

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

Eduardo Fabrício Gomes Trindade*
Felipe Silveira de Almeida*, e
Lourenço Alves Pereira Junior*

Instituto Tecnológico de Aeronáutica (ITA)

17 de setembro de 2024

{trindade,felipefsa,ljr}@ita.br



Sumário

Motivação

Objetivos

Trabalhos Relacionados

Proposta

Resultados

Conclusões

Motivação

Fatores de Autenticação

- **Fator de conhecimento:** o que você sabe.
- **Fator de posse ou propriedade:** o que você tem.
- **Fator de inerência ou existência:** o que você é.

Motivação

Fraudes e Deep Fake



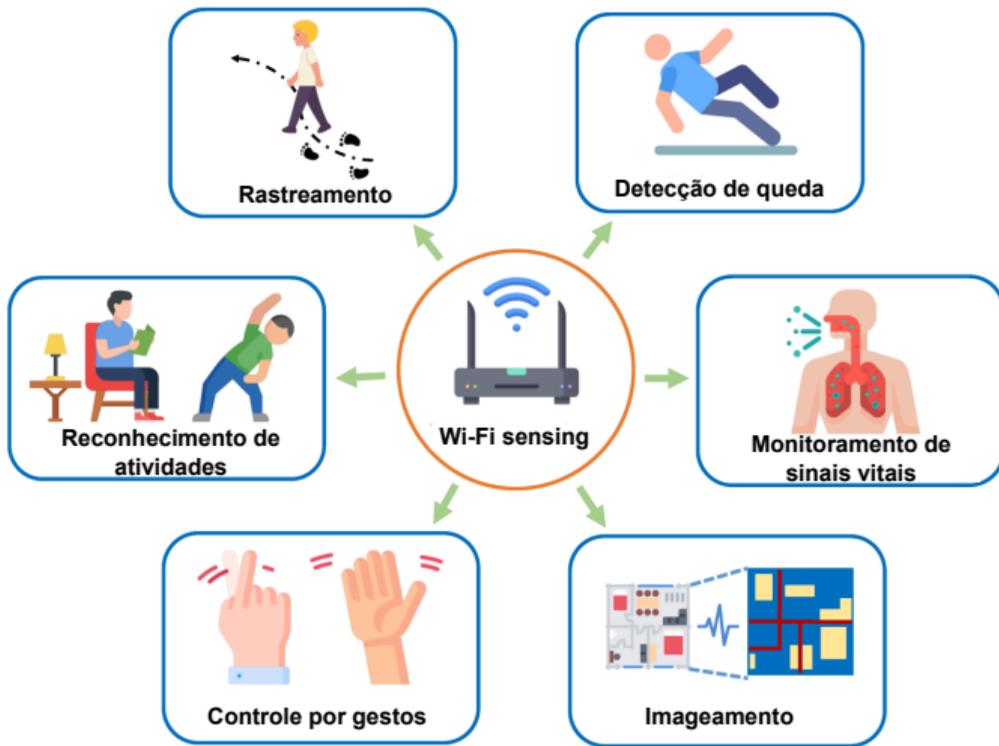
Motivação

Máscaras realistas e Golpes



Motivação

Wi-Fi Sensing



Motivação

- **Aumento das Ameaças de Segurança:** Ameaças cibernéticas cada vez mais sofisticadas têm colocado em xeque os métodos tradicionais de autenticação, como senhas, biometria e reconhecimento facial.
- **Potencial da autenticação baseada em CSI:** Abordagem baseada em padrões biofísicos dos indivíduos oferece uma forma passiva de autenticação, aumentando a conveniência, a segurança e a confiabilidade.
- **Expansão da IoT e Redes Wi-Fi:** Aumento do número de dispositivos conectados e da dependência a redes sem fio.

Objetivos

- Explorar a utilização do CSI em complemento a Sistemas de Controle de Acesso.
- Avaliar a viabilidade e eficácia de utilizar dados biofísicos de indivíduos, coletados do Wi-Fi CSI, em sistemas de autenticação.
- Propor um sistema de controle de acesso baseado em características biofísicas, extraídas do Wi-Fi CSI com Raspberry Pi.

Contribuição

- Controle de acesso pelo Wi-Fi, utilizando dispositivos portáteis, eliminando a necessidade de interação com o usuário e apresentando-se como uma proposta complementar de segurança.

