Cross-domain inference for human localization: Applying Wi-Fi RSSI data to CSI-trained models

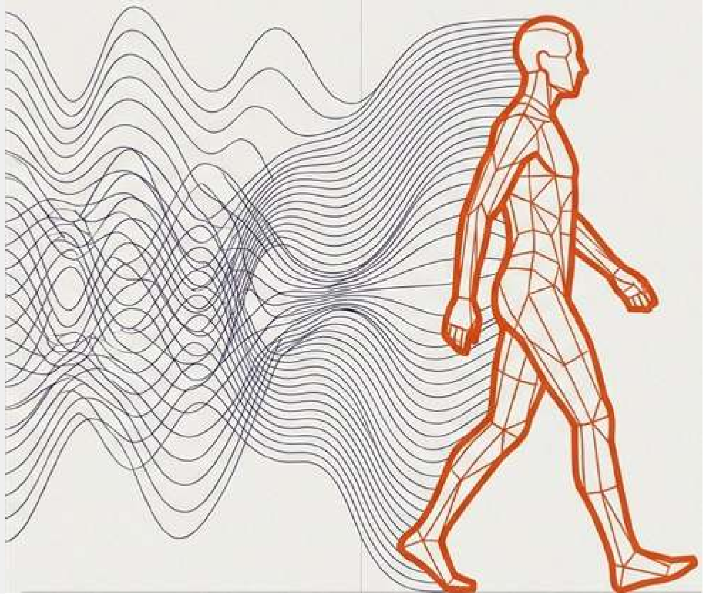


Image source: AI-generated

Ariel Duschanek-Myers,
Thomas Welsh,
Helmut Neukirchen

Department of Computer Science
helmut@hi.is · https://uni.hi.is/helmut

UNIVERSITY OF ICELAND
FACULTY OF INDUSTRIAL ENGINEERING, MECHANICAL ENGINEERING AND COMPUTER SCIENCE

Government of Iceland Ministry of Culture, Innovation and Higher Education · defend Iceland · EYVÖR | NCC-IS

This project has received co-funding from the European Union's Digital Europe Programme under grant agreement no. 101226821 Advancing Eyvör – The National Coordination Centre for Cybersecurity in Iceland and 101127307 Defend Iceland: Nationwide bug bounty platform.

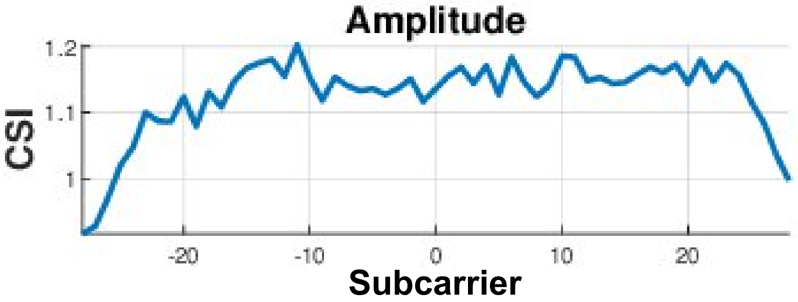
Co-funded by the European Union · ECCC

Motivation

- Most are probably aware that you can be tracked based on your phone's Bluetooth or Wi-Fi MAC address.
- Even if your phone is switched off…
- …our environment is full of Wi-Fi senders and receivers.
- Gets even worse with the advent of IoT and smart devices:
  - Wi-Fi is everywhere: not just your device, but e.g. someone else's smart TV!
- But it is also possible to localize humans passively:
  - Using some Wi-Fi radio waves as "radar":
    - The human body blocks or attenuates radio waves.

Wi-Fi foundations: CSI

- CSI (Channel State Information)
  - Each single Wi-Fi channel is split into multiple subcarrier frequencies.
- CSI measures for every single subcarrier:
  - Amplitude: signal strength for each subcarrier.
  - Phase: phase shift for each subcarrier, typically from –π (=–180°) to +π (=+180°).
  - For each single subcarrier frequency f, the channel response H_f is a complex number consisting of the amplitude and the phase.
  - In addition, MIMO (Multiple-Input Multiple-Output) uses multiple antennas.
    - Individual channel response not only for each subcarrier frequency f, but also for each antenna a.
- A single CSI measurement consists of K × N complex numbers:
  - K subcarrier frequencies,
  - N antennas.
  - (Per sender-receiver pair.)



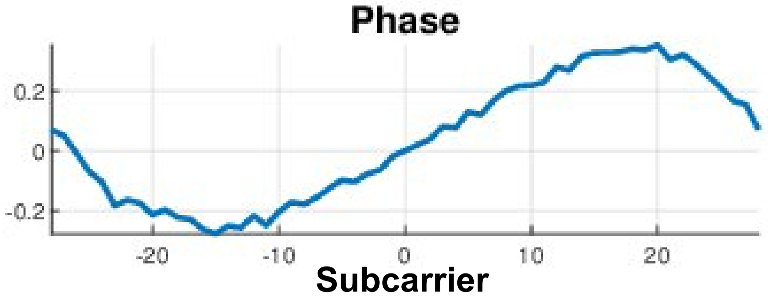


Image source: Kong, Chen: *CSI-RFF: Leveraging Micro-Signals on CSI for RF Fingerprinting of Commodity WiFi*. IEEE Transactions on Information Forensics and Security, 2024

Related work

- Wang et al.: Person-in-WiFi: Fine-grained person perception using WiFi, 2019 IEEE/CVF International Conference on Computer Vision (ICCV), 2019 https://doi.org/10.1109/ICCV.2019.00555
- Able to create 2D wireframes from a 1D Wi-Fi connection:
  - 1 transmitter-receiver pair, with 3 MIMO antennas each.
- CSI as input for a neural network that was trained using 2D wireframes as labels.
  - Created from video recording where wireframes of people have been extracted using the OpenPose software.

