CPS-SR
CPS-IoT Week 2019
April 15 - 18, 2019
Montreal, Canada

Tsinghua University

Intrusion Detection of Networked Cyber-Physical Systems via Three-Level Deep Packet Inspection

Jianghai LI, Wen Si, Xiaojin Huang
Institute of Nuclear Energy Technology (INET)
Tsinghua University
April, 2019

Outline

- Introduction of INET of Tsinghua Univ.
- Cybersecurity of Networked CPS
- Three Level of Deep Packet Inspection
- Intrusion Detection based on Neural Network
- Data Capture and Results
- Conclusions

Tsinghua University

A comprehensive and research-intensive university

- **Founded in 1911**

19 schools
55 departments

- **Engineering**
- **Science**
- **Humanities and Social Sciences**
- **Architecture**
- **Arts and Design**
- **Medicine**
- **……**

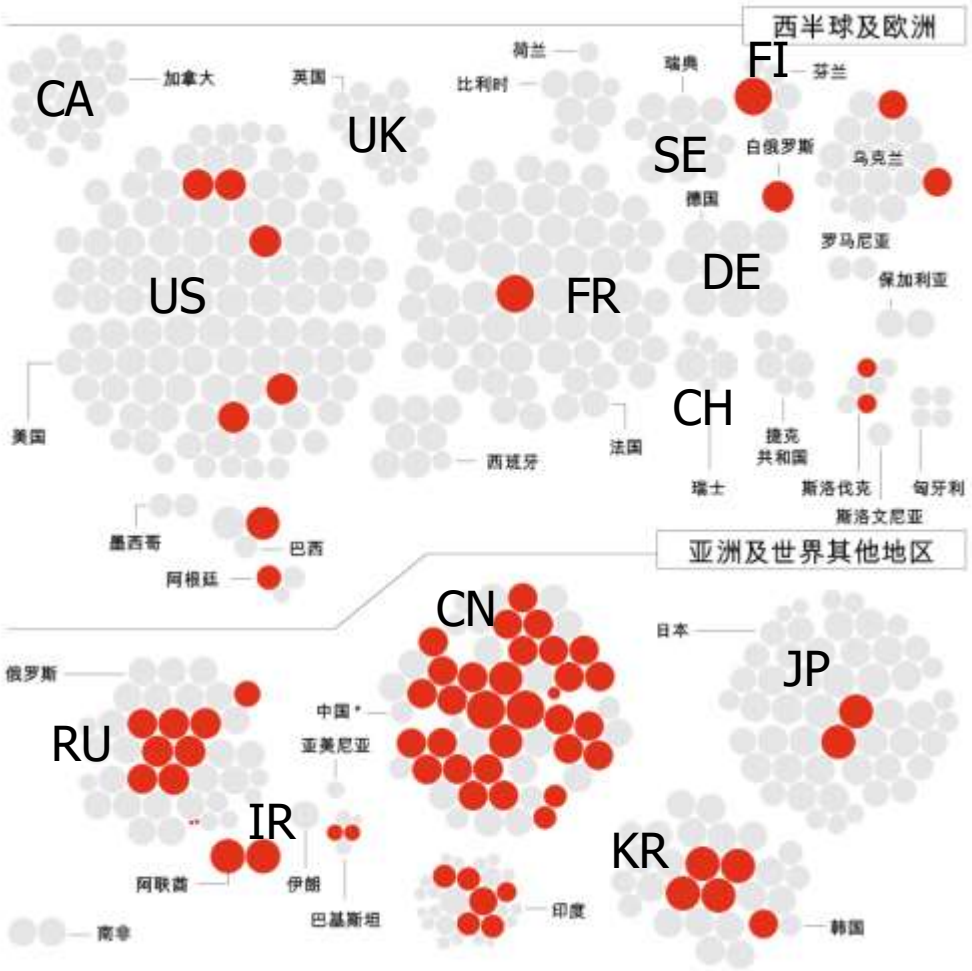
INET

- INET
  - Institute of Nuclear and New Energy Technology, Tsinghua University, Beijing, China
  - Founded in 1960s
- Research Areas
  - Advanced Nuclear Energy Technology (three research reactors)
    - A twin-core experimental shielding reactor
    - A 5MW nuclear heating reactor (NHR-5)
    - A 10MW modular high temperature gas-cooled reactor (HTR-10): a type of Gen-IV reactor
  - Nuclear Technology
    - ^{60}Co container inspection system
  - New Energy Technology
    - Lithium-ion batteries and fuel cells
  - Energy Policy Research

HTR-PM: a commercial NPP

- High Temperature Gas-cooled Reactor - Pebble-Bed Module
  - Total thermal power: 2*250MWth
  - Rated electrical power: 210MWe
  - Primary helium press: 7MPa
  - Temperature at inlet/outlet: 250/750 ℃

