Identification of Cyberattacks in Industrial Control Systems

Alireza Dehlaghi Ghadim

Licentiate Degree

Main Supervisor:
Hans Hansson

Co supervisor:
Ali Balador

Co supervisor
Mahshid Helali Moghadam

Mälardalen University

RI.SE
Research Institutes of Sweden

Outline

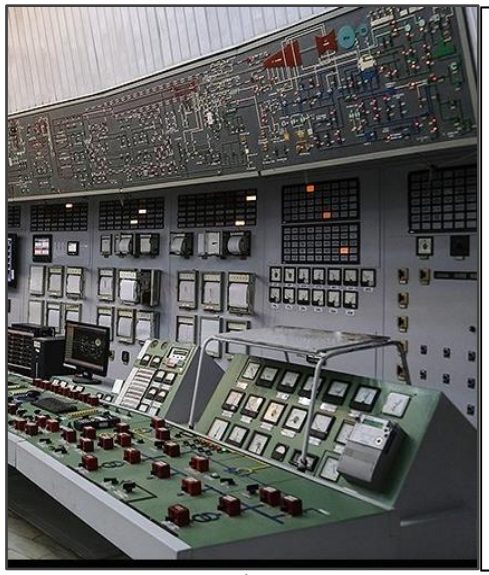
1- Introduction
2- Thesis goals
3- Paper A
4- Paper B
5- Paper C
6- Paper D
7- Conclusion and Future works

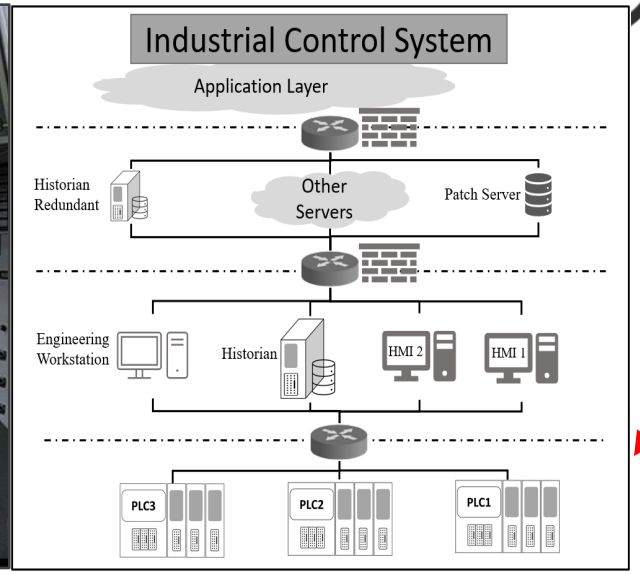
1- Introduction

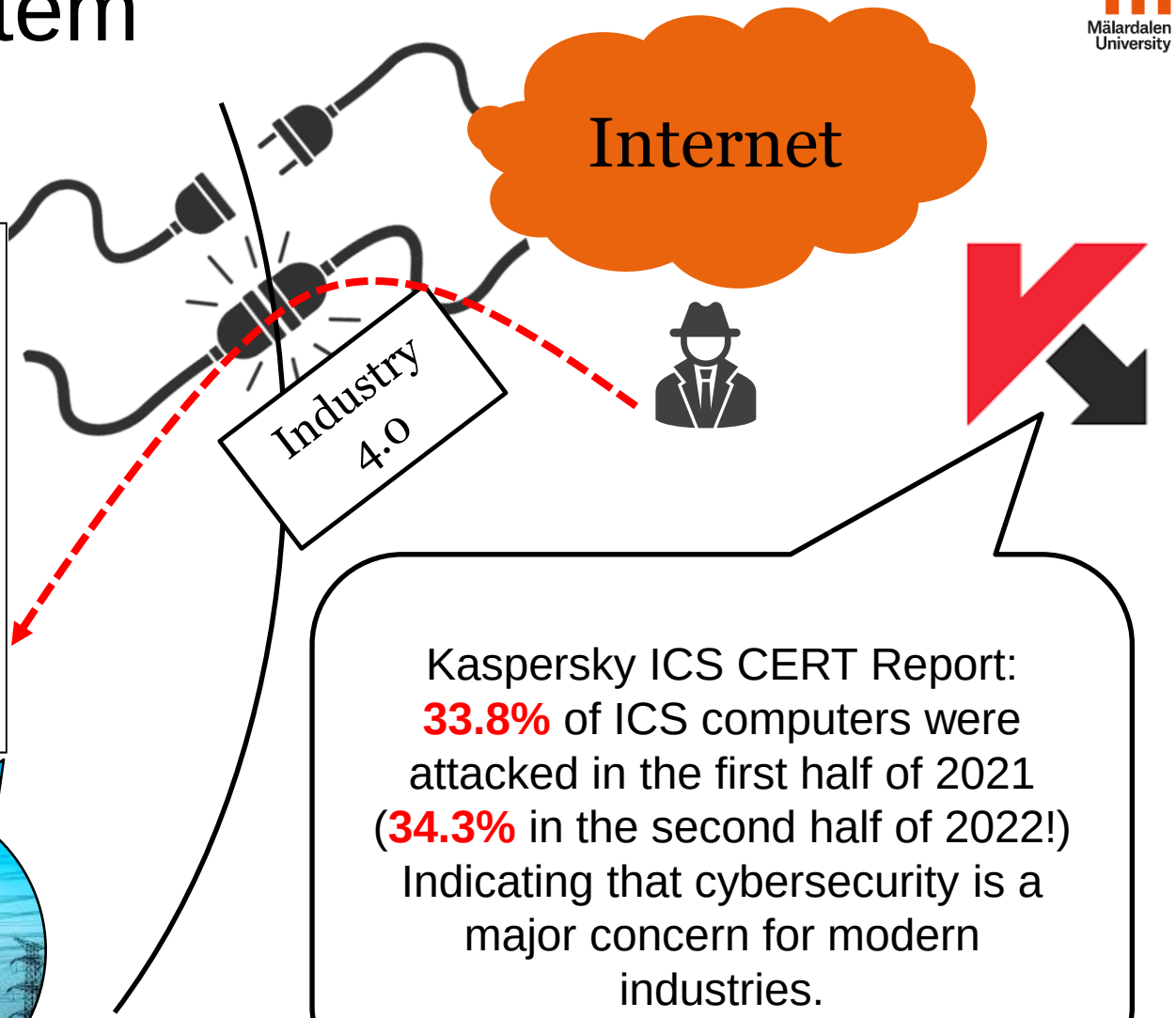
Define:

- Industrial Control System (ICS)
- Intrusion Detection Systems (IDS)
- Thesis Scope

Industrial Control System (ICS)

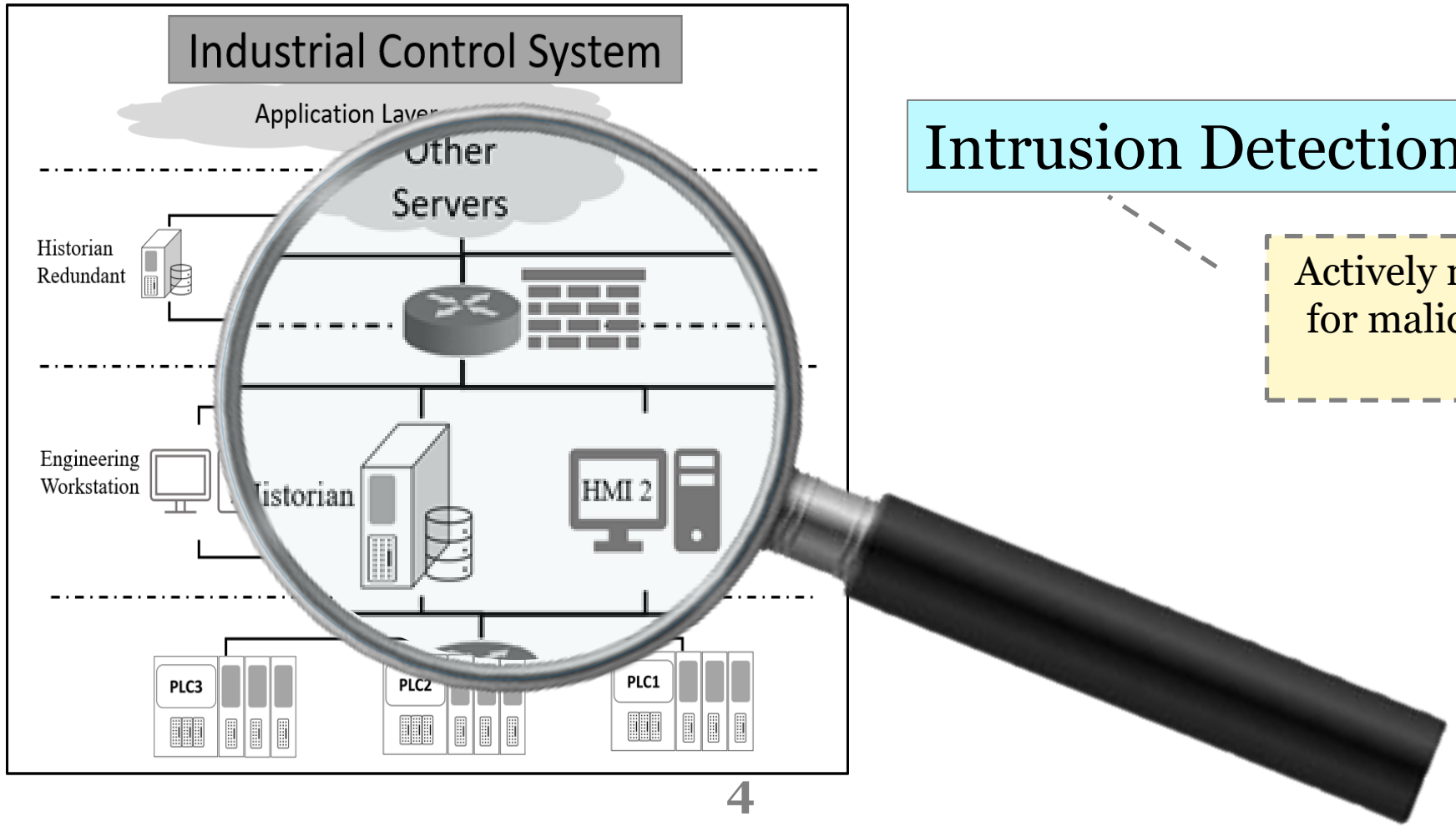






Kaspersky ICS CERT Report:
33.8% of ICS computers were attacked in the first half of 2021 (**34.3%** in the second half of 2022!)
Indicating that cybersecurity is a major concern for modern industries.

Attack Detection in ICS



Intrusion Detection Systems (IDS)

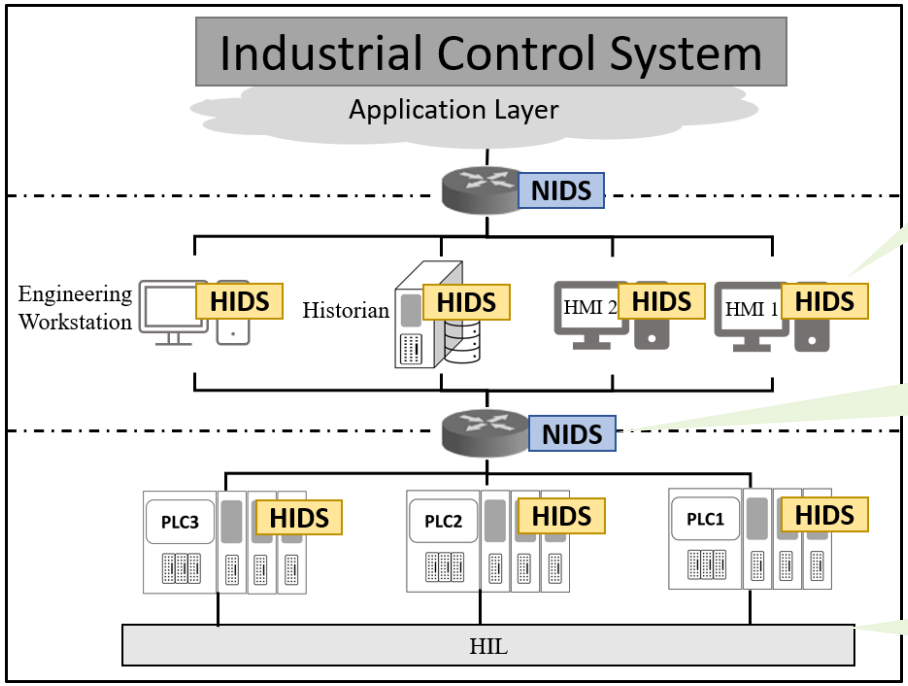
Actively monitor ICSs and look for malicious activities to find attacks.

