Detecção de pessoas e dispositivos utilizando Channel State Information: IDS com features de camada física

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

[1]Divisão de Ciência da Computação – ITA – São Jose dos Campos, SP – Brazil

{trindade,felipefsa,ljr}@ita.br

Abstract. *Intrusion Detection Systems in Networks (NIDS) have been extensively developed over time. However, sophisticated attacks have demanded additional layers of protection. Thus, this study proposes to use data from Channel State Information (CSI) Wi-Fi with machine learning techniques for detection at the physical and link layers, aiming to identify unauthorized access attempts to a Wi-Fi network. The study analyzes 70,513 instances collected in two environments and identifies activities considered malicious with 94.24% accuracy, using the RandomForest algorithm. It stands out as an innovative approach, exploring CSI data and incorporating characteristics from layers 1 and 2 in the context of NIDS.*

Resumo. *Sistemas de Detecção de Intrusão em Redes (NIDS) têm sido amplamente desenvolvidos ao longo do tempo. No entanto, ataques sofisticados têm demandado camadas de proteção adicionais. Assim, este estudo propõe utilizar dados do Channel State Information (CSI) Wi-Fi com técnicas de aprendizado de máquina para detecção nas camadas física e de enlace, visando identificar tentativas de acesso não autorizado a uma rede Wi-Fi. O estudo analisa 70.513 instâncias coletadas em dois ambientes e identifica atividades consideradas maliciosas com 94,24% de precisão, utilizando o algoritmo RandomForest. Destaca-se como uma abordagem inovadora, explorando CSI e incorporando características das camadas 1 e 2 no contexto de NIDS.*

1. Introdução

A transformação digital é marcada por uma interconexão global e uma dependência cada vez maior de redes sem-fio. Assim, a necessidade de avanços em tecnologias de comunicação e segurança é mais premente do que nunca. Segundo [Gao et al. 2021], cerca de 75% do tráfego da Internet, à época, já era feito por conexões sem-fio, abrindo brechas para que os desafios enfrentados pelas redes Wi-Fi atuais sejam multifacetados, com incidentes de segurança tornando-se cada vez mais frequentes e sofisticados. Neste cenário, a preocupação com a integridade de informações críticas evidencia a necessidade de implantar ferramentas que possam monitorar o ambiente de rede e detectar atividades suspeitas e possíveis violações, alertando os administradores. Por isso, diversos Sistemas de Detecção de Intrusão (IDS) foram desenvolvidos e têm contribuído sobremaneira para a detecção antecipada de incidentes. Contudo, a maioria das soluções conhecidas monitoram o ambiente a partir da camada de rede, em outras palavras, tradicionalmente o monitoramento ocorre no momento em que o atacante encontra-se dentro da rede explorada.

Ao longo dos anos, as tecnologias Wi-Fi evoluíram significativamente. Isso permitiu aumentos na capacidade de largura de banda, velocidade e estabilidade na transmissão do sinal. Nessa evolução, destaca-se o emprego do CSI como um elemento importante na compreensão detalhada das propriedades dos canais de comunicação sem-fio em conexões Wi-Fi, adequando o sinal às variações ambientais para melhorar a eficiência e a confiabilidade da transmissão.

[Zhang et al. 2020] mostram que aspectos como potência, atenuação e reflexão, ficam registrados no CSI de dispositivos Wi-Fi e são utilizados para melhorar a qualidade da conexão. Porém, essas informações podem também ser exploradas mais amplamente, permitindo um mapeamento eletromagnético do ambiente e viabilizando a identificação de indivíduos e dispositivos. [Galdino et al. 2023], por exemplo, construíram um conjunto de dados CSI com 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. Essa expansão de função ressalta a crescente importância do CSI, transcendendo suas aplicações convencionais em redes Wi-Fi modernas. Assim, o CSI revela-se como uma ferramenta complementar na identificação antecipada da presença de seres humanos e dispositivos na área de cobertura de uma *Basic Service Set* (BSS) Wi-Fi, complementando os IDSs atuais e trazendo a possibilidade de monitoramento ativo de ameaças antes de os atacantes se associarem a uma rede.

Este artigo propõe uma exploração aprofundada da utilização do CSI em Sistemas de Detecção de Intrusão, com enfoque particular na coleta de dados, usando dispositivos de baixa capacidade computacional, como o ESP32. Essa abordagem é estratégica, pois busca avaliar a viabilidade e eficácia do CSI em ambientes de Internet das Coisas (IoT) com mecanismos mínimos de segurança e baixa potência computacional, o que é essencial para sua aplicação prática em uma variedade de contextos. A escolha do ESP32 para a coleta de dados de CSI foi motivada por sua ampla adoção como *gateway* em aplicações de IoT e sua forte presença no mercado, o que permite a implementação de funcionalidades como a detecção de intrusão.

Dessa forma, o artigo avança o estado da arte ao apresentar um método inovador para detectar anomalias no sinal eletromagnético causadas por dispositivos e seres humanos. No melhor de nossos esforços, este é o primeiro estudo a empregar dados CSI Wi-Fi, coletados por dispositivos de baixa capacidade computacional, especificamente para Detecção de Intrusão. Assim, o estudo traz as seguintes contribuições:

1. Dataset rotulado com ações maliciosas e neutras em dois ambientes físicos;
2. Proposta de um sistema de detecção antecipada (antes do atacante ter acesso à rede) em complemento à abordagem tradicional de NIDS; e
3. Avaliação de desempenho dos algoritmos *Support Vector Machine (SVM)*, *Random Forest*, *K-Nearest Neighbors (KNN)*, *Random Tree* e *Naive Bayes* para identificação de ações maliciosas.

