ORCA-PROJECT.EU

CSI-MURDER

Francesco Gringoli

University of Brescia

ORCA OC3 Review meeting

Sept 2020 Gent

ORCHESTRATION AND RECONFIGURATION CONTROL ARCHITECTURE

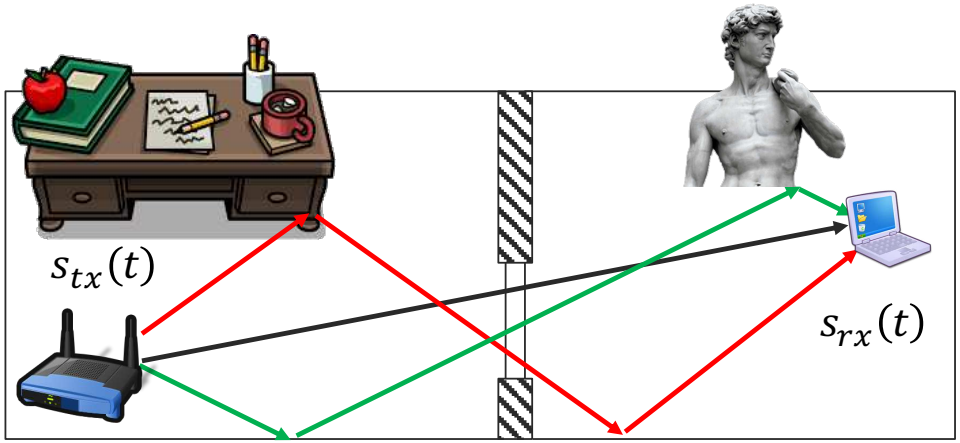
Outline

- Concept and objectives
- High level functional description
- Technical results & lessons learnt
- Experience with ORCA facility
- Experience with testbed

Concept: sensing and privacy

Passive indoor **sensing** is becoming a thing

- Exploits 802.11 OFDM modulation opportunistically
- Channel-State-Information (CSI) at receiver
- Device-free:
  - Interaction "signal/body"

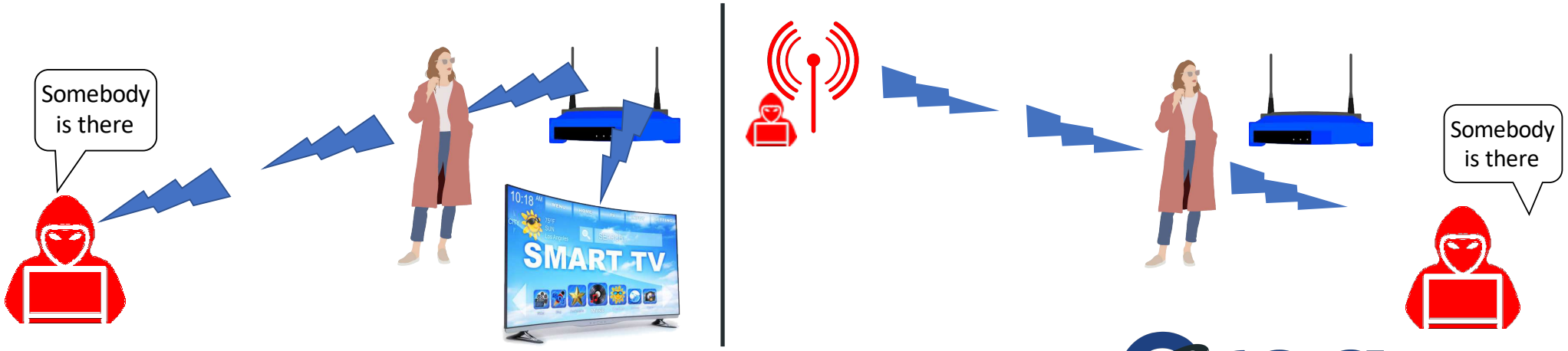


Question: Is **privacy** at risk?

