

ANOMALY DETECTOR FOR CYBER-PHYSICAL INDUSTRIAL SYSTEMS

ANNA GUINET TELECOM SUDPARIS FRANCE

> iCIS Radboud University



9th November 2018

CONTENTS

1. PRESENTATION

2. CYBER-PHYSICAL SYSTEMS

- 2.1 Presentation
- 2.2 Networked control systems
- 2.3 Cyber-physical attacks

3. PIETC-WD

- 3.1 Presentation
- 3.2 Normal functioning
- 3.3 First sensor alarm
- 3.4 Second sensor alarm
- 3.5 Validation

4. CONCLUSION

PRESENTATION



Master's De Telecom Su <i>Cybersecur</i>	egree dParis ty spe	cialization	Cy Tr In	/bersecurity engineer hales C&S tegration & risk analysis
2016		2017		2018
	Senio Univer <i>Trust r</i>	r Internship sity of Malaga <i>metrics for the l</i>	оТ	Research associate (<i>Ingénieure de recherche</i>) Telecom SudParis <i>CPS resilience</i>
 Cryptog Networl Darknet Risk and 	graphy k secui ts stud alysis :	rity (IP protocols y (senior projec EBIOS 2010	 Industrial control systems (ICS) SCADA systems & protocols roject) Human threats in CPS : HCI, etc. 	

CONTENTS

1. PRESENTATION

2. CYBER-PHYSICAL SYSTEMS

- 2.1 Presentation
- 2.2 Networked control systems
- 2.3 Cyber-physical attacks

3. PIETC-WD

- 3.1 Presentation
- 3.2. Normal functioning
- 3.3 First sensor alarm
- 3.4 Second sensor alarm
- 3.5 Validation
- 4. CONCLUSION

Cyber-Physical System (CPS): Systems that integrate Computation, Communication and Control-Physical processes

Lee and Seshia (2016). Introduction to embedded systems: A cyber-physical systems approach. MIT Press.

Moreover...

Systems with integrated computational and physical capabilities that **can interact with humans** through many new modalities

Baheti and Gill (2011). Cyber-physical systems. The impact of control technology.

Cyber-physical systems have today the following features:

- Large scale large number of physically distributed subsystems
- **Complex** large number of variables, non-lineary & uncertainty
- Human in the loop human beings & feedback control systems

Examples:

- Industrial control systems
- Intelligent transportation systems

Smart cities

E-health



Difference between ICT and ICS

	ICT	ICS
Aim	Information protection	Safety of services and people
Lifetime	<5 years	>10 years
Security	↑ Confidentiality	↑ Availability
properties	Integrity	Integrity
priorities	Availability	Confidentiality
Network	TCP/IP	SCADA (and TCP/IP)
Connectivity	Connected to Internet	Isolated (or strong restrictions)

Cyber-physical resilience

Offer critical functionalities (e.g. safety functions) under the presence of

failures and attacks

A resilient control systems should*:

Identify threats

Minimize their impact

Mitigate them, or recover to a normal operation in a reasonable time

*Queiroz (2012). A holistic approach for measuring the survivability of SCADA systems. PhD, RMIT University.

Networked control system: Control system whose control loops are connected through a communication network



Modeling of CPS using feedback control theory

Controller commands the system using corrective feedback, based on the distance between a reference signal and the system output

2 CYBER-PHYSICAL SYSTEMS 2.3 CYBER-PHYSICAL ATTACKS

A **cyber-physical attack** exploits vulnerabilities, to harm the physical processes through the network



Teixeira, Shames, Sandberg, & Johansson (2015). A secure control framework for resource-limited adversaries. *Automatica*, *51*, 135-148.

False-data injection attack

- How: Modification of sensors reading by physical interferences, by the communication channel or individual meters to generate wrong control decisions
- Attack capabilities: Limited knowledge of the physical system required
- **Countermeasure:** Comparison of sensor measurements and system dynamics



Replay attack

- **How**: Replay previous sensor measurements and modification of control inputs
- > Attack capabilities: No knowledge of the physical system required
- **Countermeasure:** Add some protection on input control signals



Replay attack

- **How**: Replay previous sensor measurements and modification of control inputs
- > Attack capabilities: No knowledge of the physical system required
- **Countermeasure:** Add some protection on input control signals



Replay attack

- **How**: Replay previous sensor measurements and modification of control inputs
- > Attack capabilities: No knowledge of the physical system required
- **Countermeasure:** Add some protection on input control signals



Covert attack

- **How**: Modification of control inputs and sensor measurements
- > Attack capabilities: Knowledge of the physical system required
- **Countermeasure:** Undetectable from the regular system operation



DoS attack

How: Disrupt the communication on a channel to isolate the monitor process

Zero dynamic attack

- **How:** Disrupt the unobservable part of the system
- **Countermeasure:** Verify if all the states are observable

Command injection attack

- **How:** Exploit protocols and devices vulnerabilities to inject false commands
- **Countermeasure:** Signature-based IDS

CONTENTS

1. PRESENTATION

2. CYBER-PHYSICAL SYSTEMS

- 2.1 Presentation
- 2.2 Networked control systems
- 2.3 Cyber-physical attacks

3. PIETC-WD

- 3.1 Presentation
- 3.2 Normal functioning
- 3.3 First sensor alarm
- 3.4 Second sensor alarm
- 3.5 Validation

4. CONCLUSION

Periodic and intermittent event-triggered control watermark detector

System specifications:

- Discrete linear time-invariant LTI system
- Linear Quadratic Gaussian LQG controller

Strategy:

