High-Performance Unsupervised Anomaly Detection for Cyber-Physical System Networks

Peter Schneider, Konstantin Böttinger, October 19, 2018 / CPS-SPC

Fraunhofer
AISEC

Nationales Referenzprojekt
IT-Sicherheit in Industrie 4.0

Anomaly Detection for CPS Networks

Intro

Who	*Peter Schneider*, Konstantin Böttinger
What	Anomaly Detection
When	Online Detection
Where	Cyber-Physical System Networks
Why	High-Performance, Unsupervised
How	Stacked Denoising Autoencoders
For what	Detection in proprietary and/or binary protocols

Anomaly Detection for CPS Networks

Motivation

- Rising number of attacks on cyber-physical systems (CPS)
- 100%-secure systems are impossible
- Network-based Anomaly Detection widely suggested as solution

Anomaly Detection for CPS Networks

The Problem

- Detection systems for business IT already available
- Adaptation of systems to CPS domain still ongoing
- Including domain-specific knowledge should increase detection capabilities

Anomaly Detection for CPS Networks

What happens now

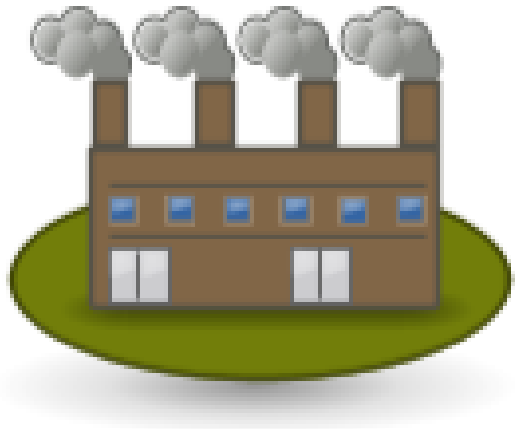


Figure: Insecure manufacturing system.

Anomaly Detection for CPS Networks

What happens now

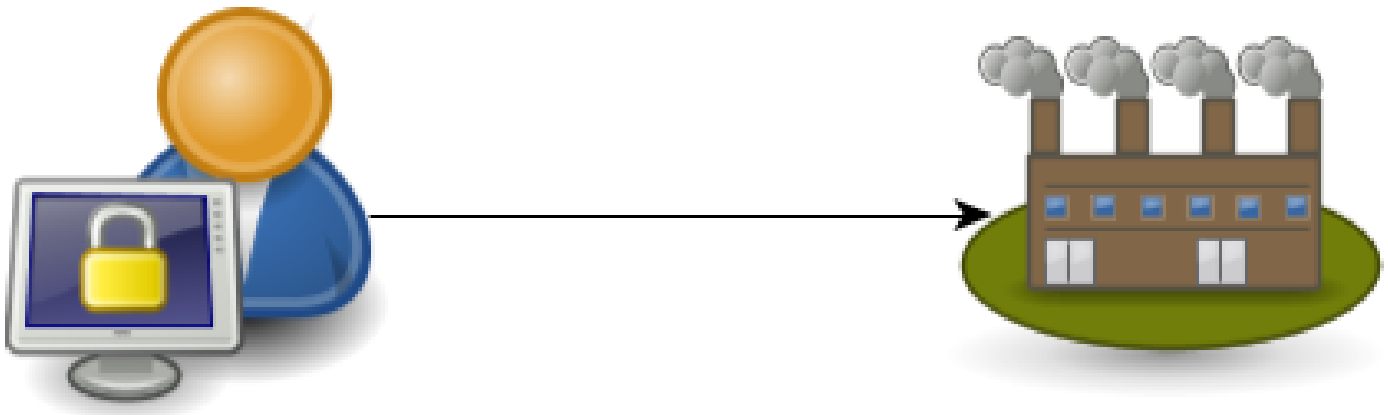


Figure: Secure manufacturing system.

Anomaly Detection for CPS Networks

Challenges

- slow updates
- long product lifetime
- once protected environments
- high damage potential
- specialized attacks
- binary/proprietary protocols

Anomaly Detection for CPS Networks

Challenges

- slow updates
- long product lifetime
- once protected environments
- high damage potential
- specialized attacks
- binary/proprietary protocols