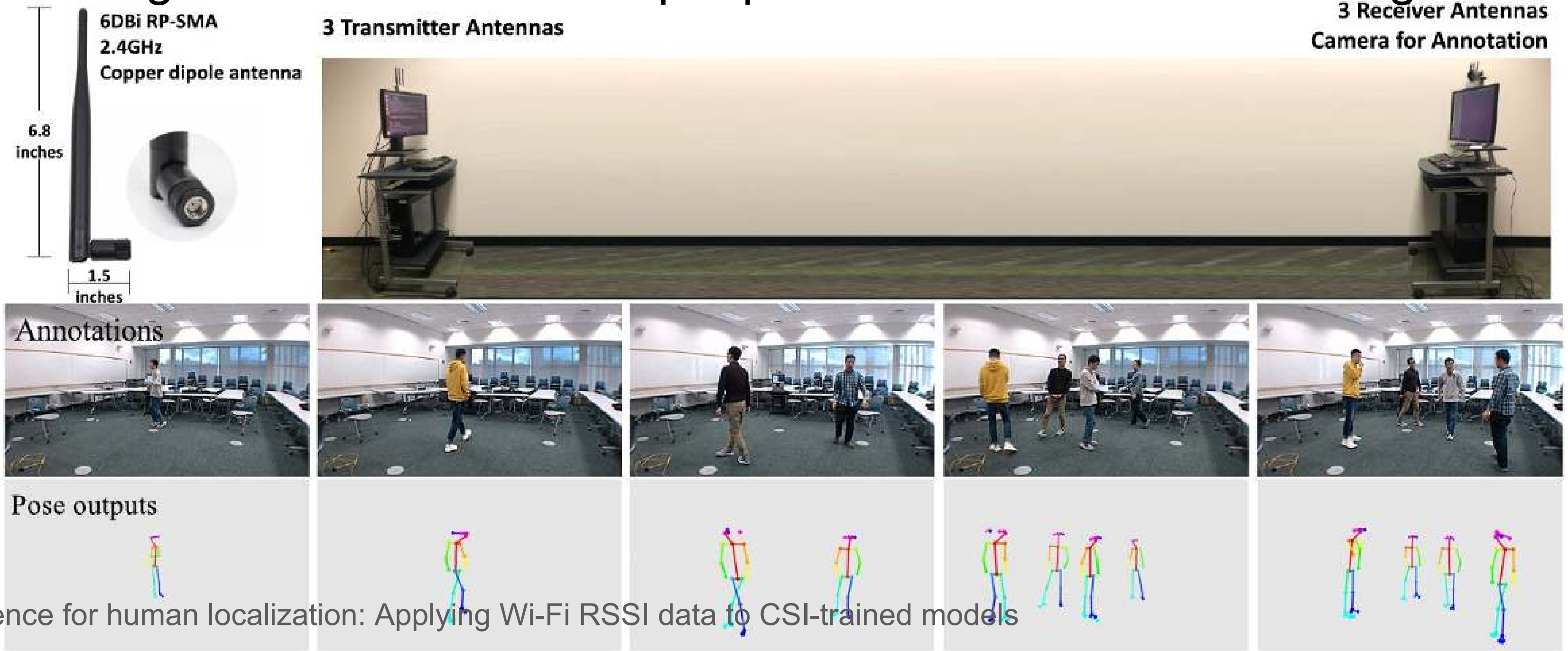
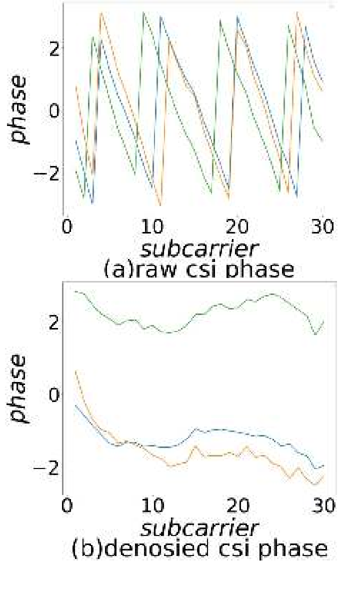
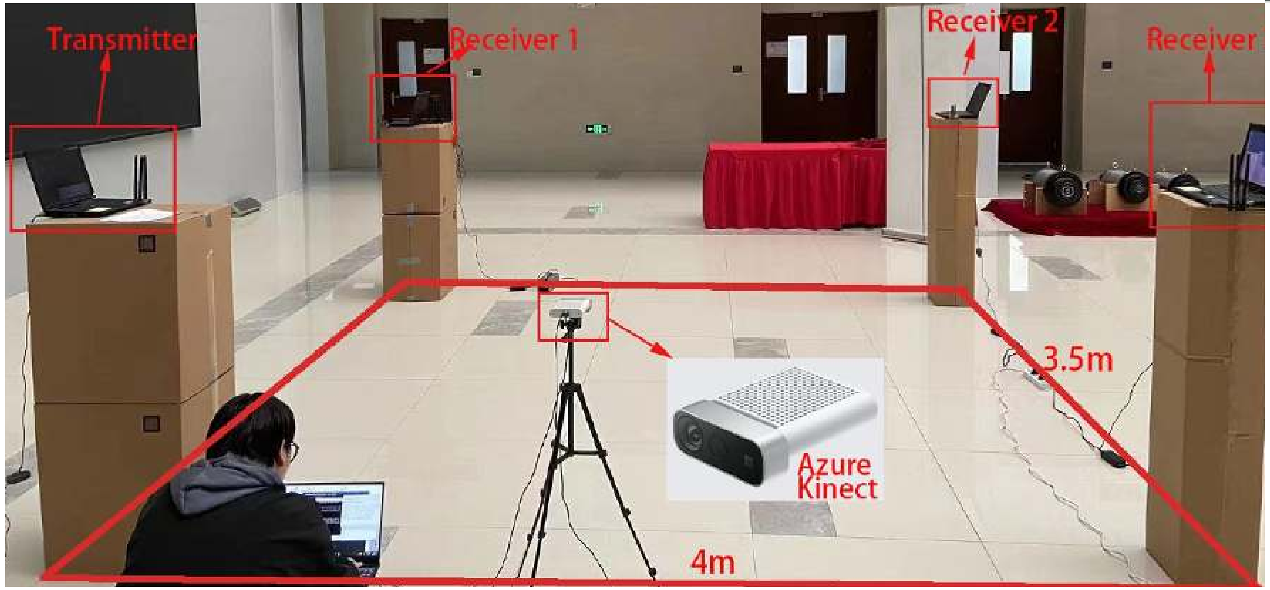


Image source: Wang et al. *Person-in-WiFi: Fine-grained person perception using WiFi*

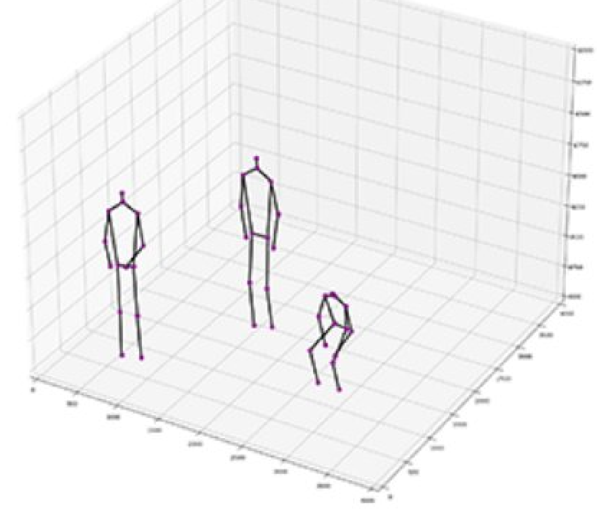
Related work: Person-in-WiFi 3D

- Yan et al.: “Person-in-WiFi 3D: End-to-end multi-person 3D pose estimation with Wi-Fi,” 2024 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2024, https://doi.org/10.1109/CVPR52733.2024.00098
- Able to create 3D wireframes from 2D Wi-Fi connections:
  - 3 transmitter-receiver pair, with 3 MIMO antennas each.
- CSI as input for a neural network, trained using 3D wireframe labels.
  - Labels for training are Microsoft Azure Kinect-generated.
  - Supports location & poses of multiple people in the surveilled room.
  - CSI denoising approach used.





Images source: Yan et al.
Person-in-WiFi 3D



Wi-Fi foundations: RSSI

- All the related work uses CSI:
  - Requires special Wi-Fi drivers and/or superuser privileges to access CSI-data.
  - I.e. someone surveilling you using an innocent-looking smart TV, would need to root that TV.
- As rooting a smart device may not always be possible:
  - **What kind of Wi-Fi-based surveillance is possible as a normal (=non-root) app(lication)?**
- RSSI (Received Signal Strength Indication):
  - A single, scalar value (e.g., -29 dBm):
    - measures the total received power of a Wi-Fi signal,

    Þ In contrast to CSI, RSSI includes also power induced by noise.
  - Can be typically accessed by a normal app(lication) without any special privileges or drivers.
    - Just install your innocent looking app on smart TV and it can access RSSI.

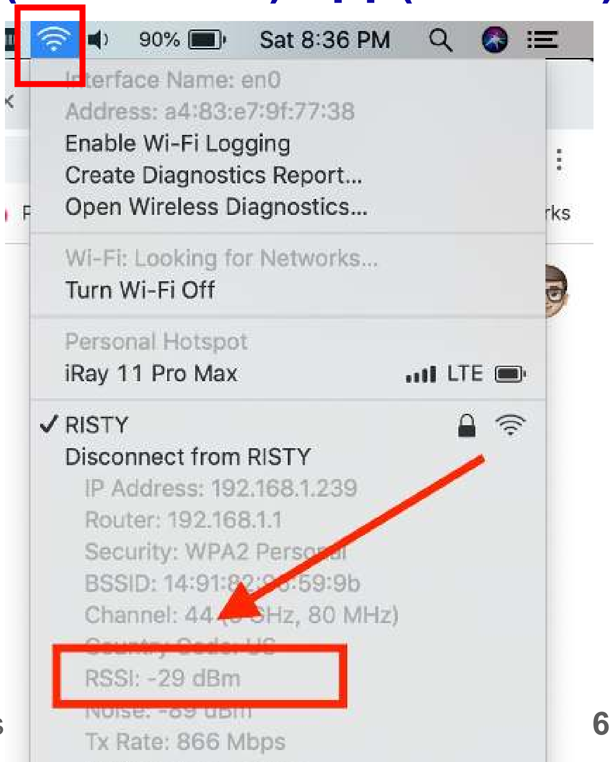


Image source: https://support.uscsd.k12.pa.us/kb/article/262-checking-your-wifi-signal-strength-on-your-macbook-air/

Research questions

1. What Wi-Fi data do ubiquitous device operating systems provide?
   - E.g.: Android – used by many smart devices (e.g. a smart TV).

