Securing Smart Grid Infrastructure against Emerging Cyber Threats

Daisuke Mashima
Illinois at Singapore Pte Ltd
Advanced Digital Sciences Center

April 16, 2019
at
National University of Singapore

ADSC
ADVANCED DIGITAL SCIENCES CENTER

Version 2, WGT

Brief Bio

Daisuke MASHIMA

Experience

Senior Research Scientist at ADSC and Research Affiliate at University of Illinois at Urbana Champaign

- 2 government-funded smart grid security projects

Formerly research scientist at Fujitsu Laboratories of America

- Smart energy and smart home IoT systems
- Security and privacy in smart metering
- OpenADR2.0 standardization

Education

PhD in Computer Science from Georgia Tech in 2012

- Security and privacy in Electronic Healthcare Records

Award

- **Best paper award** from IEEE SmartGridComm 2014
- **Silver Prize** in App Contest at ACM MobiCom 2015
- **President Awards** and **Standardization Promotion Award** from Fujitsu

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

FUJITSU

Georgia Tech

Advanced Digital Sciences Center

ADSC is a research center of Illinois at Singapore Pte. Ltd., an affiliate of the University of Illinois / supported by NRF's CREATE programme.

ADSC's research is led by faculty from Electrical & Computer Engineering and Computer Science

We have diverse staff of **20** full-time researchers–more than half with PhDs

We have **11** Illinois professors involved in SG

The TSCP CREATE Programme

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE
Research . Innovation . Enterprise

The Challenge

Assurance that a system is both *trustworthy* (meaning it is trusted to behave as expected, even during an accidental or intentional disruption) **and *secure*** (meaning it is hardened against malicious attacks)

CREATE Centre for a Trusted and Secure Cyber Plexus (TSCP)

Trustworthy System Architecture

Standards, Validation, Verification

Technology of Trust

Monitoring, Analysis, Interdiction and Recovery

- **SUTD is Illinois' primary partner**

Outline

01 Cyber Threats in Smart Grid Infrastructure

- Smart grid overview
- Security threats in smart grid

02 Measures for Securing Smart Grid Systems

- IEC 62351
- Intrusion detection systems
- Bump-in-the-wire security

03 Defending against Malicious Command Injection

- SCADA command authentication
- Artificial Command-delaying

04 Countering Data Falsification Attacks in AMI

- Anomaly Detection in Smart Meter Data
- Evaluation Framework for Anomaly Detectors

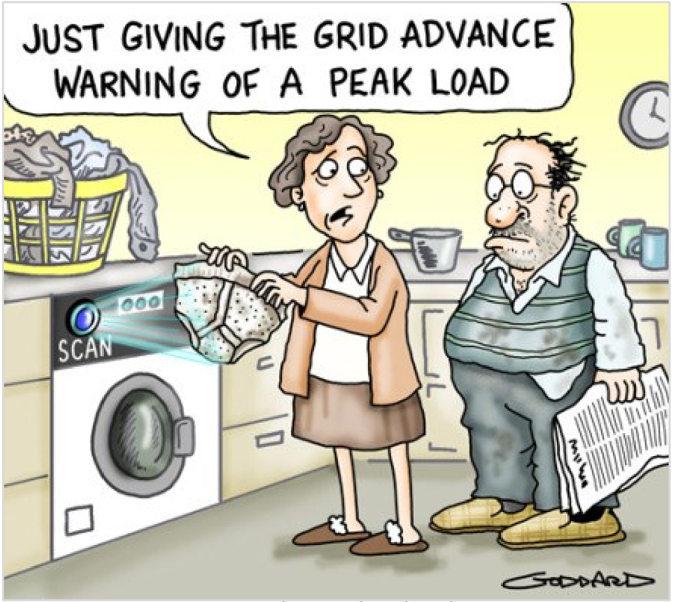
05 Ongoing Projects & Concluding Remark

- High-fidelity Smart Grid Honeypot

What is Smart Grid?

Power grid enhanced with ICT (information and communication technologies)

- Reliability
- Efficiency
- Security
- Safety



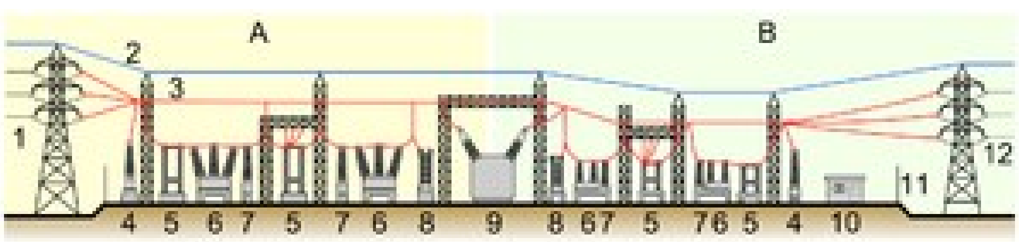
https://alittlefridaystory.com/2016/01/22/solar-power-a-new-hope/

Modernized substations & Smart metering (AMI)

ADSC
ADVANCED DIGITAL SCIENCES CENTER

Modernization of Electrical Substations

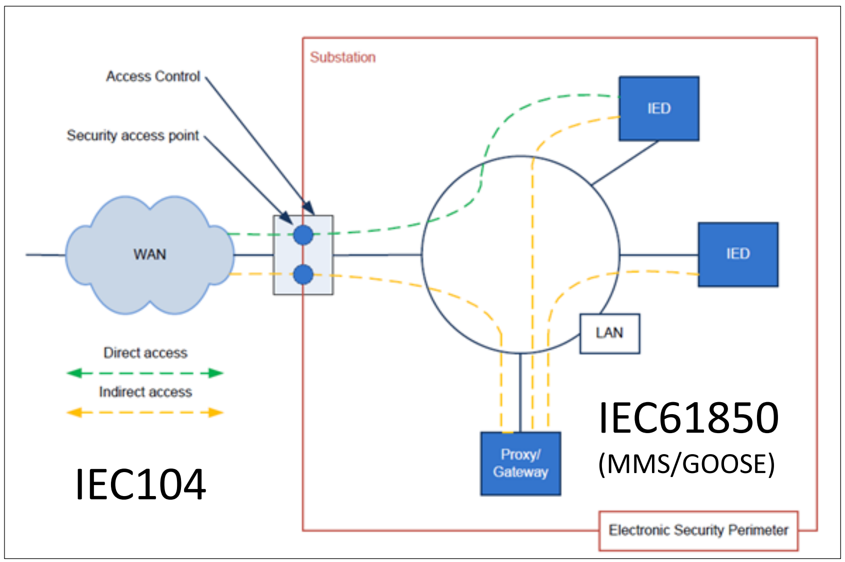
- **Crucial component of power grid** system for delivery of electricity (e.g., voltage transformation)
- Over 10,000 substations in Singapore
- **Remotely managed or controlled** for load/power shedding, voltage regulation, and topology control



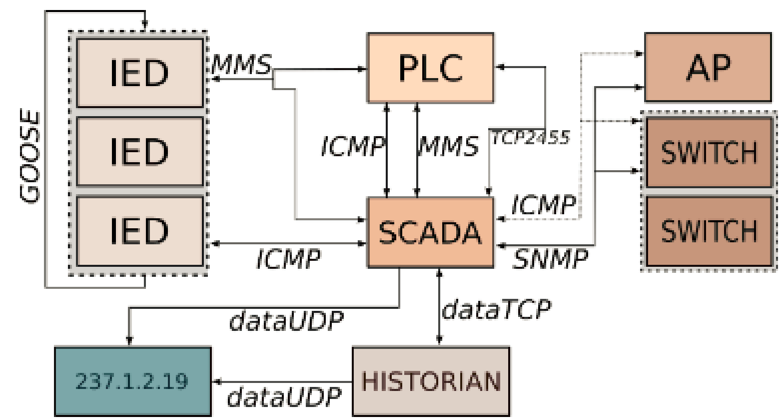
https://en.wikipedia.org/wiki/Electrical_substation

Modernization of Electrical Substations

- Adoption of standard technologies such as IEC 60870-5-104 (or IEC104) or DNP3 and IEC 61850 for remote control and automation



IEC 61850-90-2 TR: Communication networks and systems for power utility automation – Part 90-2: Using IEC 61850 for the communication between substations and control centres - Page 10

