Além do Sinal: Autenticação Biofísica com Wi-Fi CSI e Raspberry Pi

Eduardo Fabrício Gomes Trindade[1], **Felipe Silveira de Almeida**[1], **Lourenço Alves Pereira Junior**[1]

[1]Divisão de Ciência da Computação
Instituto Tecnológico de Aeronáutica (ITA) – ITA – São Jose dos Campos, SP – Brazil

{trindade,felipefsa,ljr}@ita.br

Abstract. *Wi-Fi Channel State Information (CSI) has been widely studied for sensing activities. However, practical implementations aimed at user authentication have been less explored. This study proposes using Raspberry Pi devices to collect CSI data in a controlled environment and applies supervised learning to recognize biophysical and behavioral characteristics for physical access control. The research also explores the use of Hampel and Savitzky-Golay (SG) filters in data pre-processing and compares the performance of classification algorithms, with emphasis on K-Nearest Neighbors (KNN), achieving 99.9972% accuracy in user authentication.*

Resumo. *O Channel State Information (CSI) do Wi-Fi tem sido amplamente estudado em atividades de sensoriamento. No entanto, implementações práticas voltadas à autenticação de pessoas são pouco exploradas. Este estudo propõe o uso de dispositivos Raspberry Pi para coleta dados de CSI em um ambiente controlado e aplica aprendizado supervisionado para reconhecer características biofísicas e comportamentais visando controle de acesso físico. A pesquisa também explora o uso dos filtros de Hampel e Savitzky-Golay (SG) no pré-processamento dos dados e compara o desempenho de algoritmos de classificação, com destaque para o K-Nearest Neighbors (KNN), alcançando 99,92% de precisão na autenticação de usuários.*

1. Introdução

Ao longo dos anos, os sistemas de segurança baseados em reconhecimento têm evoluído significativamente no sentido de autenticar usuários e limitar o acesso, principalmente com a finalidade de resguardar ambientes e dados sensíveis. Contudo, o aumento das ameaças cibernéticas maliciosas tem colocado em xeque os métodos tradicionais de autenticação, como senhas, biometria e reconhecimento facial. Além disso, o extravio de dispositivos como *tokens*, cartões e QR Code facilita ações de falsificação comprometendo a segurança. Assim, faz-se necessário o desenvolvimento de novos métodos de autenticação que oferecem uma abordagem passiva de autenticação, onde a presença e os gestos dos usuários possam ser monitorados sem a necessidade de interação direta, aumentando a conveniência, a segurança e a confiabilidade.

Recentemente, pesquisadores têm investigado a utilização de dados do *Channel State Information (CSI)* do Wi-Fi para atividades de sensoriamento, valendo-se das características do ambiente e dos indivíduos. Essa tecnologia foi implementada,

inicialmente, com o intuito de adaptar o sinal às variações do ambiente, resultando em uma transmissão mais eficiente e confiável. Contudo, [Zhang et al. 2020] destacaram que os dados CSI possibilitavam um mapeamento eletromagnético do ambiente, viabilizando a identificação de anomalias no sinal e a autenticação de usuários por meio de sinais e gestos. Por outro lado, [Chen et al. 2023] demonstraram que os aspectos capturados no CSI de dispositivos Wi-Fi também poderiam ser amplamente explorados para fins de autenticação. Apesar disso, abordagens como as de [Shahzad et al. 2013], [Lee and Lee 2017] e [Handa et al. 2018] exigiam alguma ação do usuário para que fosse feita a autenticação, contrastando com nosso estudo, que foca em características biofísicas intrínsecas a cada usuário.

Atualmente, o potencial da autenticação baseada em CSI é amplamente discutido na literatura. [Galdino et al. 2023] desenvolveram um conjunto de dados CSI que inclui características físicas e sinais vitais de seres humanos, enquanto [Soto et al. 2023] apresentaram uma nova metodologia para identificar uma pessoa usando CSI do Wi-Fi, ilustrando que os dados CSI podem ser uma fonte de dados valiosa para a autenticação de indivíduos com a finalidade de controle de acesso. Entretanto, sua implementação prática ainda é pouco explorada, especialmente empregando dispositivos do contexto IoT, como o Raspberry Pi. Além disso, a utilização de equipamentos de tamanho reduzido para coletar as informações necessárias para uma autenticação eficaz representa um desafio significativo, sobretudo considerando a capacidade de extração, armazenamento e processamento destes dados.

Nesse sentido, este manuscrito investiga a viabilidade do uso de dispositivos portáteis para a coleta de dados CSI e propõe uma abordagem baseada em padrões biofísicos dos indivíduos, complementada por técnicas de *machine learning* e algoritmos de classificação. Dessa forma, o artigo avança o estado da arte ao sugerir um método inovador de controle de acesso com autenticação dos usuários utilizando características individuais extraídas do Wi-Fi. No melhor de nossos esforços, este é o primeiro estudo a empregar dados Wi-Fi CSI coletados por Raspberry Pi, baseado em características biofísicas e especificamente voltado para controle de acesso físico. Assim, o estudo traz as seguintes contribuições:

1. *Dataset* rotulado com 5 atividades distintas, compreendendo silhuetas, gestos e leitura labial;
2. Proposta de um sistema de controle de acesso baseado em características biofísicas, extraídas do Wi-Fi com Raspberry Pi; e
3. Avaliação de desempenho dos algoritmos *Support Vector Machine (SVM)*, *Random Forest (RF)*, *K-Nearest Neighbors (KNN)*, *Árvore de Decisão J48* e *Naive Bayes (NB)* para identificação de usuários.

O restante deste estudo está estruturado da seguinte forma: a Seção 2 discute trabalhos anteriores estabelecendo o contexto para nossa pesquisa. A Seção 3 descreve a metodologia adotada, detalhando as abordagens e ferramentas utilizadas. Na Seção 4, apresentamos os experimentos conduzidos, explicando cada passo da execução. A Seção 5 é dedicada à análise e discussão dos resultados obtidos, explorando suas principais implicações. Por fim, a Seção 6 conclui o estudo, resumindo os principais achados e propondo trabalhos futuros.

2. Trabalhos relacionados

Os estudos atuais têm explorado uma variedade de técnicas que fazem uso dos dados de CSI, como o reconhecimento de atividades, gestos, jeito de andar, localização, presença e sensoriamento em geral. As abordagens de autenticação, como pode ser observado em [Ma et al. 2019] e em [Wang et al. 2019], concentram-se, principalmente, nos métodos baseados em padrões, modelos matemáticos e aprendizado profundo, cada um com suas próprias vantagens e desafios.

2.1. Baseado em padrões

A autenticação baseada em padrões é obtida a partir da identificação de comportamentos humanos aproveitando o padrão de variação do CSI. Nesse sentido, [Shah and Kanhere 2017] propuseram um sistema de autenticação de dois fatores (2FA), que utilizava dados CSI de redes Wi-Fi para verificar a proximidade física entre dispositivos. No entanto, a autenticação baseava-se na associação do indivíduo ao seu próprio dispositivo wireless ou a um dispositivo próximo, sendo dependente de um equipamento adicional ficando fora do escopo deste estudo.

