A Usable Authentication System Using Wrist-worn Photoplethysmography Sensors on Smartwatches

Jiacheng Shang and Jie Wu

Center for Networked Computing

Dept. of Computer and Info. Sciences

Temple University

Smartwatches & Threats

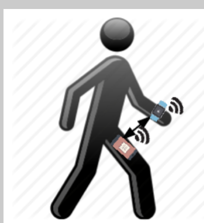
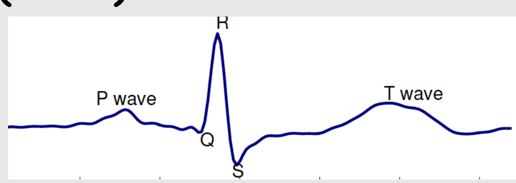
- Smartwatches
  - Potentially more fashionable
  - More immediate
  - Allowing users to stay better engaged with the environment
  - Rich features: various sensors, powerful CPU

- Apple Watch
- Samsung Gear
- Fitbit

Smartwatches & Threats

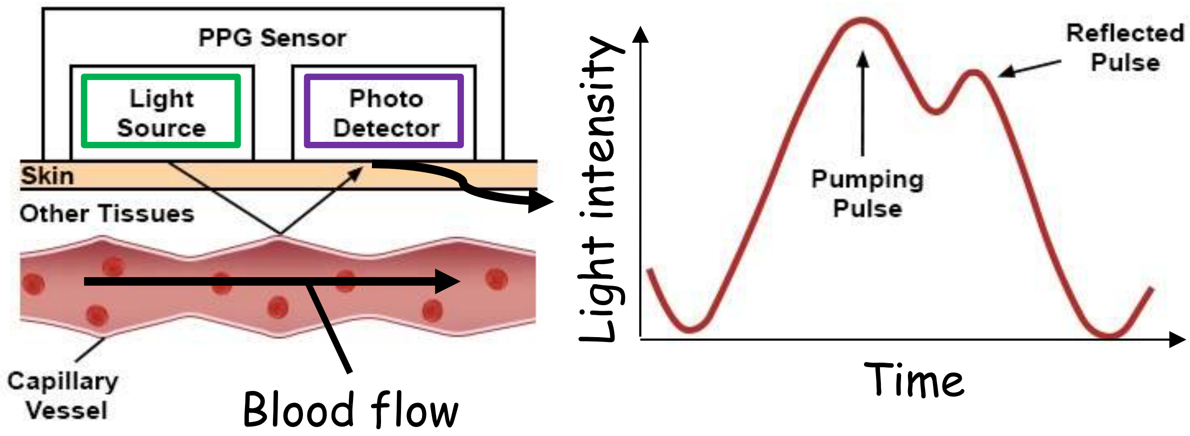
- Threats:
  - Collecting personal information (name, messages, emails,…)
  - The data on smartwatches is not well protected
  - Only a few devices provide simple authentication

Existing Solutions

Solutions	Limitations
PIN or pattern	• Brute force and shoulder surfing attacks
Voiceprint	• Replay attack
Motion 	• Low randomness • Cannot work if the user is not performing pre-defined activities A. Johnston "Smartwatch-based biometric gait recognition" BTAS 2015
Electrocardiogram (ECG) 	• Not available on existing smartwatches S. Chun "ECG based user authentication for wearable devices using short time Fourier transform" TSP 2016