2. Can RSSI Wi-Fi data be used to estimate spatial localization?

3. How confident are the resulting predictions?

Research question 1:

UNIVERSITY OF ICELAND

- What Wi-Fi data do ubiquitous device operating systems provide?
  - E.g.: Android – used by many smart devices (e.g. a smart TV): app that simply scans Wi-Fi:

```java
private void scanWifi() {
    if (ActivityCompat.checkSelfPermission( context: this, Manifest.permission.ACCESS_FINE_LOCATION) != PackageManager.PERMISSION_GRANTED) {
        return;
    }
    isScanCompleted = false;
    wifiManager.startScan();
}
```

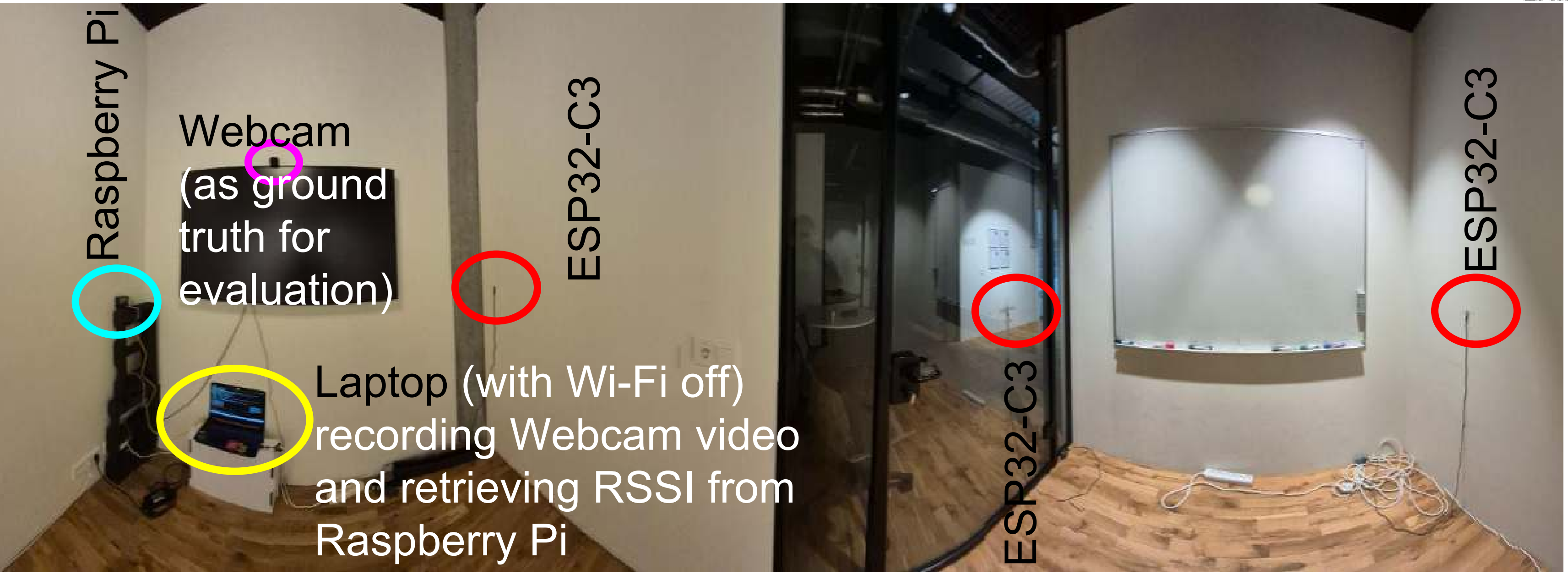
```xml
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools">
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE"
        tools:ignore="ForegroundServicesPolicy" />
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE"/>
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION" />
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_BACKGROUND_LOCATION" />
    <uses-permission android:name="android.permission.NEARBY_WIFI_DEVICES" />
```

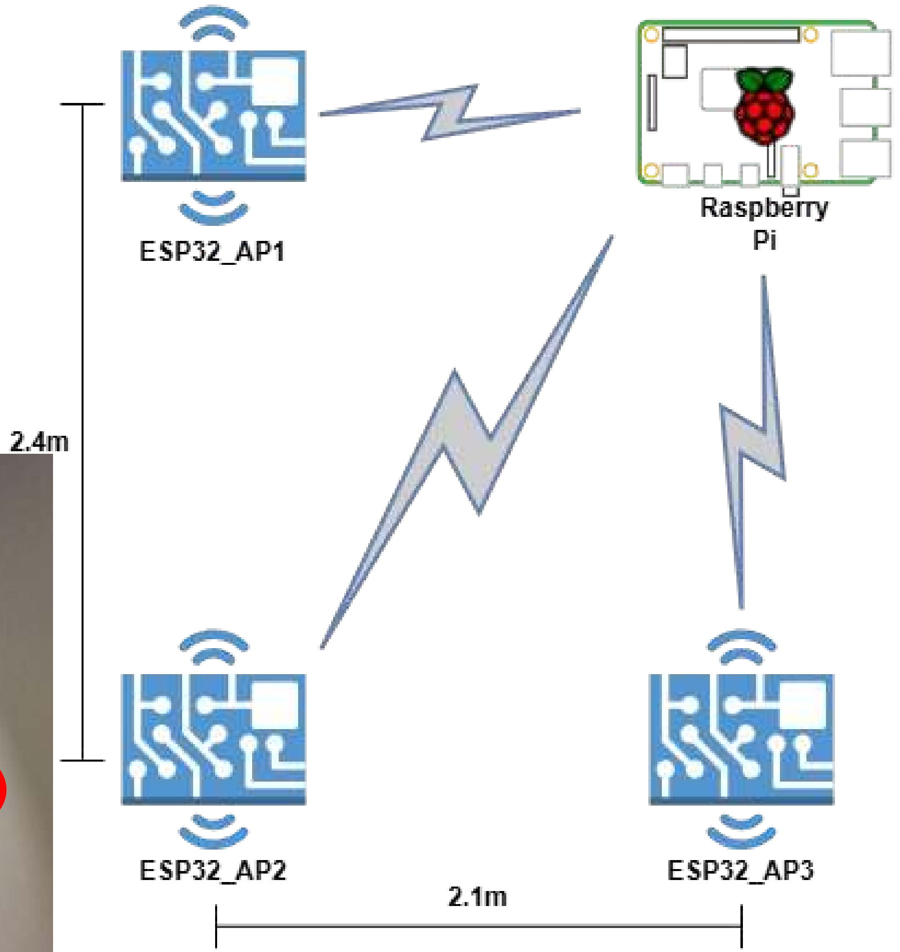
- Install and start evil app,
- Approve permissions,
- Enable developer options and disable there scan throttling.

Þ Access to real-time RSSI values possible for Android app!

Research question 2: Can RSSI Wi-Fi data be used to estimate spatial localization? Lab setup

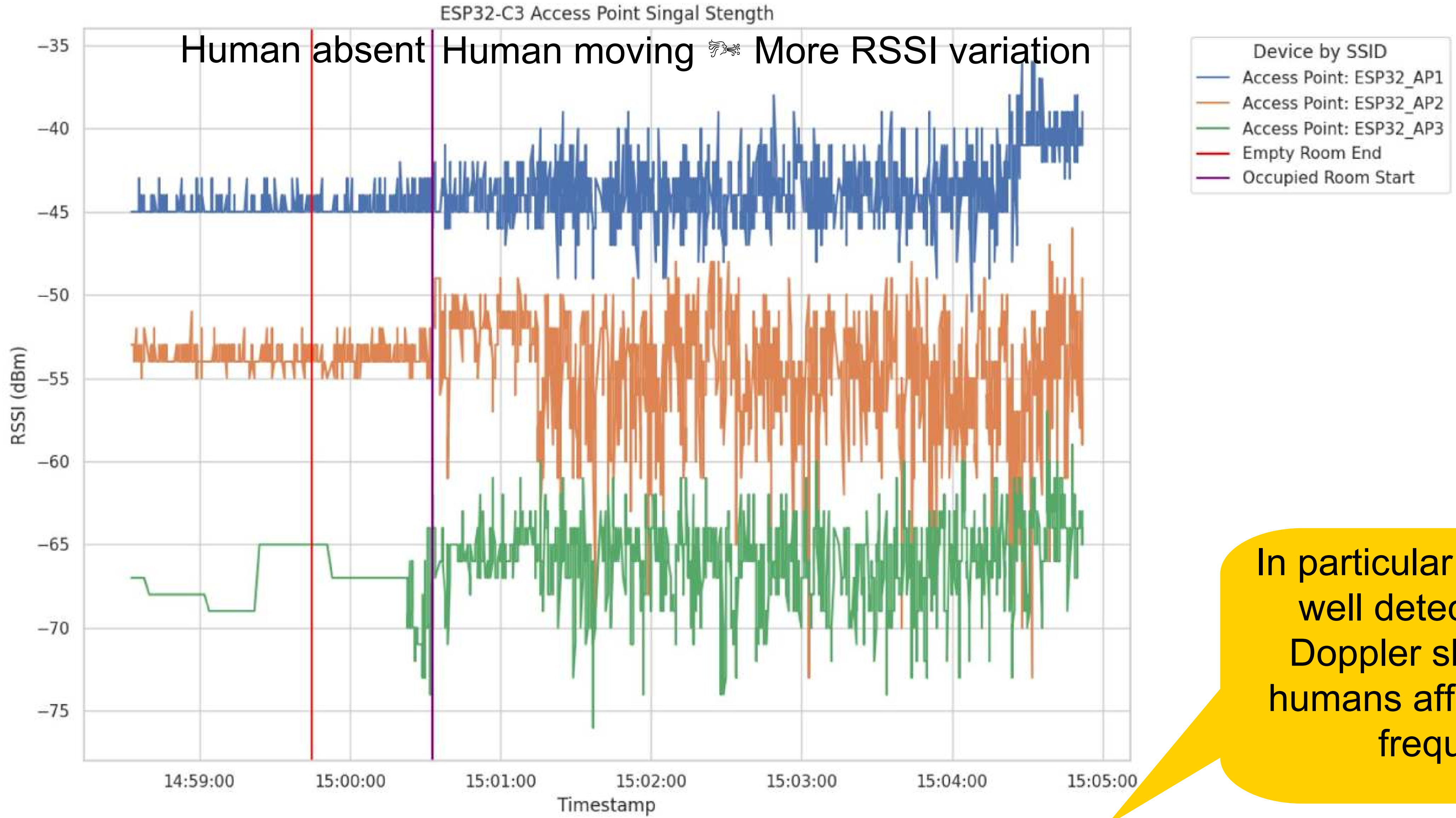
- Three ESP32-C3 boards:
  - Running as Wi-Fi Access Points (APs),
- One Raspberry Pi with Raspbian OS: **`iw scan`**
  (as app deployment on Android is tedious):
  - Running as Wi-Fi client, receiving RSSI data from the APs.





