JOHANNES KEPLER
UNIVERSITÄT LINZ

PHYSICAL TAMPER ATTACK DETECTION IN OFDM SYSTEMS WITH DEEP LEARNING APPROACHES

Eshagh Dehmollaian

Internal Workshop of the Doctoral School 5G Internet of Things

September 7-8, 2021

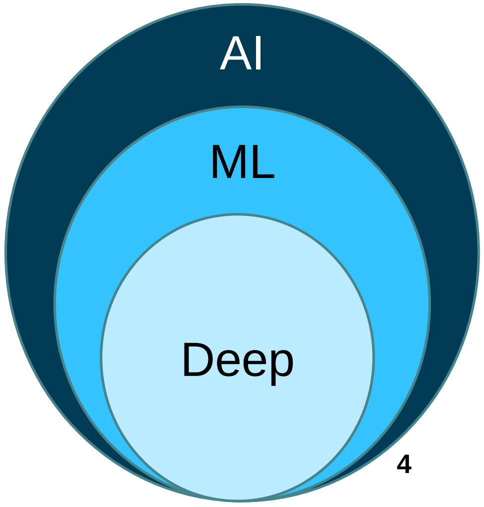
Zoom

Outline

- Introduction
- Physical Tamper Attack Detection
- Results
- Conclusion & Future direction

Introduction

- **critical structures need to be liable even when subjected to unforeseen threats or external attacks [1].**
- **Objectives:**
  - Attack detection, Mitigation, or even prevention
- **Machine learning based anomaly detection**
  - Using Deep Learning Approaches
  - Attack: kind of anomaly



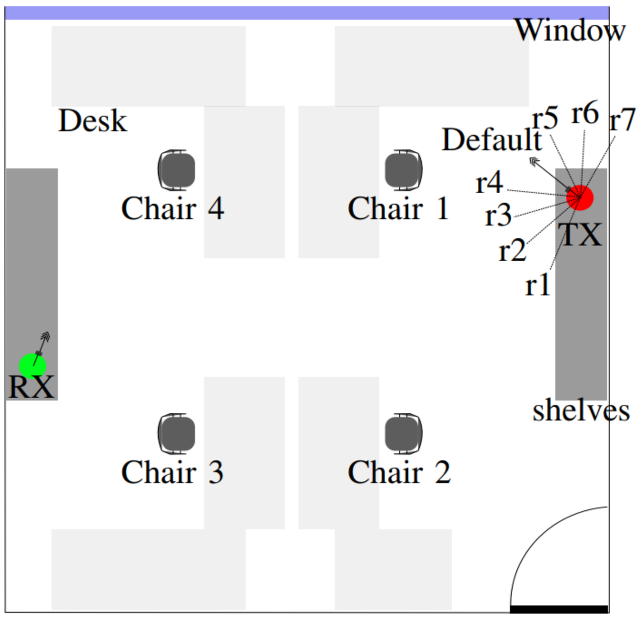
Introduction

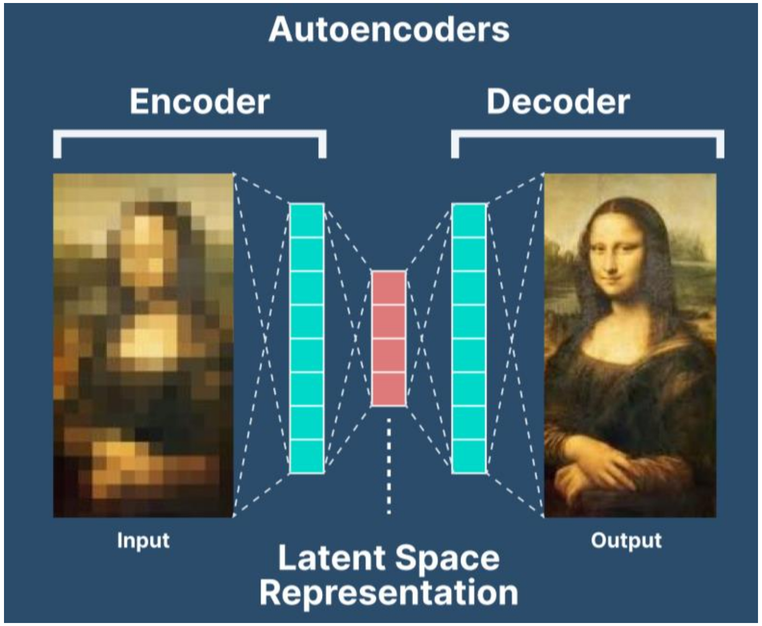
- **WSN**
  - Motivation: change detection
  - Anomalies are unusual measurements for various reasons:
    - faulty sensors
    - actual events
    - faulty communication system among sensors

