# Know Me by My Pulse: Toward Practical Continuous Authentication on Wearable Devices via Wrist-Worn PPG

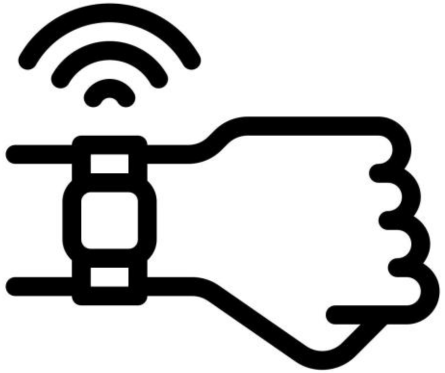
**Wei Shao**, Zequan Liang, Ruoyu Zhang, Ruijie Fang, Ning Miao, Ehsan Kourkchi,
Setareh Rafatirad, Houman Homayoun, and Chongzhou Fang

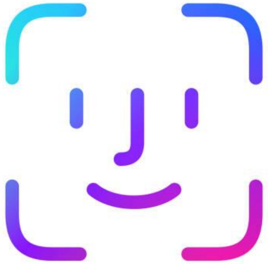
UCDAVIS
UNIVERSITY OF CALIFORNIA

RIT Rochester Institute of Technology

# Wearables Authenticate Once — Then Trust Forever

- Smartwatches store health, messages, payment data
- Typically authenticate once (PIN / phone unlock)
- Remain trusted afterward
- **If stolen or removed, access persists**





**Wearables lack secure continuous authentication.**

# Why Is Continuous Authentication Hard on Wearables?

**Constraints of Wearables:**

- Limited battery capacity
- Limited computation capability
- Limited sensing modalities

**Existing Approaches Fall Short:**

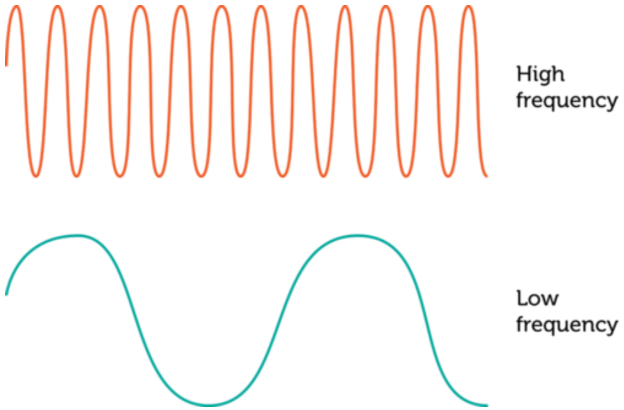
- Behavioral biometrics → context-dependent
- ECG → requires special hardware
- High-frequency PPG (100–500 Hz) → high energy cost

**We need a low-power, robust biometric already embedded in commercial wearables.**

# Key Insight: Low-Rate Multi-Channel PPG Is Enough

**Observation:**

- PPG is already embedded in all commercial smartwatches
- Prior work assumes high sampling rates (75–500 Hz)
- High sampling rate → high energy cost



**Our Hypothesis:**

- 25 Hz PPG is sufficient for biometric authentication
- Multi-channel PPG improves robustness
- Proper modeling compensates for lower resolution

**Low-frequency, multi-channel PPG enables practical continuous authentication.**

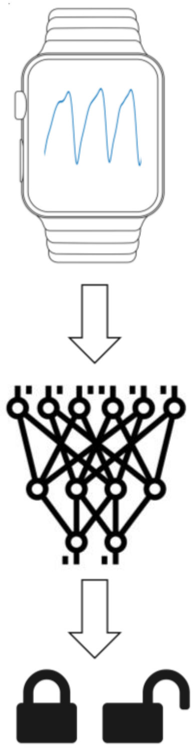
# System Overview: Continuous PPG Authentication Pipeline

**Data Collection:**

- Wrist-based multi-channel PPG
- 25 Hz sampling
- Continuous streaming

**Preprocessing:**

- Bandpass filtering
- 4s windows with 50% overlap
- Normalization



**Model:**

- BiLSTM + Attention
- Transformer (comparison)
- Class-weighted loss to address class imbalance

**Decision Logic:**

- Sliding window authentication
- Threshold-based acceptance
- Continuous identity verification