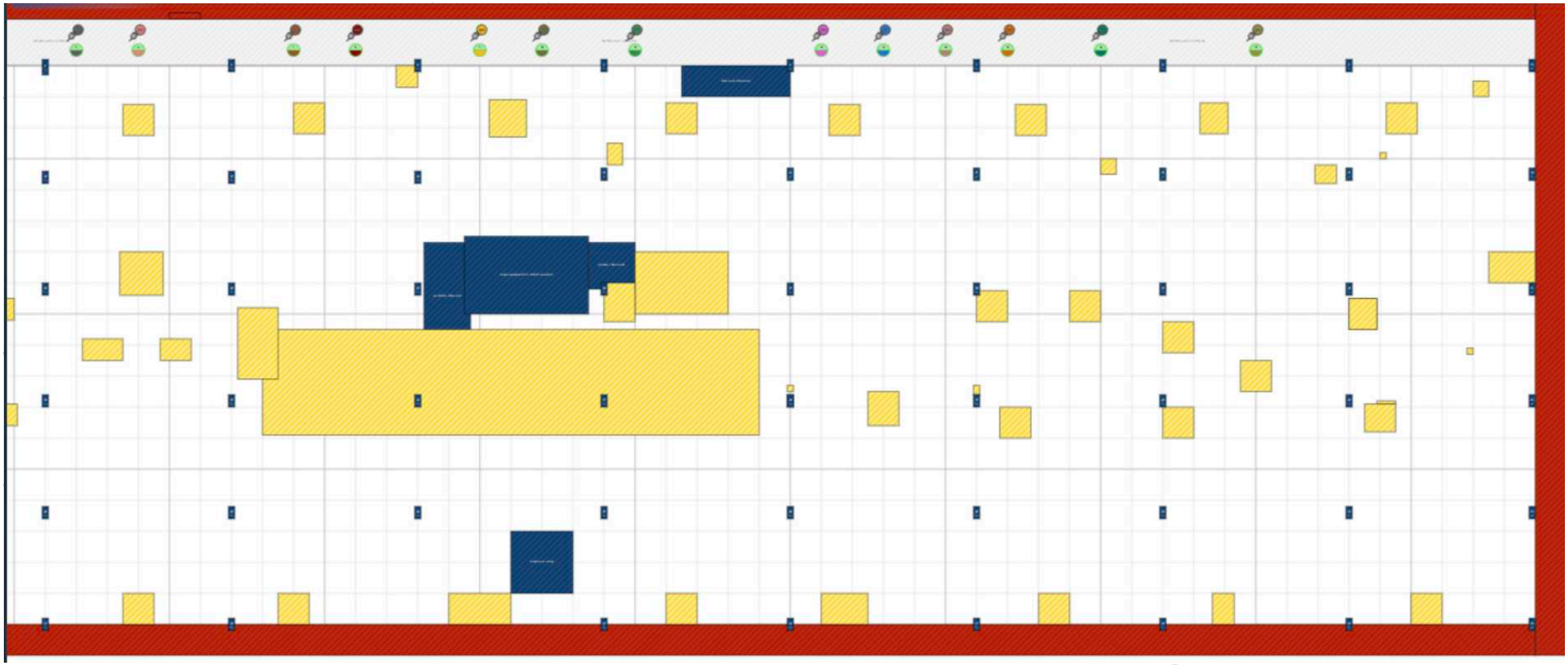
- Yes: motion detection, positioning, health monitoring
- Thorough evaluations missing, but ...
- ... there is a lack of research on possible countermeasures

Objectives

- **Investigate the impact** of CSI-based localization techniques and **propose mechanisms** to neutralize them
- Two scenarios:
  1. Passive, *exploiting other communications (left)*
  2. Active, *setting up ad-hoc communications (right)*



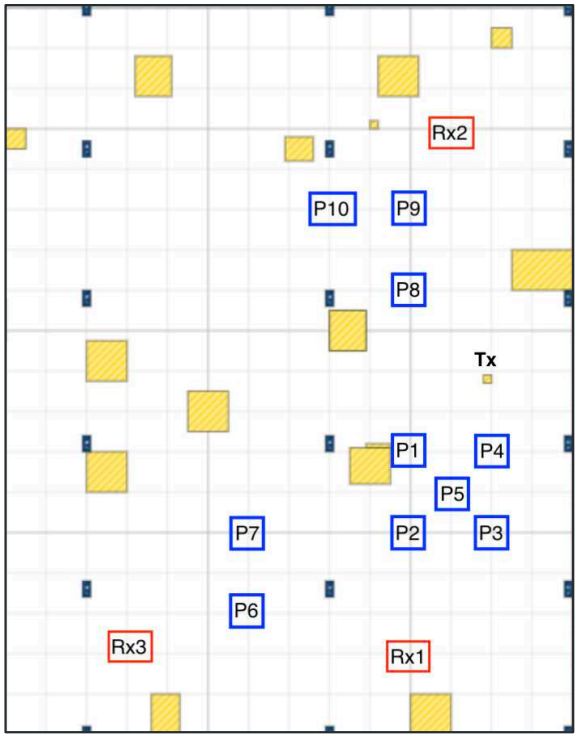
High level functional description: w-iLab.2



High level functional description: w-iLab.2

Run experiments in w-iLab.2

- Receivers
  - Nexus 6P mounted on robots (Rx_n)
  - Deploy at different locations
  - Use nexmon- csi for extracting CSI
- Targets to localize:
  - other robots, in several different positions (P_k)
- Transmitter (Tx):
  - passive scenario: zynq with openwifi
  - active scenario: Ettus B210 boards



Privacy breach & Neutralization mechanisms

- We set up (and demoed) a localization technique
  - based on Neural-Network
  - trained using samples collected on specific positions…
  - …to predict when objects move to those positions

THIS IS PRIVACY BREACH!