- **Network Security: Attack Detection**
  - intrusion detection
    - modeling normality
    - any deviation from this model → anomalous case

PHY Tamper Attack Detection

- **Tamper Detection [2]**
  - Using Autoencoders

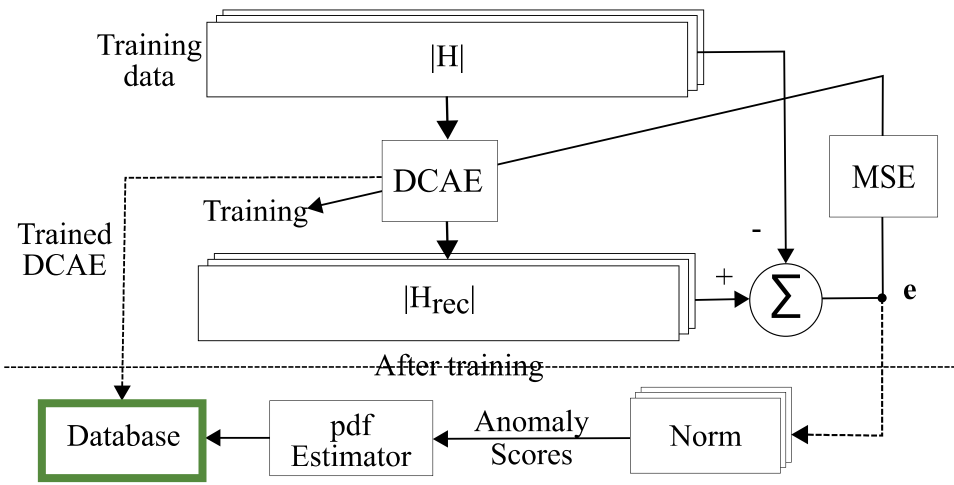




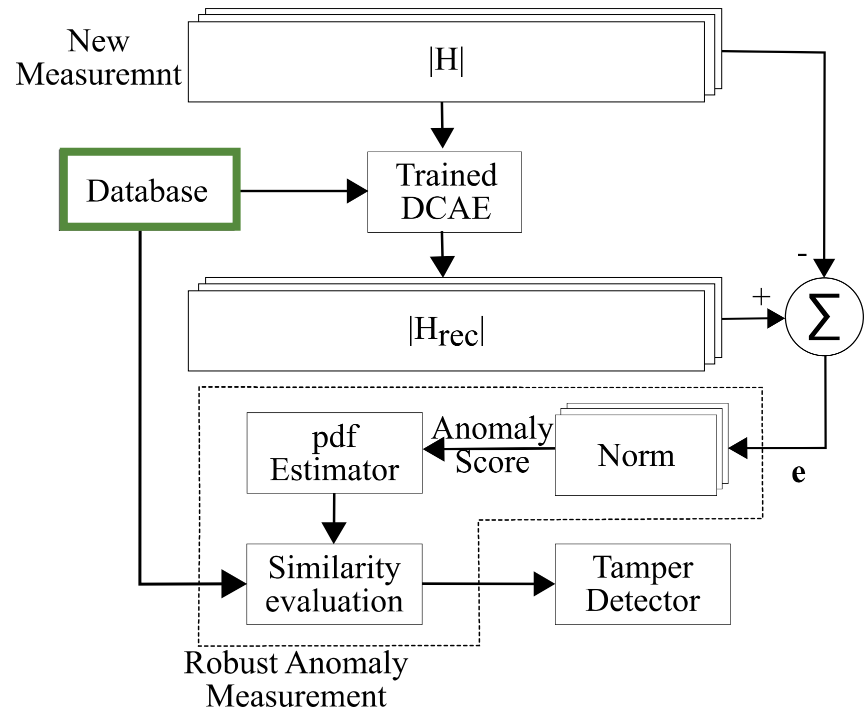
[3]