RSSI values with and without human moving in room

UNIVERSITY OF ICELAND



In particular movement is well detected due to Doppler shift: moving humans affect RF wave frequency.

- Moving of objects (e.g. a human) can easily be detected. Can we do locations?

RQ2 twist: Cross-domain inference – Applying Wi-Fi RSSI data to a CSI-trained model

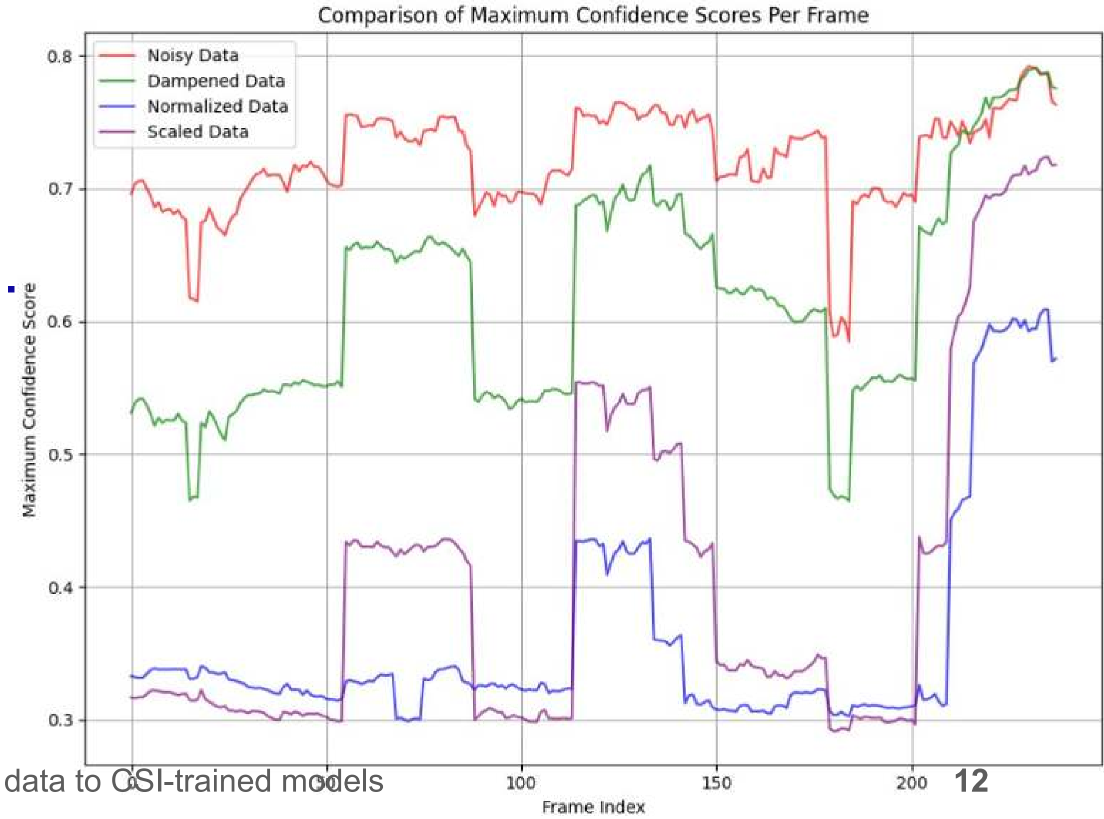
UNIVERSITY OF ICELAND

- For spatial localization of humans using Wi-Fi, we wanted to avoid creating own prediction model (incl. gathering labeled training data).
- Idea: reuse the CSI-based *Person-in-WiFi 3D* model from related work.
- Convert the RSSI data to CSI data and feed it into the CSI-based model (“cross-domain inference”):
  - As RSSI is just a single scalar, simply the same RSSI value is fed into the model for *all* subcarriers of CSI.
  - Conversion from RSSI to CSI is needed:
    - RSSI dBm has a base 10 logarithmic scale, whereas CSI has linear scale: $CSI \sim 10^{RSSI}$
    - The “d” in dBm means “deci”, need to scale RSSI values by a factor of 10: $CSI \sim 10^{RSSI/10}$
    - RSSI values measure electrical power, whereas CSI amplitude is a voltage: $P \sim V^2$ 🌧 $V \sim P^{1/2}$

Þ **$CSI = 10^{RSSI/10x2}$** (Note: complex part, i.e. the phase is ignored; also: RSSI includes noise.)

RQ2: Denoising RSSI data to be used for CSI-model

- In contrast to CSI values, RSSI values include noise:
  - Þ Noise needs to be removed from RSSI in order to use them for CSI model.
- CSI-based model provides prediction confidence score:
  - Þ High confidences used as indicator that the RSSI signal has been well denoised.
- Experiments did show that simply subtracting the mean of the three RSSI values (for the three AP-client pairs) for the empty room time series resulted in best confidence scores.
  - Shown by red graph.

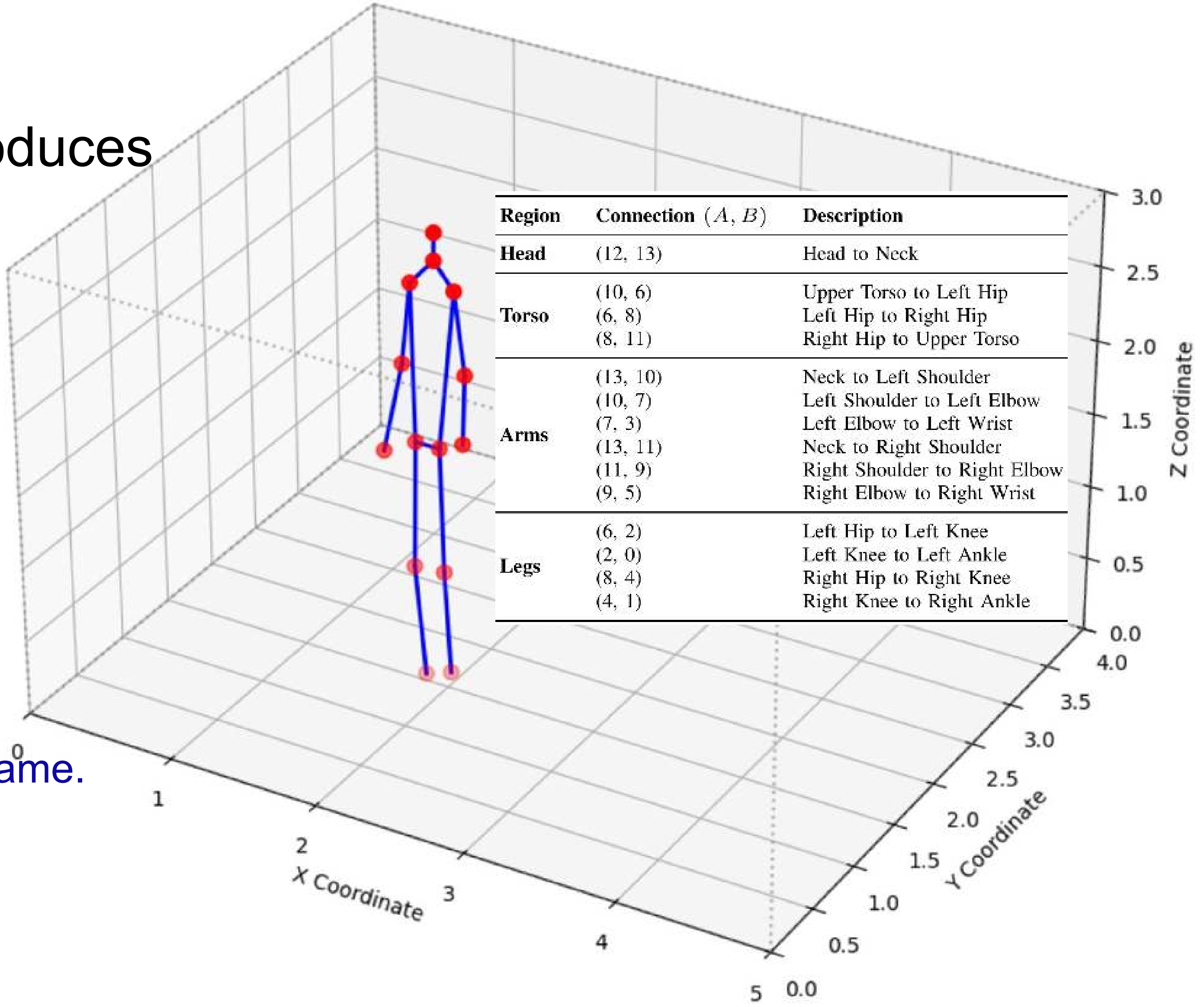


Þ This denoising approach is used in the remainder.