NPP Plan of China



Fortune China, 2014

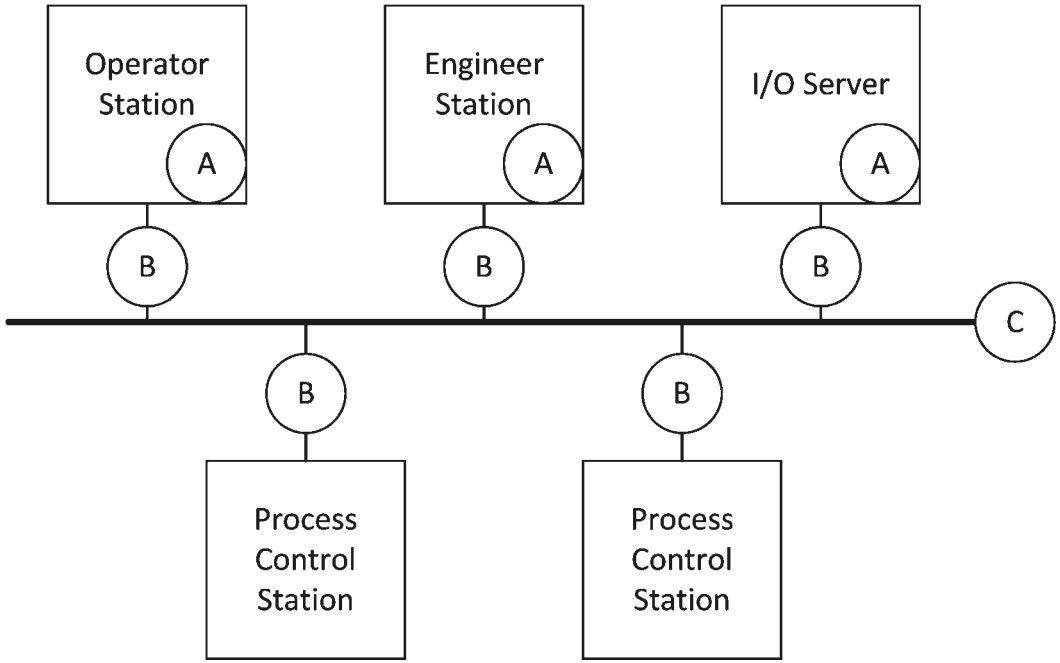
Main Control Room - 3D Model

Outline

- Intro of INET of Tsinghua Univ.
- Cybersecurity of Networked CPS
- Three Level of Deep Packet Inspection
- Intrusion Detection based on Neural Network
- Data Capture and Results
- Conclusions

Networked CPS

- Industrial Control Systems (ICS)
  - P: sensors and actuators
  - C: control programs



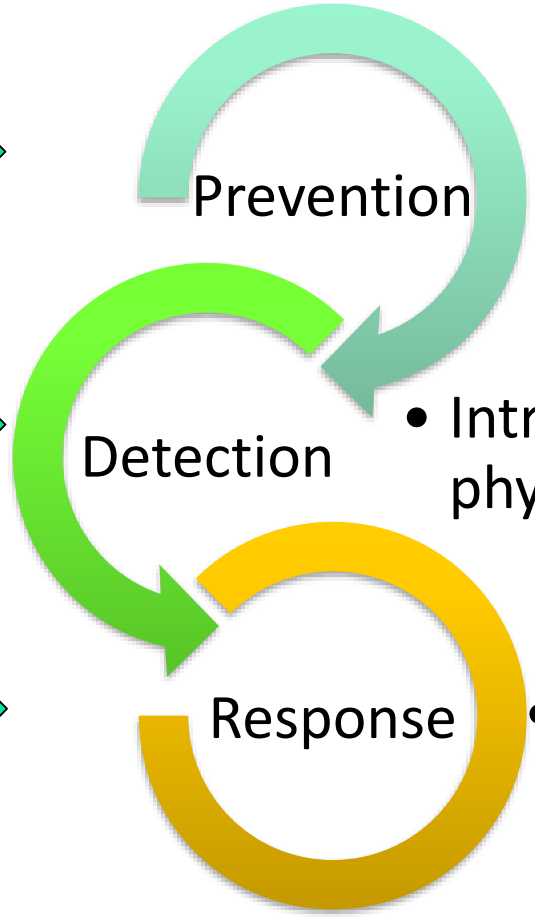
- Networking Protocols
  - Not standard TCP/IP
  - Modbus, Siemens S7, OPC UA
- Commercial IDS
  - Proprietary ones
  - TCP/IP variants

Difficulties

Real-time Requirement

Proprietary Protocol

Operational continuity



- ICS-SIEM
- Intrusion Detection based on physical data
- Intrusion-tolerant Control

Outline

- Intro of INET of Tsinghua Univ.
- Cybersecurity of Networked CPS
- Three Level of Deep Packet Inspection
- Intrusion Detection based on Neural Network
- Data Capture and Results
- Conclusions

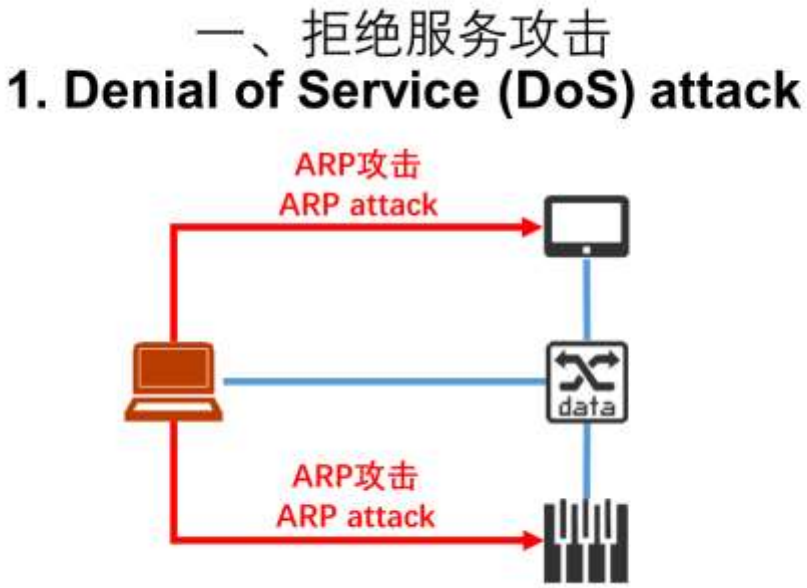
Categories of Hackers based on Their Abilities

