



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

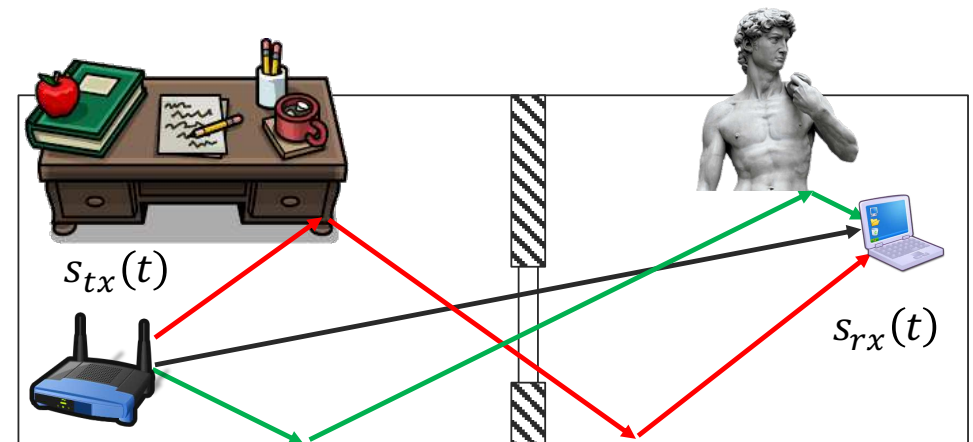
Concept: sensing and privacy

Passive indoor **sensing** is becoming a thing

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

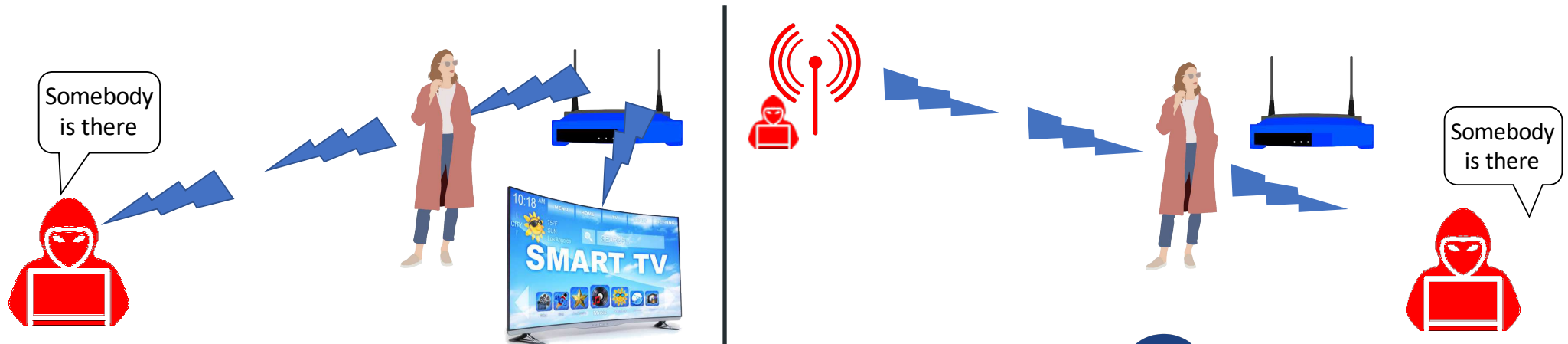
Question: Is **privacy** at risk?