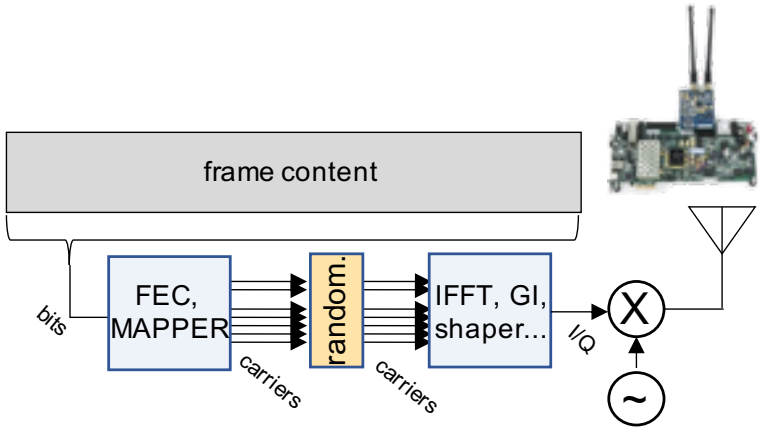
HOWTO NEUTRALIZE THIS?

- "**do something**" so that received CSI appear as **random**
- NN cannot be trained(!), and will not recognize new samples
- I.e., modify OFDM symbols to emulate artificial-**randomized** channel

Neutralization mechanisms: passive/active

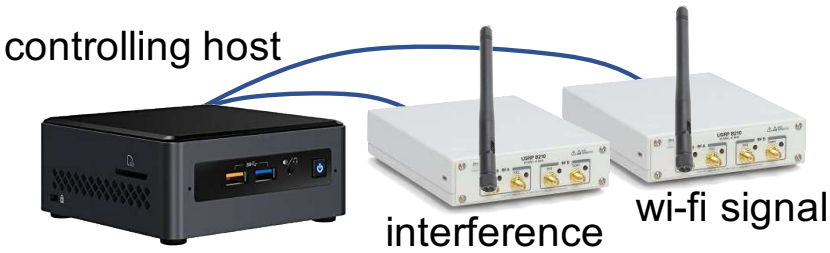
Passive scenario:

- signal randomized per symbol in frequency domain before IFFT
- still retains all 802.11 features for being correctly decoded
- implemented in **openwifi** stack



Active scenario

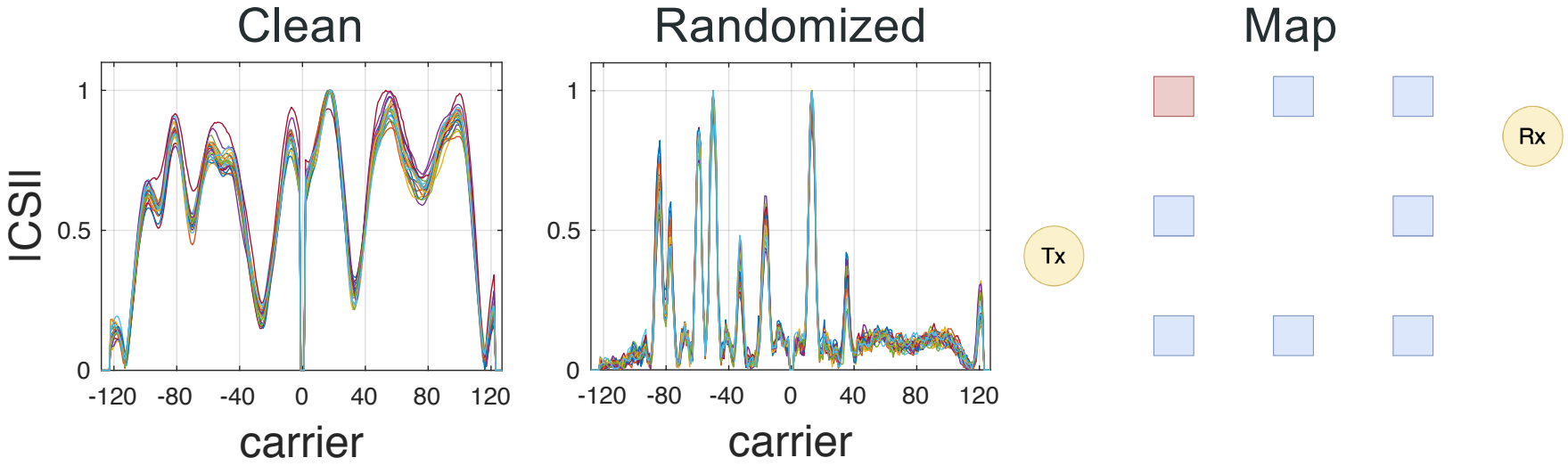
- in parallel to signal transmit/overlap sinusoidal “interference”
- only during physical preamble
- validated with **Matlab**
- implemented on **SDR** (B210)