A pesquisa de [Wang et al. 2016] inspira o nosso trabalho ao traçarem um perfil do movimento humano a partir da transformação dos dados CSI em espectrogramas, semelhante àqueles gerados por radares *Doppler*. Enquanto o trabalho de [Guo et al. 2017], apresentam uma abordagem para a autenticação de atividades humanas baseadas no início e fim da variância do sinal Wi-Fi. Entretanto, ambos estudos utilizam sensores para aprender e caracterizar as atividades, e também exploraram a faixa de frequência de 2.4 GHz, com menos granularidade para coleta dos dados CSI e diferente dos experimentos deste estudo, realizados com Raspberry Pi na faixa de 5 GHz.

[Tan and Yang 2016] conduziram um trabalho com foco no reconhecimento refinado de gestos com os dedos usando um único dispositivo Wi-Fi comum, sem exigir que o usuário utilizasse quaisquer sensores. Da mesma maneira, os trabalhos de [Ma et al. 2018], [Tian et al. 2018] e [Ren et al. 2019] também utilizaram as informações de estado do canal para reconhecer o movimento de gestos dos usuários. Contudo, apesar da capacidade de reconhecimento, os estudos utilizaram notebooks para coleta dos dados CSI, equipamentos fora do contexto real de IoT.

2.2. Baseado em modelos

O reconhecimento baseado em modelo aproveita a matemática ou a física para descrever e interpretar a variação do sinal causada pelo comportamento humano. Assim, [Zhang et al. 2017] foram pioneiros na construção de modelos ao quantificar a correlação entre a dinâmica dos valores CSI, as velocidades de movimento humano, as partes do corpo e uma atividade específica.

Os trabalhos de [Niu et al. 2018] e [Zhang et al. 2019] propuseram sistemas de reconhecimento de atividade humana usando dispositivos COTS Wi-Fi, conseguindo distinguir usuários através de modelos de detecção baseados em difração. Já [Kong et al. 2021] trouxeram um sistema de autenticação multiusuário utilizando um modelo que mede o Tempo de Chegada (ToA) da propagação do sinal para criação de um perfil e o Ângulo de Chegada (AoA) para separar os dados CSI por usuário. No entanto, essas abordagens sofrem com as variações ambientais, exigindo muitas vezes

uma configuração específica de hardware e uma alta qualidade dos dados CSI coletados, o que pode comprometer a precisão dos modelos de reconhecimento, especialmente em atividades de controle de acesso.

A pesquisa de [Afshar et al. 2022] propôs uma autenticação em ambientes de multiusuários utilizando uma normalização para obter os AoAs e, a partir de *clusters*, identificar quais AoAs correspondiam aos respectivos usuários. Contudo, a pesquisa ocorreu no campo da simulação e trouxe dados fictícios, desconsiderando as variações e ruídos presentes num ambiente real. [Meneghello et al. 2023] realizaram um estudo sobre a limpeza e processamento da fase de resposta da frequência do canal (CFR) do Wi-Fi para estimar o deslocamento *Doppler* em um dispositivo de radiomonitoramento, visando distinguir atividades humanas. Entretanto, o estudo enfrentou dificuldades para discernir movimentos que geram efeitos *Doppler* quase idênticos, mesmo após retreinamento, diminuindo a confiança na capacidade de autenticação.

No contexto de IoT, [Zhao et al. 2021] apresentaram um sistema de autenticação baseado em modelos HMM e Zona de Fresnel para reconhecer os gestos e extrair recursos ocultos de forma robusta e eficientea partir de dados do CSI. Já [Cheng et al. 2021], modelaram a atividade humana utilizando o processo de Markov, empregando múltiplas funções de densidade gaussianas para ajustar os padrões complexos da atividade. Porém, tanto os modelos HMM quanto os baseados na Zona de Fresnel podem ser fortemente afetados pelas diversas interferências observadas no contexto IoT, levando a erros na autenticação de usuários.

2.3. Baseado em aprendizado profundo

O aprendizado profundo pode aprender e extrair automaticamente características significativas dos dados de entrada, eliminando a necessidade de etapas manuais de extração de características. Nesse sentido, [Yousefi et al. 2017] reuniram as principais técnicas de aprendizado profundo, como redes neurais recorrentes (RNN) e de memória de longo e curto prazo (LSTM), demonstrando o desempenho aprimorado de cada uma delas.

Aproveitando-se deste estudo, [Lin et al. 2018] propuseram a segmentação automática de atividades e marcha usando um algoritmo de segmentação automática (ASA), seguido de Resnet para validar usuários legais e reconhecer usuários ilegais. Já [Zou et al. 2018] introduziram o *Autoencoder Long-term Recurrent Convolutional Network* (AE-LRCN), para higienizar o ruído em dados CSI brutos, extrair recursos representativos de alto nível e revelar as dependências temporais entre os dados para o reconhecimento preciso da atividade humana. Entretanto, no contexto de controle de acesso, essas abordagens enfrentam desafios relacionados à complexidade computacional, à necessidade de grandes volumes de dados para um treinamento eficaz, a sensibilidade às variações na disposição física do ambiente e às interferências de outros dispositivos, comprometendo a robustez do sistema em cenários reais.

[Chen et al. 2019] apresentaram um estudo que utiliza memória bidirecional de longo prazo baseada em atenção (ABLSTM) para reconhecimento passivo de atividade humana usando sinais Wi-Fi CSI. Na mesma época, [Ding and Wang 2019] propuseram o HARNN, uma abordagem de reconhecimento de atividade humana baseada em Wi-Fi CSI usando rede neural recorrente profunda para reconhecer diferentes atividades

humanas. Ambas pesquisas contribuíram significativamente para o reconhecimento de atividades humanas usando informações CSI. No entanto, ambas também são dependentes da complexidade computacional, necessidade de treinamento extensivo e sensibilidade ambiental, aspectos críticos no contexto IoT e no controle de acesso.

[Gu et al. 2021] aplicaram aprendizado profundo ao comportamento físico do usuário capturado pelas informações do estado do canal Wi-Fi (CSI) para identificar distinguir usuários legítimos de falsificadores. Já [Gu et al. 2022] procuraram autenticar usuários pela dinâmica da digitação de teclas durante tentativas de login. No entanto, as pesquisas focaram principalmente no comportamento do usuário e no ritmo de digitação, deixando brechas para tentativas de imitação do comportamento físico dos usuários autorizados (personificação) e tornando essas abordagens inadequadas para aplicações de controle de acesso.