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

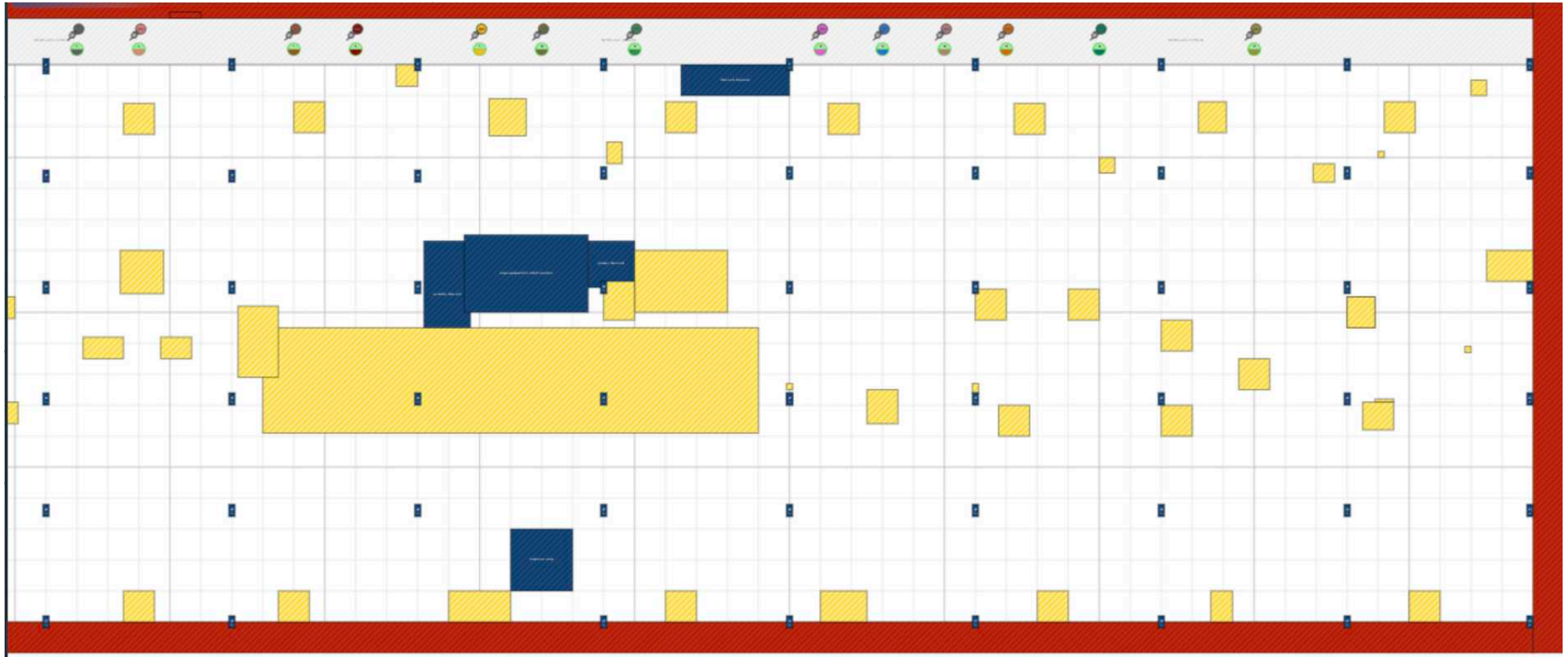


Objectives

- **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)*



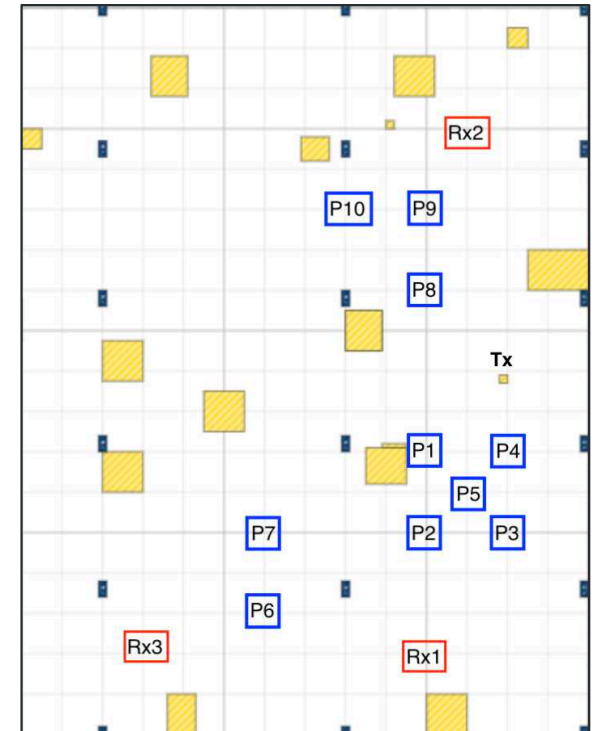
High level functional description: w-iLab.2



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!