**Lightweight signal processing + sequence modeling → real-time continuous authentication**

# Research Questions

**We investigate multiple research questions, here summarized into three themes:**

- **RQ1 — Is low-frequency PPG sufficient?**
  - Compare 25 Hz vs 100–500 Hz
  - Compare single- vs multi-channel
  - Accuracy, EER, FAR/FRR
- **RQ2 — Is the system practical for real deployment?**
  - Continuous authentication performance
  - Robustness across sessions
  - Realistic user scenarios
- **RQ3 — How much energy can we save?**
  - Power consumption vs sampling rate
  - Wearable battery implications

**Can we make continuous authentication both secure and practical?**

# Datasets & Experimental Setup

## Datasets

- **We-Be Dataset (real-world, non-laboratory)**
  - 26 subjects
  - 4-channel wrist PPG
  - 25 Hz sampling
  - Multiple sessions
  - Collected across natural daily activities
- **PTTPPG (public)**
  - High-frequency PPG (512 Hz)
  - Used for sampling-rate comparison

## Evaluation Protocol

- Subject-disjoint train/test splits
- Cross-session evaluation
- Continuous authentication simulation
- Metrics: Accuracy, Macro-F1, FAR, FRR, EER

# RQ1 — Is 25 Hz PPG Sufficient?

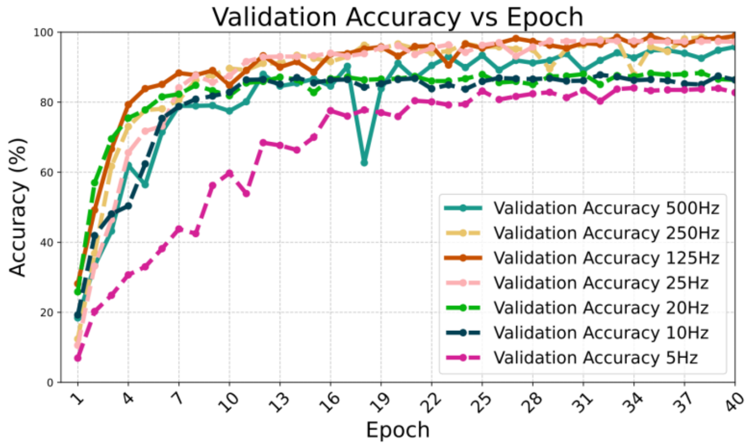
## Comparison:

- Sampling rate from 5 to 512 Hz
- Single- vs multi-channel signals

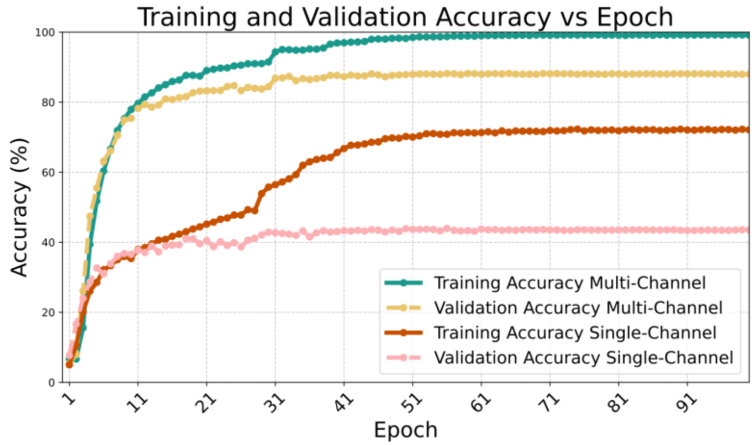
## Key Results:

- Multi-channel 25 Hz achieves comparable accuracy and remains stable
  - Average Test Accuracy: **88.11%**
  - EER: **2.76%**
- Performance Drops significantly below 25 Hz