Neutralization: overview

Target object in different positions

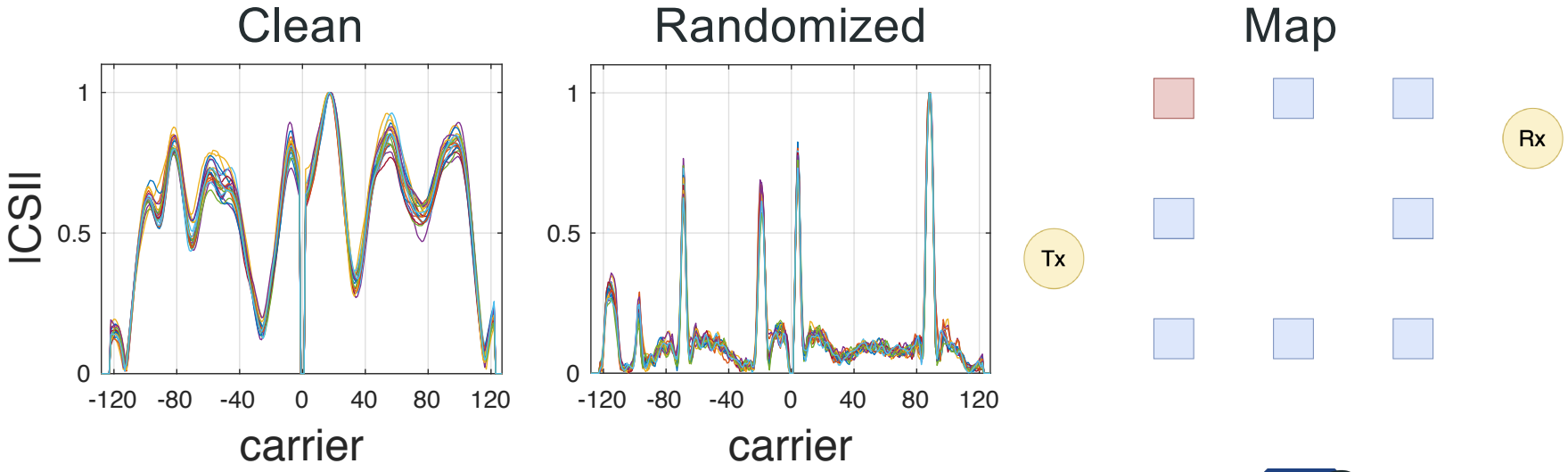
- "Clean CSIs" change very slowly
  - NN still able to distinguish with such soft modifications
- "Randomized CSIs" cannot be distinguished!