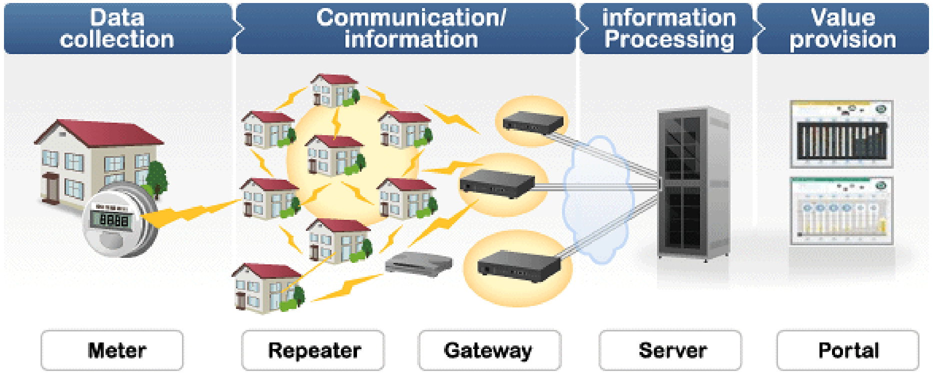


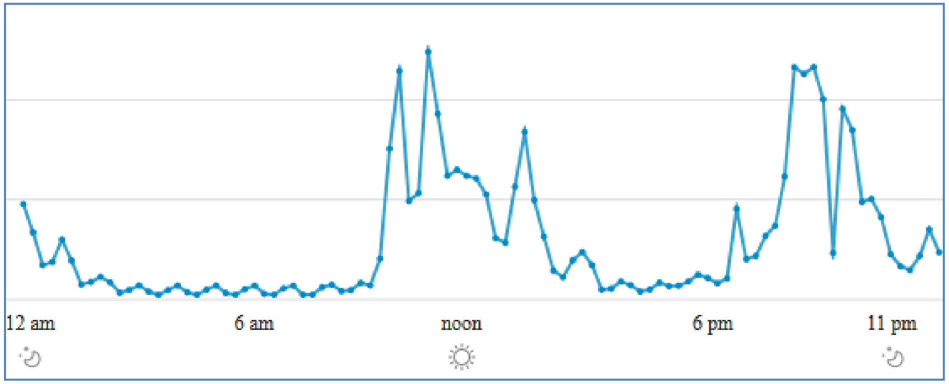
Protocols used in EPIC smart grid testbed

Ahnaf Siddiqi, Nils Ole Tippenhauer, Daisuke Mashima, and Binbin Chen, "On Practical Threat Scenario Testing in an Electric Power ICS Testbed." To appear at the 4th ACM Cyber-Physical System Security Workshop (ACM CPSS 2018) in June, 2018.

Smart Metering

- **Real-time electricity usage** monitoring
- Enable accurate load forecasting, peak prediction (i.e., **Feedback into control loop**)





Security by “Air Gap.” Myth or Truth?

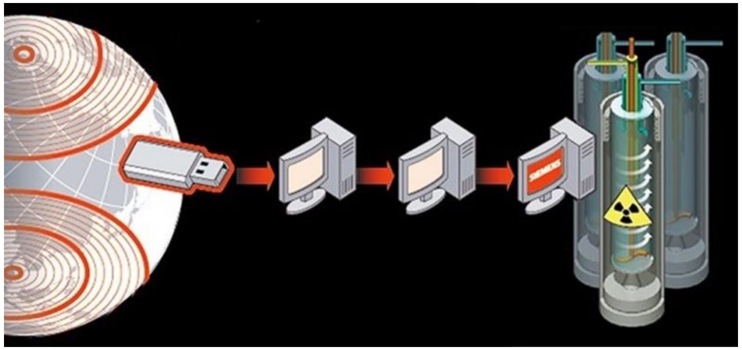
https://www.belden.com/blog/industrial-security/goodbye-air-gaps-hello-improved-ics-security

- **Isolation** from other systems or external network
- **Dedicated** communication infrastructure
- ***All devices were trusted.***
- ***Security was not part of protocol or system design.***

Stuxnet Worm

- Targeted **nuclear plants** in Iran
- Exploited multiple zero-day vulnerabilities on Windows

- Can infect via **USB drive**
- Successfully compromised PLC connected to centrifuge units



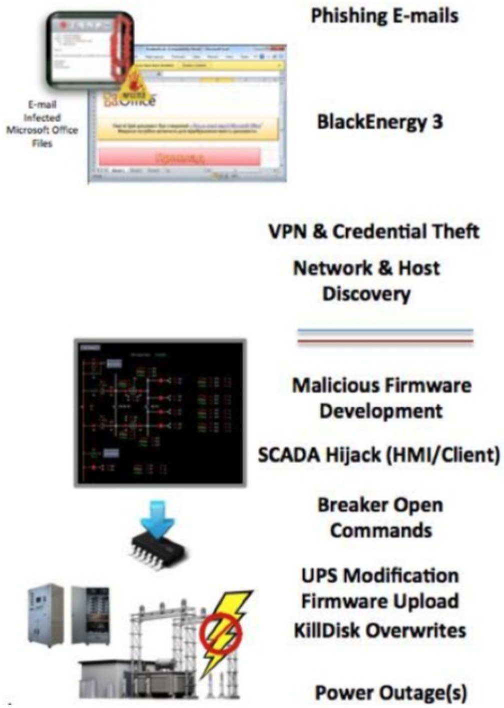
(null-byte.wonderhowto.com)

Ukraine Power Plant Attacks

- Caused **massive power outage** in Ukraine in 2015

(https://www.youtube.com/watch?v=8ThgK1WXUgk)

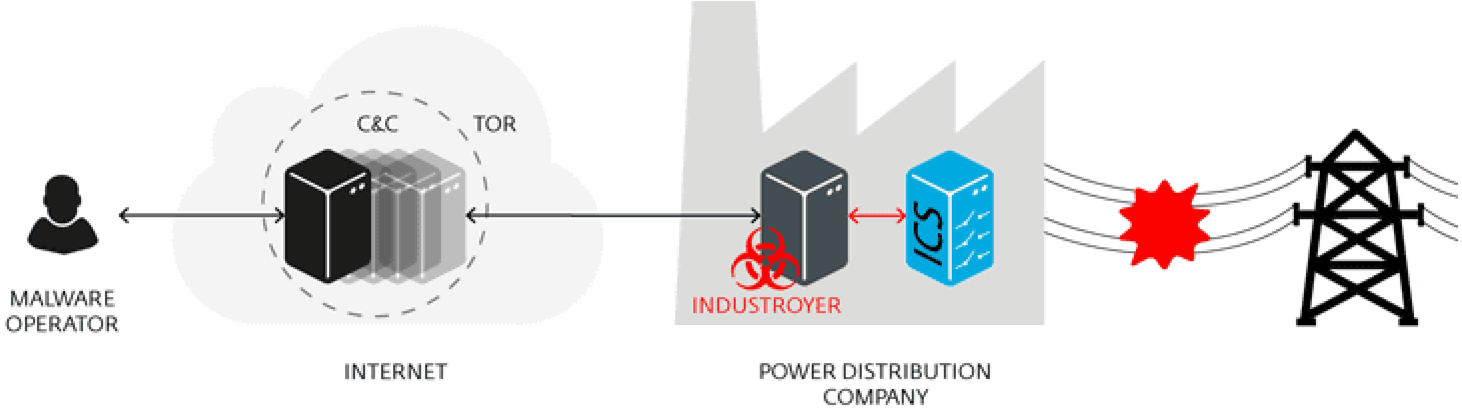
- Ironically demonstrated **"ICS Cyber Kill Chain"**



(https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf)

CrashOverride/Industroyer

- Reported in the Ukraine incident in 2016
- **Abuses widely-used ICS protocols**, including IEC 60870-5-104 and IEC 61850
  - Capable of issuing valid SCADA commands



https://gigazine.net/news/20170613-crashoverride/

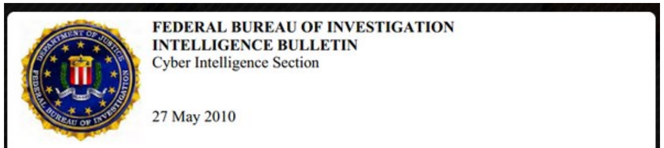
Aurora Generator Test

- Conducted by Idaho National Lab in 2007
- **Demonstrated** how a cyber-originated attack can damage physical power grid components.
- Succeeded in **exploding a diesel generator** in 3 minutes!

https://en.wikipedia.org/wiki/Aurora_Generator_Test

ADSC
ADVANCED DIGITAL SCIENCES CENTER

Data Falsification on AMI


FEDERAL BUREAU OF INVESTIGATION
INTELLIGENCE BULLETIN
Cyber Intelligence Section

27 May 2010


Singapore to launch smart meter trial for electricity, water and gas

THE Singapore government is studying a wider deployment of smart meters for electricity, gas and water supply.

The Energy Market Authority (EMA), together with national water agency and grid operator Singapore Power, will be issuing a call for proposals for a smart meter trial, aimed at helping consumers to be more efficient in their power, water and gas consumption, said Minister for Trade and Industry (Industry) S Iswaran on Monday at the Singapore International Energy Week.

Currently, most electricity meters in Singapore are read manually once every two months, together with gas and water meters. The agencies hope to have technical solutions developed for remotely reading all three meters reliably and in a cost-effective manner.