Trabalhos Relacionados

Comparativo entre trabalhos relacionados.

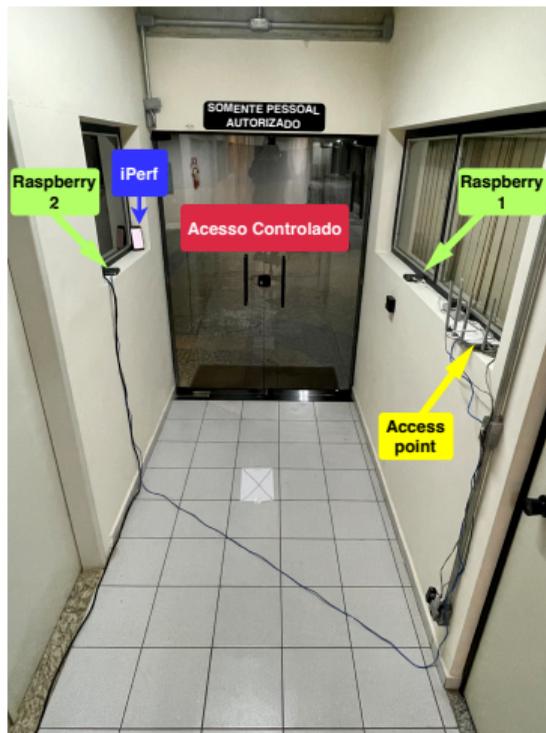
Estudo	Abordagem	Dispositivo de Coleta	Frequência utilizada / Largura de banda	Ferramenta de extração CSI	Aplicação em controle de acesso
Shah and Kanhere 2017	Padrões	Notebook	2.4GHz (20MHz)	Não especificado	Não
Wang et al. 2016	Padrões	Notebook	5GHz (80MHz)	Linux 802.11n CSI Tool	Não
Guo et al. 2017	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 (40MHz)	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

Proposta

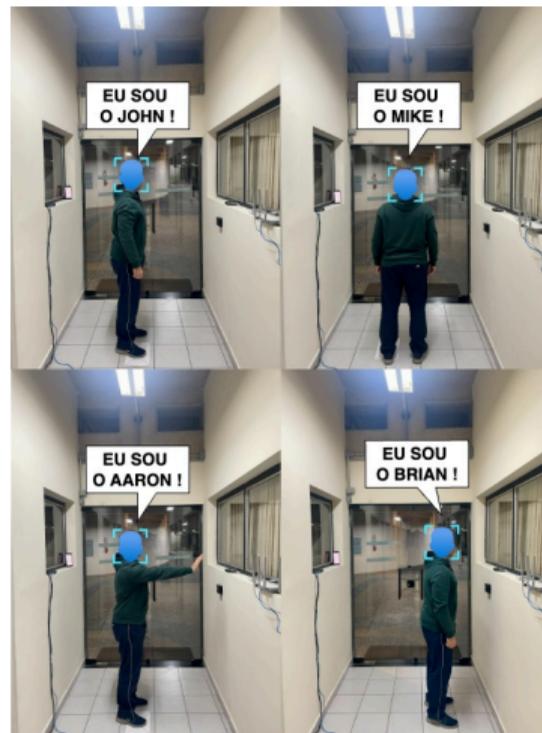


- Utilização de 2 Raspberry Pi para capturar características biofísicas, silhuetas, movimentos e variações comportamentais dos usuários.
- Extração de dados de amplitude e a fase do sinal registrados no CSI.
- Processamento dos dados e criação de um modelo para classificar usuários autorizados e não autorizados.