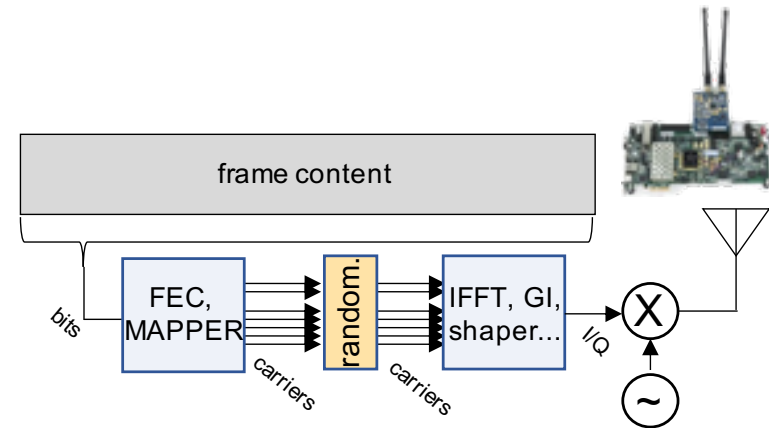
HOWTO NEUTRALIZE THIS?

- "**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

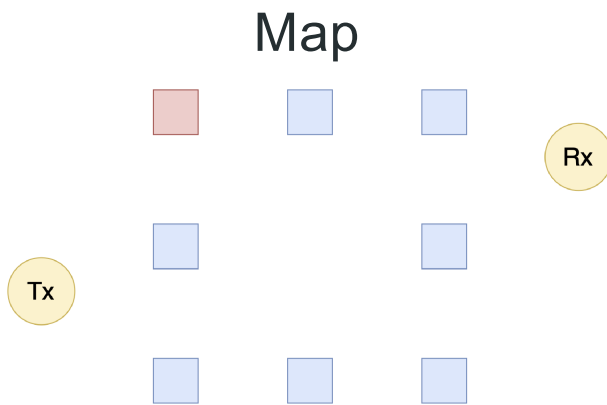
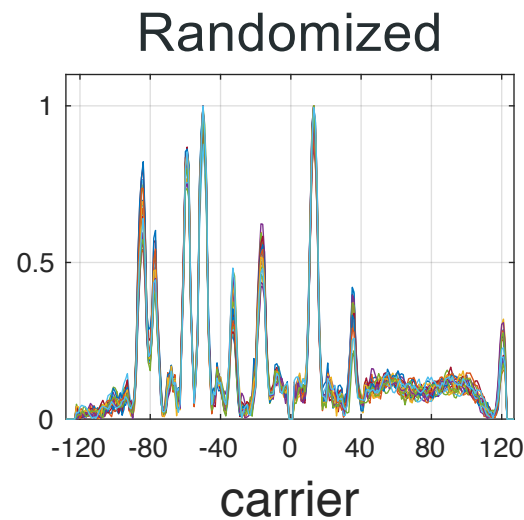
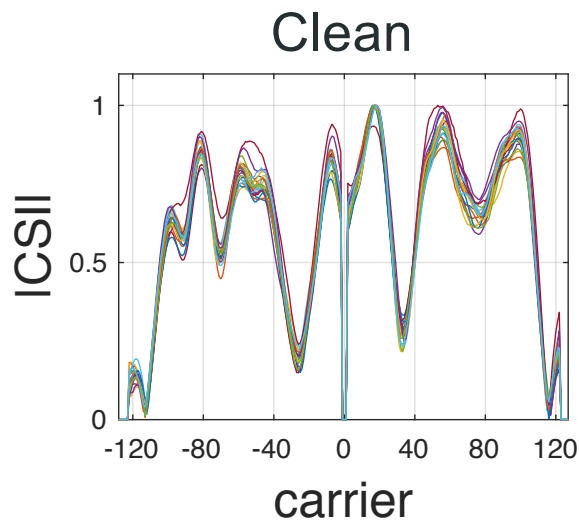
- in parallel to signal transmit/overlap sinusoidal “interference”
- only during physical preamble
- validated with **Matlab**
- implemented on **SDR** (B210)