RQ3: How confident are the resulting predictions?

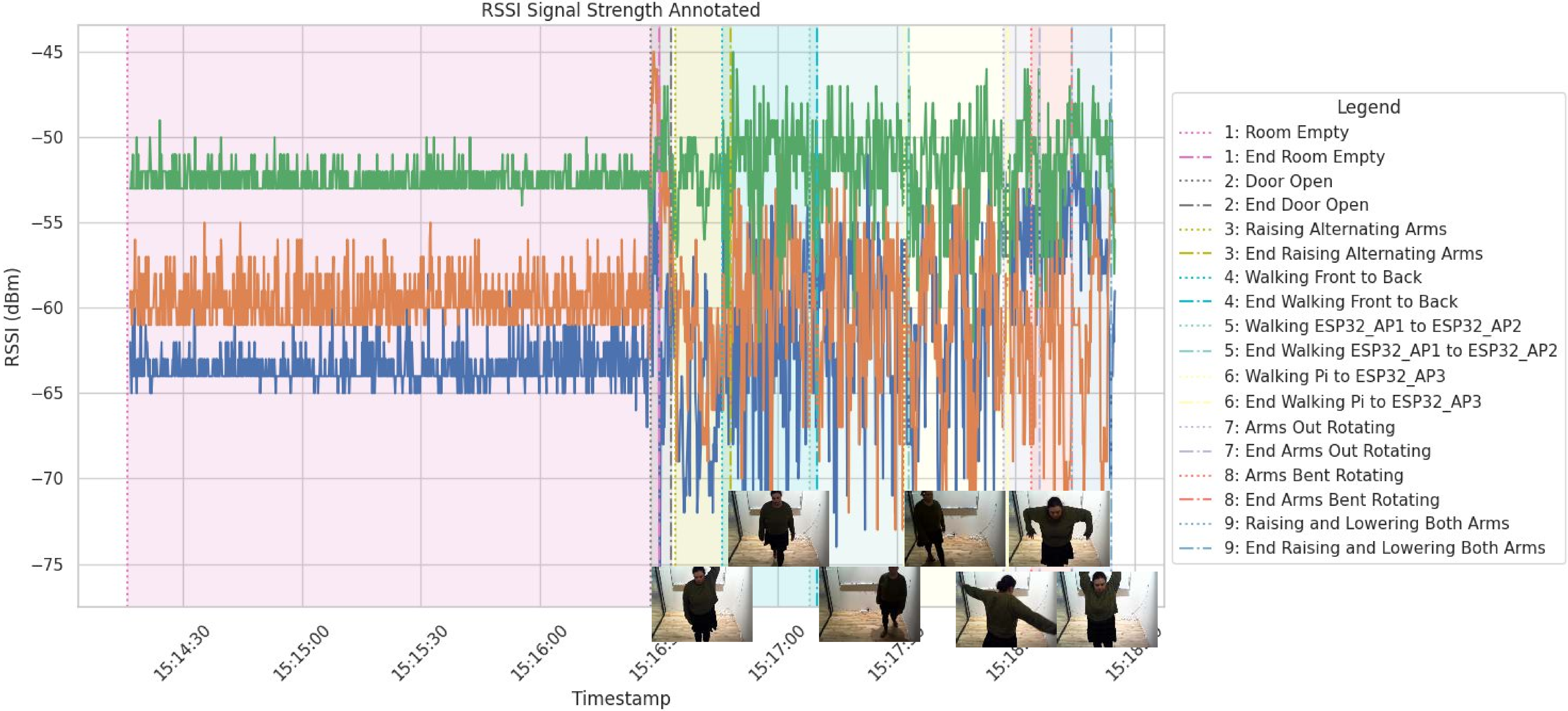
- The re-used *Person-in-WiFi 3D* produces values to be visualized by a wireframe model:
  - Location and pose (with confidence score).
  - Based on 14 “keypoints” = a specific joint of the assumed wireframe.
  - Problem: The underlying wireframe will always produce humanoid shapes – even if the confidence is low.
    - Confidence score is ignored by wireframe.

ÞFurther investigation of prediction confidence needed!



Region	Connection (A, B)	Description
Head	(12, 13)	Head to Neck
Torso	(10, 6)	Upper Torso to Left Hip
	(6, 8)	Left Hip to Right Hip
	(8, 11)	Right Hip to Upper Torso
Arms	(13, 10)	Neck to Left Shoulder
	(10, 7)	Left Shoulder to Left Elbow
	(7, 3)	Left Elbow to Left Wrist
	(13, 11)	Neck to Right Shoulder
	(11, 9)	Right Shoulder to Right Elbow
	(9, 5)	Right Elbow to Right Wrist
Legs	(6, 2)	Left Hip to Left Knee
	(2, 0)	Left Knee to Left Ankle
	(8, 4)	Right Hip to Right Knee
	(4, 1)	Right Knee to Right Ankle

RQ3: Used scenario – raw RSSI data with labeled events



RQ3: Standard deviations of the keypoints

UNIVERSITY OF ICELAND

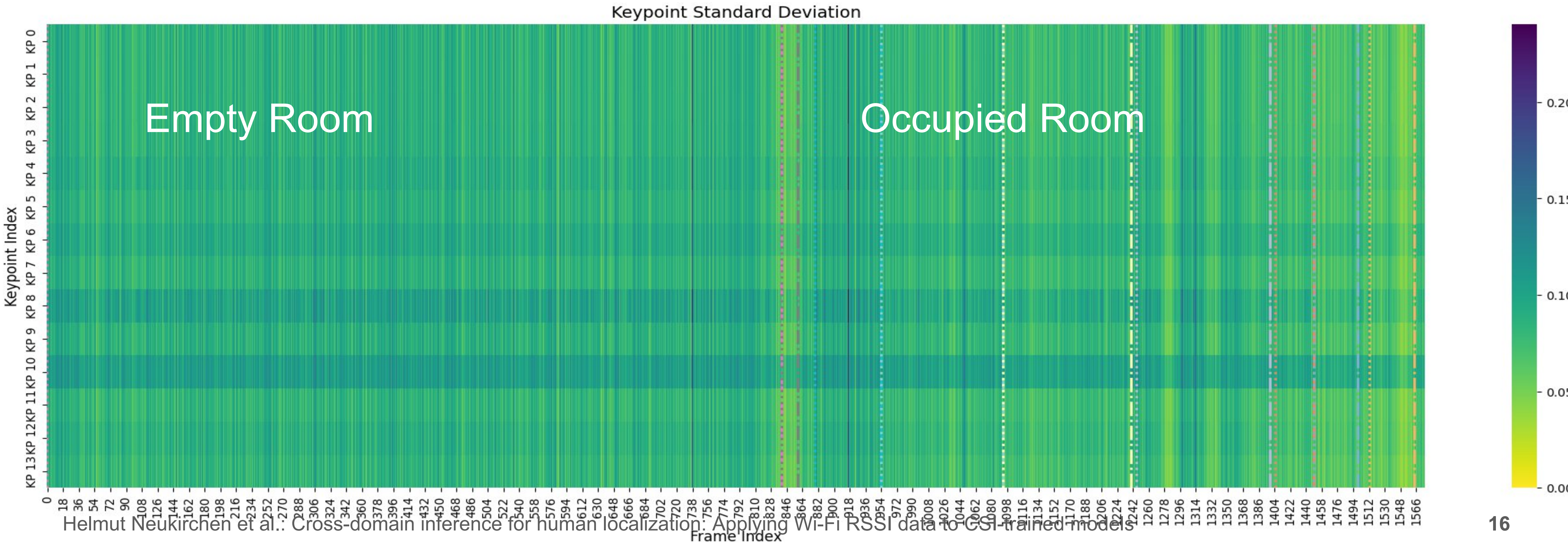
- A “frame” contains a sliding window of the most recent 100 Wi-Fi scans.
- *Person-in-WiFi 3D* model makes 100 predictions per frame,
  - i.e. the 14 keypoint values of the wireframe are predicted.