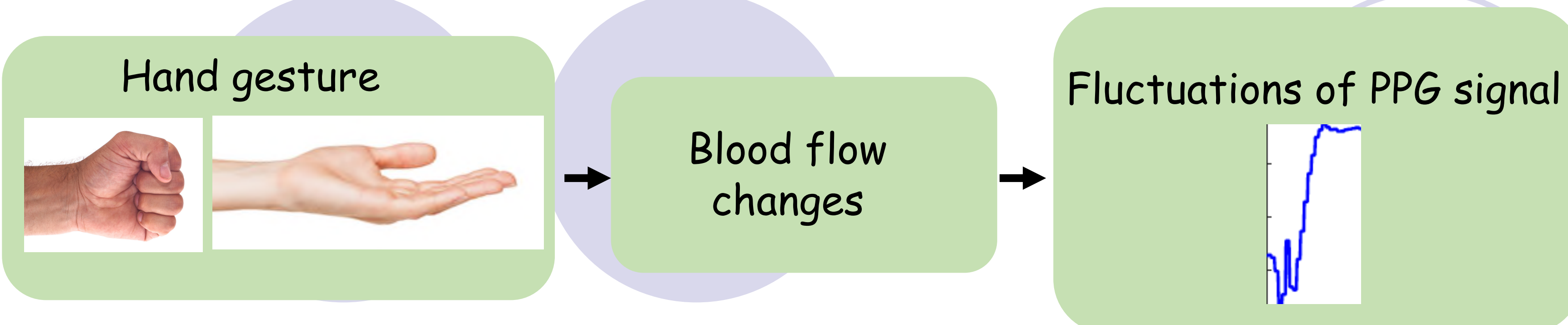
Basic Ideas

- Leveraging Photoplethysmography (PPG) signals influenced by hand gestures
  - Consisting of a light source (green light) and a photo detector
  - PPG sensor is available on smartwatches
  - used to monitor the blood flow by measuring the intensity of reflected light.



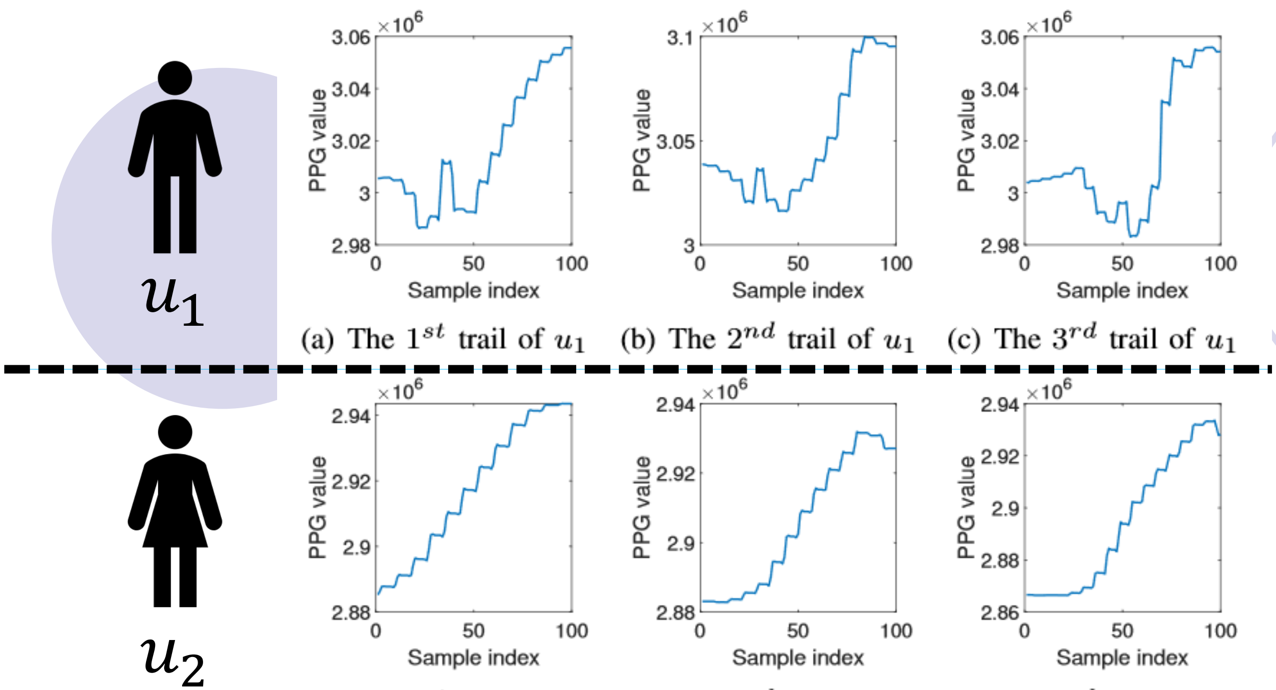
Basic Ideas

- Muscle and tendon movements change the blood flow
- Change of blood flow influences the intensity of reflected light



