# Iowa State University

## Electrical and Computer Engineering Department

*Forefront of healthcare innovation*

# Improving Authentication for Wireless Healthcare Sensors

Final Oral Summer 2025

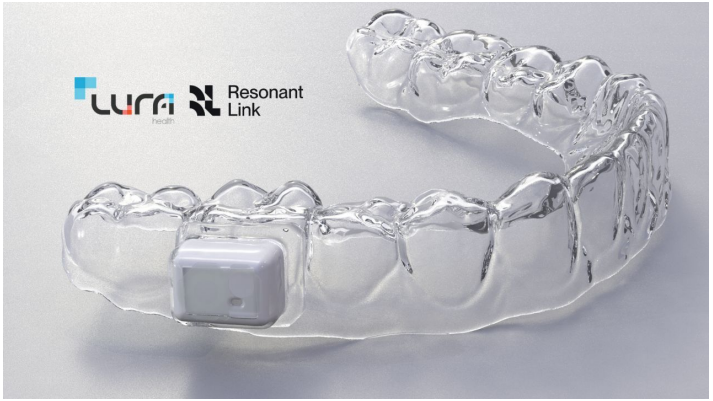
*SeyedMohammad Kashani*

*Ashfaq Khokhar*
*Sang Wu Kim*
*Farid Nait-Abdesselam*
*Thomas Daniels*
*Hongwei Zhang*
*Ashraf Gaffar*

IOWA STATE UNIVERSITY

# What is Wireless Body Area Network (WBAN)

- Insulin delivery pumps
- Glucose monitoring system
- Blood pressure sensor
- ECG sensor



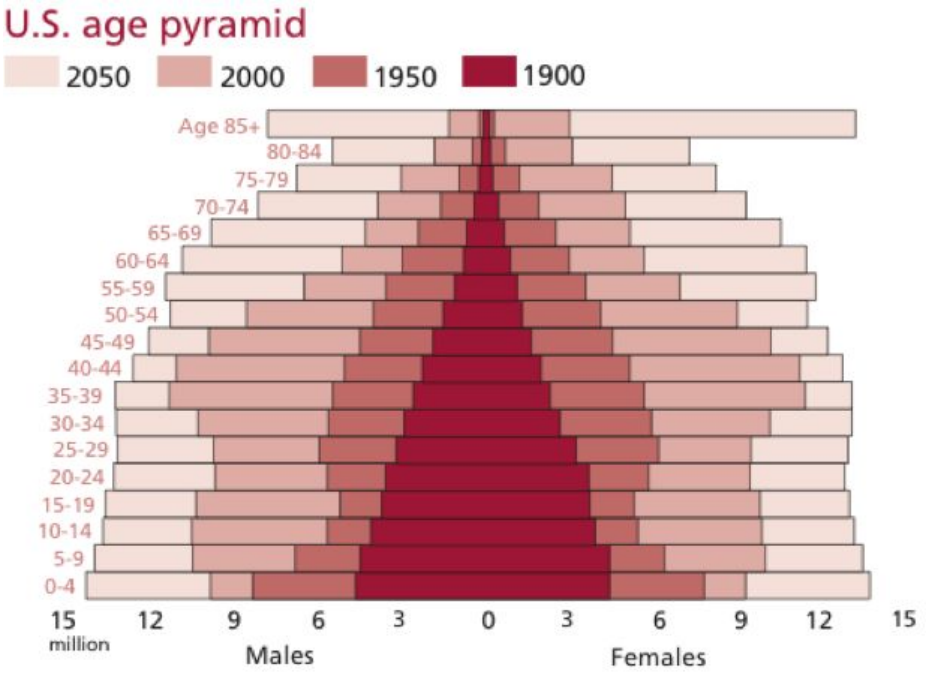

Picture from: www.resonant-link.com

Smart tiny wireless sensor -> IoHT

# Why do we need WBAN?

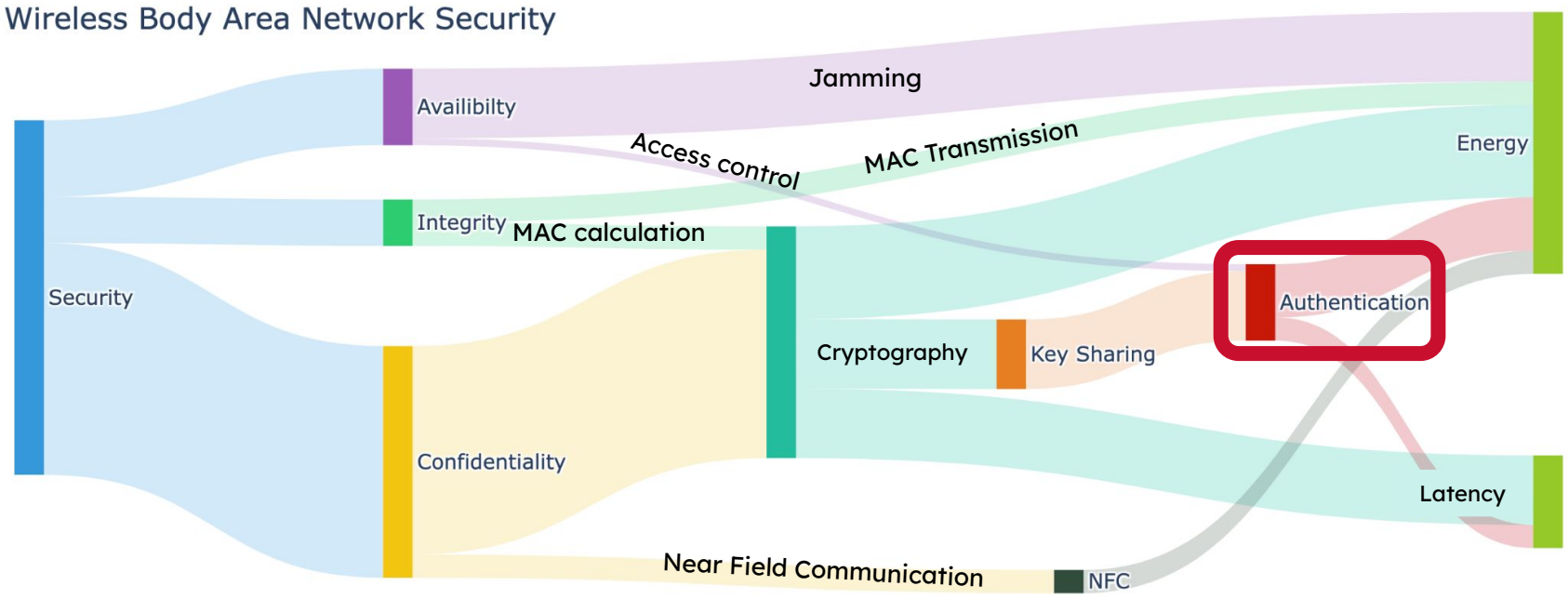
Some analysts have suggested that the adoption of **electronic medical records** (EMR) by hospitals could eventually **reduce annual U.S. healthcare expenditures by one third or more**.

Source: https://www.nber.org/digest/jan13/does-health-information-technology-reduce-costs

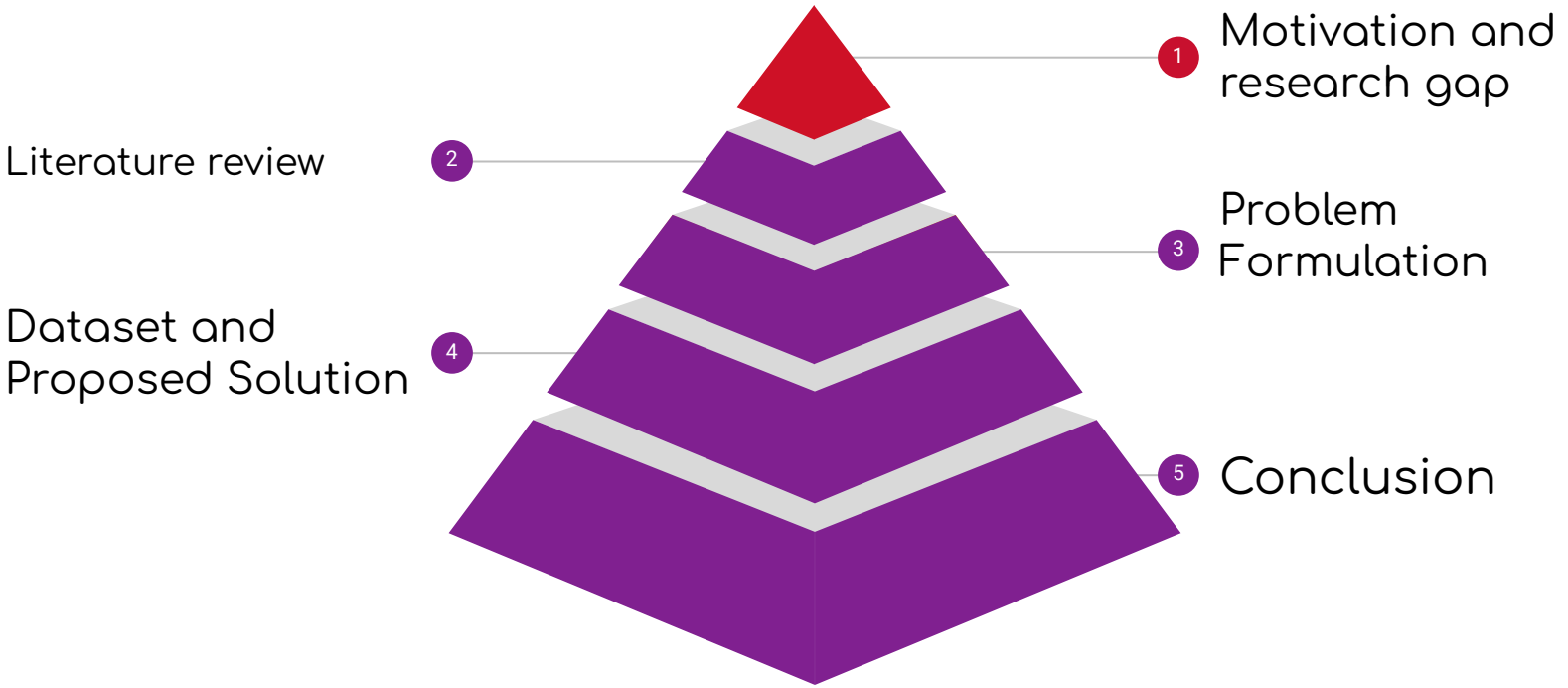



Source: http://www.ctmt.com/pdfs%5CemergingDirections%5Cdemographicsasdestiny.pdf

