al. 2022] Tan, S., Ren, Y., Yang, J., and Chen, Y. (2022). Commodity wifi sensing in ten years: Status, challenges, and opportunities. *IEEE Internet of Things Journal*, 9(18):17832–17843.

[Truong et al. 2020] Truong, H., Trovato, B., and Smith, G. W. (2020). Practical replay attacks on nfc payments: From threats to mitigations. In *Proceedings of the 2020 ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 83–93. ACM.

[Truong and Tippenhauer 2020] Truong, H. T. and Tippenhauer, N. O. (2020). Practical relay attack on contactless payments—by smartphones. In *Proc. IEEE S&P*, pages 1132–1148.

[Vanhoef 2021] Vanhoef, M. (2021). Fragment and forge: Breaking wi-fi through frame aggregation and fragmentation. In *Proc. USENIX Security*, pages 1–18.

[Viegas et al. 2020] Viegas, E., Santin, A., Santos, R., and Abreu, V. (2020). Sistema de detecção de intrusão confiável baseado em aprendizagem por fluxo. In *Anais do*

XX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, pages 382–394, Porto Alegre, RS, Brasil. SBC.

[Wang et al. 2019] Wang, F., Han, J., Lin, F., and Ren, K. (2019). Wipin: Operation-free passive person identification using wi-fi signals. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6.

[Wang et al. 2016] Wang, W., Liu, A. X., and Shahzad, M. (2016). Gait recognition using wifi signals. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '16, pages 363–373, New York, NY, USA. Association for Computing Machinery.

[Wang et al. 2017] Wang, X., Gao, L., Mao, S., and Pandey, S. (2017). Csi-based fingerprinting for indoor localization: A deep learning approach. *IEEE Transactions on Vehicular Technology*, 66(1):763–776.

[Wang et al. 2020] Wang, X., Wang, Y., and Wang, D. (2020). A real-time csi-based passive intrusion detection method. In *2020 IEEE Intl Conf on Parallel& Distributed Processing with Applications, Big Data& Cloud Computing, Sustainable Computing& Communications, Social Computing& Networking (ISPA/BDCloud/SocialCom/SustainCom)*, pages 1091–1098.

[Wang and Liu 2019] Wang, Y. and Liu, Y. (2019). A survey on wi-fi based sensing: Applications, challenges, and opportunities. *Computer Networks*, 153:95–113.

[Xie et al. 2019] Xie, Y., Li, Z., and Li, M. (2019). Precise power delay profiling with commodity wi-fi. *IEEE Transactions on Mobile Computing*, 18(6):1342–1355.

[Xu et al. 2022] Xu, X., Zhang, Y., and Li, J. (2022). A survey on relay attacks in contactless payments: Current trends and countermeasures. *IEEE Access*, 10:88234–88252.

[Yang et al. 2013] Yang, Z., Zhou, Z., and Liu, Y. (2013). From rssi to csi: Indoor localization via channel response. *ACM Comput. Surv.*, 46(2).

[Zhang et al. 2017] Zhang, D., Wang, H., and Wu, D. (2017). Toward centimeter-scale human activity sensing with wi-fi signals. *Computer Society*, 50(1):48–57.

[Zhang et al. 2019] Zhang, F., Niu, K., Xiong, J., Jin, B., Gu, T., Jiang, Y., and Zhang, D. (2019). Towards a diffraction-based sensing approach on human activity recognition. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 3(1).

[Zheng et al. 2019] Zheng, Y., Zhang, Y., Qian, K., Zhang, G., Liu, Y., Wu, C., and Yang, Z. (2019). Zero-effort cross-domain gesture recognition with wi-fi. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '19, page 313–325, New York, NY, USA. Association for Computing Machinery.

[Zhuang et al. 2021] Zhuang, W., Shen, Y., Li, L., Gao, C., and Dai, D. (2021). Develop an adaptive real-time indoor intrusion detection system based on empirical analysis of ofdm subcarriers. *Sensors*, 21(7).

[Zou et al. 2017] Zou, H., Zhou, Y., Yang, J., Gu, W., Xie, L., and Spanos, C. (2017). Freecount: Device-free crowd counting with commodity wifi. In *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pages 1–6.