Neutralization: overview

Target object in different positions

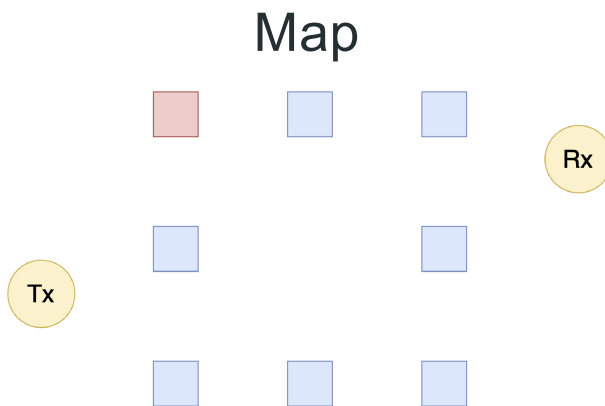
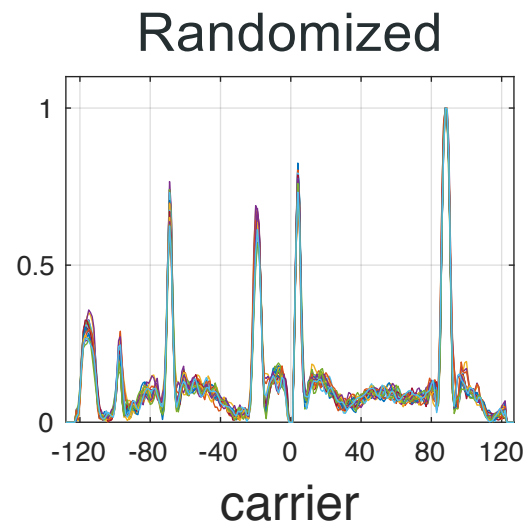
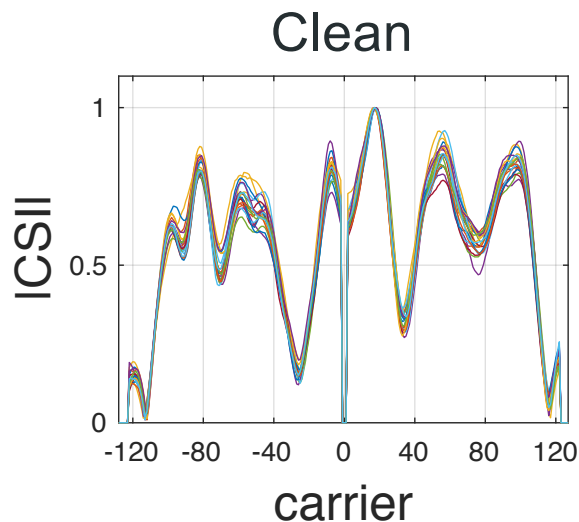
- "Clean CSIs" change very slowly
 - NN still able to distinguish with such soft modifications
- "Randomized CSIs" cannot be distinguished!