Neutralization: overview

Target object in different positions

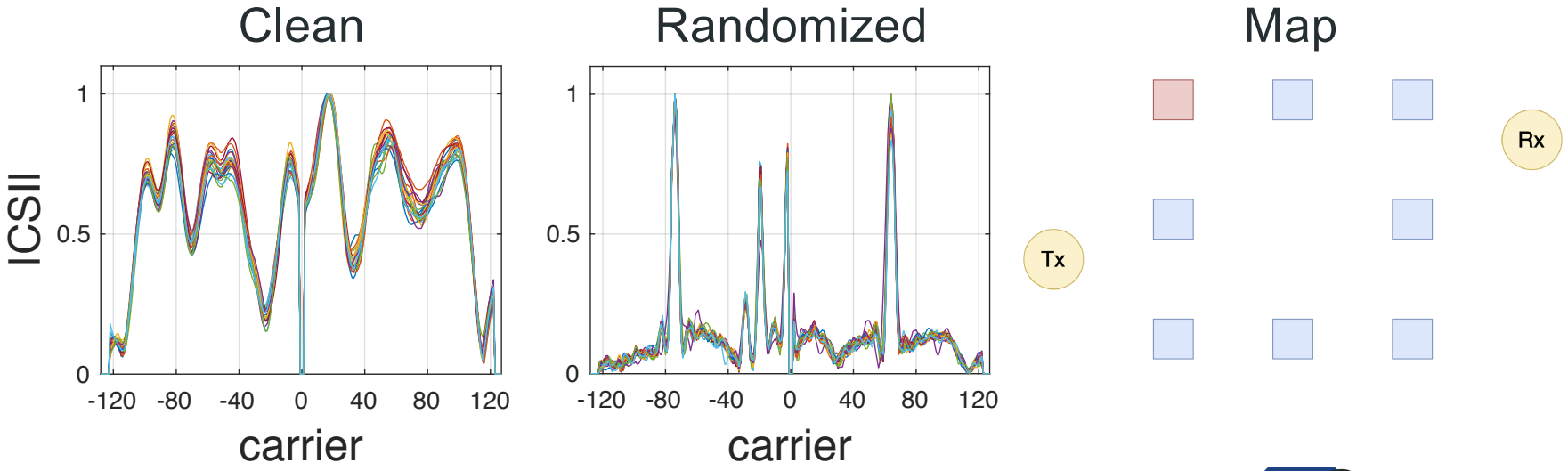
- "Clean CSIs" change very slowly
  - NN still able to distinguish with such soft modifications
- "Randomized CSIs" cannot be distinguished!



Neutralization: overview

Target object in different positions

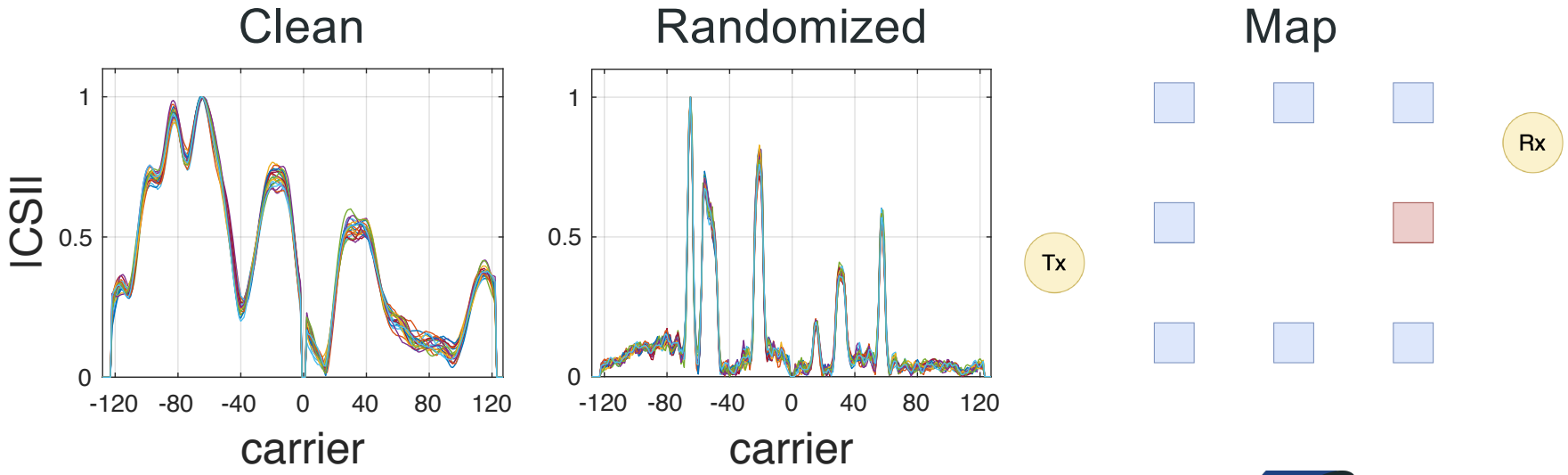
- "Clean CSIs" change very slowly
  - NN still able to distinguish with such soft modifications
- "Randomized CSIs" cannot be distinguished!