The trial will also include the development of a mobile application to provide consumers with real-time information on their electricity, water and gas consumption.

"This would allow consumers to make informed decisions on their consumption and conservation of utilities," said Mr Iswaran. "The results of the test-bed will help us assess whether and how we can deploy advanced metering solutions nation-wide, in tandem with our plans to have full retail competition in the electricity market by 2018."

- Inherently vulnerable
  - Smart meters expands the ... ece of smart
  - ...d, large-scale
  - ...of energy
  - ...ity revenue
  - ... **grid control**

Outline

01 Cyber Threats in Smart Grid Infrastructure
- Smart grid overview
- Security threats in smart grid

02 Measures for Securing Smart Grid Systems
- IEC 62351
- Intrusion detection systems
- Bump-in-the-wire security

03 Defending against Malicious Command Injection
- SCADA command authentication
- Artificial Command-delaying

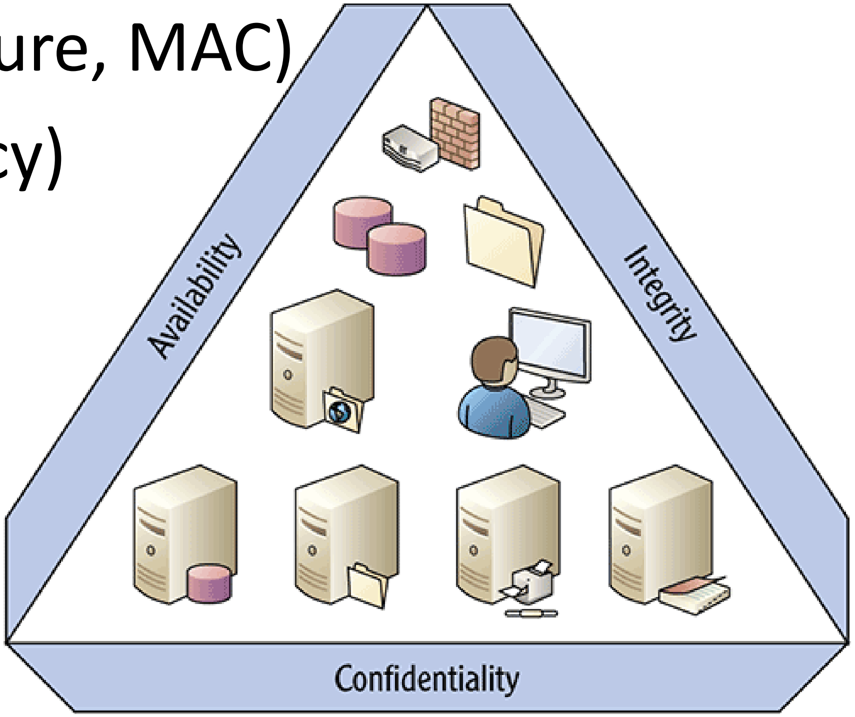
04 Countering Data Falsification Attacks in AMI
- Anomaly Detection in Smart Meter Data
- Evaluation Framework for Anomaly Detectors

05 Ongoing Projects & Concluding Remark
- High-fidelity Smart Grid Honeypot

Cyber Security vs CPS/ICS Security

What are the goals of general cyber security?

- ✓ **C**onfidentiality (E.g., Encryption)
- ✓ **I**ntegrity (E.g., Digital Signature, MAC)
- ✓ **A**vailability (E.g., Redundancy)
- ➢ **C-I-A Triad**



What's important in ICS?

- ➢ **Availability first (A-I-C)**

Cyber Security vs CPS/ICS Security

- In many cases, **resource-constrained**
  - Embedded devices (RTUs, PLCs IEDs)
  - Limited network bandwidth
- Stringent **latency** requirements
  - In particular, communication within a substation
- Need for assessment of **physical impact**

IEC 62351 Standards

- Define **security specifications** for smart grid communication protocols
  - IEC 60870-5-104, IEC 61850, DNP3, etc.

OVERVIEW OF THE IEC 62351 STANDARD

Description	Mechanism	C	I	Au	A	NR	Az
Part 3 - Security for any TCP/IP-based profiles	TLS	✓	✓	✓	-	-	-
Part 4 - Security for MMS-based profiles	Transport (T)-Profile - TLS	✓	✓	✓	-	-	-
	Application (A)-Profile - Peer authentication using certificate	-	-	✓	-	✓	-
Part 5 - Security for IEC 60870-5 and derivatives such as DNP-3	Serial version - Challenge-response protocol	-	✓	✓	-	-	-
	Networked version - TLS with encryption only	✓	✓	-	-	-	-
Part 6 - Security for IEC 61850 profiles	GOOSE and SV - Digital signature	-	✓	✓	-	-	-
	MMS - TLS and Peer authentication using certificate	✓	✓	✓	-	✓	-
Part 8 - Access control in power systems	Role-Based Access Control (RBAC)	-	-	-	-	-	✓
Part 9 - Key management for power systems	Certificate-based PKI	End-to-End Security					

C=Confidentiality; I=Integrity; Au=Authentication; A=Availability; NR=Non-repudiation; Az=Authorization
MMS=Manufacturing Messaging Service; GOOSE=Generic Object Oriented Substation Events; SV=Sampled Value

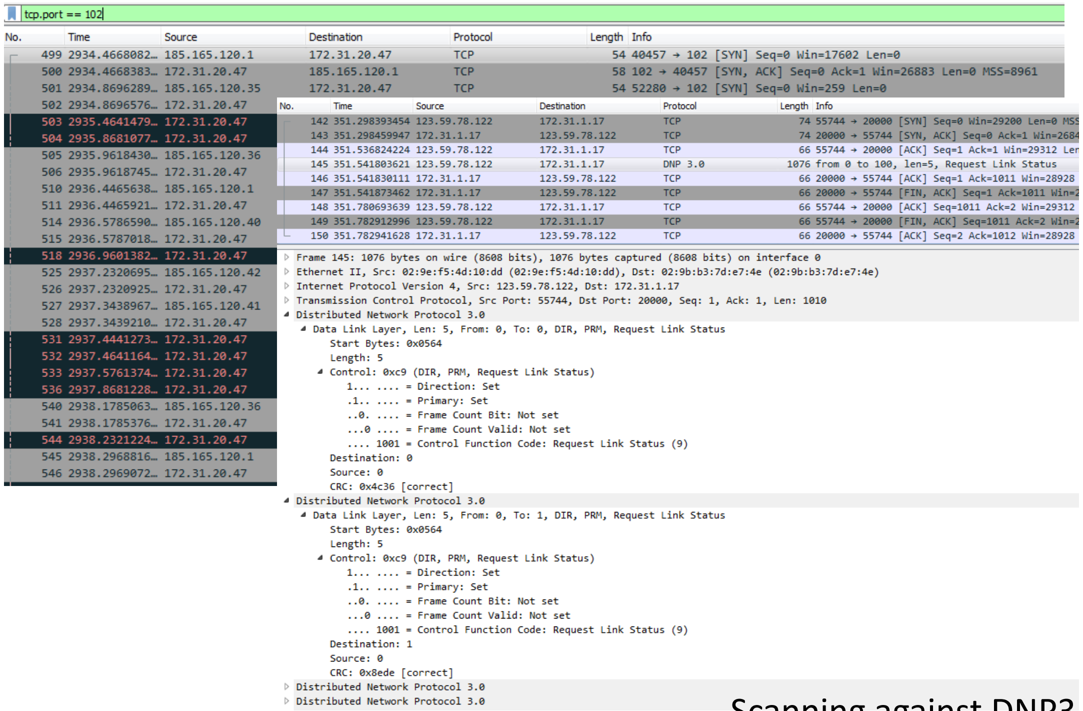
Heng Chuan Tan, Carmen Cheh, Binbin Chen, and Daisuke Mashima, **"Tabulating Cybersecurity Solutions for Substations: Towards Pragmatic Design and Planning."** Under submission.

Intrusion Detection Systems

- Detect **malicious/anomalous events** in the system
- Network-based IDS is popular in the ICS domain.