Neutralization: overview

Target object in different positions

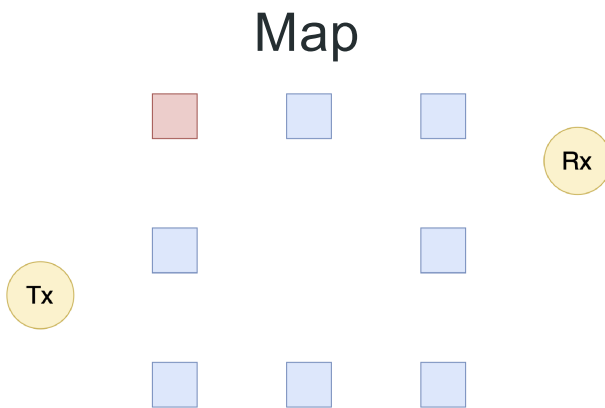
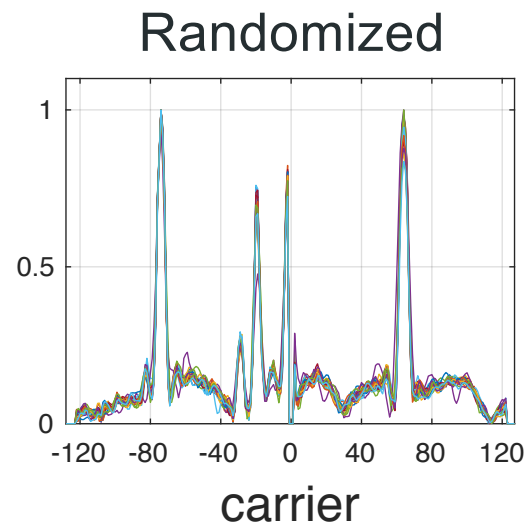
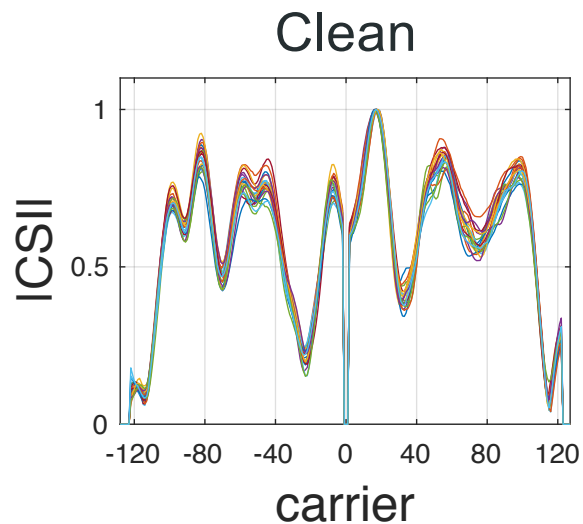
- "Clean CSIs" change very slowly
 - NN still able to distinguish with such soft modifications
- "Randomized CSIs" cannot be distinguished!



Neutralization: overview

Target object in different positions

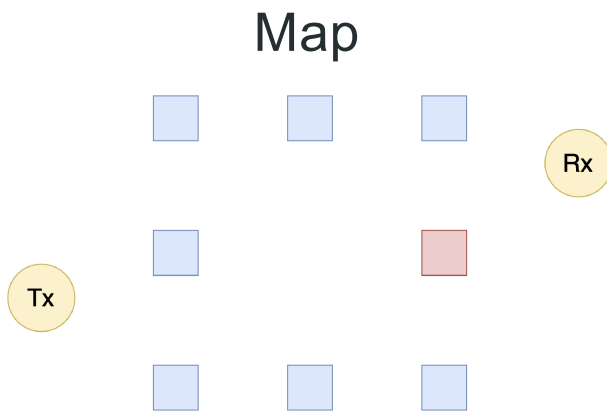
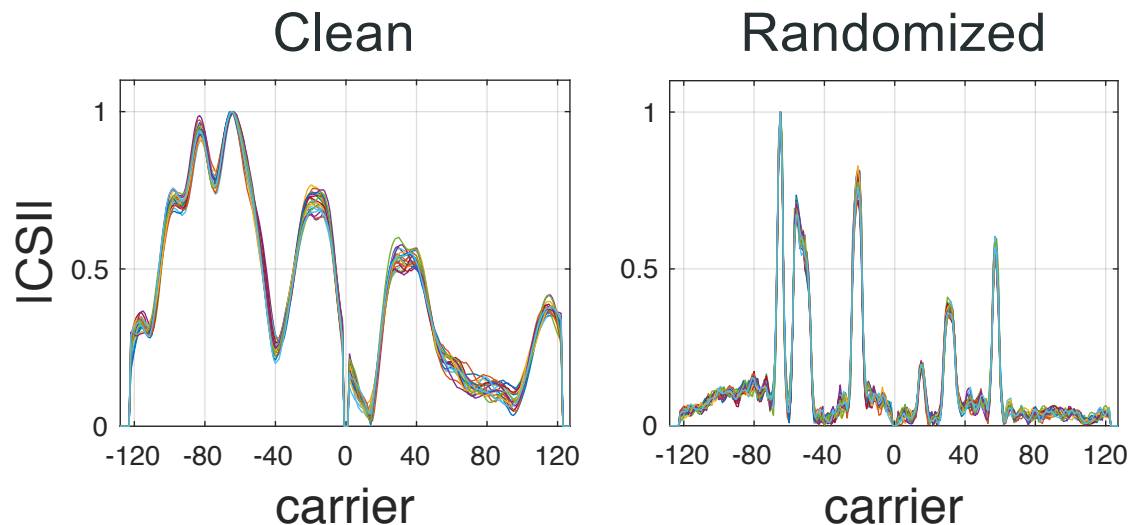
- "Clean CSIs" change very slowly
 - NN still able to distinguish with such soft modifications
- "Randomized CSIs" cannot be distinguished!