Cenários



Corredor



Capturas

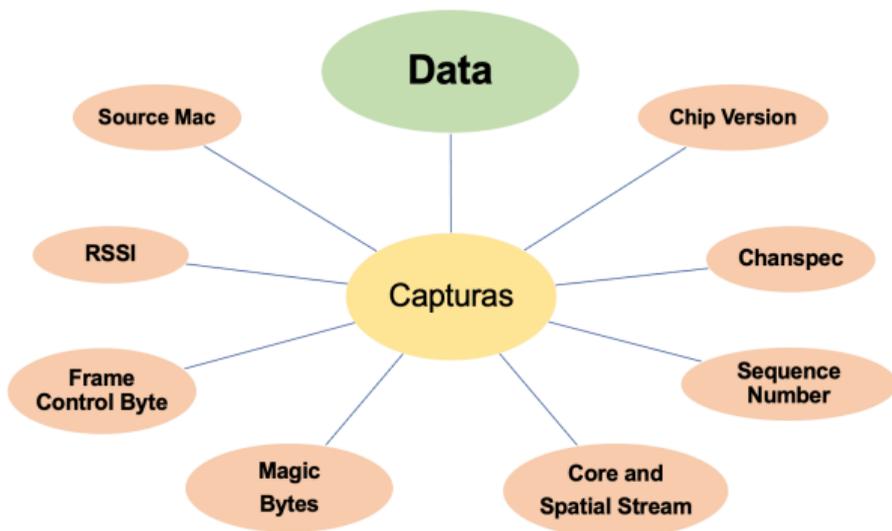
Equipamentos

- Notebook DELL Inspiron 15 Gaming 7567, com sistema operacional Windows 10 Home, processador Intel Core i7-7700HQ 2.80GHz e 16GB de memória RAM.
- TP-Link Archer C60 configurado como transmissor (Tx), operando uma rede em 5 GHz no canal 36 (80 Mhz).
- 2 Raspberry Pi 4B, com processador 64-Bit quad-core Cortex-A72, 8 GB LPDDR4 de RAM, configurados como receptores (Rx).
- 01 celular com sistema Android rodando aplicação iPerf2 com a taxa de aproximadamente 1000 pacotes UDP por segundo.
- Ferramenta Nexmon CSI Extractor para coleta dos dados.

Experimentos

- 6 usuários com características distintas
- 5 atividades diferentes
 - silhueta frente e verso
 - silhueta lateral
 - comportamento específico
 - posicionamento próximo e afastado
 - pronúncia de palavra
- Conjunto de dados composto por 600 capturas de 10 segundos, somando aproximadamente 6.000.000 instâncias.

Resultados



Maior Impacto

Atributo Data

- 256 subportadoras.
- Números complexos.
- Dados de Amplitude.

Resultados

Subportadoras

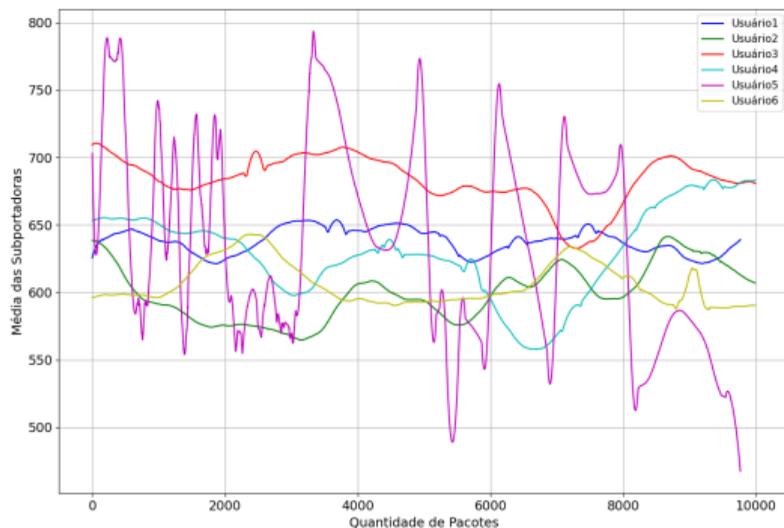
- **Nulas:** -128, -127, -126, -125, -124, -123, -1, 0, 1, 123, 124, 125, 126, 127.
- **Piloto:** -103, -75, -39, -11, 11, 39, 75, 103.

Aplicação de filtros

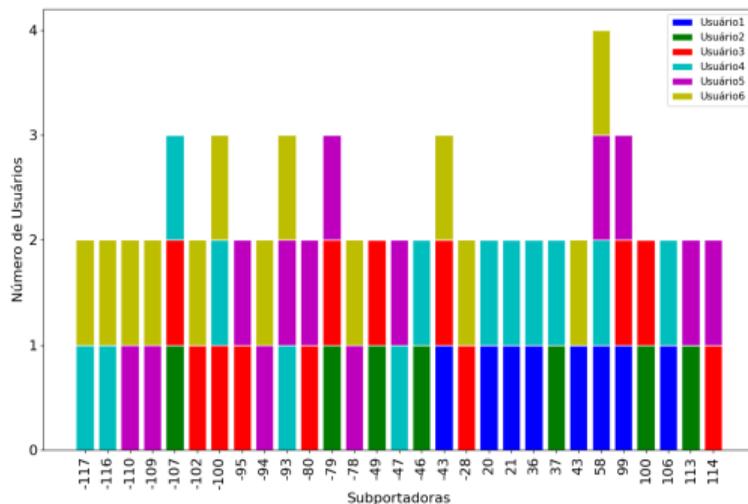
- Filtro de Hampel
- Filtro de Savitzky-Golay