Intrusions Detection Systems (IDS)

Deployment Approach

Detection Strategy

Detection Method



Host Based IDS (HIDS)

Network Based IDS (NIDS)

New Possibility to find anomalies

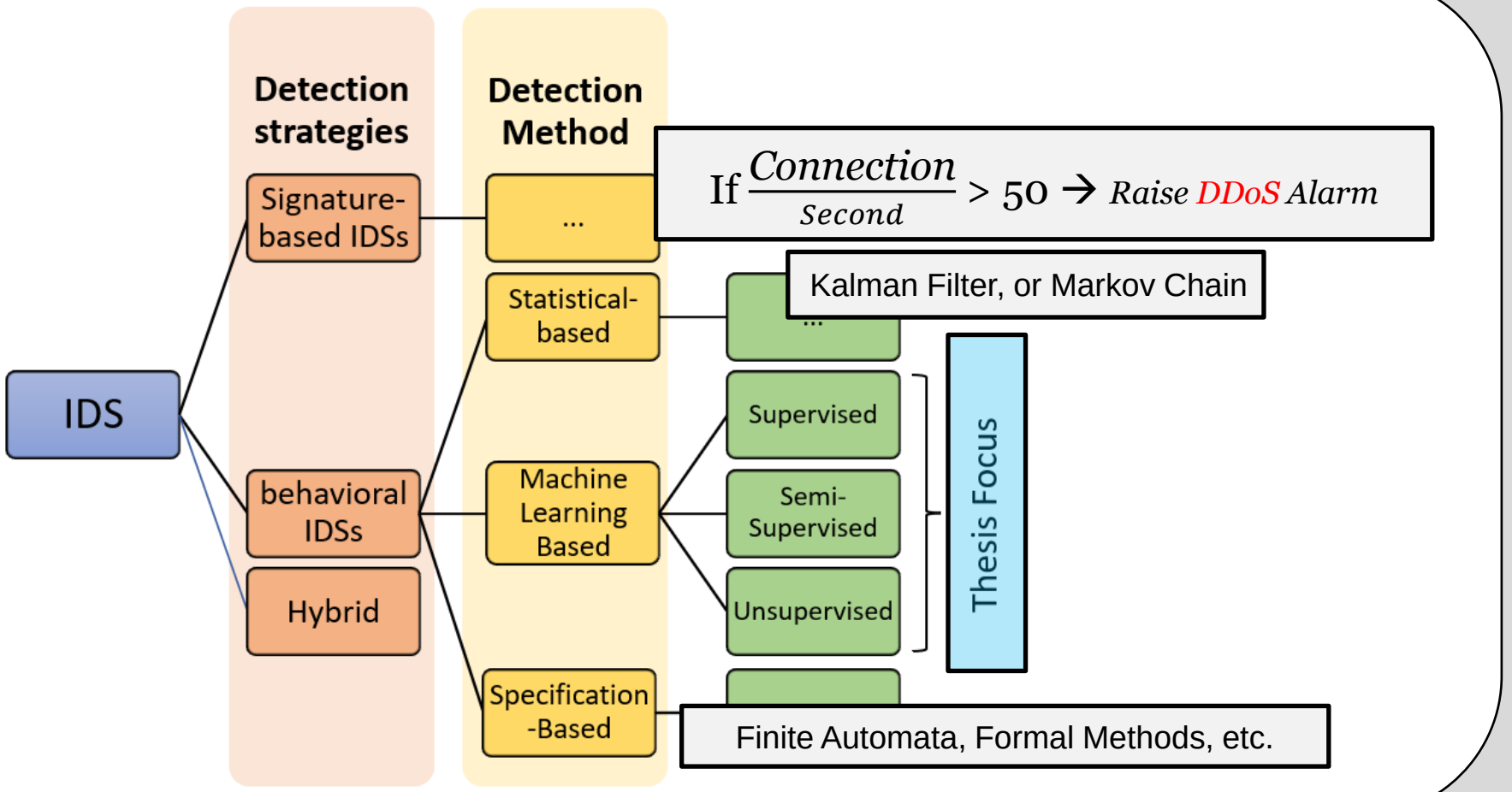
Thesis Focus: Mainly **Network Monitoring (NIDS)** + Partially **Physical Process Monitoring**

Intrusions Detection Systems (IDS) - continue

Deployment Approach

Detection Strategy

Detection Method



1- Introduction

2-Thesis Goals

3- Paper A

4- Paper B

5- Paper C

6- Paper D

7- Conclusion and Future works

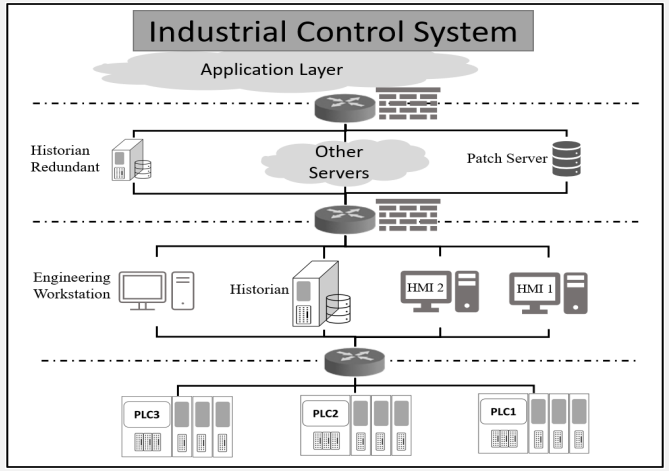
Define:

- Challenges and Motivations,
- Research Goals

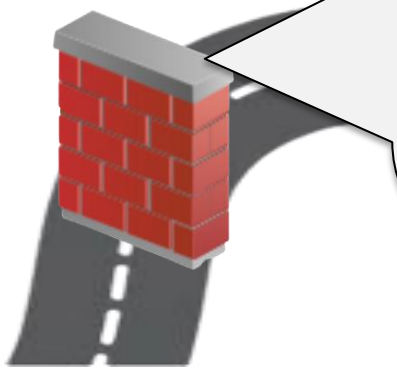
Motivations and Challenges

Explore how to detect cyberattacks on ICSs using smart intrusion detection techniques

Testbed

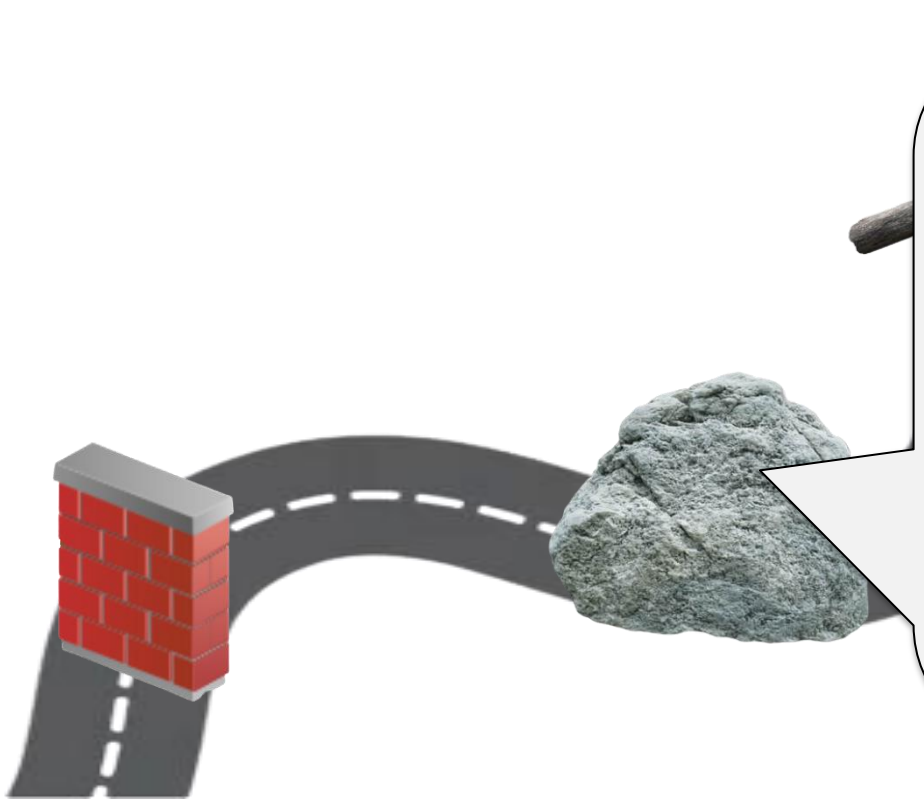


- Accessible
- Reproducible
- Versatile
- Customizable
- High Fidelity
- Realistic
- Low Cost
- Extendable



Motivations and Challenges

Explore how to detect cyberattacks on ICSs using smart intrusion detection techniques

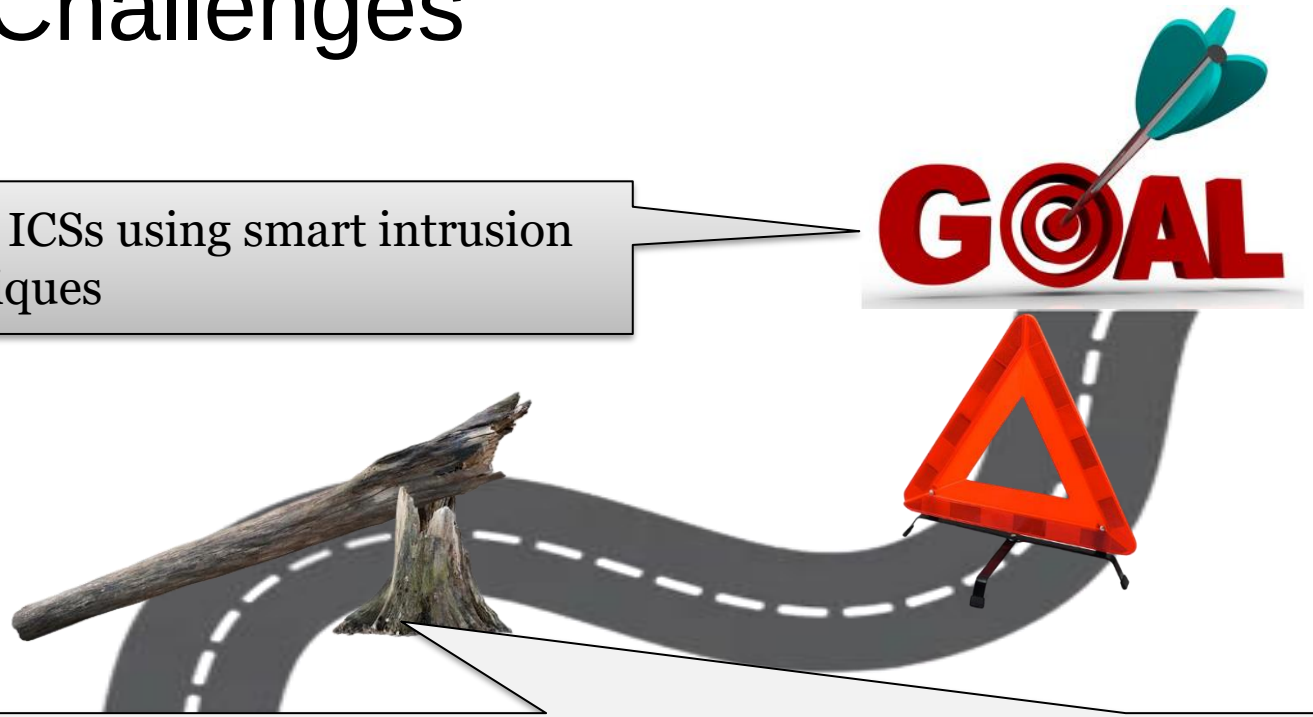


Cyberattacks

- Which attacks more target ICSs?
- What are possible consequences?
- How to implement cyberattacks?

Motivations and Challenges

Explore how to detect cyberattacks on ICSs using smart intrusion detection techniques



Dataset

How Available Datasets Could help?

What are needed to be included in Dataset?

What are features?

Feature Extraction!

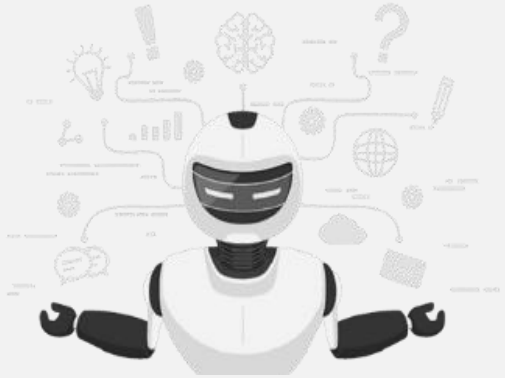
How to label records?