- Calculate standard deviation of all 100 keypoint predictions made for a frame:
  - If standard deviation is low, then all 100 predictions made for a frame are similar:
    - An indicator that the predictions have a consensus.
  - If standard deviation is high, then 100 predictions made for a frame do vary.
    - Either an indicator that the predictions are fluctuating, i.e. predictions are not very good.
    - Or (if confidence score is at same time high): an indicator that movement is going on.

- Can be visualised in a heatmap 🎭next slide.

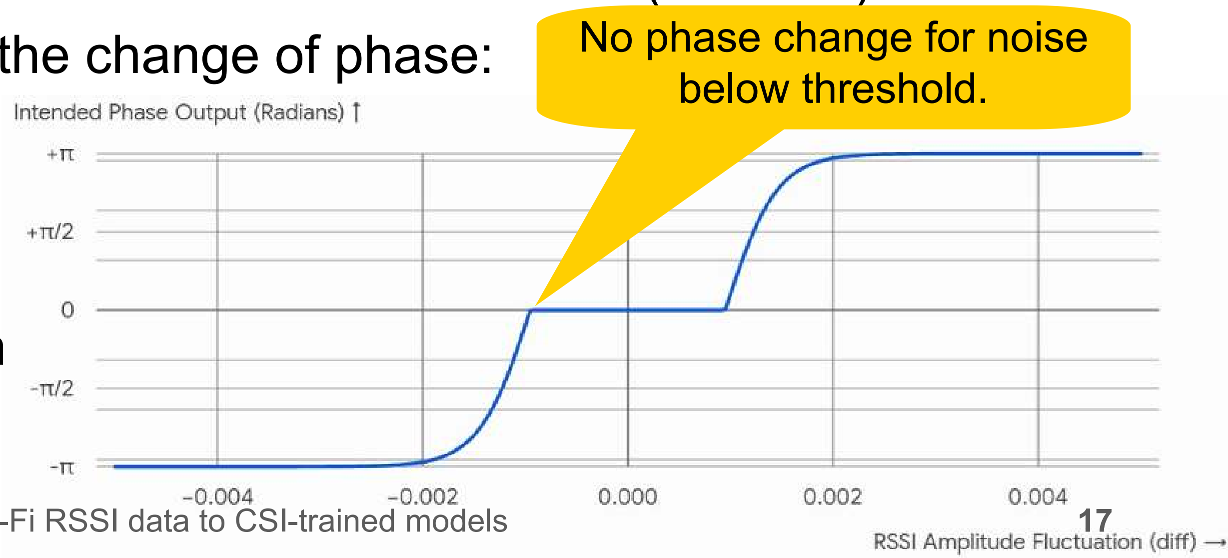
RQ3: Heatmap of standard deviations of the keypoints

- The more yellow (=low standard deviation), the more agreement of predictions within a frame of 100 scans.
- The more green/blue (=high standard deviation), the more fluctuation in the predictions within a frame.
  - E.g. due to movement of the oject/human.
- Not really a lot of difference between empty and occupied room! 🎭Next slide for improvement.

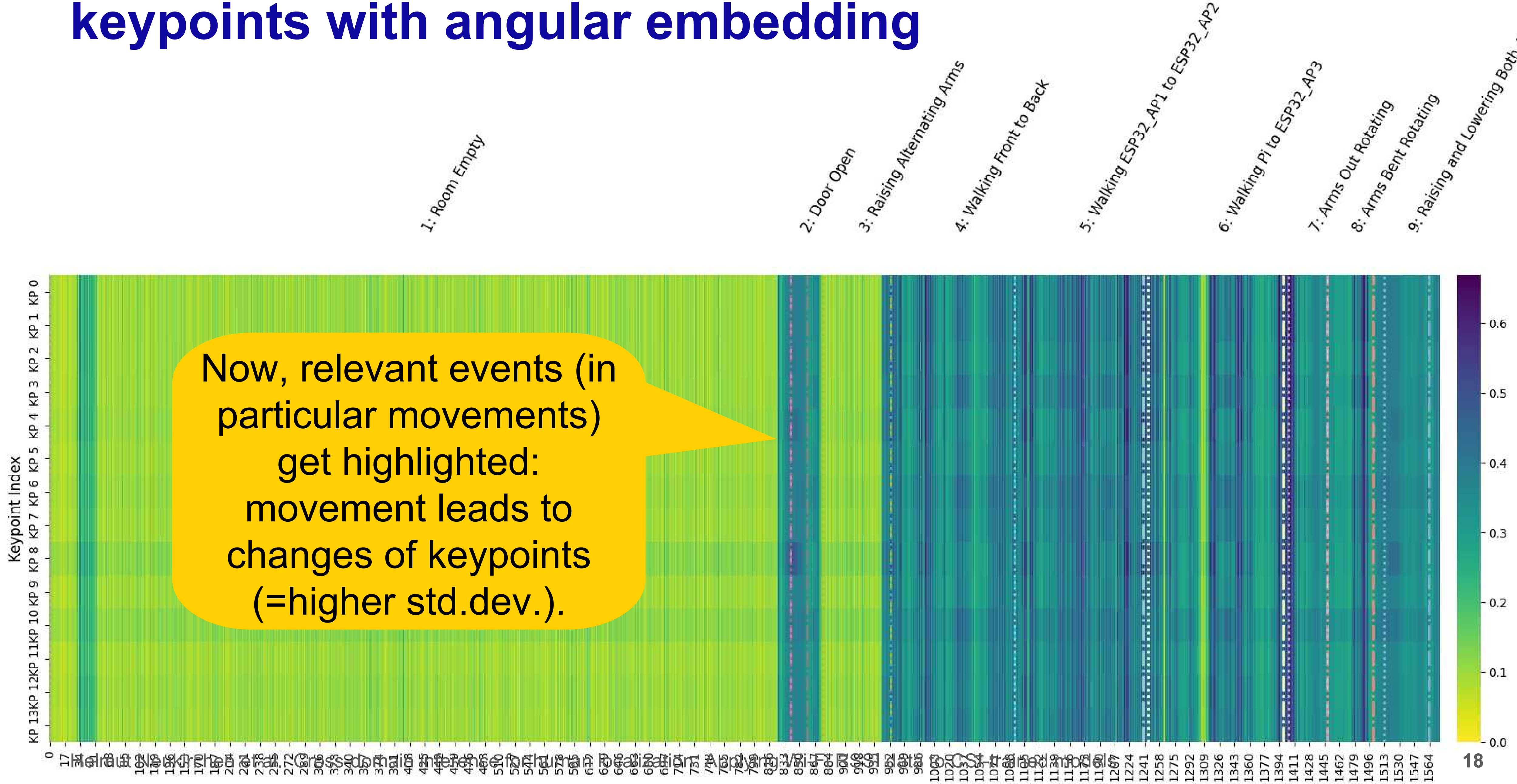


RQ3: Angular embedding

- To improve, give the *Person-in-WiFi 3D* model some phase information.
  - Reminder: the phase information is lacking in RSSI, but present in CSI.
    - Our RSSI to CSI conversion did simply set the phase to 0.
  - The *Person-in-WiFi 3D* model relies heavily on phase shifts to detect moving objects
    - as phase is what would get affected by objects.
    - They use a special phase denoising approach.
- Idea: turn fluctuations in signal strength into a phase shift:
  - But only real fluctuations, not just some tiny noise below some threshold (0.00095).
  - Use a sigmoid function (with K=4000) to limit the change of phase:
    - Up to +π for a spike of the RSSI value,
    - Up to –π for a drop of the RSSI value.
  - Feed the resulting value as phase information into the Person-in-WiFi 3D model.