# Security in WBAN

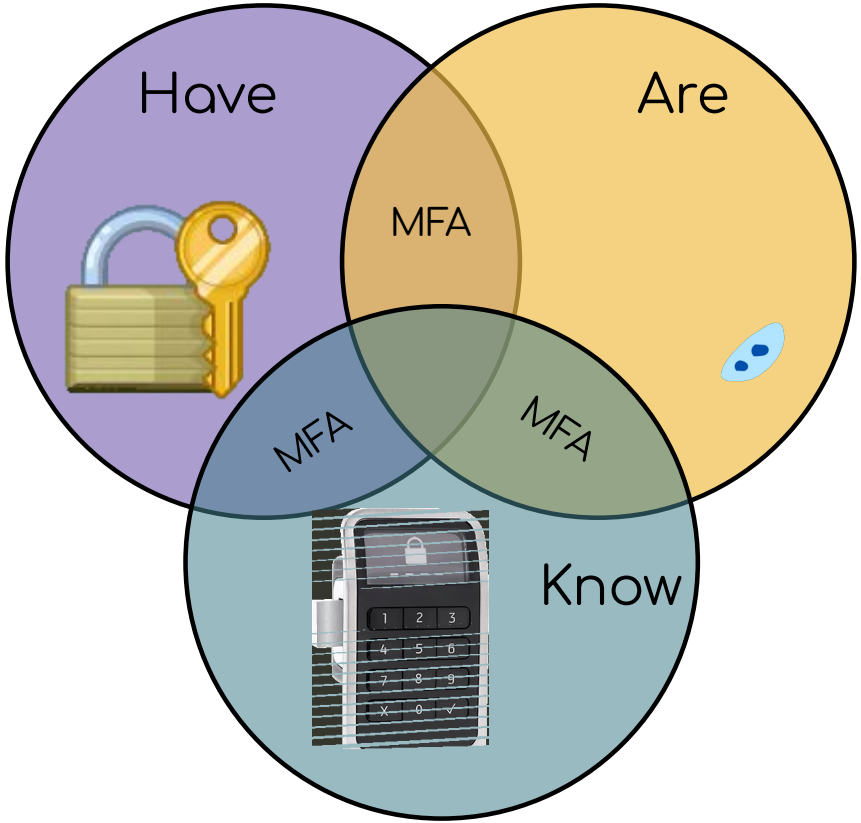


# Outline


1
Motivation and research gap
2
Literature review
3
Problem Formulation
4
Dataset and Proposed Solution
5
Conclusion

# Motivation

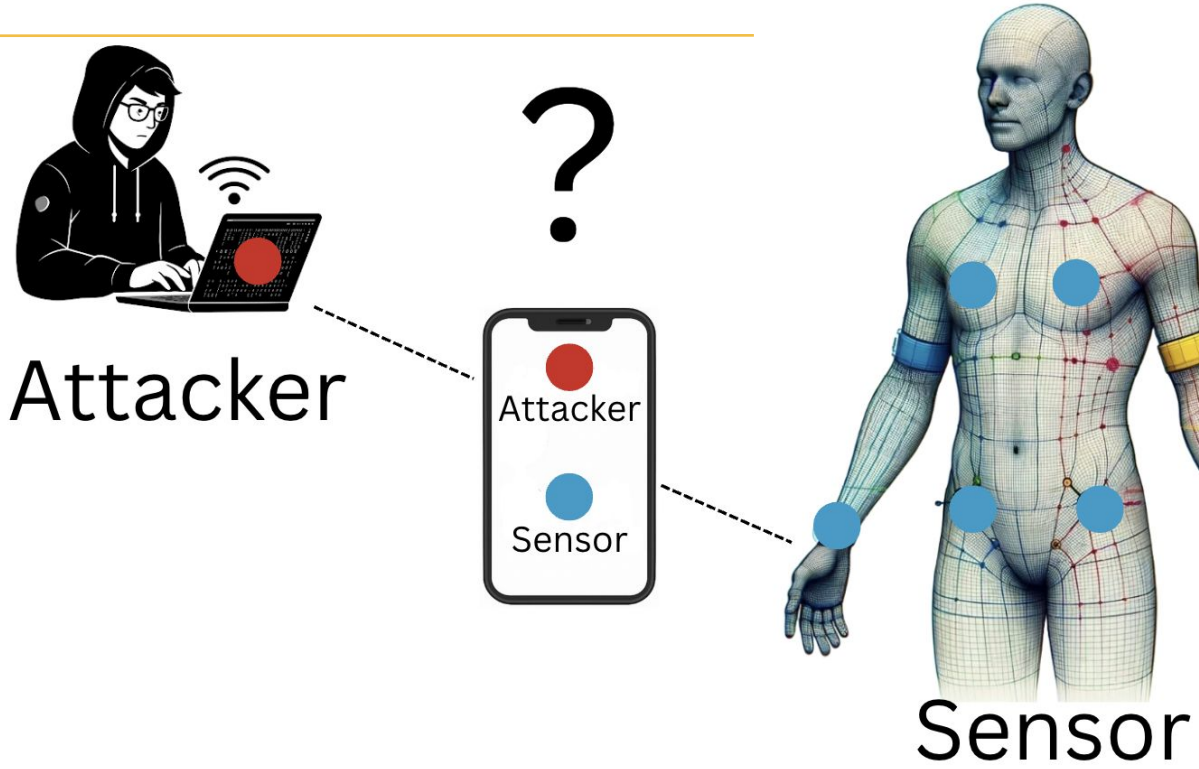
# Authentication



# Problem Statement

How does the receiver ensure the integrity of the data?

- Source Authentication
- Data Authentication



# Authentication in BLE and IEEE 802.15.6

BLE uses 3 schemes to avoid Man-In-The-Middle attacks while authentication:

- Numeric comparison
- Passkey entry
- Out-of-Bound (such as NFC)

IEEE 802.15.6:

- Similar mechanisms
- Option for pre-shared key

# Related solution

"Physiological-Signal-Based Key Agreement for Body Sensor Networks," *IEEE Transactions on Information Technology in Biomedicine*, 2016.

**Common Bio-Signals Used:**

- ECG, EEG, …

**Downside:**

- Can be forged **"Biosignal Authentication Considered Harmful Today,** Usenix 2024 Amir Rahmati, Stony Brook University

# Contributions

- Source Authentication
  - "A channel-based authentication using machine learning for body sensor networks." In *GLOBECOM 2022-2022 IEEE Global Communications Conference*,
  - "Bluetooth Low Energy (BLE) RF Dataset for Machine Learning in WBANs." In 2024 IEEE Wireless Communications and Networking Conference (WCNC):
  - "Radio Frequency Fingerprinting in WBANs Using Complex-Valued Convolutional Neural Networks." In IWCMC 2024 IoT & Wireless Sensors Symposium (pp. 6).
  - "**Towards resilient radio frequency fingerprinting: An anomaly detection-based approach.**" Manuscript
- Data Authentication
  - "**Two-Dimensional Compound Message Authentication Code in Lossy Channels**" 2025 IEEE International Conference on Communications (ICC)
  - "**Enhancing NextG Wireless Security: A Lightweight Secret Sharing Scheme with Robust Integrity Check for Military Communications,**" MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM)
  - "***OptiMAC: Optimization framework for MAC aggregation under adversarial environments.***" Manuscript

# Proposed Solution

# Physical Layer Signal's Fingerprint

Extracting unique **hardware** and **channel characteristics** for sensor authentication

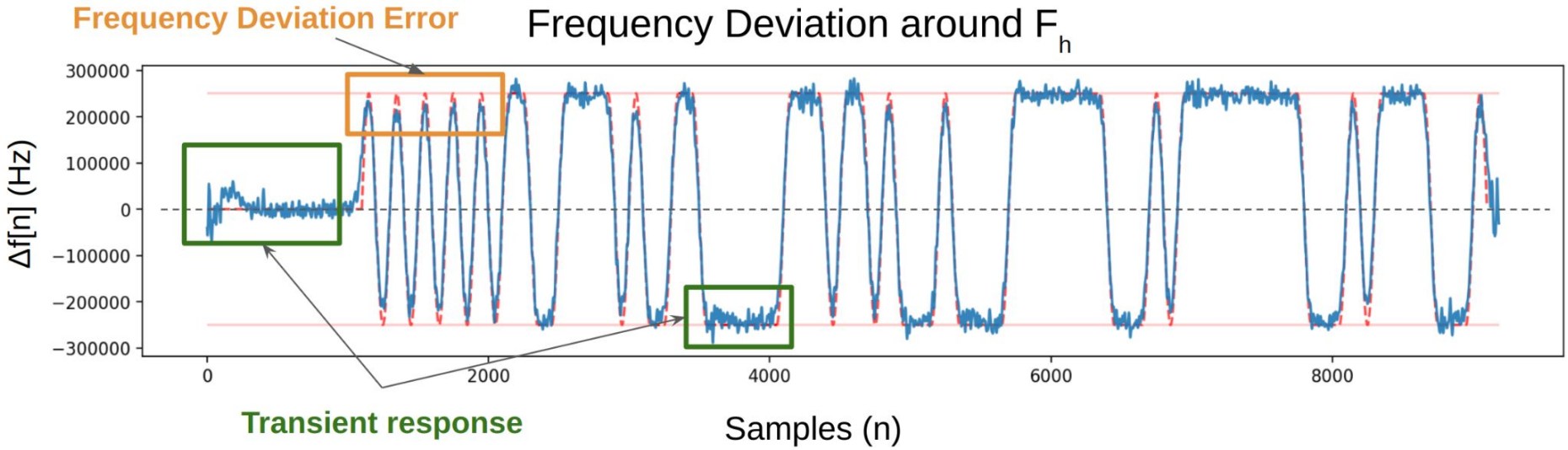
Device fingerprint:

- Hardware imperfections

Channel fingerprint:

- In WBAN, **body** affects the RF signal.

# Physical layer Signal



# Related Work

CCSS: Collaborative Research: Developing A Physical-Channel Based Lightweight Authentication System for Wireless Body Area Networks
Stevens Institute of Technology, NSF Award Abstract # 2453400 at 2017

Laxima N. Kandel and Shucheng Yu "VWAN: **Virtual WiFi ANtennas** for Increased Indoor Localization Accuracy" *2019 IEEE International Conference on Industrial Internet (ICII 2019)* , 2019

Yantian Hou, Ming Li and Shucheng Yu "Making Body Area Networks **Robust against Cross-Technology Interference**" *IEEE Transactions on Wireless Communications (TWC)* , v.16 , 2017

Laxima N. Kandel, Zhuosheng Zhang and Shucheng Yu "Exploiting **CSI-MIMO for Accurate and Efficient Device Identification**" *2019 IEEE Global Communications Conference (Globecom 2019)* , 2019

# Related Work

**A Noise-Robust Radio Frequency Fingerprint Identification Scheme for Internet of Things Devices** Yuexiu Xing et al. IEEE INFOCOM WKSHPS (2023)