What are records?
- Packets,
- Something else

Motivations and Challenges

Explore how to detect cyberattacks on ICSs using smart intrusion detection techniques

Smart Intrusion Detection



Efficient attack detection:
- Increase Performance and Accuracy
- Decrease False Alarm rate

Which ML methods?

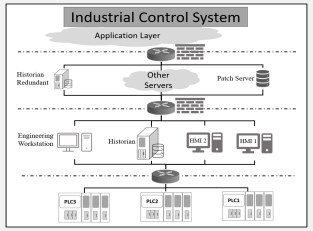
How to Identify Attack type?

How to improve IDS in ICSs

Research Goals

Testbed

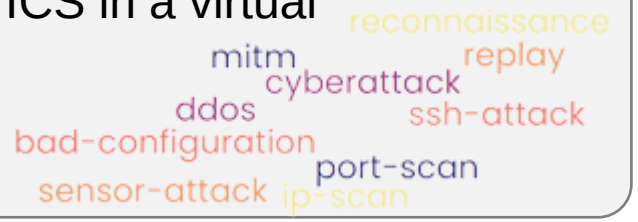
- Survey Requirements,
- Provide an experiment environment for cybersecurity



Subgoal 1:

Cyberattack demonstration

Demonstrate the consequences of common cyberattacks for ICS in a virtual environment.



Subgoal 2:

Dataset

Subgoal 3:

Develop a dataset as a validation benchmark for intrusion detection in ICSs.

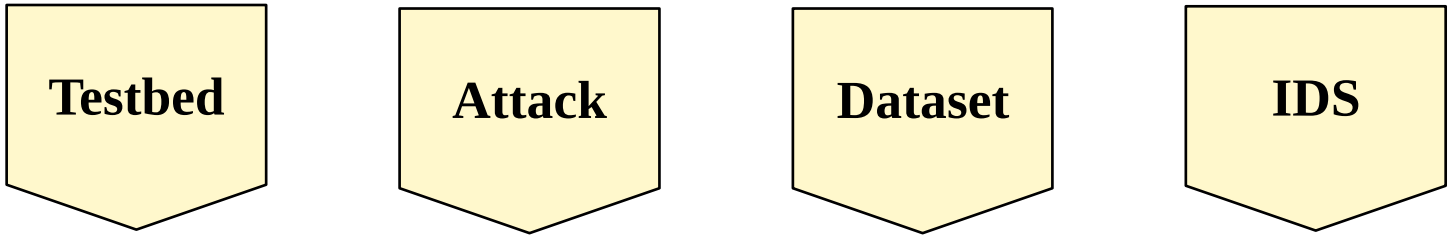
- Network traces
- System logs
- Process variables

Subgoal 4:

Intrusion Detection and Identification Using ML:

Investigate and evaluate ML techniques for identifying different cyberattack scenarios

Mapping of Research Goals to the Papers



Goals / Papers	Subgoal 1	Subgoal 2	Subgoal 3	Subgoal 4
Paper A		✓		✓
Paper B	✓	✓		
Paper C			✓	✓
Paper D				✓

1- Introduction

2- Thesis goals

3-Paper A

4- Paper B

5- Paper C

6- Paper D

7- Conclusion and Future works

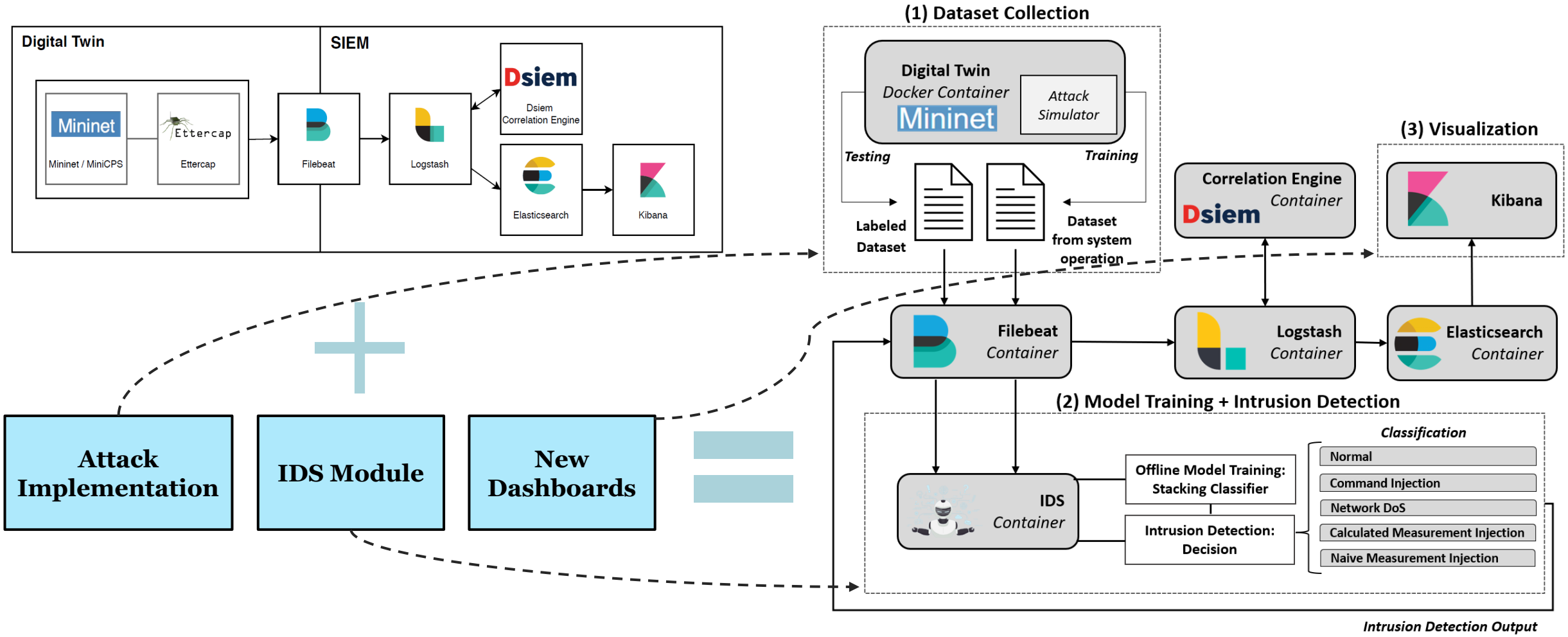
Paper A:

Digital Twin-based Intrusion Detection for Industrial Control Systems,

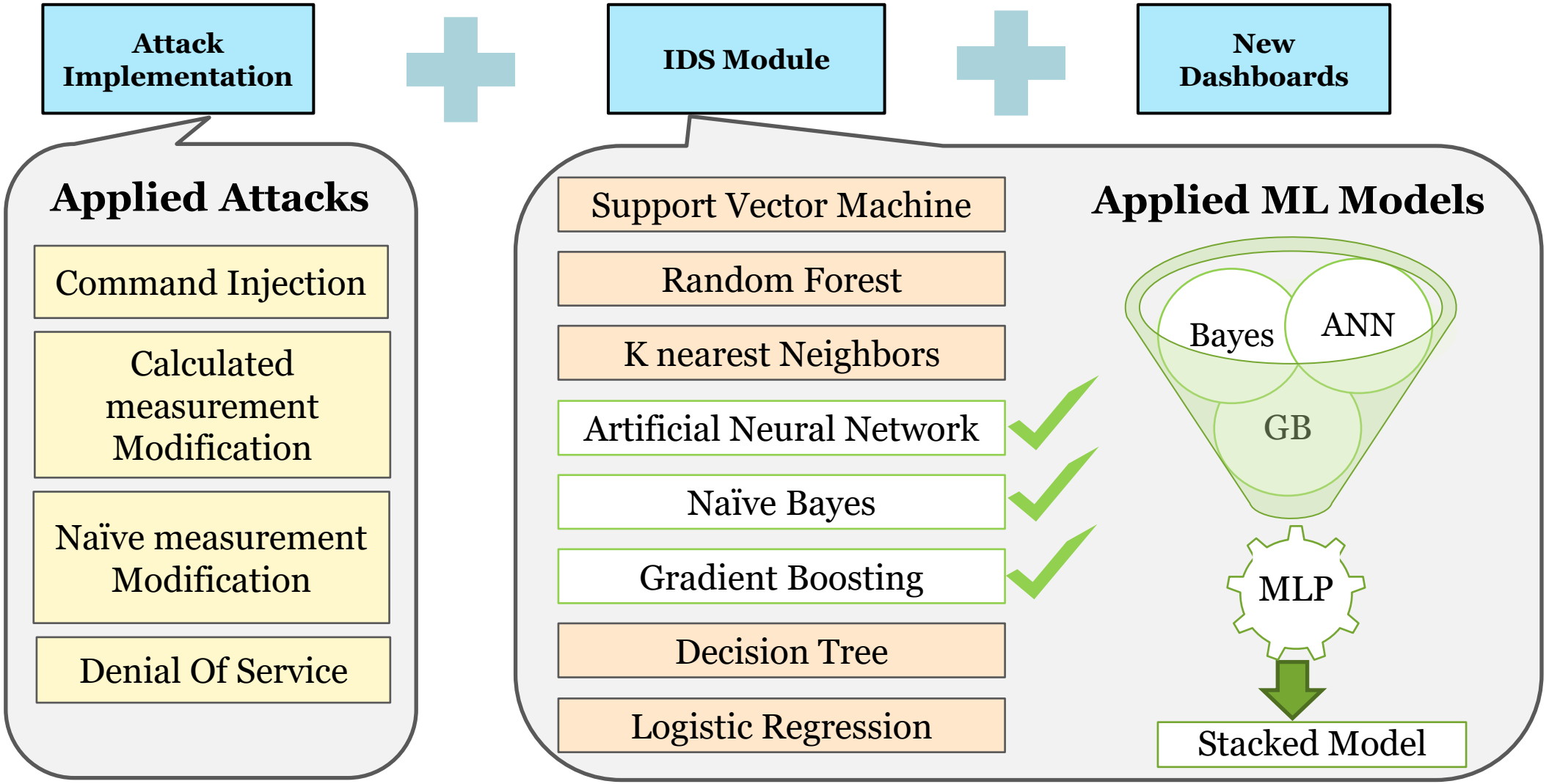
Seba Anna Varghese, Alireza Dehlaghi Ghadim, Ali Balador, Zahra Alimadadi and Panos Papadimitratos.

International Conference on Pervasive Computing and Communications (PerCom). Pisa, Italy, March 2022. (Published)

Paper A-Digital Twin-based Intrusion Detection for Industrial Control Systems



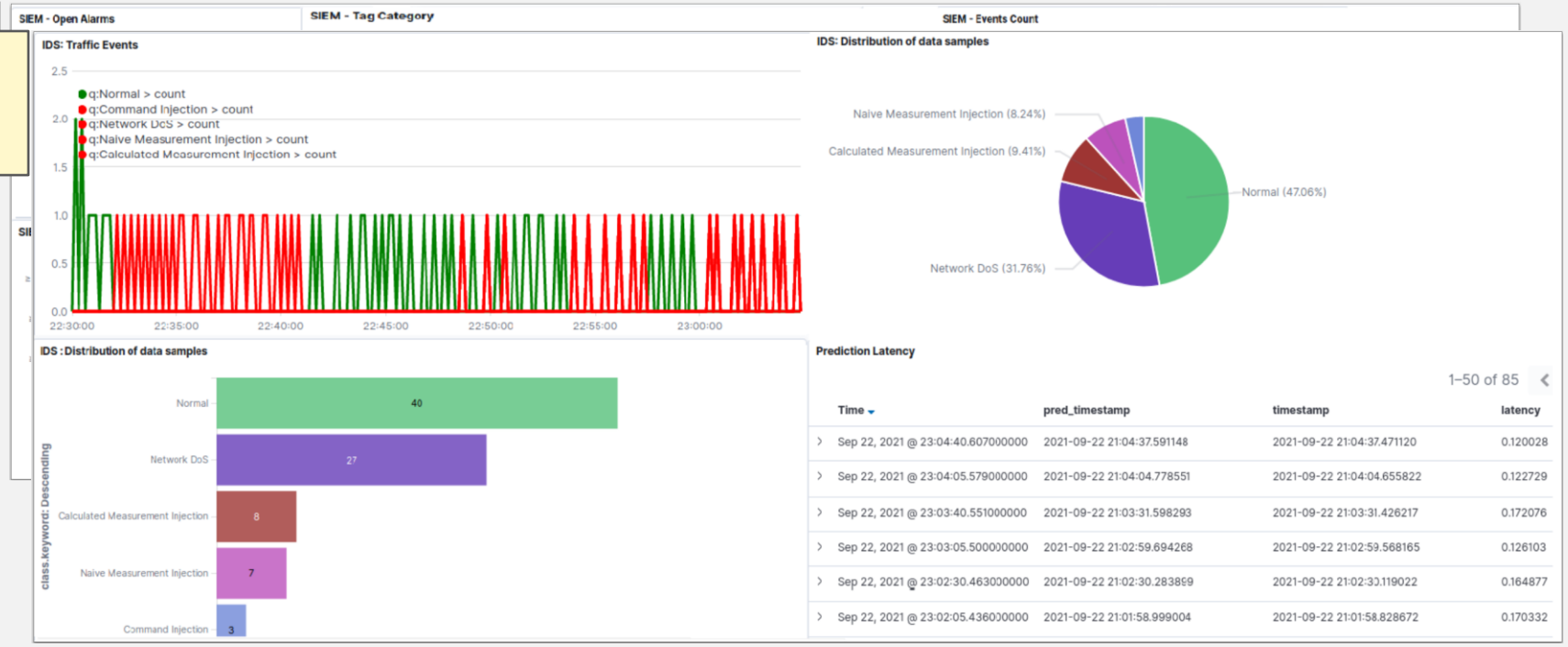
Paper A - Continue



Paper A - Continue

Attack Implementation + **IDS Module** + **New Dashboards**

Incident detection (New Dashboard)



1- Introduction

2- Thesis goals

3- Paper A

4-Paper B

5- Paper C

6- Paper D

7- Conclusion and Future works

Paper B:

ICSSIM – A Framework for Building Industrial Control Systems Security Testbeds,

Alireza Dehlaghi-Ghadim, Ali Balador, Mahshid Helali Moghadam, Hans Hansson, Mauro Conti.

