FUJITSU

shaping tomorrow with you

Securing Cyber-Physical Systems

Alvaro Cárdenas
Fujitsu Laboratories

Ricardo Moreno
Universidad de los Andes

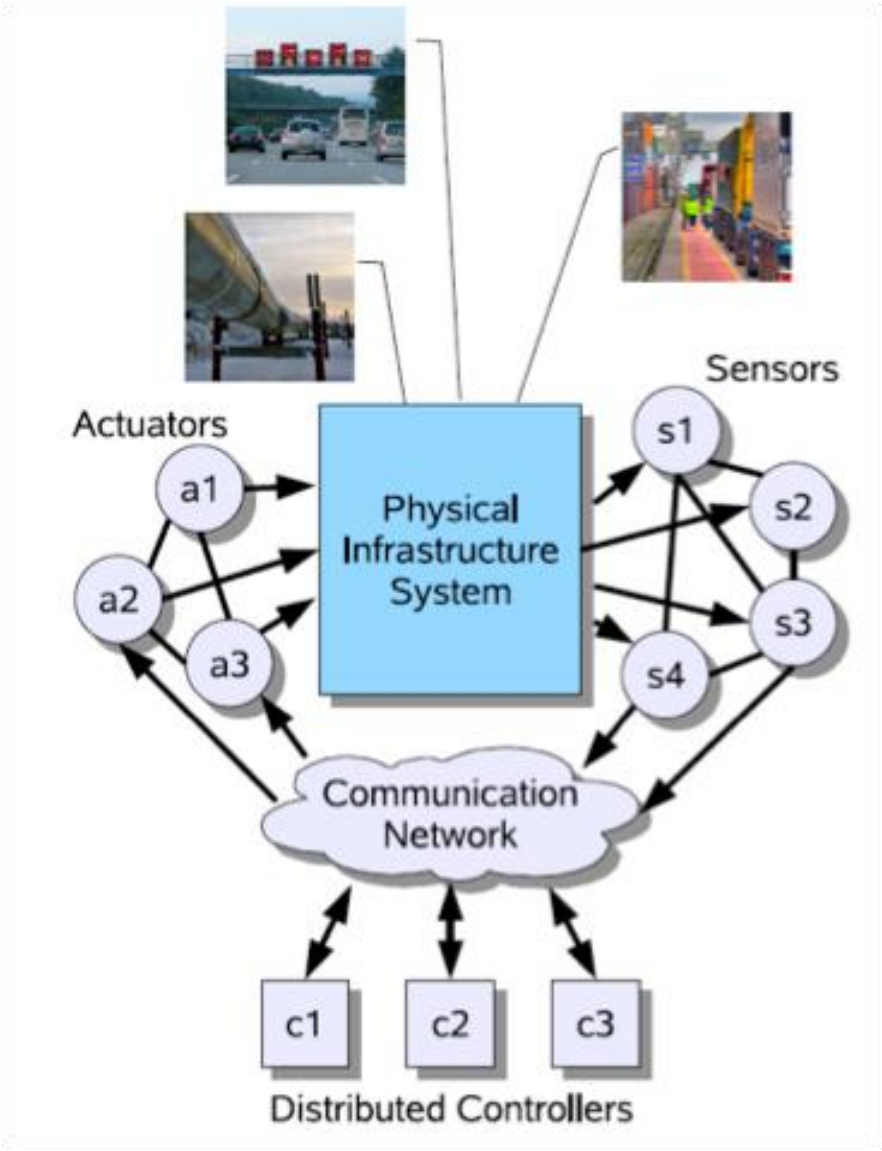
From Sensor Nets to Cyber-Physical Systems

FUJITSU

- Control
- Computation
- Communication

- Interdisciplinary Research!

- Example: Smart Grid



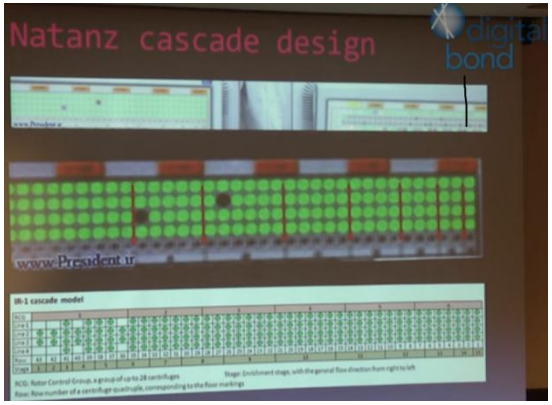
Attacks & Threats

FUJITSU

- Attacks
  - Maroochy Shire 00

  - HVAC 12

  - Stuxnet 10



- Threats

Obama Adm Demonstrates In Feb. 2012 attack to power Grid

US Video Shows Hacker Hit on Power Grid

US Video Shows Potential Destruction Caused by Hackers Seizing Control of Electrical Grid

In this image from video released by the Department of Homeland Security, smoke pours from an expensive electrical turbine during a March 4, 2007, demonstration by the Idaho National Laboratory, which was simulating a hacker attack against the U.S. electrical grid. (AP Photo/Dept. of Homeland Security)

By TED BRIDIS and EILEEN SULLIVAN
Associated Press Writers
WASHINGTON Sep 27, 2007 (AP)

The Associated Press

A government video shows the potential destruction caused by hackers seizing control of a crucial part of the U.S. electrical grid: an industrial turbine spinning wildly out of control until it becomes a smoking hulk and power shuts down.

Font Size A A A
E-mail
Print
Share

Your Opinion

Comment & Contribute

WHAT OTHERS ARE SAYING

44 Comm

I agree with the person(s) about h old t...
locoyoco2 Sep-27

'seems for every smart programm there is...
OFEARTHLYGOOD Sep-27

scare tactics,Someone already pointed out,...
tmarabu Sep-27

COMMENT

Post Video

TALK

Connect with Newsmakers

Securing CPS is Hard

FUJITSU

- Vulnerabilities are increasing
  - Sensors/Controllers are now computers (can be programmed for general purposes)
  - Networked (remotely accessible)
  - By necessity, billions of low-cost embedded devices
  - Physically insecure locations
- Attacks will continue to happen
  - Devices deployed for ~ 20-30 years

Three Steps to Improve CPS Security

FUJITSU

- **Short Term**
  - Incentives
  - Software reliability
  - Solve basic vulnerabilities
- Medium Term
  - Leverage Big Data for Situational Awareness
- Long Term Research
  - Resilient estimation and control algorithms

Security is a Hard Business Case

FUJITSU

- *"Making a strong business case for cybersecurity investment is complicated by the difficulty of quantifying risk in an environment of rapidly changing, unpredictable threats with consequences that are hard to demonstrate"*
  - DoE Roadmap
- Governments are responsible for Homeland Security, and critical infrastructure security
  - Utilities are not (outside their budget/scope?)
  - Problem:
    - Interdependencies (e.g., cascading failures)
    - It doesn't matter if one utility sets an example because this is a weakest security game
  - Nations have much more to lose from an attack than utilities

[Cardenas. CIP Report, GMU, 2012]

Short-term proposal

FUJITSU

- Vendors of equipment for managing control systems have few incentives for secure development programs because customers are not requesting them
- Asset owners need to request vendors secure coding practices, hardened systems, and quick response when new vulnerabilities and attack vectors are identified
- American Law Institute (ALI)
  - Principles of the Law of Software Contracts (2009)
  - Vendors liable for knowingly shipping buggy software
  - Implied warranty of no material hidden defects (non-disclaimable)
  - Software for CIP can be first use case
- Currently congress is debating how to give incentives for asset owners to invest in security
  - Cybersecurity Act 2012 (increase regulation)
  - SECURE-IT Act 2012 (increase data sharing)

Three Steps to Improve CPS Security

FUJITSU

- Short Term
  - Incentives
  - Software reliability
  - Solve basic vulnerabilities
- **Medium Term**
  - Leverage Big Data for Situational Awareness
- Long Term Research
  - Resilient estimation and control algorithms

Again, Security is a Hard Business Case

FUJITSU

- Push back in prices
  - Billions of low-cost embedded devices
  - Can’t have fancy tamper protection
- Security is hard to see
  - Hard to see advantages of hardening devices
- But, Situational Awareness is Fun to see
  - Understand the health of the system
    - Routing protocol, health of the system
  - Identify anomalies
- Big Data is new in Smart Grid
  - Redundancy
  - Diversity
  - Data Analytics to identify suspicious behavior

Big Data Analytics in Smart Grid

FUJITSU

GIGAOM

EVENT

HOME APPLE BROADBAND CLEANTECH CLOUD COLLABORATION MEDI

earth2tech

A note to our readers

We have updated our Privacy Policy and Terms of Service. Review continuing to use the site, you are agreeing to our updated Privacy Service.

This notice should appear only the first time you visit this site.

When big IT goes after big data on the smart grid

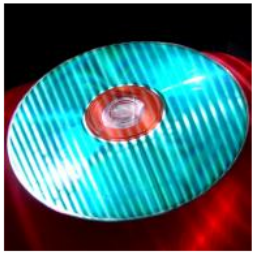
By Adam Lesser | Mar. 20, 2012, 10:49am PT | No Comments

Tweet 136 Share 37 Like 7 +1 6

This article originally appeared on GigaOM Pro, our premium research service (subscription required).

With many utilities facing the task of storing petabytes of smart meter data for as long as seven years in order to satisfy regulatory requirements, the ability to house and leverage the massive load of

Big Data Offers Big Value for Utilities



No end of possibilities for the fearless, forward thinking and imaginative.

Engerati The Final Say

03 Apr 2012 | United States

Share this

Smart meters produce data – it takes work to make the data 'smart.'

What happened

Adam Lesser of Gigaom wrote about the difficulties faced by utilities when dealing with "big data" and the opportunities that this offers to IT companies.

According to Lesser, utilities face petabytes of data that needs to be stored for up to seven years to comply with regulation. Not only that, these utilities also need to "mine" this data and be able to pull out useful information, in a usable format, to allow them to save the time and money promised when deploying smart meters. In other words, make data 'smart.' This poses a "significant IT challenge," one that is new to utilities.

In his report, "Smart Grid Billing Outlook 2012-2016," author Danny Dicks says, "While smart meter deployments have been growing steadily over the last 3-4 years, utilities' IT system priorities have been focused on preparing for how to deal with large volumes of smart meter data. This year we expect to see the emphasis change towards making use of that data – to develop innovative tariffs and new services ... All this will require changes to traditional billing systems and CISs."

Big Data Management for Energy and Smart Grid - Creating the Real-Time Utility Enterprise

Kellogg School of Management | Carnegie Mellon University Silicon Valley

Thursday, April 5, 2012 from 5:00 PM to 9:00 PM (PT)
Mountain View, United States

Ticket Information

TYPE	REMAINING	END		QUANTITY
General	Sold Out	Ended	Free	Sold Out

Enter promotional code

Share this! Email Share Tweet Like 7 people like this. Be the first of your friends.

