HealthSense project

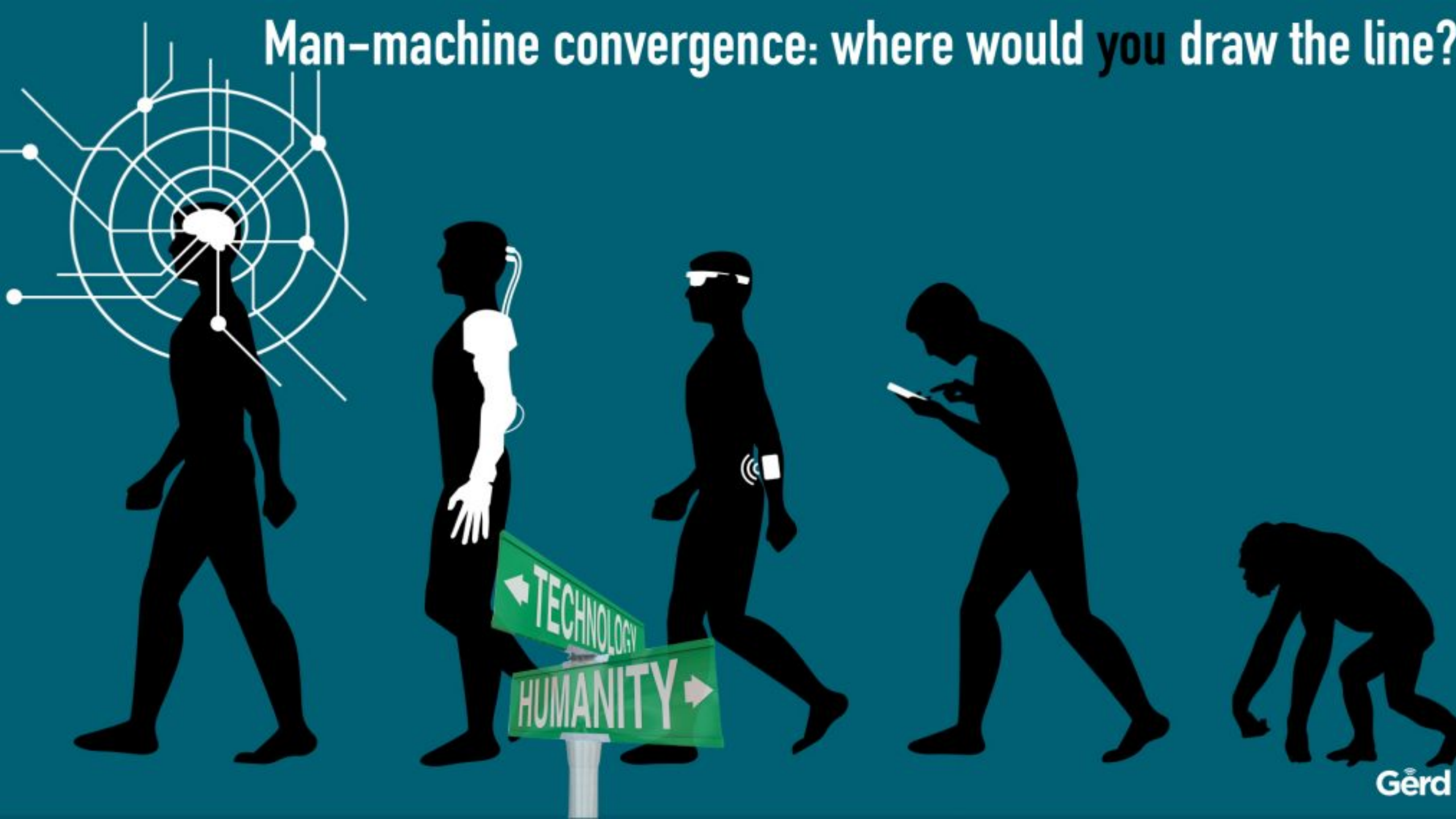
Cyber-Human System:

SECURITY ISSUES AND PERSPECTIVES FOR AUTHENTICATION AND DATA PRIVACY

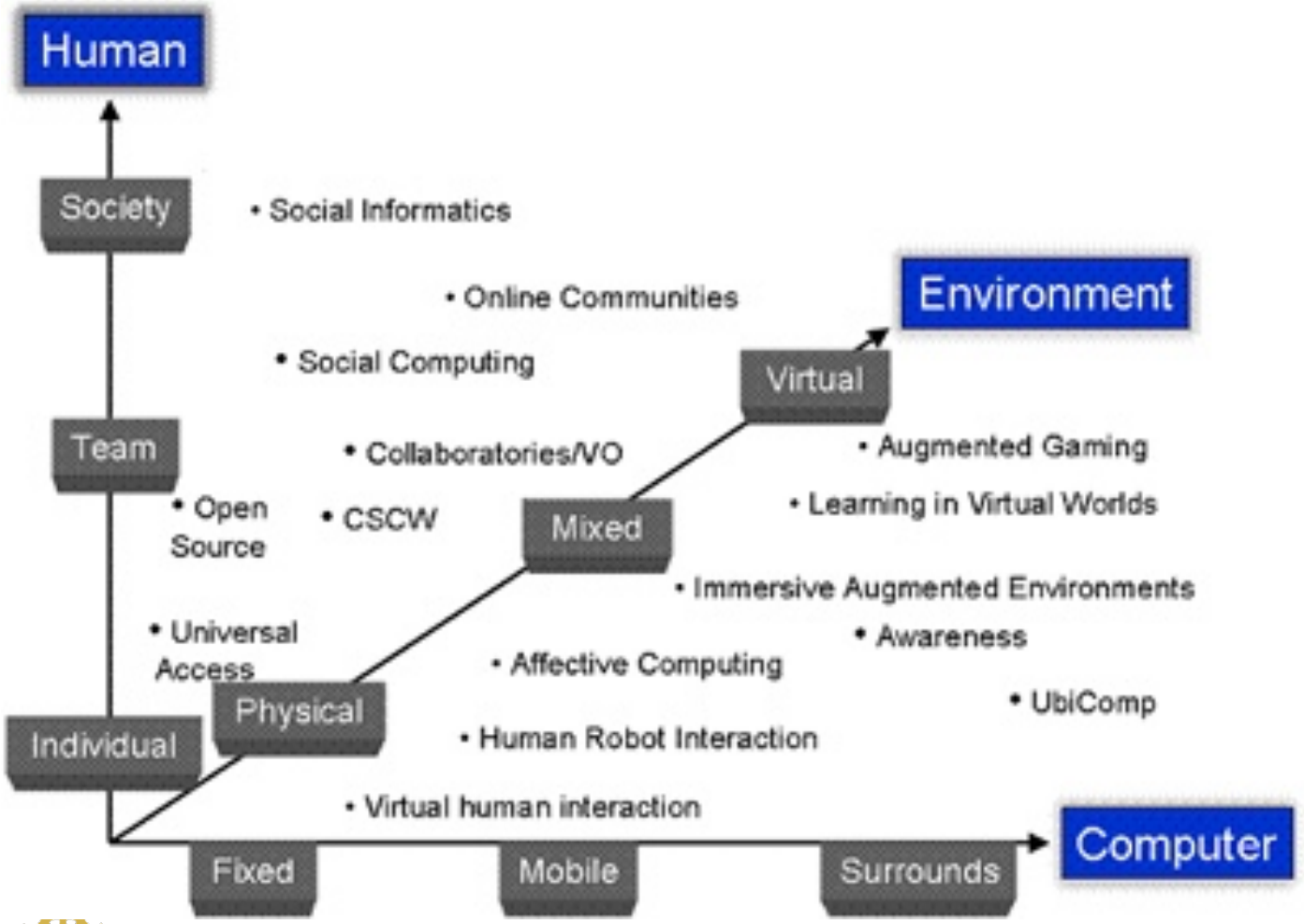
Michele Nogueira, Federal University of Paraná (UFPR)