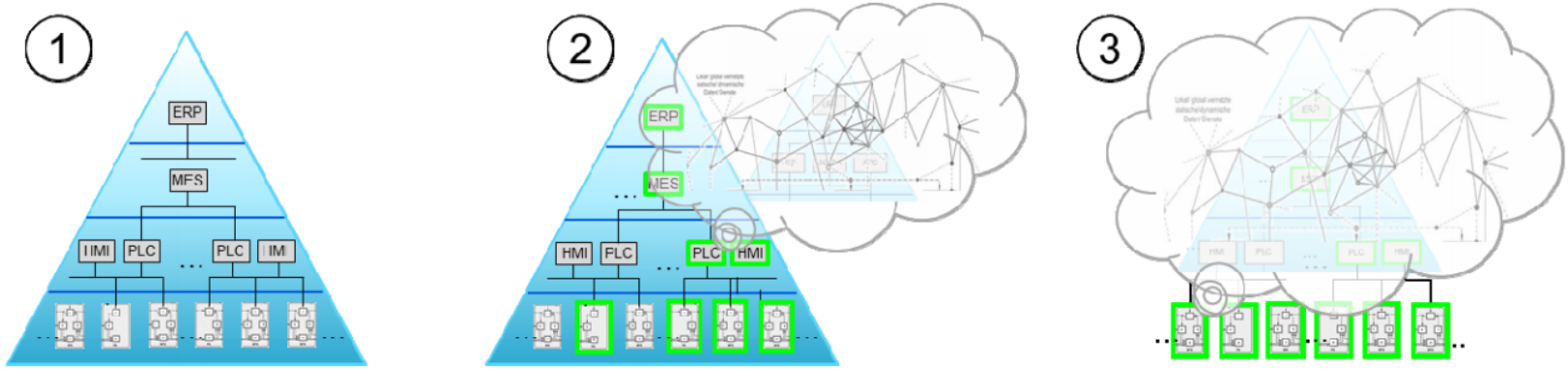


Figure: VDI, Cyber-Physical Systems: Chancen und Nutzen aus Sicht der Automation

Fraunhofer AISEC

Anomaly Detection for CPS Networks

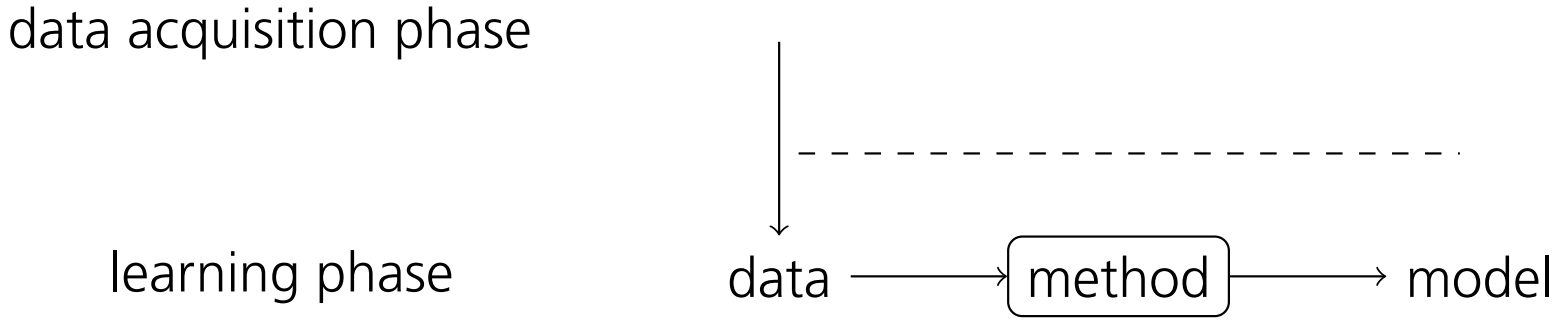
How it is usually done

data acquisition phase

data

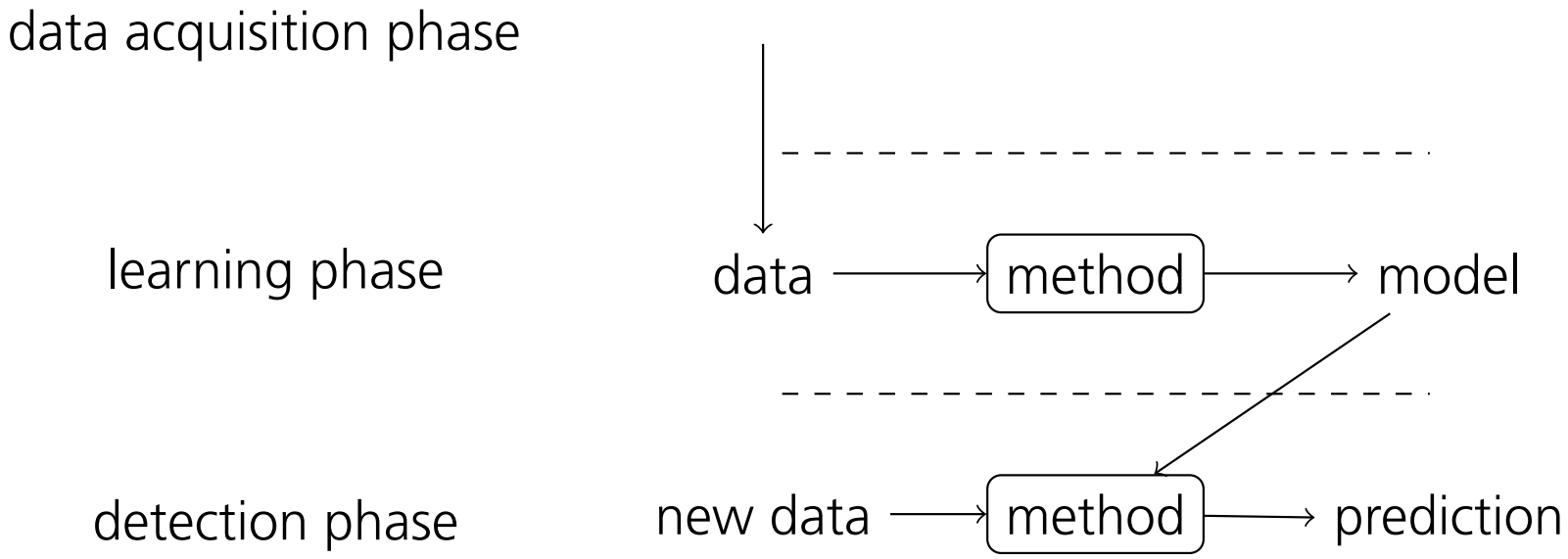
Anomaly Detection for CPS Networks

How it is usually done



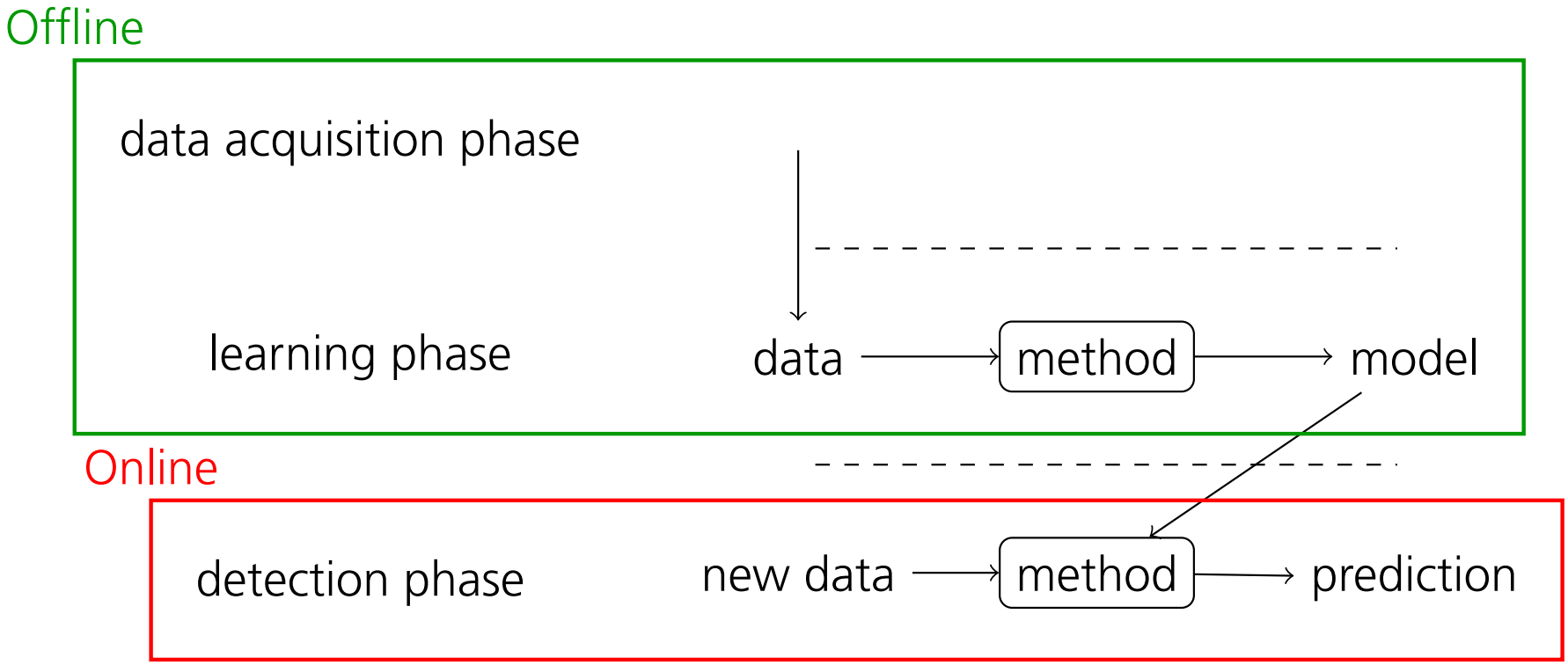