Neutralization: overview

Target object in different positions

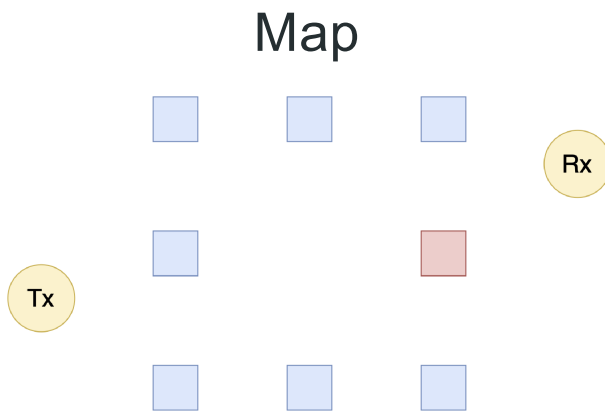
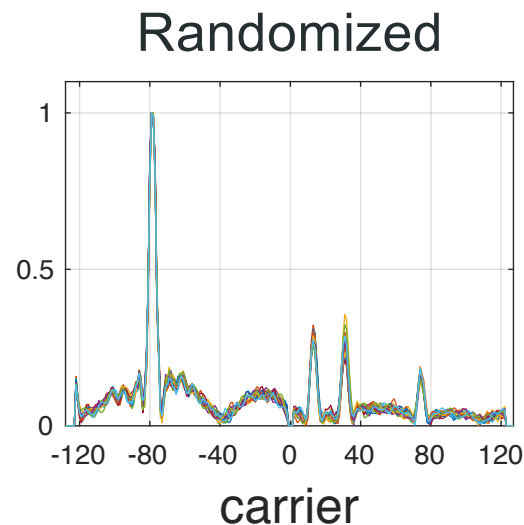
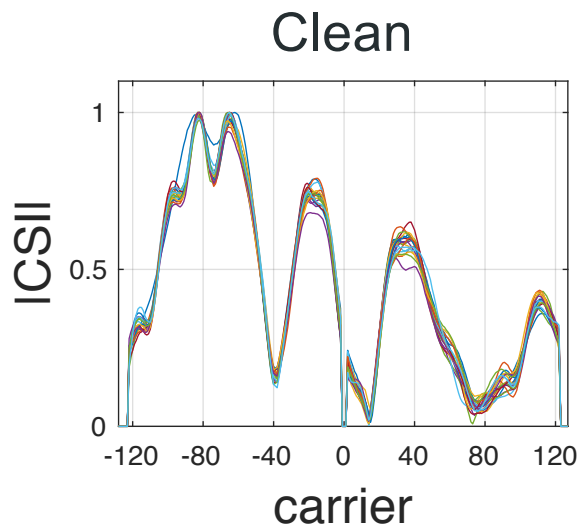
- "Clean CSIs" change very slowly
 - NN still able to distinguish with such soft modifications
- "Randomized CSIs" cannot be distinguished!