Journal of Computers in Industry Journal, 2023. (Published)

Paper B - ICSSIM – A Framework for Building Industrial Control Systems Security Testbeds

Simulation of ICS and Physical Process

Reproducible | Extendable

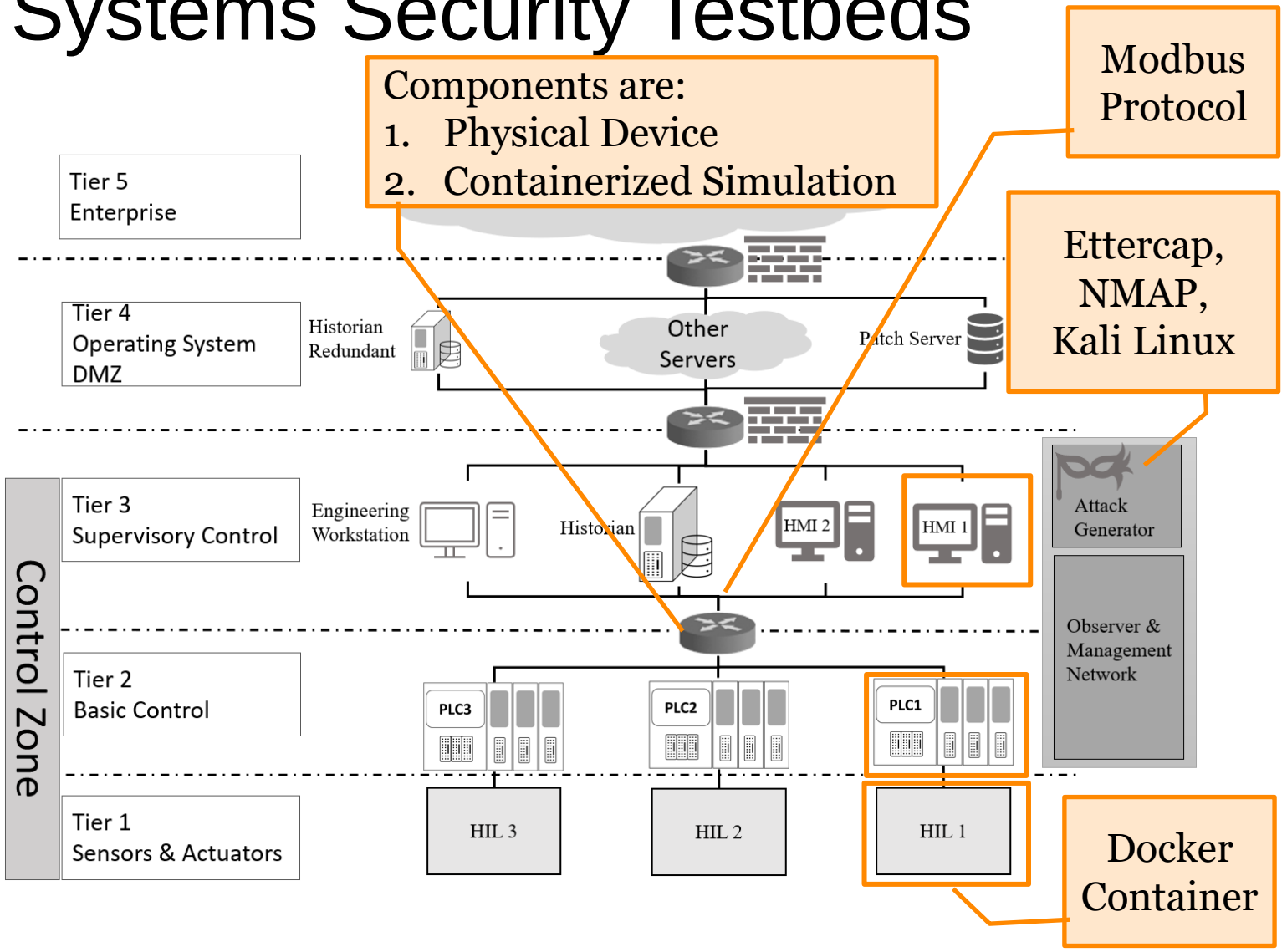
High Fidelity | Accessible

Network Emulation | Low Cost

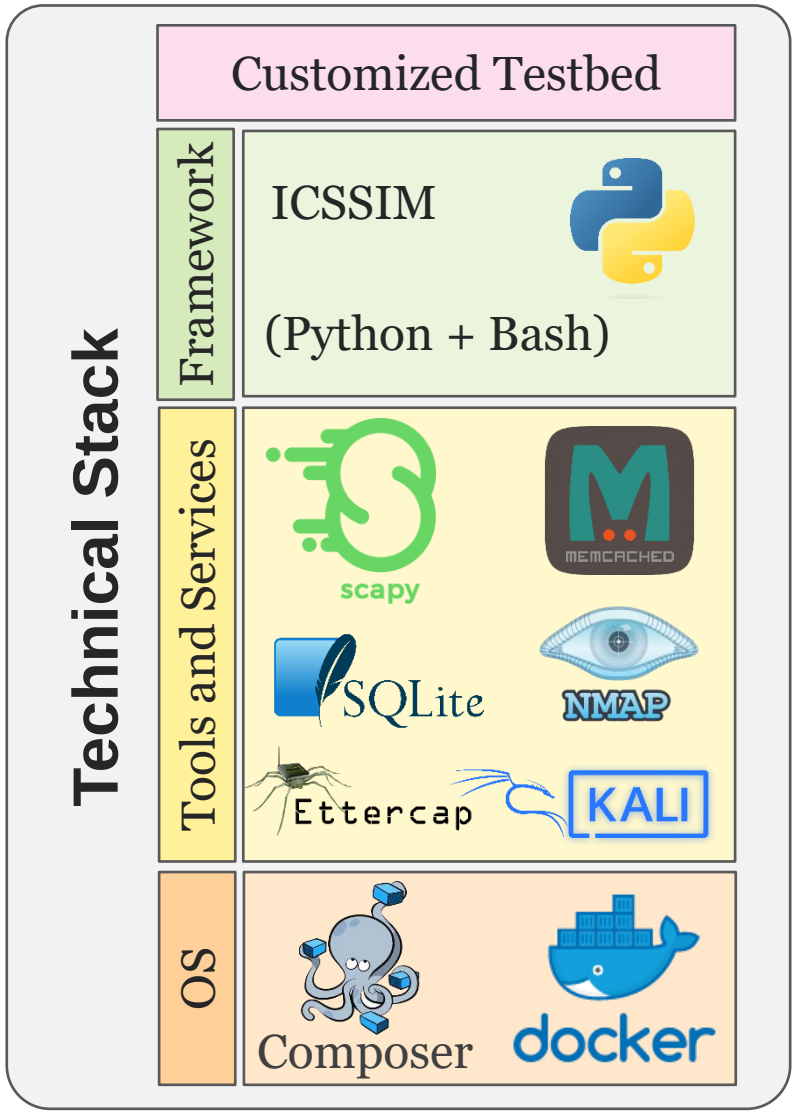
Industrial Network Protocol

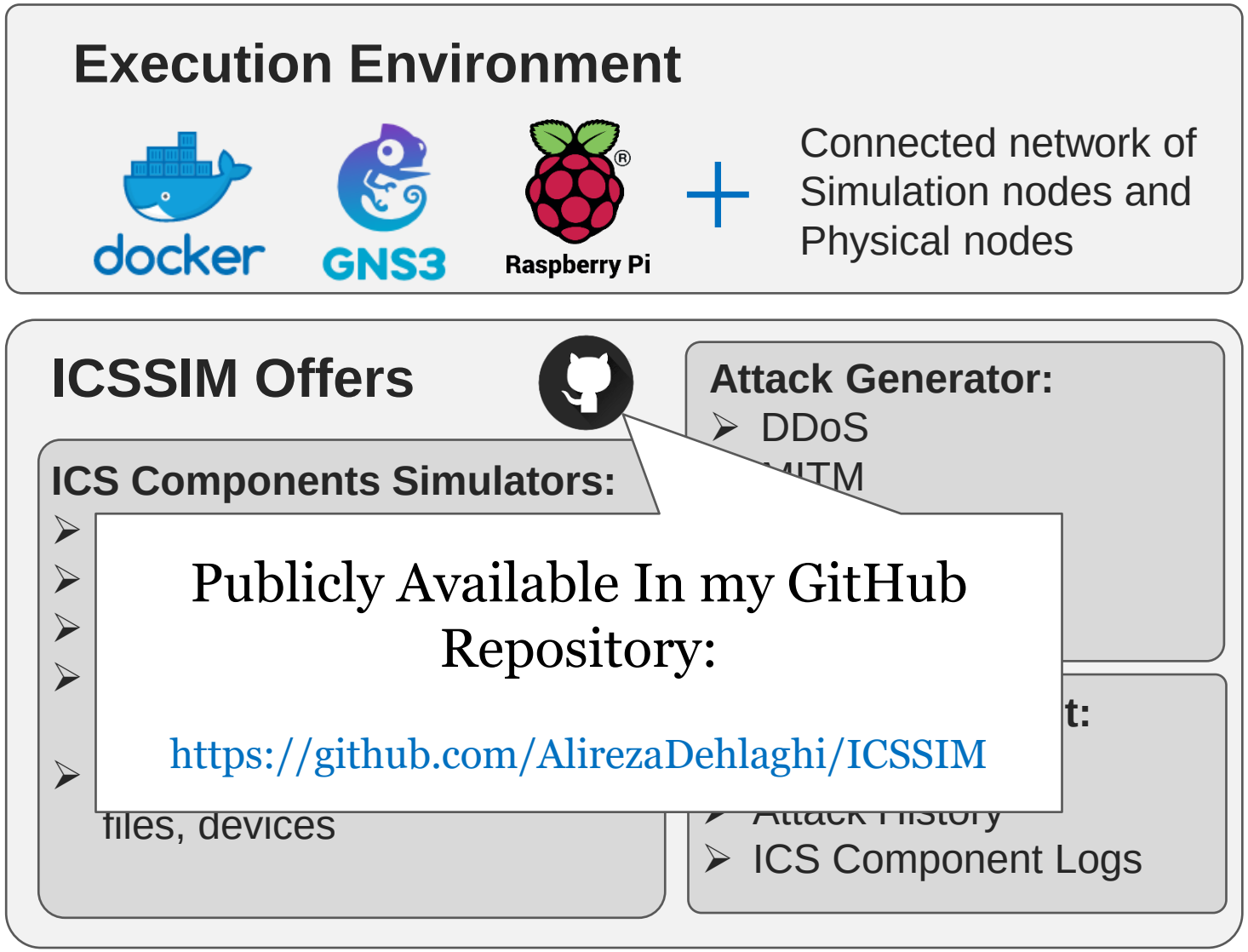
Logging Capability | Versatile

Support Physical Device



Paper B - ICSSIM





Paper B – ICSSIM (attacks)

Reconnaissance Attack

Get Information About:

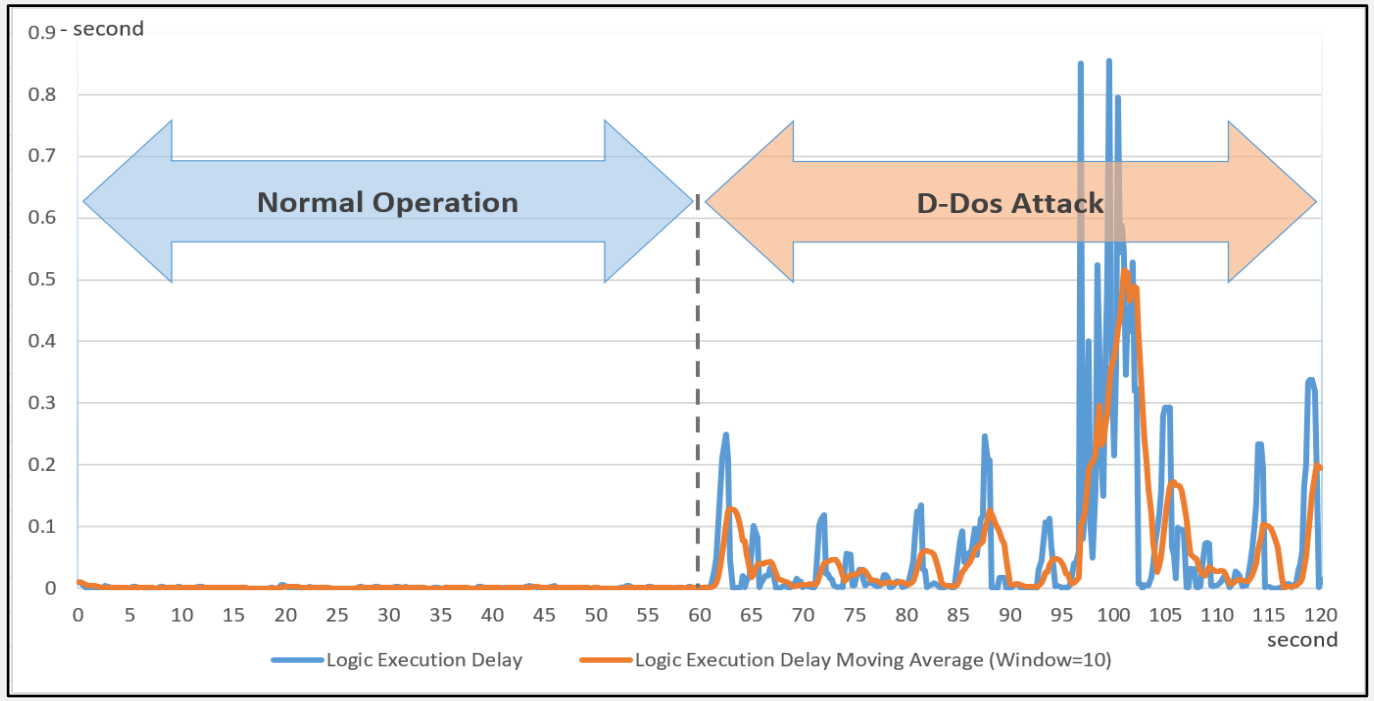
- Active IP, Open Port, Network Protocol

```
1 # Nmap 7.80 scan initiated Thu Mar  3 14:00:10 2022
  as: nmap -p- -oG ip_nmap.txt 192.168.0.1-255
2 Host: 192.168.0.1 (dlinkrouter)        Status: Up
3 Host: 192.168.0.1 (dlinkrouter)        Status: Up
4 Host: 192.168.0.11 (plc1.icsnet)       Status: Up
5 Host: 192.168.0.11 (plc1.icsnet)       Ports: 502/-
  open/tcp//mbap///      Ignored State: closed (65534)
6 Host: 192.168.0.12 (plc2.icsnet)       Status: Up
7 Host: 192.168.0.12 (plc2.icsnet)       Ports: 502/-
  open/tcp//mbap///      Ignored State: closed (65534)
8 Host: 192.168.0.21 (hmi1.icsnet)       Status: Up
9 Host: 192.168.0.21 (hmi1.icsnet)       Status: Up
10 Host: 192.168.0.22 (hmi2.icsnet)      Status: Up
11 Host: 192.168.0.22 (hmi2.icsnet)      Status: Up
12 Host: 192.168.0.41 (d793561cecd4)     Status: Up
13 Host: 192.168.0.41 (d793561cecd4)     Status: Up
14 # Nmap done at Thu Mar  3 14:00:24 2022 -- 255 IP
  addresses (6 hosts up) scanned in 13.37 seconds
```

```
7 Nmap scan report for plc1.icsnet (192.168.0.11)
8 Host is up (0.000014s latency).
9 Not shown: 65534 closed ports
10 PORT    STATE SERVICE
11 502/tcp open  mbap
12 MAC Address: 02:42:C0:A8:00:0B (Unknown)
```

DDoS attack

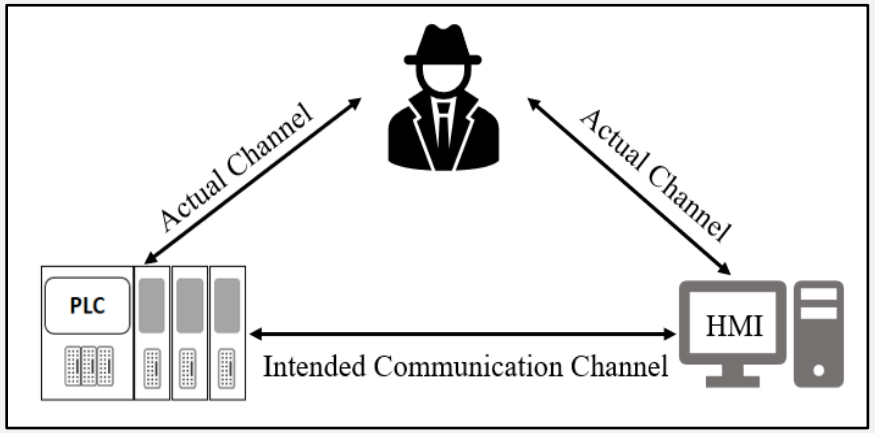
Many Agent Send Read And write messages to PLCs



Paper B – ICSSIM (attacks)

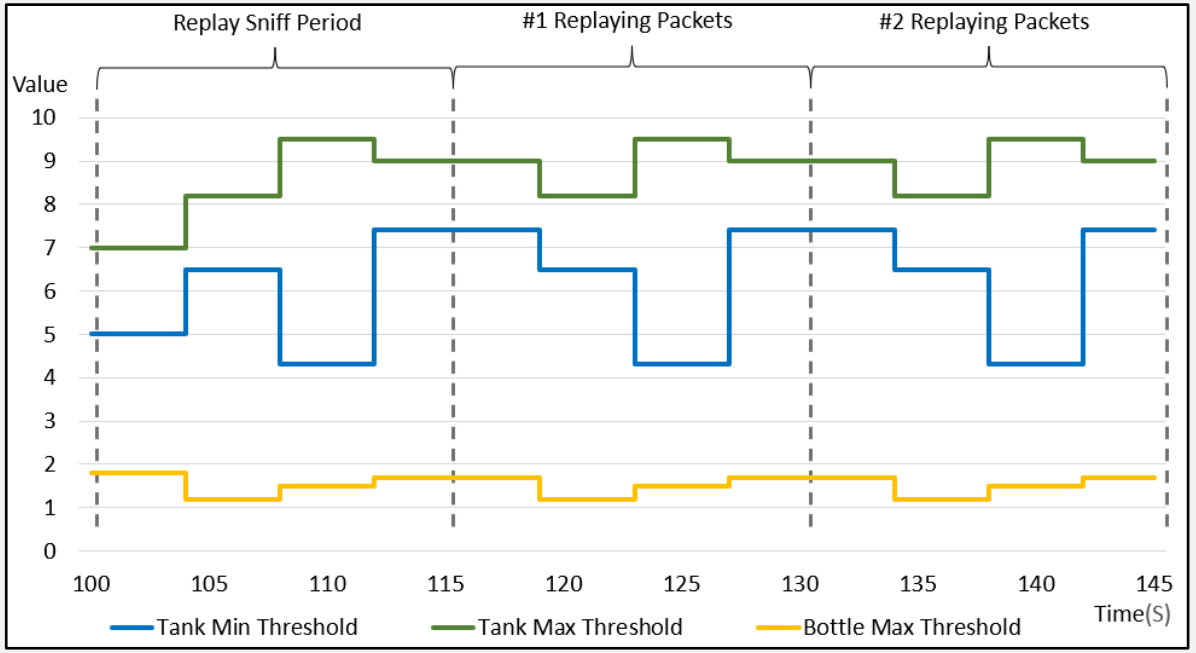
MITM Attack

1. Redirecting Packets
2. Decoding Packets using SCAPY
3. Resubmit Manipulated packet



Replay Attack

1. Redirecting Packets
2. Sniff for a period
3. Relay sniffed packets multiple time



1- Introduction

2- Thesis goals

3- Paper A

4- Paper B

5-Paper C

6- Paper D

7- Conclusion and Future works

Paper C:

Anomaly Detection Dataset for Industrial Control Systems,

Alireza Dehlaghi-Ghadim, Mahshid Helali Moghadam, Ali Balador, and Hans Hansson.

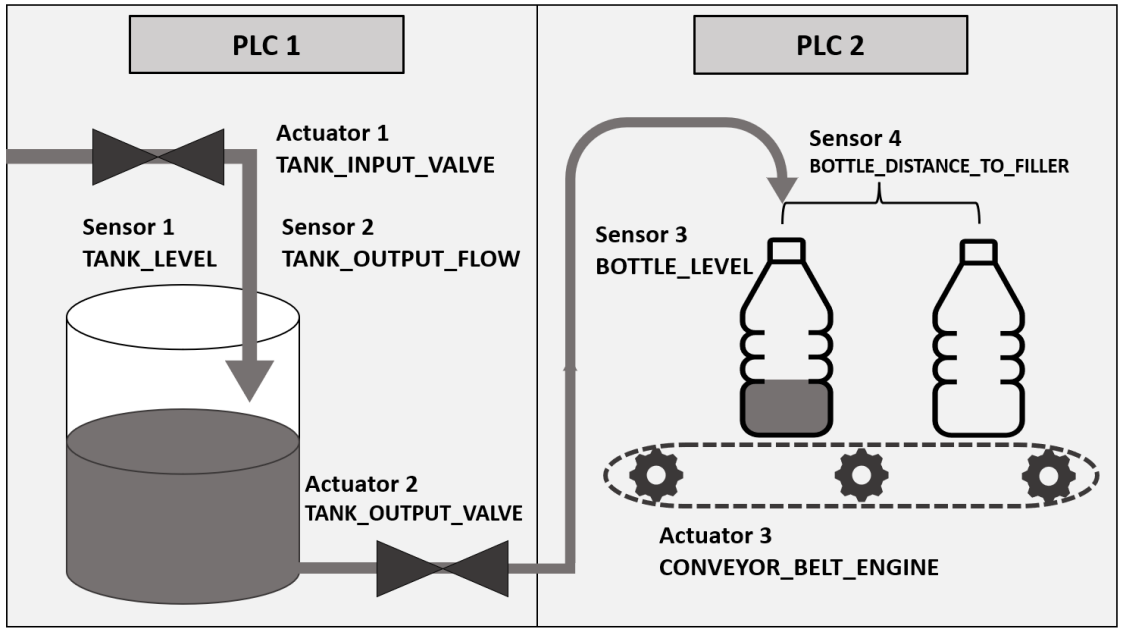
(Submitted for publication)

Paper C - Anomaly Detection Dataset for Industrial Control Systems

Paper C → Create Testbed Using ICSSIM → Apply Cyberattacks → Driving Network Features → Labelling → Dataset → ML experiments

Step 1:

Implement Sample Bottle Filling Factory



Step 2:

Implement Several Attack Scenarios:

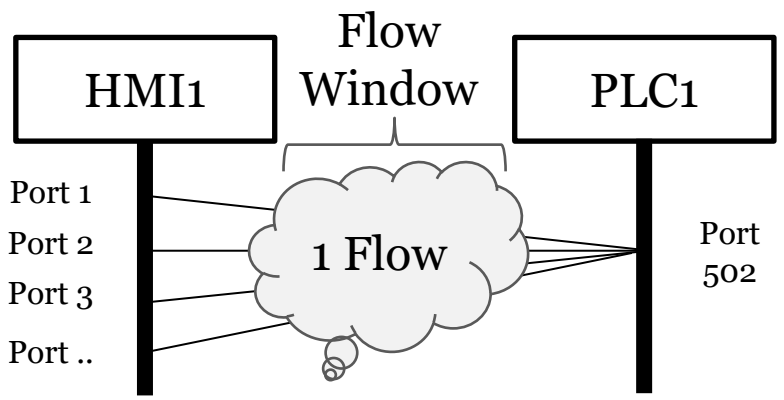
Paper C – Dataset Features

Step 3: Driving Network Features

Network Flow → Aggregate Packets with same :