Event Details

Producer

Kellogg School of Management | Carnegie Mellon University Silicon Valley

Main Sponsor

ORACLE UTILITIES

When & Where

Building 152
Moffett Field, Hwy 101
Mountain View, 94035

Thursday, April 5, 2012 from 5:00 PM to 9:00 PM (PT)

Add to my calendar

CSA Created Working Group on Big Data

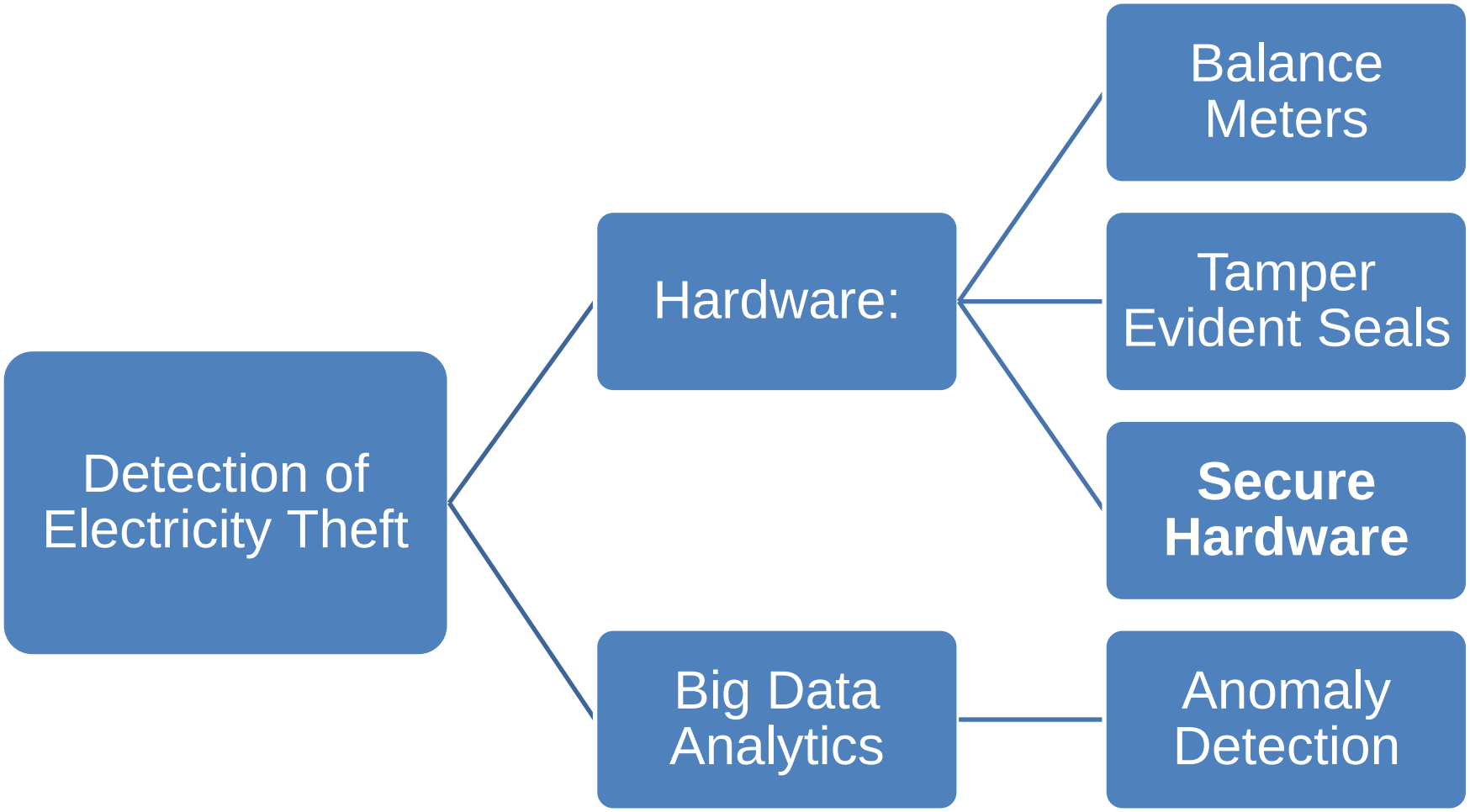
FUJITSU

- Fujitsu is chairing the working group

- Please consider contributing

Case Study: Detection of Electricity Theft

FUJITSU

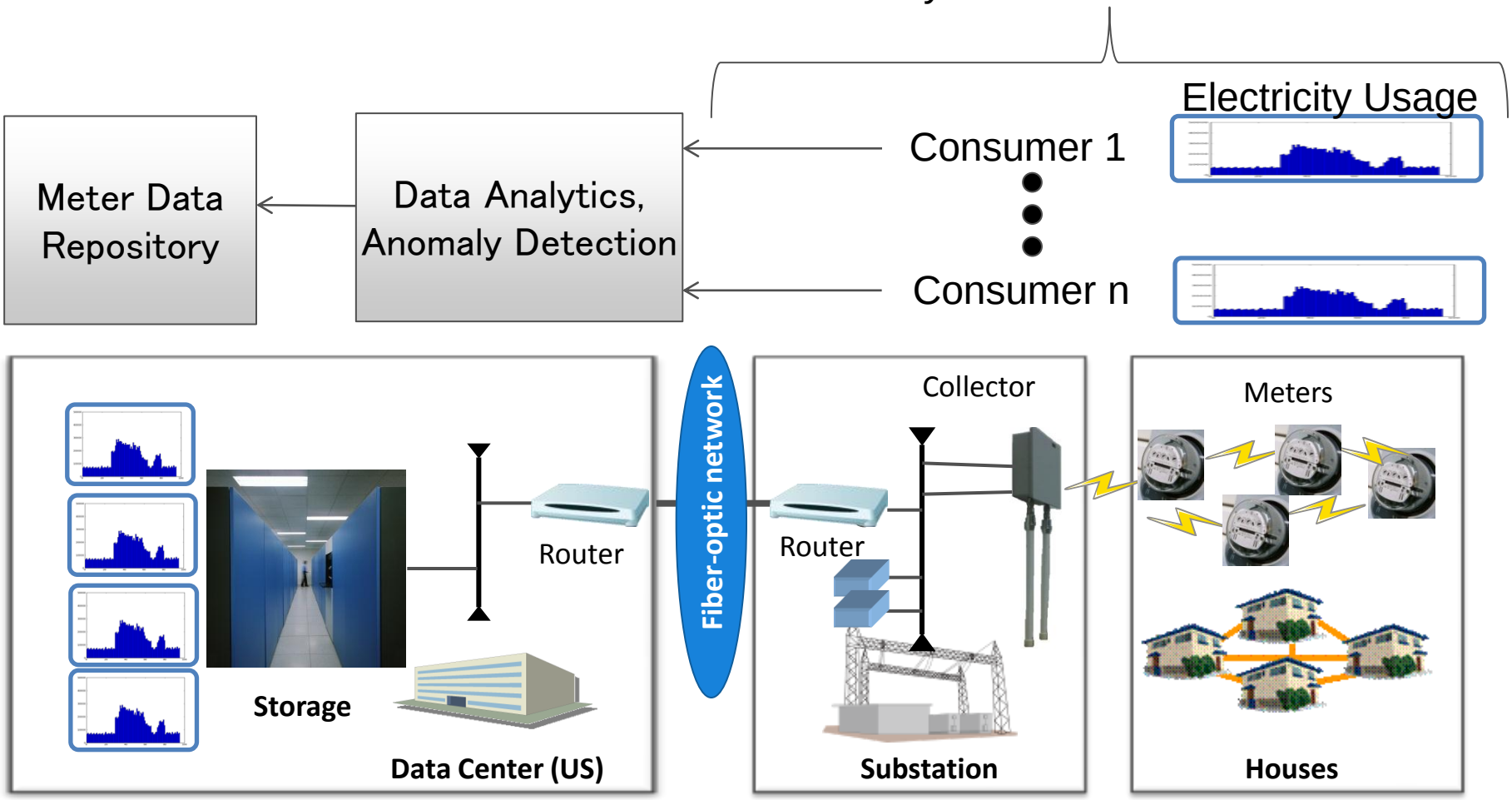


[Mashima, Cardenas. Submitted to RAID, 2012]

Big Data Analytics to Identify Fraud

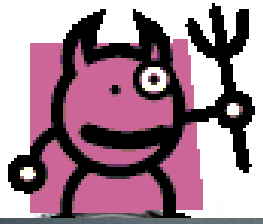
FUJITSU

AMI: Advanced Metering Infrastructure. Smart Meters send consumption data frequently (e.g., every 15 minutes) to the utility



Adversary Model

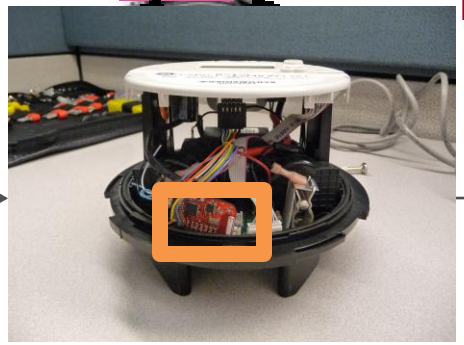
FUJITSU



f(t)

Real Consumption

$$Y_1, \ldots, Y_n$$



a(t)

Fake Meter Readings

$$\hat{Y}_1, \ldots, \hat{Y}_n$$

Utility

Goal of attacker: Minimize Energy Bill:

$$\min_{\hat{Y}_1,\ldots,\hat{Y}_n} \sum_{i=1}^{n} \hat{Y}_i$$

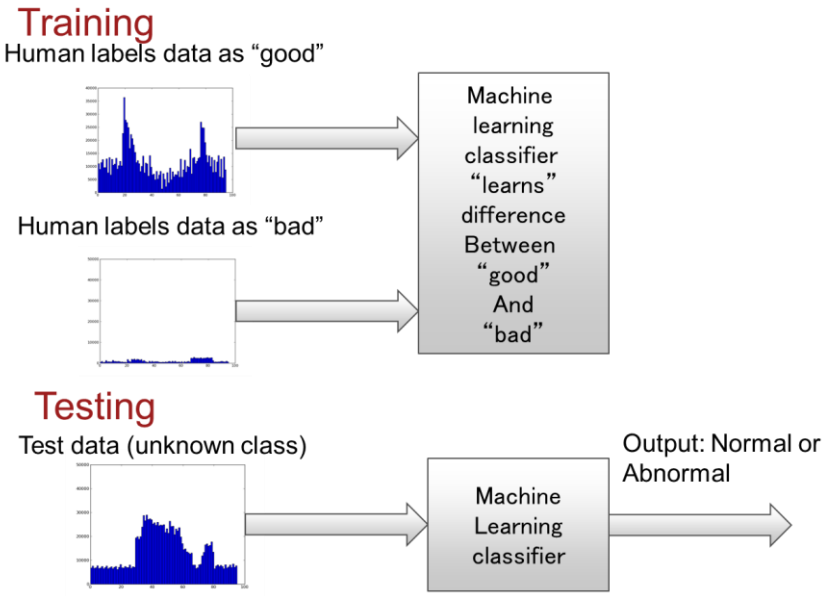
Goal of Attacker: Not being detected by classifier “C”:

$$C(\hat{Y}_1, \ldots, \hat{Y}_n) = \text{ normal}$$

Related Work

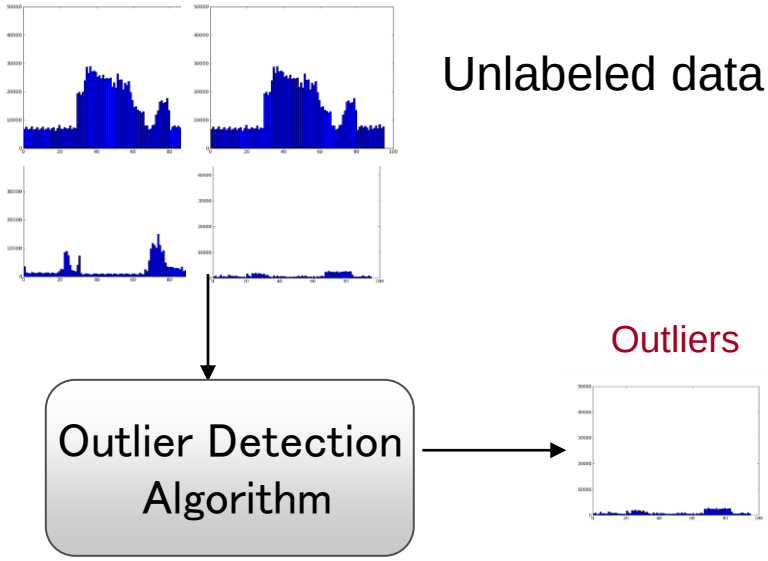
FUJITSU

Supervised Learning



- Problems
  - It is not easy to get “Attack” data
  - A classifier trained with attack data might not be able to generalize to new “smart” attacks