Neutralization: overview

Target object in different positions

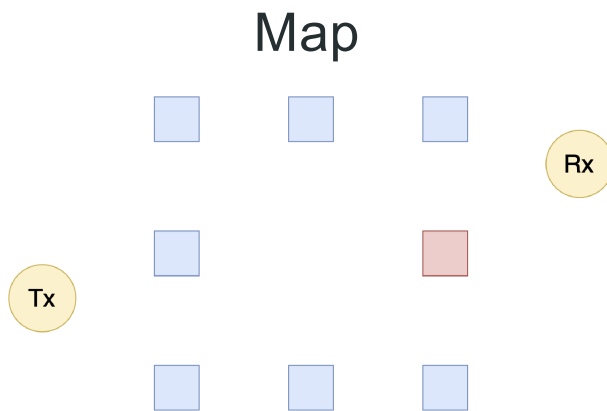
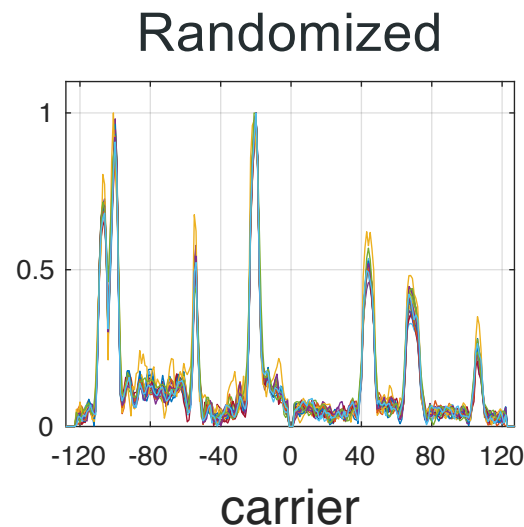
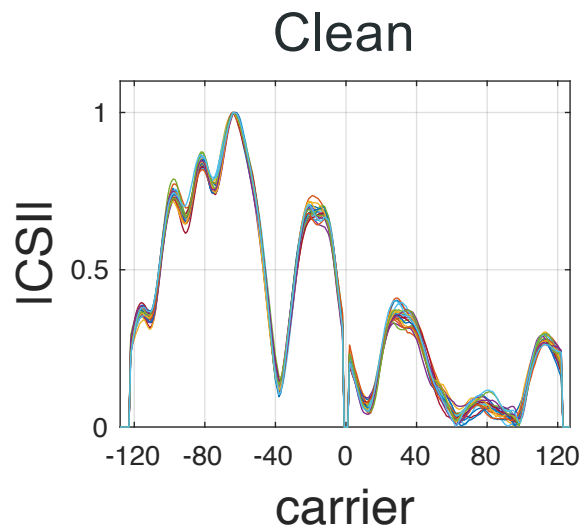
- "Clean CSIs" change very slowly
 - NN still able to distinguish with such soft modifications
- "Randomized CSIs" cannot be distinguished!



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

Confusion Matrix										
Output Class	1	2	3	4	5	6	7	8	9	10
1	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	NaN% NaN%
2	11 1.6%	70 10.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	21 3.0%	1 0.1%	68.0% 32.0%
3	20 2.9%	0 0.0%	70 10.0%	0 0.0%	0 0.0%	0 0.0%	9 1.3%	0 0.0%	0 0.0%	70.7% 29.3%
4	3 0.4%	0 0.0%	0 0.0%	70 10.0%	0 0.0%	0 0.0%	17 2.4%	0 0.0%	0 0.0%	77.8% 22.2%
5	0 0.0%	0 0.0%	0 0.0%	0 0.0%	58 8.3%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
6	5 0.7%	0 0.0%	0 0.0%	0 0.0%	12 1.7%	45 6.4%	3 0.4%	0 0.0%	0 0.0%	59.2% 40.8%
7	1 0.1%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	10 1.4%	0 0.0%	0 0.0%	90.9% 9.1%
8	5 0.7%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	54 7.7%	1 0.1%	90.0% 10.0%
9	25 3.6%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	16 2.3%	16 2.3%	48 6.9%	45.7% 54.3%
10	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	25 3.6%	15 2.1%	0 0.0%	0 0.0%	59.2% 40.8%
	0.0% 100%	100% 0.0%	100% 0.0%	100% 0.0%	82.9% 17.1%	64.3% 35.7%	14.3% 85.7%	77.1% 22.9%	68.6% 31.4%	69.0% 31.0%
Target Class	1	2	3	4	5	6	7	8	9	10