RQ3: Heatmap of standard deviations of the keypoints with angular embedding



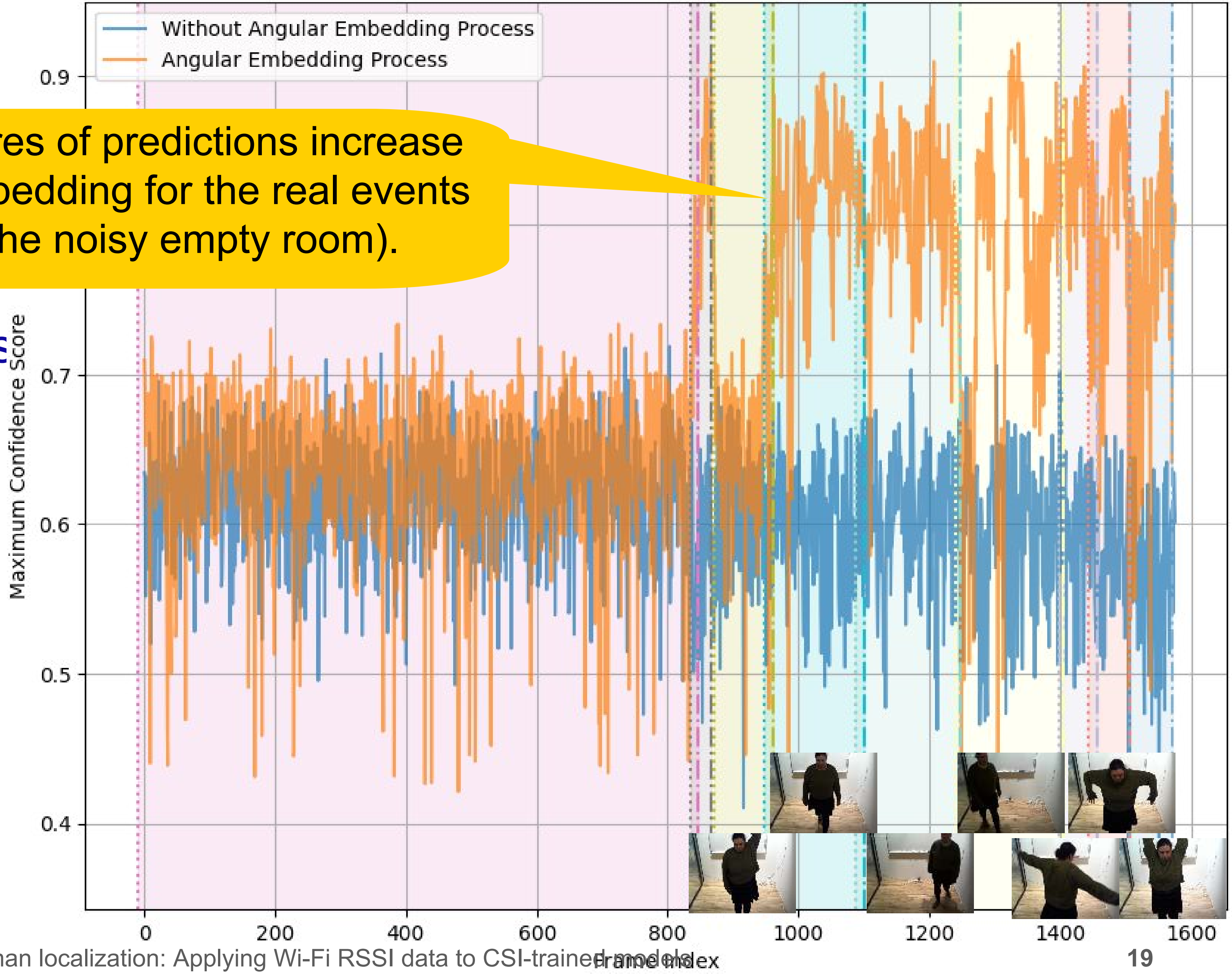
RQ3: Confidence scores with angular embedding

Confidence scores of predictions increase with angular embedding for the real events (but low for the noisy empty room).

- Confidence score increases from ca. 60% to ca. 80%.
- Both high standard deviations and high confidence score:

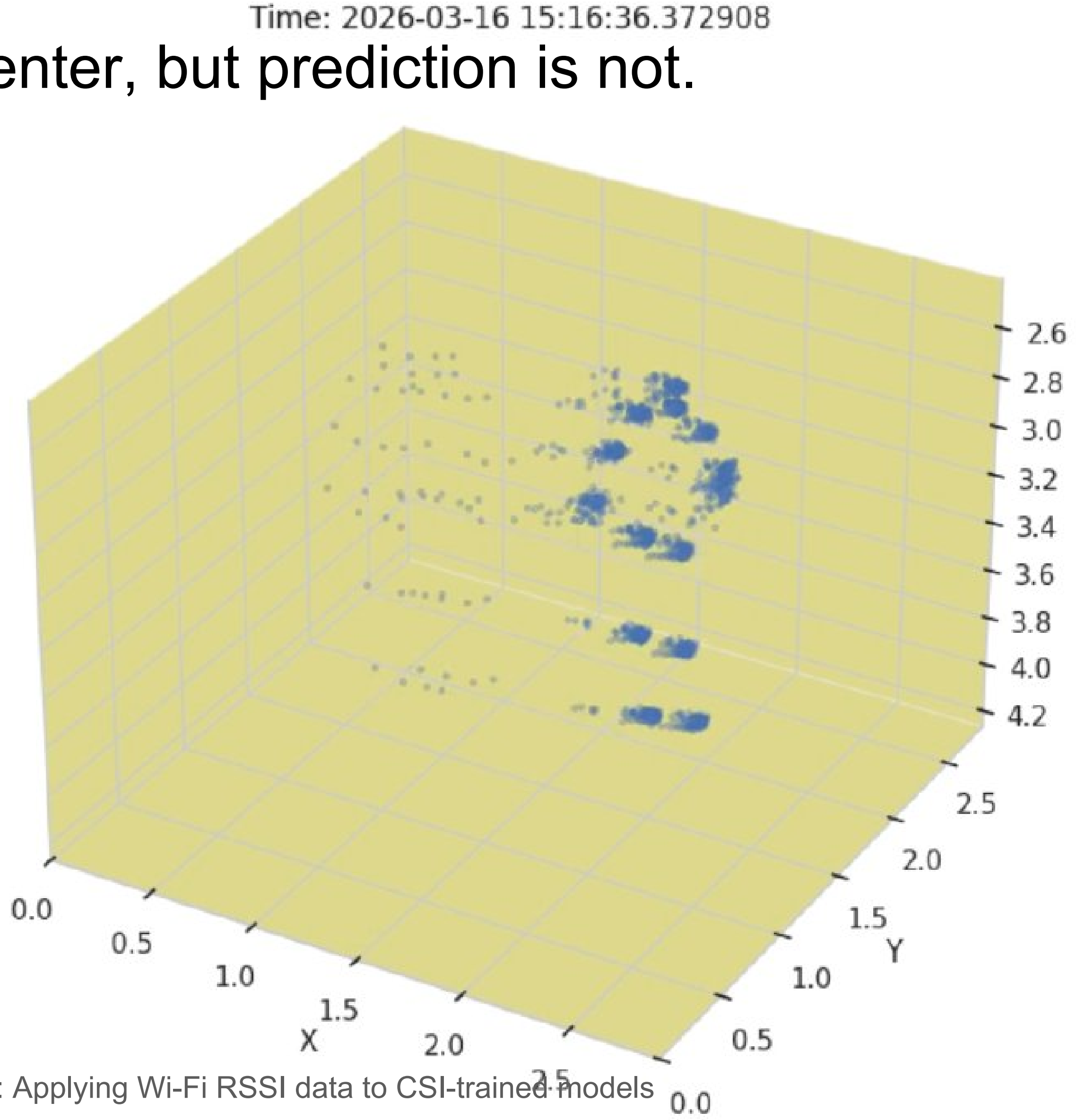
Þ these are real movements.

  - Confirmed by ground truth.