Unsupervised Learning



- Problems
  - Easier to attack
  - More false positives
  - E.g. Local Outlier Factor (LOF) did poorly in our tests

New Idea:

FUJITSU

- We only have “good” data
  - Do not assume we have access to “attack” data
  - Train only one class (“good” class)
- We have prior knowledge of attack invariant
  - We know attackers want to lower energy consumption
  - Include this information for the “bad” class
- Composite Hypothesis Testing formulation:

$$H_0 : P_0$$

$$H_1 : P_\gamma \text{ s.t. } \mathbb{E}_\gamma[Y] < \mathbb{E}_0[Y]$$

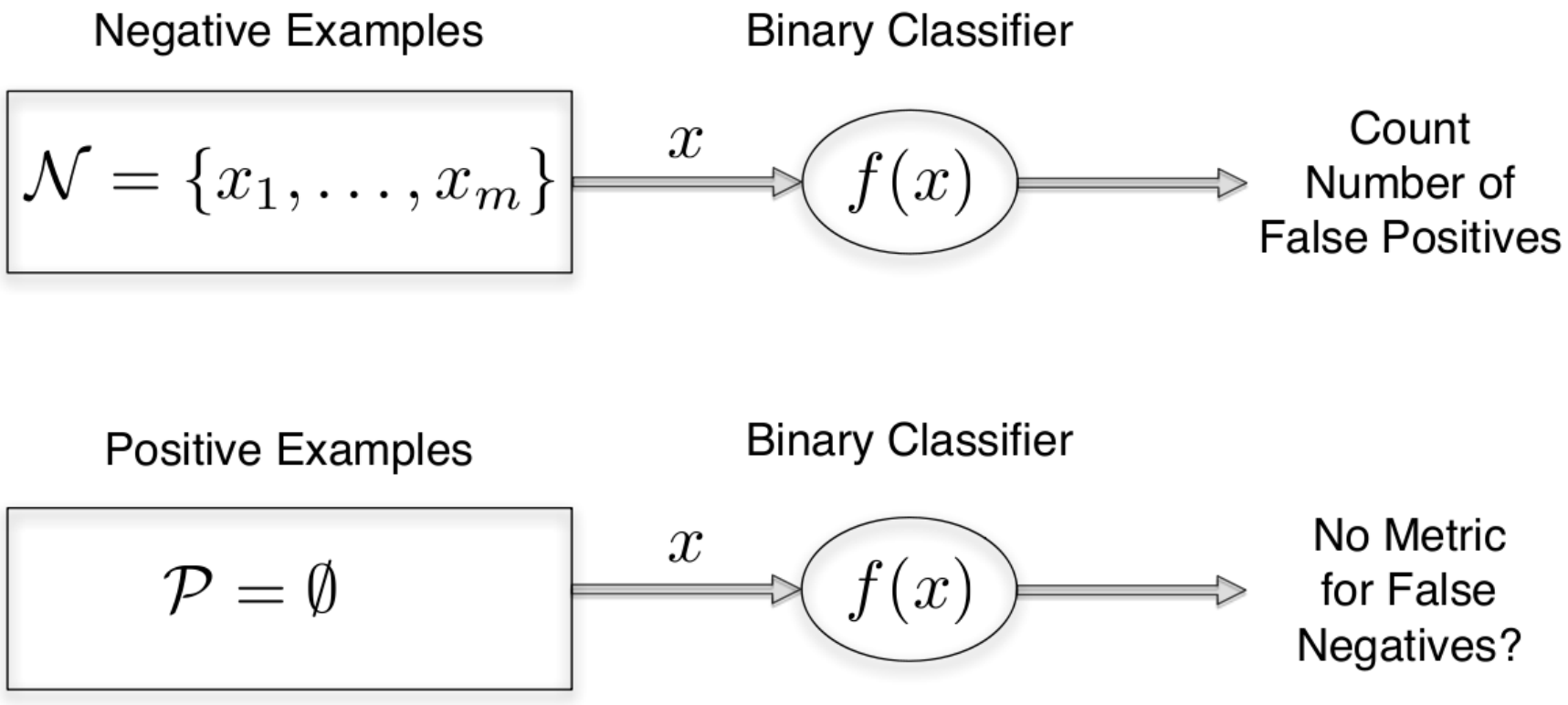
$$Y_{k+1} = \sum_{i=1}^{p} A_i Y_{k-i} + \sum_{j=0}^{q} B_j (V_{k-j} + \theta)$$

$$\text{under } H_0 : \theta = 0 \text{ and under } H_1 : \theta = -\gamma, \gamma > 0.$$

Problem: We Do Not Have Positive Examples

FUJITSU

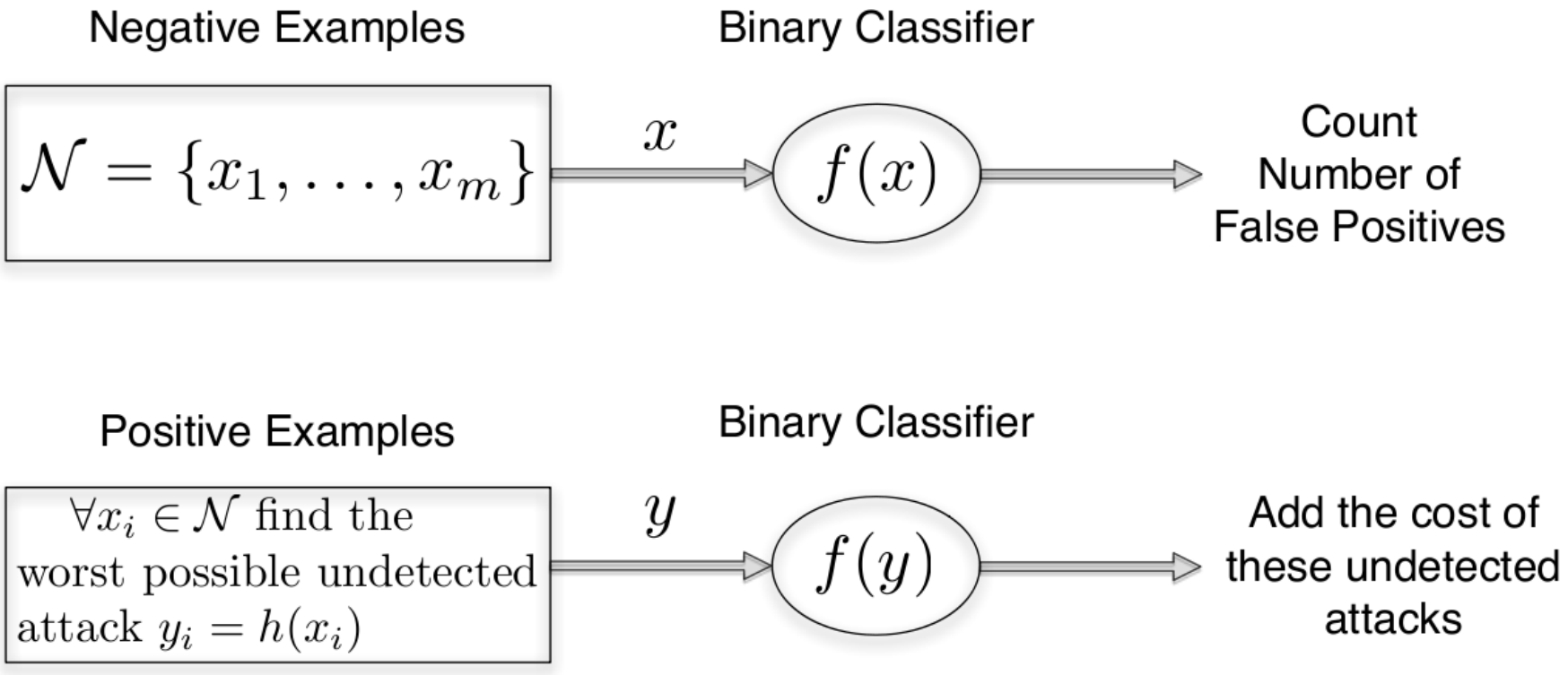
- Because meters were just deployed, we do not have examples of “attacks”



Our Proposal:

FUJITSU

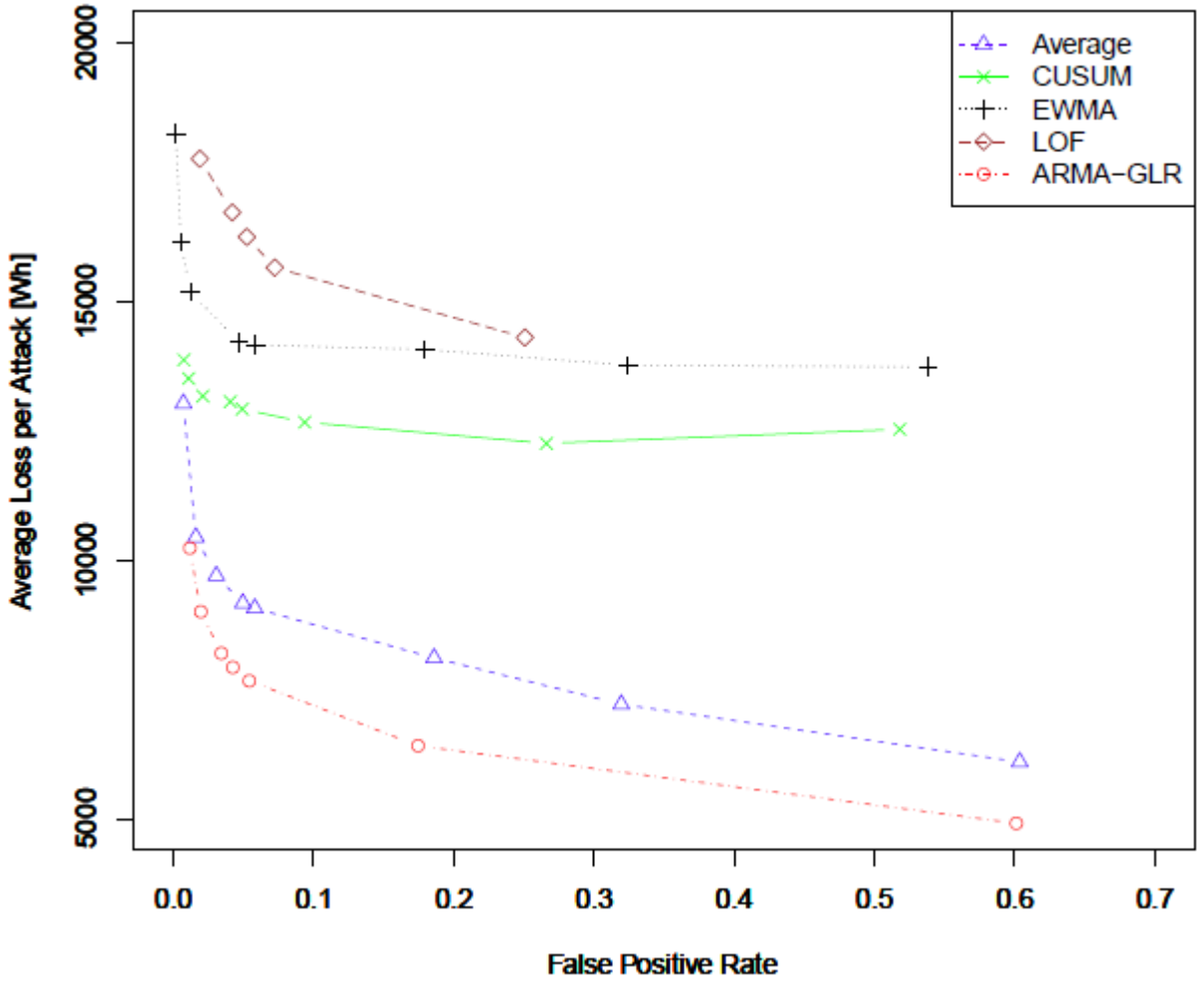
- Find the worst possible undetected attack for each classifier, and then find the cost (kWh Lost) of these attacks



Evaluation

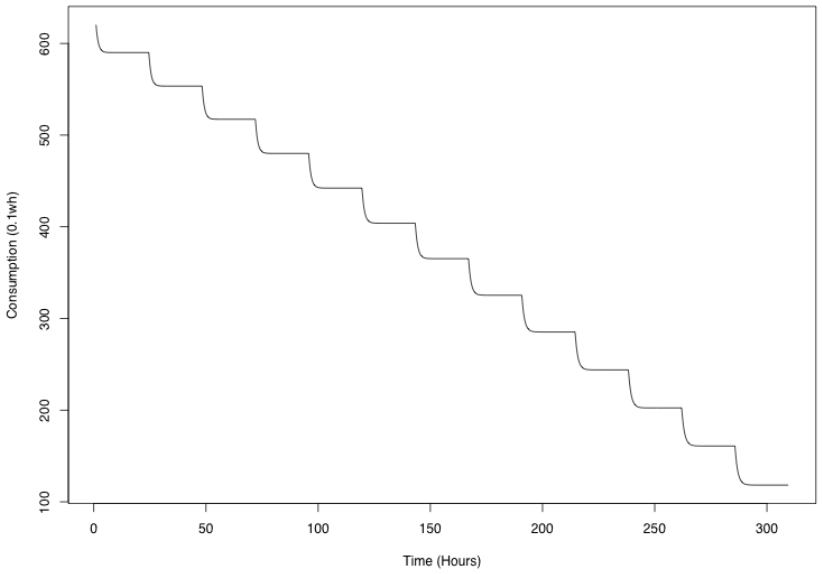
FUJITSU

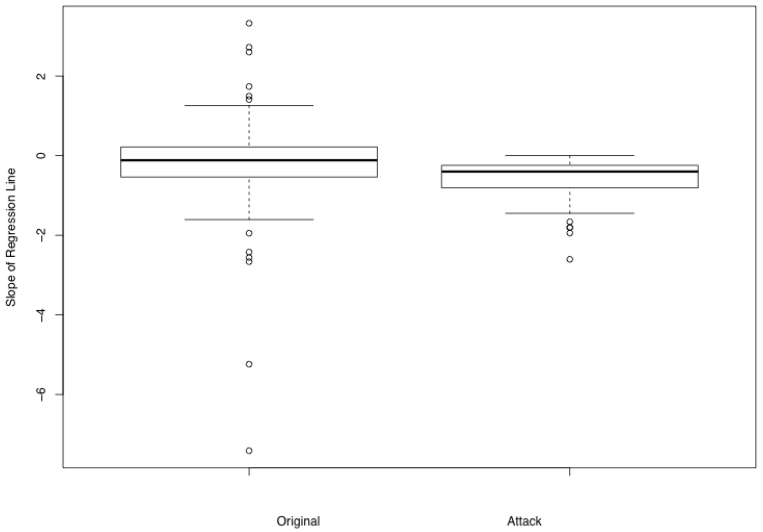
- We tried many anomaly detectors
  - Average
  - CUSUM
  - EWMA
  - LOF
  - ARMA-GLR
- ARMA GLR is the best detector:
  - For the same false positive rage, it minimizes the ability of an attacker to create undetected attacks



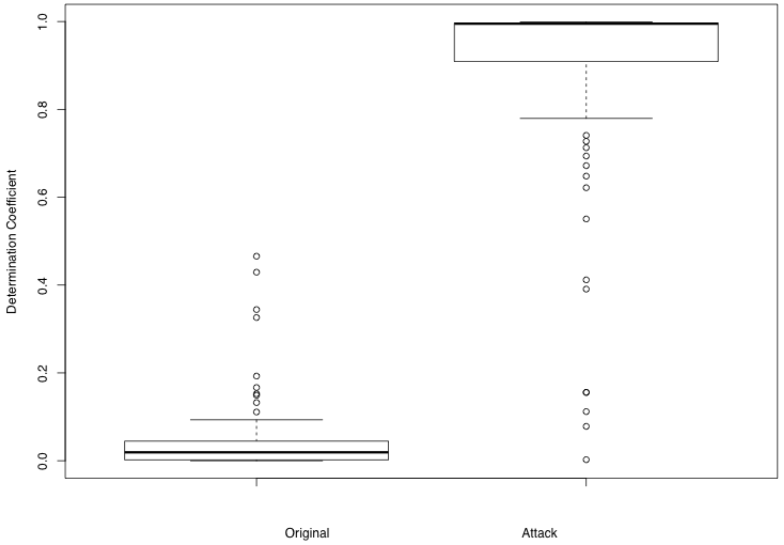
Preventing Poisoning Attacks

FUJITSU





- Electricity consumption is a non-stationary distribution
- We have to “retrain” models
- Attacker might use fake data to mislead the classifier

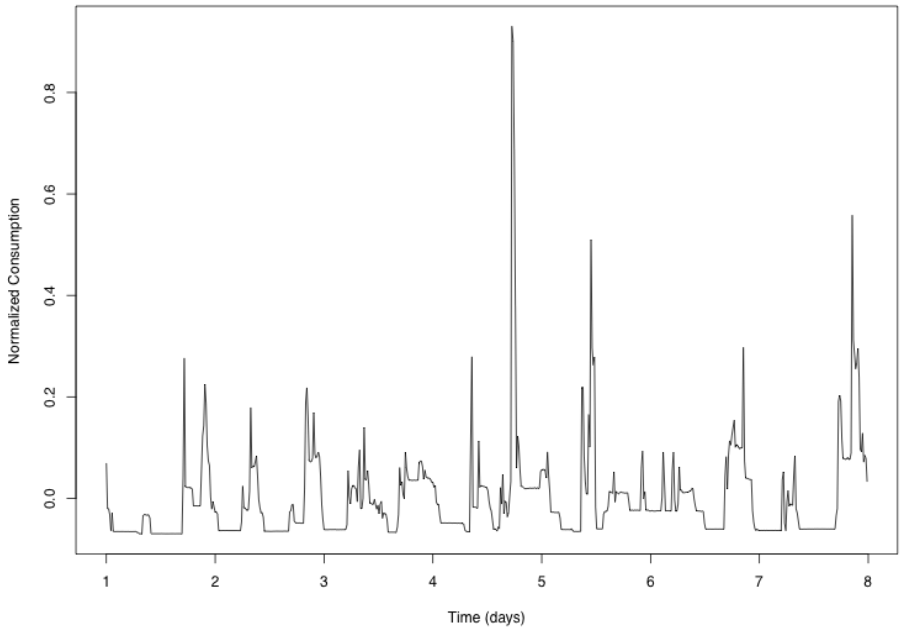


Ongoing Work

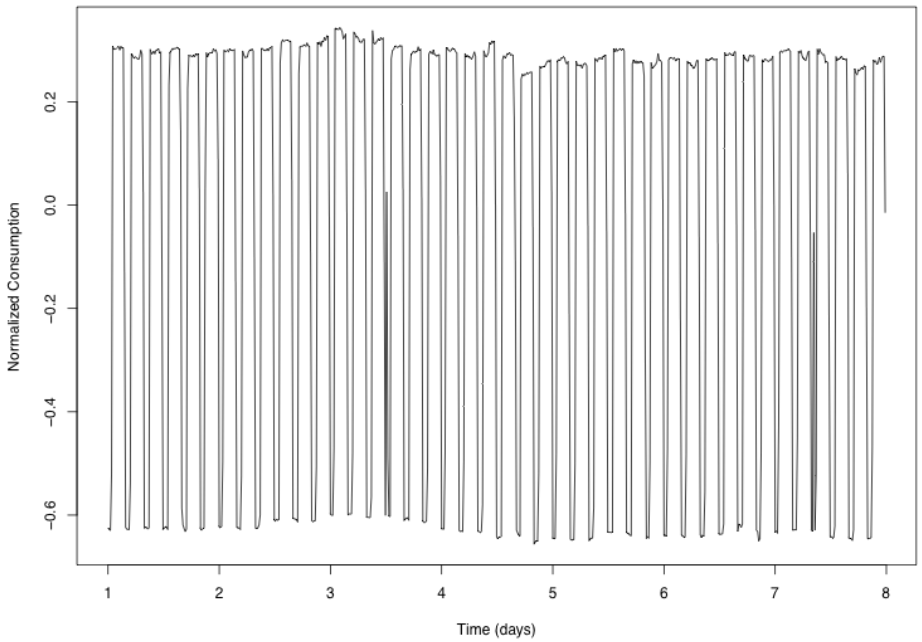
FUJITSU

- Use in production system, experience and feedback
- Detecting other anomalies.

Normal Consumption Profile



Abnormal Consumption Profile



Three Steps to Improve CPS Security

FUJITSU

- Short Term
  - Incentives
  - Software reliability
  - Solve basic vulnerabilities
- Medium Term
  - Leverage Big Data for Situational Awareness
- **Long Term Research**
  - Resilient estimation and control algorithms

Previous Work in Security: What can Help in Securing CPS?