Neutralization: overview

Target object in different positions

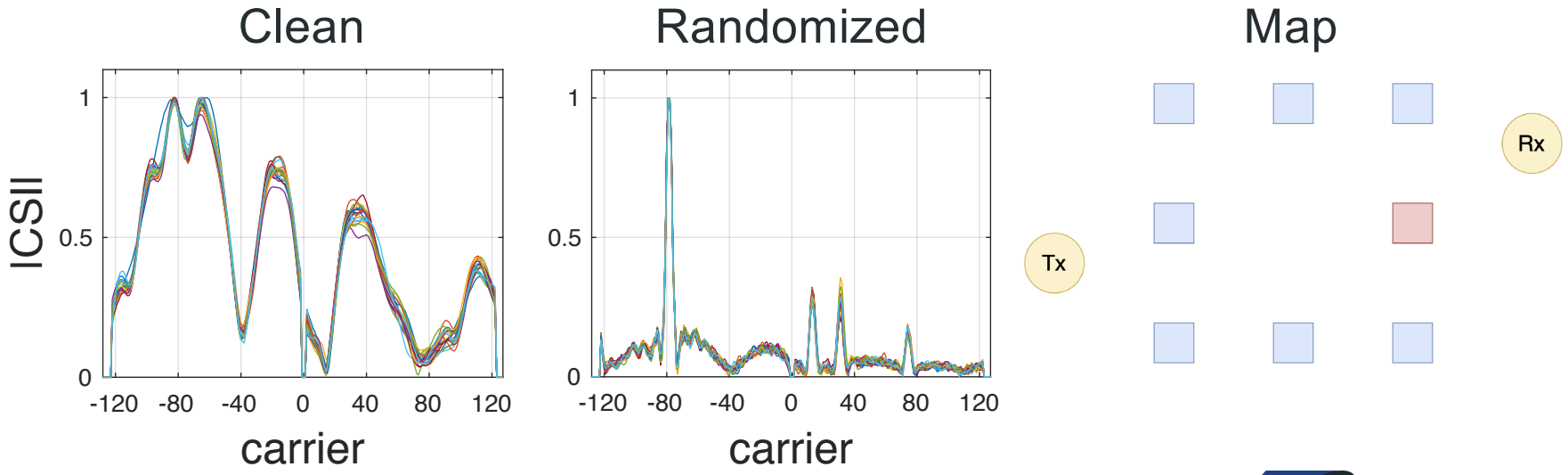
- "Clean CSIs" change very slowly
  - NN still able to distinguish with such soft modifications
- "Randomized CSIs" cannot be distinguished!



Neutralization: overview

Target object in different positions

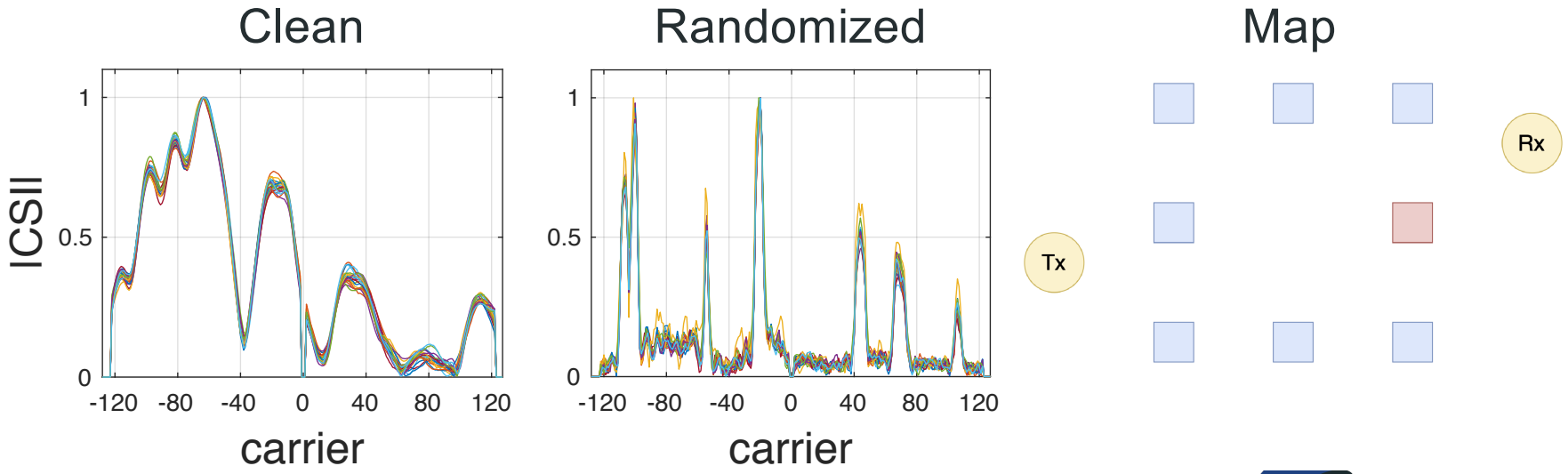
- "Clean CSIs" change very slowly
  - NN still able to distinguish with such soft modifications
- "Randomized CSIs" cannot be distinguished!