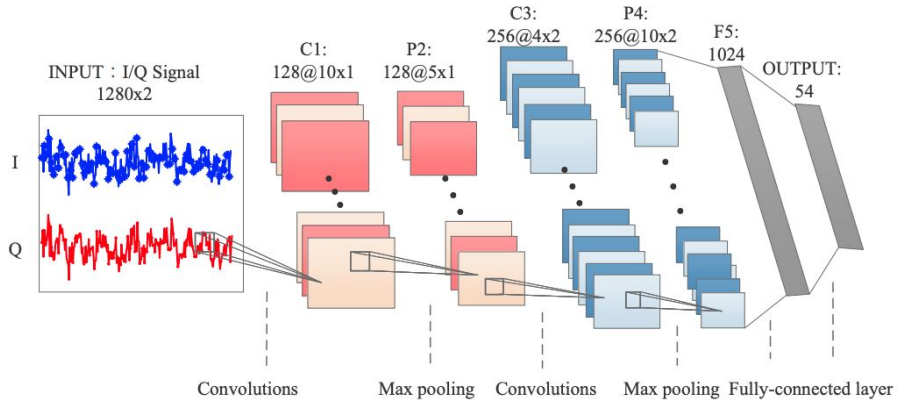


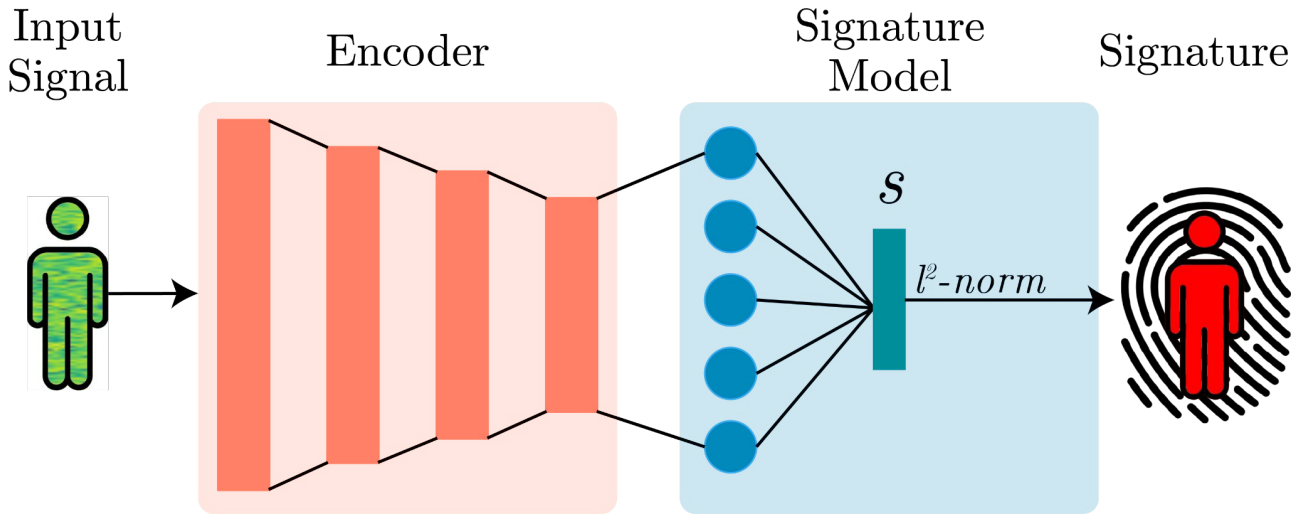

Fig. 4. The architecture of the proposed CNN.

Accuracy of 54 Zigbee node classification from 30% to 99% In different SNR

# Related Work

**WhoFi: Deep Person Re-Identification via Wi-Fi Channel Signal Encoding,**

Danilo Avola, Daniele Pannone, Dario Montagnini, Emad Emam - 17 July 2025 Arxiv - La Sapienza University of Rome




- 14 people
- 95.5 % accuracy

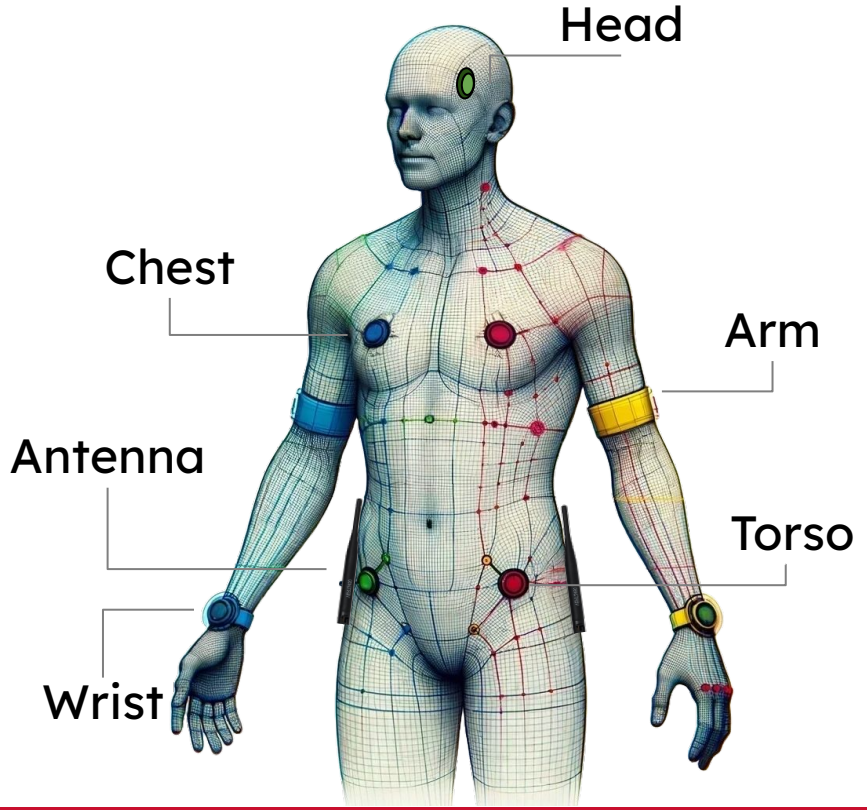
# Dataset

- **On** and **off body** recordings
- **Two** different USRP X310 **SDRs** for recordings
- Recording inside **anechoic chamber**


- **Entire BLE spectrum** with high sampling rate of **100 MSps**

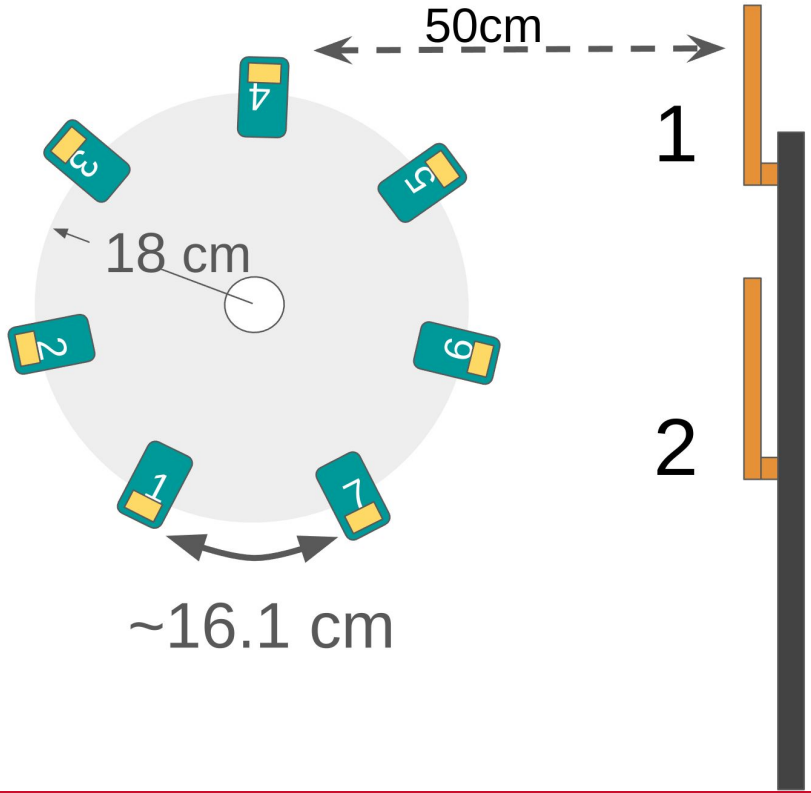
# BLE-WBAN (on-body)

- **12** BLE devices on the body
- **Two** receiving **antennas** on the left and right side of the hip
- Body at **rest** and body in **motion** recordings
- **Dataset Size = 10GB**



# BLE-WBAN (off-body)

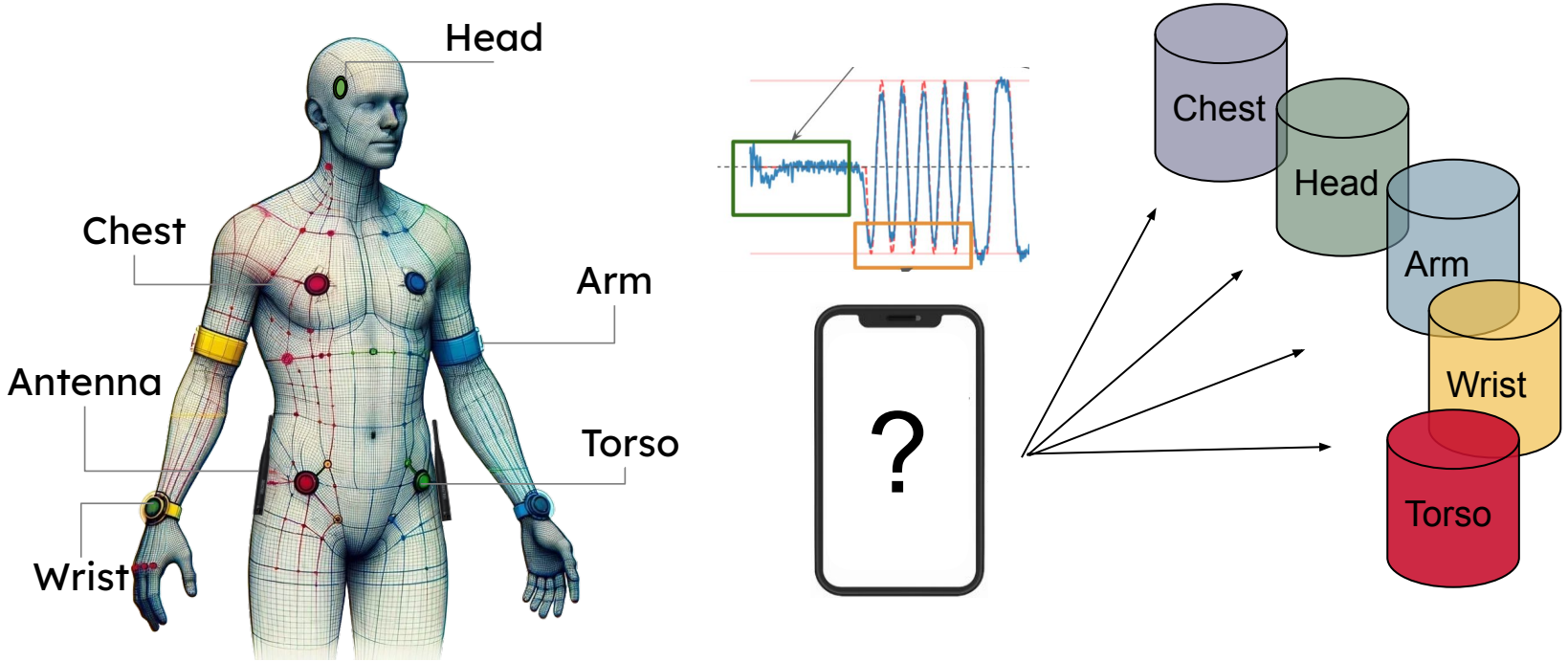
- 13 BLE **devices** on
- 7 different **positions**
- 2 different **TX power** levels
- 2 receiving **antenna**
- **Dataset Size = 40GB**




Appeared on:
**"Bluetooth Low Energy (BLE) RF Dataset for Machine Learning in WBANs."** In 2024 IEEE Wireless Communications and Networking Conference (WCNC):