- Source Address
- Destination Address
- Network Protocol

Within Time Interval (Flow Window)



ICSFLowGenerator Tool

A tool for analyzing Raw packets ... rating ... res

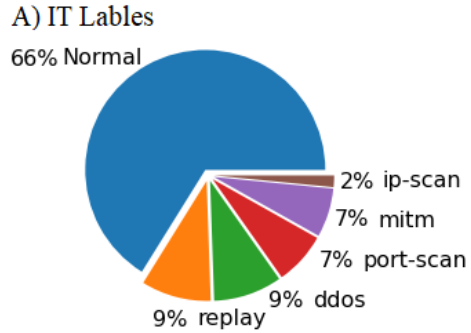
Publicly Available In my GitHub Repository:

https://github.com/AlirezaDehlaghi/ICSFlow

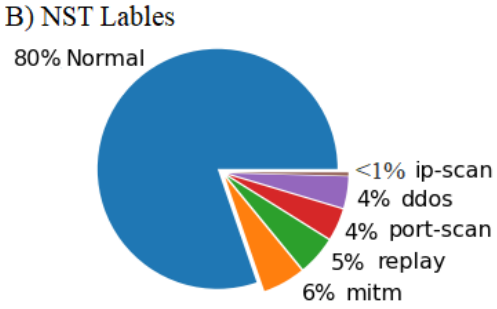
Paper C – Dataset and Experiment

Step 4: Labelling

Injection Timing (IT)



Network Security Tool (NST)



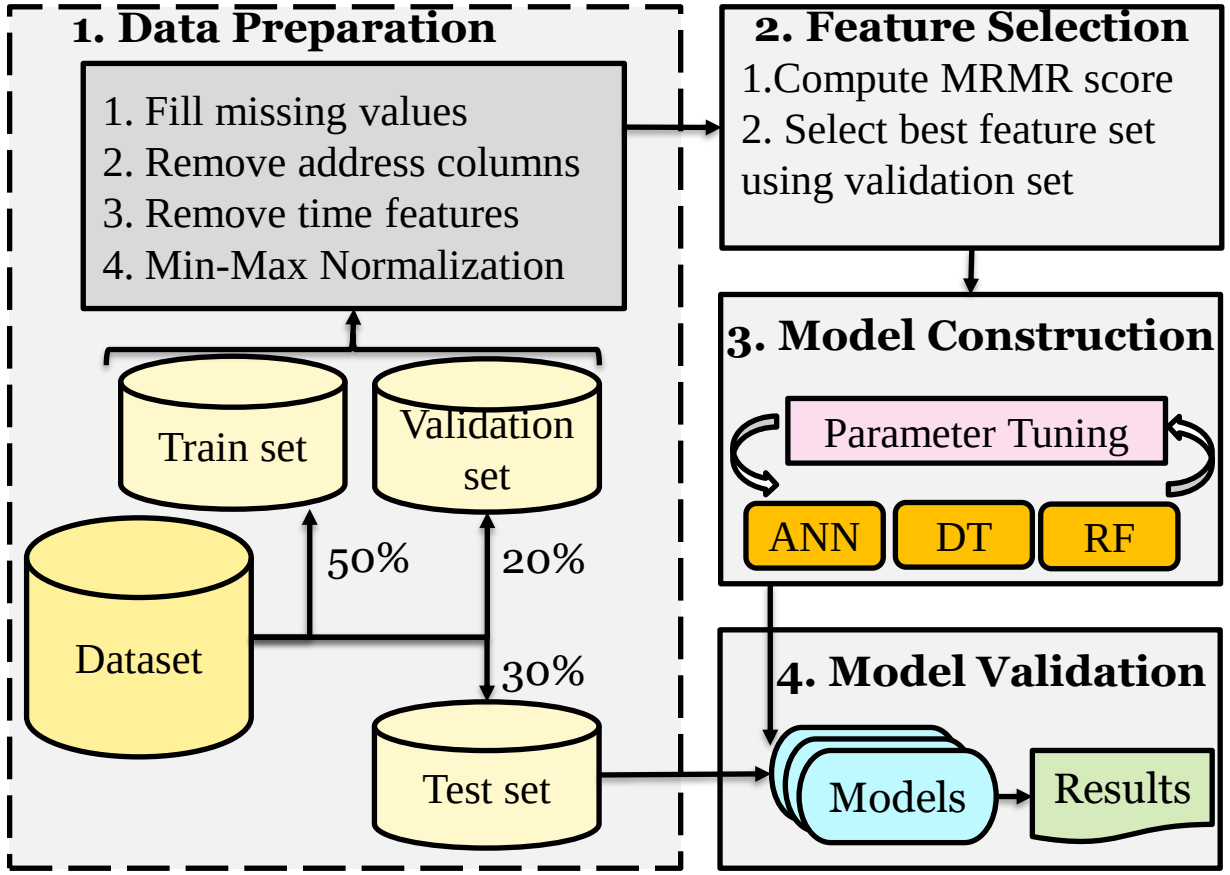
Step 5: Publish Dataset

- Raw Packets
- Flow Dataset
- Component Logs
- Attack History

Publicly Available In:

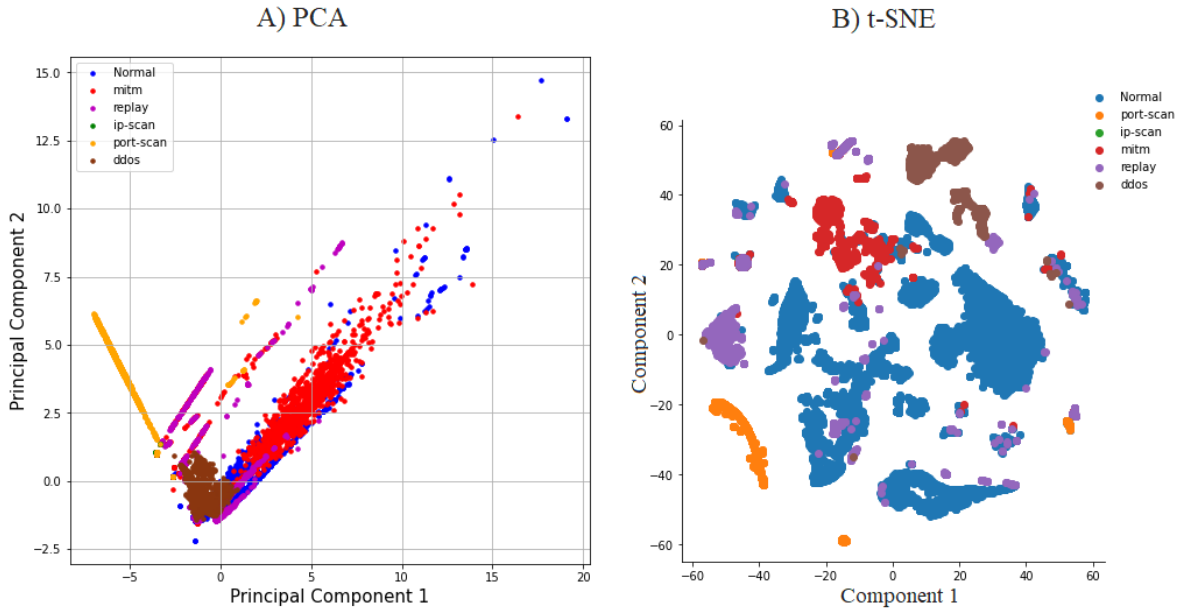
https://www.kaggle.com/datasets/alirezadehlaghi/icssim

Step 6: Experiment with the Dataset:

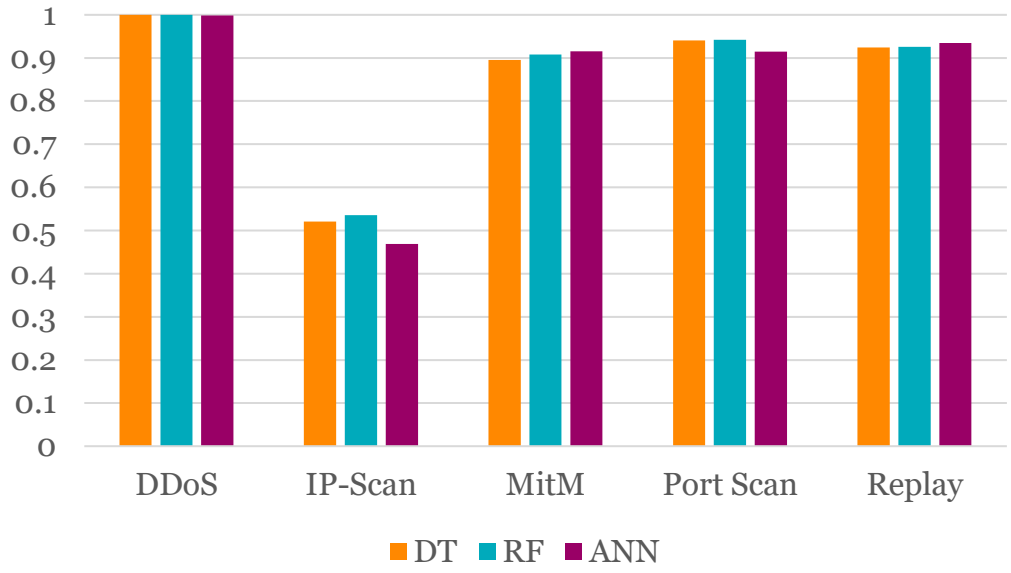


Paper C (Experiment with the Dataset)