Basic Ideas

- Feasibility study
  - The patterns of the same user are consistent
  - The patterns of different users differ a lot

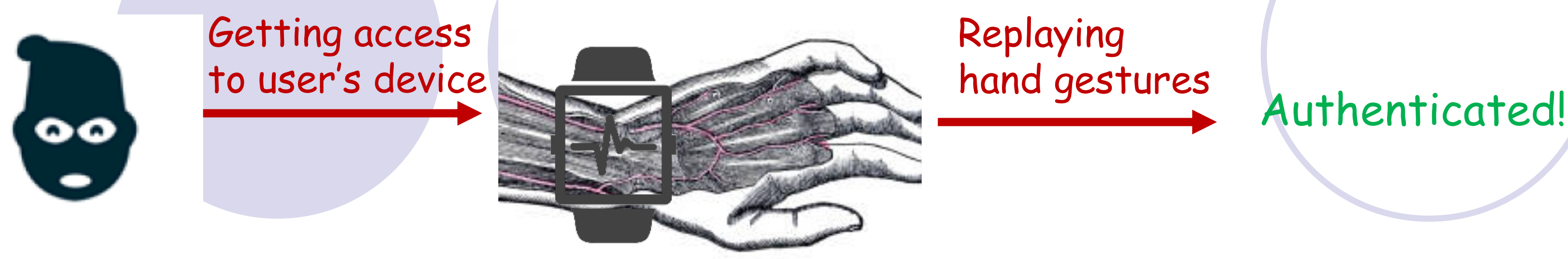


(a) The 1^{st} trail of u_1 (b) The 2^{nd} trail of u_1 (c) The 3^{rd} trail of u_1