- Signature-based IDS
  - Based on “known” attack patterns
- Anomaly-based IDS
  - Statistics-based
  - Machine-learning-based
- Physics-based IDS
  - Power-system physical laws (e.g., state estimation)
- Ensemble IDS

DoS (SYN-flood) attack against IEC 61850 MMS



Scanning against DNP3

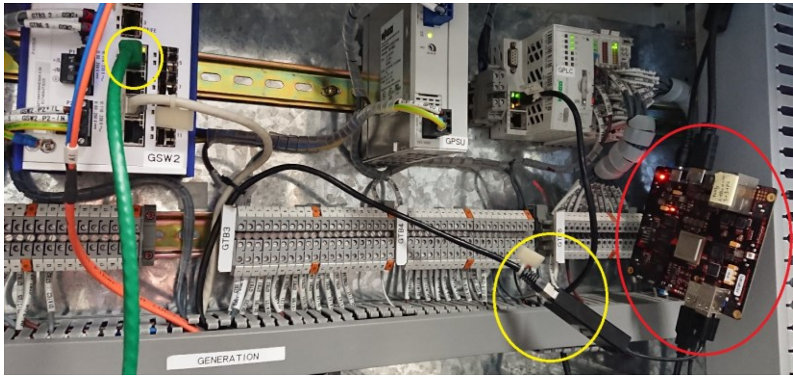
Bump-in-the-wire Solutions

- Introduce devices to provide security features in **add-on** manner
- **Network traffic control** with firewall and data diode

https://www.tofinosecurity.com/products/Tofino-Firewall-LSM

https://www.stengg.com/en/electronics/companies-affiliates/st-electronics-info-security/digisafe-data-diode-solution/

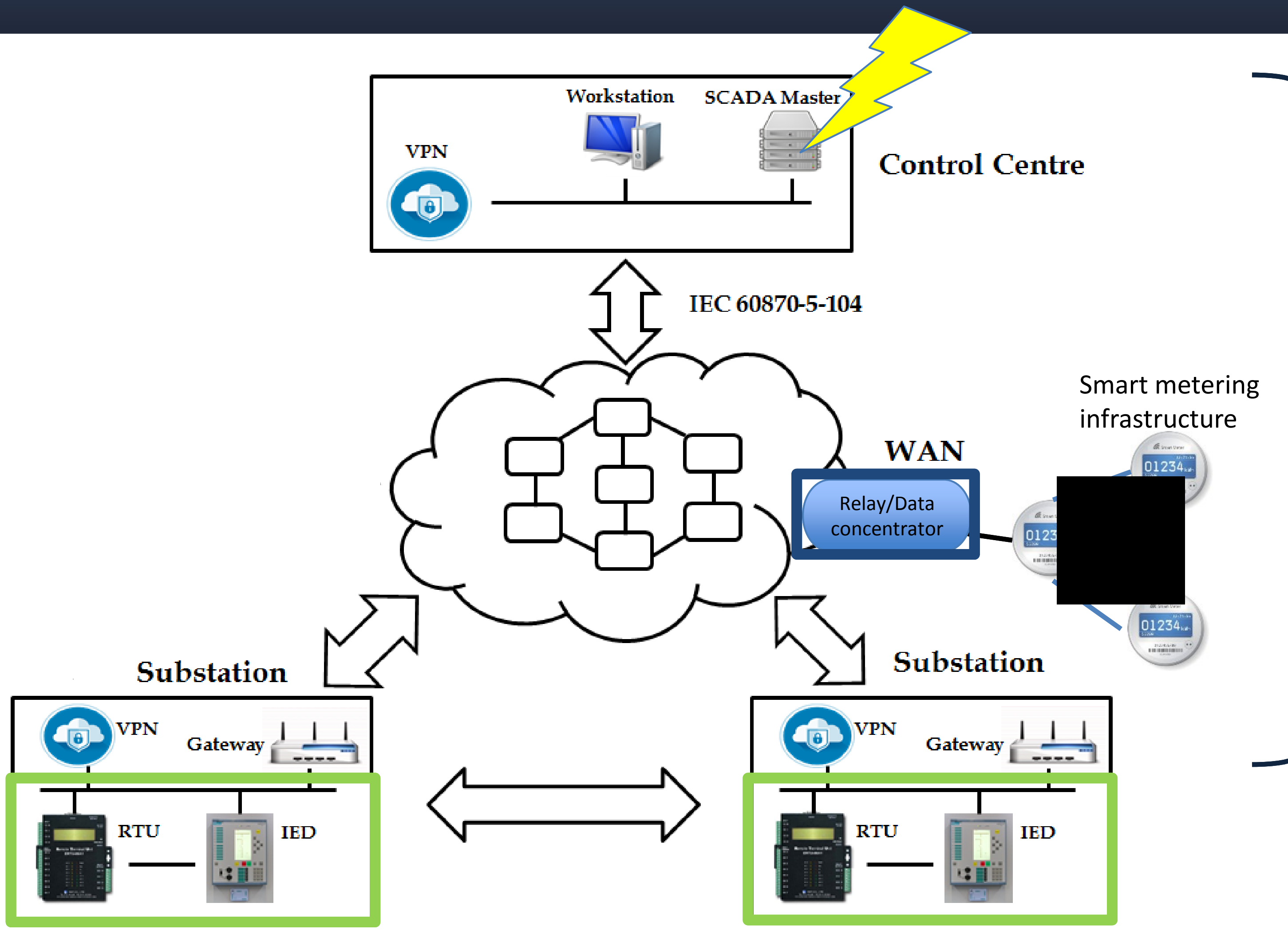
- Enhanced **message authentication**
  - Add bump-in-the-wire (BITW) devices that handle **cryptographic protocols** in a transparent manner



BITW device integrated into EPIC Testbed

02

Need for Additional Lines of Defense



- Authentication
- Access Control
- Security Patch
- Anti-virus
- ~~Firewall~~
- ~~Data diode~~
- ~~Intrusion Detection~~
- ~~IEC 62351~~
- Etc.

Outline

01 **Cyber Threats in Smart Grid Infrastructure**
- Smart grid overview
- Security threats in smart grid

02 **Measures for Securing Smart Grid Systems**
- IEC 62351
- Intrusion detection systems
- Bump-in-the-wire security

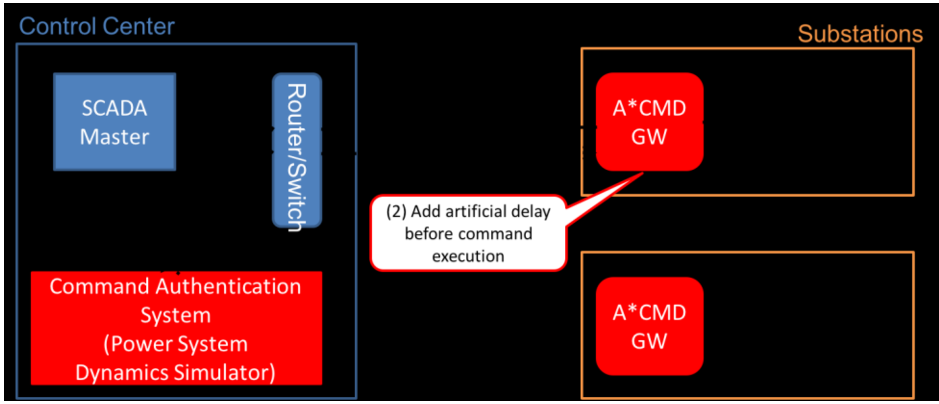
03 **Defending against Malicious Command Injection**
- SCADA command authentication
- Artificial Command-delaying

04 **Countering Data Falsification Attacks in AMI**
- Anomaly Detection in Smart Meter Data
- Evaluation Framework for Anomaly Detectors

05 **Ongoing Projects & Concluding Remark**
- High-fidelity Smart Grid Honeypot

SCADA Command Authentication

- Deployed **at (near) the edge** of cyber infrastructure
- **Reliably mediate** incoming remote control commands
- **Evaluate legitimacy/validity** of the commands before execution

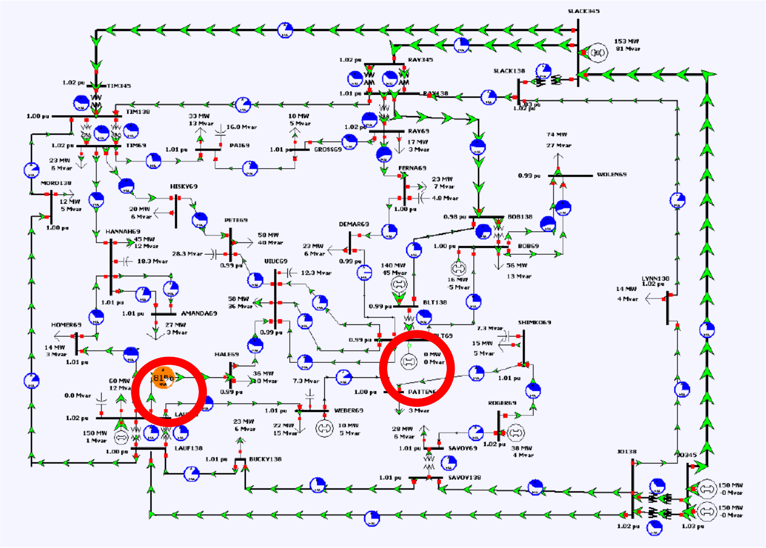


*A*CMD stands for Active Command Mediation Defense.*

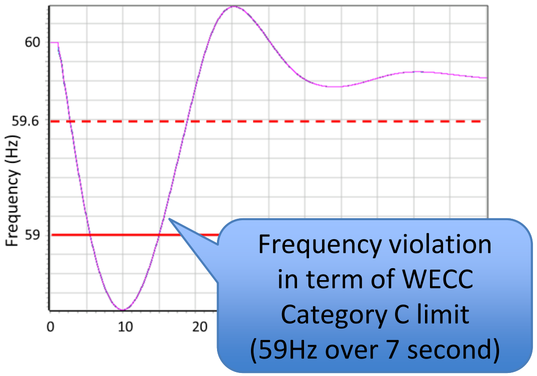
Daisuke Mashima, Prageeth Gunathilaka, and Binbin Chen, "**An Active Command Mediation Approach for Securing Remote Control Interface of Substations**." In Proc. of IEEE SmartGridComm 2016 in November, 2016.
Daisuke Mashima, Prageeth Gunathilaka, and Binbin Chen, **“Artificial Command-delaying for Securing Substation Remote Control: Design and Implementation."** In press for IEEE Transactions on Smart Grid.
Daisuke Mashima, Binbin Chen, Toby Zhou, Ramkumar Rajendran, and Biplab Sikdar, **“Securing Substations through Command Authentication Using On-the-fly Simulation of Power System Dynamics.”** In Proc. of IEEE SmartGridComm 2018.
Daisuke Mashima, Ramkumar Rajendran, Toby Zhou, Binbin Chen, and Biplab Sikdar,