IT Hackers	• skilled with IT security • unaware of industrial control
ICS Hackers	• skilled with IT security • familiar with ICS and protocols
NPP Hackers (Process Hackers)	• skilled with IT security • familiar with I&C systems • access **NPP (Process) information**

INIT

Deny of Service

- by IT hackers
  - Intercept data packets of HMI commands
- Effect: operators lose control of PLC

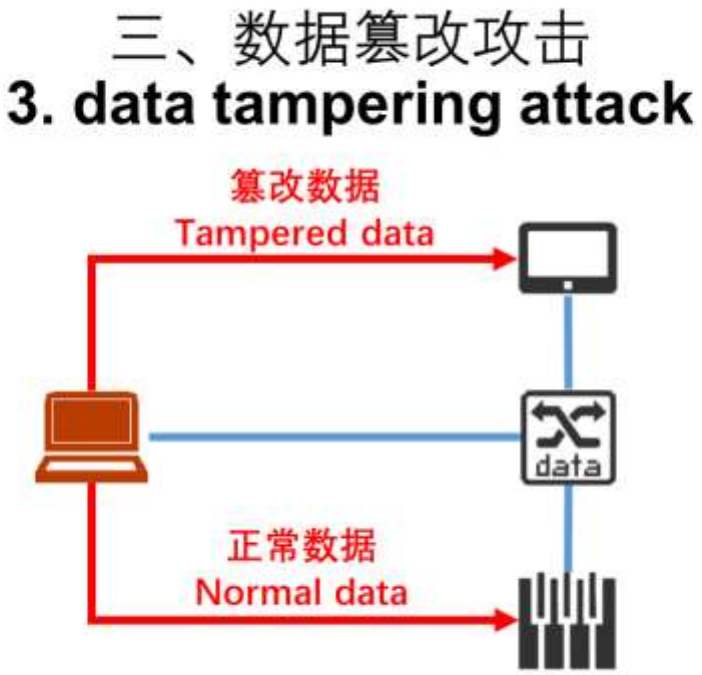


Command Injection

- by ICS hackers
  - Inject the STOP command of PLC
- Effect: PLC offline

Data Falsification

- by NPP hackers
  - falsify the feedback data to HMI
- Effect: Operators deceived



Three-level Deep Packet Inspection

- 1. Network level
  - Inspection with networking protocols (TCP/IP)
  - Network flow statistics and packet analysis
  - Commercial IDS for Internet
- 2. Control level
  - Inspection with control protocols (Modbus, S7, ...)
  - Values of the protocol fields
  - ICS-IDS
- 3. Process level
  - Inspection with control configuration
  - Physical data: Quantities or commands, such as temperature, pressure, valve status, motor start/stop command
  - ICS-IDS customized for NPP

Deep Packet Inspection

```
00 04 17 02 58 b7 78 e7  d1 e0 02 5e 08 00 45 00
00 34 70 27 40 00 80 06  00 00 8d 51 00 0a 8d 51
00 56 df 60 01 f6 54 dc  43 66 80 54 d3 26 50 18
f9 71 1b 29 00 00 00 00  00 00 00 06 ff 04 08 d2
00 02
```

```
00 04 17 02 58 b7 78 e7  d1 e0 02 5e 08 00 45 00
00 34 70 27 40 00 80 06  00 00 8d 51 00 0a 8d 51
00 56 df 60 01 f6 54 dc  43 66 80 54 d3 26 50 18
f9 71 1b 29 00 00 00 00  00 00 00 06 ff 04 08 d2
00 02
```

```
00 04 17 02 58 b7 78 e7  d1 e0 02 5e 08 00 45 00
00 34 70 27 40 00 80 06  00 00 8d 51 00 0a 8d 51
00 56 df 60 01 f6 54 dc  43 66 80 54 d3 26 50 18
f9 71 1b 29 00 00 00 00  00 00 00 06 ff 04 08 d2
00 02
```

- IPv4
  Src IP = 141.81.0.10
  Dest IP = 141.81.0.86
  Src port = 57184
  Dest port = 502
- Function code = 4 (Read input registers)
  Reference number = 2258 (Staring address)
  Word count = 2 (Number of registers)