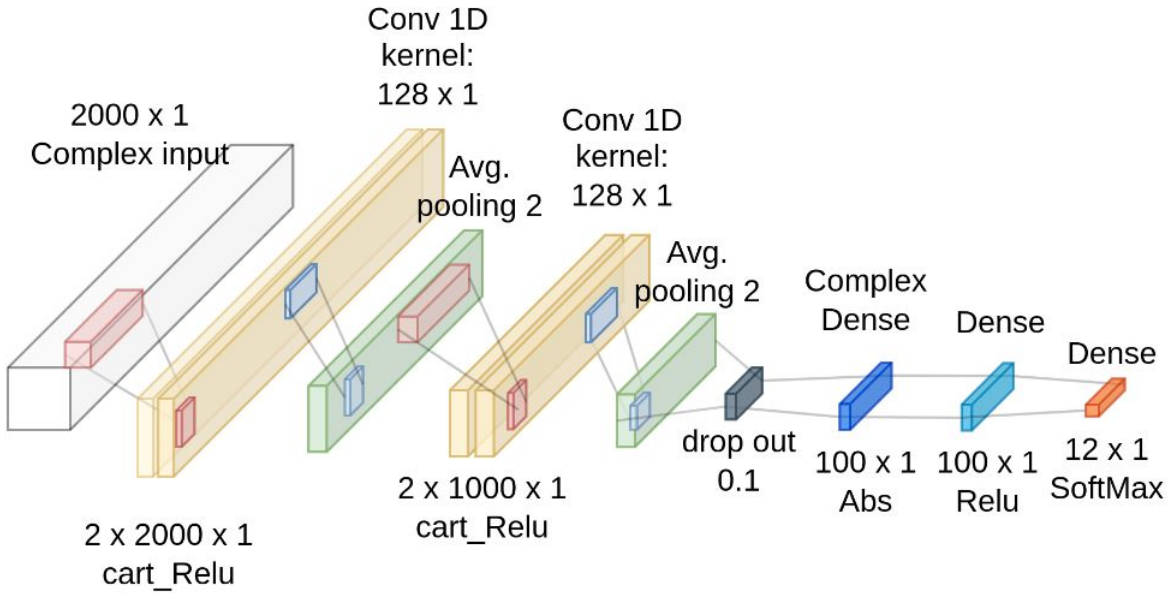
# Proposed Solutions

# Source Classification Problem Definition



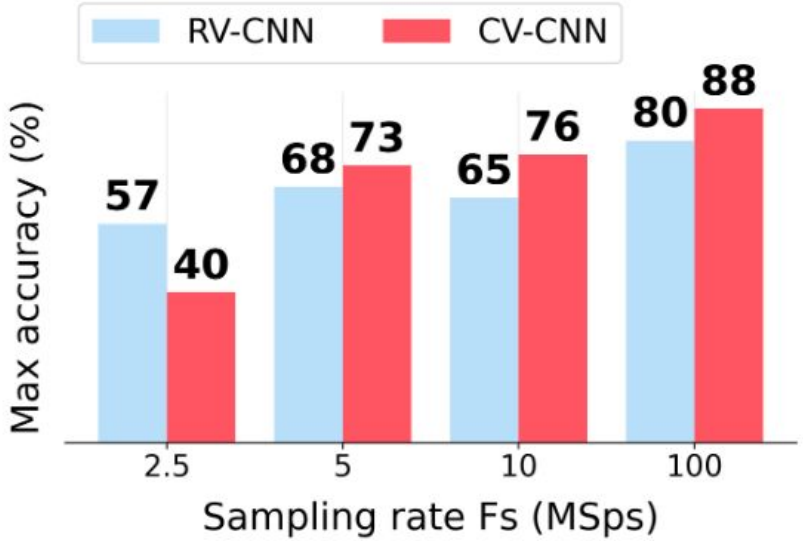
# Proposed Complex-Valued Architecture

Preamble
(first 2000 samples)



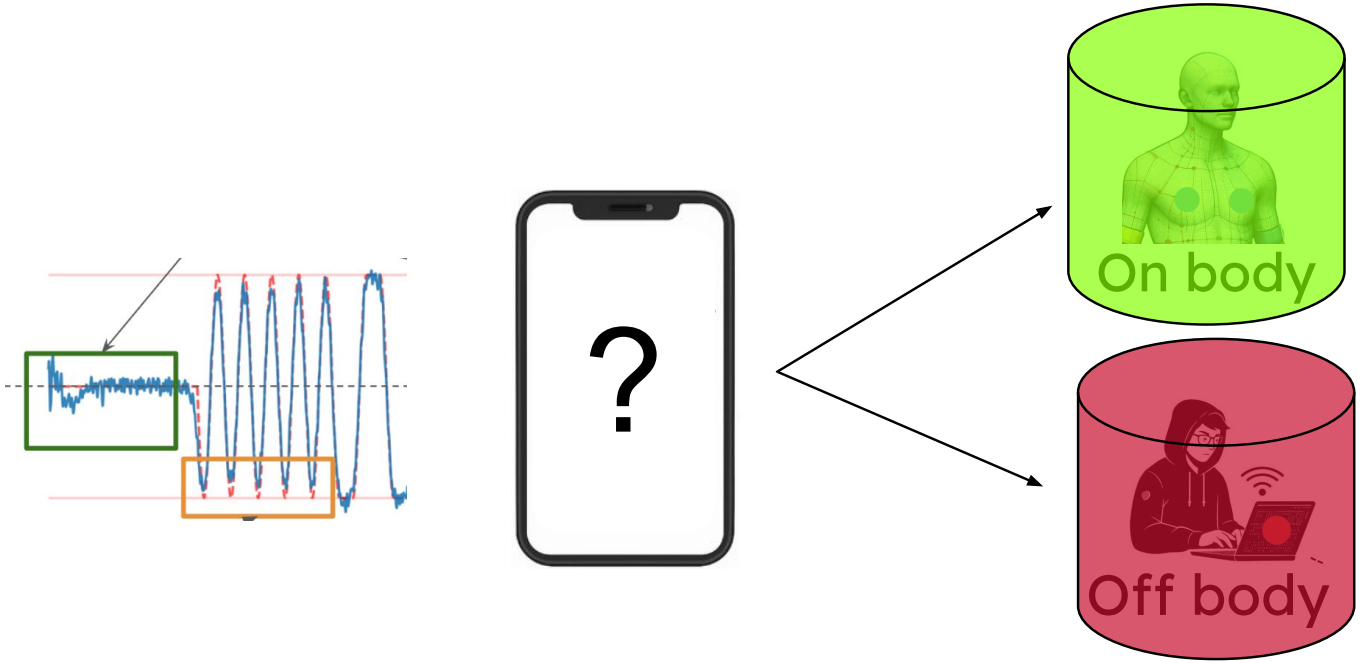

174,757 Parameters in total

# Fingerprinting Results



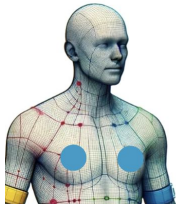

Appeared on:
"**Radio Frequency Fingerprinting in WBANs Using Complex-Valued Convolutional Neural Networks.**" In IWCMC 2024 IoT & Wireless Sensors Symposium (pp. 6).