FUJITSU

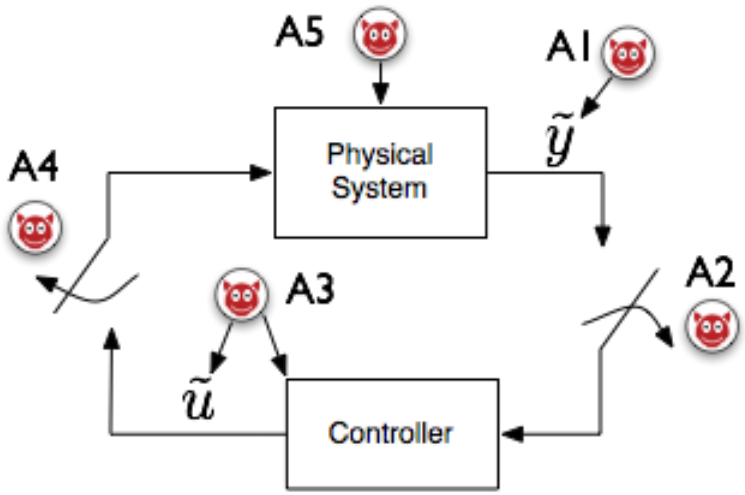
- Prevention
  - Authentication, Access Control, Message Integrity, Software Security, Sensor Networks
- Detection
- Resiliency
  - Separation of duty, least privilege principle
- Incentives for vendors and asset owners to implement security best practices

Previous Work in Security: What is Missing for Secure CPS?

FUJITSU

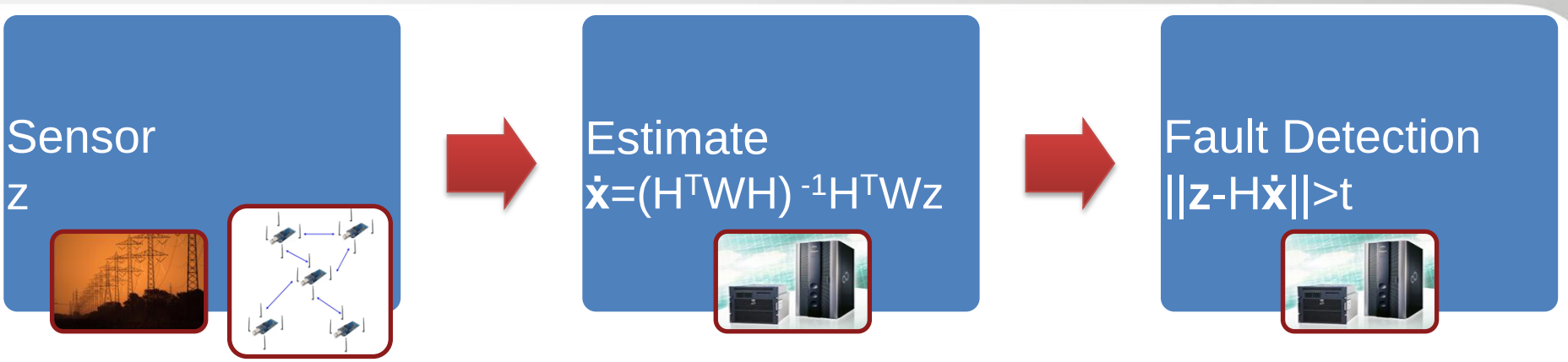
- What is new and fundamentally different in control systems security?
- Model interaction with the physical world
  - How can the attacker manipulate the physical world?

- Attacks to Regulatory Control
  - A1 and A3 are deception attacks: the integrity of the signal is compromised
  - A2 and A4 are DoS attacks
  - A5 is a physical attack to the plant



Safety Mechanisms do not Work Against Attacks

FUJITSU



- Fault-Detection Algorithms do not Work Against Attackers
  - Liu, Ning, Reiter. CCS 09
- Attacks are different than failures!
  - Non-correlated, non-independent, etc.
- Their study is missing:
  - Impact (risk assessment) of attacks?
  - Countermeasures?

CPS security is different from IT and Control Systems Safety/Fault Detection

FUJITSU

- So security is important; but are there new research problems, or can the problems be solved with
  - Traditional IT security? AC, IDS, AV, Separation of duty, least priv. etc.
  - Control Algorithms? Robust control, fault-tolerant control, safety, etc.
- Missing in IT Security
  - Understanding effects in the physical world
  - Attacker strategies
  - Attack detection algorithms based on sensor measurements
  - Attack-resilient estimation and control algorithms
- Missing in Control
  - Realistic attack models
  - Failures are different from Attacks!
    - Liu et.al. CCS 09, Maroochy, Stuxnet, etc.
- Argument: Robust Control + IT Security => Resilient CPS

New CPS Research Directions

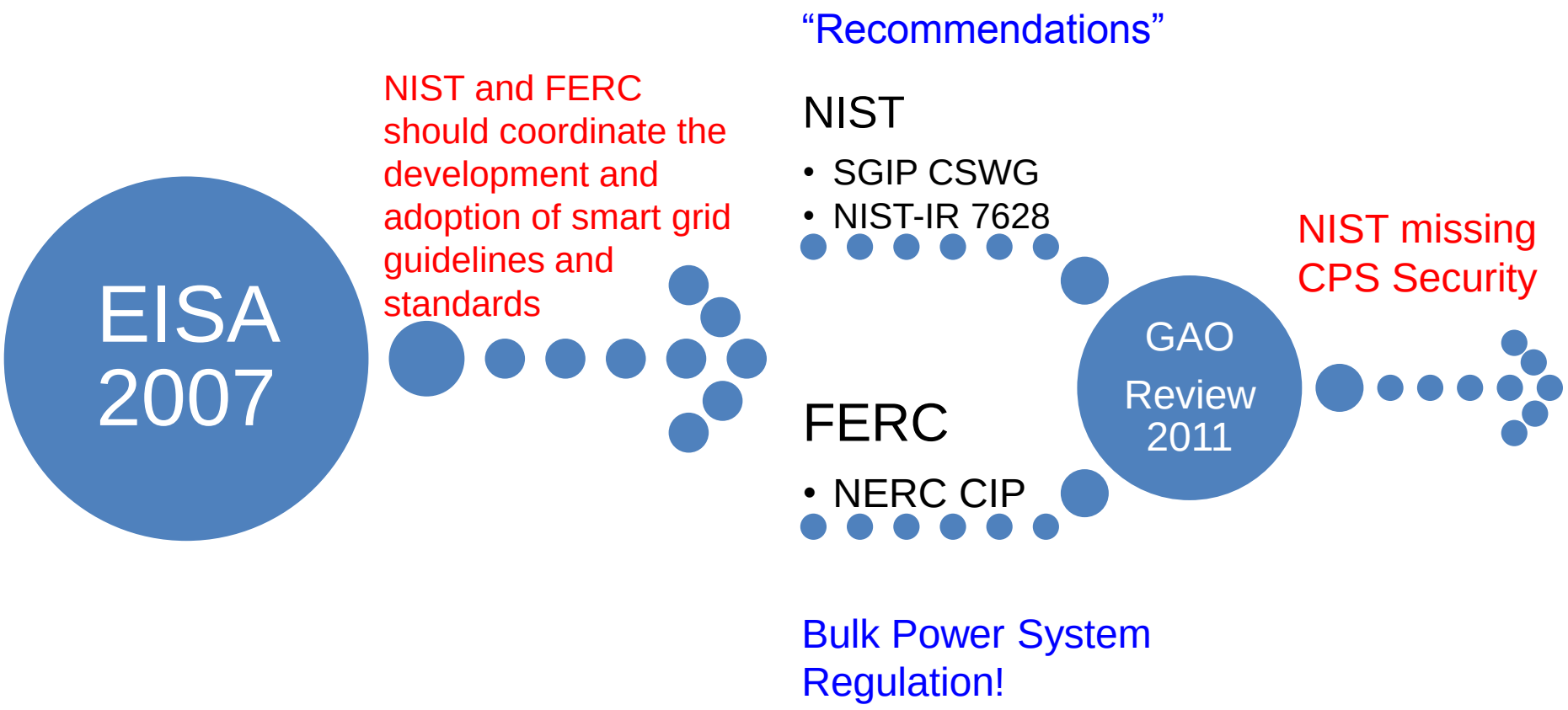
FUJITSU

- Threat assessment:
  - How to model attacker and his strategy
  - Consequences to the physical system
- Attack-resilient control algorithms
  - CPS systems that degrade gracefully under attacks
- Attack-detection by using models of the physical system
  - Study stealthy attacks (undetected attacks)
- Big Data Analytics
  - Situational awareness
- Privacy
  - Privacy-aware CPS algorithms

Papers articulating new research for CPS security
Cardenas, Amin, Sastry, HotSec 08, & ICDCS Workshop (08)

GAO Agrees: We Need new Research for CPS Security

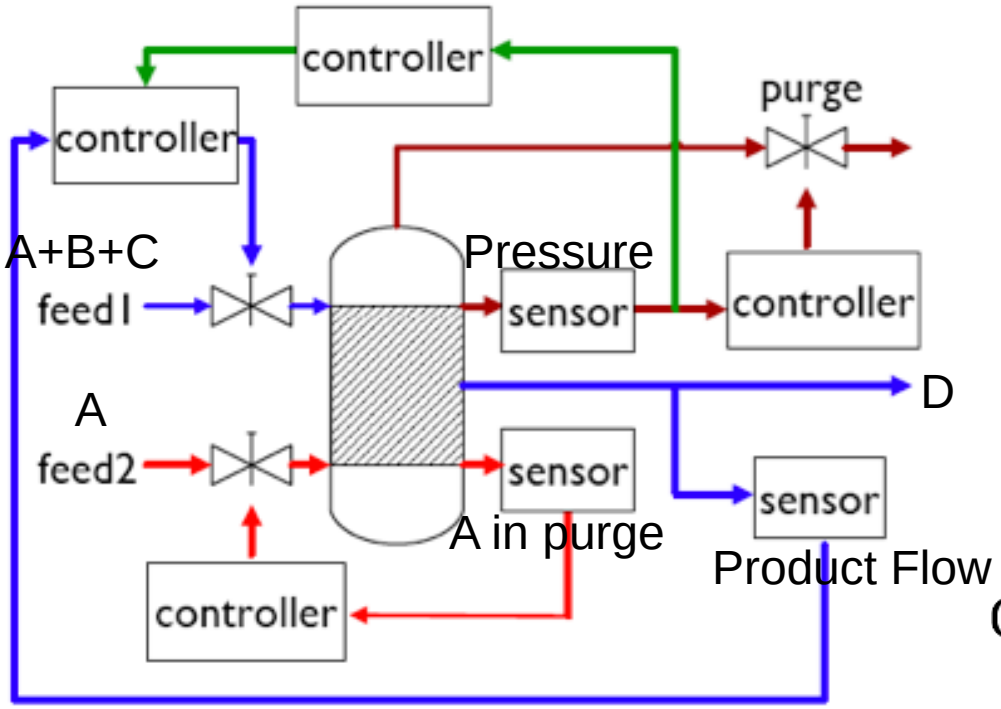
FUJITSU



Requirements for Secure Control

FUJITSU

- Step 1: Threat Model/Assessment
  - Identify requirements
- Traditional Security Requirements: CIA (Confidentiality, Integrity, Availability)
  - What are the requirements of secure control?