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 as implicações e

significados. Por fim, a Seção 6 conclui o estudo, resumindo os principais achados e refletindo sobre suas contribuições.

2. Trabalhos Relacionados

A fortificação de redes sem-fio diante de ataques cada vez mais avançados representa um desafio constante. O estudo de [Steinmetzer et al. 2018] destaca as fraquezas das redes IEEE 802.11ad, revelando a técnica de *Beam-Stealing*, que abre caminho para ataques do tipo Man-in-the-Middle (MITM), salientando a necessidade crítica de desenvolver estratégias defensivas mais sofisticadas e resilientes. O presente trabalho reitera essa necessidade e se dedica a aperfeiçoar a detecção com uma metodologia inovadora que identifica antecipadamente potenciais ataques nas camadas física e de enlace, empregando apenas cinco etapas.

A pesquisa conduzida por [Wang et al. 2022] demonstrou a eficácia da detecção e autenticação sem a necessidade de dispositivos adicionais. Este estudo visa ampliar a gama de aplicações existentes, analisando detalhadamente o espectro eletromagnético e introduzindo a capacidade de detectar potenciais ameaças antes da camada de rede, estabelecendo assim um mecanismo de alerta para movimentos suspeitos e que possam indicar antecipadamente atividades ofensivas iminentes.

A detecção de intrusos em redes Wi-Fi é um campo crítico para a segurança cibernética. Técnicas sofisticadas são empregadas na proteção contra acessos não autorizados e ações mal-intencionadas, conforme explorado nos trabalhos de [Lv et al. 2018, Wang et al. 2019, Satam and Hariri 2021]. Estes estudos fornecem um arcabouço robusto para a segurança em redes Wi-Fi, contribuindo para a identificação e mitigação de invasões, assegurando, assim, a integridade e a privacidade dos dados. Contudo, essas técnicas são comumente aplicadas a partir da camada 3. A pesquisa atual propõe uma abordagem inédita que se concentra nas camadas 1 e 2, habilitando a criação de um mecanismo proativo de segurança para adicionar uma barreira em profundidade contra potenciais ameaças.

[Prakash and Ahmed 2017] destacam o uso do RSSI (Received Signal Strength Indicator) para identificar acessos físicos não autorizados e representa um importante passo na segurança de redes industriais. Entretanto, a preocupação de detecção de acesso à rede Wi-Fi ficou fora do escopo daquele estudo. Assim, nossa proposta expande a escala e o escopo dessa técnica ao integrar CSI, que oferecem um espectro mais abrangente de informações e permitem a análise de variações em amplitude e fase, indicando um prévio movimento ofensivo de dispositivos combinados com ação humana.

O estudo de [Liu et al. 2022], apresentou uma metodologia para a identificação de dispositivos IoT empregando técnicas avançadas de aprendizado de máquina. Este artigo aprofunda a investigação nessa área, focando na identificação do recurso mais eficaz para distinguir comportamentos ofensivos e não ofensivos. Esta análise será realizada a partir de dados CSI coletados por um único ESP32, buscando determinar quando um padrão de sinal indica uma potencial ameaça à segurança da rede.

Os estudos de [Adib and Katabi 2013, Cominelli et al. 2023, Gu et al. 2023] e o tutorial de [Yang et al. 2022], contribuem para o campo de Wi-Fi *sensing* e segurança. Eles inspiram este trabalho no uso do CSI com dispositivos de baixa capacidade. No entanto, sua aplicação na detecção de intrusão ativa ainda é inexplorada.

A Tabela 1 traz uma visão comparativa entre este estudo e os trabalhos relacionados, destacando a camada de atuação, a análise principal, o tipo de dados analisados, os equipamentos utilizados e a sua aplicabilidade em IoT.

Tabela 1. Análise comparativa entre estudos atuais.

Estudo	Camada OSI	Análise Principal	Uso exclusivo do CSI	Tipo de Dados Analisados	Equipamentos Utilizados	Aplicabilidade em IoT
[Steinmetzer et al. 2018]	1 e 2	Beam-Stealing	Não	Dados de Rede	Roteador Talon AD7200	Limitada
[Wang et al. 2022]	3	Autenticação	Não	Dados de Rede	NIC Intel 5300 com 3 antenas	Limitada
[Lv et al. 2018]	3	Proteção Acesso	Não	Dados de Rede	Roteador FAST FW150RW	Limitada
[Wang et al. 2019]	3	Proteção Acesso	Não	Dados de Rede	Módulo Wi-Fi ESP8266	Limitada
[Satam and Hariri 2021]	3	Proteção Acesso	Não	Dados de Rede	Não especificado	Limitada
[Prakash and Ahmed 2017]	1 e 2	RSSI	Não	Dados de Rede	Não especificado	Limitada
[Liu et al. 2022]	3	ML para IoT	Não	Dados de Rede	NIC Intel 5300	Ampliada
[Adib and Katabi 2013]	3	Sensing Wi-Fi	Não	Dados de Rede	Rádios USRP N210	Limitada
[Cominelli et al. 2023]	3	Sensing Wi-Fi	Não	Dados de Rede	Roteador ASUS RT-AX86U	Limitada
[Gu et al. 2023]	3	Sensing Wi-Fi	Não	Dados de Rede	Roteador TP-Link C7A4 e Roteador CISCO RV100W	Limitada
[Yang et al. 2022]	3	Sensing Wi-Fi	Não	Dados de Rede	Não especificado	Limitada
[Estudo atual]	**1 e 2**	**Dados do CSI / IDS**	**Sim**	**Dados das Subportadoras CSI**	**1 ESP32 com 1 antena**	**Ampliada**