CYBER PHYSICAL SYSTEMS WORKSHOP
Montevideo, Uruguay

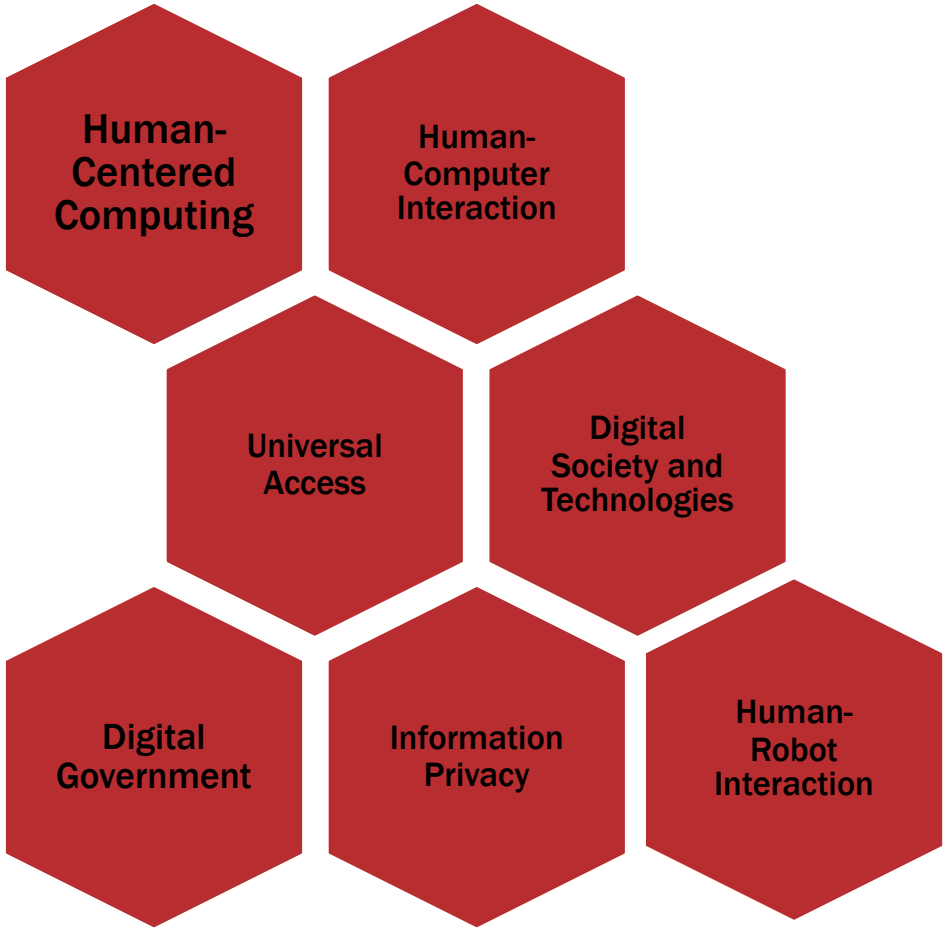
Man-machine convergence: where would you draw the line?



NSF Cyber-Human Systems

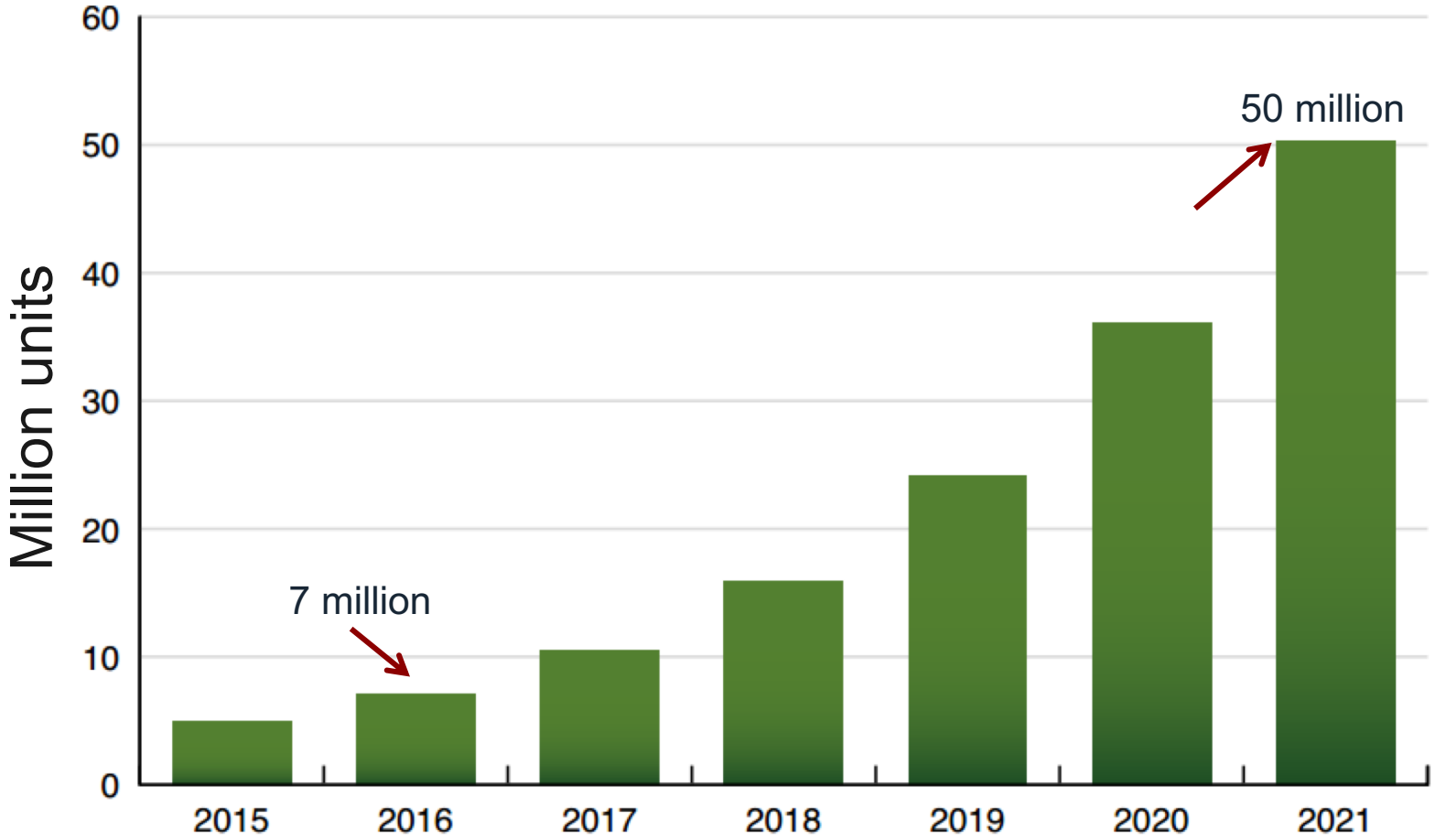


Cyber-Human Systems



Introduction

Use of medical applications and devices

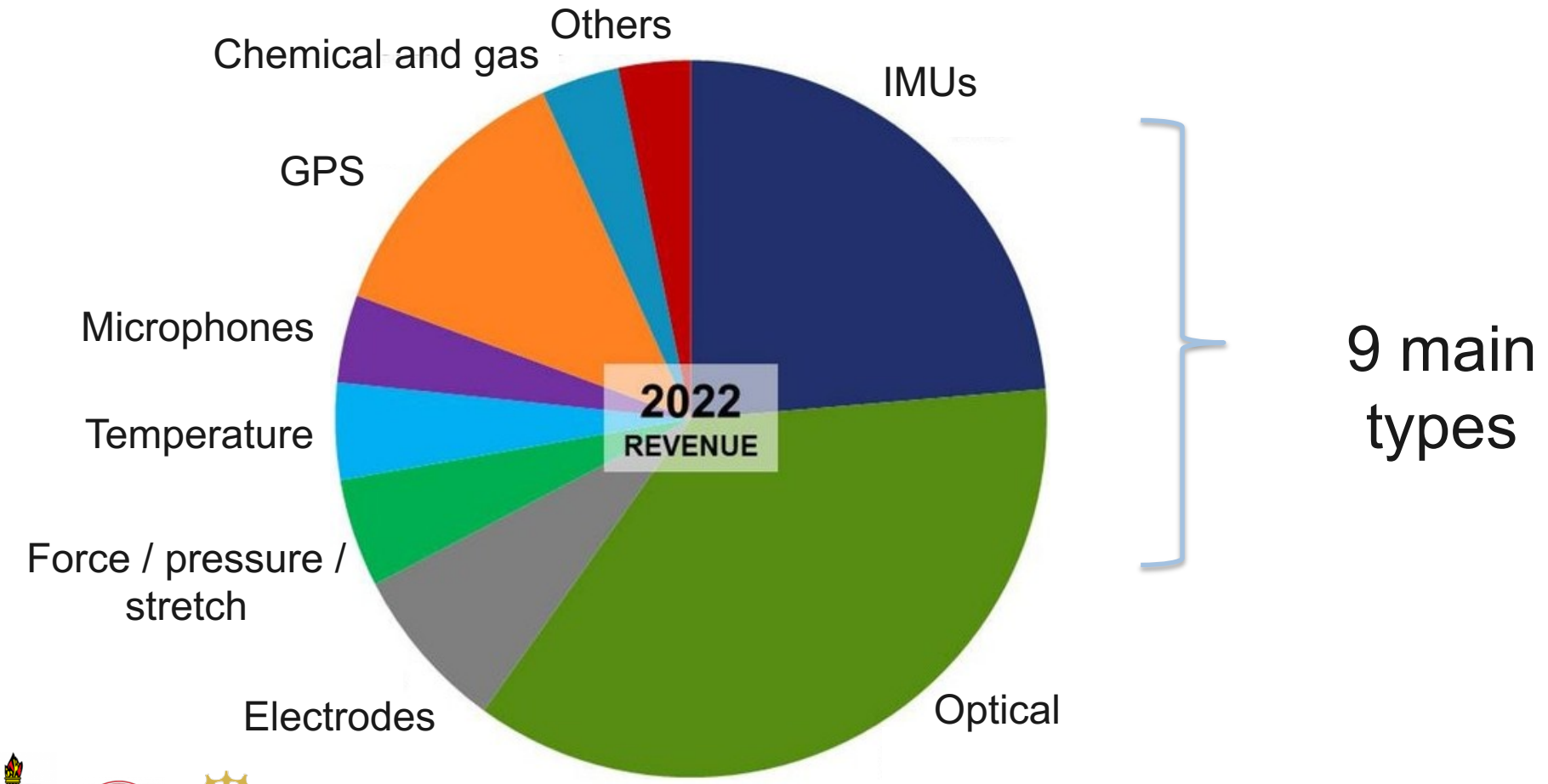


Home-connected medical monitoring devices
(World from 2015 to 2021)