# Anomaly Problem Definition



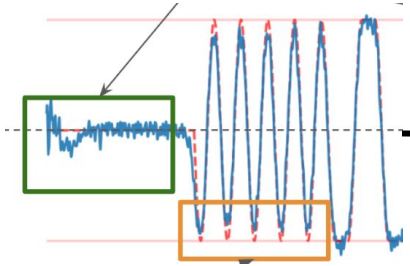
# Anomaly Detection

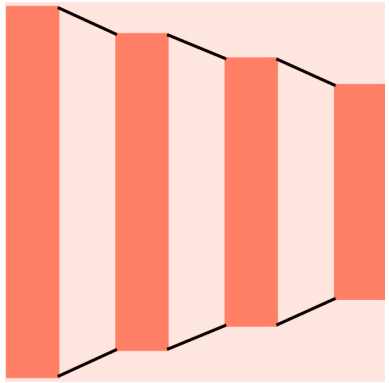
# Embedding Model



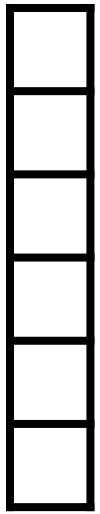
On body

Off body



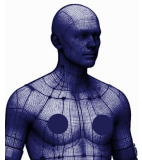


Complex valued Encoder

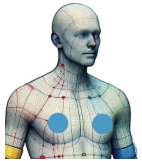


Vector

# Triplet Ranking Loss

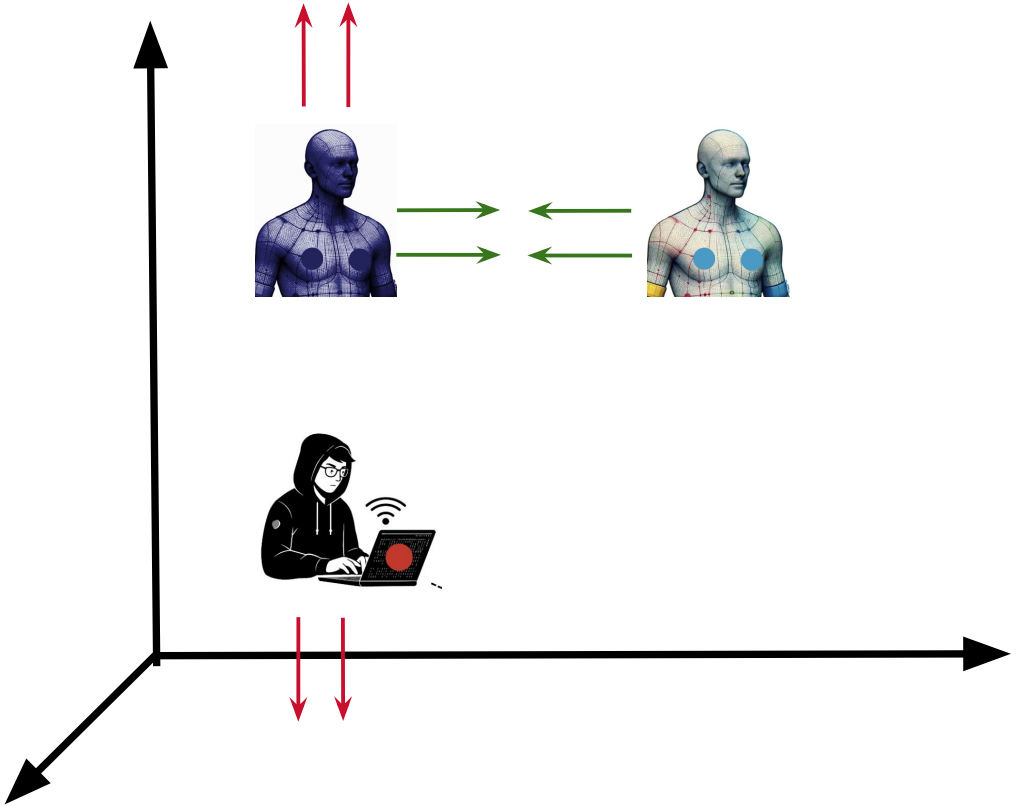


Anchor

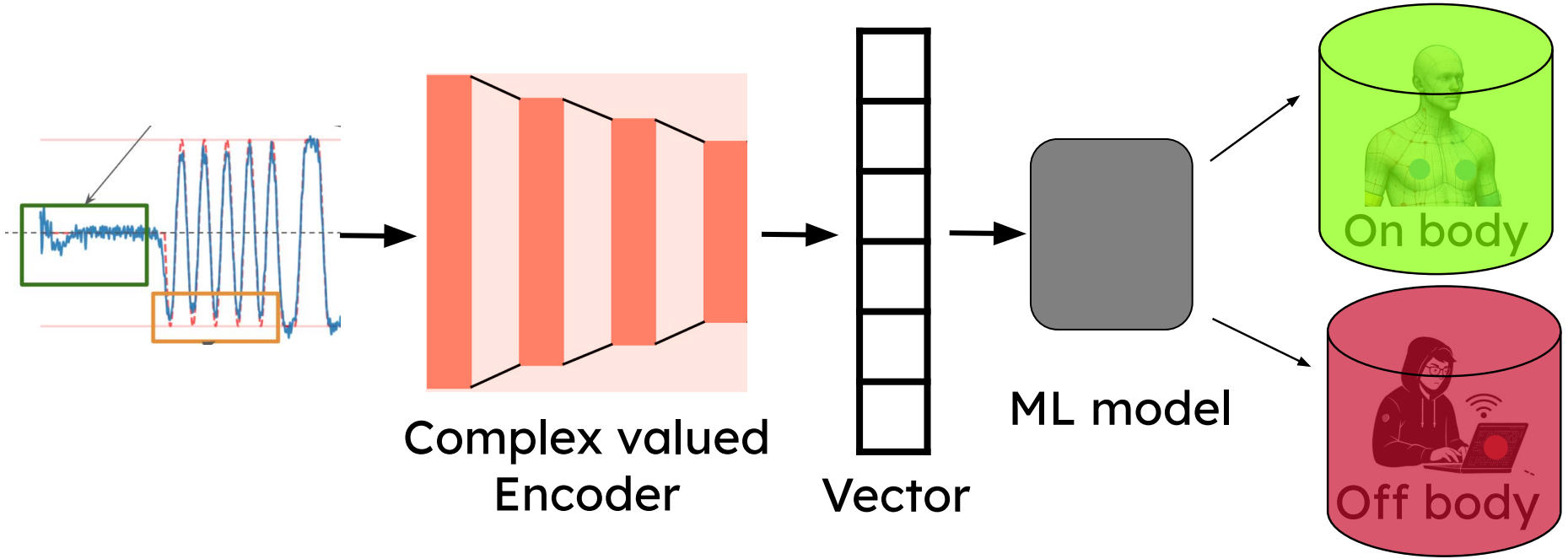


Positive

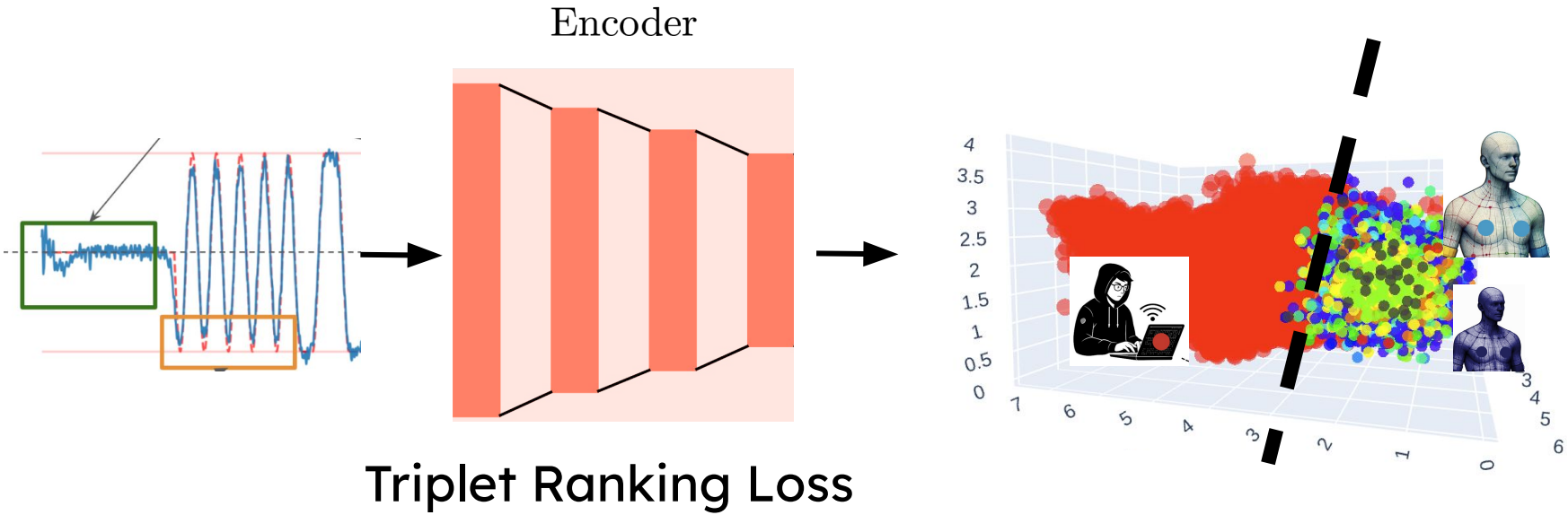
Negative



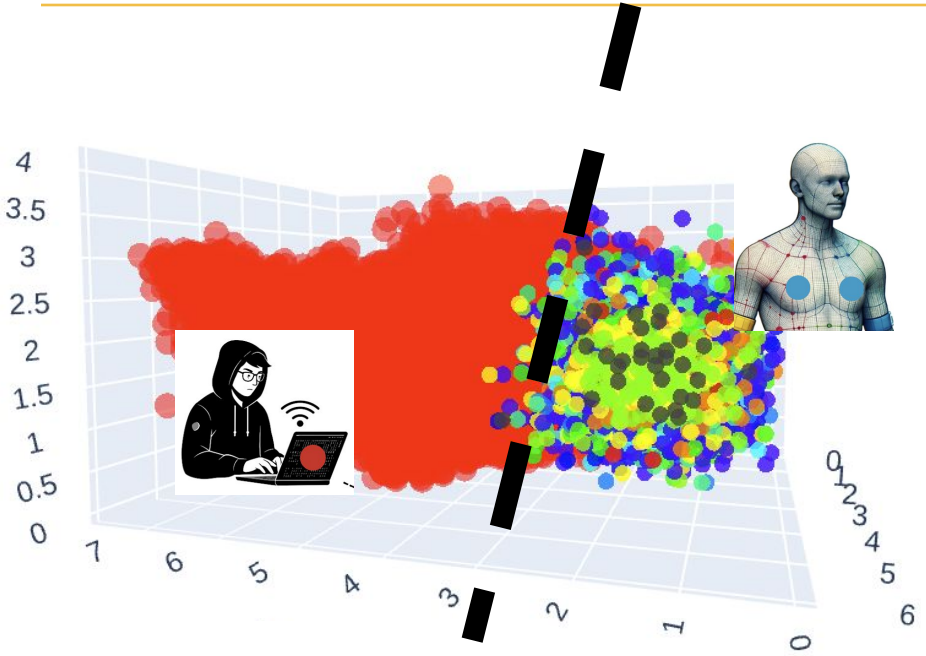
# Embedding Model



# Proposed Anomaly Detection Model



# Anomaly Detection Results




- 12 sensors
- 98 % accuracy

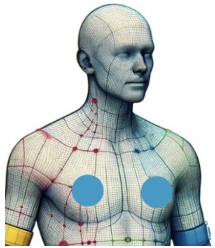
Manuscript:

**“Towards resilient radio frequency fingerprinting: An anomaly detection-based approach.”**

# Message Authentication Code (Part 2)

# Problem Definition

How to ensure a message is not modified?

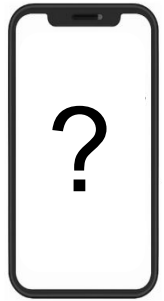


CGM Sensor

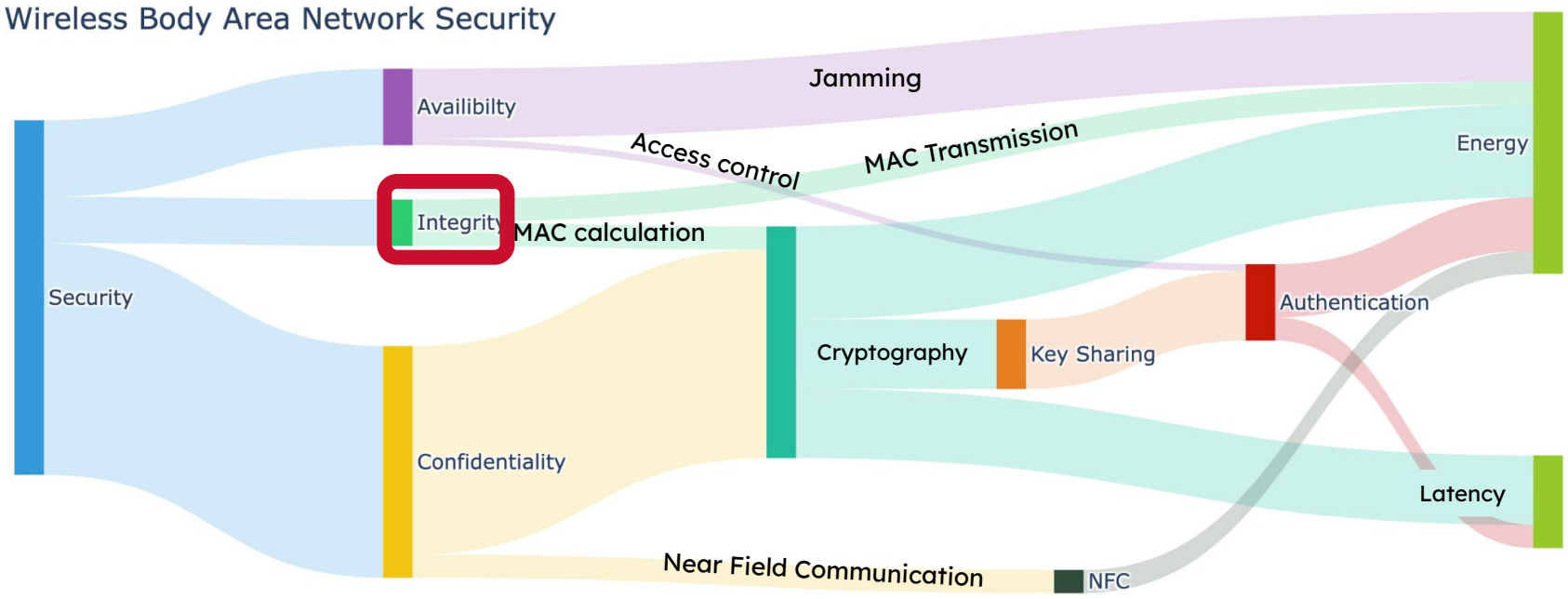
Glucose Level
400

Glucose Level
120

Modification



# Security in WBAN



# Problem Definition


**Figure 1:** Traditional MAC

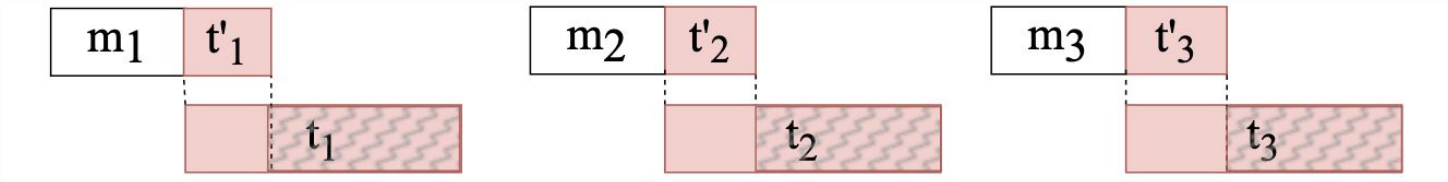



**Figure 2:** Truncated MAC

# Related Work

- Aggregate tag or compound messages to reduce tag transmissions.