Command Authentication Based on Power System Dynamics Simulation

- Steady-state power flow simulation
  - Employed by many state-of-the-art schemes
  - ***Fast to calculate***
  - ***Provides only limited information***



- Power system dynamics simulation
  - ***Transient-state behavior (e.g., frequency change) as well as cascading events***



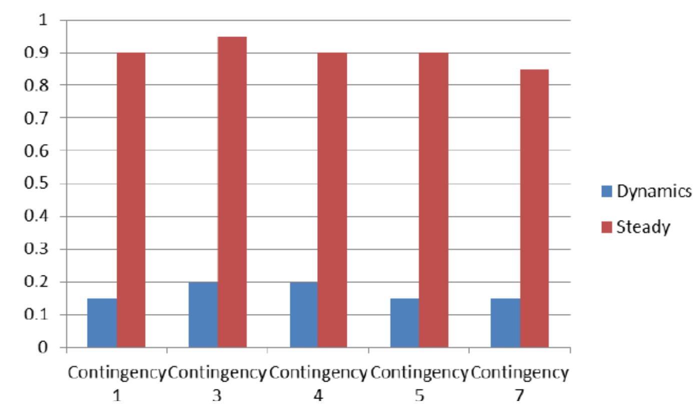
Command Authentication Based on Power System Dynamics Simulation

- Implemented authentication logic
  - **On-the-fly** dynamics simulation
  - Compare simulations with and without the command execution

Algorithm 1 Command Authentication

Require: $PG \leftarrow$ Latest power grid model and status snapshot
Require: $event_{pre} \leftarrow$ Preceeding events to be jointly simulated
Require: $cmd_{new} \leftarrow$ Reported control command to be authenticated
  $Res_0 \leftarrow$ DynSim(PG, $event_{pre}$, $null$)
  $Res_{cmd} \leftarrow$ DynSim(PG, $event_{pre}$, cmd_{new})
  if $isWorse(Res_0, Res_{cmd})$ **then**
    Block execution of cmd_{new}
  else
    Allow execution of cmd_{new}
  end if

- Designed experiments based on N-1 contingency scenarios
  - **No false positive** on the 37-bus model
  - **Lower false negative rate** than the steady-state-based approach



False Negative Rate Comparison

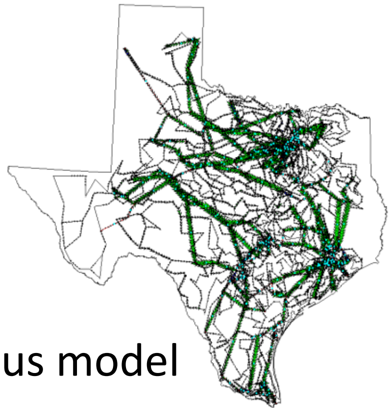
- ***Takes longer time (e.g., 900ms, including pre-/post-processing time)***

Daisuke Mashima, et al., "**Securing Substations through Command Authentication Using On-the-fly Simulation of Power System Dynamics.**" In Proc. of IEEE SmartGridComm 2018 in October, 2018.

ADSC
ADVANCED DIGITAL SCIENCES CENTER

Shortening Simulation Latency

- Shortening simulation duration
- Use simplified model
  - E.g., Thevenin Equivalent Circuit
  - **Trade-off** between accuracy and latency



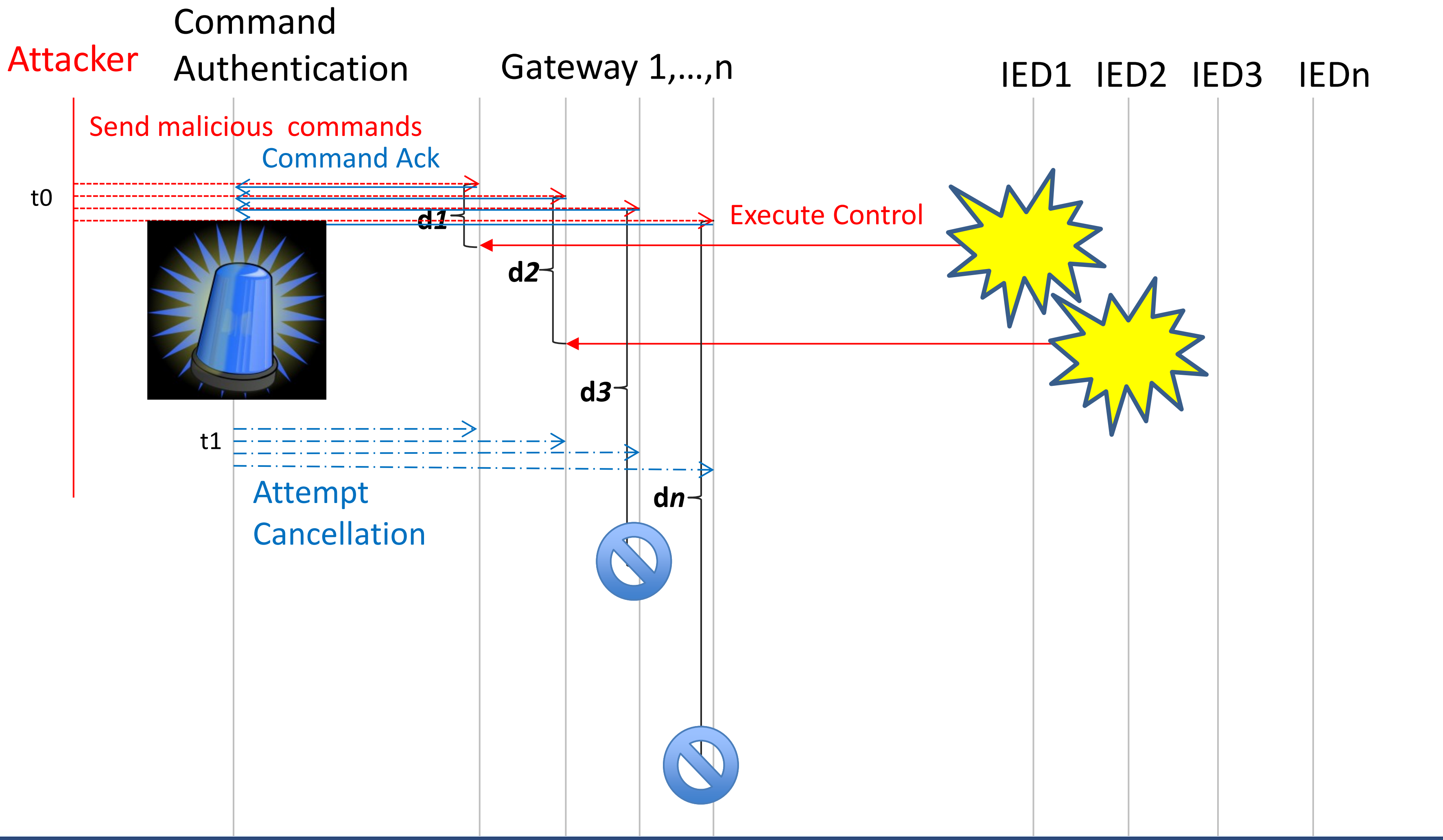
Texas 2000-bus model

POWER SYSTEM DYNAMICS SIMULATION LATENCY WITH VARYING COMPLEXITY OF MODELS

Base Model	Model Size	Duration [sec]	Latency [ms]
37-bus [22]	37 buses	30	458
	23 buses	30	298
	11 buses	30	151
2000-bus [23]	2,007 buses	30	9,134
	1,132 buses	30	5,041
	447 buses	30	1,684
2000-bus [23]	2,007 buses	10	3,083
	1,132 buses	10	1,645
	447 buses	10	578