Apesar dos avanços em estudos utilizando CSI para diversas aplicações, implementações práticas focadas na autenticação de pessoas ainda são escassas na literatura. Em contraste com os estudos anteriores, nosso trabalho diferencia-se dos demais pela simplicidade da proposta, pelo uso de Raspberry Pi para coleta dos dados na frequência de 5 GHz e pelo emprego de características biofísicas (que identificam o usuário pelo que ele é) e não por atividades realizadas (que identificam o usuário por atividades que ele faz), visando controlar o acesso por meio da autenticação pelo Wi-Fi. A Tabela 1 confronta os manuscritos relacionados com o atual estudo e ressalta que ainda há espaço para a implementação de um sistema de controle de acesso a partir de dados CSI. Destaca-se que, até onde se tem conhecimento, o modelo proposto neste trabalho é o primeiro a utilizar características combinadas e extraídas do CSI do Wi-Fi por dispositivos portáteis no contexto de controle de acesso, apresentando-se como uma proposta complementar de segurança.

Tabela 1. Comparativo entre trabalhos relacionados.

Estudo	Abordagem	Dispositivo de Coleta	Frequência utilizada / Largura de banda	Ferramenta de extração CSI	Aplicação em controle de acesso
[Shah and Kanhere 2017]	Padrões	Notebook	2.4GHz (20MHz)	Não especificado	Não
[Wang et al. 2016]	Padrões	Notebook	5GHz (80MHz)	Linux 802.11n CSI Tool	Não
[Guo et al. 2017]	Padrões	Notebook	2.4GHz (20MHz)	Não especificado	Não
[Tan and Yang 2016]	Padrões	Notebook	2.4GHz (20MHz)	Não especificado	Não
[Ma et al. 2018]	Padrões	Notebook	5GHz (20MHz)	Open RF Linux 802.11n CSI Tool	Não
[Tian et al. 2018]	Padrões	Notebook	2.4GHz (20MHz) e 5GHz (80MHz)	Linux 802.11n CSI Tool	Não
[Ren et al. 2019]	Padrões	Mini-ITX	5.36GHz (40MHx)	Não especificado	Não
[Zhang et al. 2017]	Modelos	Par de Antenas	5.24GHz	Não especificado	Não
[Niu et al. 2018]	Modelos	Par de Antenas	5.24GHz	Não especificado	Não
[Zhang et al. 2019]	Modelos	Par de Antenas	5.24GHz	Linux 802.11n CSI Tool	Não
[Kong et al. 2021]	Modelos	Notebook	2.4GHz até 70MHz) e 5GHz (até 200MHz)	Atheros CSI-Tool	Não
[Afshar et al. 2022]	Modelos	MATLAB	-	-	Não
[Meneghello et al. 2023]	Modelos	Netgear X4S AC2600	5GHz (80MHz)	Nexmon CSI Tool	Não
[Zhao et al. 2021]	Modelos	Intel NUC	5GHz (20MHz)	Não especificado	Não
[Cheng et al. 2021]	Modelos	Lenovo Desktop	5.32GHz	Linux 802.11n CSI Tool	Não
[Lin et al. 2018]	Aprendizado Profundo	Notebook	Não especificado	Linux 802.11n CSI tool	Não
[Zou et al. 2018]	Aprendizado Profundo	-	-	TP-Link C7A4	Não
[Chen et al. 2019]	Aprendizado Profundo	Notebook	Não especificado	Linux 802.11n CSI tool	Não
[Ding and Wang 2019]	Aprendizado Profundo	Notebook	5GHz (20MHz)	Linux 802.11n CSI tool	Não
[Gu et al. 2021]	Aprendizado Profundo	Mini PC	2.4GHz (20MHz) e 5GHz (80MHz)	Linux 802.11n CSI tool	Não
[Gu et al. 2022]	Aprendizado Profundo	Mini PC	5GHz (80MHz)	Linux 802.11n CSI tool	Não
Presente estudo	**Padrões**	**Raspberry Pi**	**5GHz (80MHz)**	**Nexmon CSI Tool**	**Sim**

3. CSI

Esta seção apresenta uma visão geral sobre as propriedades do *Channel State Information*, os princípios básicos da autenticação de usuários e descreve a arquitetura do sistema proposto para o controle de acesso.

3.1. Propriedades do CSI

O CSI do Wi-Fi registra informações sobre como os sinais sem fio se propagam do transmissor para o receptor, descrevendo o comportamento das ondas eletromagnéticas ao longo das frequências. Essas informações incluem a amplitude e a fase do sinal, que podem ser alteradas por reflexões, obstruções e outros fatores no ambiente. Cada elemento do CSI mostra como o ambiente impacta a propagação do sinal, formando uma função chamada Resposta em Frequência do Canal (CFR). Em sistemas Wi-Fi que usam múltiplas antenas, a tecnologia divide o espectro em várias subportadoras através de uma técnica chamada OFDM (Multiplexação por Divisão de Frequência Ortogonal). O transmissor envia sinais de treinamento especiais no início da transmissão, que o receptor usa para estimar como o canal Wi-Fi afeta cada subportadora. Essencialmente, isso ajuda o receptor a entender o comportamento do sinal em diferentes condições, ajustando-se para garantir uma melhor transmissão e recepção dos dados.

Segundo [Ma et al. 2019], a matriz CSI, ilustrada na Figura 1, é um conjunto tridimensional de valores complexos que o receptor estima a partir do sinal recebido. Este processo envolve a remoção do prefixo cíclico, o desmapeamento e a demodulação OFDM. Na prática, o CSI medido é afetado por canais de multipercurso, processamento no transmissor e receptor, e inconsistências no hardware e software. A representação do CSI no domínio *baseband* é uma abstração complexa que considera todos esses fatores, incluindo deslocamentos cíclicos e variações no tempo e frequência de amostragem.

A série temporal das matrizes CSI capta as mudanças no canal MIMO ao longo do tempo, frequência e espaço. Para um canal MIMO-OFDM com (M) antenas transmissoras, (N) antenas receptoras e (K) subportadoras, a matriz CSI forma um cubo de dados, expresso como $(H \in C^{(N \times M \times K \times T)})$. Este cubo registra como os sinais sofrem atenuação de amplitude e deslocamento de fase ao percorrerem múltiplos caminhos. Assim, o CSI fornece uma quantidade de informações muito mais rica do que outras métricas, como o Indicador de Força do Sinal Recebido (RSSI).

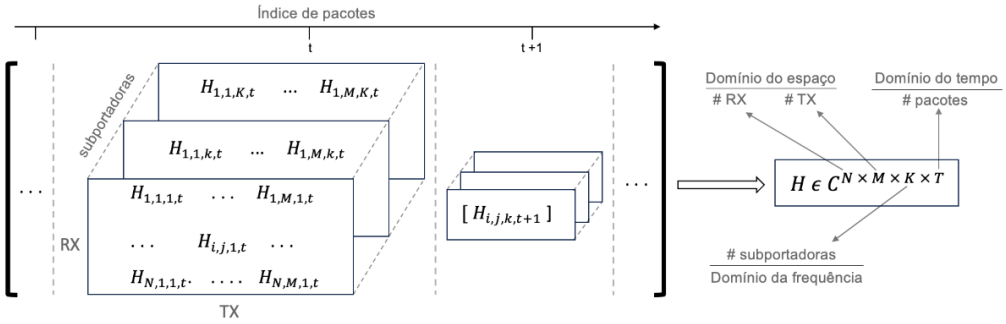


Figura 1. Matriz CSI adaptada de [Ma et al. 2019].