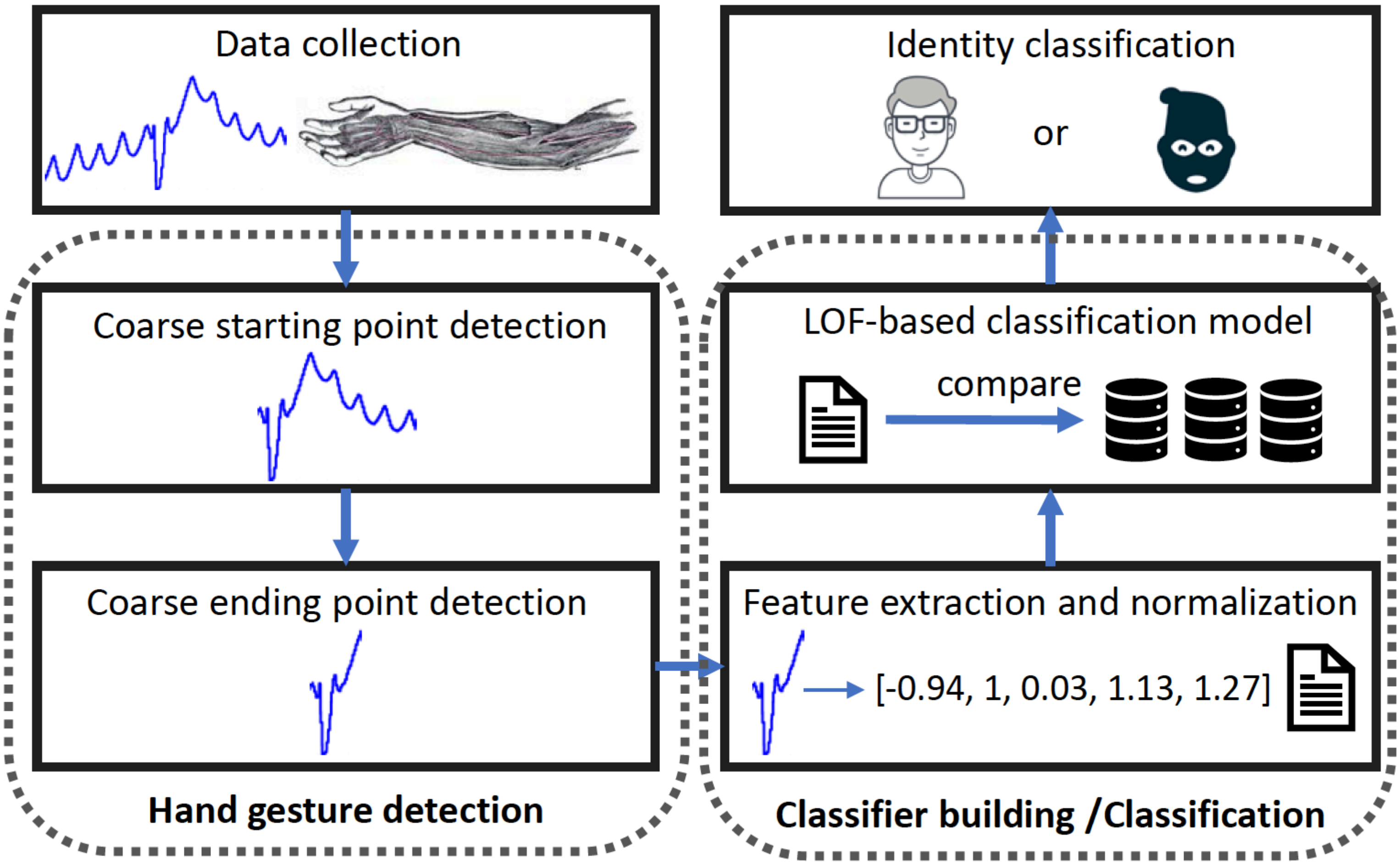
(d) The 1^{st} trail of u_2 (e) The 2^{nd} trail of u_2 (f) The 3^{rd} trail of u_2

Attack Models

- Random guess attack
  - Without knowing the gesture that normal user picks
- Mimicry attack
  - Knowing the gesture that normal user picks