Como evidenciado, este artigo pretende desenvolver uma camada inovadora de defesa, que atua na detecção ativa e antecipada de atividades suspeitas ou mal-intencionadas nas camadas 1 e 2 da infraestrutura monitorada de Internet das Coisas. Ao implementar essa solução proativa, este é o primeiro estudo que utiliza CSI para fins de detecção de intrusão. Assim, demonstramos a eficácia de nossa proposta ao trazer um sistema de alerta antes de o atacante se associar a uma rede Wi-Fi vítima, reforçando significativamente a segurança do ambiente antes que ameaças potenciais se concretizem.

3. Fundamentação Teórica e Metodologia

Esta seção apresenta a fundamentação para a adoção do CSI, integrado aos métodos empregados na realização dos experimentos e na análise dos dados obtidos.

3.1. Fundamentação Teórica

O CSI do Wi-Fi registra informações sobre a trajetória dos sinais sem-fio entre o transmissor e o receptor, detalhando o comportamento da onda eletromagnética nas frequências portadoras. Essa descrição engloba tanto a amplitude quanto a fase do sinal, que são afetadas pelos fenômenos de multipercurso, manifestando-se como atenuações e deslocamentos de fase. Cada elemento do CSI expressa a Resposta em Frequência do Canal (CFR), uma função complexa que sintetiza a influência do ambiente na propagação do sinal. Em sistemas Wi-Fi que empregam Múltiplas Entradas e Múltiplas Saídas (MIMO), o sinal é dividido em subportadoras pelo método de Multiplexação por Divisão de Frequência Ortogonal (OFDM). O transmissor Wi-Fi emite Símbolos de Treinamento Longo (LTFs) no preâmbulo do pacote, que são utilizados pelo receptor para estimar a matriz CSI com base nos sinais recebidos e na configuração original dos LTFs. Essa estimativa é um exercício de modelagem do canal Wi-Fi para cada subportadora.

Segundo [Ma et al. 2019], a matriz CSI estimada pelo receptor e exemplificada na Figura 1, é um conjunto tridimensional de valores complexos, resultante do

processamento do sinal recebido, que inclui a eliminação do prefixo cíclico, o desmapeamento e a demodulação OFDM. Na prática, o CSI medido é influenciado por canais de multipercurso, processamento de transmissão/recepção e inconsistências no hardware/software. A representação de *baseband* para *baseband* do CSI medido é uma abstração complexa que leva em conta todos esses fatores, além de variáveis como deslocamento cíclico e divergências de tempo e frequência de amostragem. A série temporal de matrizes CSI mapeia as variações do canal MIMO em domínios temporais, de frequência e espaciais. Para um canal MIMO-OFDM com (M) antenas transmissoras, (N) antenas receptoras e (K) subportadoras, a matriz CSI é um cubo de dados representado pela expressão $(H \in C^{(N \times M \times K \times T)})$, que registra a atenuação de amplitude e o deslocamento de fase dos sinais de multipercurso. O CSI, portanto, oferece um espectro de informações substancialmente mais rico em comparação com outras métricas como o Indicador de Força do Sinal Recebido (RSSI).

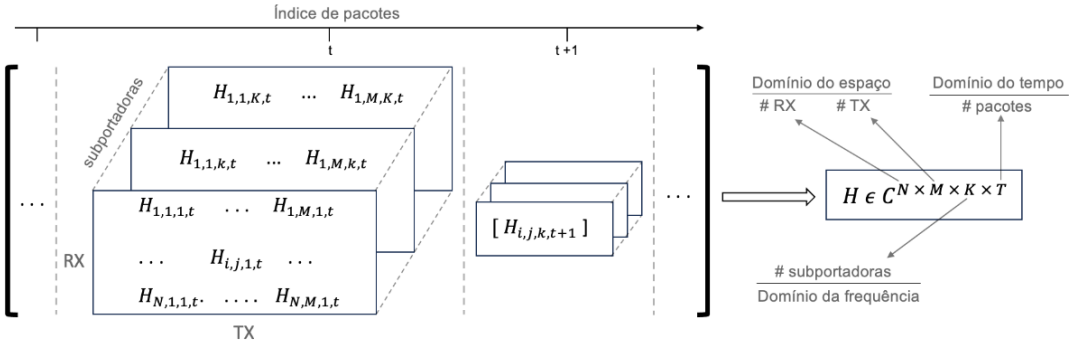


Figura 1. Matriz CSI adaptada de [Ma et al. 2019].