Anomaly Detection for CPS Networks

How it is usually done



Anomaly Detection for CPS Networks

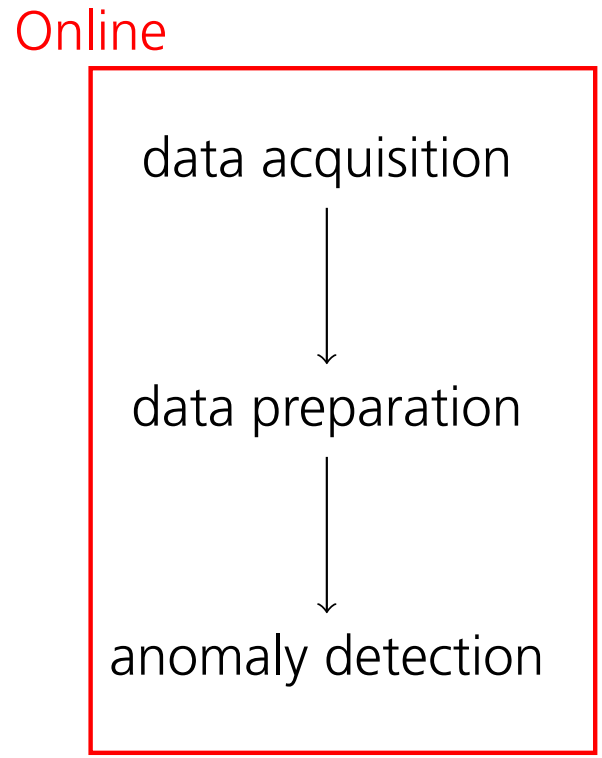
How it is usually done



Fraunhofer AISEC

Anomaly Detection for CPS Networks

How it (not) works



Fraunhofer AISEC

Anomaly Detection for CPS Networks

Performance

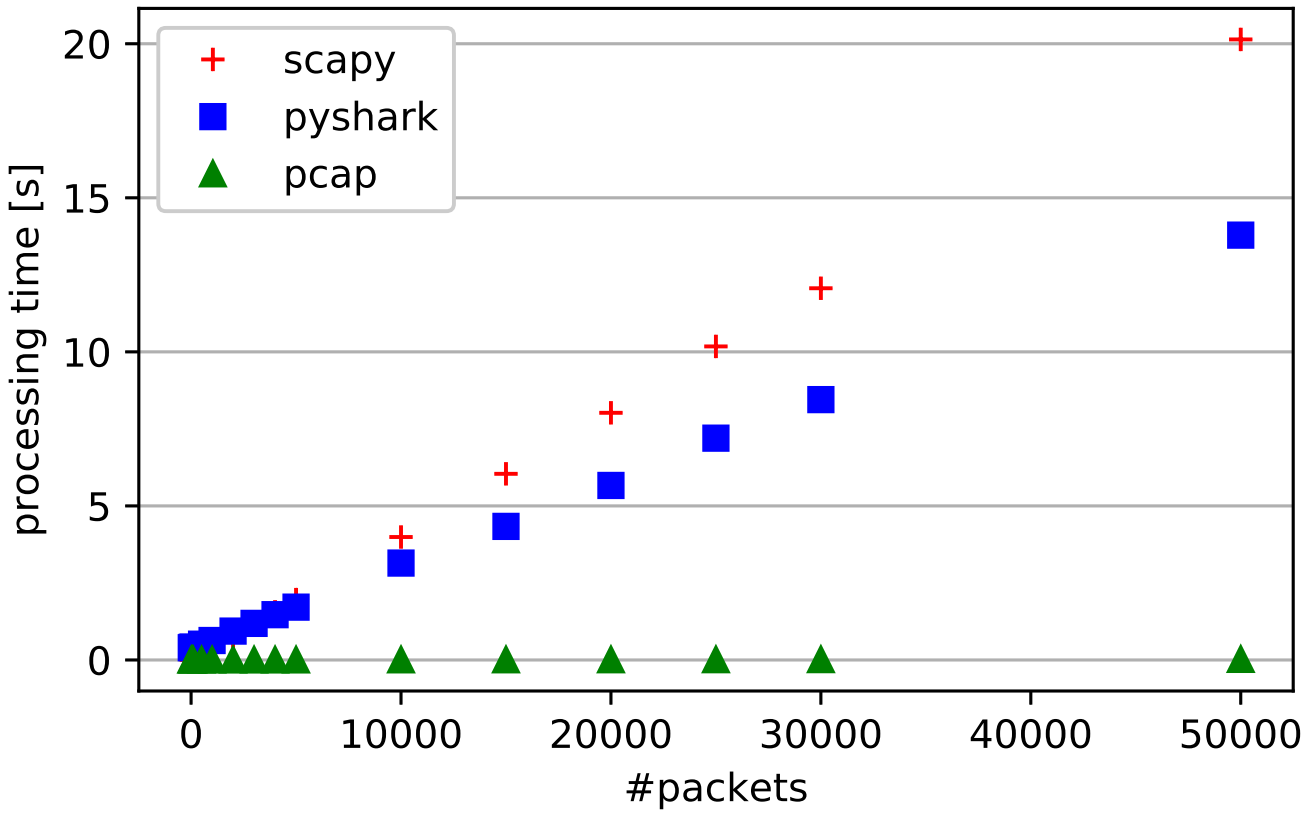


Figure: Performance comparison using different data aggregation strategies.