Os cálculos matriciais sobre os dados brutos do CSI resultam em números complexos que capturam como o sinal varia ao longo do tempo. Esses números são representados como $z = a + bi$, onde a é a parte real, b é a parte imaginária, e i é a unidade imaginária, com a propriedade $i^2 = -1$. Dessa forma, podemos obter a Amplitude (ou módulo) de um número complexo usando a equação $|z| = \sqrt{a^2 + b^2}$. Aqui, a é a parte real e b é a parte imaginária. Também é possível calcular a Fase (ou ângulo) θ, que é o ângulo formado pelo vetor que representa o número complexo no plano complexo em relação ao

eixo real. Isso é feito com a fórmula $\theta = \text{atan2}(b, a)$, onde $\text{atan2}(b, a)$ é a função arco tangente de duas variáveis que retorna o ângulo cuja tangente é b/a, considerando o sinal de ambos para determinar o quadrante correto. Dessa maneira, as variações na amplitude e na fase do sinal proporcionam uma compreensão mais detalhada do comportamento analisado.

[Wu et al. 2017] relataram que identificando padrões no sinal e relacionando-os com determinadas características ou comportamentos dos usuários é possível, a partir de uma abordagem apoiada em aprendizado de máquina, identificar um usuário com precisão. Nesse sentido, nosso estudo permeia os métodos de pré-processamento do sinal, extração das características e aplicação de algoritmos de aprendizado de máquina para classificar padrões.

3.2. Autenticação com CSI

Segundo [Meneghello et al. 2023], a utilização do CSI para autenticação de seres humanos explora a ideia de que diferentes usuários geram variações únicas de CSI quando estão dentro da cobertura do sinal. Isso significa que é possível reconhecer a identidade de um usuário analisando o perfil dinâmico do CSI. Contudo, a autenticação de usuários utilizando dados CSI para o controle de acesso físico é uma abordagem inovadora.

Essencialmente, existem dois tipos principais de autenticação de usuário, uma baseada nas flutuações do CSI causadas pelos movimentos do usuário, como passos, atividades e gestos, e outra que utiliza as características de propagação estática do CSI quando o usuário está parado. Assim, uma investigação supervisionada, rotulando os dados de entrada e tratando os problemas de reconhecimento como classificação, facilita a identificação de padrões e a regularidades nos dados.

A abordagem baseada em ação é amplamente empregada devido à capacidade do movimento humano de gerar flutuações evidentes no CSI, que podem ser medidas e processadas por diversos algoritmos disponíveis. Por outro lado, a autenticação baseada em imobilidade exige a extração de características biofísicas únicas, como silhueta, taxa de água, gordura e músculo, ou pela combinação de localização do usuário. Assim, a autenticação do usuário com base no CSI oferece uma maneira promissora de identificar indivíduos com precisão, explorando as nuances das variações do sinal.

3.3. Proposta de controle de acesso

Neste estudo, com o objetivo de capturar tanto características biofísicas, como silhuetas e movimentos, quanto variações comportamentais dos usuários, propomos um sistema de autenticação para controle de acesso físico em ambientes monitorados, conforme a Figura 2. Inicialmente, os dados CSI são coletados por dois Raspberry Pi operando em modo monitor. Durante a captura, é feita uma transformação do domínio do tempo para o domínio da frequência, entregando o resultado em formato hexadecimal. Em seguida, os dados precisam ser reordenados com o *FFT Shift* para centralizar o zero da frequência, permitindo a conversão em números complexos. Com isso, é possível extrair a amplitude e a fase do sinal e realizar o pré-processamento.

O pré-processamento dos dados envolve diversas operações para extrair as características desejadas. Inicialmente, os valores do CFR são normalizados pela amplitude média dos 242 subcanais monitorados, visando remover amplificações

indesejadas. Depois, é aplicado um algoritmo de sanitização de fase, com um parâmetro de ajuste fixo em $\lambda = 10^{-1}$. Os valores do CFR são então reconstruídos e combinados, resultando em um vetor complexo de CFR com 245 componentes, contendo amplitudes e fases. Além disso, utilizamos os filtros de *Hampel* e *Savitzky-Golay* para obter uma visão mais clara e precisa do comportamento do sinal ao longo do tempo.

Após o pré-processamento, é feita uma análise de como as amplitudes variam em cada subportadora conforme os dados capturados e aplicado o algoritmo *Random Forest* para extrair as subportadoras mais relevantes. Em seguida, desenvolvemos um modelo de aprendizado de máquina, treinado com validação cruzada de dez etapas, para estimar as características individuais de cada usuário. Finalmente, a autenticação do usuário é realizada por meio da classificação dos dados, utilizando o algoritmo *KNN*. Dessa forma, usuários autorizados têm suas identidades reconhecidas e o acesso é concedido conforme as permissões concedidas.

Figura 2. Modelo proposto.

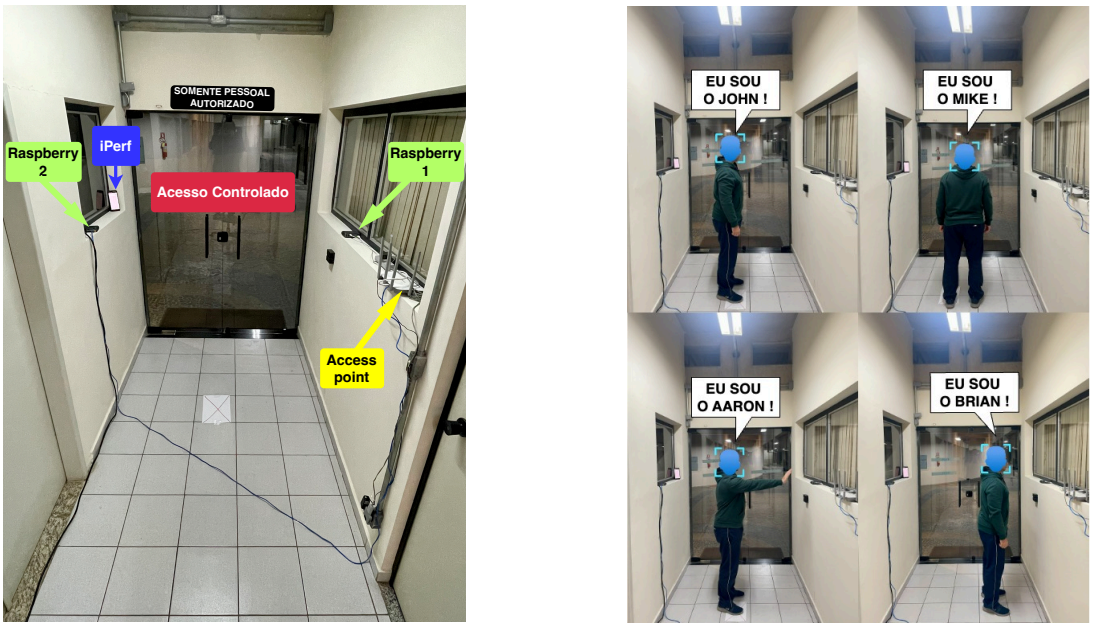
4. Experimentos

Esta seção tem por objetivo apresentar como foram realizados os experimentos, a coleta dos dados e qual foi o protocolo de captura utilizado. Assim, entende-se que é possível replicar o trabalho e agregar melhorias no futuro.