Os cálculos matriciais sobre os dados brutos do CSI resultam em números complexos que carregam informações da variação do sinal ao longo do tempo. Estes números são definidos como $z = a + bi$, onde a é a parte real, b é a parte imaginária, e i é a unidade imaginária, satisfazendo $i^2 = -1$. Assim, é possível chegar aos registros da Amplitude ou módulo de um número complexo, dado pela fórmula: $|z| = \sqrt{a^2 + b^2}$, onde a é a parte real e b é a parte imaginária do número complexo. Pode-se, também, obter os dados da Fase ou ângulo θ, formado pelo vetor que representa o número complexo no plano complexo com o eixo real e calculado como: $\theta = \text{atan2}(b, a)$, onde $\text{atan2}(b, a)$ é a função arco tangente de duas variáveis que retorna o ângulo cuja tangente é b/a, levando em consideração o sinal de ambos para determinar o quadrante correto. Dessa maneira, as variações em amplitude e fase do sinal trazem um melhor entendimento do comportamento analisado.

De maneira geral, as metodologias para detecção de presença humana buscam capturar uma gama abrangente de informações contextuais. [Wu et al. 2017] relataram que, identificando padrões consistentes e relacionando-os com determinadas ações ou comportamentos humanos, é possível reconhecer padrões e, a partir de uma abordagem apoiada em aprendizado, efetivamente identificar a presença de seres humanos de maneira precisa, explorando as características desses padrões do sinal. Para a identificação de dispositivos, a análise dos dados CSI engloba métodos de pré-processamento do sinal, seguida por seleção das características e aplicação de algoritmos de aprendizado de máquina para classificar padrões. Embora estudos anteriores dependam de coletas

extensivas, realizadas por múltiplos dispositivos, esta pesquisa adota uma abordagem mais focada. Propõe-se o uso de uma única antena ESP32 para captura dos dados, acompanhada de uma análise minuciosa das flutuações observadas no sinal. Esse método busca não apenas simplificar o processo de coleta, mas também aprimorar a interpretação das nuances do sinal captado.

3.2. Metodologia

No âmbito deste estudo, os dados coletados pelo dispositivo ESP32 reúnem um conjunto de informações armazenadas em arquivos no formato .CSV. A partir do método, representado na Figura 2, essas informações passam detalhadamente por etapas de pré-processamento, extração de características e de classificação.

Figura 2. Método.

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 delidos 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.

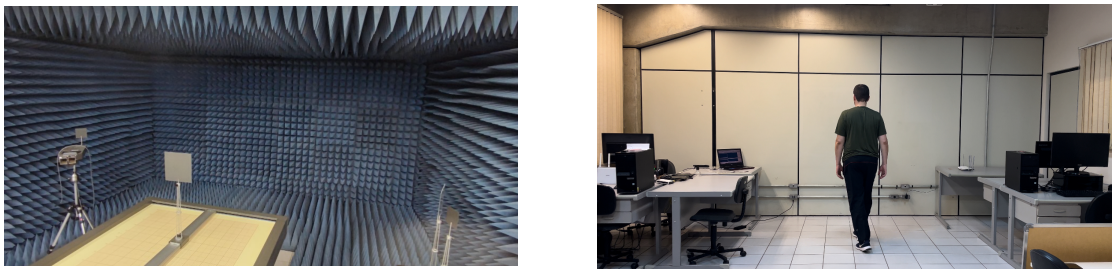
No sentido de aperfeiçoar a detecção e classificação de seres humanos e dispositivos com capacidade Wi-Fi em ambientes internos, uma gama diversificada de algoritmos e técnicas de análise de sinais tem sido meticulosamente explorada. Cada um destes algoritmos apresenta uma abordagem única e especializada, 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 2 reúne as principais técnicas e algoritmos abordados neste estudo.

Tabela 2. 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. Experimentos

Os testes foram realizados em dois ambientes controlados: uma câmara semi-anecóica, ilustrada na Figura 3(a), e o Laboratório de Comando e Controle & Defesa Cibernética (Lab-C2DC) do ITA, mostrado na Figura 3(b). O primeiro foi escolhido por apresentar um ambiente controlado, com baixa taxa de perturbação do mundo externo, a fim de absorver as reflexões provocadas por ondas eletromagnéticas e reduzir significativamente as reflexões internas. Já o Lab foi escolhido por ser um ambiente mobiliado e com uma variedade de equipamentos eletrônicos, repleto de objetos com características reflexivas e composto por diversos tipos de ruídos, contrastando com o cenário anterior e aproximando a pesquisa da realidade, onde as características de multicaminhos do sinal Wi-Fi sofrem influências diversas e dificultam o refino dos dados.



(a) Câmara semi-anecóica. **(b) Lab-C2DC**

Figura 3. Experimentos.

Nesses ambientes, foi utilizado uma Placa ESP32 Wi-Fi como receptor (Rx), desenvolvida pela empresa Heltec Automation e voltada ao mundo da Internet das Coisas - *Internet of Things (IoT)*. Este dispositivo foi escolhido por ser pequeno (25x52x10mm), com reduzida capacidade computacional em comparação com sensores 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)*.