Fraunhofer AISEC

Anomaly Detection for CPS Networks

Performance

# packets	scapy	pyshark	pcap
1000	0.38*s*	0.63*s*	$< 0.01s$
3000	1.17*s*	1.19*s*	$< 0.01s$
10000	3.99*s*	3.15*s*	$< 0.01s$
50000	20.14*s*	13.79*s*	0.02*s*

Anomaly Detection for CPS Networks

Performance

# packets	scapy	pyshark	pcap
1000	0.38*s*	0.63*s*	$< 0.01s$
3000	1.17*s*	1.19*s*	$< 0.01s$
10000	3.99*s*	3.15*s*	$< 0.01s$
50000	20.14*s*	13.79*s*	0.02*s*

Assumptions bandwidth: $100 Mbit/s$, average packet length: $100 bytes$

Result up to **131072** network packets per second

Fraunhofer AISEC

Anomaly Detection for CPS Networks

Observations

- packet parsing infeasible for larger CPS networks
- classic ML feature extraction not possible

We need a faster solution for **feature extraction** and **anomaly detection**!

Anomaly Detection for CPS Networks

Pipeline

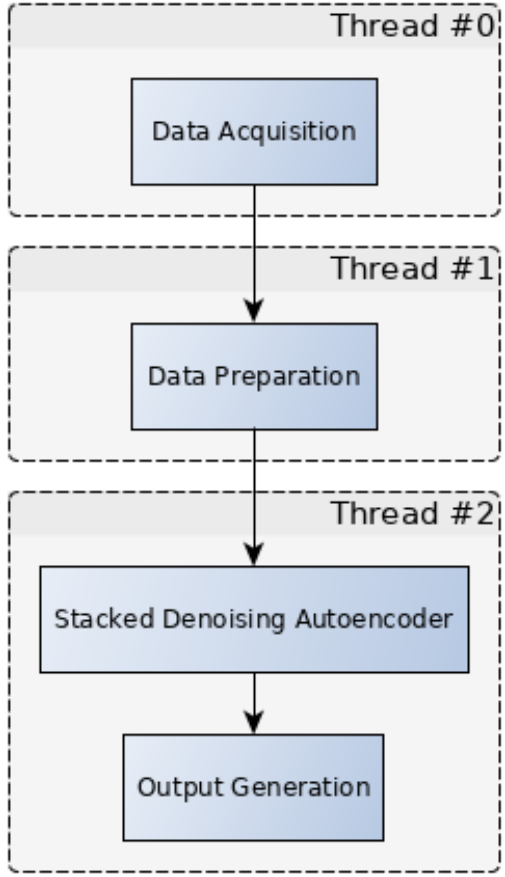


Figure: High-Performance Pipeline

Anomaly Detection for CPS Networks

Pipeline

data acquisition real-time capturing

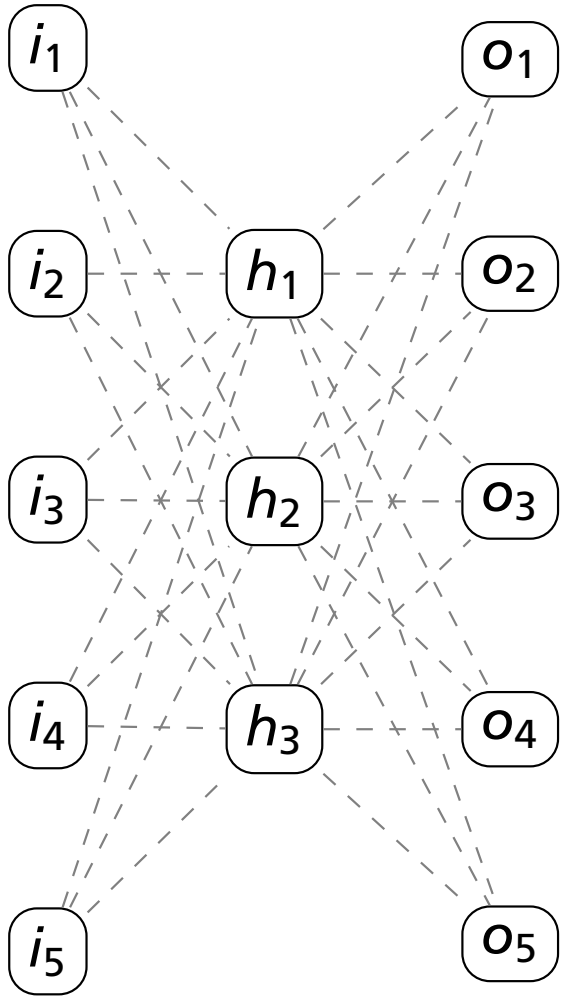
data preparation length cut-off or padding