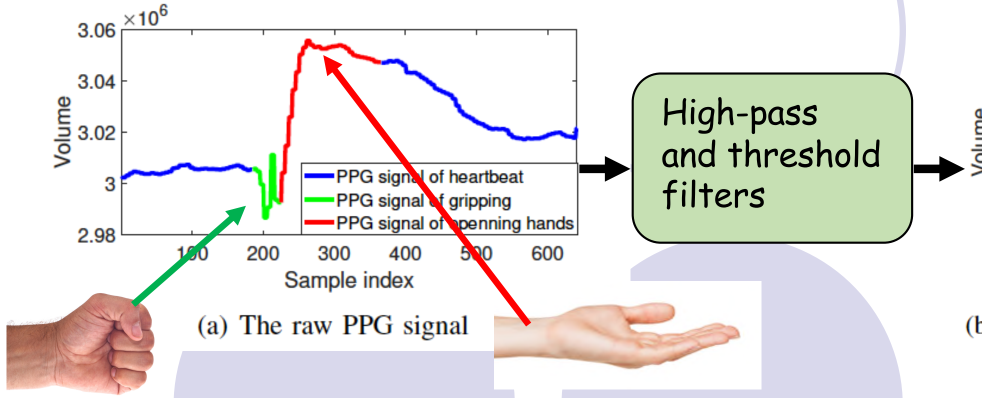


System Architecture

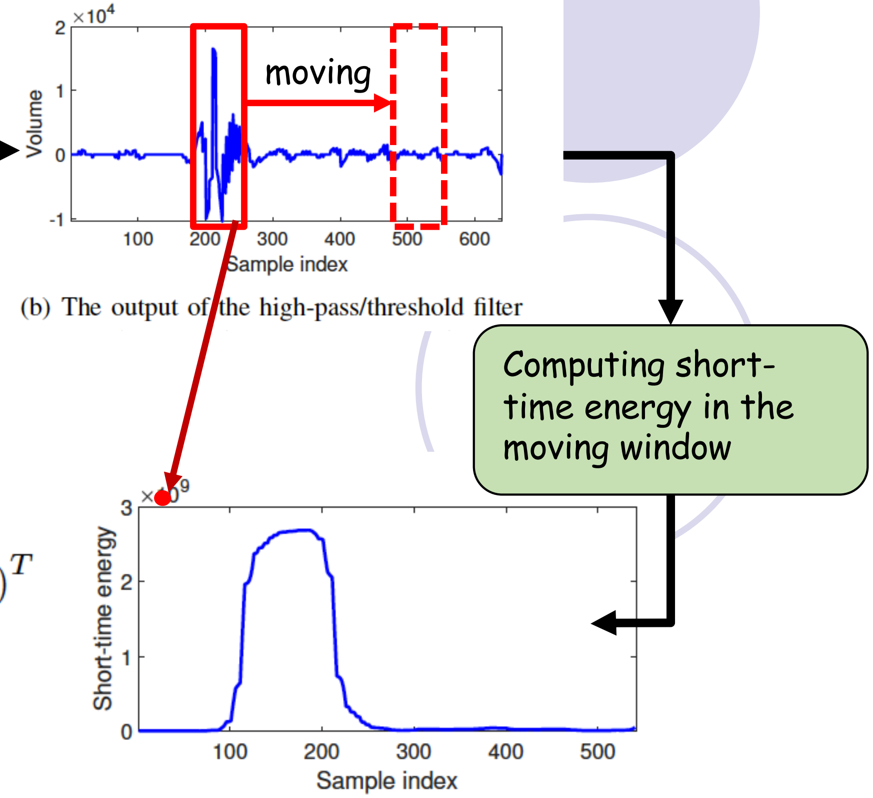


Solutions

- Detecting coarse starting point



(a) The raw PPG signal



(b) The output of the high-pass/threshold filter

(c) The short-time energy of filtered PPG signal

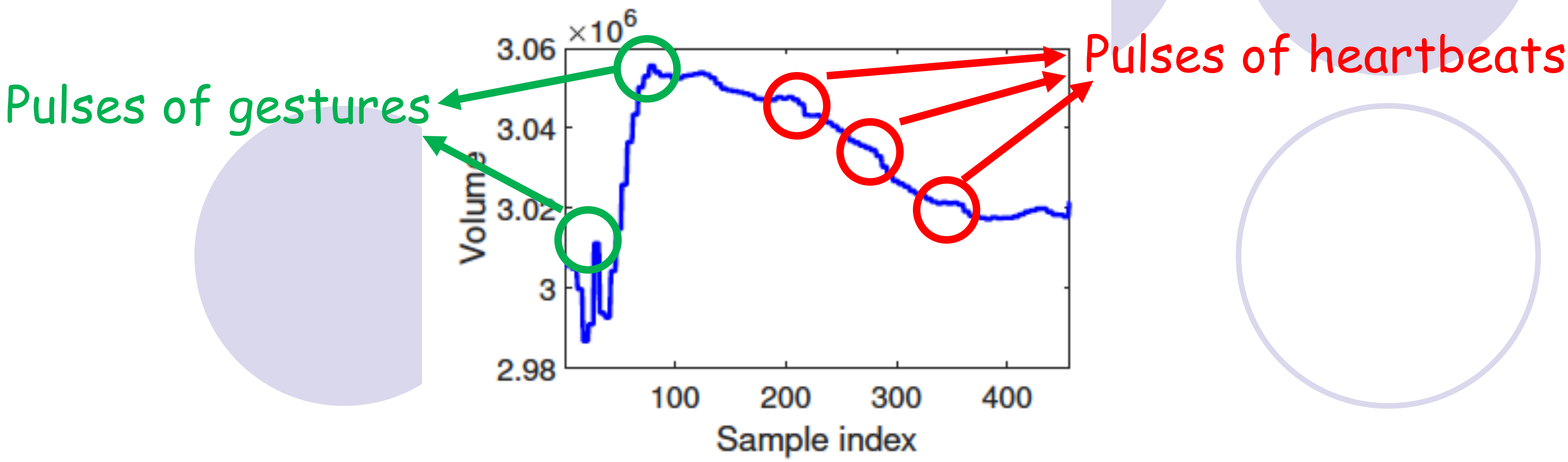
The starting point is detected
when the energy is maximized