Source: MobiHealthNews, 2017

Introduction

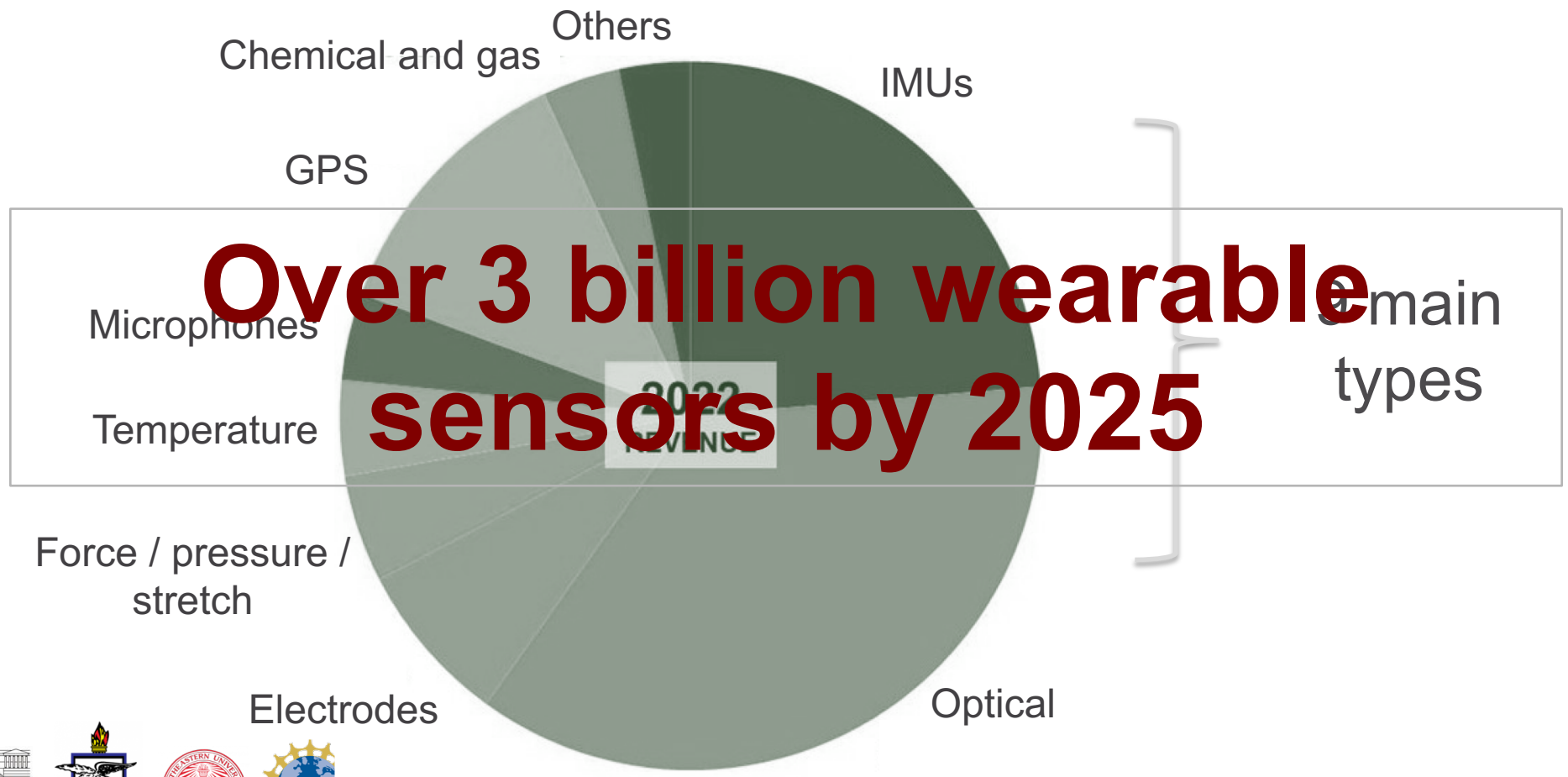
Over 42 different types of wearable sensors



Source: IDTechEx, 2017

Introduction

Over 42 different types of wearable sensors



Over 3 billion wearable sensors by 2025

Source: IDTechEx, 2017

Problem

User's vital physiological data privacy

Increase attack vectors!

New attack vectors!

(e.g. intrusive and data leakages)

Secure transmission sensed data through wearable sensors

Problem

Wearable Sensors

Sensitive data

Resource constraints
(e.g. computationally)

Software and hardware security vulnerabilities

These three factors make wearable sensors a target of new attack vectors

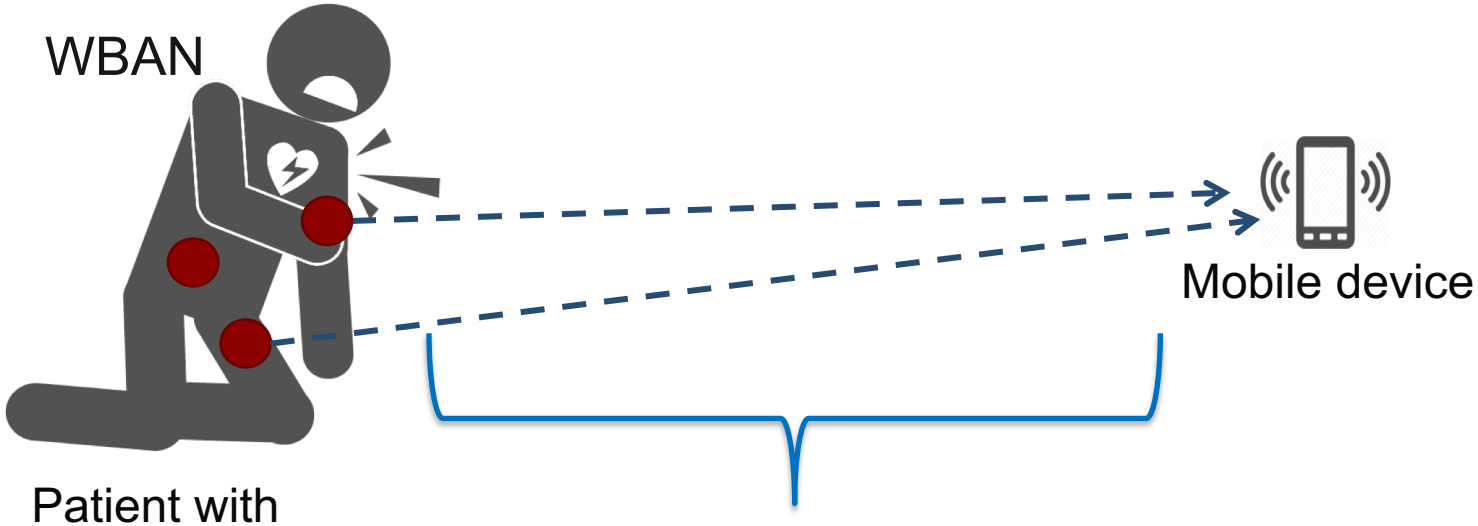
Attack Vector

- Leakage of private information
- Cross-layer fingerprinting
  - Fingerprint some radio
  - Cross-layer information
    - Possibility to calculate operational bandwidth and link layer rates

Attack Vector
Cross-layer fingerprinting

HealthSense project

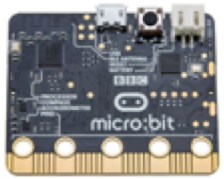
- **Communication with mobile device**



It is easy identify the device and the wireless model

Attacks On Apple Wireless Direct Link (AWDL)

HealthSense project



- Apple Wireless Direct Link (AWDL) based on Wi-Fi ad hoc mode
  - AWDL is widely used (over billion iOS, macOS, tvOS, watchOS devices)
  - Device-to-device services e.g., Apple AirDrop, and by Apple Watch & TV
  - Services rely on a combination of AWDL and Bluetooth LE
- Design and implementation flaws [Stute et al. 2019]
  - Attacks without connecting to the same network
  - Expose users' long-term information
    - Real MAC address, device owner names, etc.
    - Enables efficient tracking
  - Denial of service attack
    - Targeted crashing
    - Simultaneously crash (blackout)
  - Man-in-the-middle AirDrop file transfers, intercept and modify
- Disclosed to Apple, released fix to DoS [November 2018]
- Beyond Apple ecosystem: Wi-Fi Neighbor Awareness Networking (NAN), Google Android NAN

RNP UFPR 100 Anos 1912 - 2012 NSF

HealthSense Framework

How can we improve

security and **privacy**

in the transmission of user's data?

HealthSense Framework

- **Two-fold approach:**

  1. Assessing privacy intrusion and attack vectors

  Objective: Analyze and explore characteristics of wearable devices, Apps and network stacks.

HealthSense Framework

- **Two-fold approach:**

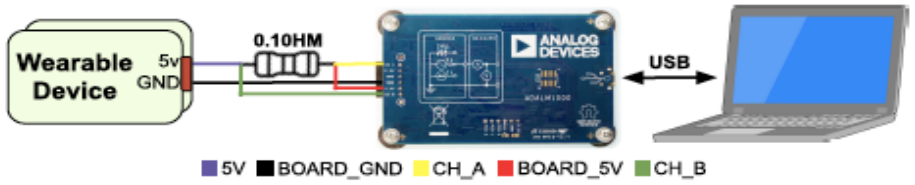
  2. Privacy protection

Objective: A side channel using the body's own conducting medium to protect the transmission of the secret information.