A captura dos dados CSI foi realizada num corredor com acesso a um ambiente controlado, ilustrado na Figura 3. O corredor, de dimensões de 1,5 m (largura) x 15 m (profundidade) x 3 m (altura), foi instrumentado para simular a autenticação por meio do Wi-Fi. O local foi escolhido por canalizar o acesso e pela maior capacidade reflexiva, favorecendo as tecnologias MIMO e OFDM presentes no Wi-Fi.

Neste cenário, foram utilizados como receptores (Rx) dois dispositivos Raspberry Pi 4 modelo B, com processador 64-Bit quad-core Cotex-A72, 8 GB LPDDR4 de RAM, capacidade de conexão wireless no padrão 802.11b/g/n/ac, bluetooth 5.0, capacidade PoE e consumindo apenas 5V/3A, podendo ser alimentada por *Powerbank* com conexão USB-C. Este equipamento foi escolhido por ser pequeno (25x52x10 mm), com baixo consumo energético em comparação com dispositivos utilizados em outros estudos e por ser ideal para o desenvolvimento de inúmeras aplicações de automação direcionadas a IoT e comunicação Machine to Machine (M2M).

Os Raspberry Pi foram controlados por um notebook DELL Inspiron 15 Gaming 7567, com sistema operacional Windows 10 Home, processador Intel octa-core i7-7700HQ 2.80 GHz e 16 GB de memória RAM, com acesso por ssh. E para simular o sinal Wi-Fi de uma rede fictícia, empregou-se um roteador TP-Link Archer C60 configurado



(a) Corredor. **(b) Capturas.**

Figura 3. Experimentos.

como transmissor (TX), operando uma rede em 5 GHz a 80 MHz, no canal 36. O protocolo de captura seguiu o exibido na Tabela 2, considerando os objetos de interesse posicionados a 75 cm de distância entre os 2 dispositivos.

Foram monitorados seis usuários com características físicas diferentes, sendo 5 do sexo masculino e 1 do sexo feminino. Para fins de precisão e reprodutibilidade futura, os usuários possuíam entre 1,65 m e 1,85 m de altura, entre 60 e 93 quilos e entre 18 e 43 anos. Foram utilizados, ainda, um dispositivo celular para geração de tráfego empregando a aplicação *iperf2* com a taxa de aproximadamente 1000 pacotes UDP por segundo, executado num sistema Android e configurado com os seguintes parâmetros: `-c 192.168.1.1 -u -b 500M -t 60 -i 1 -l 1400`.

Durante as capturas foram realizadas cinco atividades distintas. Nas atividades *(A), (B), (C) e (D)*, os usuários mantiveram uma distância de 75 cm em relação aos dispositivos, enquanto na atividade *(E)* estavam a 30 cm do Raspberry 1 e a 1,20 m do Raspberry 2. Na atividade (A) posicionavam-se com a silhueta frontal voltada para

Tabela 2. Protocolo de captura.

Usuário	Altura	Peso	Gênero	Atividade	Total de registros por Dispositivo	Tempo de atividade (s)	Total de capturas
1	1.78 m	79 kg	M	A, B, C, D e E	Rasp 1: 10, Rasp 2: 10	10	100
2	1.66 m	77 kg	M	A, B, C, D e E	Rasp 1: 10, Rasp 2: 10	10	100
3	1.85 m	93 kg	M	A, B, C, D e E	Rasp 1: 10, Rasp 2: 10	10	100
4	1.65 m	64 kg	F	A, B, C, D e E	Rasp 1: 10, Rasp 2: 10	10	100
5	1.83 m	90 kg	M	A, B, C, D e E	Rasp 1: 10, Rasp 2: 10	10	100
6	1.73 m	90 kg	M	A, B, C, D e E	Rasp 1: 10, Rasp 2: 10	10	100

o Raspberry 1 e a traseira voltada para o Raspberry 2. Já na atividade (B), estavam com a silhueta lateral direita voltada para o Raspberry 1 e a esquerda voltada para o Raspberry 2. A atividade (C) exigia que os usuários ficassem de frente para o Raspberry 1 e levantassem o braço direito com a mão aberta em direção ao Raspberry 1. Na atividade (D), posicionavam-se de frente para o Raspberry 1 e levantavam o braço direito com a mão aberta em direção ao peitoral esquerdo. Por fim, na atividade (E), os usuários posicionavam-se de frente para o Raspberry 1 e pronunciavam a palavra *(ALOHOMORA)*. Ao todo, o conjunto de dados analisado é composto por 600 capturas de 10 segundos, somando aproximadamente 6.000.000,00 instâncias que registraram os resultados das reflexões, atenuações e difrações sofridas pelo sinal eletromagnético ao longo do seu percurso no ambiente analisado.

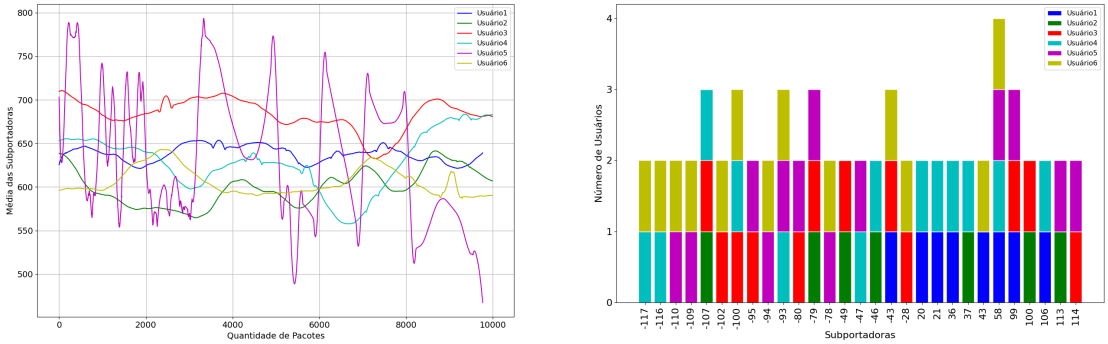
Além disso, cada atividade teve um *delay* inicial de 5 segundos para o início da gravação e a ferramenta foi calibrada para que cada sessão de captura tivesse a duração de 10 segundos, garantindo assim, a consistência, precisão e padronização dos dados coletados. Ressalta-se, também, que foi utilizado o modo *Line-of-Sight* (LOS), evitando a presença de obstáculos entre o ponto de transmissão e o ponto de recepção. Dessa maneira, os cenários sofrem menor atenuação e dispersão do sinal, proporcionando uma comunicação mais limpa e robusta.