anomaly detection stacked denoising autoencoders

Fraunhofer AISEC

Anomaly Detection for CPS Networks

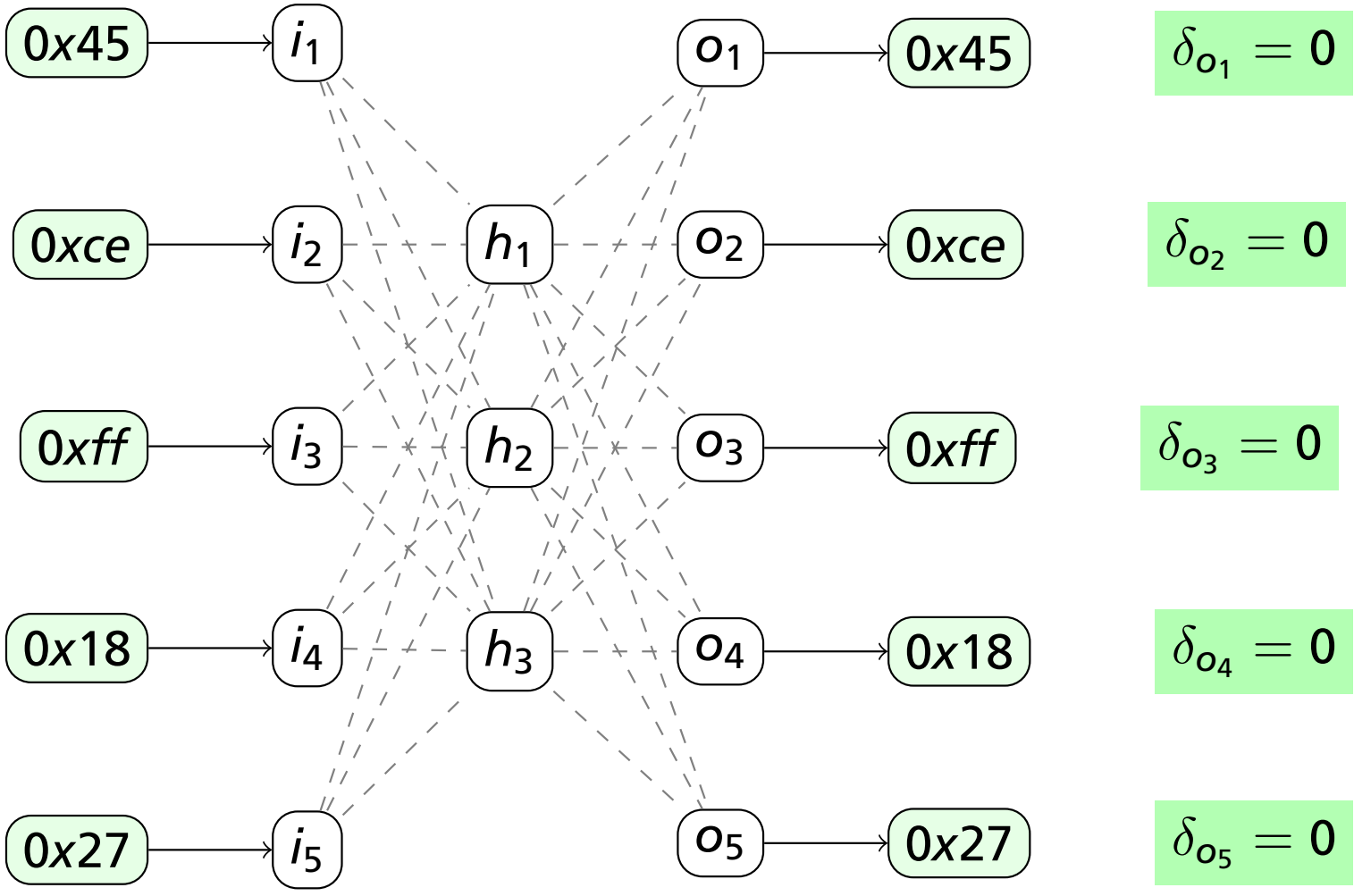
Autoencoder-based Detection



Fraunhofer AISEC

Anomaly Detection for CPS Networks

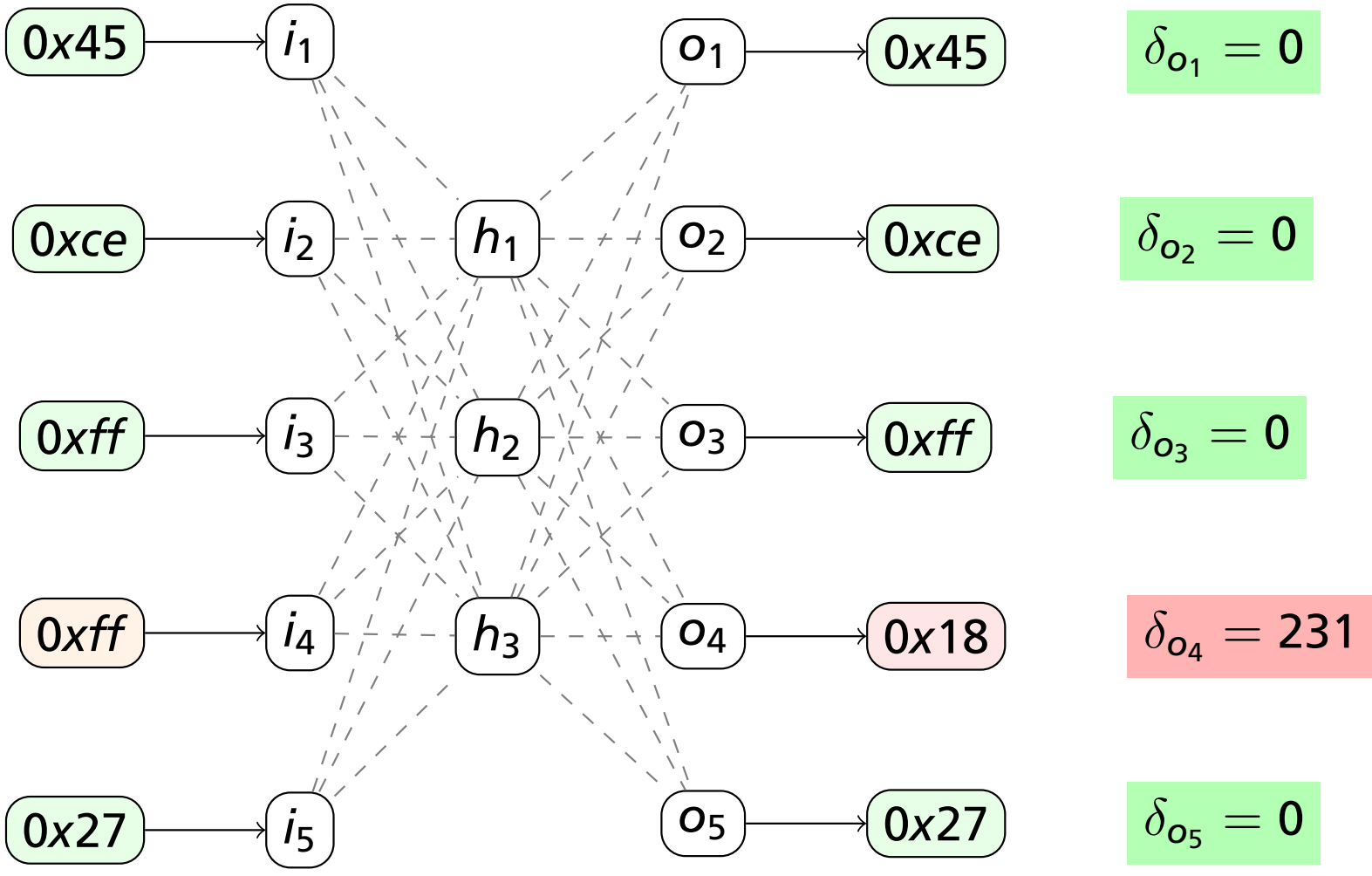
Autoencoder-based Detection



Fraunhofer AISEC

Anomaly Detection for CPS Networks

Autoencoder-based Detection



Fraunhofer AISEC

Anomaly Detection for CPS Networks

SDA

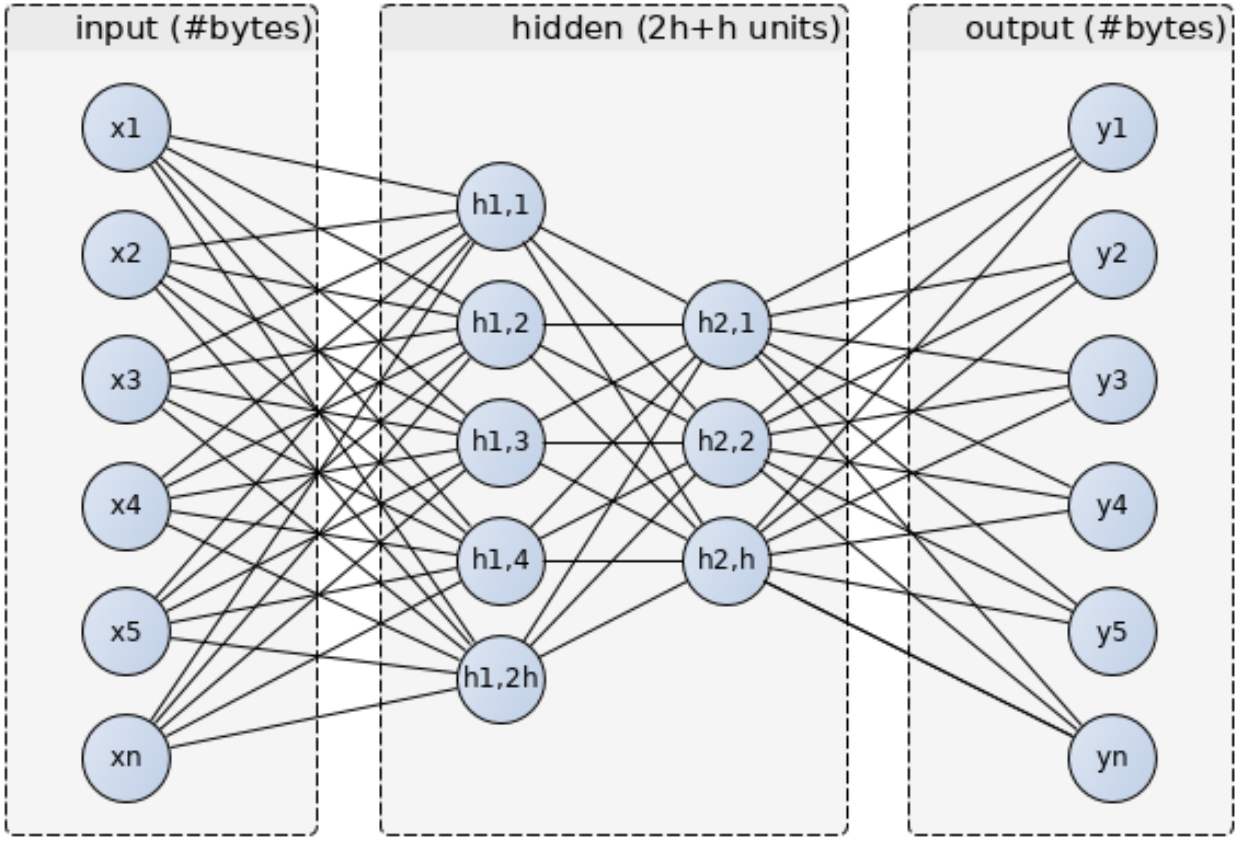


Figure: Stacked auto-encoders.

Fraunhofer AISEC