Data Demonstration of ICSFlow Dataset Using PCA and t-SNE

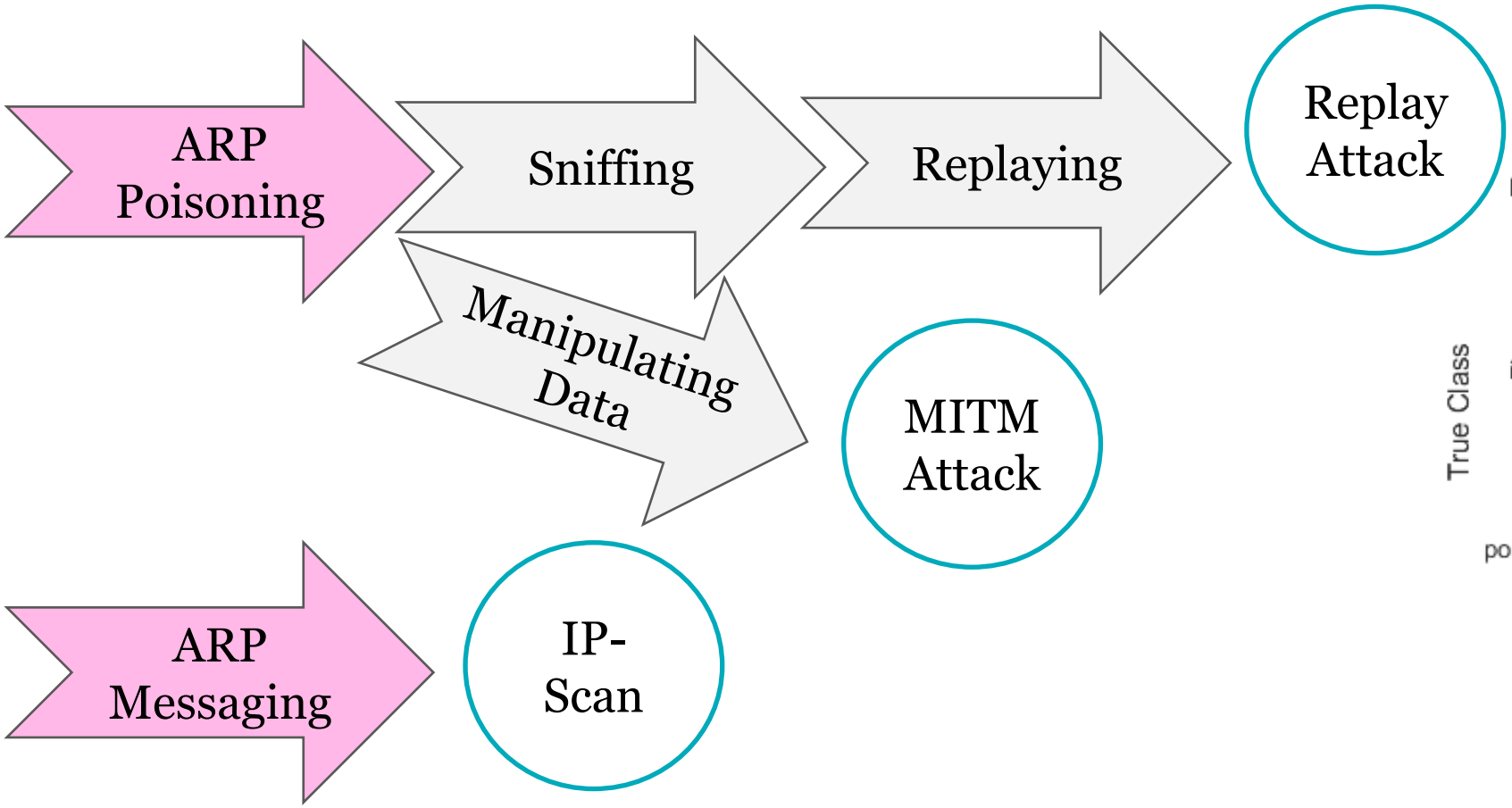


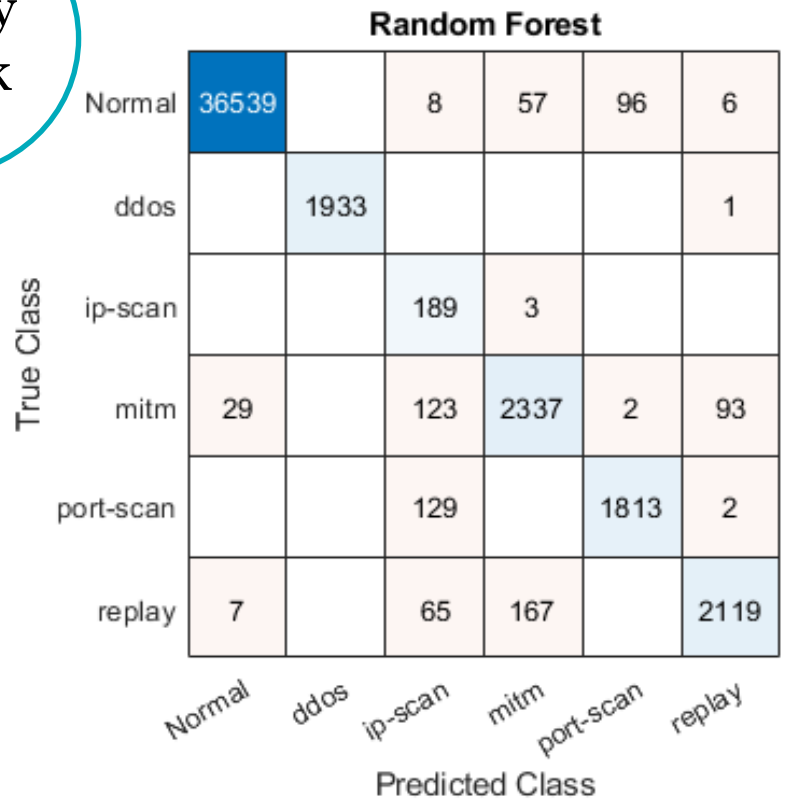
F1-Score of Intrusion Detection Models on ICSFlow Dataset



Paper C analysis (Motivation for Paper D)

- Why Sequence anomaly detection is promising.





1- Introduction

2- Thesis goals

3- Paper A

4- Paper B

5- Paper C

6-Paper D

7- Conclusion and Future works

Paper D:

Time-series Anomaly Detection and Classification with Long Short-Term Memory Network on Industrial Manufacturing Systems,

Tijana Markovic, Alireza Dehlaghi-Ghadim, Miguel Leon, Ali Balador, Sasikumar Punnekkat.

(Submitted for publication)

Paper D

Dataset

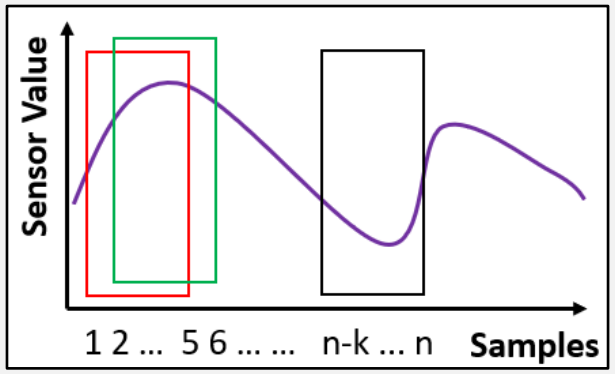
Modular Ice-cream factory Dataset

- Anomaly Detection (AD)
- Anomaly Classification (AC)

Preprocess

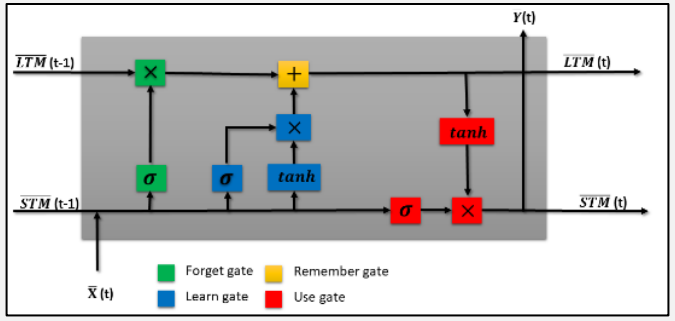
- Anomaly (Ramp, Step, Freeze) balancing in train, validation, and test dataset.
- Normalization
- Missing Values
- Type Converting

Windowing

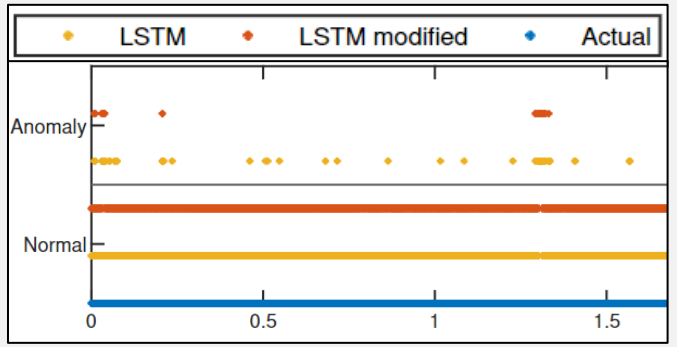


LSTM

Hyper Parameter Tunning +



Refinement



Results

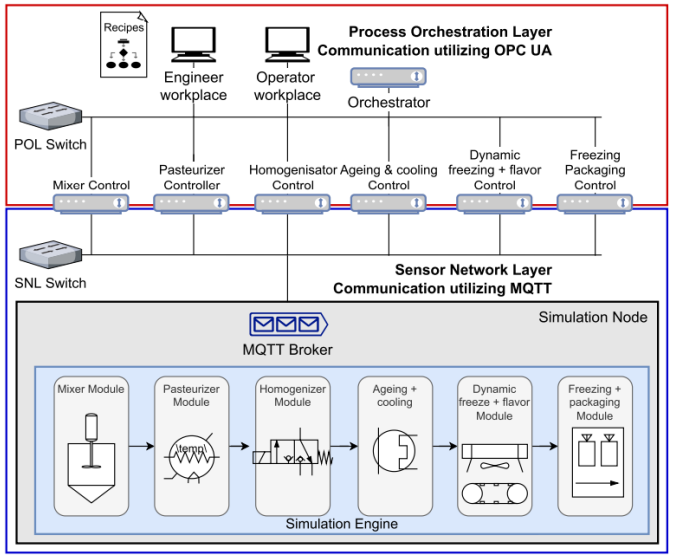
Analyze Performance:

- Accuracy
- Execution Time
- Memory Consumption

Paper D- Dataset & Preprocess

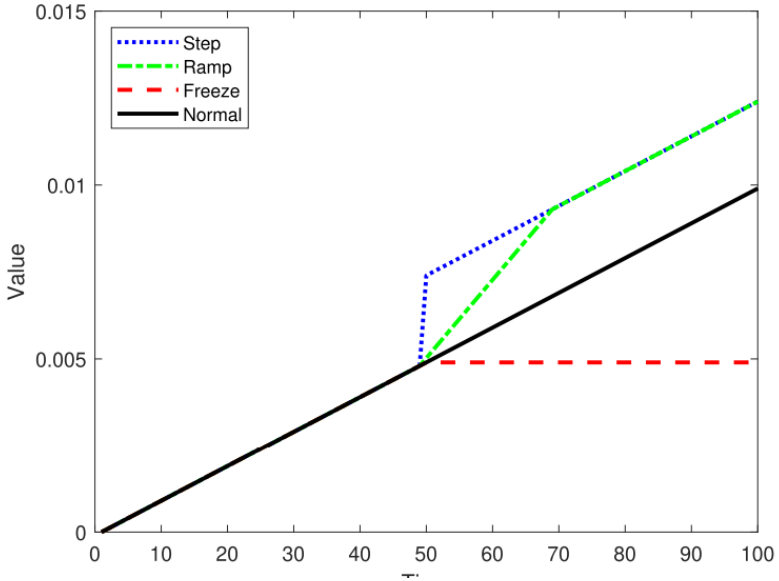
Taken from paper: "A modular ice cream factory dataset on anomalies in sensors to support machine learning research in manufacturing systems,"

Ice-Cream Factory Simulation



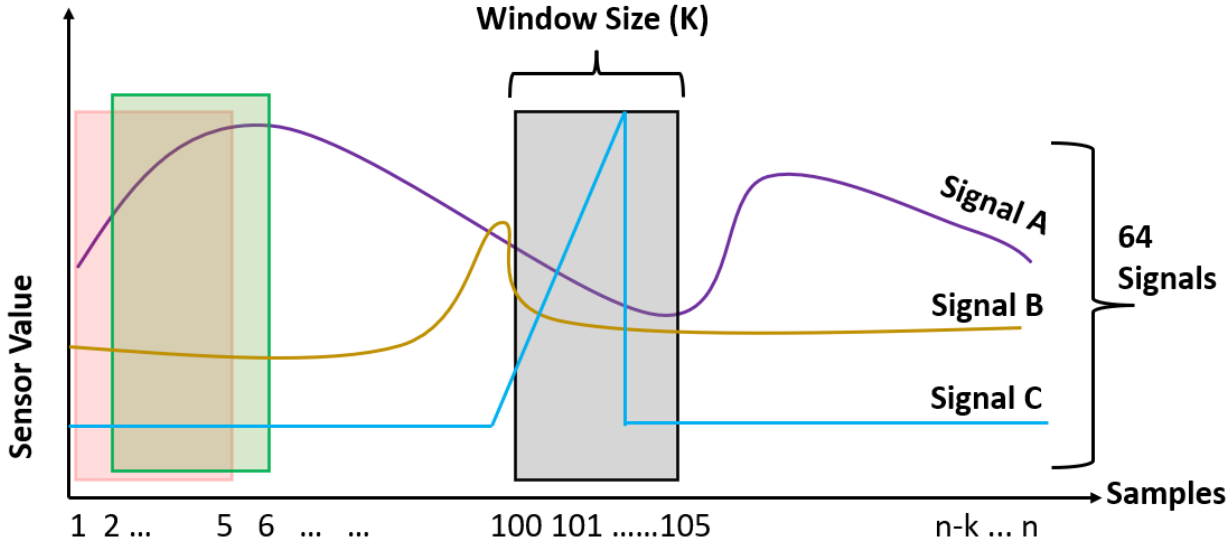
Sensor Anomalies
(Failure Or Cyber Attack)