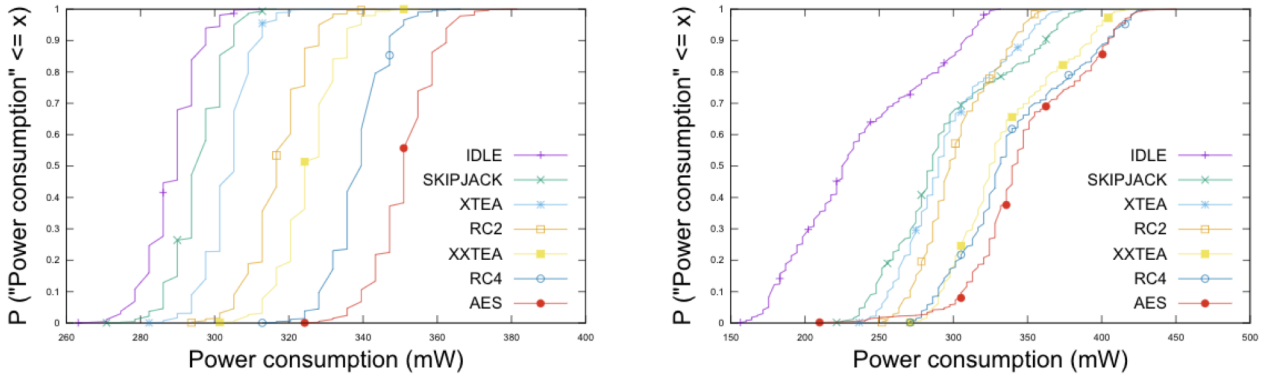
Assessing privacy and intrusion

HealthSense project

- Empirical analysis of cryptographic algorithms in wearable communication
  - Real implementation
  - Block and stream ciphers
  - Different metrics
    - Memory and energy consumption
    - Security
  - AES, the best in security, but it still requires improvements



ALGORITHM	COMPLEXITY	MEMORY CONSUMPTION (BYTES)			
		Shimmer 2R		Teensy 3.2	
		ROM	RAM	ROM	RAM
SKIPJACK	$O(1)$	6,834	608	13,892	4,584
XTEA	$O(1)$	6,772	612	13,360	4,620
RC2	$O(1)$	6,786	726	14,028	4,828
XXTEA	$O(n)$	7,064	604	13,456	4,556
RC4	$O(n)$	6,994	604	13,348	4,556
AES	$O(1)$	24,068	1,978	14,048	4,812



(a) Power consumption per state Teensy 3.2 (b) Power consumption per state Shimmer 2R

Figure 3: Power consumption in milliwatts on the *run* state

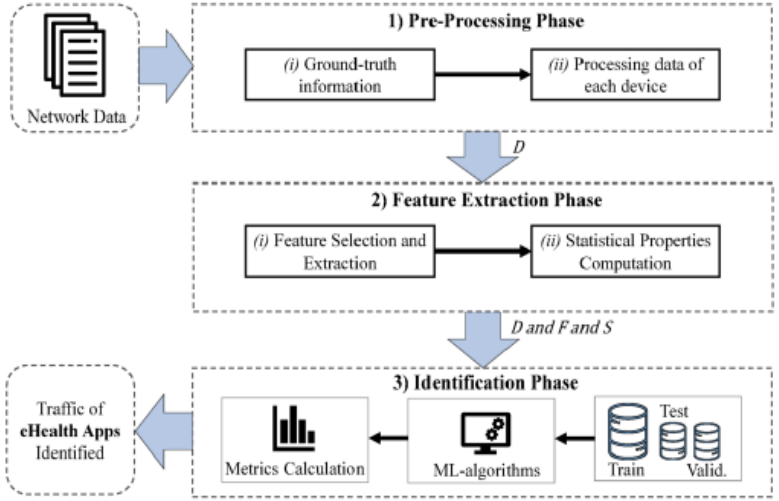
Assessing privacy and intrusion

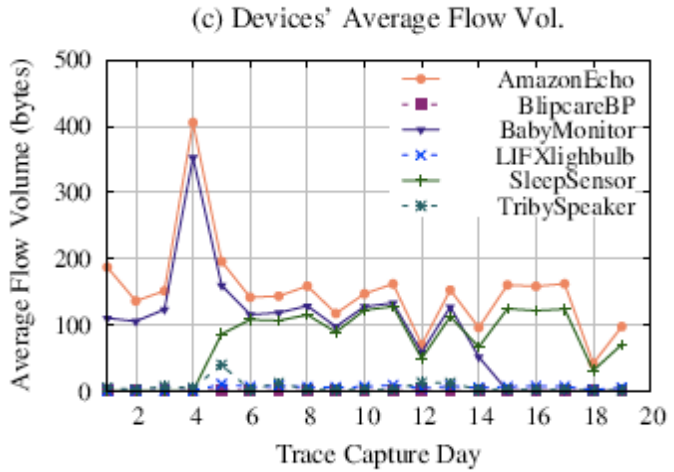
On going empirical investigations

HealthSense project

- A. Vergutz, I. Medeiros, D. Rosario, E. Cerqueira, A. Santos, M. Nogueira. A Method for Identifying eHealth Applications using Side-Channel Information. IEEE GLOBECOM 2019 (to appear)

- P. Resque, S. Costa, D. Rosário, E. Ceruqueira, A. Vergutz, A. Santos, M. Nogueira. Assessing Data Traffic Classification to Priority Access for Wireless Healthcare Application. IEEE LATINCOM 2019 (to appear).





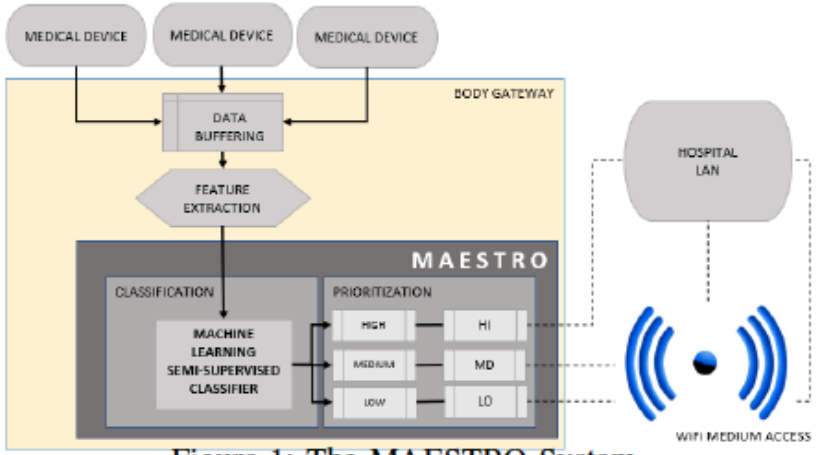


Figure 1: The MAESTRO System

HealthSense Framework

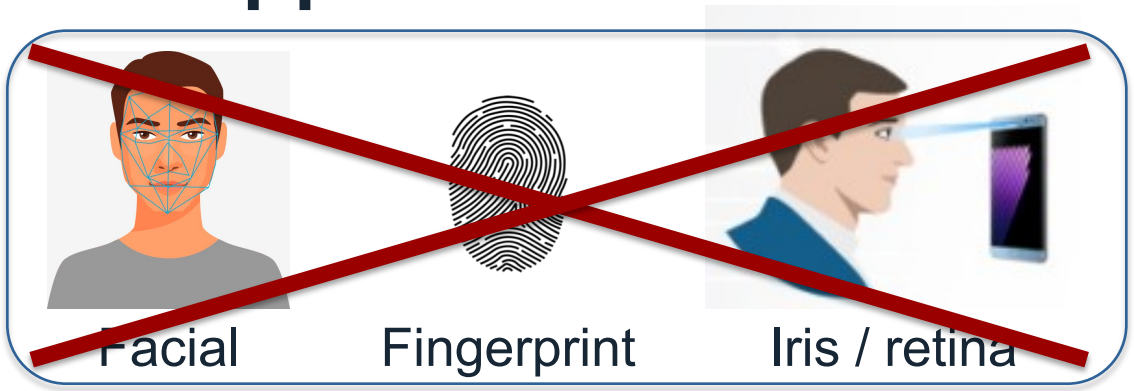
Privacy Protection

A side channel using the body's own conducting medium to protect the transmission of the secret information

Privacy Protection
Unique Biomarkers

HealthSense project

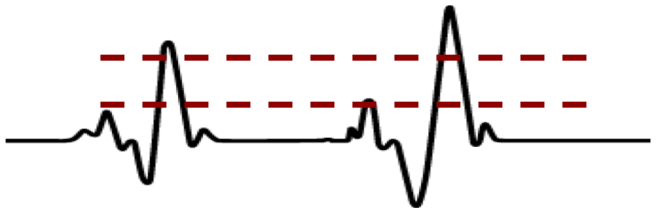
- Exchange patient-physician information
  - Biometric applications