A placa foi acoplada a um notebook *DELL Inspiron 15 Gaming 7567*, com sistema operacional Windows 10 Home, processador Intel Core i7-7700HQ 2.80GHz e 16GB de memória RAM. E para simular o sinal Wi-Fi de uma rede fictícia, empregou-se um roteador TP-Link Archer C60 configurado como transmissor (Tx), operando uma rede em 2.4Ghz a 20MHz, no canal 11. Durante todo o experimento Tx e Rx se comunicavam por meio de mensagens *echo request* e *echo reply*. O protocolo de captura exibido na Tabela 3 seguiu o mesmo padrão nos dois ambientes, considerando os objetos de interesse posicionados a 1,5m de distância entre os 2 dispositivos, conforme representação exibida na Figura 4, onde as silhuetas refletem o movimento realizado pelo indivíduo.

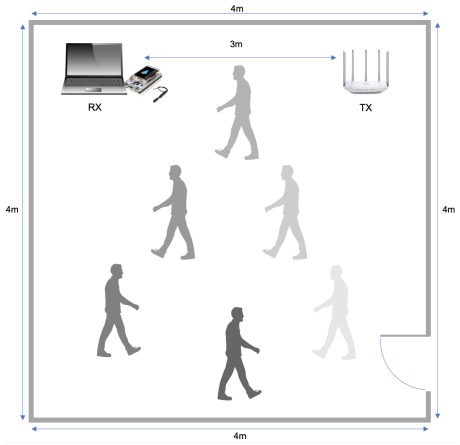


Figura 4. Protocolo de captura

O monitoramento teve como objetivo a detecção de dois usuários com características físicas diferentes e quatro dispositivos com hardware e softwares distintos. Para fins de precisão e reprodutibilidade futura, destaca-se que o usuário 1 possuía 1,73m de altura e pesava 92 quilos e o usuário 2 possuía 1,85m de altura e pesava 98 kg. Os dispositivos utilizados foram 02 celulares - um com sistema IOS e outro com sistema Android, 01 tablet - com sistema IOS, e 01 Macbook Pro - com sistemas IOS. Utilizou-se, ainda, a ferramenta ESP-CSI[1] no processo de registro dos usuários e captura das informações.

Para facilitar o deslocamento do usuário, um intervalo de 10 segundos foi estabelecido antes de iniciar a coleta de dados. A ferramenta foi então calibrada, e cada sessão de captura durou 20 segundos, garantindo a consistência e precisão dos dados. Ressalta-se, também, que foi utilizado o modo *Line-of-Sight (LOS)* para análise das capturas, evitando a presença de obstáculos entre o ponto de transmissão e o ponto

[1] *https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-guides/wifi.html?highlight=csi#wi-fi-channel-state-information.*

Tabela 3. Procolo de Captura

Usuário 1 e Usuário 2 - individualmente no cenário	
Captura	**Configuração**
Captura 1 - User 1 Captura 1 - User 2	Someone (presença parado)
Captura 2 - User 1 Captura 2 - User 2	Someone (presença - celular com Wi-Fi desligado)
Captura 3 - User 1 Captura 3 - User 2	Move (3x entrada e saída sem celular)
Captura 4 - User 1 Captura 4 - User 2	Move (3x entrada e saída - celular com Wi-Fi desligado)
Captura 5 - User 1 Captura 5 - User 2	Move (1x entrada - celular com Wi-Fi desligado, liga Wi-Fi e 2x tentativas de conectar com senha errada)
Usuário 1 e Usuário 2 - juntos no cenário	
Captura	**Configuração**
Captura 6 - User 1 e 2	Someone (usuário 1 e usuário 2 - presença parado)
Captura 7 - User 1 e 2	Move (usuário 1 e usuário 2 - 2x entradas e saídas)
Sem usuários e dispositivos	
Captura	**Configuração**
Captura 8 - Sem User e sem dispositivo	None (ambiente sem nada)
Dispositivos	
Captura	**Configuração**
Captura 9 - Celular Android	Static (com Wi-Fi ligado e tela ligada)
Captura 10 - Celular IOS	Static (com Wi-Fi ligado e tela ligada)
Captura 11 - Tablet IOS [iPad]	Static (com Wi-Fi ligado e tela ligada)
Captura 12 - MacBook Pro	Static (com Wi-Fi ligado e tela ligada)

de recepção. Com isso, os cenários sofriam menor atenuação e dispersão do sinal, proporcionando uma comunicação mais limpa e robusta.

A ferramenta ESP-CSI, empregada nas capturas utilizando o ESP32, gerou 32 arquivos no formato .CSV. Destes, 15 foram capturados na câmara semi-anecóica, enquanto os 17 restantes foram obtidos no Lab-C2DC.

5. Análise e Discussão dos Resultados

A análise e discussão dos resultados descreve e resume os principais registros obtidos, oferecendo uma percepção mais ampla da base utilizada e uma melhor contextualização da pesquisa. Além disso, aborda as suas limitações e contribuições.

As capturas do CSI WiFi realizadas nos experimentos trouxeram informações de 52 subportadoras, sendo cada arquivo composto por cerca de 2200 instâncias. As características reveladas pelas interferências no sinal são descritas pelos seguintes atributos: *type*, *seq*, *timestamp*, *target_seq*, *target*, *mac*, *rssi*, *rate*, *sig_mode*, *mcs*, *cwb*, *smoothing*, *not_sounding*, *aggregation*, *stbc*, *fec_coding*, *sgi*, *noise_floor*, *ampdu_cnt*, *channel_primary*, *channel_secondary*, *local_timestamp*, *ant*, *sig_len*, *rx_state*, *len*, *first_word_invalid* e *data*. Grande parte dos atributos apresentaram valor repetido ou nulo e foram descartados ao longo da análise. No entanto, o atributo *data* contém números complexos, resultantes de cálculos matriciais aplicados aos dados brutos obtidos do CSI.