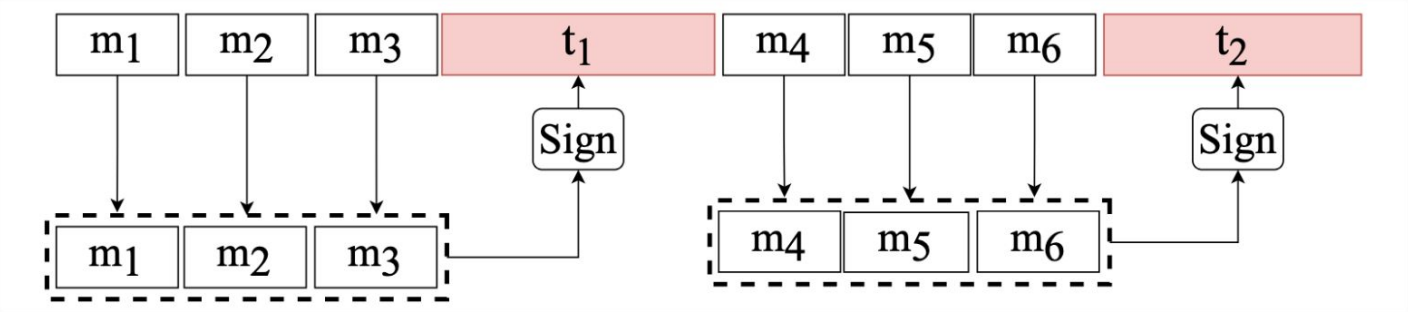
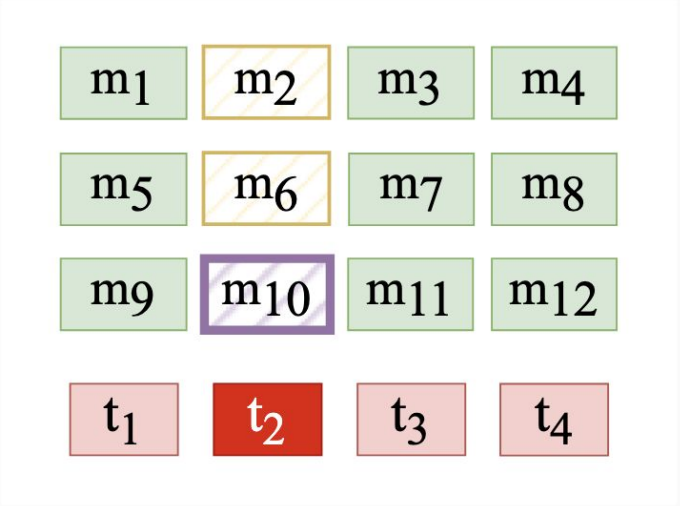



**Figure 3:** Compound MAC

Nilsson, D. K., Larson, U. E., Jonsson, E. (2008, September). Efficient in-vehicle delayed data authentication based on compound message authentication codes. In 2008 IEEE 68th Vehicular Technology Conference (pp. 1-5). IEEE.

# Related Work Limitation

- Column integrity check fails if there is one loss. For instance, loss of m10 will prevent m2 and m6 from verification.
- Requires finer-grain verification.



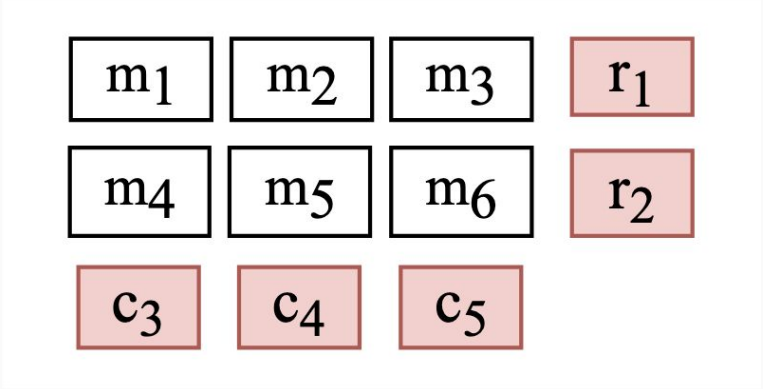
# Proposed Solution

# 2D MAC

Arrange $m \times n$ messages in a grid, compute:

- One tag per **row**
- One tag per **column**

A single loss affects only its row and column.



# 2D MAC vs 1D MAC

| | Trad | 1D | 2D |
|---|---|---|---|
| Number of tags for $m \times n$ messages | $m \times n$ | $n$ | $m + n$ |

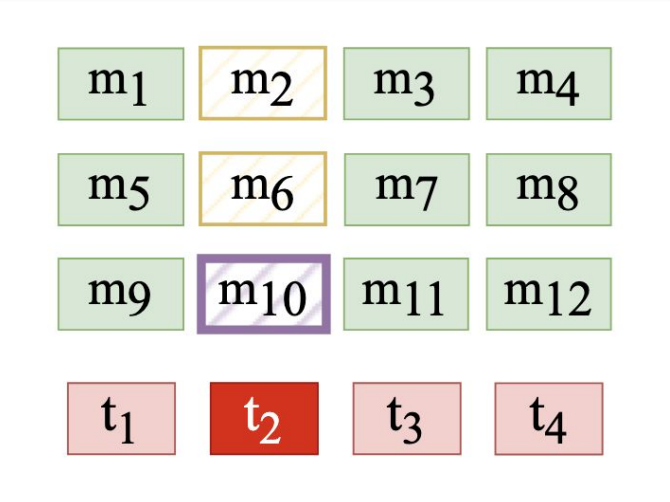



**Figure 4:** 1D-MAC

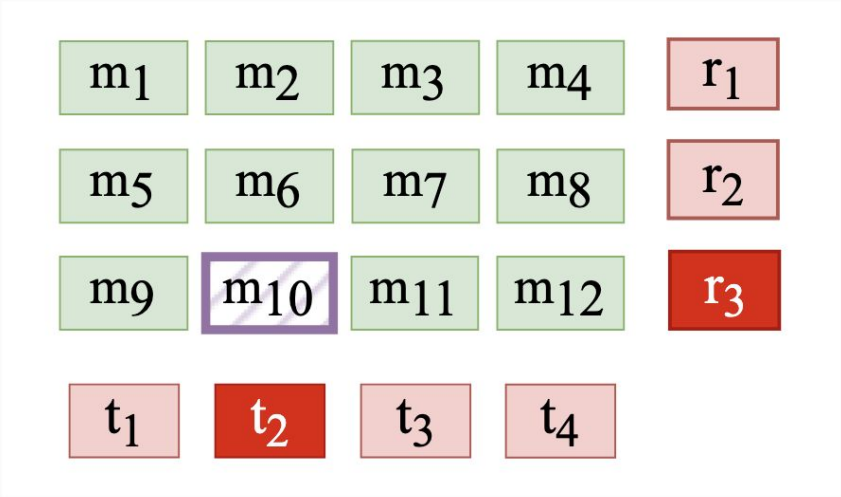
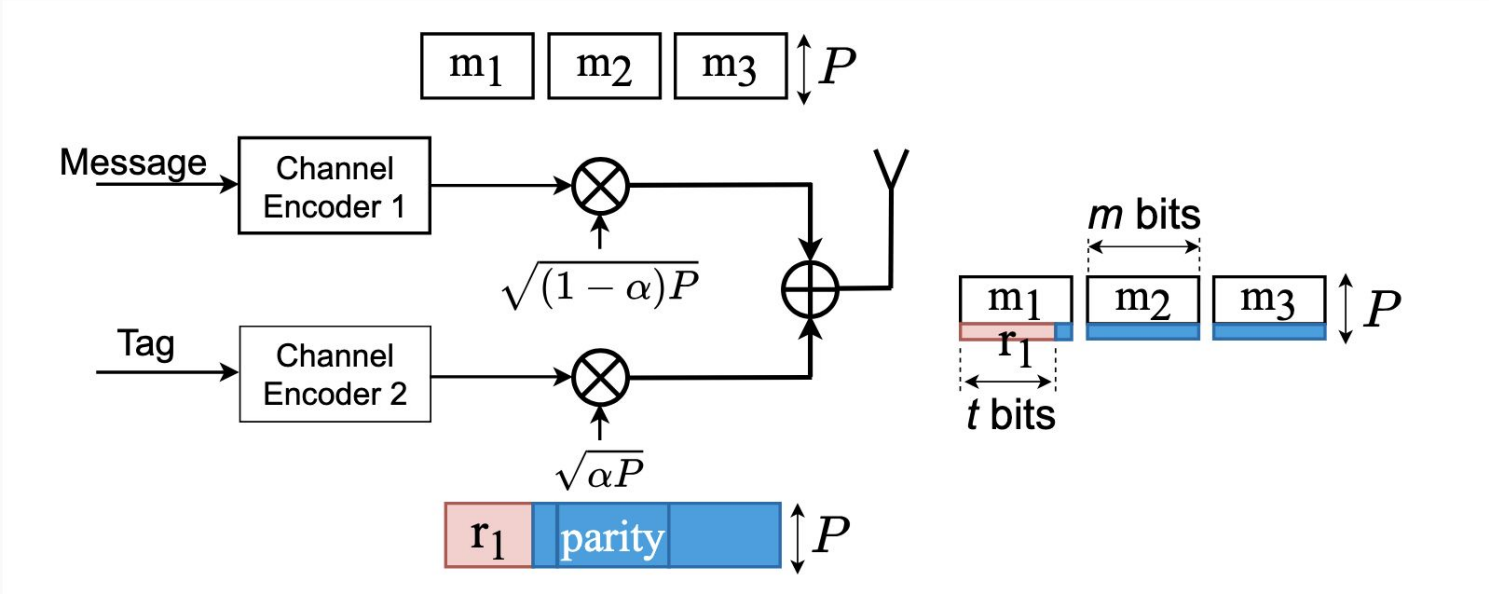



**Figure 5:** 2D-MAC

# Superposition Coding

**Key Idea**

Embed row tags into the messages to reduce the overhead.