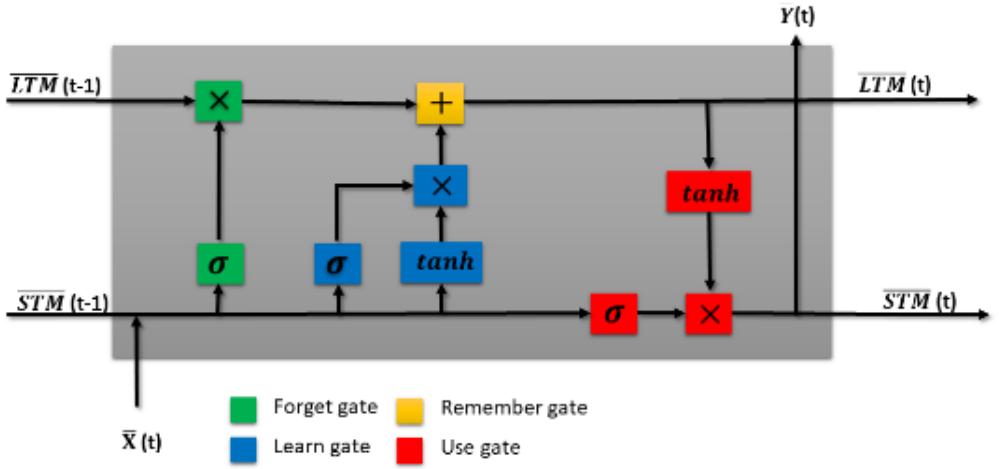
3 Types of Anomalies



Preprocess → Datasets Balancing → Fill Missing Values → Normalization

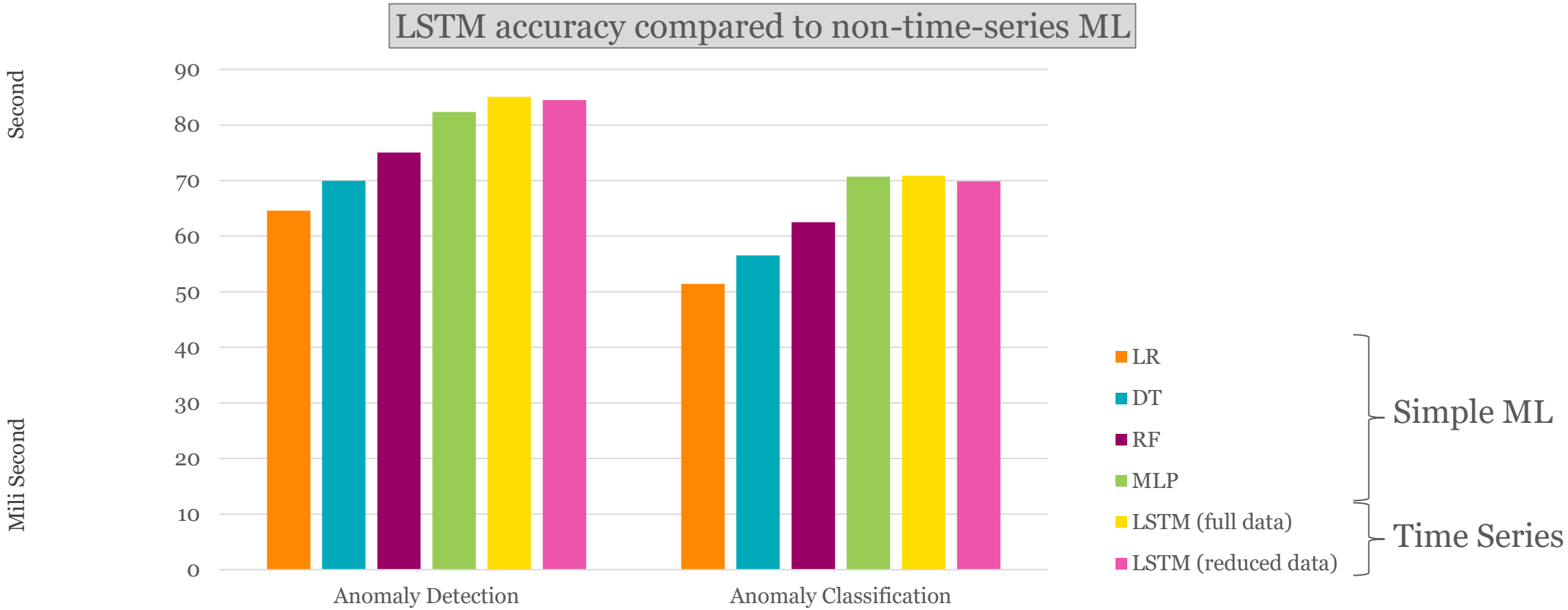
Paper D-Windowing



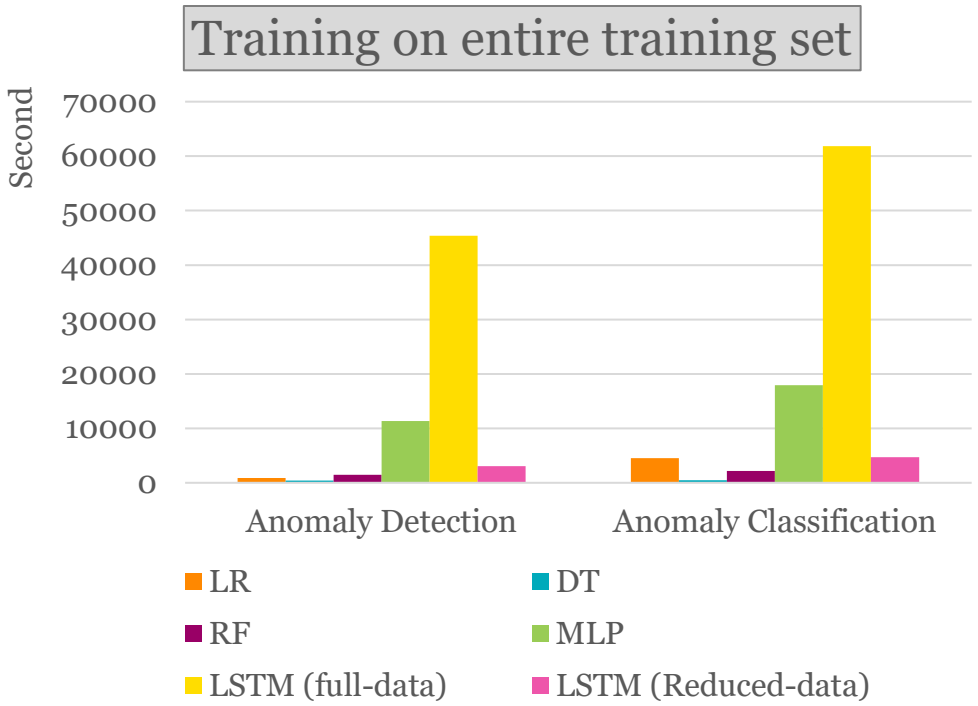


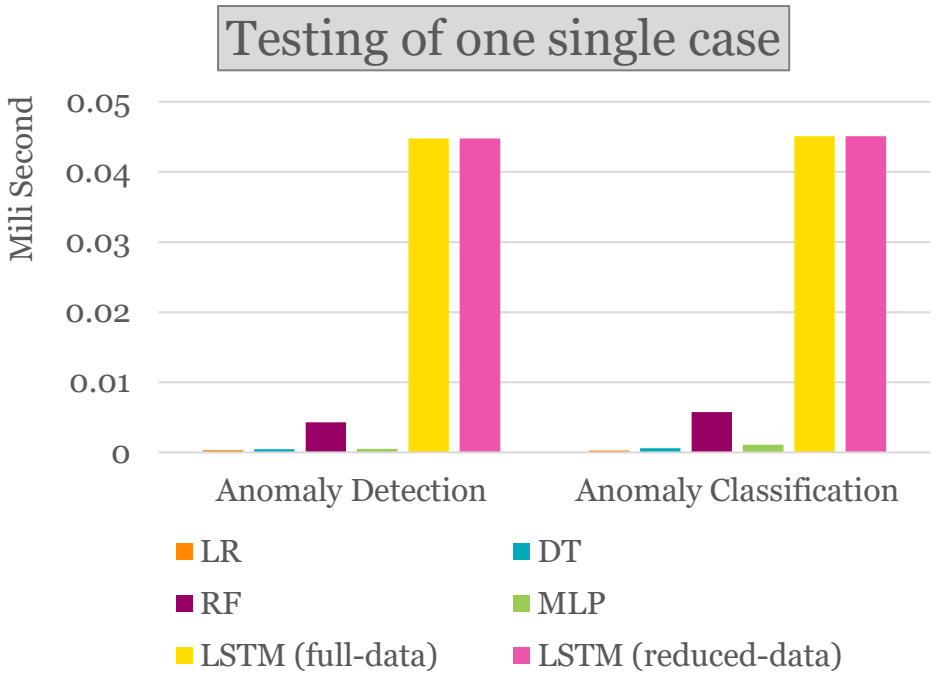
Hyper-Parameter Tunning → Window Size K → Number Of Hidden Neurons → Epochs → Activation Function

Paper D – Accuracy Results



Paper D - Results





1- Introduction

2- Thesis goals

3- Paper A

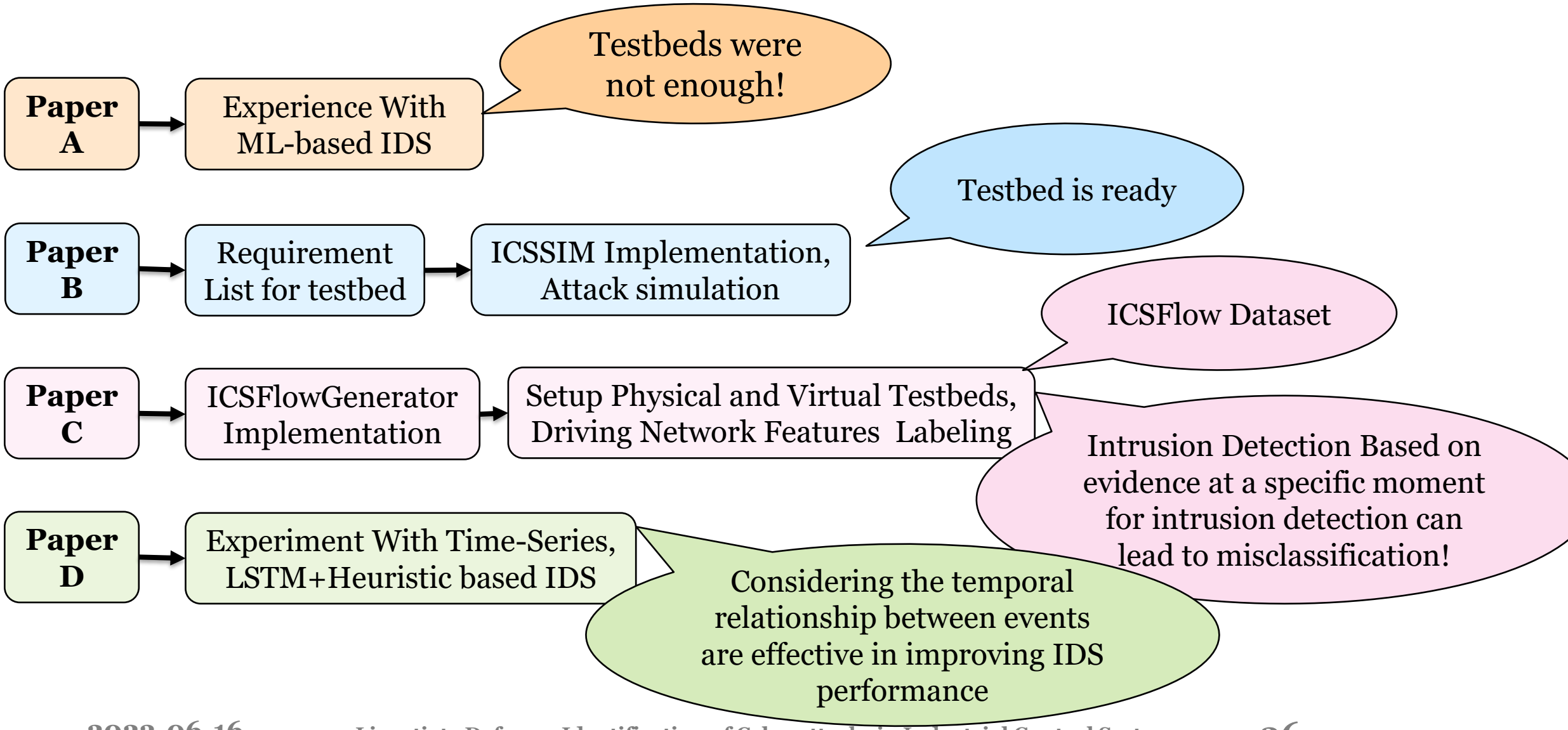
4- Paper B

5- Paper C

6- Paper D

7- Conclusion and Future works

Conclusion


Paper A
Experience With ML-based IDS
Testbeds were not enough!
Paper B
Requirement List for testbed
ICSSIM Implementation, Attack simulation
Testbed is ready
Paper C
ICSFlowGenerator Implementation
Setup Physical and Virtual Testbeds, Driving Network Features Labeling
ICSFlow Dataset
Intrusion Detection Based on evidence at a specific moment for intrusion detection can lead to misclassification!
Paper D
Experiment With Time-Series, LSTM+Heuristic based IDS
Considering the temporal relationship between events are effective in improving IDS performance

Future Works

Idea for future research

Unsupervised ML
(Complex or Zero-days attacks)

Investigate on ML Deep models Such as CNN

Integrate physical process evidences with network data

Extending ICSSIM - and Compare with real environment

THANK You