$$\arg\max_{s} \quad ([y_s, y_{s+1}, \ldots, y_{s+w}])([y_s, y_{s+1}, \ldots, y_{s+w}])^T$$

$y = [y_1, y_2, \ldots, y_n]$: filter PPG signal
s: start of the window
w: window size

Solutions

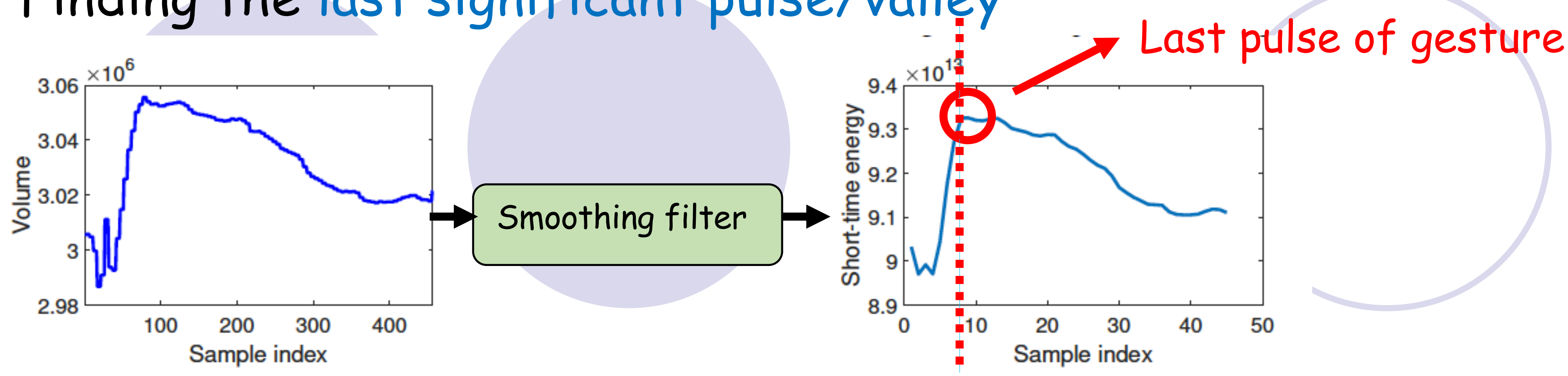
- Detecting coarse ending point
  - Gestures introduce stronger fluctuations vs. the heartbeat



(a) PPG signal from starting point

Solutions

- Detecting coarse ending point
  - Smoothing the raw PPG signal (remove small spikes)
    - Cutting the PPG signal into non-overlapped segments
    - Computing the short-time energy in each segment
  - Finding the last significant pulse/valley



(a) PPG signal from starting point

(b) Short-time energy of PPG signal

Significant pulses/valleys: higher peak-to-peak distance than heartbeats

Solutions

- Feature extraction
  - 5 features are selected:
    - The mean value, excluding the highest and lowest 20% values
    - The location of the lowest valley
    - Peak to peak distance
    - Num. of peaks that are 0.2 seconds around the lowest valley
    - The minimal dynamic time wrapping distance between a new PPG signal and those in the training dataset (normalized to (0,1])