Resultados

Subportadoras



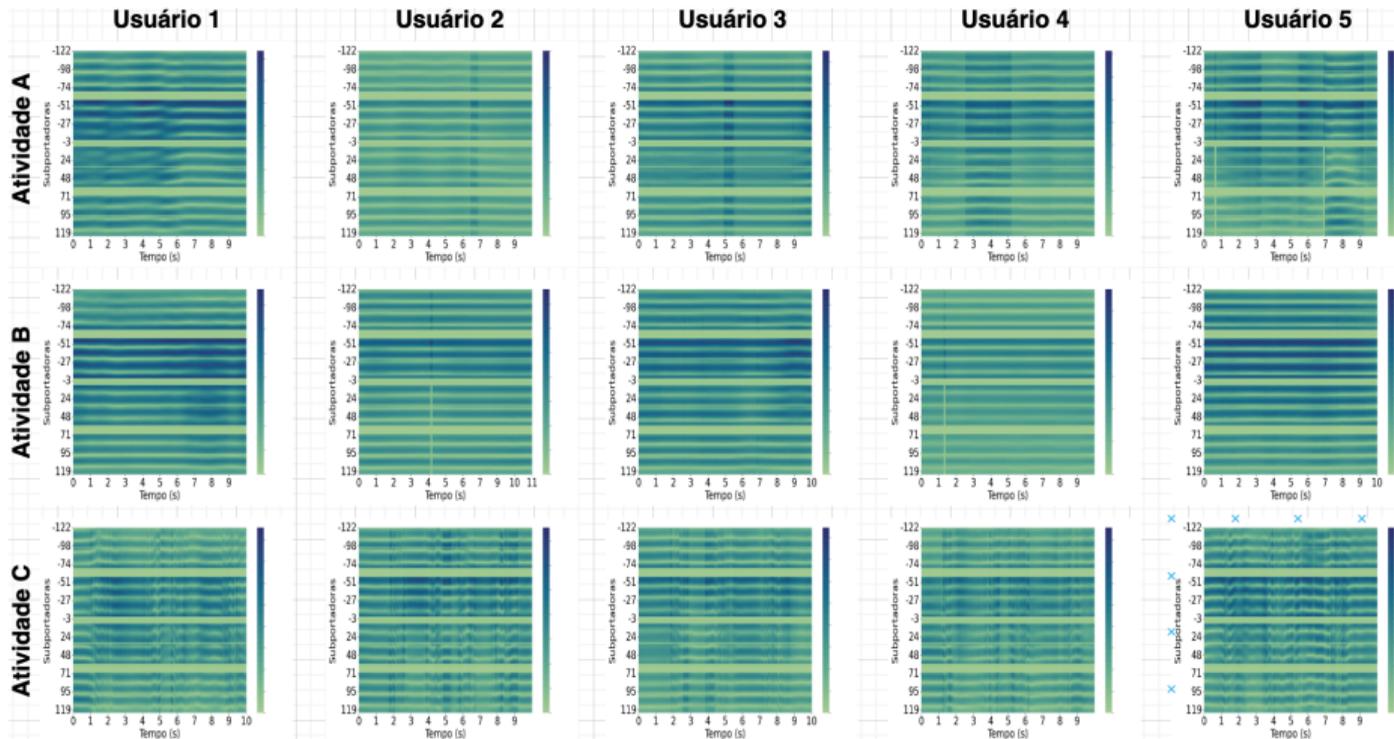
Amplitude média.



Suportadoras em comum.

Resultados

Interferência das atividades no sinal



Resultados

Desempenho do modelo

- Atividade A - Amostra de 10 segundos por usuário.

Treinamento do modelo

- Validação cruzada (10 *folds*).