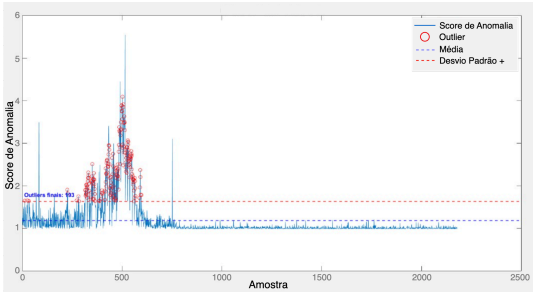
As transformações aplicadas aos dados brutos permitiram acesso direto às informações de amplitude e fase de cada uma das 52 subportadoras, porém, através de nossas análises e observações experimentais notou-se que os registros relativos à fase do sinal apresentavam muita aleatoriedade, não agregando valor à pesquisa, enquanto que os dados de amplitude do CSI eram informativos e mais robustos. Ao todo, foram encontrados 104 valores com informações efetivamente recebidas. Destes, metade

representava a parte real e, a outra metade, os números complexos correspondentes, com índices ímpares, indicando a parte imaginária e os índices pares, a parte real. Foi observado, também, que a primeira subportadora de todos os arquivos estava corrompida. Portanto, as análises se concentraram nas informações das 51 subportadoras subsequentes. Esses dados são cruciais pois trazem detalhes sobre as mudanças na amplitude e na resposta de frequência do sinal, facilitando a identificação das variações.

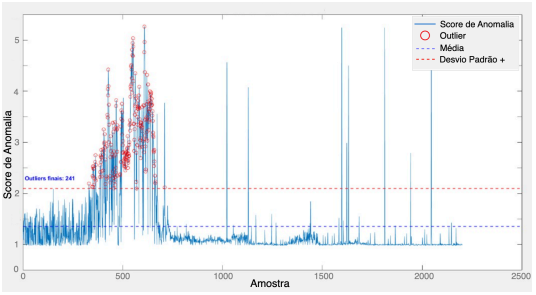
Em seguida, procedeu-se à investigação dos padrões de sinal nos diversos cenários experimentais para compreender as flutuações no CSI. Foi aplicado um pré-processamento nos dados empregando as técnicas de Filtro de Hampel, Filtro Passa-baixa, Calibração de Fase, Transformada Discreta de Hilbert, Análise de Componentes Principais (PCA) e a Transformada Wavelet Discreta (TWD). Dentre estas, a TWD com coeficiente db5 e nível de decomposição 3 foi a que trouxe um melhor resultado, fornecendo uma visão granular do comportamento do sinal ao longo do tempo, enquanto as outras não trouxeram a visão esperada para este experimento.

Após o pré-processamento, utilizou-se a ferramenta MATLAB para comparar os dados da captura 5 com os da captura 8. Empregou-se o algoritmo Local Outlier Factor (LOF) ajustado para considerar a média, o desvio padrão dos Outliers e uma taxa de amostragem de 110 pacotes por segundo (k=110). A análise permitiu identificar que as tentativas de conexão presentes nas capturas realizadas possuem um padrão similar e específico de interferência no sinal.

Os *outliers* assinalados indicam variações relevantes no sinal Wi-Fi ao longo do tempo. Os achados da análise estão visualmente apresentados na Figura 5(a) e ilustram a tentativa de conexão do usuário 1, usando um iPhone, e, na Figura 5(b), a tentativa de conexão do usuário 2, utilizando um dispositivo Android. Ambas as figuras revelam padrões de flutuação no sinal Wi-Fi, sugerindo que as tentativas de conexão dos dispositivos afetam de maneira semelhante a estabilidade do sinal.



(a) Tentativas do iPhone.

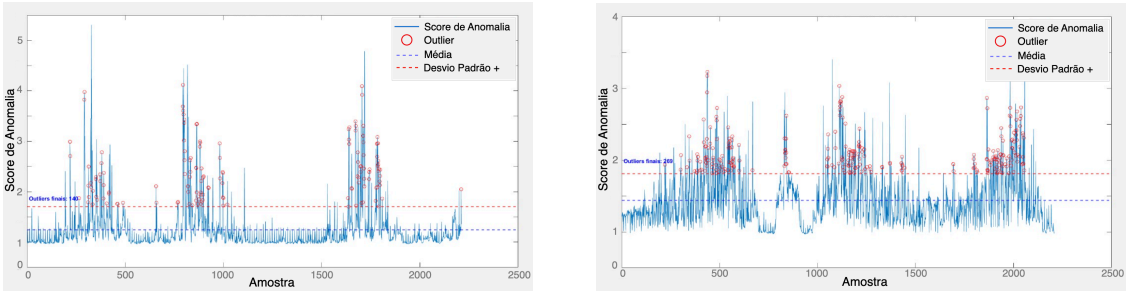


(b) Tentativas do Android.