Outline

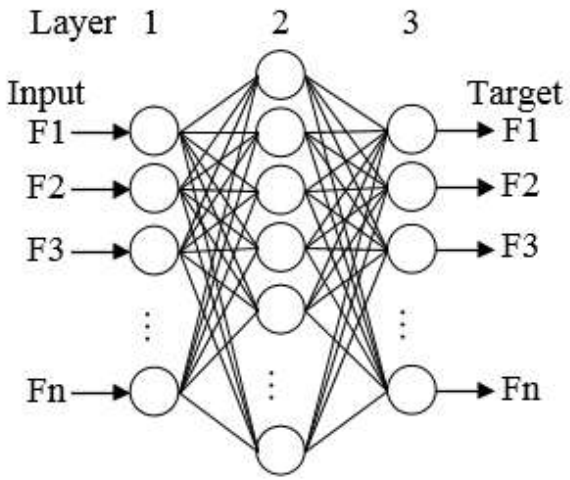
- Intro of INET of Tsinghua Univ.
- Cybersecurity of Networked CPS
- Three Level of Deep Packet Inspection
- Intrusion Detection based on Neural Network
- Data Capture and Results
- Conclusions

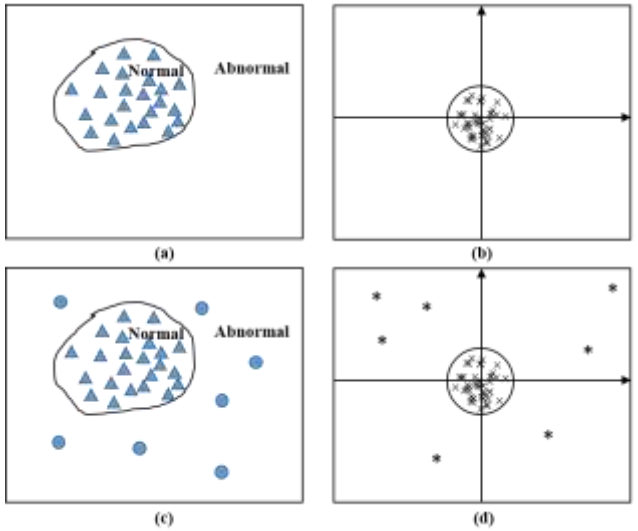
Intrusion Detection Algorithms

- Characteristic detection
  - Based on known malicious data models
  - Efficient and accurate, only for known attacks
  - Applied in control level inspection
- Anomaly detection
  - Based on a legal behavior model, either by experts, or by machine learning
  - for unknown attacks, false alarms
  - Applied in process level inspection
- Still an open question

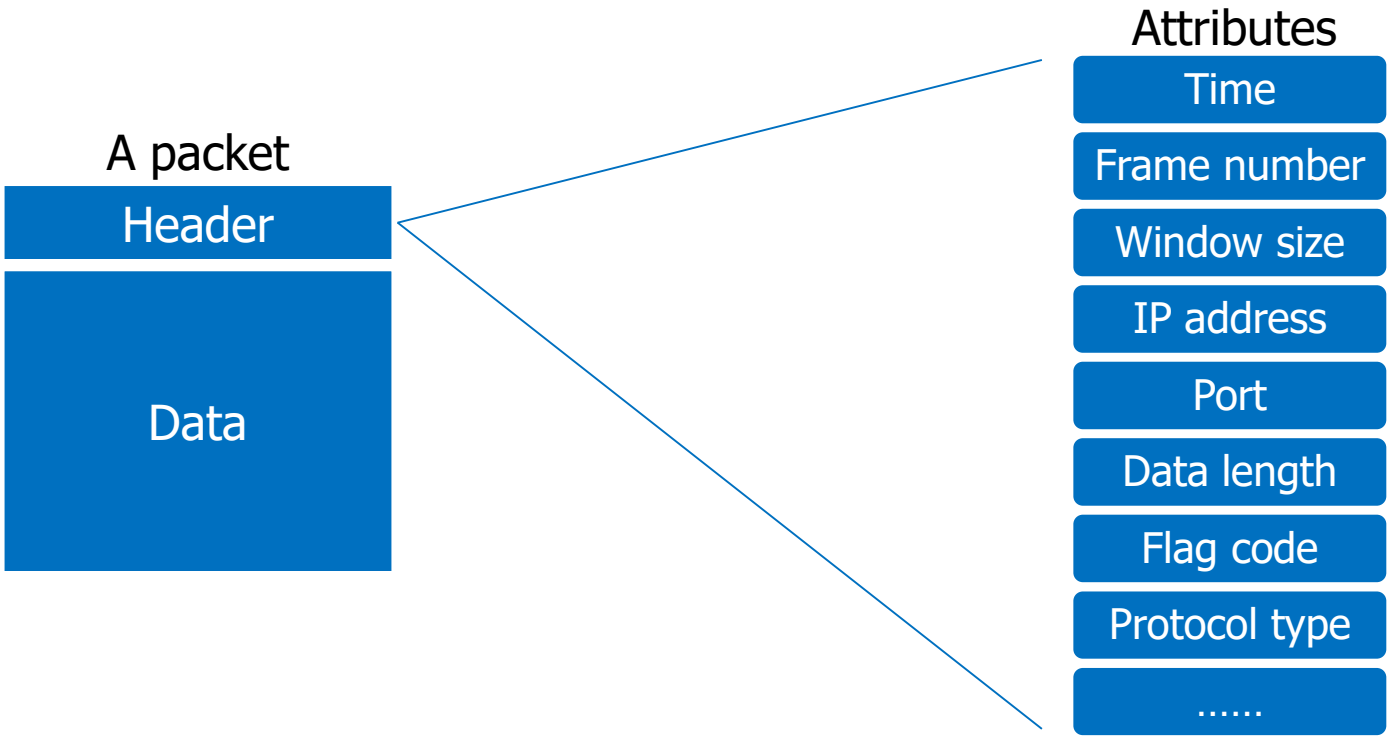
One-class Detection based on RNN

- Why One-class?
  - Few attack data, while abundant normal data
- Replicator neural network (RNN)
  - replicating the input data as the desired outputs, with the same number of neurons in output layer and the input layer