**Low-frequency PPG preserves authentication performance.**



Validation Accuracy vs Epoch

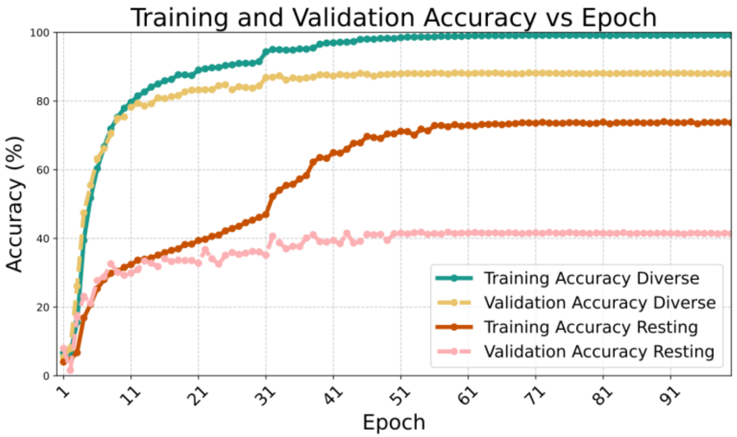


Training and Validation Accuracy vs Epoch

# RQ2 — Is the System Practical for Real Deployment?

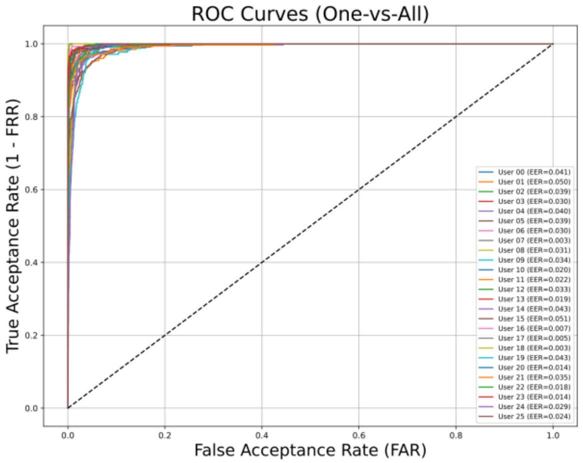
**Evaluation Focus:**

- Cross-session generalization
- Continuous sliding-window authentication
- Real-world activity data



**Key Findings:**

- Stable performance across sessions
- Low False Acceptance Rate (0.48%)
- Acceptable False Rejection Rate (11.77%)
- Activity diversity during training is essential for robustness