PHY Tamper Attack Detection

➢ **The Proposed Approach**



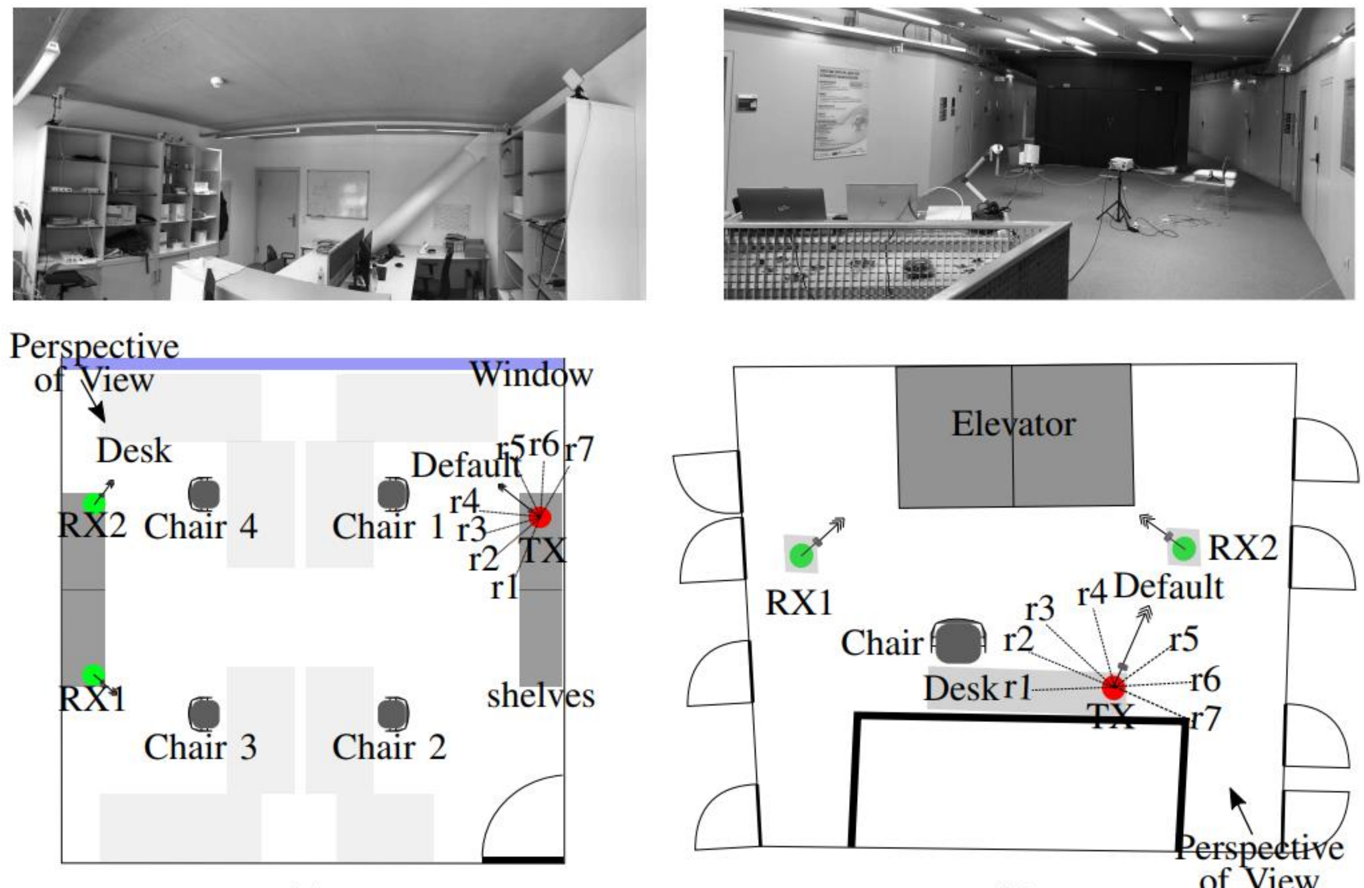
Offline Phase



Online Phase

Results

➢ **Layout**

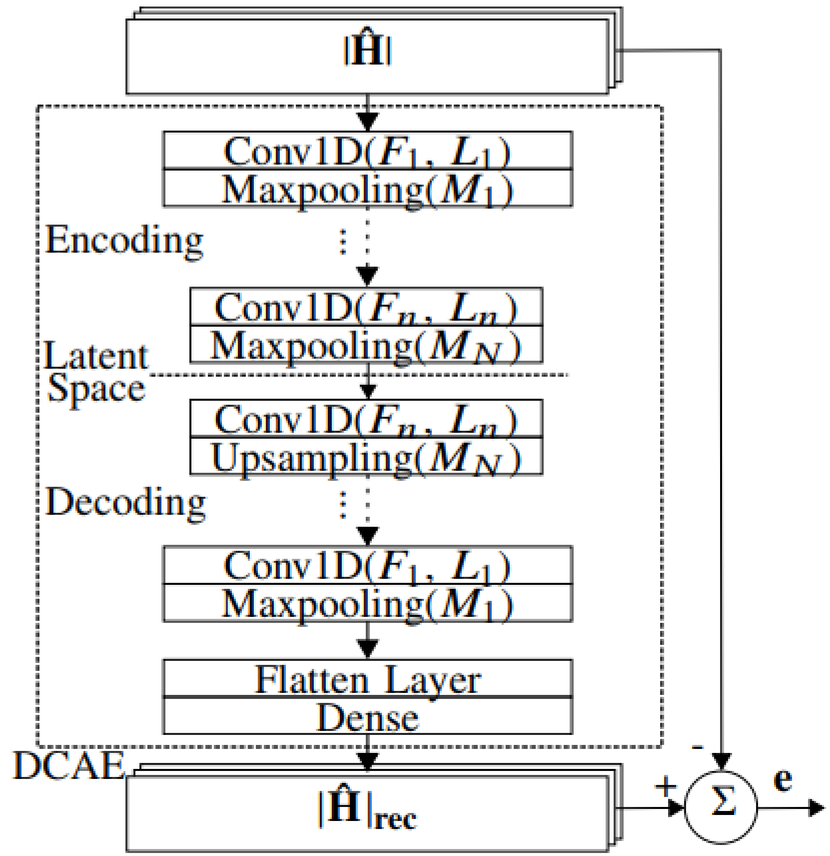


(a) (b)

Results

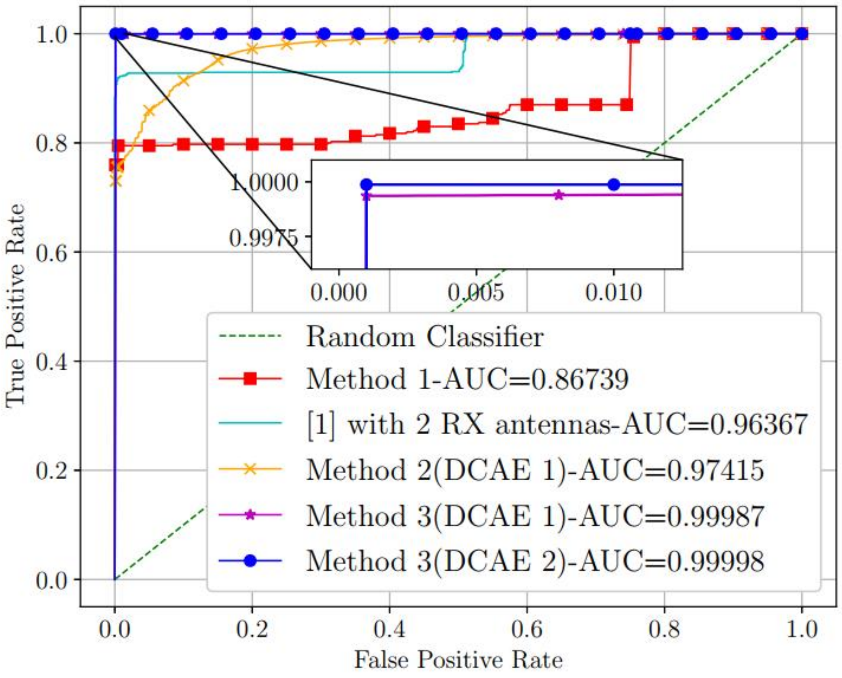
Table I: DCAE parameters

Description	Value
Optimizer	Adam
Batch Size	100
Number of Epochs	20
Learning Rate	0.001
DCAE1= $\begin{bmatrix} F_1 & L_1 & M_1 \\ F_2 & L_2 & M_2 \\ F_3 & L_3 & M_3 \end{bmatrix}$	$\begin{bmatrix} 10 & 52 & 2 \\ 10 & 26 & 2 \\ 10 & 1 & 2 \end{bmatrix}$
DCAE2= $\begin{bmatrix} F_1 & L_1 & M_1 \\ F_2 & L_2 & M_2 \\ F_3 & L_3 & M_3 \\ F_4 & L_4 & M_4 \end{bmatrix}$	$\begin{bmatrix} 10 & 104 & 2 \\ 10 & 52 & 2 \\ 10 & 26 & 2 \\ 10 & 1 & 2 \end{bmatrix}$