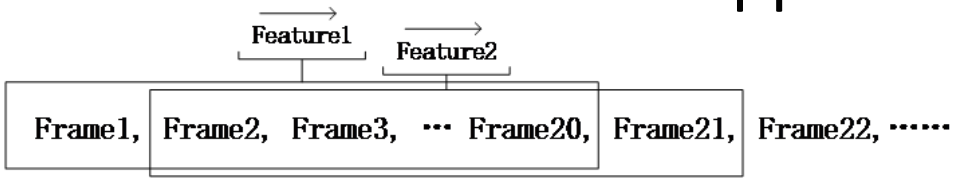


Feature extraction



Feature extraction

- Sliding window feature extraction approach



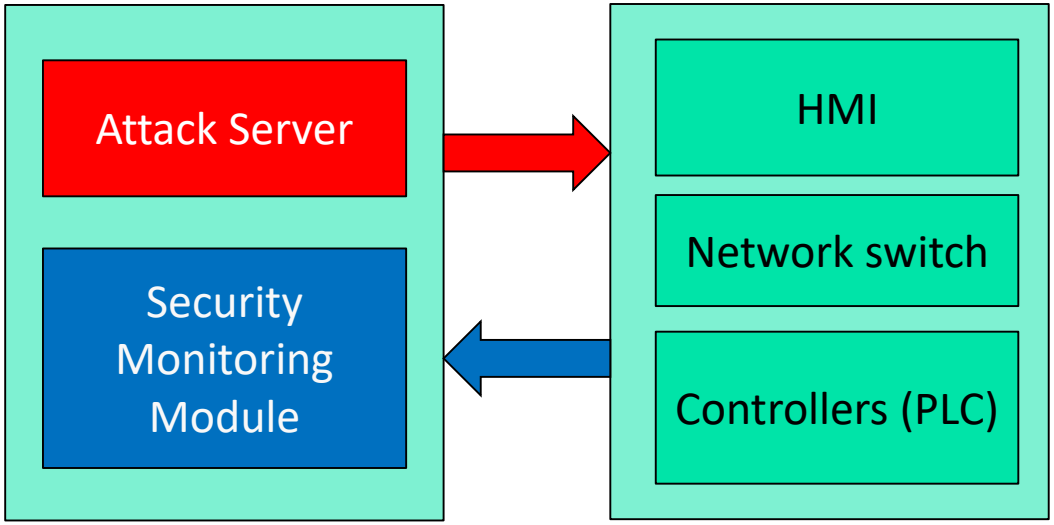
Features extracted from packet headers	
Average time interval	Number of packets with a 0 data length
Number of IP addresses	Number of ports
Number of packets using ARP protocol	Average data length
Number of sorts of flag codes	Average frame length
Number of packets with a 0 window size	Average total length of packets

Outline

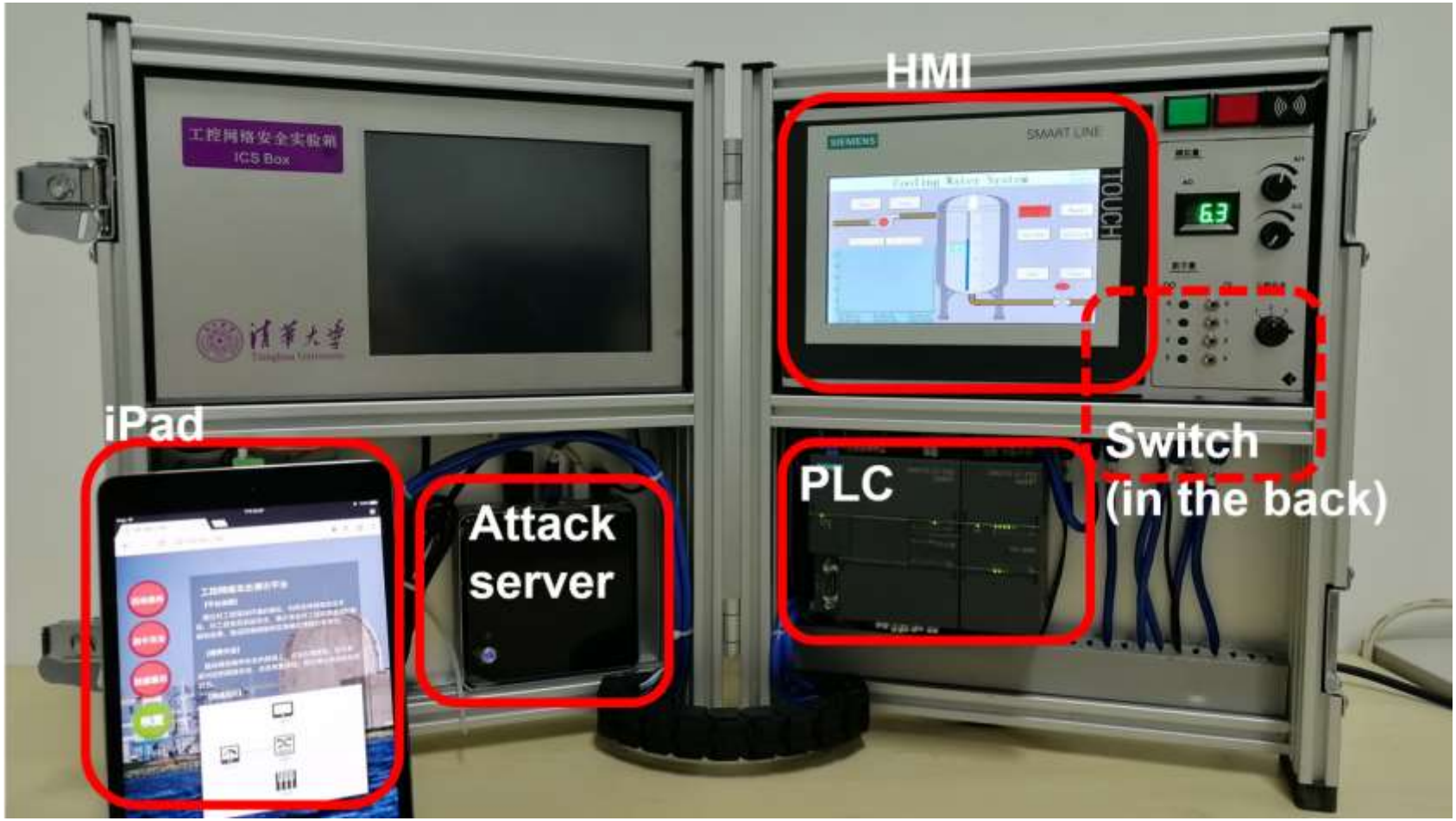
- Intro of INET of Tsinghua Univ.
- Cybersecurity of Networked CPS
- Three Level of Deep Packet Inspection
- Intrusion Detection based on Neural Network
- Data Capture and Results
- Conclusions