Common target for spoofing

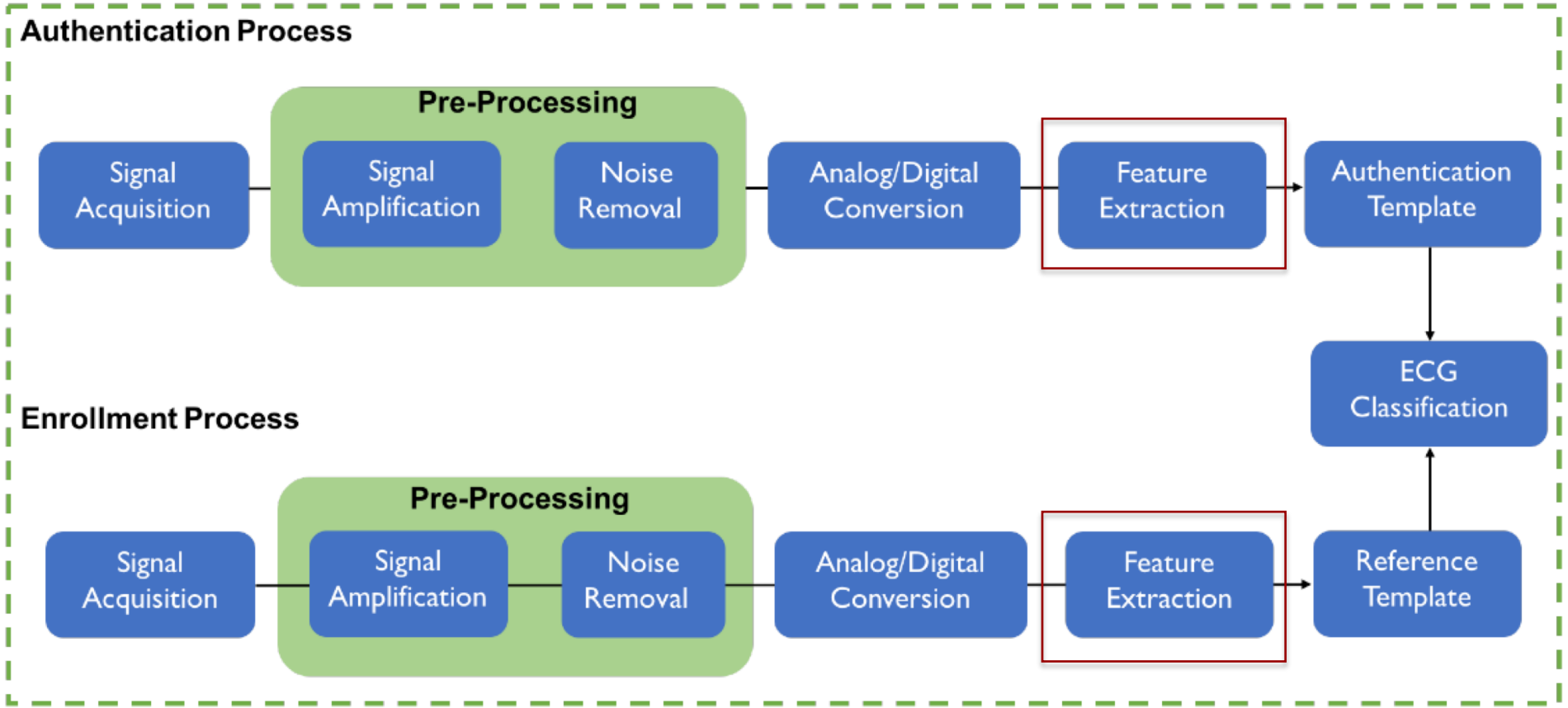
  - Body's naturally generated bioelectrical signals

E.g.: ECG, EMG and PPG signals



Unique Biomarkers

Typical ECG authentication system



Unique Biomarkers

- Feature extraction from an ECG signal to identify **levels of uniqueness**:
  - ECG temporal features (*Fiducial*)
  - ECG frequency domain features (*Non-fiducial*)
  - Both ECG features (*Hybrid*)
  - Signal classification through machine learning
    - E.g.: neural networks and K-NN

Unique Biomarkers

HealthSense project

- Accuracies from literature:
  - Fiducial classification presented 99.2%
  - Non-fiducial classification shown 98.8%
  - K-NN classification presented 96.76%

Wearable sensors have resource constraints, so low complexity classification is needed!

Recent trends: joint **ECG** and **EMG**

Now, we investigate **PPG**

Unique Biomarkers

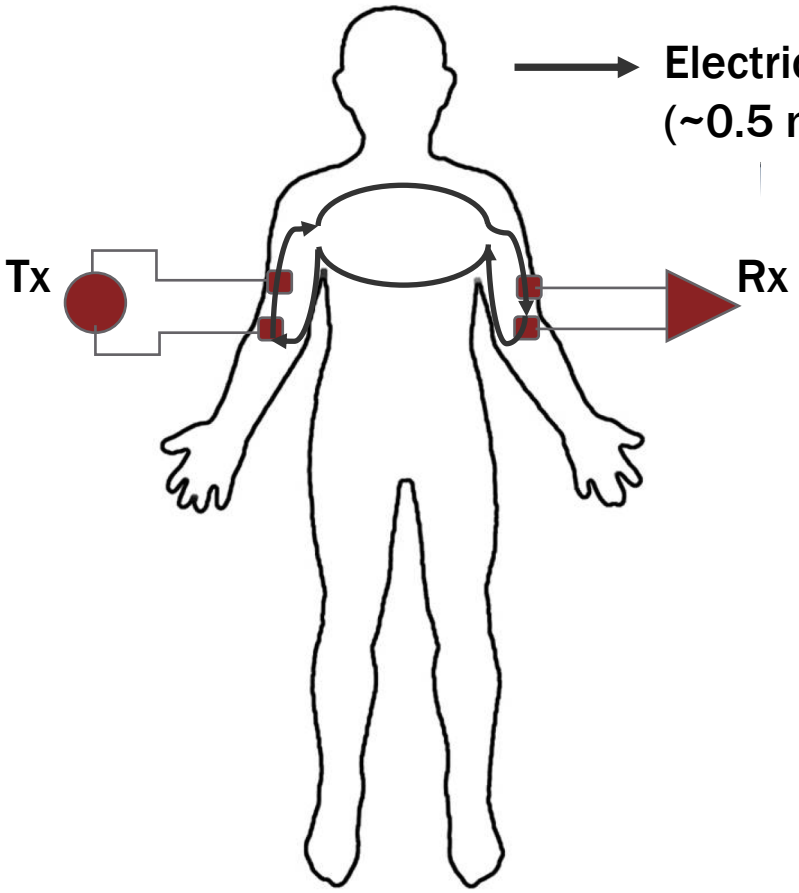
HealthSense project

HealthSense Framework:

Examine and implement PPG extraction algorithms for joint ECG signal

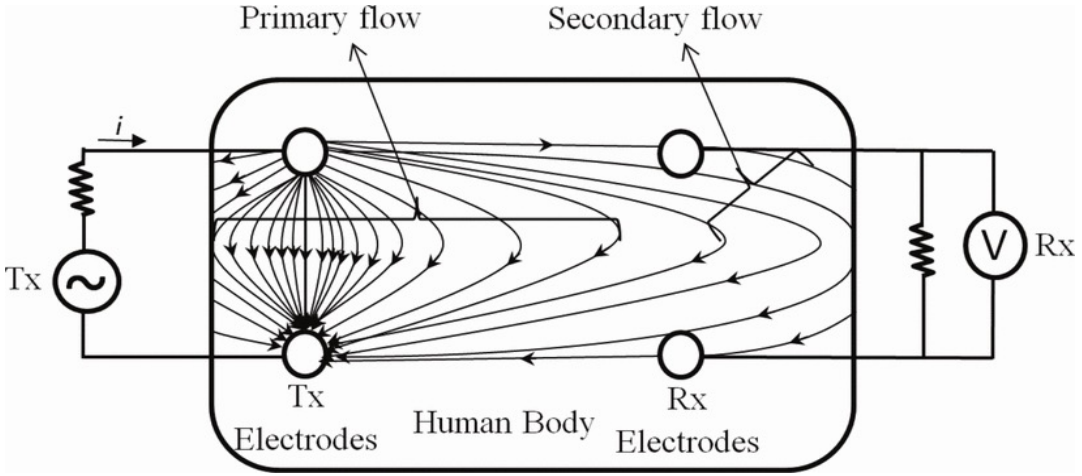
Sensing and Communication

Galvanic coupling



In galvanic coupled IBC, an electrical signal is applied differentially between the two electrodes of the transmitter

- Sensitive to body locations due to the dependence on inter-electrode distance and orientation along the body