# 1D vs 2D vs 2D MAC with Superposition Coding

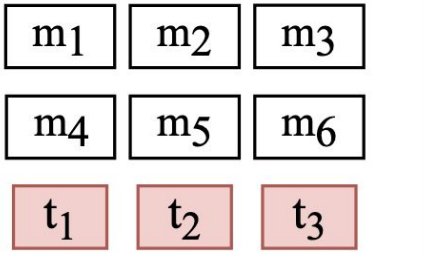



**Figure 6:** 1D-MAC

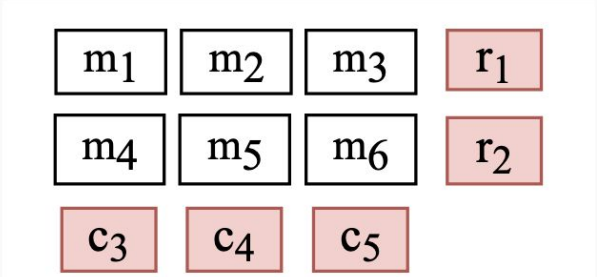



**Figure 7:** 2D-MAC

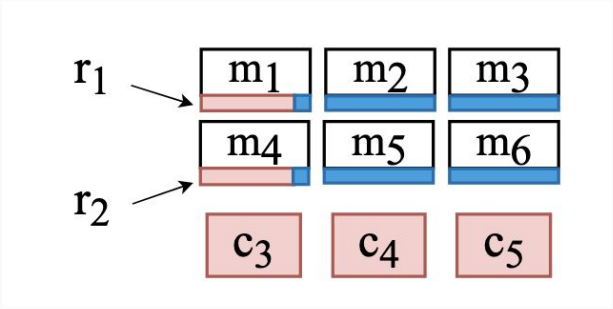


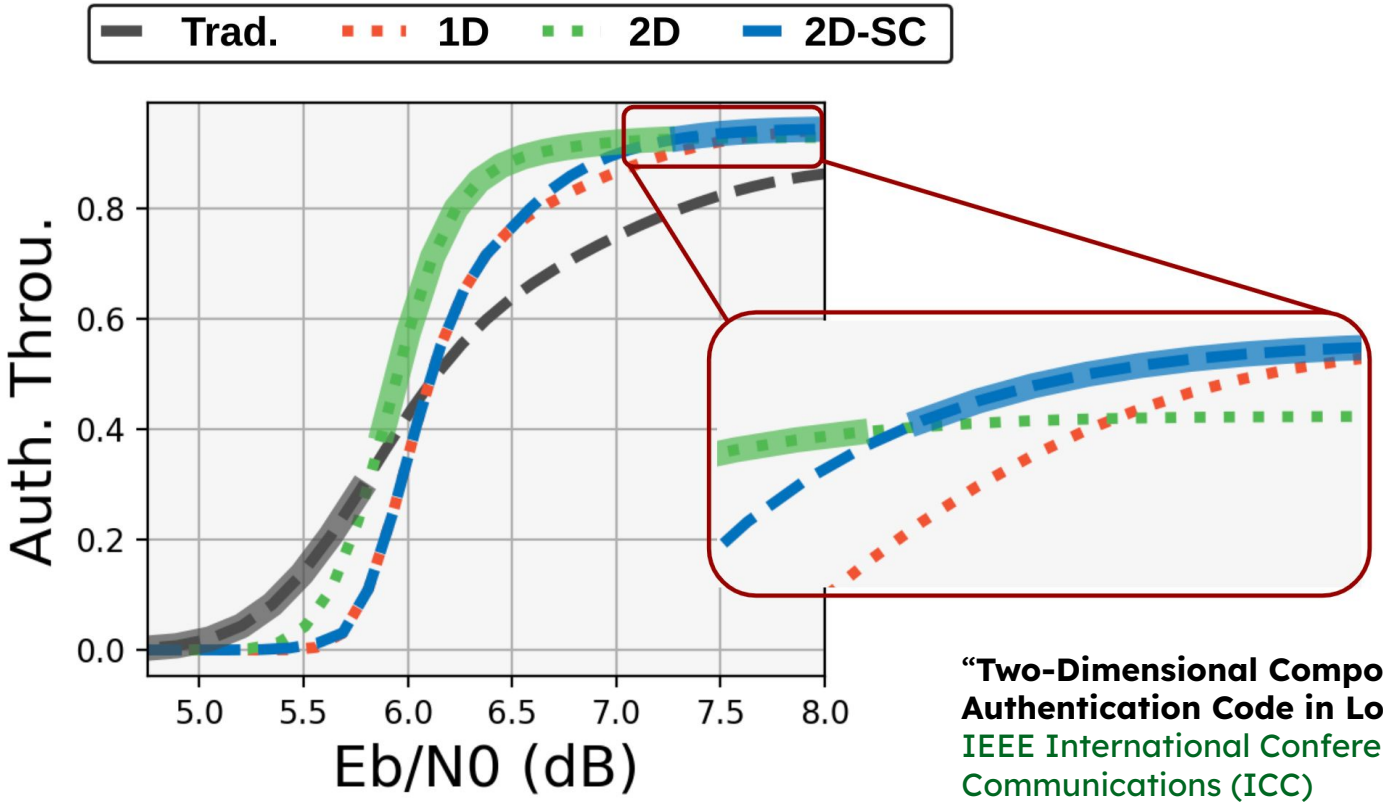

**Figure 8:** 2D-SC

# Authentication Throughput (AT)

$$AT = \frac{\sum_i Pr(\text{verifying received } m_i)|m_i| \times R}{|M| + |T|}$$

$$\sum_{i=1}^{M} |m_i| = |M|, \sum_{i=1}^{T} |t_i| = |T|$$

# Results

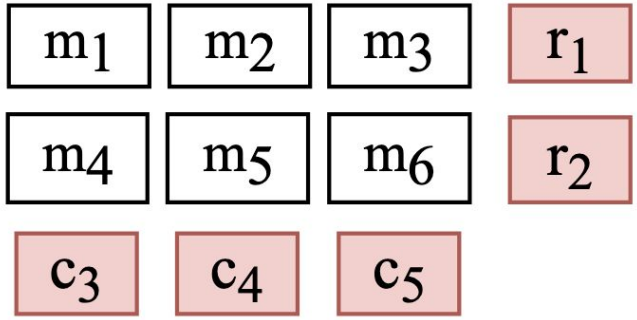



**"Two-Dimensional Compound Message Authentication Code in Lossy Channels"** 2025 IEEE International Conference on Communications (ICC)

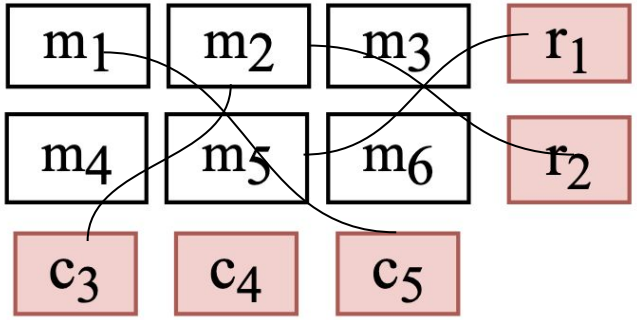
# OptiMAC

# Problem Definition

What is the best tag to message assignment?

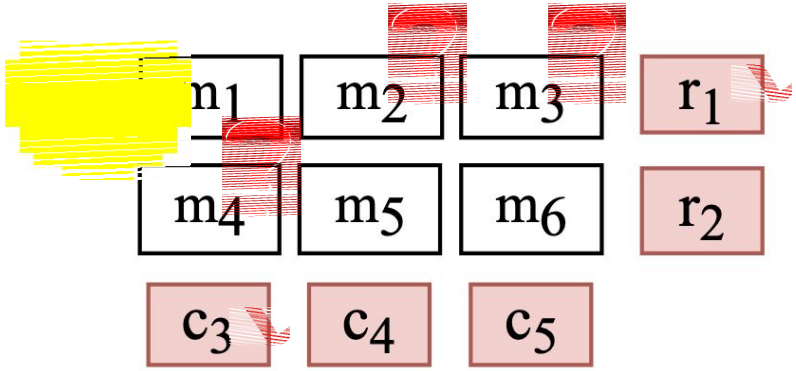


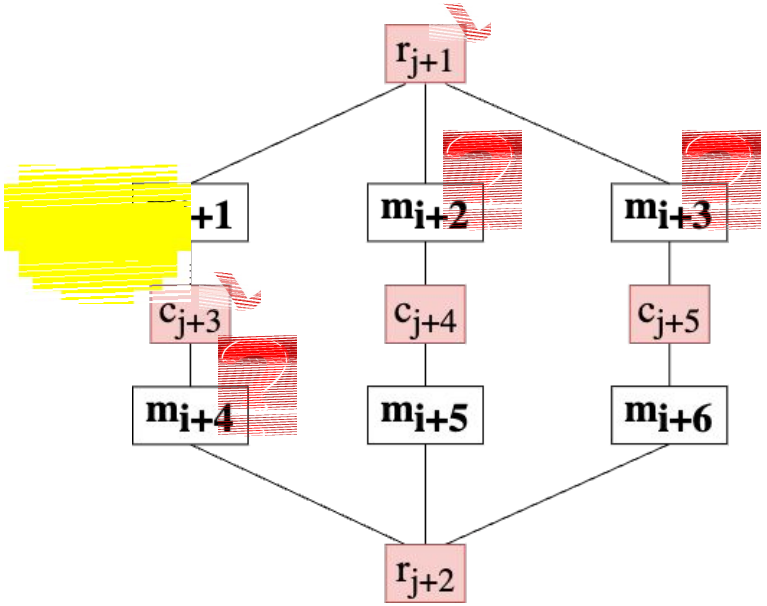

2D MAC




nD MAC

# Dependency Graph



# Dependency Matrix

$$\mathbf{X} = \begin{array}{c|ccccccc} & t_1 & \cdots & t_{j+1} & t_{j+2} & t_{j+3} & \cdots & t_n \\ \hline m_1 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{i-1} & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ m_i & 0 & \cdots & 1 & 1 & 0 & \cdots & 0 \\ m_{i+1} & 0 & \cdots & 1 & 1 & 1 & \cdots & 0 \\ m_{i+2} & 0 & \cdots & 0 & 1 & 1 & \cdots & 0 \\ m_{i+3} & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m_m & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{array}$$

Tag to Message Ratio (TMR).

$$\frac{n}{m} = \frac{\text{total number of tags}}{\text{total number of messages}}$$

## Optimize Using MILP

The objective function is to maximize the **expected number of usable tags** for all messages given the likelihood of packet loss or modification rate and $m$,$n$.

$$\max \quad \sum_{i\in I}\sum_{j\in J}\sum_{k\in K} U_{ij}^{k} \tag{9}$$

$$s.t.$$

$$w^k y_{ij}^k |t_j| = U_{ij}^k \qquad \forall i \in I, j \in J, k \in K \tag{10}$$

$$\sum_{i\in I} x_{ij} = \sum_{k\in K} k z_j^k \qquad \forall j \in J \tag{11}$$

$$\sum_{k\in K} z_j^k \leq 1 \qquad \forall k \in K \tag{12}$$

$$x_{ij} + z_j^k \geq 2y_{ij}^k \qquad \forall i \in I, j \in J, k \in K \tag{13}$$

$$\sum_{j\in J}\sum_{k\in K} U_{ij}^k = A' \qquad \forall i \in I \tag{14}$$

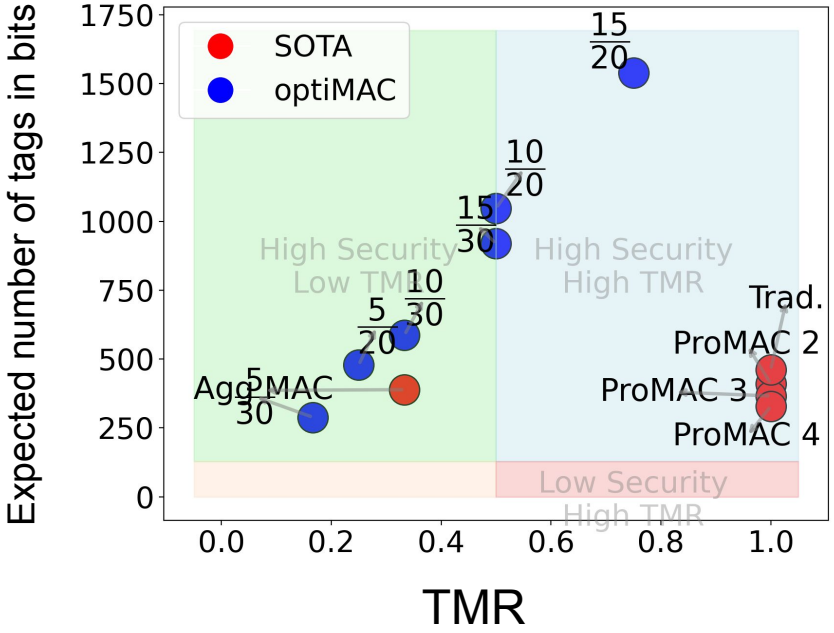
$$\sum_{j\in J} x_{ij} \geq 1 \qquad \forall i \in I \tag{15}$$