Security Test Box

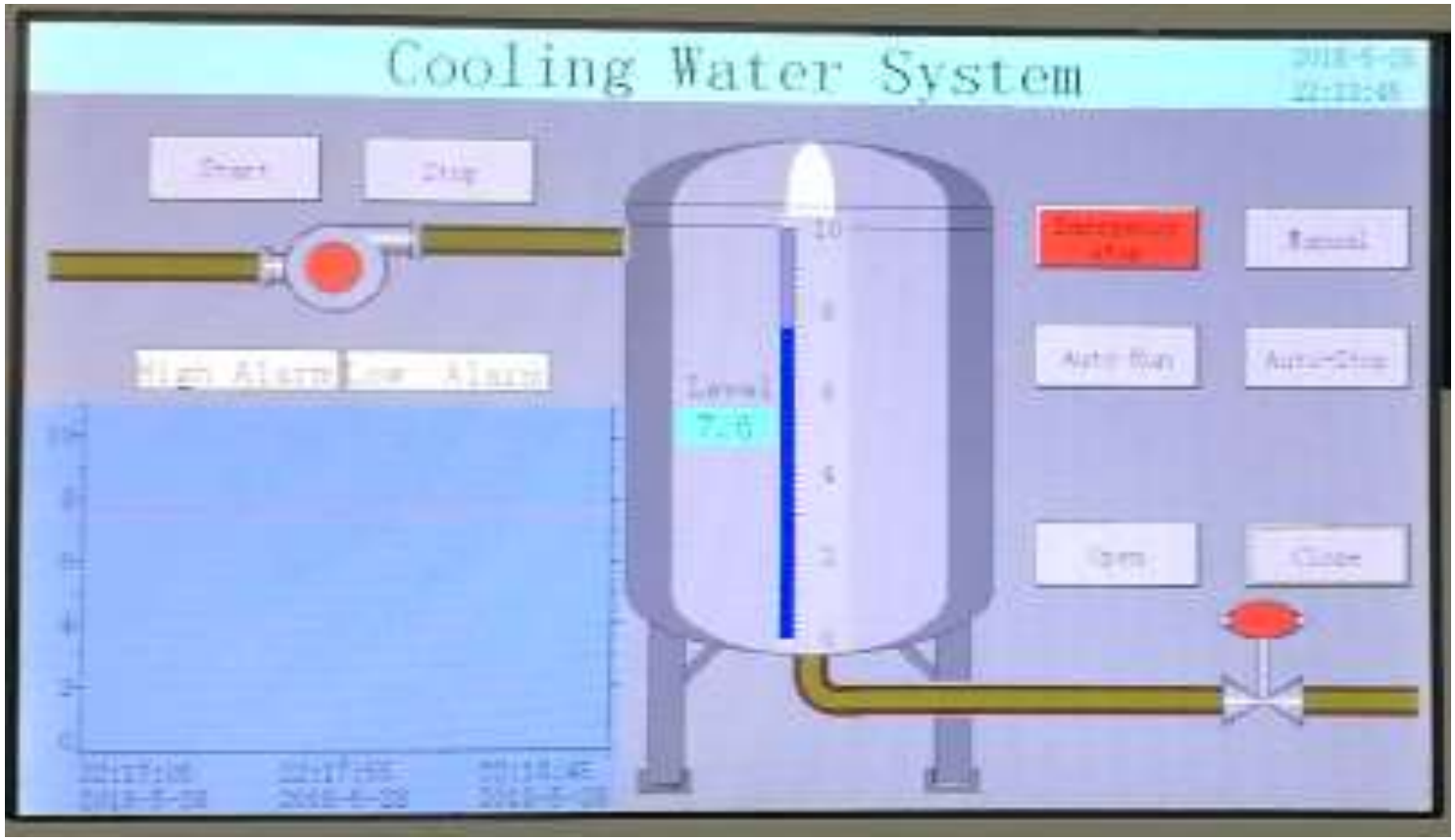
- Attack Generation
- Intrusion Detection
- I&C Testbed