Solutions

- Normalizing extracted features
  - Achieve good classification performance and balance the influences of different features
  - Z-score

$$F = \begin{bmatrix} f_{11} & f_{12} & \cdots & f_{15} \\ f_{21} & f_{22} & \cdots & f_{25} \\ \vdots & \vdots & \vdots & \vdots \\ f_{d1} & f_{d2} & \cdots & f_{d5} \end{bmatrix}$$

For each entry f_{ij}:
i: the i^{th} PPG signal
j: the j^{th} feature

Each $f_{i,j}$ is normalized using Z-score

$$z_{ij} = (f_{ij} - mean(F_j))/std(F_j)$$

Solutions

- User authentication
  - Challenge: the device only has the knowledge of normal user
    - Classification without attackers' data
  - Normalizing new gesture using the knowledge of user's gestures

Normal user

$$F = \begin{bmatrix} f_{11} & f_{12} & \cdots & f_{15} \\ f_{21} & f_{22} & \cdots & f_{25} \\ \vdots & \vdots & \vdots & \vdots \\ f_{d1} & f_{d2} & \cdots & f_{d5} \end{bmatrix}$$

New gesture (normal user/attacker)

Solutions

- User authentication
  - We use local outlier factor (LOF) as the classification model
  - Given a normalized feature vector $z = [z_{d1}, z_{d2}, \dots, z_{d5}]$
  - The local reachability density (LRD) is computed by

$$\mathrm{lrd(z)} = 1/\left(\frac{\sum_{r \in N_k(z)} \max\{k - distance(r), d(z,r)\}}{|N_k(z)|}\right)$$

$N_k(z)$ the k nearest neighbors of z

$d(z,r)$ the Euclidean distance between z and r

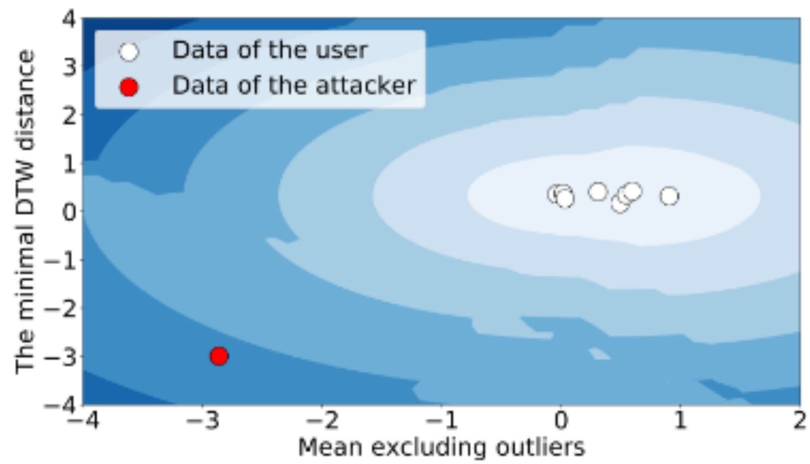
$k - distance(r)$ the distance of r to the k^{th} nearest neighbor

Solutions

- User authentication
  - Comparing the LRD of the new gesture and the training data

$$LOF_k(z) = \frac{\sum_{r \in N_k(z)} \frac{lrd(r)}{lrd(z)}}{|N_k(z)|}$$

  - An attacker is detected if LOF is larger than a threshold
  - The darkness represents the LOF value (the darker, the larger)



Evaluation

- We build a prototype implemented on the Samsung Gear 3 smartwatch running Tizen OS 3.0
- A graphical user interface (GUI) for data collection
- 12 volunteers where 7 of them act as normal users
- For each normal user:
  - 4 random guess attackers
  - 5 mimicry attackers

Evaluation

- Overall performance
  - Average authentication accuracy: 96.31%
  - Average true rejection rate of random attack: 95.89%
  - Average true rejection rate of mimicry attack: 91.64%