- Safety Constraint:
  - Pressure < 3000kPa
- Operational Goal:
  - Cost:
    - Proportional to the quantity of A and C in purge,
    - Inversely proportional to the quantity of the final product D

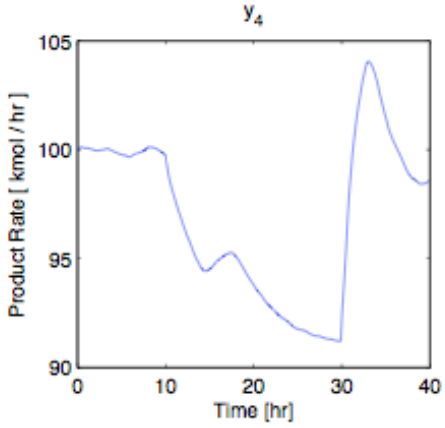
$$\text{Cost} = \frac{F_3}{F_4}(2.206 y_{A3} + 6.177 y_{C3})$$

[Journal of Critical Infrastructure Protection 2009]

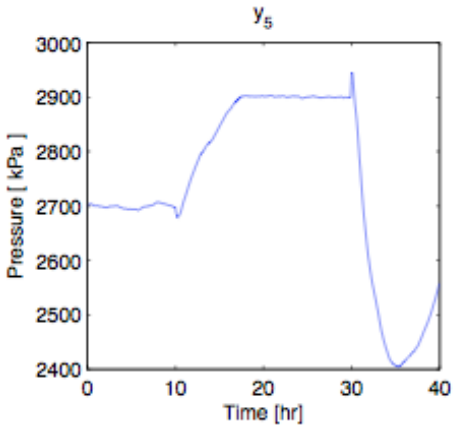
Not all Compromises affect Safety

FUJITSU

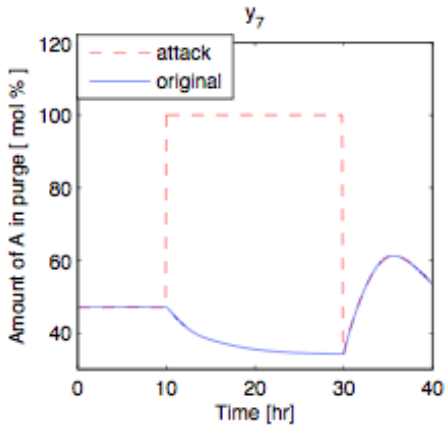
Production



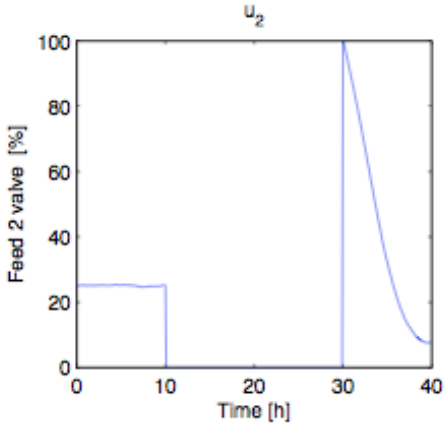
Pressure



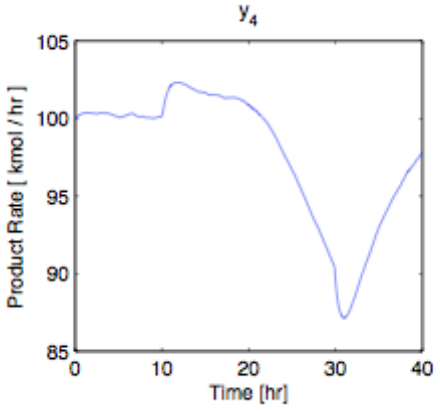
A in Purge

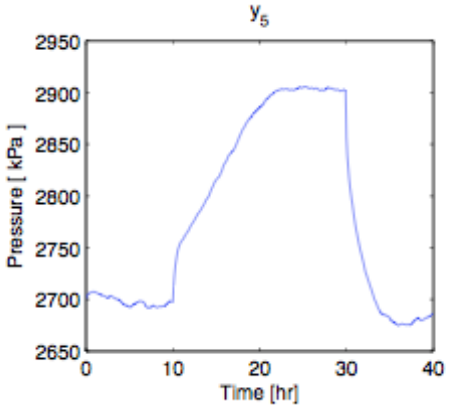


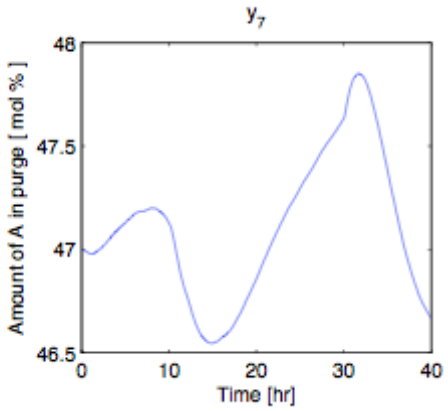
Feed of A



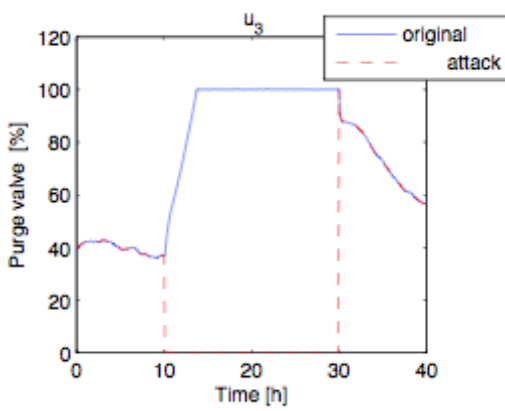
Resilient by Redundancy:







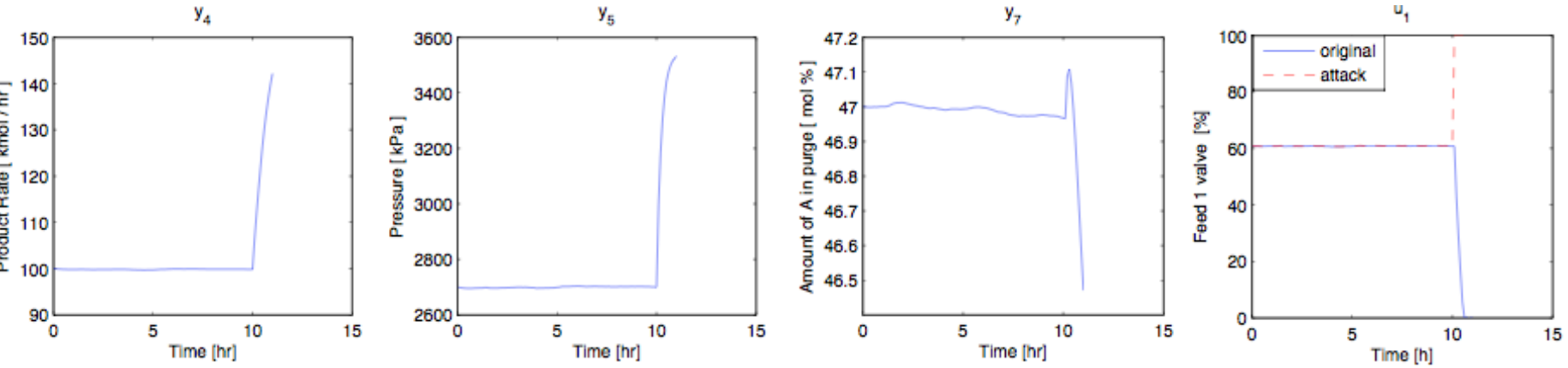
Purge Valve



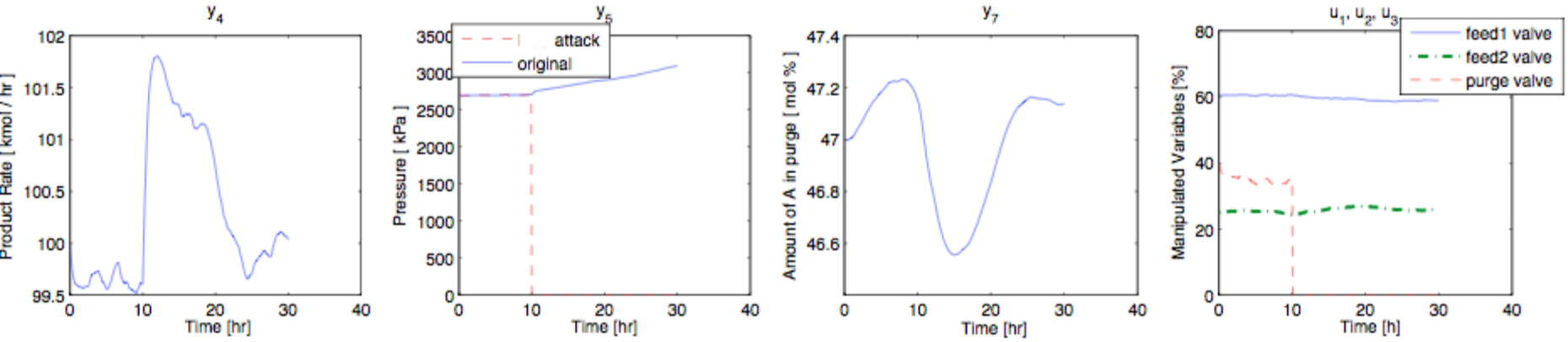
Safety can be Compromised at Different Time Scales

FUJITSU

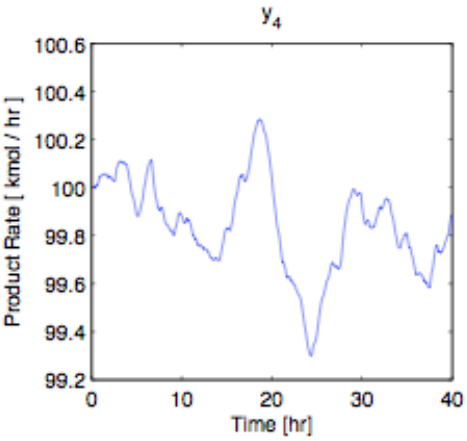
Prioritize protection of control signal for A+B+C feed

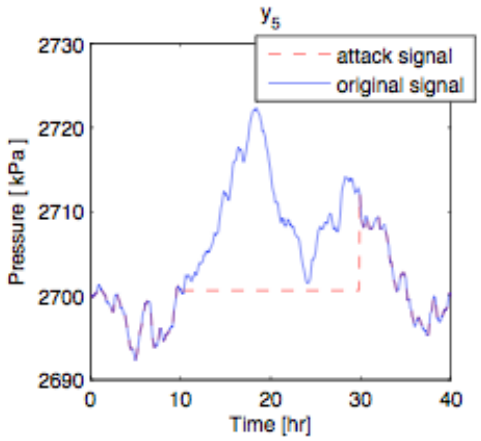


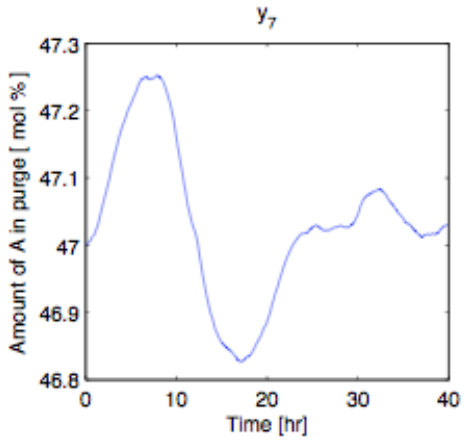
It takes 20 hours to violate Safety by compromising the pressure sensor signal (prevention vs. detection&response)