Structure of Test Box

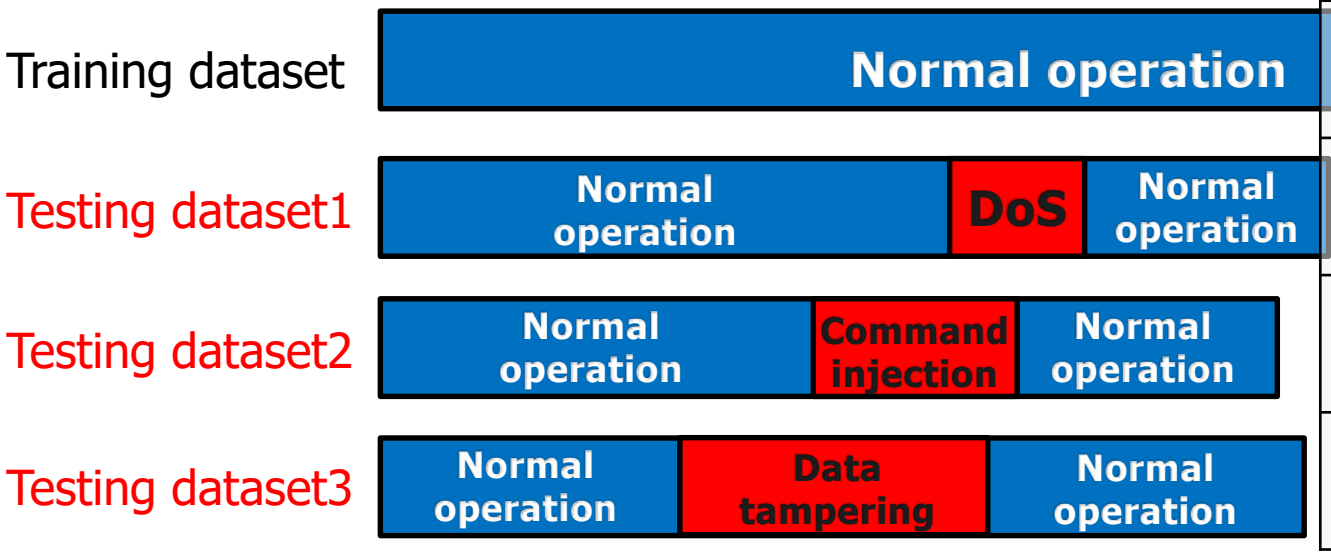


Cooling Water System



Video

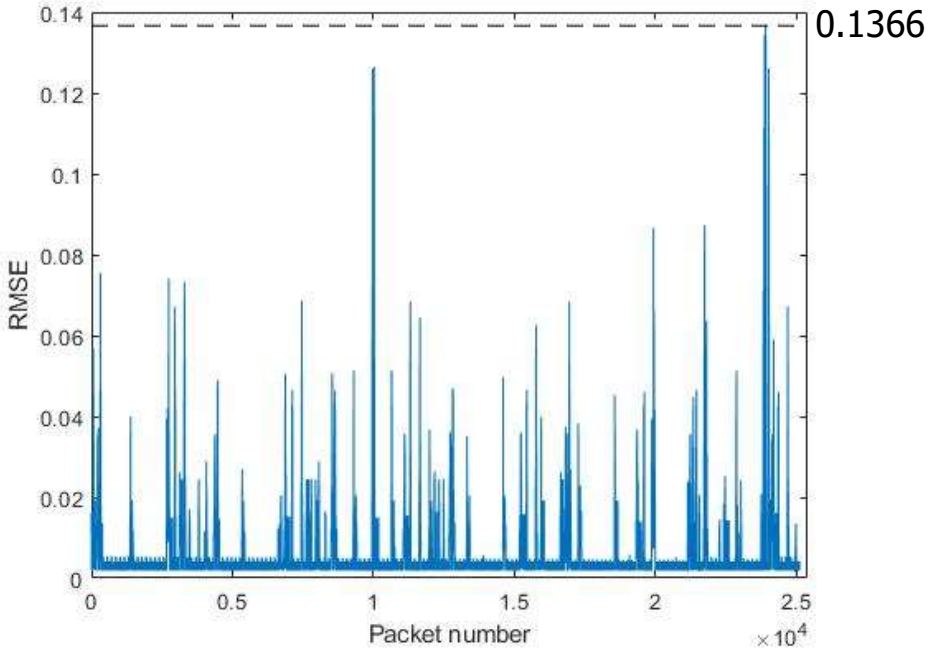
Structure of Datasets



	normal	abnormal
Training dataset	25121	0
Testing dataset1	4936	820
Testing dataset2	2688	1556
Testing dataset3	2963	2282

Training of RNN

- $RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - t_i)^2}$
- is used to measure the difference between output and input
- To enhance robustness of our model, we set 3 times of the max value of *RMSE* as the threshold



Attack Detection and Identification

Wen SI, Jianghai LI, Xiaojin HUANG, One-class Anomaly Detection for I&C Systems based on Replicator Neural Networks, NPIC-HMIT 2019, Orlando, FL, US, Feb. 2019.