5. Resultados

As capturas dos dados CSI nos experimentos foram realizadas utilizando a ferramenta Nexmon, proposta por [Gringoli et al. 2019]. Os dados extraídos incluíram informações de 256 subportadoras, com cada arquivo contendo aproximadamente 10.000 pacotes. Os dados CSI estão incorporados dentro do *payload* do pacote UDP, embutidos nos arquivos PCAP gerados pela ferramenta. Para facilitar a manipulação e análise dos dados, o conteúdo do *payload* foi extraído e convertido para arquivos CSV. As interferências no sinal foram descritas por atributos como *Magic Bytes*, *RSSI*, *FrameControl Byte*, *Source Mac*, *Sequence Number*, *Core and Spatial Stream*, *Chanspec*, *Chip Version* e *CSI Data*. No entanto, apenas o atributo *CSI Data* foi considerado relevante para a análise focada em autenticação para controle de acesso, sendo os demais descartados.

O atributo *CSI Data* forneceu números complexos resultantes de cálculos matriciais aplicados aos dados brutos do CSI. Após a transformação matemática, foram acessadas informações das 256 subportadoras, embora algumas sejam nulas (-128, -127, -126, -125, -124, -123, -1, 0, 1, 123, 124, 125, 126, 127) e outras pilotos (-103, -75, -39, -11, 11, 39, 75, 103). Portanto, restaram 234 subportadoras úteis para análise em cada captura.

Para obter uma visão mais clara dos dados CSI, aplicou-se um pré-processamento utilizando técnicas como o Filtro de Hampel, Filtro Passa-Baixa, Transformada Discreta de Hilbert, Média Móvel, Filtro de Savitzky-Golay, Filtro de Kalman e Transformada Wavelet Discreta (DWT). Dentre estes, os filtros de *Hampel* e *Savitzky-Golay* proporcionaram os maiores ganhos na suavização do sinal, preservando suas características e possibilitando identificar que cada usuário influenciava as subportadoras de maneira distinta, como visto na Figura 4a, onde estão representadas as amplitudes médias das subportadoras afetadas por cada usuário durante a atividade "A".



(a) Amplitude média. **(b) Suportadoras em comum.**

Figura 4. Influência dos usuários nas subportadoras.

A Figura 4b apresenta as 29 subportadoras que tiveram influência comum no reconhecimento de cada usuário ao longo das atividades. Dentre estas, destaca-se a suportadora 58, aparecendo como uma das mais importantes no reconhecimento dos usuários 1, 4, 5 e 6.

A visualização do comportamento distinto das subportadoras de acordo com o usuário analisado, permitiu confirmar que aspectos biofísicos e comportamentais podem ser utilizados para autenticação dos usuários e que, por suas nuances claramente distintas, contribuem para um bom desempenho do modelo no reconhecimento dos usuários e atividades.

Verificou-se, também, a influência do uso de filtros no desempenho do modelo. Uma análise dos dados utilizando o algoritmo *KNN* mostrou que mesmo sem a aplicação do filtro de Hampel o modelo ainda mantém um alto desempenho para reconhecer os usuários, conforme ilustrado na Tabela 3. Entretanto, a utilização dos filtros, de uma maneira geral, é relevante pois reduz a complexidade, o tamanho do modelo e seu tempo de construção. Verifica-se, também, que quanto maior a quantidade de dados coletados, maior a granularidade de informações obtidas pelo modelo e, consequentemente, maior a acurácia na autenticação dos usuários.

Tabela 3. Comparativo de desempenho utilizando o filtro de Hampel.

Reconhecimento	Atividade	Quantidade de pacotes	Tempo de construção	Desempenho (%)
Sem filtro	A	10.000	0.02	99,92
Com filtro	A	10.000	0.01	99,99
Sem filtro	A	20.000	0.04	99.92
Com filtro	A	20.000	0.02	99,99
Sem filtro	A	30.000	0.09	99,90
Com filtro	A	30.000	0.03	99,99

Para avaliar a abrangência do modelo, testou-se a capacidade de autenticação considerando todas as atividades do conjunto de dados. Os resultados mostram que cada atividade causa uma interferência única no sinal, conforme indicado nos mapas de calor da Figura 5. As diferenças observadas indicam que é possível autenticar o usuário tanto por

suas características intrínsecas quanto pela atividade realizada, viabilizando o uso dessas informações para autenticação e controle de acesso. Ressalta-se que o CSI é diretamente influenciado pelo usuário monitorado, com a correlação das subportadoras variando ao longo do tempo conforme suas características biofísicas e ações.