69.0%

VS

18.9%

Confusion Matrix										
Output Class	1	2	3	4	5	6	7	8	9	10
1	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	NaN% NaN%
2	0 0.0%	2 0.3%	0 0.0%	2 0.3%	0 0.0%	1 0.1%	0 0.0%	0 0.0%	0 0.0%	40.0% 60.0%
3	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	27 3.9%	0 0.0%	0.0% 100%
4	0 0.0%	0 0.0%	0 0.0%	68 9.7%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
5	20 2.9%	0 0.0%	17 2.4%	0 0.0%	0 0.0%	2 0.3%	0 0.0%	0 0.0%	0 0.0%	0.0% 100%
6	0 0.0%	18 2.6%	1 0.1%	0 0.0%	0 0.0%	3 0.4%	0 0.0%	13 1.9%	0 0.0%	8.6% 91.4%
7	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	10 1.4%	57 8.1%	0 0.0%	14.9% 85.1%
8	0 0.0%	37 5.3%	0 0.0%	0 0.0%	0 0.0%	21 3.0%	3 0.4%	0 0.0%	0 0.0%	0.0% 100%
9	0 0.0%	2 0.3%	52 7.4%	0 0.0%	70 10.0%	45 6.4%	34 4.9%	0 0.0%	1 0.1%	0.5% 99.5%
10	50 7.1%	11 1.6%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	21 3.0%	0 0.0%	42 6.0%	27.9% 72.1%
	0.0% 100%	2.9% 97.1%	0.0% 100%	97.1% 2.9%	0.0% 100%	4.3% 95.7%	14.3% 85.7%	0.0% 100%	1.4% 98.6%	18.9% 81.1%
Target Class	1	2	3	4	5	6	7	8	9	10

with randomization

Results of the experiments/active

Classification Accuracy

w/o randomization

Confusion Matrix								
Output Class	1	2	3	4	5	6	7	8
1	70 12.5%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0.0%
2	0 0.0%	70 12.5%	1 0.2%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	98.6% 1.4%
3	0 0.0%	0 0.0%	64 11.4%	0 0.0%	0 0.0%	0 0.0%	30 5.4%	68.1% 31.9%
4	0 0.0%	0 0.0%	5 0.9%	42 7.5%	0 0.0%	0 0.0%	0 0.0%	89.4% 10.6%
5	0 0.0%	0 0.0%	0 0.0%	28 5.0%	70 12.5%	70 12.5%	0 0.0%	41.7% 58.3%
6	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	NaN% NaN%
7	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	39 7.0%	100% 0.0%
8	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	1 0.2%	98.6% 1.4%
	100% 0.0%	100% 0.0%	91.4% 8.6%	60.0% 40.0%	100% 0.0%	0.0% 100%	55.7% 44.3%	75.9% 24.1%
Target Class	1	2	3	4	5	6	7	8

75.9%

VS

33.6%

Confusion Matrix								
Output Class	1	2	3	4	5	6	7	8
1	62 11.1%	1 0.2%	10 1.8%	0 0.0%	0 0.0%	0 0.0%	1 0.2%	20 3.6%
2	0 0.0%	0 0.0%	0 0.0%	1 0.2%	8 1.4%	0 0.0%	1 0.2%	0 0.0%
3	0 0.0%	0 0.0%	0 0.0%	37 6.6%	0 0.0%	21 3.8%	12 2.1%	0 0.0%
4	0 0.0%	1 0.2%	14 2.5%	3 0.5%	37 6.6%	29 5.2%	0 0.0%	0 0.0%
5	0 0.0%	2 0.4%	27 4.8%	0 0.0%	4 0.7%	0 0.0%	4 0.7%	0 0.0%
6	0 0.0%	66 11.8%	19 3.4%	29 5.2%	21 3.8%	20 3.6%	0 0.0%	0 0.0%
7	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	52 9.3%	3 0.5%
8	8 1.4%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	47 8.4%
	88.6% 11.4%	0.0% 100%	0.0% 100%	4.3% 95.7%	5.7% 94.3%	28.6% 71.4%	74.3% 25.7%	33.6% 66.4%
Target Class	1	2	3	4	5	6	7	8

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