Anomaly Detection for CPS Networks

Experiments

Modbus dataset

- labeled network packets
- several traces with and without attacks

SWaT dataset

- large dataset (~500GB)
- traces from several days with and without attacks
- pcap traces not labeled

Anomaly Detection for CPS Networks

Modbus dataset – training data

Figure: RMSE on the `run1_3rtu_2s` trace.

Fraunhofer AISEC

Anomaly Detection for CPS Networks

Modbus dataset – validation data

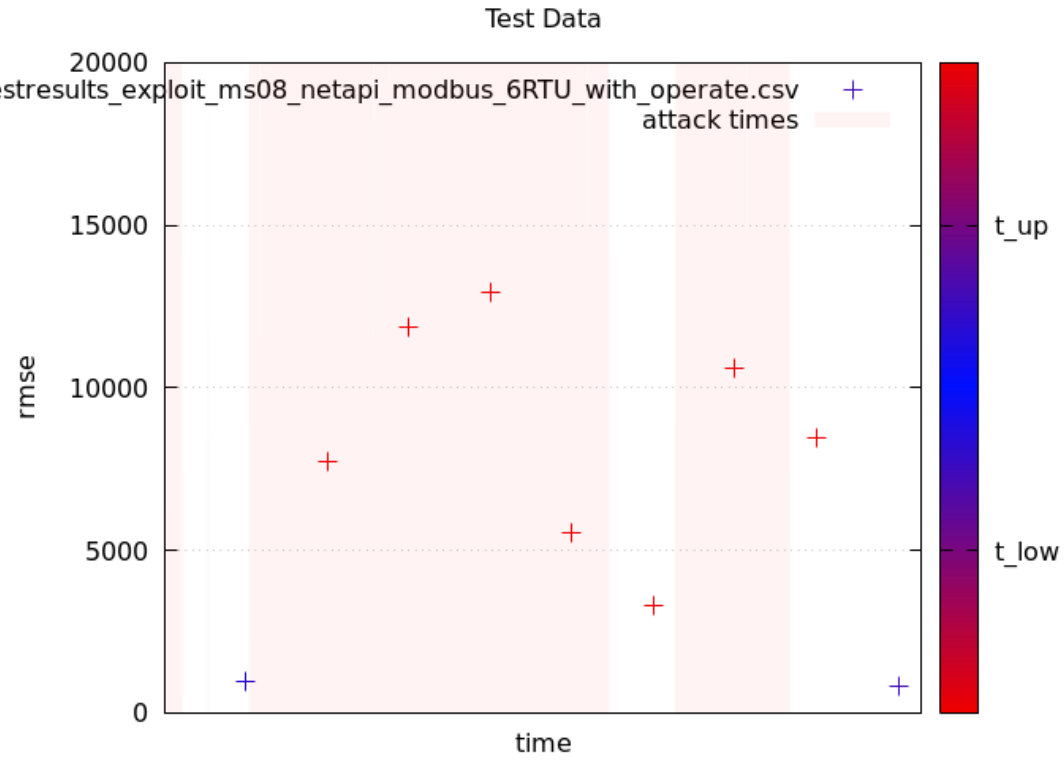


Figure: RMSE on the `exploit_ms08_netapi_modbus_6RTU_with_operate` trace.