Figura 5. *Outliers* das tentativas de conexão.

Prosseguindo com a análise, o algoritmo LOF foi novamente empregado, desta vez para contrastar a captura 4, que registrava usuários em movimento, com a captura 8, que representava um ambiente sem presença de pessoas. Os resultados dessa comparação, ilustrados na Figura 6(a) para o usuário 1 em movimento, e na Figura 6(b) para o usuário 2 igualmente em movimento, revelaram que a dinâmica do ambiente, marcada pela movimentação das pessoas, também induz variações significativas no sinal Wi-Fi.

A similaridade entre os padrões de interferência no sinal foi validada através do



(a) Usuário 1 em movimento. **(b) Usuário 2 em movimento.**

Figura 6. *Outliers* da presença de usuários em movimento.

cálculo do coeficiente de correlação de Pearson. Ao comparar as tentativas de conexão, foi observado um coeficiente de correlação de 0.5306, o que reflete uma correlação positiva de intensidade moderada. Por outro lado, a comparação entre os movimentos dos usuários resultou em um coeficiente de 0.8376, denotando uma forte correlação linear positiva. Esses resultados sugerem que, tanto as ações de tentativa de conexão pelos dispositivos, quanto os movimentos dos usuários influenciam de forma substancial e correspondente o sinal Wi-Fi, mesmo na ausência de uma conexão de rede efetiva.

A partir das inferências obtidas, a pesquisa avançou para o desenvolvimento de um modelo destinado a identificar e classificar comportamentos anômalos como ofensivos, especialmente aqueles que apresentam características similares às observadas nas capturas de tentativas de conexão. Dessa vez, todos os arquivos foram rotuladas de acordo com os experimentos realizados, no intuito de avaliar o modelo englobando os dois ambientes experimentados. As capturas onde houve tentativa de conexão foram marcadas como ofensivas e as demais como neutras.

O conjunto analisado é composto por 32 capturas, somando um total de 70.513 instâncias que registram os resultados das reflexões, atenuações e difrações sofridas pelo sinal eletromagnético ao longo do seu percurso no ambiente analisado. Dentre essas, 61.713 instâncias são (28 capturas) rotuladas como Neutras e 8.800 (4 capturas) como Ofensivas. É importante notar que a captura é influenciada diretamente pelo ambiente monitorado, variando a correlação dos atributos de acordo com o local. Assim, as subportadoras que sofreram mais interferência na câmara semi-anecóica são diferentes das que mais variaram no Lab-C2DC. Aplicando-se o método *WrapperSubsetEval*, com o algoritmo de Árvore de Decisão J48 e o método *GreedyStepwise*, observou-se que as subportadoras 7, 8, 9, 12, 14, 20, 38, 43 e 52 foram as mais afetadas na câmara semi-anecóica, enquanto que no Lab-C2DC, as que sofreram maior interferência foram as de número 2, 8, 22, 29, 48.

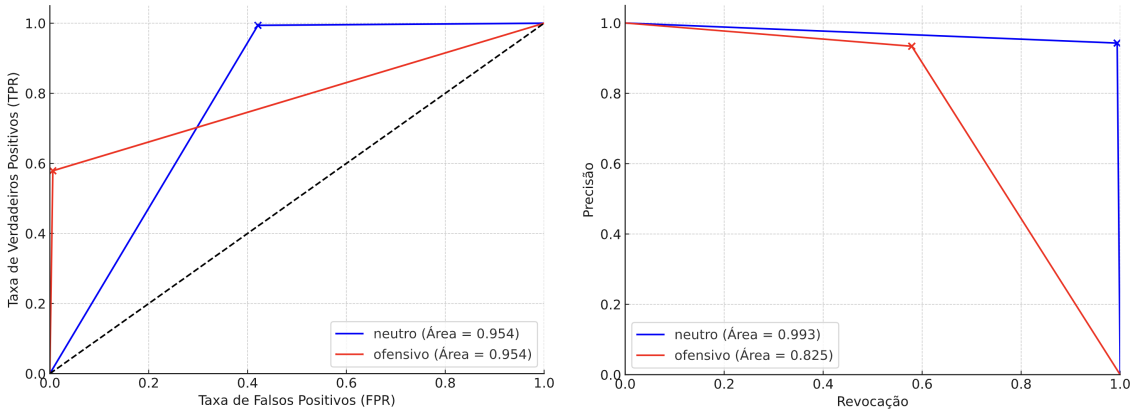
O conjunto de dados rotulado em capturas neutras e ofensivas apresenta uma disparidade, podendo indicar uma tendência do modelo de aprendizado de máquina em favor da classe predominante. No entanto, foi implementada uma estratégia de ponderação de classe, atribuindo-se um peso de valor 7 para as capturas da classe minoritária durante a fase de treinamento do modelo. O valor é resultante da proporção entre instâncias analisadas. Assim, o modelo pode ser treinado com validação cruzada em dez folds. O método divide os dados em dez partes, treina o modelo em nove delas e testa

na que restou, repetindo o processo dez vezes. Isso ajuda a evitar o sobreajuste e fornece uma estimativa mais realista do desempenho do modelo em amostras não vistas.