- Secondary path of propagation is used for potential difference detection at Rx

Sensing and Communication

Galvanic coupling

HealthSense project

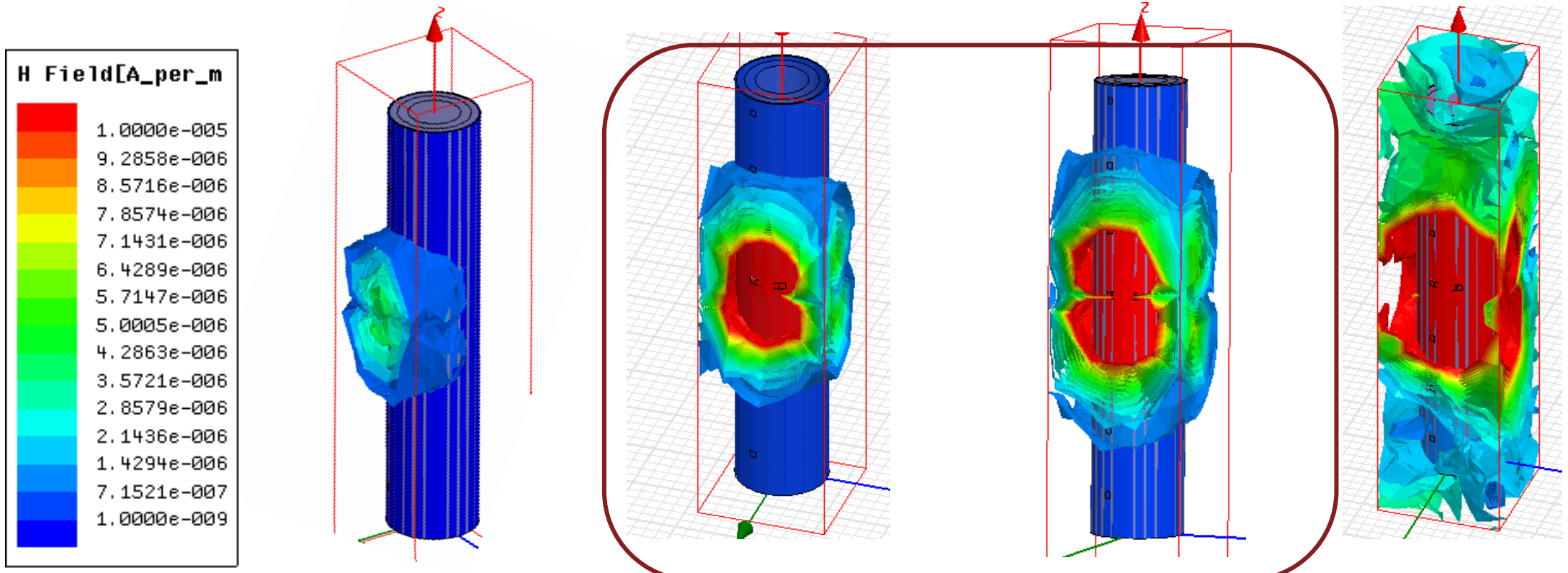
- An alternative to over-the-air radio frequency communication
- Energy efficient
- Signals cannot be eavesdropped
- Data transfer through the human tissues

Sensing and Communication

Galvanic coupling

HealthSense project

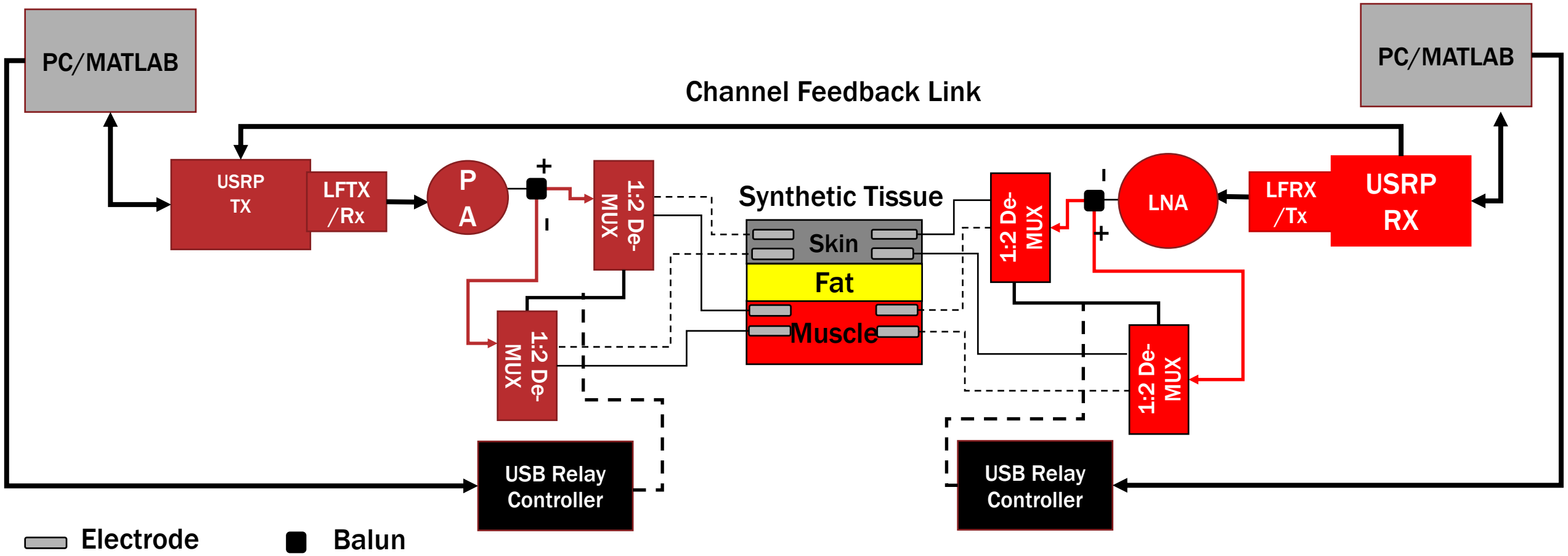
Limit signal “leakage” from the body, prevents sniffing attacks



← Frequency →

Sensing and Communication

Galvanic coupling



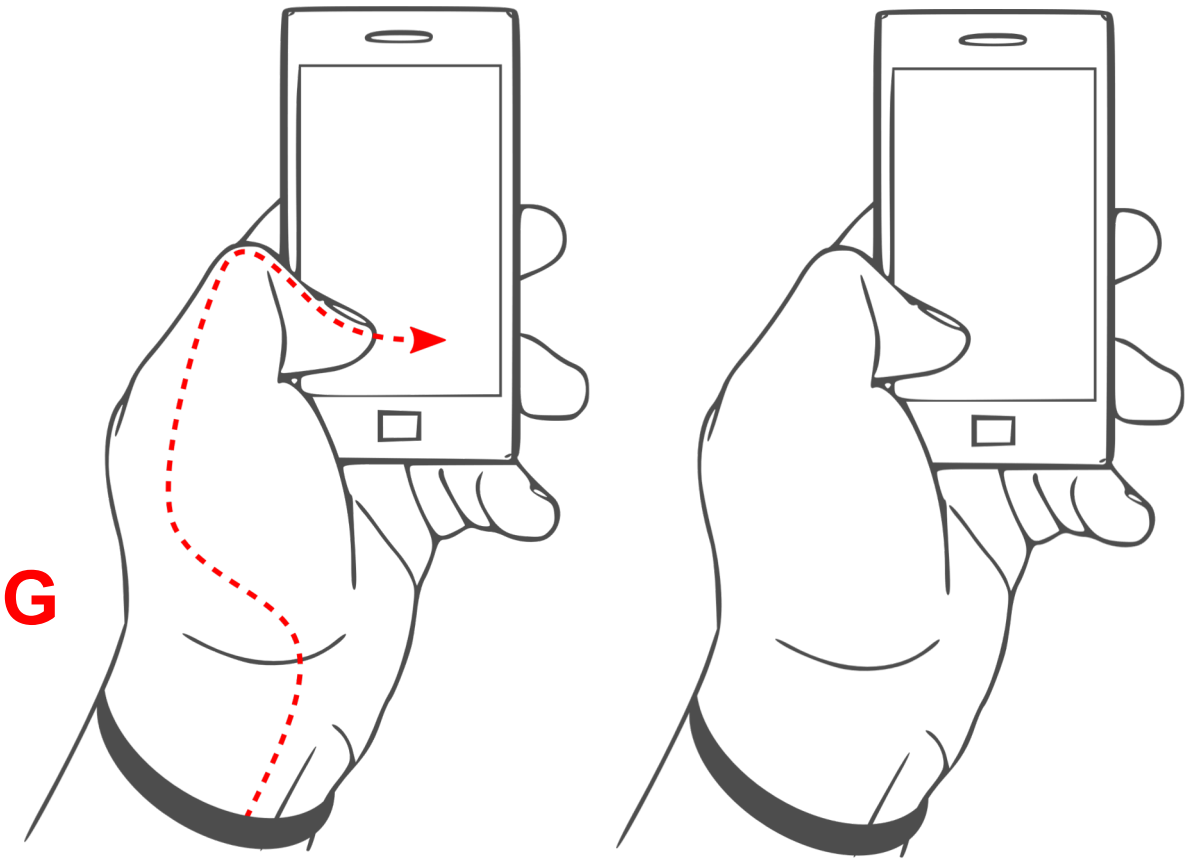
US-Brazil Galvanic Coupled Communication Testbed

Sensing and Communication
Proposed system

HealthSense project

- Wristband with ECG/PPG sensing capabilities
- Smart phone with pair of electrodes integrated