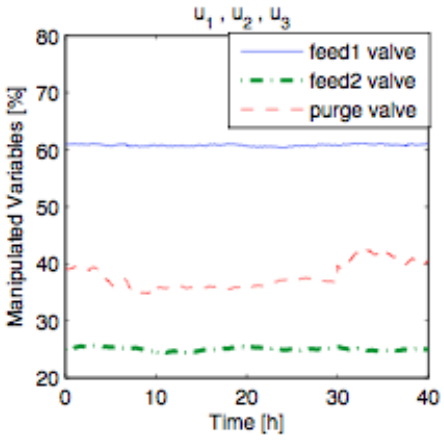


DoS Attacks: No Impact when the System is at Steady State

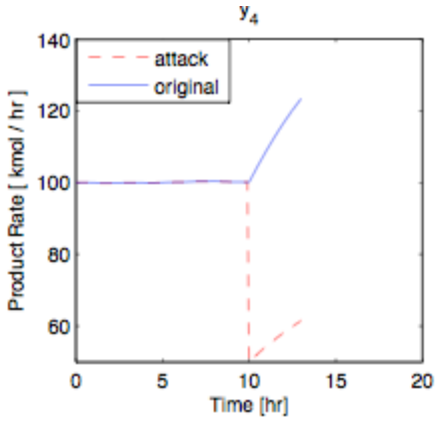


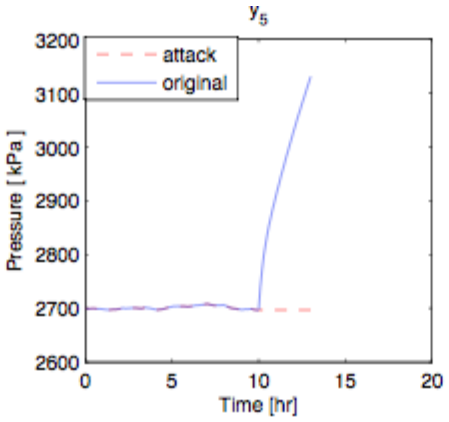


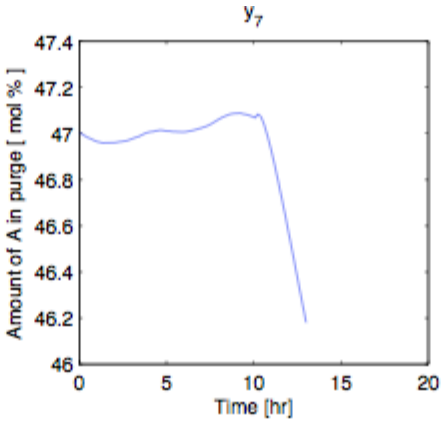


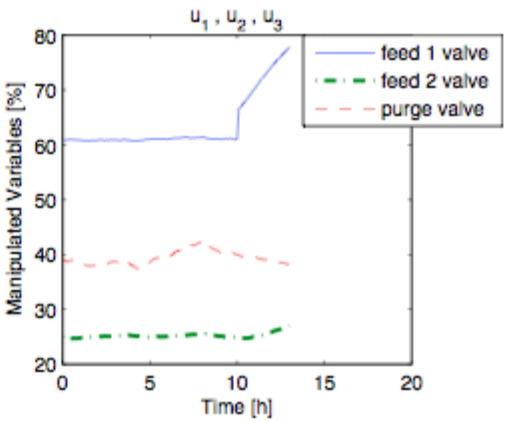


However: A previous “innocuous” integrity attack becomes significant with the help of DoS attacks



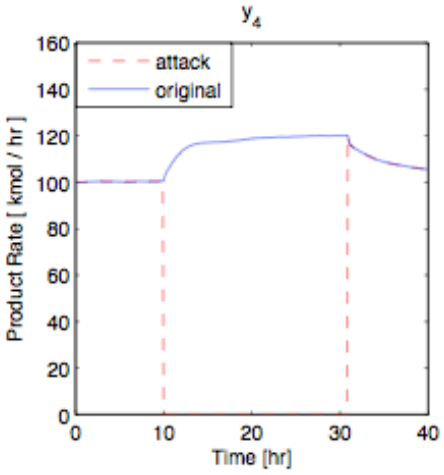


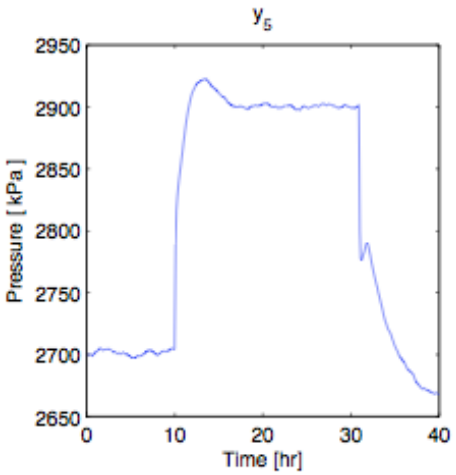


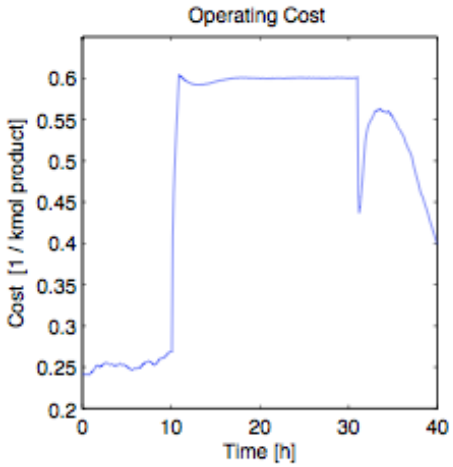


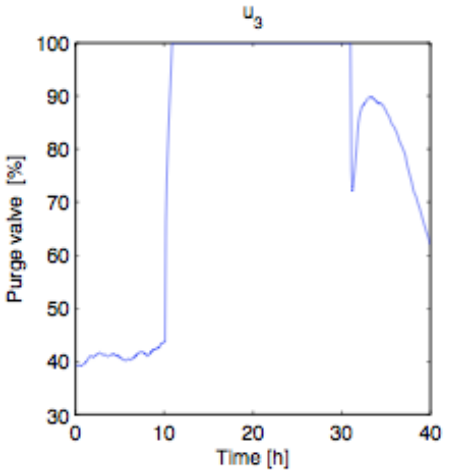
Attacks to the Operational Cost Involve Devices that do not Matter in Safety

FUJITSU

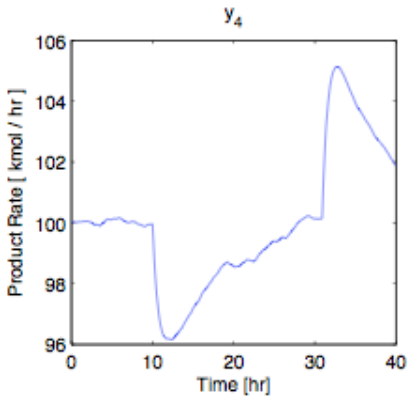


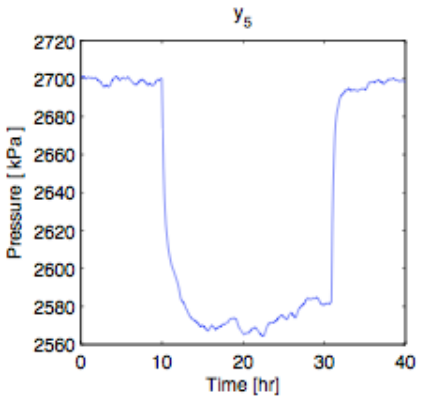


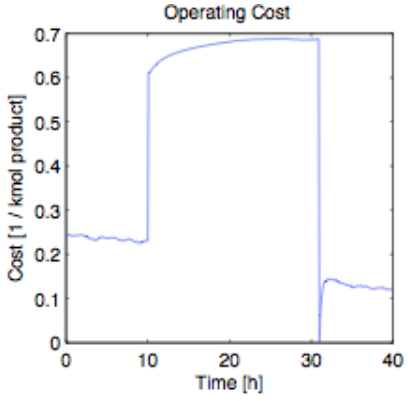


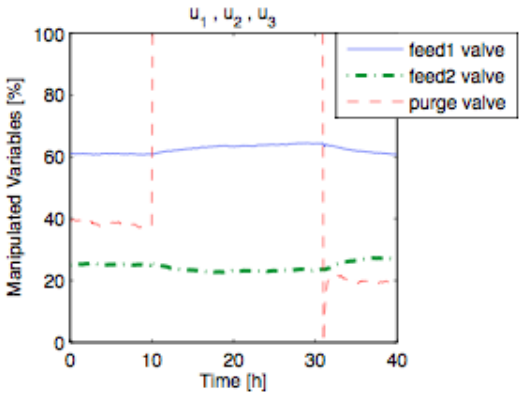


Attack increases safety but lowers profits





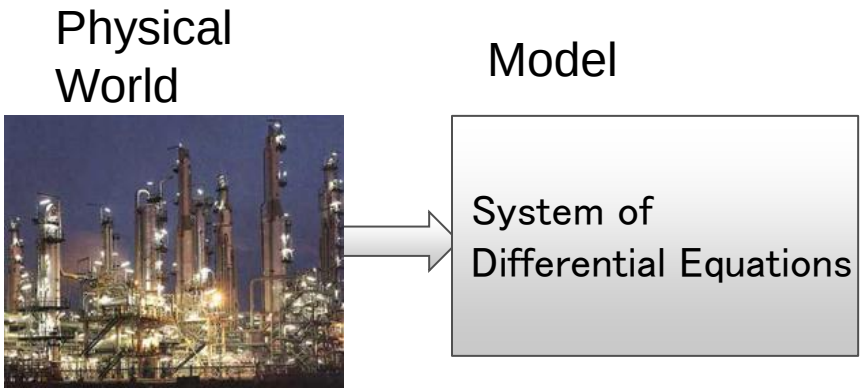




New Attack-Detection Mechanisms

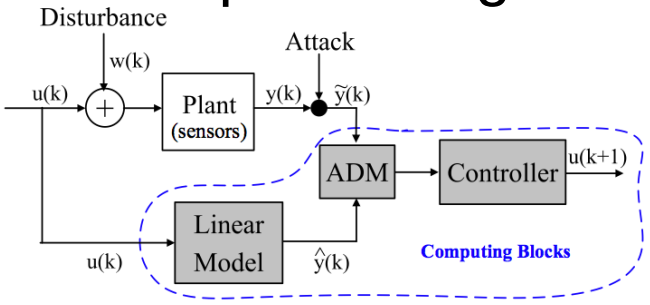
FUJITSU

1st Step: Model the Physical World



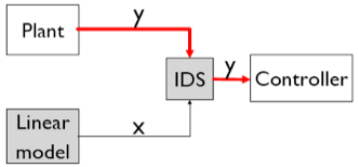
2nd Step: Detect Attacks

- Compare received signal from expected signal

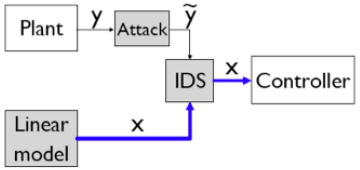


3rd Step: Response to Attacks

- **No attack**
  - Use real plant signal



- **IDS detects attack**
  - Switch to linear model
  - Detection time
  - False alarm