A precisão global foi medida empregando-se os algoritmos *SVM*, *Random Forest*, *KNN*, *Random Tree* e *Naive Bayes*. Dentre estes, o *SVM* foi o que apresentou o melhor desempenho para distinguir comportamentos neutros e ofensivos, conforme a Tabela 4. Contudo, apesar do *SVM* ter apresentado o melhor desempenho de Precisão e F1-Score, o tempo de construção do modelo foi 1.158,42% mais lento que o RF, e por isso foi descartado. Já o *KNN*, embora tenha o menor tempo de construção, utiliza um modelo de aprendizado transdutivo, implicando em manter uma cópia completa dos dados em memória, inviabilizando a implantação num dispositivo como ESP32.

Tabela 4. Resultados obtidos pelos classificadores.

Classificador	Precisão (%)	F1-Score	Tempo de Construção (s)
SVM	94.43	0.969	360.79
RandomForest	94.24	0.968	28.67
KNN	92.76	0.959	0.04
RandomTree	90.93	0.948	0.60
NaiveBayes	86.64	0.928	0.13



(a) Curva ROC. **(b) Curva PRC.**

Figura 7. Análise do desempenho.

O Random Forest foi escolhido por apresentar a maior precisão considerando um tempo de construção inferior a um minuto. O resultado é refletido pela Taxa de Verdadeiro Positivo (*TPR*) de 0,994 para comportamentos neutros e de 0,579 para comportamentos ofensivos, indicando a capacidade do modelo em distinguir com precisão os comportamentos monitorados. Acredita-se que o *Random Forest* obteve o melhor resultado por sua característica de combinação aleatória das árvores de decisão, que ajuda o modelo a reduzir a tendência de superajustar-se (*overfitting*) aos dados de treinamento.

6. Conclusões

Este artigo traz à tona a utilização do Wi-Fi como uma inovação nos Sistemas de Detecção de Intrusão. Foram realizados experimentos em dois ambientes diferentes,

comprovando a eficácia do CSI na identificação de intrusões. O conjunto produzido, contendo 70.513 pacotes rotulados, possibilitou demonstrar a habilidade de distinguir usuários e dispositivos sob variadas condições com uma precisão de 94,24%, utilizando o algoritmo RandomForest. Portanto, o estudo introduz uma camada de segurança complementar para redes Wi-Fi, capaz de detectar proativamente ações maliciosas por meio de características (features) das camadas física e de enlace.

Como trabalhos futuros, visualiza-se encorpar a base de dados e integrar mais dispositivos ESP32 para capturar uma quantidade maior de variâncias do sinal. Assim, a granularidade de informações será expandida, favorecendo um alerta antecipado e uma detecção de intrusos ainda mais eficaz. Os dados e o código-fonte utilizados neste artigo estão disponíveis em `https://github.com/c2dc/sbrc2024-csi`.

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 and #2022/00741-0, e da CAPES. Agradecemos ao LabGE/ITA por disponibilizar a câmara semi-anecoica para execução dos experimentos.

Referências

Adib, F. and Katabi, D. (2013). See through walls with wifi! *SIGCOMM Comput. Commun. Rev.*, 43(4):7586.

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.

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.

Gao, D., Lin, H., Li, Z., Qian, F., Chen, Q. A., Qian, Z., Liu, W., Gong, L., and Liu, Y. (2021). A nationwide census on wifi security threats: Prevalence, riskiness, and the economics. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, MobiCom '21, page 242255, New York, NY, USA. Association for Computing Machinery.

Gu, Y., Chen, J., He, K., Wu, C., Zhao, Z., and Du, R. (2023). Wifileaks: Exposing stationary human presence through a wall with commodity mobile devices. *IEEE Transactions on Mobile Computing*, pages 1–15.

Liu, Y., Wang, J., Li, J., Niu, S., and Song, H. (2022). Machine learning for the detection and identification of internet of things devices: A survey. *IEEE Internet of Things Journal*, 9(1):298–320.

Lv, J., Man, D., Yang, W., Du, X., and Yu, M. (2018). Robust wlan-based indoor intrusion detection using phy layer information. *IEEE Access*, 6:30117–30127.

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

Prakash, J. and Ahmed, C. M. (2017). Can you see me on performance of wireless fingerprinting in a cyber physical system. In *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, pages 163–170.

Satam, P. and Hariri, S. (2021). Wids: An anomaly based intrusion detection system for wi-fi (ieee 802.11) protocol. *IEEE Transactions on Network and Service Management*, 18(1):1077–1091.

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.

Steinmetzer, D., Yuan, Y., and Hollick, M. (2018). Beam-stealing: Intercepting the sector sweep to launch man-in-the-middle attacks on wireless ieee 802.11ad networks. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '18, page 1222, New York, NY, USA. Association for Computing Machinery.

Wang, D., Yang, J., Cui, W., Xie, L., and Sun, S. (2022). Caution: A robust wifi-based human authentication system via few-shot open-set recognition. *IEEE Internet of Things Journal*, 9(18):17323–17333.

Wang, S., Li, B., Yang, M., and Yan, Z. (2019). Intrusion detection for wifi network: A deep learning approach. In *International Wireless Internet Conference*, pages 95–104. Springer.

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.

Yang, Z., Zhang, Y., Chi, G., and Zhang, G. (2022). Hands-on wireless sensing with wi-fi: A tutorial.

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*, pages 730–742. Springer.