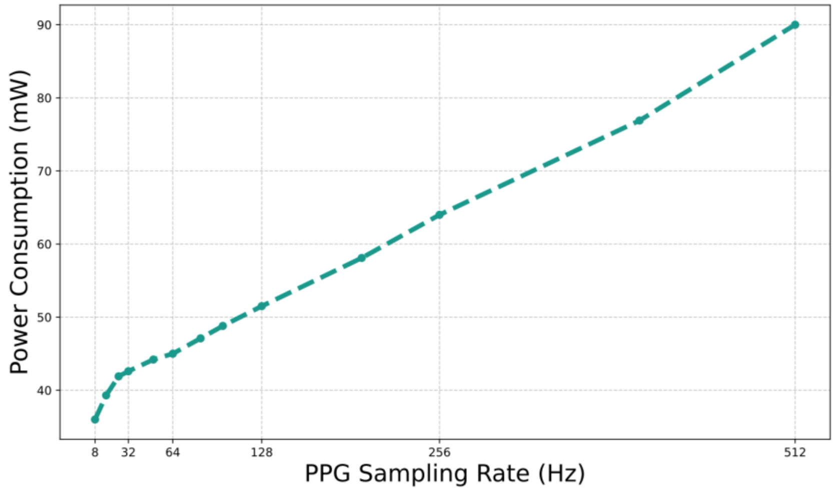


**Low-rate multi-channel PPG supports stable, real-world continuous authentication.**

# RQ3 — How Much Energy Can We Save?

## Power Consumption vs Sampling Rate:

- Measured sensor power on We-Be smartwatch
- 8 to 512 Hz



## Key Results:

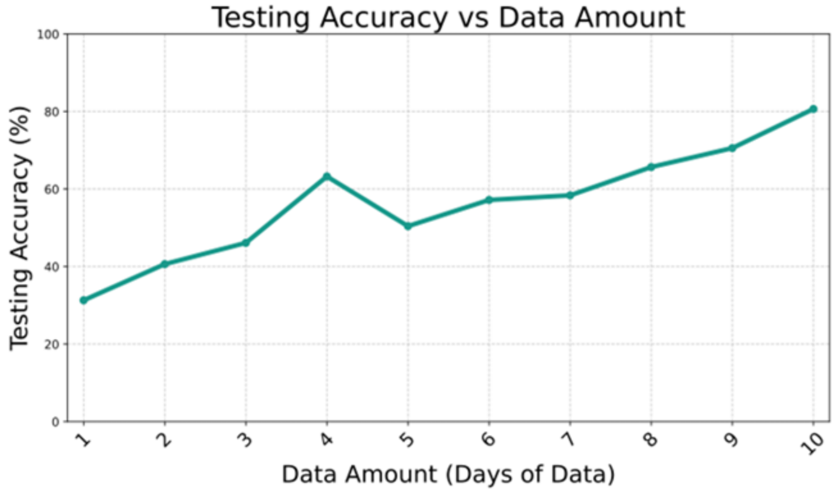
- 25 Hz reduces power by:
  - **53% vs 512 Hz**
  - **19% vs 128 Hz**
- Further reduction to 20 Hz gives only marginal additional savings but performance drops sharply
- 25 Hz is the practical sweet spot

**Low-frequency PPG enables secure authentication without draining battery life.**

# Long-Term Continuous Authentication Stability

## Evaluation Setup

- Multi-session data collected over time
- Cross-session generalization
- Sliding-window continuous authentication



## Findings

- Identity performance remains stable across sessions
- No catastrophic degradation over time
- Activity-diverse training improves long-term robustness

**Authentication remains stable beyond single-session evaluation.**

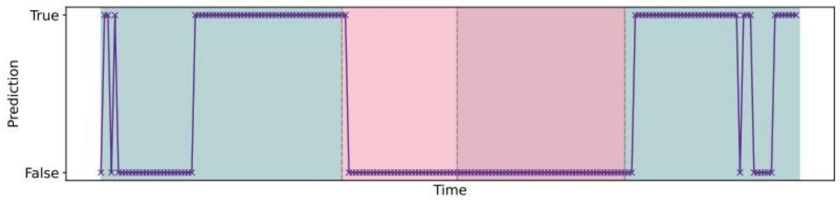
# Real-Time Deployment on Smartwatch

## Implementation

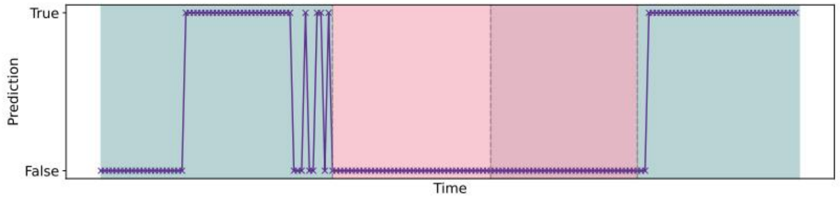
- Deployed on We-Be smartwatch
- On-device 25 Hz multi-channel PPG collection
- Real-time sliding-window inference
- BiLSTM + Attention model

## System Behavior

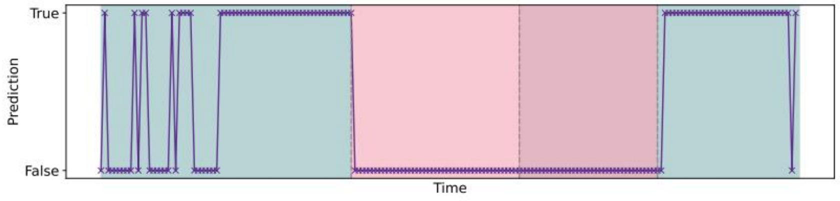
- Continuous authentication decisions
- Real-time score updates
- No user interruption
- Imposters consistently rejected (<5s).



(b) User 1, with a sliding-window filter applied.



(d) User 2, with a sliding-window filter applied.



(f) User 3, with a sliding-window filter applied.

**End-to-end continuous authentication runs in real time on wearable hardware.**

# Takeaways & Contributions

- Low-Frequency (25 Hz) PPG Is Sufficient for Continuous Authentication
- Multi-Channel Modeling Enables Cross-Session Robustness
- Energy-Efficient, Real-Time Deployment on Commodity Smartwatches

**Secure, practical continuous authentication is achievable on commodity smartwatches.**

# Thank You!

Q&A