ECG and PPG signals



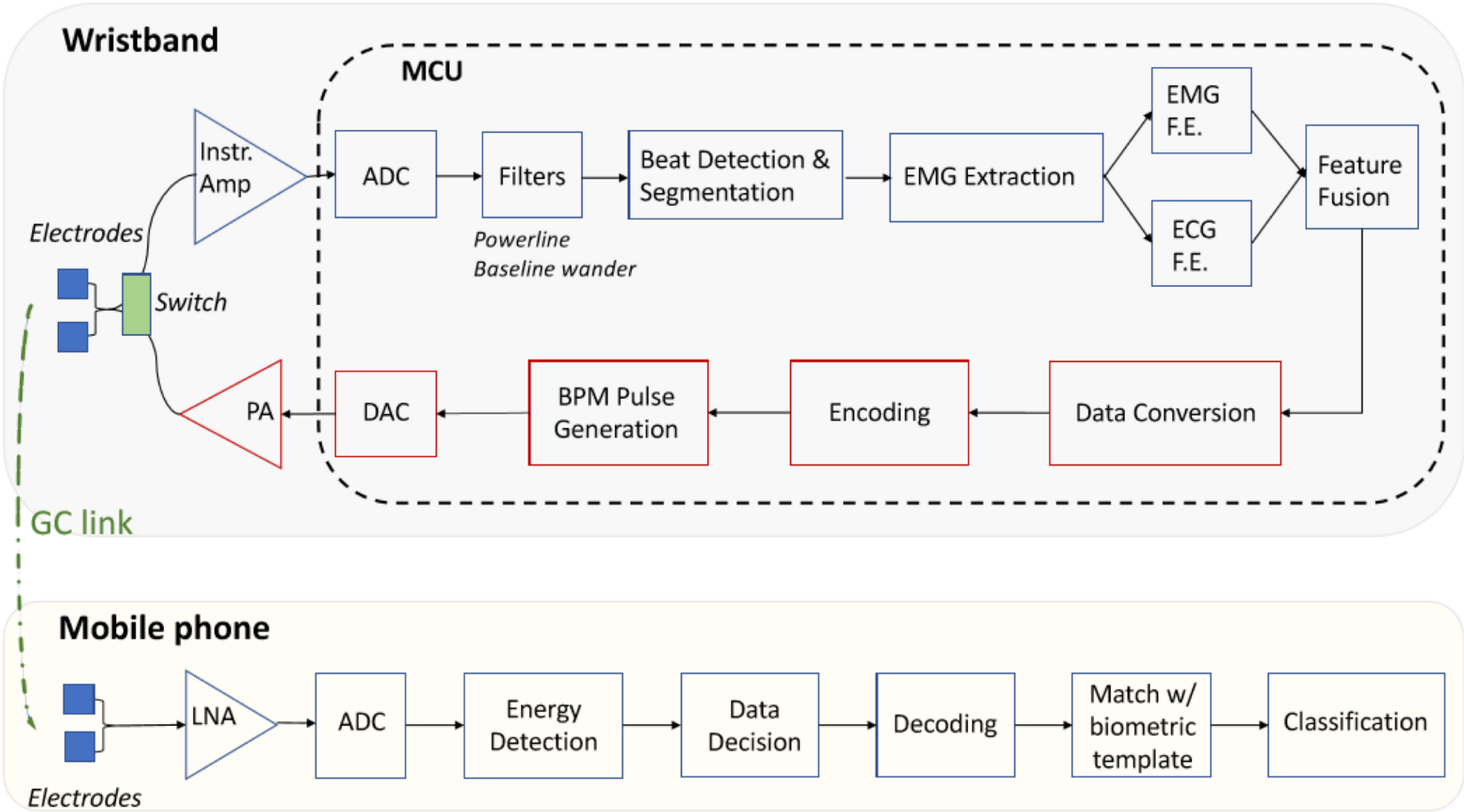
Sensing and Communication
Bio-authentication

HealthSense project

- Enables a secure transfer of the biometric information
- A unique “code” based on the biometric features of the ECG and PPG signals
- Replaces the use of the fingerprint sensor

Sensing and Communication

System design



Sensing and Communication
System design

HealthSense project

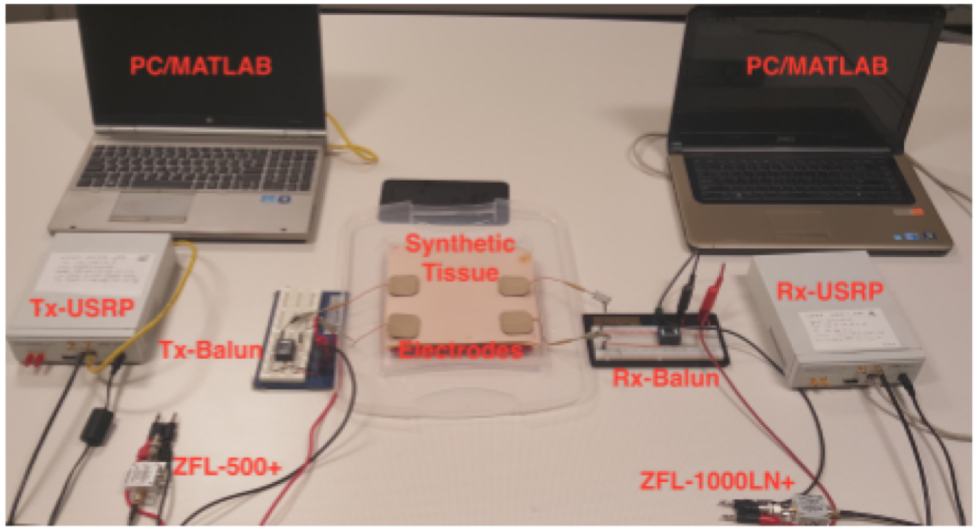
- Biometric acquisition and analysis mode
  - Collects the ECG/PPG signal
  - Extracts the features
  - Transmission mode
  - Communicates the unique features to the phone

Sensing and Communication

Bio-authentication testbed

HealthSense project

- Software Defined Radio platform
- Communication link to propagate data across a synthetic tissue phantom



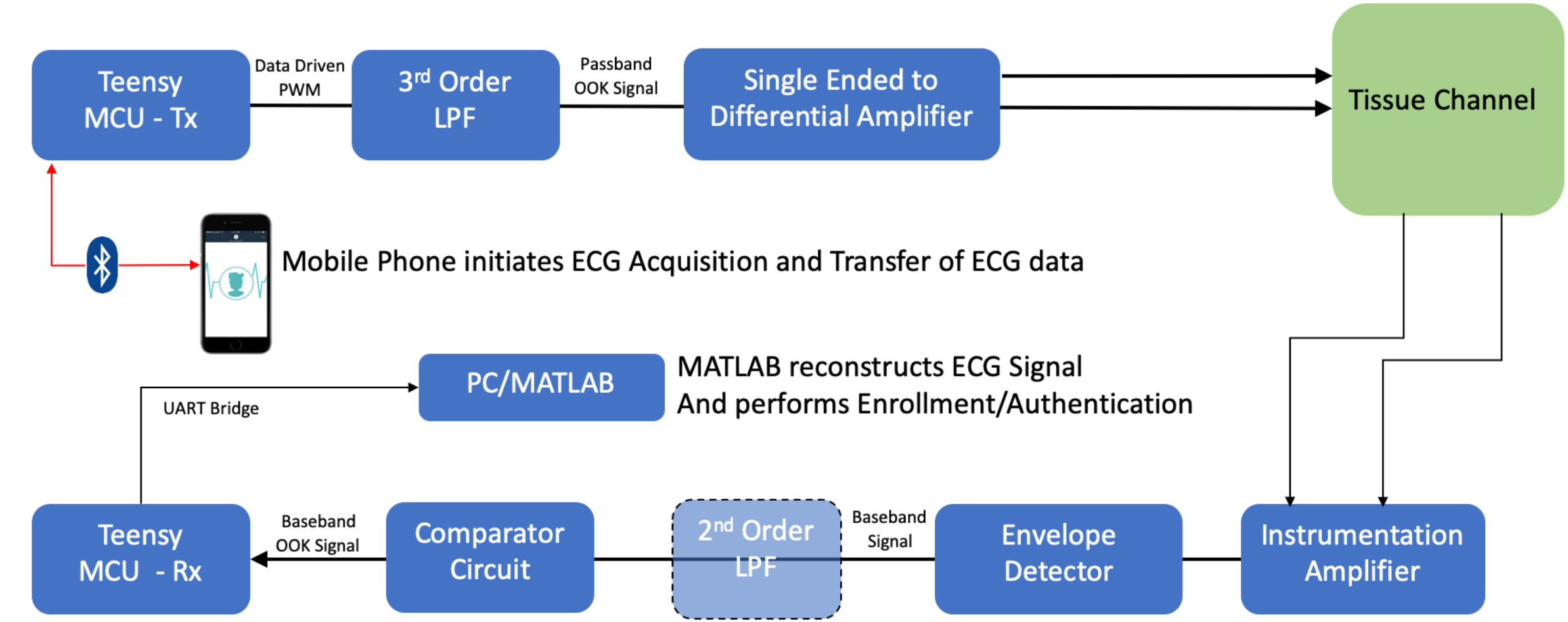
Choice of OOK

HealthSense project

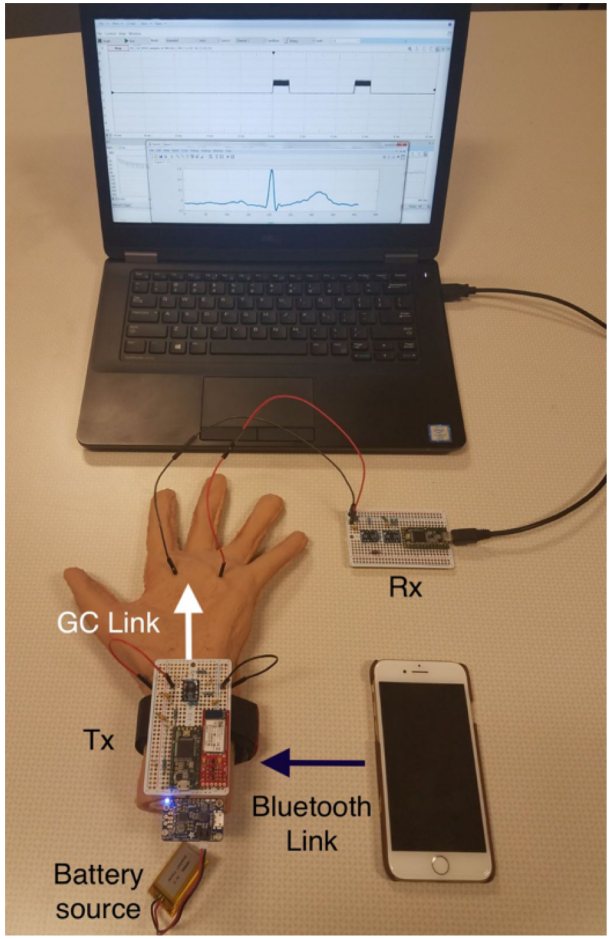
System Architecture	Occupied Bandwidth	Minimum Tx Power	Max Bit rate	Energy Consumption	Modulation Order (M)
BFSK	209.5 kHz	-8 dBm	50 kbps	590μJ	2
BPSK	52.3 kHz	-13 dBm	50 kbps	2.75 mJ	2
OOK	52.57 kHz	-9 dBm	50 kbps	158.2μJ	2