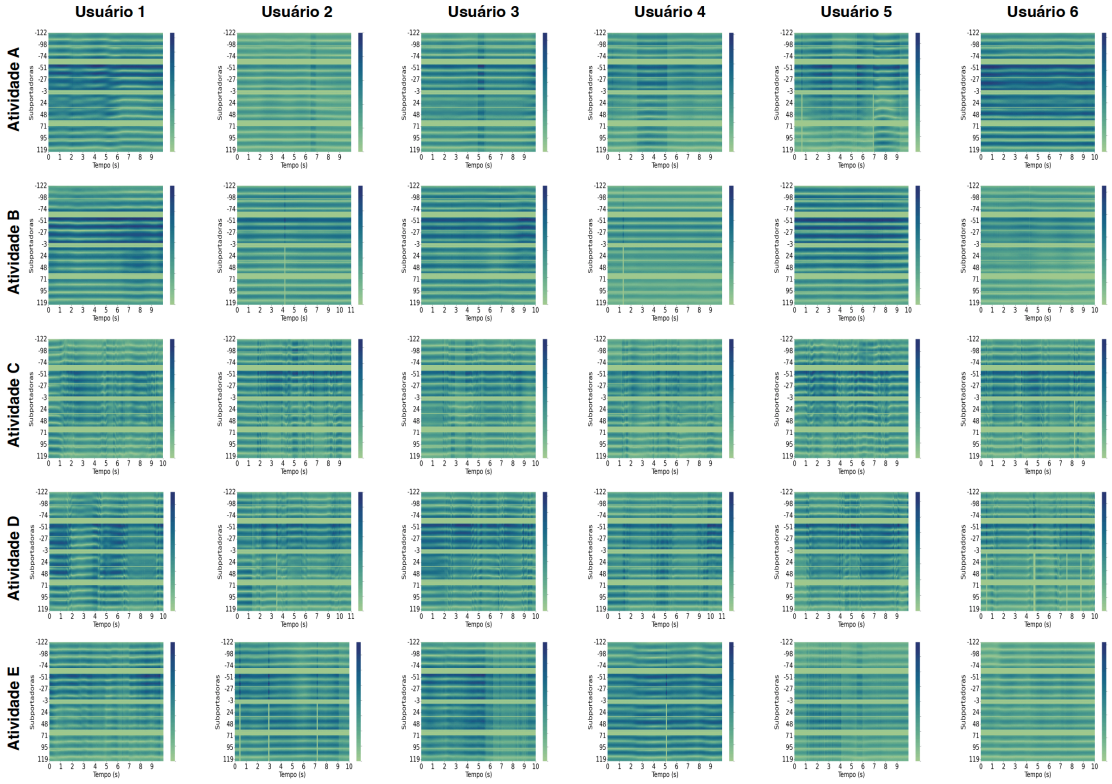


Figura 5. Subportadoras mais afetadas pelos usuários durante as atividades

A partir das inferências observadas, separou-se os dados da atividade (A) para avaliação. A seleção desta atividade justifica-se por ser a atividade que exige menos ação do usuário, extraindo o máximo de informações peculiares de cada indivíduo. Além disso, utilizou-se apenas uma amostra de 10 segundos por usuário, com o objetivo de identificar o melhor desempenho com o mínimo de amostras. Salienta-se, também, que todos os algoritmos foram treinados com validação cruzada em 10 etapas, evitando o sobreajuste e fornecendo uma estimativa mais realista.

5.1. Desempenho do modelo

A acurácia média global foi medida empregando-se os algoritmos *KNN*, *RF*, *SVM*, *J48* e *NB* com e sem a utilização do Filtro de Hampel, conforme visto na Tabela 4. A comparação dos resultados mostra que a utilização do filtro provoca uma melhora no desempenho. Entretanto, sabe-se que o processo de filtragem pode eliminar informações relevantes nos dados, levando a interpretações errôneas. Por isso, para fins de medição do desempenho do modelo, este trabalho considerou apenas as métricas obtidas a partir dos dados não filtrados. Dentre estes, o *KNN* foi o que apresentou o melhor desempenho, chegando a alcançar uma precisão de 99,92% para distinguir os usuários, enquanto os demais atingiram, 99,88%, 99,72%, 99,60% e 87,36%, respectivamente.

Tabela 4. Resultado dos classificadores.

Métricas	Com Filtro					Sem Filtro				
	KNN	**RF**	**SVM**	**J48**	**NB**	**KNN**	**RF**	**SVM**	**J48**	**NB**
Acurácia Média (%)	99.99	99.99	100.00	99.93	94.11	99.92	99.88	99.72	99.60	87.36
F1-Score	100.00	100.00	100.00	100.00	99.50	100.00	100.00	99.72	99.80	97.00
Tempo de Construção (s)	0.02	13.92	153.81	31.27	2.85	0.01	15.85	289.98	32.74	2.83
Kappa	1.00	1.00	1.00	0.99	0.92	0.99	0.99	0.99	0.99	0.84
MCC	1.00	1.00	1.00	0.99	0.92	0.99	0.99	0.99	0.99	0.85

O *KNN* foi escolhido por diversos fatores, dentre eles, a maior acurácia e um menor tempo de construção. O resultado é refletido pela TPR média de 0,999 para reconhecer as características biofísicas dos indivíduos, indicando a uma alta capacidade de autenticação do modelo. Sua característica transdutiva desempenha um papel decisivo em nossa abordagem de autenticação, pois permite que o modelo proposto seja adaptativo e preciso. O classificador faz previsões baseadas diretamente nos exemplos de treinamento disponíveis, e portanto não necessita construir um modelo geral para capturar todas as nuances dos dados. Isso facilita a comparação das características de acesso com as características dos usuários autorizados, garantindo uma identificação precisa mesmo com variações sutis nos dados de CSI capturados.

Além disso, a transdutividade do *KNN* facilita a atualização contínua do sistema. Sempre que novos usuários forem adicionados ou ajustes nos dados de treinamento forem necessários, o algoritmo pode integrar essas mudanças facilmente sem a necessidade de reconfigurar completamente o modelo. Essa versatilidade é essencial para ambientes dinâmicos, permitindo uma manutenção eficiente e assegurando que o sistema de controle de acesso permaneça robusto e confiável.

Os altos valores de desempenho dos modelos são elucidados pela Função de Distribuição Cumulativa (CDF), mostrando que as características individuais dos usuários resultam em padrões distintos no sinal, como mostrado na Figura 6. Neste caso, observa-se uma aproximação semelhante a uma distribuição mais linear para alguns usuários, enquanto para outros uma distribuição mais semelhante a uma Gaussiana.

As métricas obtidas nos experimentos apresentaram resultados que permitem a autenticação dos usuários, possibilitando identificar aqueles com acesso autorizado. Ainda, acredita-se que seria possível obter uma melhor performance empregando mais equipamentos de captura, coletando mais dados, eliminando o nível de ruído do ambiente e analisando o espectro eletromagnético numa câmara totalmente anecóica. Contudo, o estudo foi norteado para uma aplicação prática, com o mínimo de equipamentos possíveis.

6. Conclusão e Trabalhos Futuros

Este estudo traz à tona a utilização dos dados do Wi-Fi como uma inovação para autenticação de usuários em sistemas de controle de acesso físico. Empregando dispositivos Raspberry Pi num ambiente controlado e aplicando técnicas de aprendizado supervisionado, foi possível identificar usuários com acurácia de 99,92% utilizando o classificador *K-Nearest Neighbors (KNN)*. A pesquisa validou que características biofísicas e comportamentais capturadas pelo CSI podem ser utilizadas de forma confiável para autenticação de usuários, oferecendo uma alternativa eficiente aos

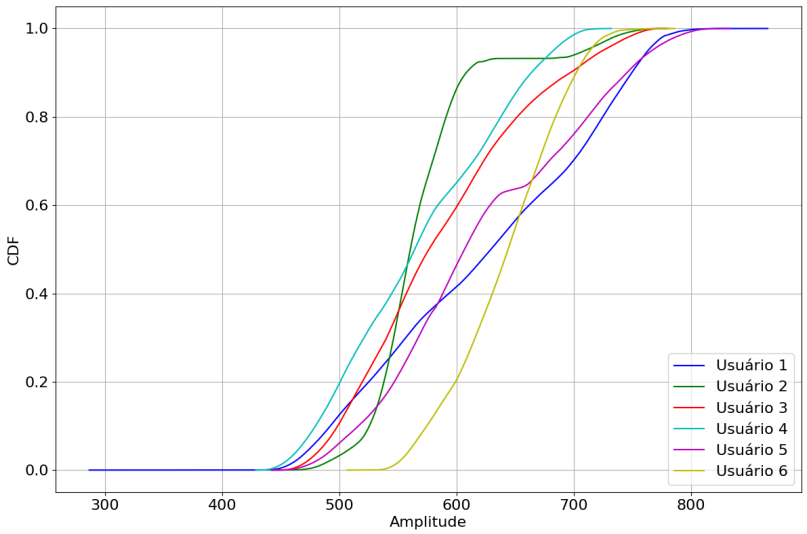


Figura 6. Curvas de Função de Distribuição Acumulada (CDF) para cada usuário.

métodos tradicionais de controle de acesso, coletando dados passivamente para confirmar credenciais sem a necessidade de interação direta. Além disso, a transdutividade do algoritmo é especialmente benéfica, pois permite que o sistema se adapte facilmente a novas entradas de dados sem a necessidade de reconfigurações exaustivas. Portanto, o estudo mostra-se robusto para ambientes dinâmicos e em constante evolução.