ADSC
ADVANCED DIGITAL SCIENCES CENTER

Artificial Command-delaying



General Guidelines for Latency

- IEEE PES (Power & Energy Society) Guideline
  - Communication for line sectionalizing: **5 seconds**
  - Communication for load shedding: **10 seconds**
  - Communication for transfer switching: **1 second**
- US DoE guideline
- Survey done by academia

Finding Tolerable Delay

- **Delay tolerance (D_t)** of the power grid
  - Find through contingency simulations with different time delay before executing recovery controls

Algorithm 1 Finding D^* for Given Power Grid Model

Require: $PG \leftarrow$ Power grid model and topology
Require: $SC \leftarrow$ Power grid stability conditions
Require: $CTG \leftarrow$ List of contingencies in scope
$D^* \leftarrow$ Initialize with maximum delay to be considered
for each C in CTG **do**
$Ctl \leftarrow findRecoveryControl(C, PG, SC)$
$Delay_c \leftarrow findTolerableDelay(C, PG, SC, Ctl)$
$D^* \leftarrow Min(Delay_c, D^*)$
end for
return D^*

Name of Gen.	Gen. MW	# of Loads Shed	Max Latency [s]
JO345 #1	150	5	0.9
JO345 #2	150	5	0.9
LAUF69	150	5	1.0
BLT138	140	3	1.2
BLT69	75.23	2	2.5
ROGER69	38	1	3.0

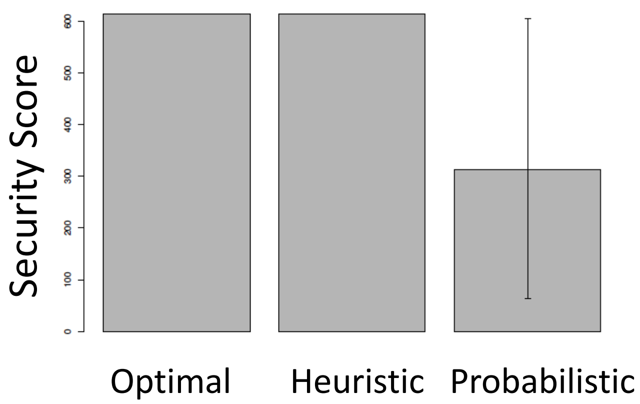
Experiments based on N-1 generator-loss contingencies on 37-bus model

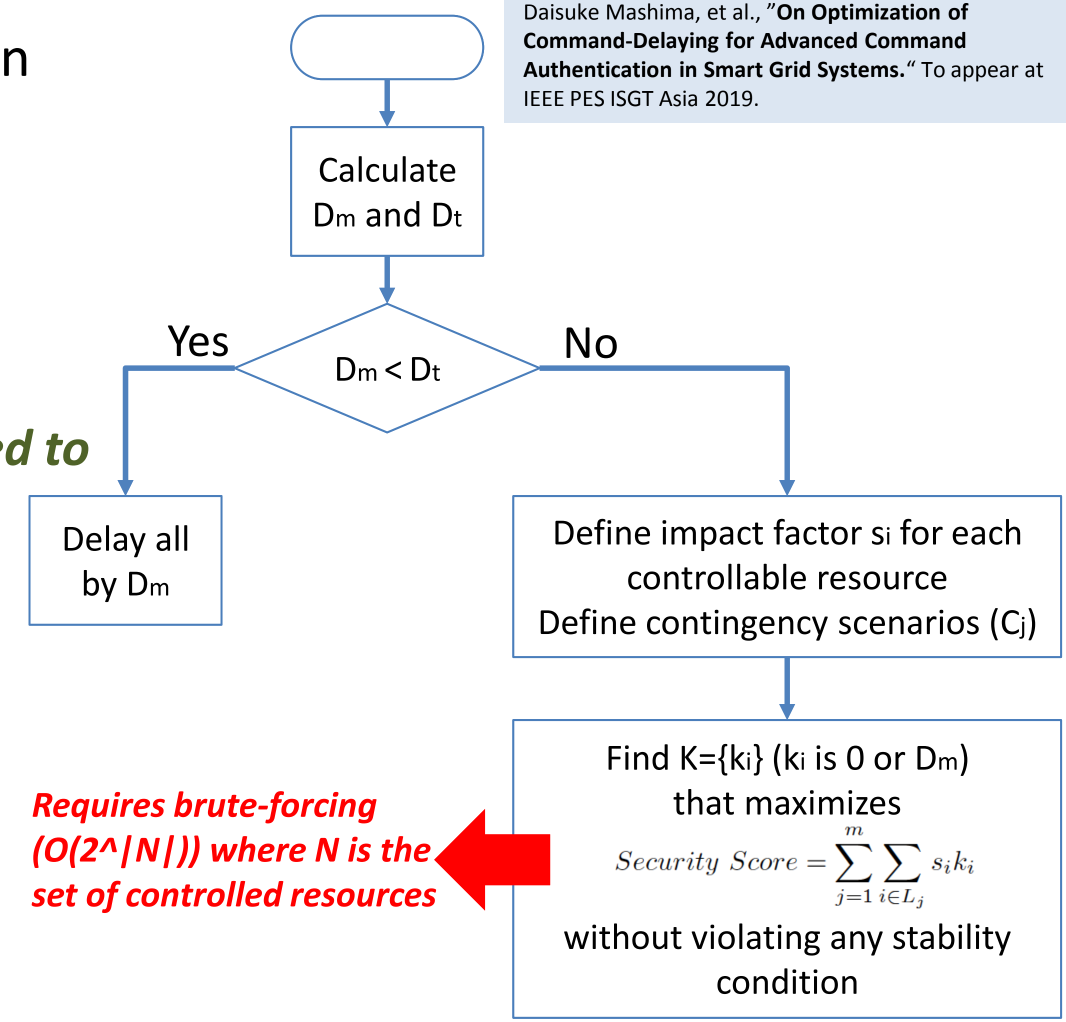
Optimal Command Delaying

Daisuke Mashima, et al., "**On Optimization of Command-Delaying for Advanced Command Authentication in Smart Grid Systems.**" To appear at IEEE PES ISGT Asia 2019.

- **Mandatory latency (D_m)** : Given
- **Delay tolerance (D_t)** : Found

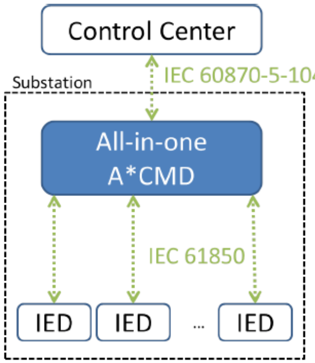
- Defined efficient, heuristic algorithm to find near-optimal solution
  - ***Computational cost is reduced to O(|N|)***



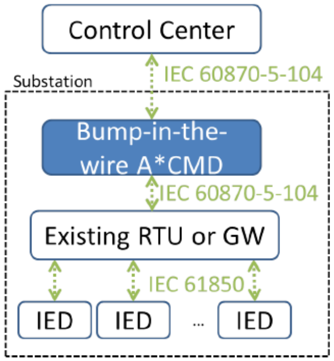


A*CMD-Pi: Prototype Implementation

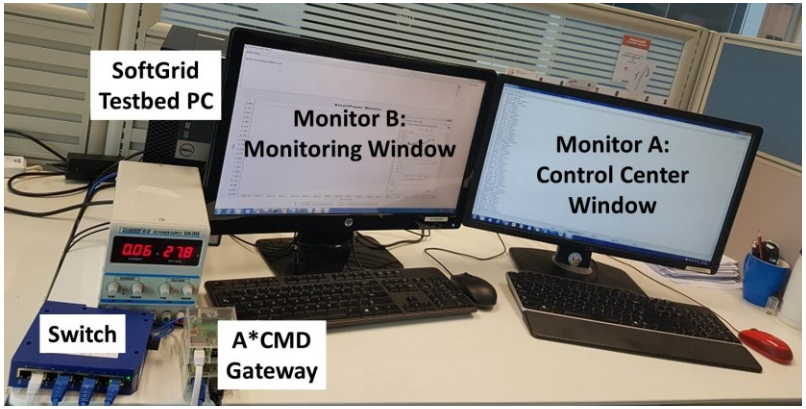
- Implemented on low-cost, embedded platform
- 2 practical deployment options
- Measured throughputs and resource consumption
  - **SoftGrid**: Software-based substation testbed



(a) All-in-one



(b) Bump-in-the-wire (BITW)



PERFORMANCE MEASUREMENTS

Setup	Sustainable Throughput (Commands / sec)	CPU Usage (%)	Memory Usage (%)
All-in-one	33	36.70	15.40
BITW w/ RPi	33	26.16	8.60
BITW w/ PC	65	37.50	8.80
BITW only	over 87	44.28	16.20
No A*CMD	33	23.97	13.60
ZNX 202 [31]	less than 10	-	-