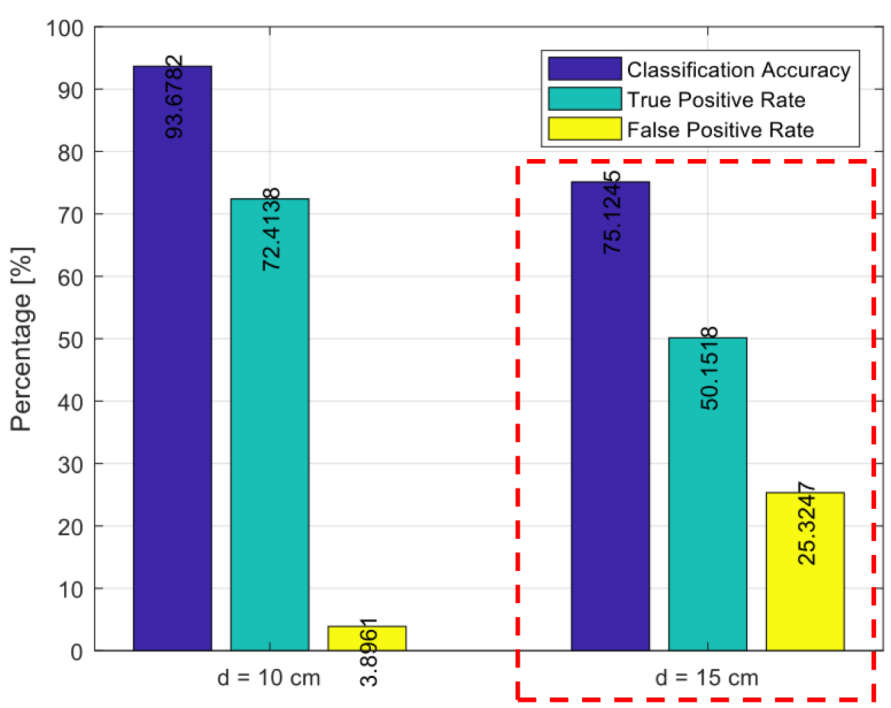
Link Distance: 10 cm
Tissue Layer Communication Scenario:
Skin to Skin
Target BER: 10e-4

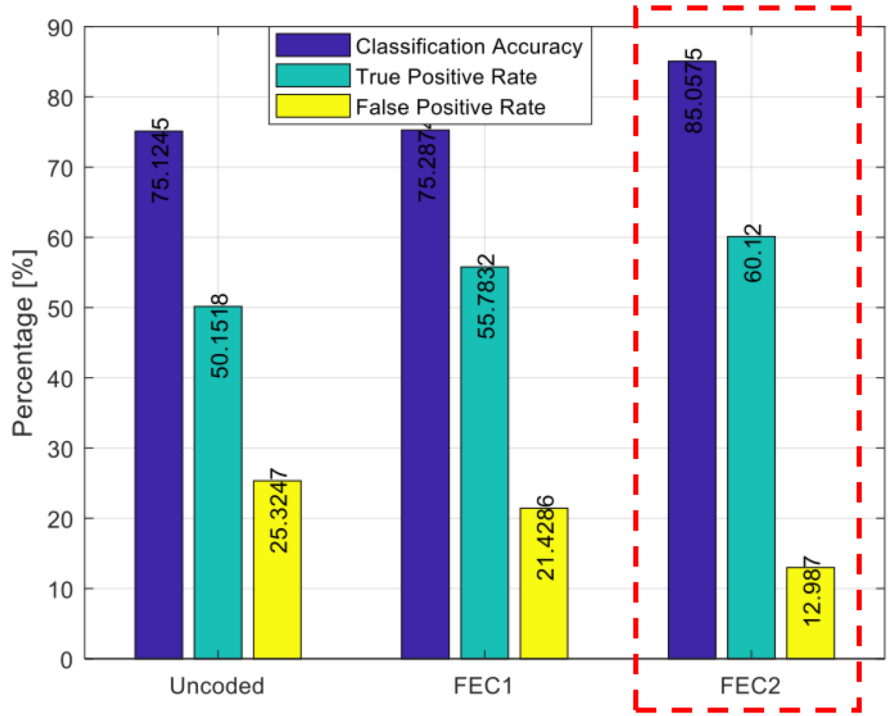
Phone Authentication



Results

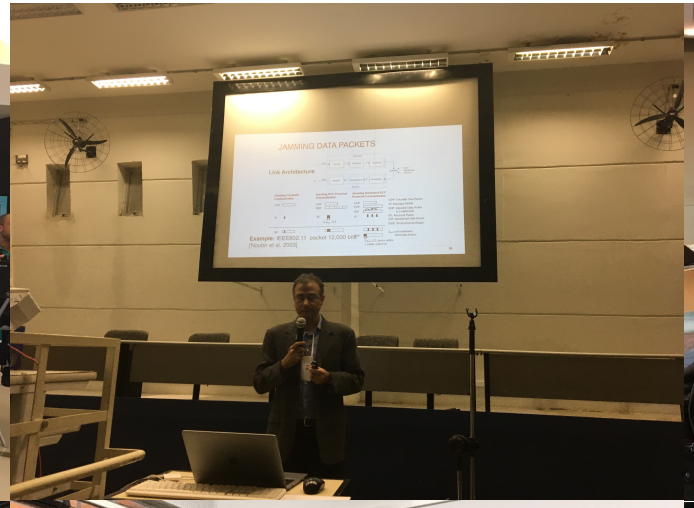

GC Link
Rx
Tx
Bluetooth
Link
Battery
source


Classification Accuracy
True Positive Rate
False Positive Rate
Percentage [%]
100
90
80
70
60
50
40
30
20
10
0
93.6782
72.4138
3.8961
75.1245
50.1518
25.3247
d = 10 cm
d = 15 cm


Classification Accuracy
True Positive Rate
False Positive Rate
Percentage [%]
90
80
70
60
50
40
30
20
10
0
75.1245
50.1518
25.3247
75.2874
55.7832
21.4286
85.0575
60.12
12.987
Uncoded
FEC1
FEC2

Team work

HealthSense project

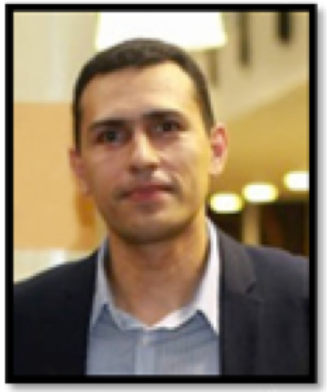


RNP UFPR 100 Anos 1912 - 2012 UNIVERSIDADE FEDERAL DO PARÁ NORTHEASTERN UNIVERSITY BOSTON, MASSACHUSETTS NSF

Researchers

HealthSense project

Brazil | **U.S.**




Prof. Santos and Prof. Nogueira - UFPR

Prof. Noubir - NU

Computer Science

Prof. Cerqueira - UFPA

Prof. Chowdhury - NU

Electrical and Computer Engineering

RNP UFPR 100 Anos 1912 - 2012 Universidade Federal do Pará Northeastern University NSF

Curitiba


VENEZUELA
Georgetown
Bogota
Paramaribo
GUIANA
Guyane (France)
COLOMBIA
SURINAM
BRAZIL
Lima
Brasilia
PERU
BOLIVIA
La Paz
PACIFIC
OCEAN
Rio de Janeiro
PARAGUAY
Curitiba
São Paulo
Asunción
CHILE
ARGENTINA
ATLANTIC
OCEAN
URUGUAY
Santiago
Montevideo
Buenos Aires
0
1 000 km


Saída


UFPR | CICLO BÁSICO
#SOUMEDICINA
MEDGRUPO

The Fourth Industrial Revolution

HealthSense project

"Ubiquitous, mobile supercomputing. Intelligent robots. Self-driving cars. Neuro-technological brain enhancements. Genetic editing. The evidence of dramatic change is all around us and it's happening at exponential speed."

(Klaus Schwab, the founder of the world economic forum)

HealthSense project

www.healthsenseproject.net

michele.nogueira@ufpr.br

RNP UFPR 100 Anos 1912 - 2012 NSF