$$A' \geq 0 \tag{16}$$

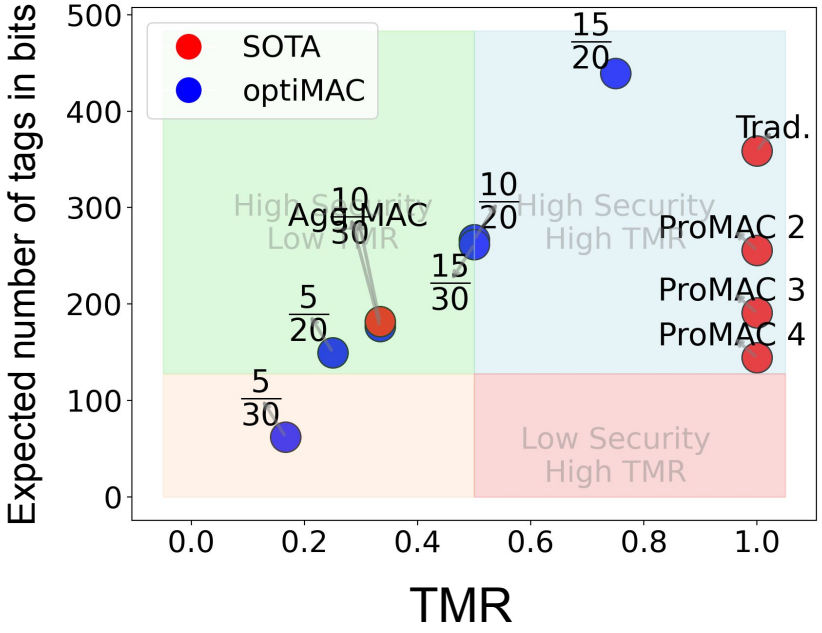
$$x_{ij}, z_j^k, y_{ij}^k \in \{0,1\} \tag{17}$$

# Results

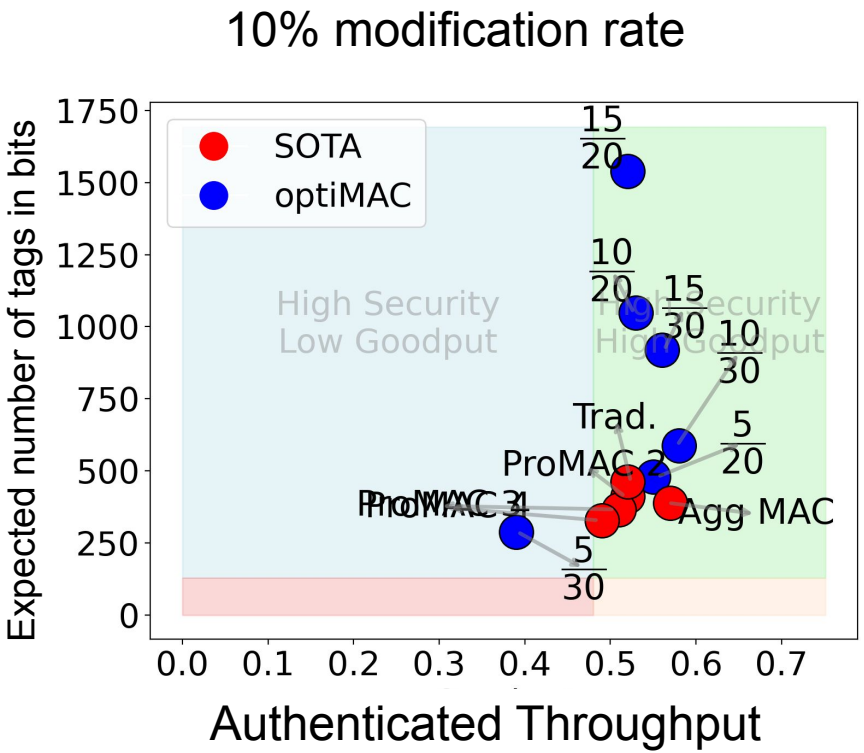
10% modification rate

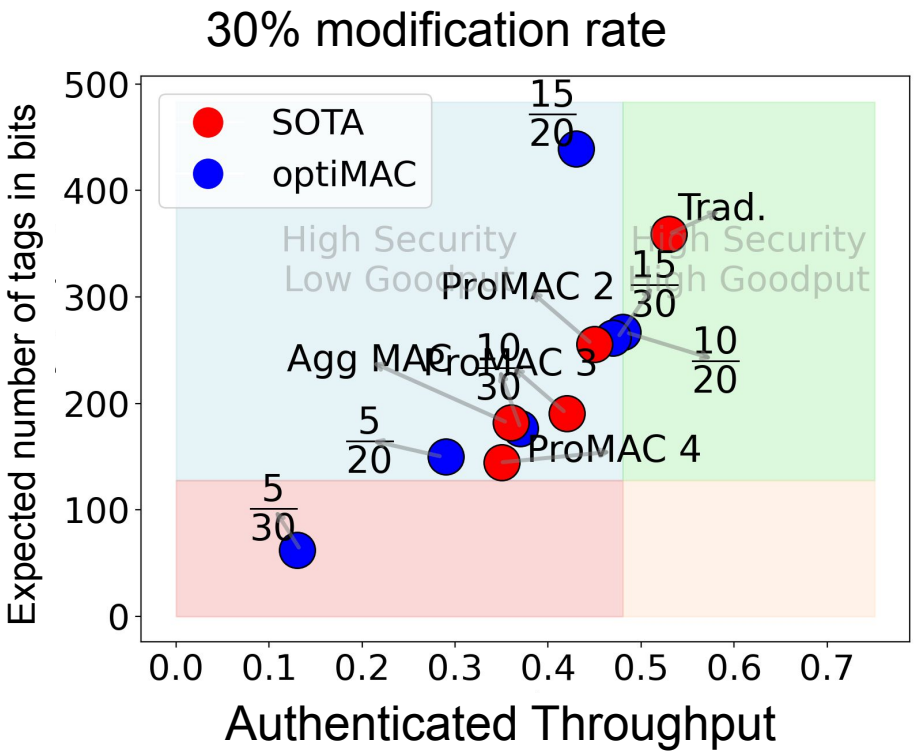



30% modification rate



# Results


10% modification rate
SOTA
optiMAC
High Security
Low Goodput
High Security
High Goodput
15/20
10/20
15/30
10/30
Trad.
5/20
ProMAC 2
ProMAC 3
ProMAC 4
Agg MAC
5/30
Expected number of tags in bits
Authenticated Throughput
0
250
500
750
1000
1250
1500
1750
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7


30% modification rate
SOTA
optiMAC
High Security
Low Goodput
High Security
High Goodput
15/20
Trad.
ProMAC 2
15/30
10/30
10/20
Agg MAC
ProMAC 3
5/20
ProMAC 4
5/30
Expected number of tags in bits
Authenticated Throughput
0
100
200
300
400
500
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7

# Will be appeared on

"***OptiMAC: Optimization framework for MAC aggregation under adversarial environments.***" Manuscript

# Conclusion

# Conclusion

In this PhD, we addressed two critical aspects of securing wireless healthcare sensors:

1. **Source Authentication**, using complex-valued RF fingerprinting models, achieving 98% accuracy in distinguishing on-body from off-body devices.

2. **Message Authentication**, through the design of a 2D MAC scheme and OptiMAC optimized message to tag assignments.

- Collected a high-quality, large-scale BLE dataset.
- I have had a lot of stress and fun.

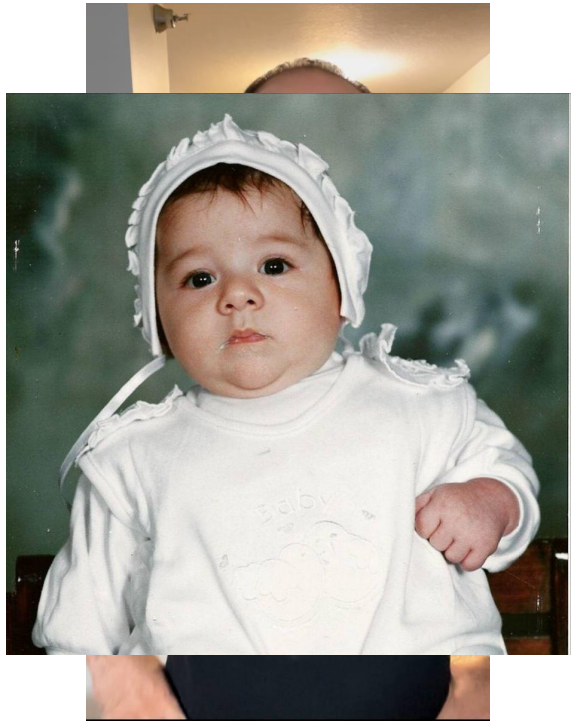
# Future Research

- Deploy our anomaly detection and MAC optimization in a real-time system.
- Extend evaluation to more users and dynamic movement scenarios.
- Investigate integration with quantum-resilient authentication techniques.

# Publications to-date

- Kashani, SeyedMohammad, Farid Nait-Abdesselam, and Ashfaq Khokhar. "**A channel-based authentication using machine learning for body sensor networks.**" In *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pp. 1103-1108. IEEE, 2022.
- Kashani, S., Sherazi, S., Khokhar, A., Kim, S., & Nait-Abdesselam, F. (2024). "**Bluetooth Low Energy (BLE) RF Dataset for Machine Learning in WBANs.**" In 2024 IEEE Wireless Communications and Networking Conference (WCNC): Track 3 – Resource Allocation and Machine Learning (IEEE WCNC 2024 - Track 3) (pp. 6).
- Kashani, S., Sherazi, S., Khokhar, A., Kim, S., & Nait-Abdesselam, F. (2024). "**Radio Frequency Fingerprinting in WBANs Using Complex-Valued Convolutional Neural Networks.**" In IWCMC 2024 IoT & Wireless Sensors Symposium (pp. 6).
- Kashani, S., Sherazi, A., Kim, S., Khokhar "**Two-Dimensional Compound Message Authentication Code in Lossy Channels**" 2025 IEEE International Conference on Communications (ICC)
- A. Jha *et al.*, "**Enhancing NextG Wireless Security: A Lightweight Secret Sharing Scheme with Robust Integrity Check for Military Communications,**" MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM)
- [Draft] Kashani, S., Emirhüseyinoğlu, G., Khademnia, E., Dong, Y., Wu, T., Hussain, S. R., Kim, S. W. & Khokhar, A. "***OptiMAC: Optimization framework for MAC aggregation under adversarial environments.***" manuscript, Department of Electrical and Computer Engineering, Iowa State University; School of Electrical Engineering and Computer Science, Pennsylvania State University.

# Conclusion Cont'd



Before

After

# Thank you