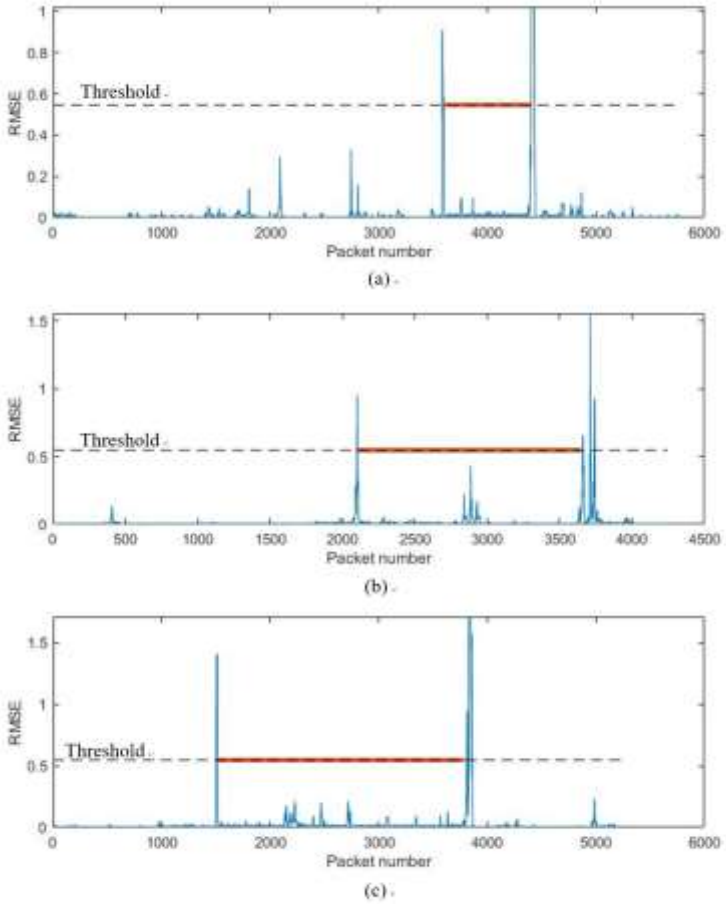
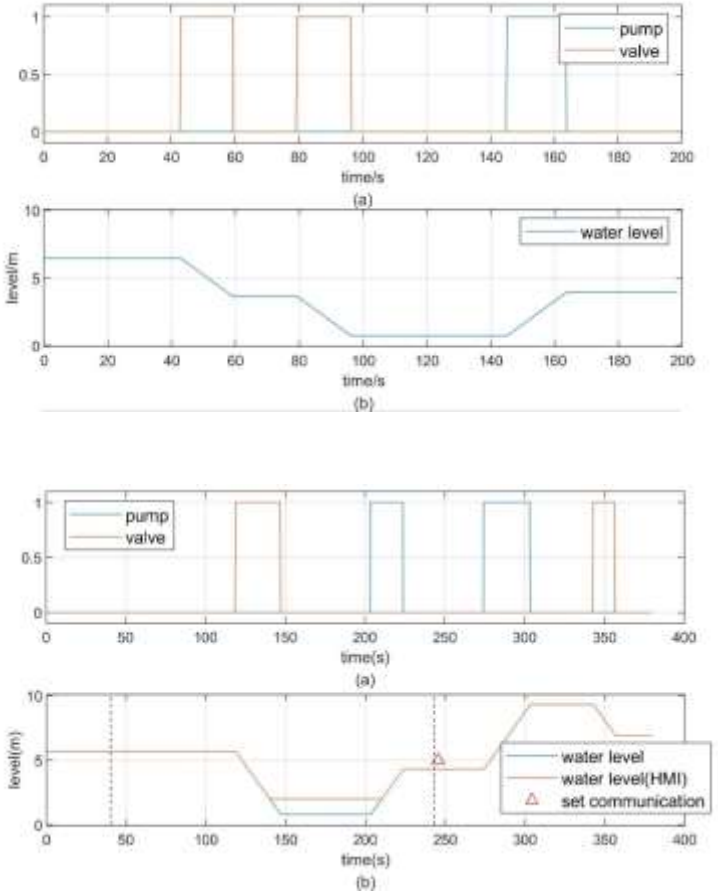


Figure 8. Anomaly detection evaluation using 3 testing datasets. (a) Testing dataset1 (b) Testing dataset2 (c) Testing dataset3

Wen SI, Jianghai LI, Xiaojin HUANG, Attack Identification In I&C Systems based on Physical Data, ICONE27, accepted



Conclusions

- Three classes of hackers and attacks
- Three levels of DPI
- Intrusion detection based on replicator neural network
- ICS security test box for data capture

清華大學
Tsinghua University

Thank you.

Jianghai LI

+86-133-6647-7697

lijianghai@tsinghua.edu.cn

INET