Outline

01 Cyber Threats in Smart Grid Infrastructure

- Smart grid overview
- Security threats in smart grid

02 Measures for Securing Smart Grid Systems

- IEC 62351
- Intrusion detection systems
- Bump-in-the-wire security

03 Defending against Malicious Command Injection

- SCADA command authentication
- Artificial Command-delaying

04 Countering Data Falsification Attacks in AMI

- Anomaly Detection in Smart Meter Data
- Evaluation Framework for Anomaly Detectors

05 Ongoing Projects & Concluding Remark

- High-fidelity Smart Grid Honeypot

Anomaly Detection in Smart Meter Data

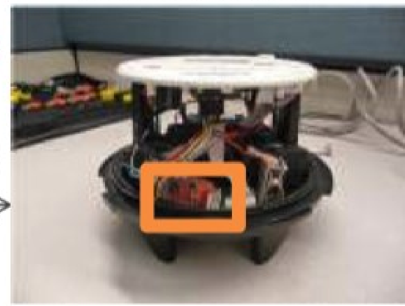
- Adversary Model

Compromised Smart Meter

f(t)

Real Consumption

$$Y_1, \ldots, Y_n$$

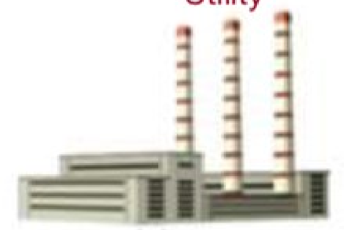


a(t)

Fake Meter Readings

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

Utility



- For electricity theft detection:

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":

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

Electricity Theft Detectors

Various candidates:

- **ARMA generalized likelihood ratio test** — $\bar{\epsilon}^2$ > τ, where $\bar{\epsilon} = \frac{1}{n}\sum_{i=1}^{n} \epsilon_i$
- Simple average energy consumption — $\bar{Y}$ < τ, where $\bar{Y} = \frac{1}{N}\sum_{i=1}^{N} Y_i$
- Non-parametric statistics (CUSUM, EWMA) — S_i > τ, where $S_i = MAX(0, S_{i-1} + (\mu - Y_i - b))$
- Unsupervised learning (LOF)

Which is better? How good are these?

Challenge: Lack of real attack data for evaluation!

Evaluation of Detectors

- Evaluate performance in terms of **worst-case loss**
  - Define worst-possible attack strategy for each detector

$\bar{Y} < \tau$, where $\bar{Y} = \frac{1}{N}\sum_{i=1}^{N} Y_i$

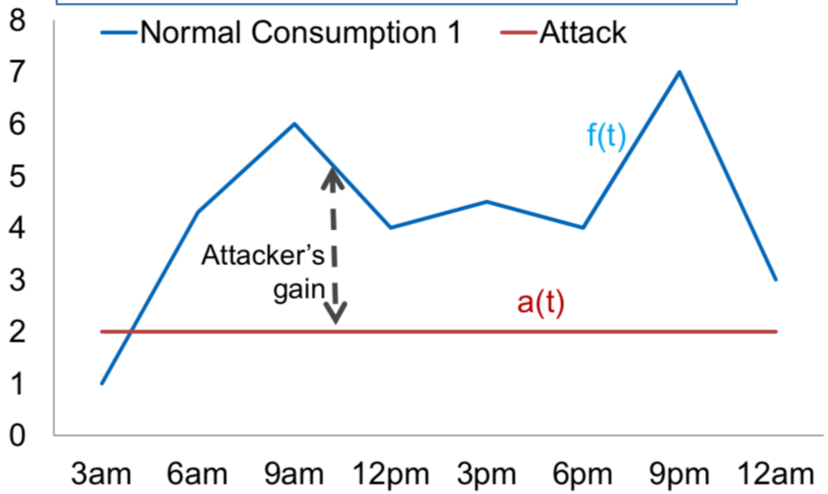


Illustration with Simple Average Detector

- Attack against ARMA-GLR detector

$\bar{\epsilon}^2 > \tau$, where $\bar{\epsilon} = \frac{1}{n}\sum_{i=1}^{n} \epsilon_i$

1. Calculate $E = \sqrt{\tau}$
2. Send $\hat{Y}_i = \mathbb{E}_0[Y_i|\hat{Y}_1, \ldots, \hat{Y}_{i-1}] - E$

- Attack against CUSUM detector

Calculate $M = \frac{\tau + Nb}{N}$

send $\hat{Y}_i = \mu - M$

Daisuke Mashima and Alvaro A. Cardenas, "**Evaluating Electricity Theft Detectors in Smart Grid Networks.**" In Proc. of the 15th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2012), Amsterdam, Netherlands, 2012.

Evaluation of Detectors

- Experiments with **real-world energy consumption data**
  - 15-minute interval reading
  - Collected from 108 residential customers in the US

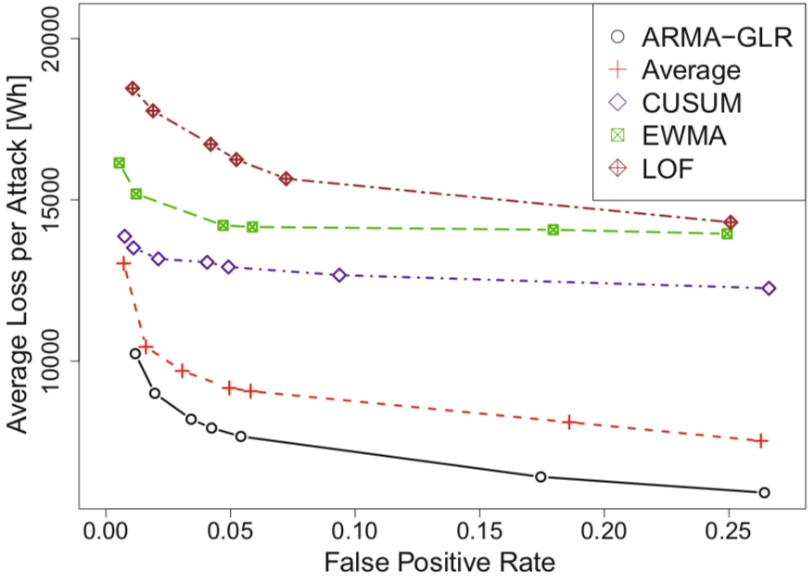


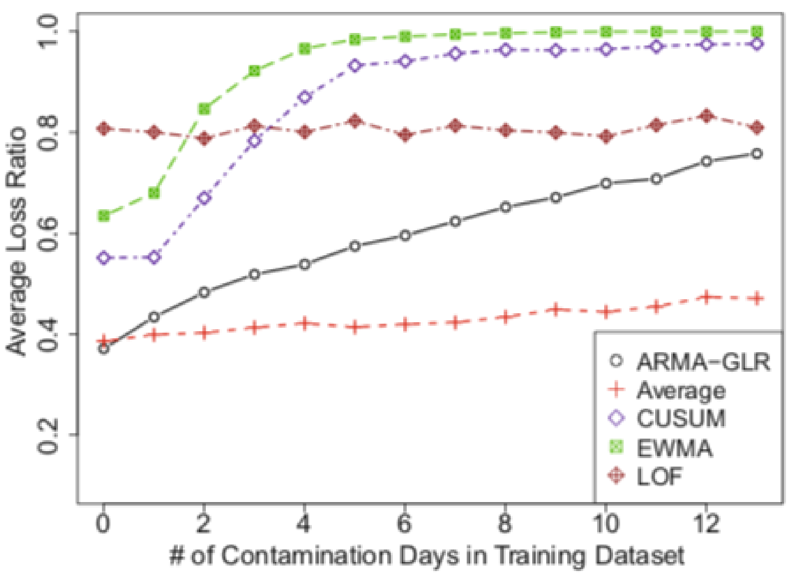
Table 1. Monetary loss caused by undetected electricity theft (5% false positive rate)

Detector	FP Rate	Average Loss	Revenue Lost
Average	0.0495	\$0.55	43%
EWMA	0.0470	\$0.852	68%
CUSUM	0.0491	\$0.775	62%
LOF	0.0524	\$0.975	77%
ARMA-GLR	0.0423	\$0.475	38%

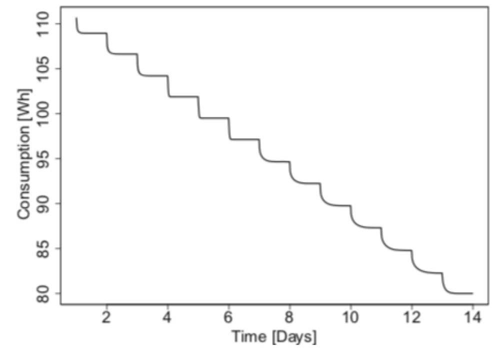
Daisuke Mashima and Alvaro A. Cardenas, "**Evaluating Electricity Theft Detectors in Smart Grid Networks.**" In Proc. of the 15th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2012), Amsterdam, Netherlands, 2012.