- Challenge-response authentication scheme
- Non-stationary watermark-based (noise) to verify the integrity of the

control loop

Countermeasure against adversaries that have partial or full knowledge of the

system dynamics

Penalty: performance loss

Mo, Weerakkody, & Sinopoli. (2015). Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Systems*, *35*(1), 93-109. Rubio-Hernan, De Cicco & Garcia-Alfaro (2016). Event-triggered watermarking control to handle cyber-physical integrity attacks. In *Nordic Conference on Secure IT Systems* (pp. 3-19). Springer, Cham.





$$x_{t+1} = Ax_t + Bu_t + w_t$$

with $A \in \mathbb{R}^{p \times p}$ state matrix $B \in \mathbb{R}^{p \times m}$ input matrix $w_t \sim N(0, Q)$ noise

$$y_t = Cx_t + v_t$$

with $C \in \mathbb{R}^{n \times p}$ output matrix $v_t \sim N(0, R)$ noise

3 PIETC-WD 3.2 NORMAL FUNCTIONING



Cyber-physical adversary

Aim: Use identification methods to gain knowledge about the system parameters, from the network, to influence the physical behavior.



3 PIETC-WD 3.3 FIRST SENSOR ALARM



3 PIETC-WD 3.4 SECOND SENSOR ALARM



SCADA Testbed

- LEGO Mindstorm EV3 & Raspberry Pi
- Closed-loop system with wired and wireless communications



3 PIETC-WD 3.5 VALIDATION



CONTENTS

1. PRESENTATION

2. CYBER-PHYSICAL SYSTEMS

- 2.1 Presentation
- 2.2 Networked control systems
- 2.3 Cyber-physical attacks

3. PIETC-WD

- 3.1 Presentation
- 3.2. Normal functioning
- 3.3 First sensor alarm
- 3.4 Second sensor alarm
- 3.5 Validation

4. CONCLUSION

▶ PIETC-WD

- Decentralized detection mechanism with non-stationary watermark
- Detection of integrity cyber-physical attacks
- Impacts:
 - Performance
 - Detection time

Future Work: Resilient CPSs

- More thorough analysis of PIETC-WD
- Mitigation of cyber-physical attacks
 - Programmable networking

References

- Lee and Seshia (2016). Introduction to embedded systems: A cyber-physical systems approach. MIT Press.
- Baheti and Gill (2011). Cyber-physical systems. The impact of control technology.
- Queiroz (2012). A holistic approach for measuring the survivability of SCADA systems. PhD, RMIT University.
- Teixeira, Shames, Sandberg, & Johansson (2015). A secure control framework for resourcelimited adversaries. *Automatica*, 51, 135-148.
- Rubio-Hernan (2017). Detection of attacks against cyber-physical industrial systems, PhD, INT.
- Rubio-Hernan, De Cicco & Garcia-Alfaro (2016). Event-triggered watermarking control to handle cyber-physical integrity attacks. In *Nordic Conference on Secure IT Systems* (pp. 3-19). Springer, Cham.
- Mo, Weerakkody, & Sinopoli. (2015). Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Systems*, 35(1), 93-109.

ANNEXES

31

1 / Bridge and toll testbed

3 / Railway control testbed

2 / Industrial chain testbed

4 / Autonomous industrial agents testbed

Local controllers architecture

Performance loss

LQG controller performance loss: quadratic cost J

$$J = \lim_{n \to \infty} E\left[\frac{1}{n} \sum_{i=0}^{n-1} \left(x_i^T \Gamma x_i + u_i^T \Omega u_i\right)\right] \text{ with}$$

 $u_t \in \mathbb{R}^m$ control input $x_t \in \mathbb{R}^p$ state vector $\Gamma \in \mathbb{R}^{p \times p}$ positive definite cost matrix $\Omega \in \mathbb{R}^{m \times m}$ positive definite cost matrix

Non-stationary performance loss: quadratic cost ΔJ_s

$$J = J^* + \Delta J_s$$

$$\beta = E[\Delta s^{(i)}] + Var[\Delta s^{(i)}]$$

SCADA Components

Supervisory Control And Data Acquisition (SCADA): A technology to

monitor industrial environments

Programmable Logic Controller (PLC): Microprocessors-based devices

to control and acquire inputs/outputs

- Intelligent Electronic Device (IED): Small microprocessors with limited capabilities in power systems
- Remote Terminal Unit (RTU): Stand-alone data acquisition and control units on a remote site via telemetry
- Master Terminal Unit (MTU): Control center of the system to collect, store and control data from RTUs and PLCs
- Human-Machine Interface (HMI): Displays real-time operation information about the processes to the operators to coordinate and control the system

ISA 95

Definition of the different levels of SCADA Systems

- Level 0 Field level: Physical plant
- **Level 1 Direct control**: Measurement and manipulation of the plant
- **Level 2 Plant Supervisory**: Control and supervision systems of the plant
- Level 3 Production control: Work flow to produce the desired end products and optimization of the system
- Level 4 Production scheduling: Establishment of the basic plant

schedule (production, delivery, inventory, etc.)

5 ANNEXES 5.3 SCADA & PROTOCOLS

SCADA protocols

Modbus

PROFINET

▶ PROFIBUS

DNP3

IEC-60870-5-104

EtherNet/IP

Ethernet Powerlink

AGA-12, etc.

/!\ Designed for safety and not security /!\

OSI Level	Industrial protocols					
7		PowerLink				
6	PROFINET IO					
5	EtherNet/IP					
4	TCP/UDP					
3	IP					
2	Ethernet	Ethernet PowerLink	Modbus ASCII/RTU PROFIBUS DNP3 AGA-12 IEC-60870-5-101			
1	Physical					

Cyber-physical systems & Software-defined network

Rubio-Hernan, Sahay, De Cicco & Garcia-Alfaro (2018). Cyber-physical architecture assisted by programmable networking. *Internet Technology Letters*, e44.