Fraunhofer AISEC

Anomaly Detection for CPS Networks

Modbus dataset – validation data

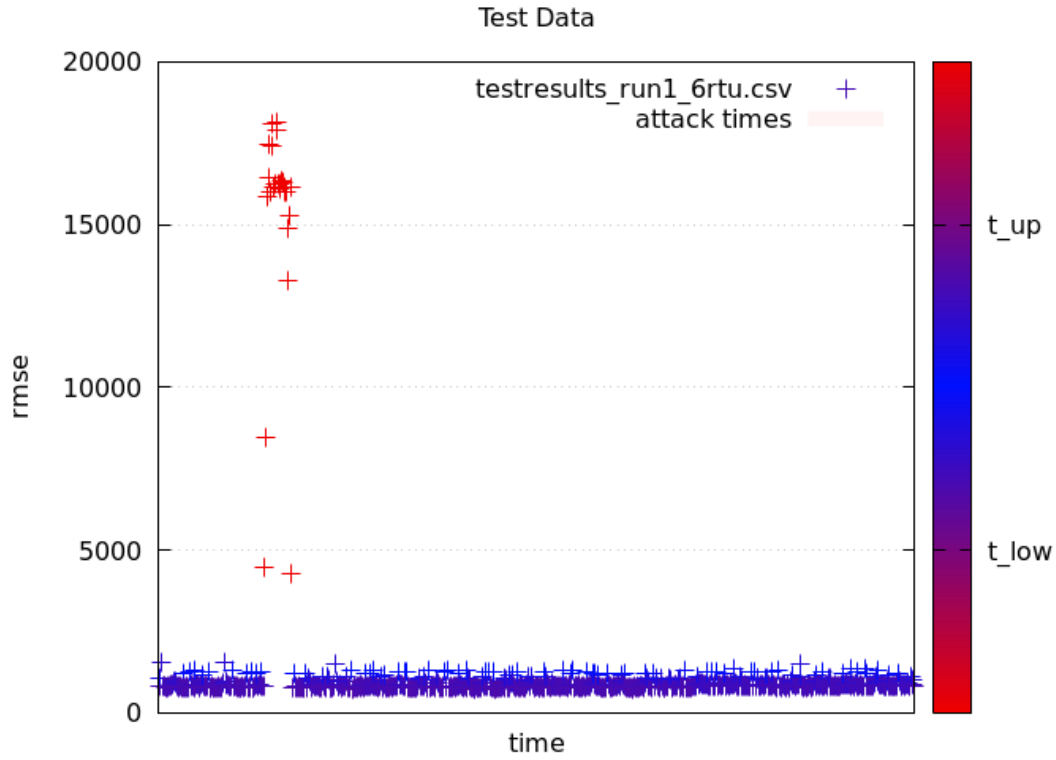


Figure: RMSE on the `run1_6rtu` trace.