Performance under Data Contamination

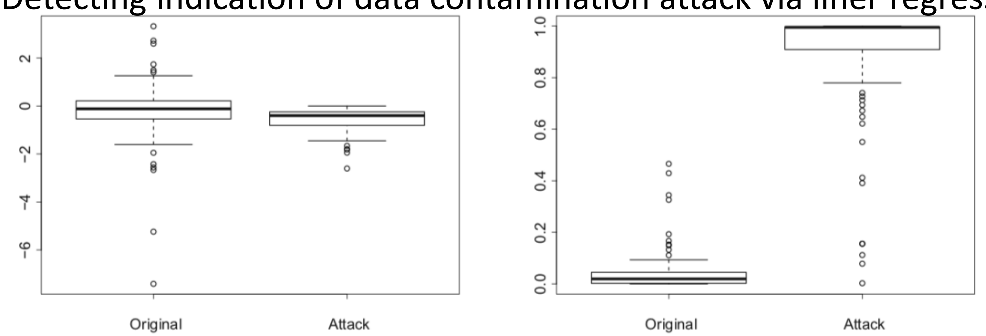
- Undetected attack data would mislead detectors



Example of attack against ARMA-GLR detector with data contamination



Detecting indication of data contamination attack via liner regression



(a) Distribution of slopes of fitted linear Models (b) Distribution of determination Coefficients of fitted linear models

Outline

01 **Cyber Threats in Smart Grid Infrastructure**
- Smart grid overview
- Security threats in smart grid

02 **Measures for Securing Smart Grid Systems**
- IEC 62351
- Intrusion detection systems
- Bump-in-the-wire security

03 **Defending against Malicious Command Injection**
- SCADA command authentication
- Artificial Command-delaying

04 **Countering Data Falsification Attacks in AMI**
- Anomaly Detection in Smart Meter Data
- Evaluation Framework for Anomaly Detectors

05 **Ongoing Projects & Concluding Remark**
- High-fidelity Smart Grid Honeypot

Honeypot for Smart Grid Systems

honeypot
/ˈhʌnɪpɒt/

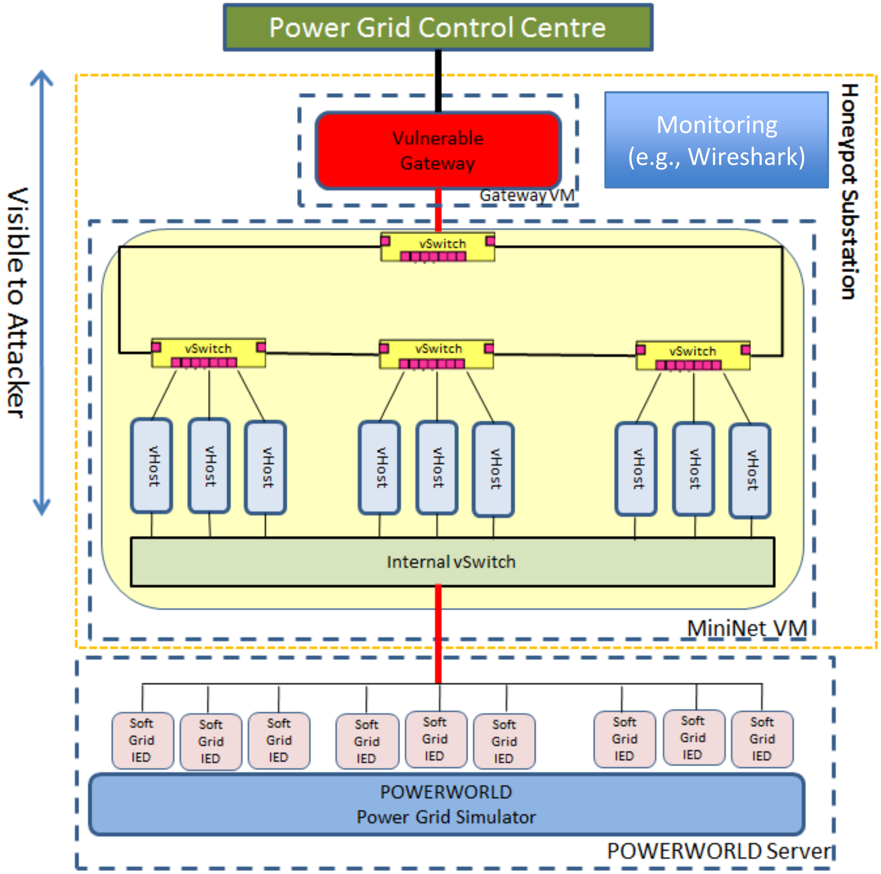
noun
noun: **honeypot**; plural noun: **honeypots**; noun: **honey-pot**; plural noun: **honey-pots**

1. a container for honey.
   "an earthenware honeypot"

- In cybersecurity domain, honeypot is **a dummy system to attract attackers**.
  - Should look like a valuable, real system
  - Intentionally exposed to attackers
- Honeypot can be used to:
  - Collect **threat intelligence**
  - **Buy time** before actual attacks
  - Detect **persistent attackers**

High-fidelity Substation Honeypot

- Honeypot system for smart grid / ICS is not mature yet.
  - Lack of physical-system behavior
- Integrate power system simulation for consistent, cyber-physical system view
  - Use **system and network virtualization** for realism and scalability
  - Implemented on top of **SoftGrid** (http://www.illinois.adsc.com.sg/softgrid/)
- Funded by **Singapore Cybersecurity Consortium** for enhancement of realism and functionality (2018-)
  - https://sgcsc.sg/event-2018-09-seedgrant.html

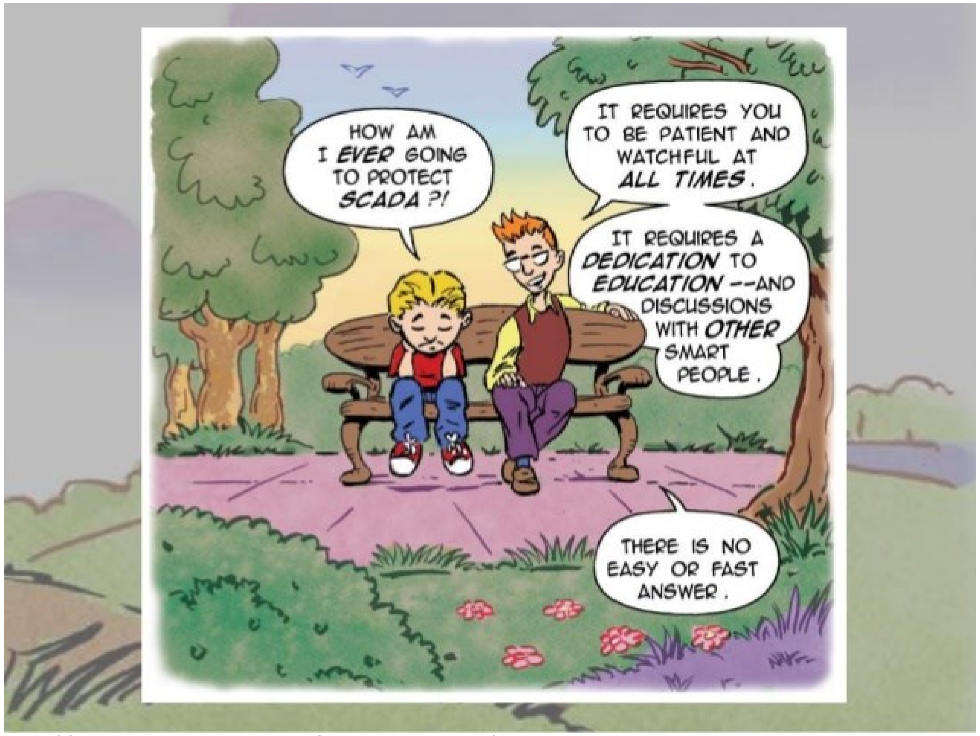


Daisuke Mashima, Binbin Chen, Prageeth Gunathilaka, and Edwin Tjiong, **"Towards a Grid-wide, High-fidelity electrical Substation Honeynet."** In Proc. of IEEE SmartGridComm 2017.

Concluding Remarks

- Power grid is under cyber attack in reality!
- Existing security measures are not enough to counter emerging cyber threats.
- SCADA command authentication and anomaly detection in sensor data provided additional lines of defense before attacks are reaching physical systems.
- Substation honeypot is effective for collecting threat intelligence as well as for countering persistent attackers.
- Power grid operators, industry, and academia (CS and EE/ECE experts) should join force. Please feel free to contact us for any interest in collaboration and internship opportunities!

Questions?



https://www.slideshare.net/RobertMLee1/a-child-like-approach-to-grid-cybersecurity

Web: https://adsc.illinois.edu

Email: daisuke.m@adsc-create.edu.sg