Neutralization: overview

Target object in different positions

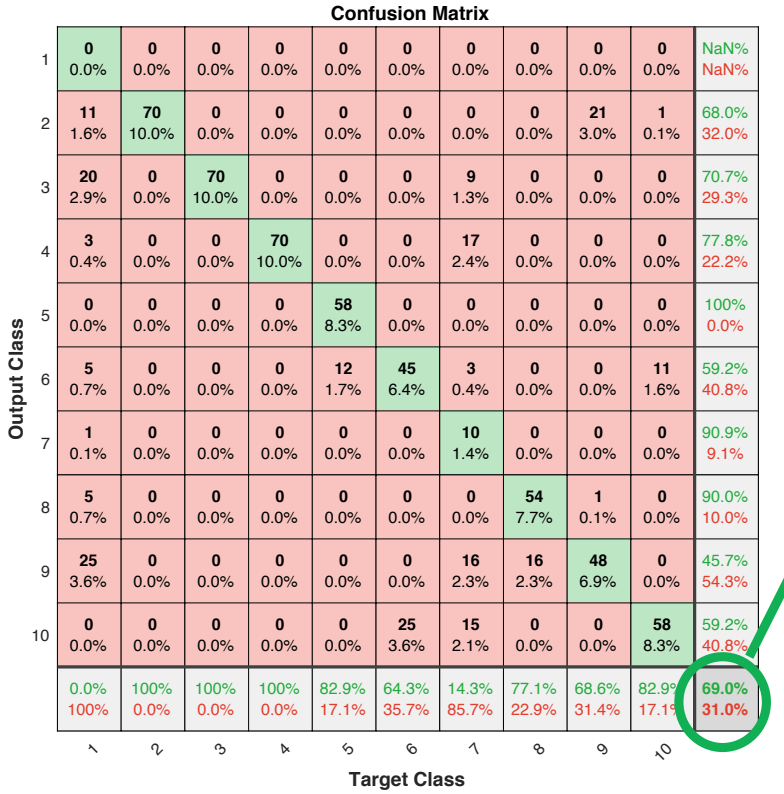
- "Clean CSIs" change very slowly
  - NN still able to distinguish with such soft modifications
- "Randomized CSIs" cannot be distinguished!