Fraunhofer AISEC

Anomaly Detection for CPS Networks

SWaT dataset

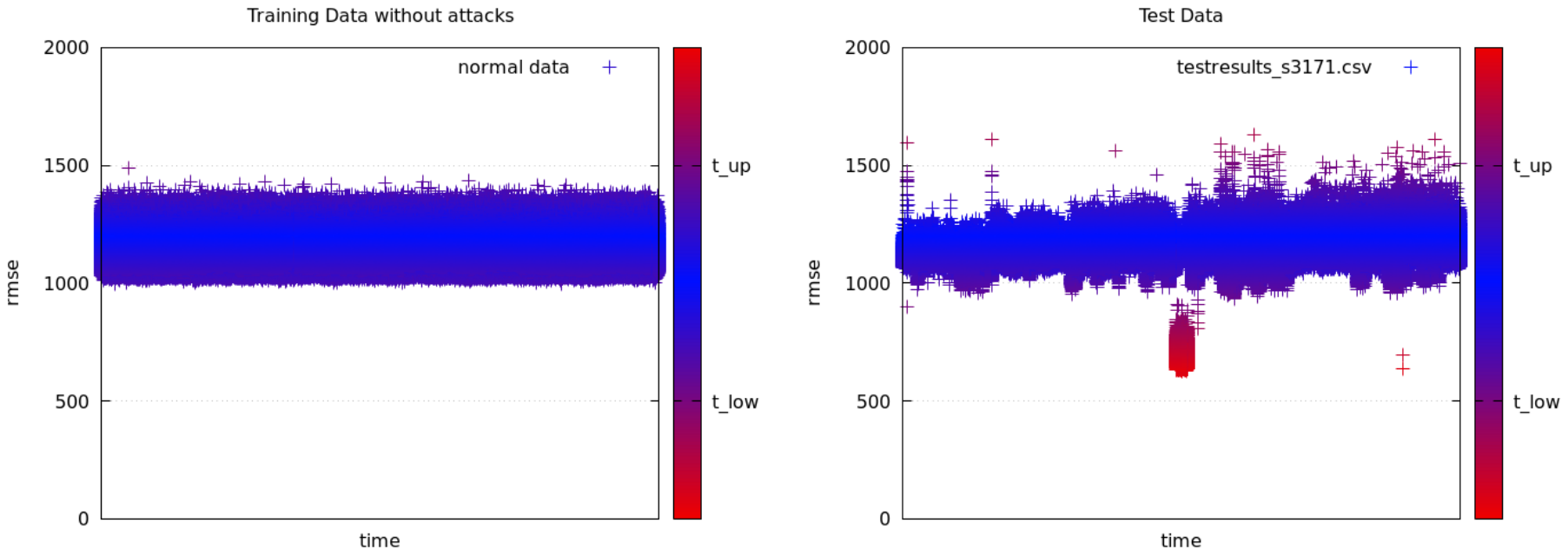
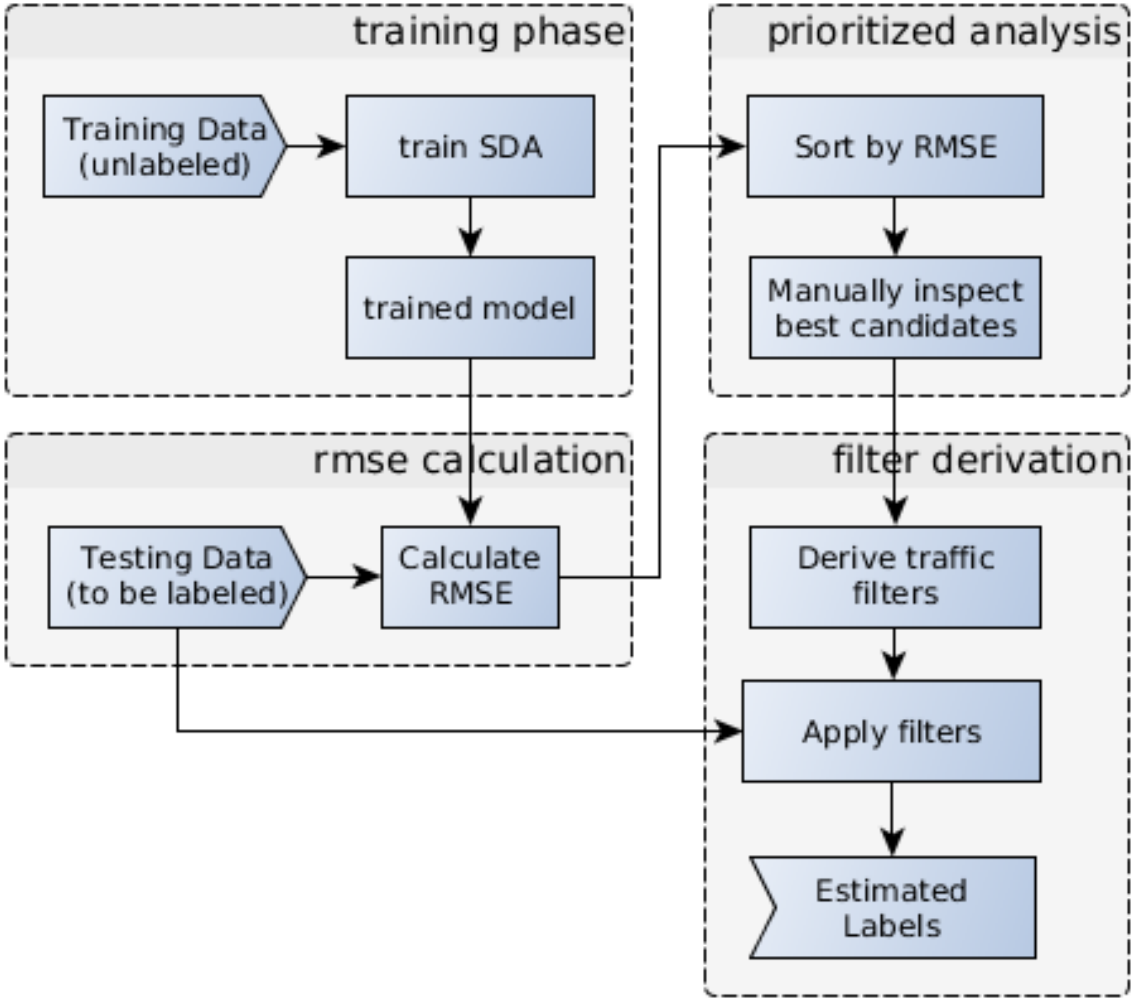


Figure: Results on SWaT dataset.

Fraunhofer AISEC

Anomaly Detection for CPS Networks

Label Estimation



Fraunhofer AISEC

Anomaly Detection for CPS Networks

Labels Estimated

dupack duplicated acknowledgements
tcp.analysis.duplicate_ack

retransmit retransmitted packets
tcp.analysis.retransmission or tcp.analysis.fast_retransmission

unknownproto-tls newly introduced TLS layers
manual analysis

tcpreset connection resets using TCP RST flag
tcp.flags.reset==1

synflood flooding using TCP SYN packets
transum.status=="Response missing" and tcp.connection.syn

Anomaly Detection for CPS Networks

SWaT dataset, detailed results

Line		dupack	retransmit	unknownproto-tls
1	precision	6.38%	2.22%	4.35%
2	recall	3.95%	1.00%	0.38%
3	f1	4.88%	1.38%	0.70%

Table: Anomaly detection performance in problematic scenarios.

Anomaly Detection for CPS Networks

SWaT dataset, detailed results

Line		tcpreset	synflood
1	precision	99.80%	99.80%
2	recall	99.77%	99.99%
3	f1	99.78%	99.89%

Table: Anomaly detection performance in well-working scenarios.

Naive classifier Using packet length $\rightarrow$ 0% f1-score

Fraunhofer AISEC

Anomaly Detection for CPS Networks

Conclusion

Where Cyber-Physical System Networks

→ **SWaT** (EtherNet/IP) and **Modbus** datasets for validation

Anomaly Detection for CPS Networks

Conclusion

Where Cyber-Physical System Networks
→ **SWaT** (EtherNet/IP) and **Modbus** datasets for validation

Why High-Performance
→ fast **data acquisition** omitting packet parsing
Unsupervised
→ **feature learning** using SDAs

Anomaly Detection for CPS Networks

Conclusion

Where Cyber-Physical System Networks
→ **SWaT** (EtherNet/IP) and **Modbus** datasets for validation

Why High-Performance
→ fast **data acquisition** omitting packet parsing
Unsupervised
→ **feature learning** using SDAs

For what Detection in proprietary and/or binary protocols
→ up to **99%** f1-scores

Contact Information

Peter Schneider, Konstantin Böttinger

Product Protection & Industrial Security

Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Parkring 4
85748 Garching (near Munich)
Germany
Internet: http://www.aisec.fraunhofer.de

Phone: +49 89 3229986-142
Fax: +49 89 3229986-222
E-Mail: peter.schneider@aisec.fraunhofer.de

Fraunhofer AISEC