4th Step: Security Analysis

- Missed Detections
  - Study stealthy attacks
- False Positives
  - Ensure safety of automated response

[Cardenas. Et.al. AsiaCCS, 2011]

Attacker Strategy: Stealthy Attacks

FUJITSU

- Attacker
  - Knows our detection model and its parameters
  - Wants to be undetected for n time steps
  - Wants to maximize the pressure in the tank
- Surge attack

$$\tilde{y}_K = \begin{cases} y^{min} & \text{if } S_{k+1} \leq \tau \\ \hat{y}_K - |\tau + b - S_k| & \text{if } S_{k+1} > \tau \end{cases}$$

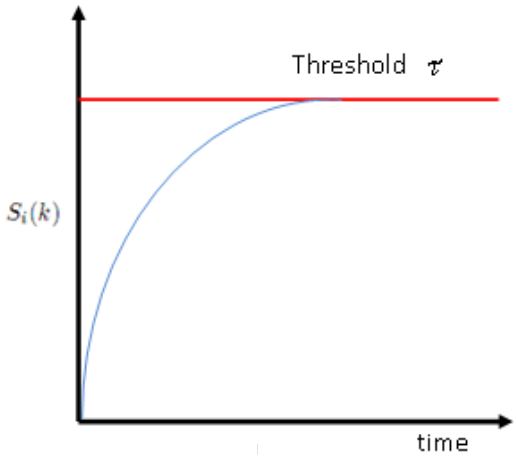
- Bias attack

$$\tilde{y}_k = \hat{y}_k - (\tau/n + b)$$

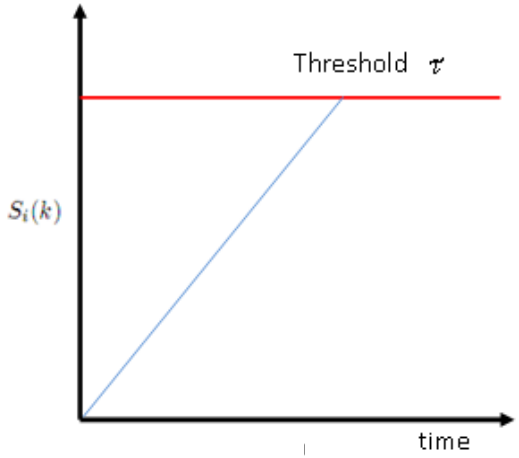
- Geometric attack

$$\tilde{y}_k = \hat{y}_k - \beta\alpha^{n-k}$$

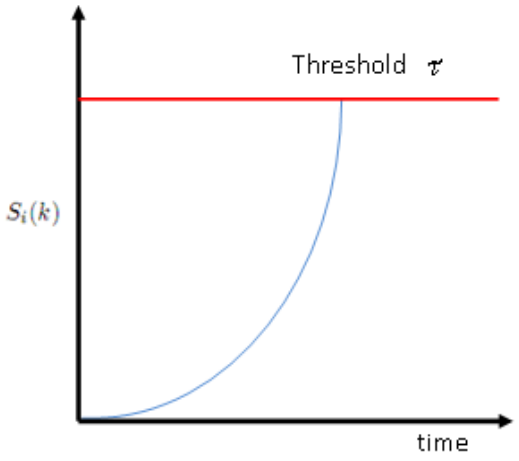
Surge Attack



Bias Attack



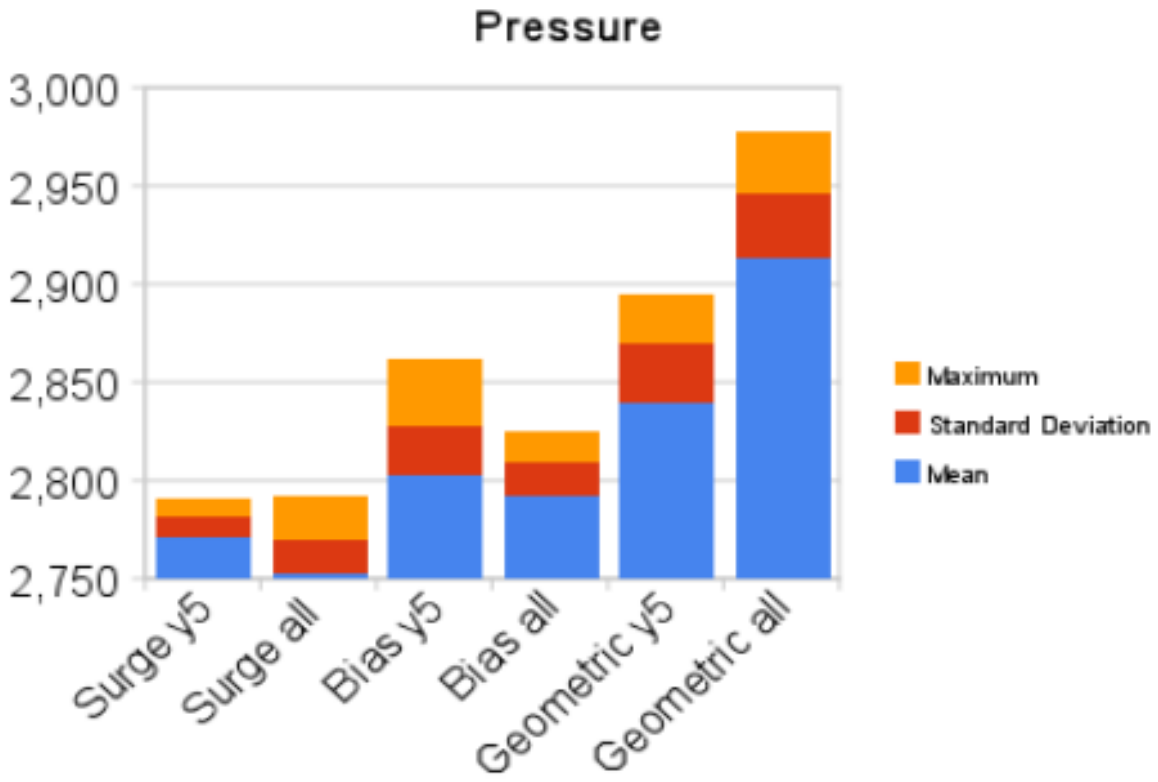
Geometric Attack



Impact of Undetected Attacks

FUJITSU

- Even geometric attacks cannot drive the system to an unsafe state
- If an attacker wants to remain undetected, she cannot damage the system



Control Resilient to DoS Attacks

FUJITSU

For constrained linear systems

$$x_{k+1} = Ax_k + Bu_k^a + w_k, \qquad k = 1, \ldots, N-1$$
$$x_k^a = \gamma_k x_k,\ u_k^a = \nu_k u_k, \qquad (\gamma_k, \nu_k) \in \{0,1\}^2$$

find causal feedback policies $u_k = \mu_k(x_0^a, \ldots, x_k^a)$, that minimize $J(x_0, \mathbf{u}, \mathbf{w}) = \sum_{k=1}^{N} x_k^\top Q^{xx} x_k + \sum_{k=1}^{N-1} \nu_k u_k^\top Q^{uu} u_k$, subject to power constraints

$$\begin{pmatrix} x_k^a \\ u_k^a \end{pmatrix}^\top \begin{pmatrix} H_i^{xx} & 0 \\ 0 & H_i^{uu} \end{pmatrix} \begin{pmatrix} x_k^a \\ u_k^a \end{pmatrix} \leq \beta_i, \qquad i = 1, \ldots, L_1,$$

and safety constraints

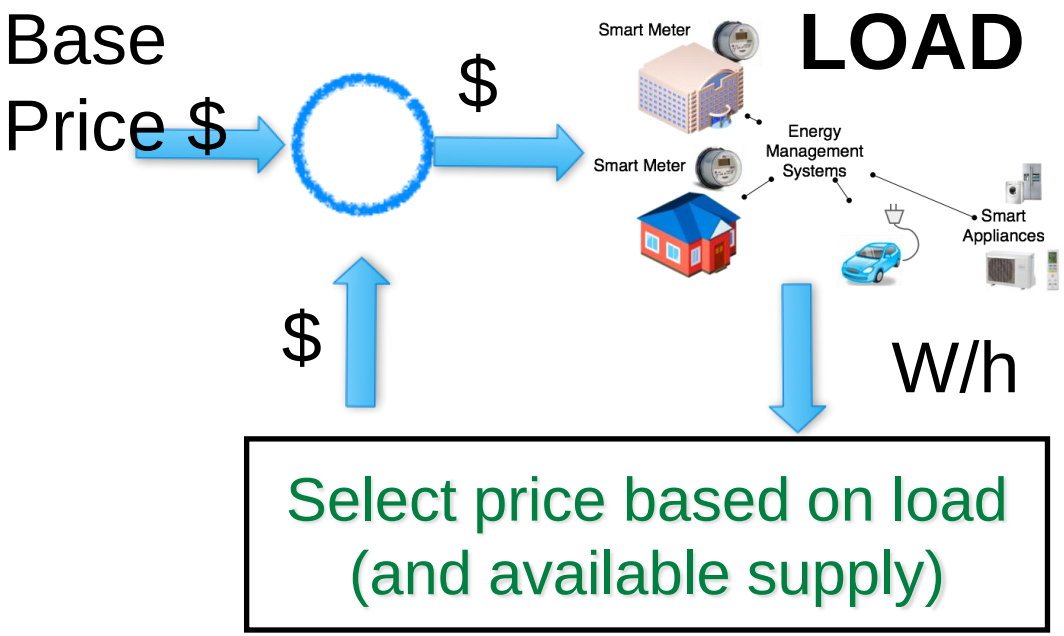
$$\begin{pmatrix} x_k^a \\ u_k^a \end{pmatrix} \in \mathcal{T}_j, \qquad j = 1, \ldots, L_2,$$

for all disturbances $\mathbf{w} \in \mathbf{W}_\alpha$ OR $\mathbf{w} \sim \mathcal{N}(0, W)$ and a given set of $(\gamma_0^{N-1}, \nu_0^{N-1}) \in \mathcal{A}_{pq}$ attack signatures.

[Amin, Cardenas, Sastry. HSCC / CPSWeek 2009]

Privacy-Preserving Control

- Data Minimization Principle
  - How much data do we really need to collect for accurate estimation/control?
  - Quantity: sampling
  - Quality: quantization
- **Demand Response (DR)**



[Cardenas, Amin, Schwartz. HiCoNS / CPSWeek 2012]

CPS Research for Smart Grid

FUJITSU

- DoE 2020 Vision:
  - Maintain Smart Grid functions under attack
- Develop resilient algorithms for:

Smart Grid Function	• Untrusted input
State Estimation	• Power flow sensors
Network Topology Processor	• Breakers
Electricity Markets	• Prices
Load balancing	• Smart meter, control data
Transmission/Distribution Automation	• Flexible Alternate Current Transmission System (FACTS)