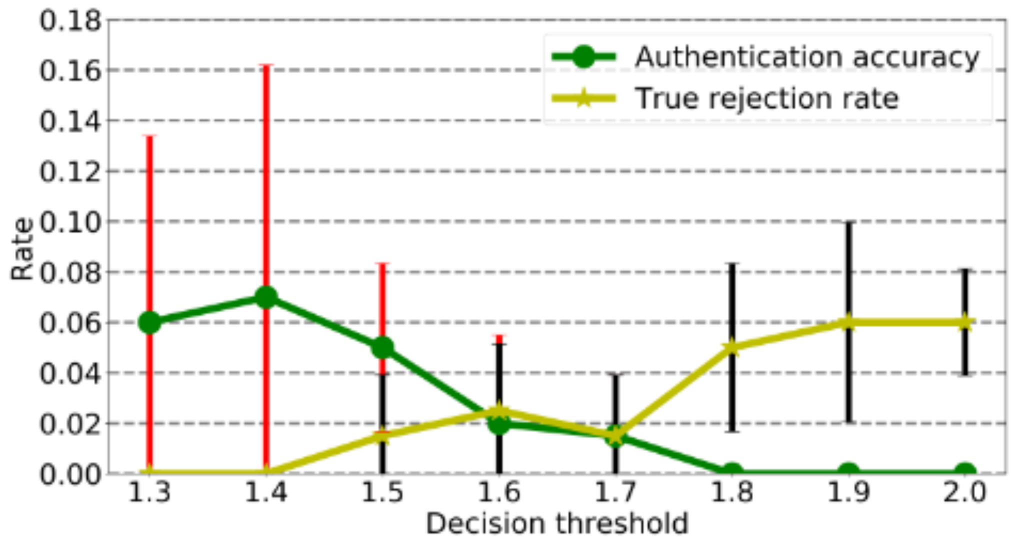
Evaluation

- Impact of training set size

7 training instances are enough to ensure good performance

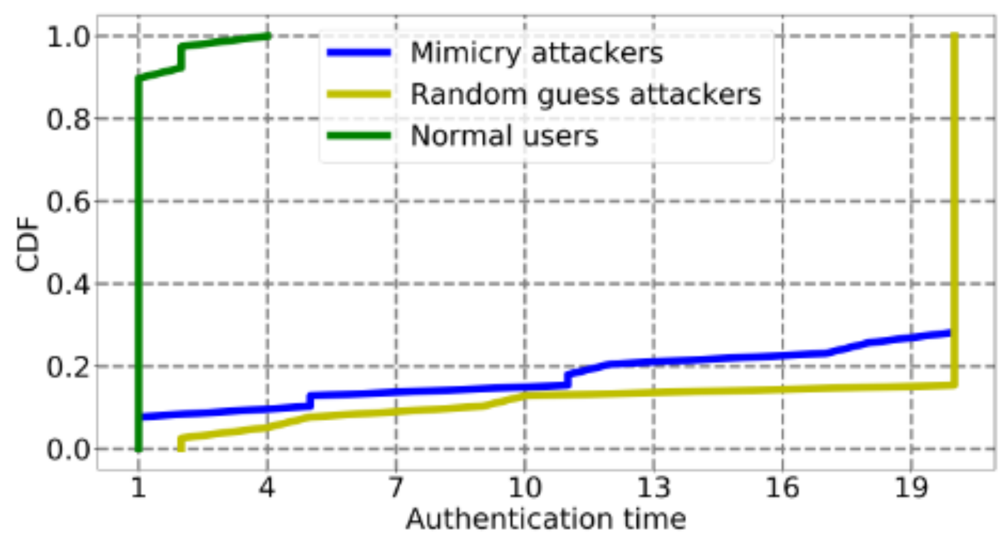
Evaluation

- Impact of decision threshold



Evaluation

- authentication time
  - Authentication time: num. of attempts until being authenticated



Conclusion

- Designing an authentication system on commercial smartwatches
  - Software-based
  - Can be quickly launched on existing smartwatches
  - Without the knowledge of attackers
- Showing that PPG signals can be used for user authentication
  - Accurately reject mimicry attackers and random guess attackers

Thanks!