Algoritmos avaliados

- K-Nearest Neighbors
- Random Forest
- Support Vector Machine
- Decision Tree J48
- Naive Bayes

Resultados

Classificadores

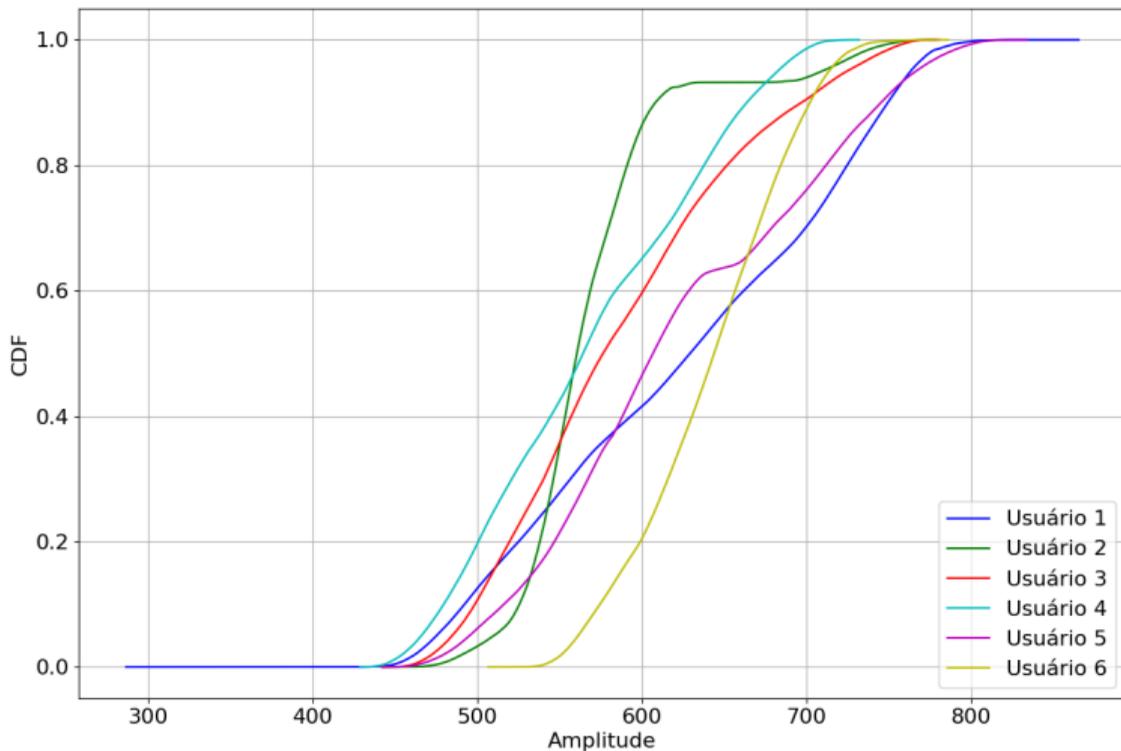
Métricas	Com Filtro					Sem Filtro				
	KNN	RF	SVM	J48	NB	KNN	RF	SVM	J48	NB
Acurácia Média (%)	99.99	99.99	100.00	99.93	94.11	99.92	99.88	99.72	99.60	87.36
F1-Score	100.00	100.00	100.00	100.00	99.50	100.00	100.00	99.72	99.80	97.00
Tempo de Construção (s)	0.02	13.92	153.81	31.27	2.85	0.01	15.85	289.98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

KNN

- TPR média de 0,999
- Maior acurácia e menor tempo de construção
- Característica transdutiva

Resultados

Cumulative Distribution Function (CDF)



Conclusões

- Utilização do Wi-Fi para autenticação em sistemas de controle de acesso físico.
- Alternativa aos métodos tradicionais de autenticação.
- Emprego de dispositivos portáteis para coleta de dados.
- Validação - utilização de características biofísicas e comportamentais para autenticação de usuários.
- Conjunto de dados e códigos disponível em:
<https://github.com/c2dc/sbseg2024-csi>

Trabalhos Futuros

- Expansão do Dataset.
- Avaliação do modelo em outros cenários.
- Experimentos com modelo de aprendizado não supervisionado.
- Experimentos para verificar a possibilidade de autenticação online.

Obrigado!

Lab-C2DC / ITA

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

Eduardo Fabrício Gomes Trindade*
Felipe Silveira de Almeida*, e
Lourenço Alves Pereira Junior*

Instituto Tecnológico de Aeronáutica (ITA)

17 de setembro de 2024

{trindade,felipefsa,ljr}@ita.br