Como trabalhos futuros, visualiza-se encorpar a base de dados, integrar mais dispositivos Raspberry Pi para capturar uma quantidade maior de características biofísicas, avaliar o modelo em outros cenários e estudar a viabilidade de utilizar aprendizado não supervisionado.

Agradecimentos

Este trabalho tem apoio financeiro do Programa de Pós-graduação em Aplicações Operacionais—PPGAO/ITA, da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) processo #2020/09850-0 e #2022/00741-0, do CNPq e da CAPES.

Referências

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.

Chen, C., Song, H., Li, Q., Meneghello, F., Restuccia, F., and Cordeiro, C. (2023). Wi-fi sensing based on ieee 802.11bf. *IEEE Communications Magazine*, 61(1):121–127.

Chen, Z., Zhang, L., Jiang, C., Cao, Z., and Cui, W. (2019). Wifi csi based passive human activity recognition using attention based blstm. *IEEE Transactions on Mobile Computing*, 18(11):2714–2724.

Cheng, X., Huang, B., and Zong, J. (2021). Device-free human activity recognition based on gmm-hmm using channel state information. *IEEE Access*, 9:76592–76601.

Ding, J. and Wang, Y. (2019). Wifi csi-based human activity recognition using deep recurrent neural network. *IEEE Access*, 7:174257–174269.

Galdino, I., Soto, J. C. H., Caballero, E., Ferreira, V., Ramos, T. C., Albuquerque, C., and Muchaluat-Saade, D. C. (2023). ehealth csi: A wi-fi csi dataset of human activities. *IEEE Access*, 11:71003–71012.

Gringoli, F., Schulz, M., Link, J., and Hollick, M. (2019). Free your csi: A channel state information extraction platform for modern wi-fi chipsets. WiNTECH '19, page 2128, New York, NY, USA. Association for Computing Machinery.

Gu, Y., Wang, Y., Wang, M., Pan, Z., Hu, Z., Liu, Z., Shi, F., and Dong, M. (2022). Secure user authentication leveraging keystroke dynamics via wi-fi sensing. *IEEE Transactions on Industrial Informatics*, 18(4):2784–2795.

Gu, Y., Yan, H., Dong, M., Wang, M., Zhang, X., Liu, Z., and Ren, F. (2021). Wione: One-shot learning for environment-robust device-free user authentication via commodity wi-fi in manmachine system. *IEEE Transactions on Computational Social Systems*, 8(3):630–642.

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.

Handa, J., Singh, A., Goyal, A., and Aggarwal, P. (2018). Behavioral biometrics for continuous authentication. In *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pages 284–289.

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. MobiHoc '21, page 3140, New York, NY, USA. Association for Computing Machinery.

Lee, W.-H. and Lee, R. B. (2017). Sensor-based implicit authentication of smartphone users. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 309–320, Denver, CO, USA.

Lin, C., Hu, J., Sun, Y., Ma, F., Wang, L., and Wu, G. (2018). Wiau: An accurate device-free authentication system with resnet. In *2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 1–9.

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

Ma, Y., Zhou, G., Wang, S., Zhao, H., and Jung, W. (2018). Signfi: Sign language recognition using wifi. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2(1).

Meneghello, F., Garlisi, D., Fabbro, N. D., Tinnirello, I., and Rossi, M. (2023). Sharp: Environment and person independent activity recognition with commodity ieee 802.11 access points. *IEEE Transactions on Mobile Computing*, 22(10):6160–6175.

Niu, K., Zhang, F., Chang, Z., and Zhang, D. (2018). A fresnel diffraction model based human respiration detection system using cots wi-fi devices. UbiComp '18. Association for Computing Machinery.

Ren, S., Wang, H., Gong, L., Xiang, C., Wu, X., and Du, Y. (2019). Intelligent contactless gesture recognition using wlan physical layer information. *IEEE Access*, 7:92758–92767.

Shah, S. W. and Kanhere, S. S. (2017). Wi-auth: Wifi based second factor user authentication. MobiQuitous 2017, page 393402, New York, NY, USA. Association for Computing Machinery.

Shahzad, M., Liu, A. X., and Samuel, A. (2013). Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it. MobiCom '13, pages 39–50, New York, NY, USA. Association for Computing Machinery.

Soto, J. C. H., Galdino, I., Caballero, E., Muchaluat-Saade, D., and Albuquerque, C. (2023). Single person identification using wi-fi signals. In *2023 IEEE Latin-American Conference on Communications (LATINCOM)*, pages 1–6.

Tan, S. and Yang, J. (2016). Wifinger: leveraging commodity wifi for fine-grained finger gesture recognition. In *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 201–210.

Tian, Z., Wang, J., Yang, X., and Zhou, M. (2018). Wicatch: A wi-fi based hand gesture recognition system. *IEEE Access*, 6:16911–16923.

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, page 363373, New York, NY, USA. Association for Computing Machinery.

Wang, Z., Jiang, K., Hou, Y., Dou, W., Zhang, C., Huang, Z., and Guo, Y. (2019). A survey on human behavior recognition using channel state information. *IEEE Access*, 7:155986–156024.

Wu, D., Zhang, D., Xu, C., Wang, H., and Li, X. (2017). Device-free wifi human sensing: From pattern-based to model-based approaches. *IEEE Communications Magazine*, 55(10):91–97.

Yousefi, S., Narui, H., Dayal, S., Ermon, S., and Valaee, S. (2017). A survey on behavior recognition using wifi channel state information. *IEEE Communications Magazine*, 55(10):98–104.

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, 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).

Zhang, Y., Zheng, Y., Zhang, G., Qian, K., Qian, C., and Yang, Z. (2020). Gaitid: Robust wi-fi based gait recognition. In *Wireless Algorithms, Systems, and Applications: 15th International Conference, WASA 2020, Qingdao, China, September 13–15, 2020, Proceedings, Part I 15*.

Zhao, Y., Gao, R., Liu, S., Xie, L., Wu, J., Tu, H., and Chen, B. (2021). Device-free secure interaction with hand gestures in wifi-enabled iot environment. *IEEE Internet of Things Journal*, 8(7):5619–5631.

Zou, H., Zhou, Y., Yang, J., Jiang, H., Xie, L., and Spanos, C. J. (2018). Deepsense: Device-free human activity recognition via autoencoder long-term recurrent convolutional network. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6.