Results

- Method 1: Euclidean threshold detection
- Method 2: DCAE with no post processing unit
- Method 3: DCAE with post processing unit



Conclusion & Future Direction

- Suitable Detection Performance compared to the literature

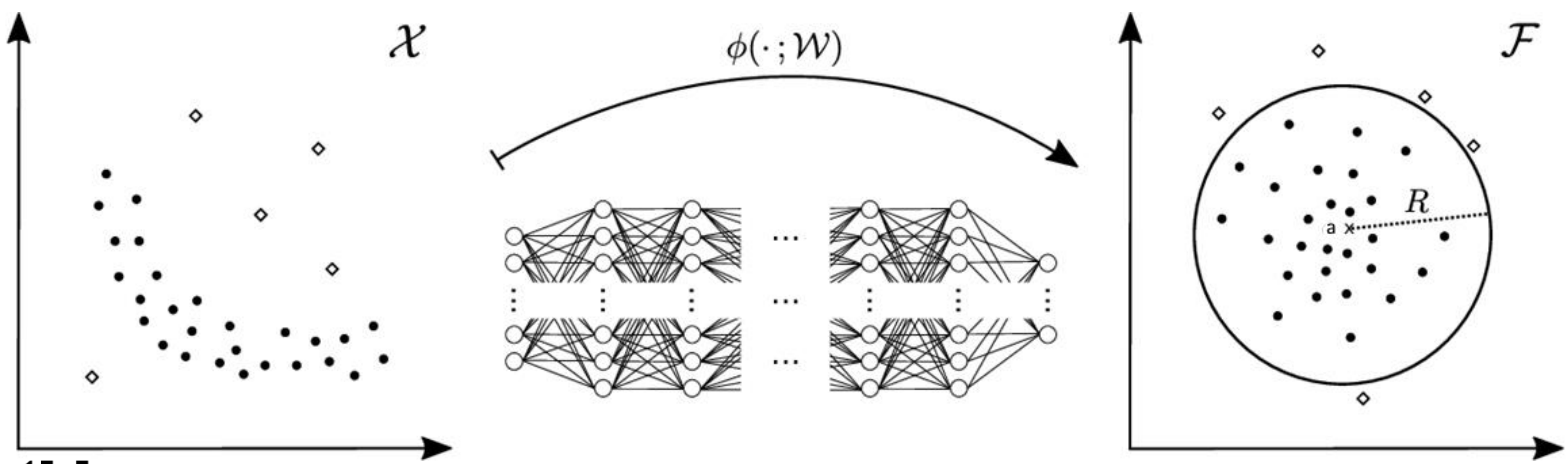
- Fully deep approaches (Deep SVDD)
- Enhanced the proposed method for multiple receivers
- Time and memory complexity

JKU

Conclusion & Future Direction

➢ **Fully deep approaches (Deep SVDD) [4]**

$$\min_{\substack{\|x_i - a\|^2 \leq R^2 + \zeta_i^2, i=1,\dots,n \\ R \in \mathbb{R}, a \epsilon \mathbb{R}^d, \zeta_i \geq 0}} \left\{ R^2 + \frac{1}{\nu n} \sum_{i=1}^{n} \max\{0, \| \phi(x_i, \mathcal{W}) - a \|^2 - R^2\} \right\}$$



References

[1] I. E. Bagci et al., “Using Channel State Information for Tamper Detection in the Internet of Things,” in Proc. Computer Security Applications Conf. (ACSAC), New York, USA, pp. 131–140, Association for Computing Machinery, Dec. 2015.
[2] E. Dehmollaian, *et al.*,” Using Channel State Information for Physical Tamper Attack Detection in OFDM Systems: A Deep Learning Approach,” IEEE Wireless Comm. Letters, Apr. 2021.
[3] v7labs, https://www.v7labs.com/blog/autoencoders-guide, available on 03.09.2021.
[4] L. Ruff *et al.*, “Deep One-Class Classification,” in *Proc*. 35th International Conference on Machine Learning, Stockholm, Sweden, pp. 4393-4402, 2018.

JOHANNES KEPLER
UNIVERSITÄT LINZ

THANK YOU

JOHANNES KEPLER
UNIVERSITÄT LINZ
Altenberger Straße 69
4040 Linz, Österreich
www.jku.at