Results of the experiments/passive

Classification Accuracy

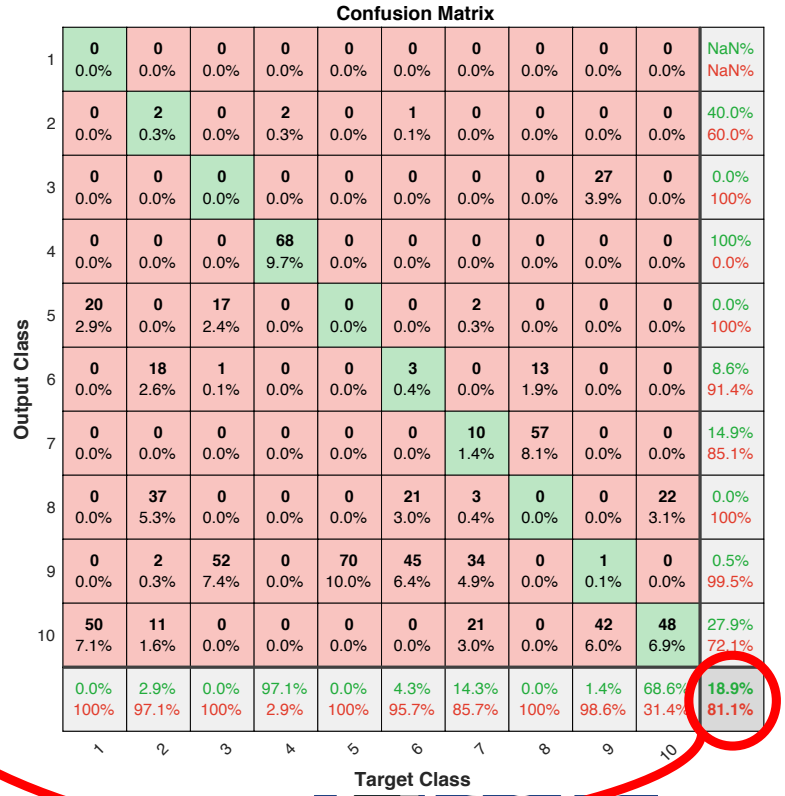
w/o randomization



69.0%

vs

18.9%

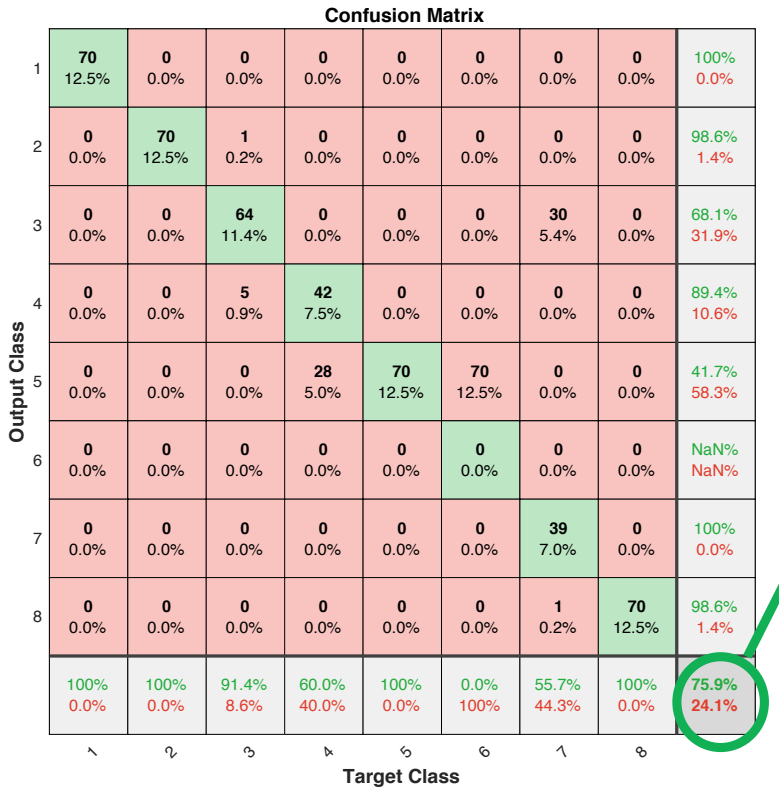


with randomization

Results of the experiments/active

Classification Accuracy

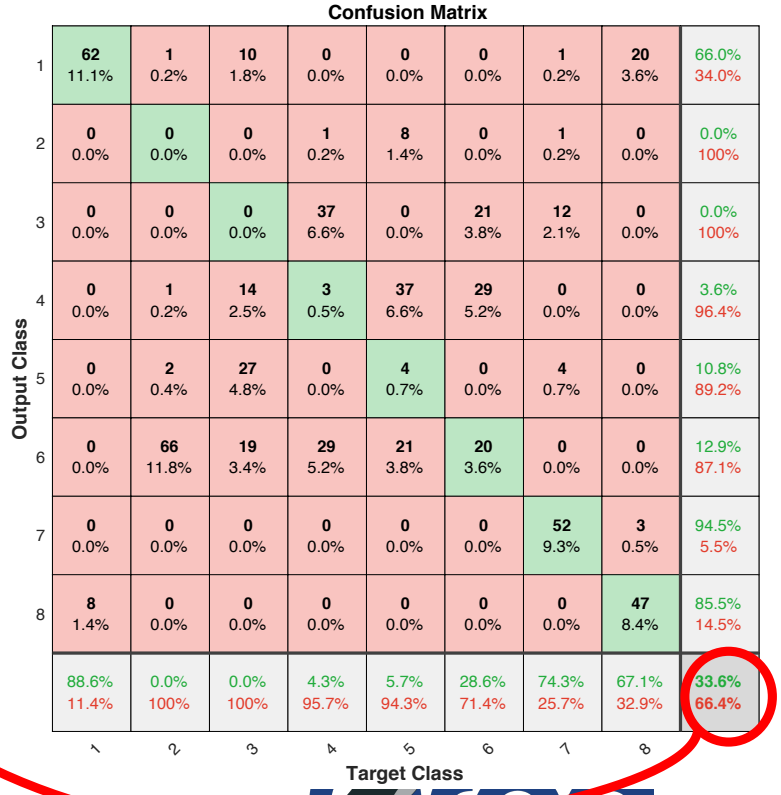
w/o randomization



75.9%

vs

33.6%



with randomization

Conclusions and lessons learnt

- Passive CSI-based localization works in w.iLab.2
  - CNN detects position of targets in the lab
  - **Possible privacy breach** of the users
- Randomization works in w.iLab.2
  - Passive/Active scenarios: randomization technique confuses CNN
  - **Privacy restored** with straightforward signal modification
  - No (limited) effects on rx
- Add CSI collection mechanism to w-iLab.2

Experience with ORCA facility

- Positive experience
  - jFed easy to use for setting up topologies and moving robots
  - Documentation very well written and exhaustive
  - Support from patron extremely professional and timely
  - Possibility to root Nexus 6P was fundamental
- Minor issues
  - Robots sometimes get lost ☺

THANK YOU
FOR YOUR ATTENTION

ORCA-PROJECT.EU

This project received funding from the European Union's Horizon2020
research and innovation programme under grant agreement No 732174