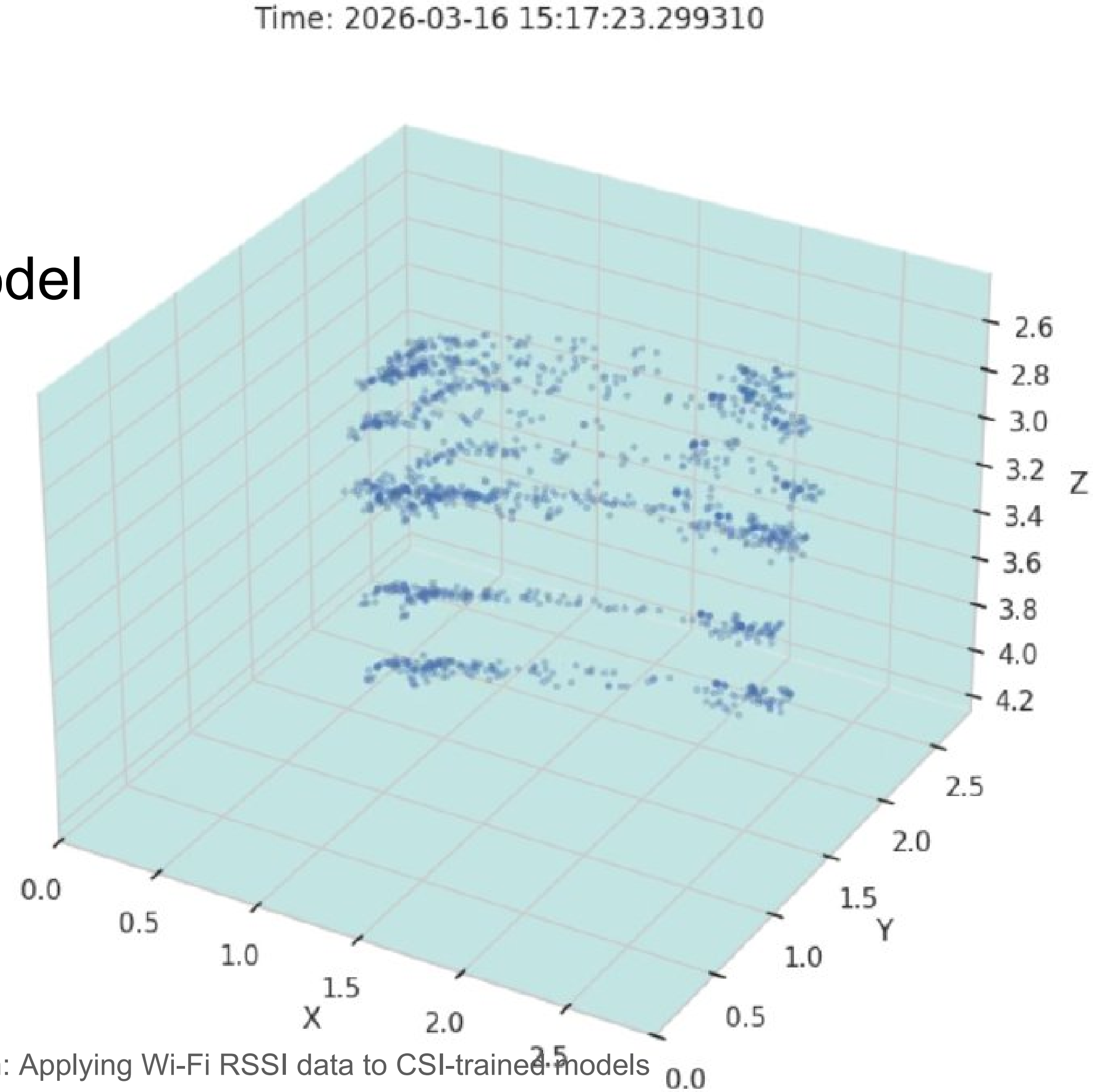
RQ2: Example prediction wireframes: Raising alternating arms (frame with 100 keypoints)

- Location should be almost in the center, but prediction is not.
- Pose (raised arm) not detected.



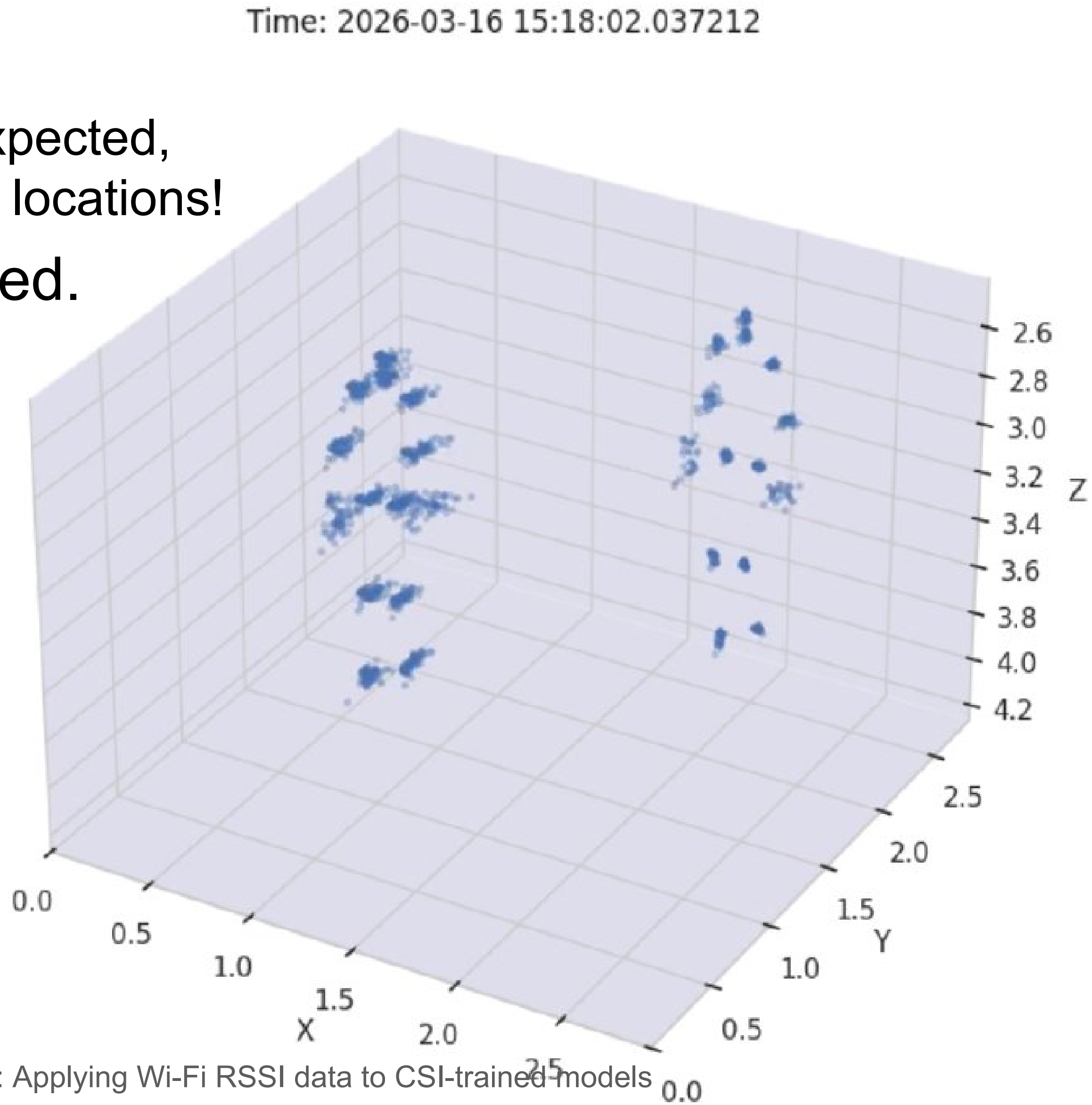
RQ2: Example prediction wireframes: Walking front to back and both diagonals (frame with 100 keypoints)

- 100 keypoints = 5 seconds,
  - The smeared wireframe locations correspond to real movement.
- Pose might be OK (but maybe, model always returns this “normal” pose).



RQ2: Example prediction wireframes: Rotating with arms straight out (frame with 100 keypoints)

- 100 keypoints = 5 seconds,
  - Smeared wireframe locations to be expected, but not at these two clearly separated locations!
- Pose (arms straight out) not detected.



Discussion and Outlook

- Discussion:
  - Re-used CSI-based model, but feeding with RSSI-data:
    - Pose detection seems unreliable.
    - Location detection works somewhat, in particular movements detected well (Doppler effect).
    - Privacy implications: Already without a neural network model, possible to detect presence (movement) vs. absence of humans. 🎭Next slide for mitigations.

- Outlook:
  - Currently, the inference is neither done on the Raspberry Pi nor on the connected Laptop, but on a NVIDIA A100 GPU on a supercomputer.
    - Can inference be done locally, in real-time?
  - Would a real RSSI-specific, RSSI-trained model perform better?

Mitigations against Wi-Fi surveillance?

- Tin foil hat?
  - Bad idea: probably a very characteristic attenuation pattern.
- User device audit:
  - Check for installed apps, activated developer options, permissions.
- Electromagnetic noise:
  - USB supply and USB cables can add a lot of noise, microwave ovens as well.
- OS vendors:
  - Decrease RSSI precision and update rate.
  - After a Raspbian OS update, the Wi-Fi driver had changed significantly and did not provide usable RSSI data anymore (had to revert to previous version).

Thank you for your attention · any questions?

UNIVERSITY OF ICELAND

Preprint DOI

Ariel Duschanek-Myers · Thomas Welsh ·
Helmut Neukirchen · helmut@hi.is · https://uni.hi.is/helmut

Government of Iceland
Ministry of Culture, Innovation and Higher Education

defend Iceland

EYVÖR | NCC-IS
ICELAND CYBERSECURITY COORDINATION CENTRE

This project has received co-funding from the European Union's Digital Europe Programme under grant agreement no. 101226821 Advancing Eyvör – The National Coordination Centre for Cybersecurity in Iceland and 101127307 Defend Iceland: Nationwide bug bounty platform.

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE