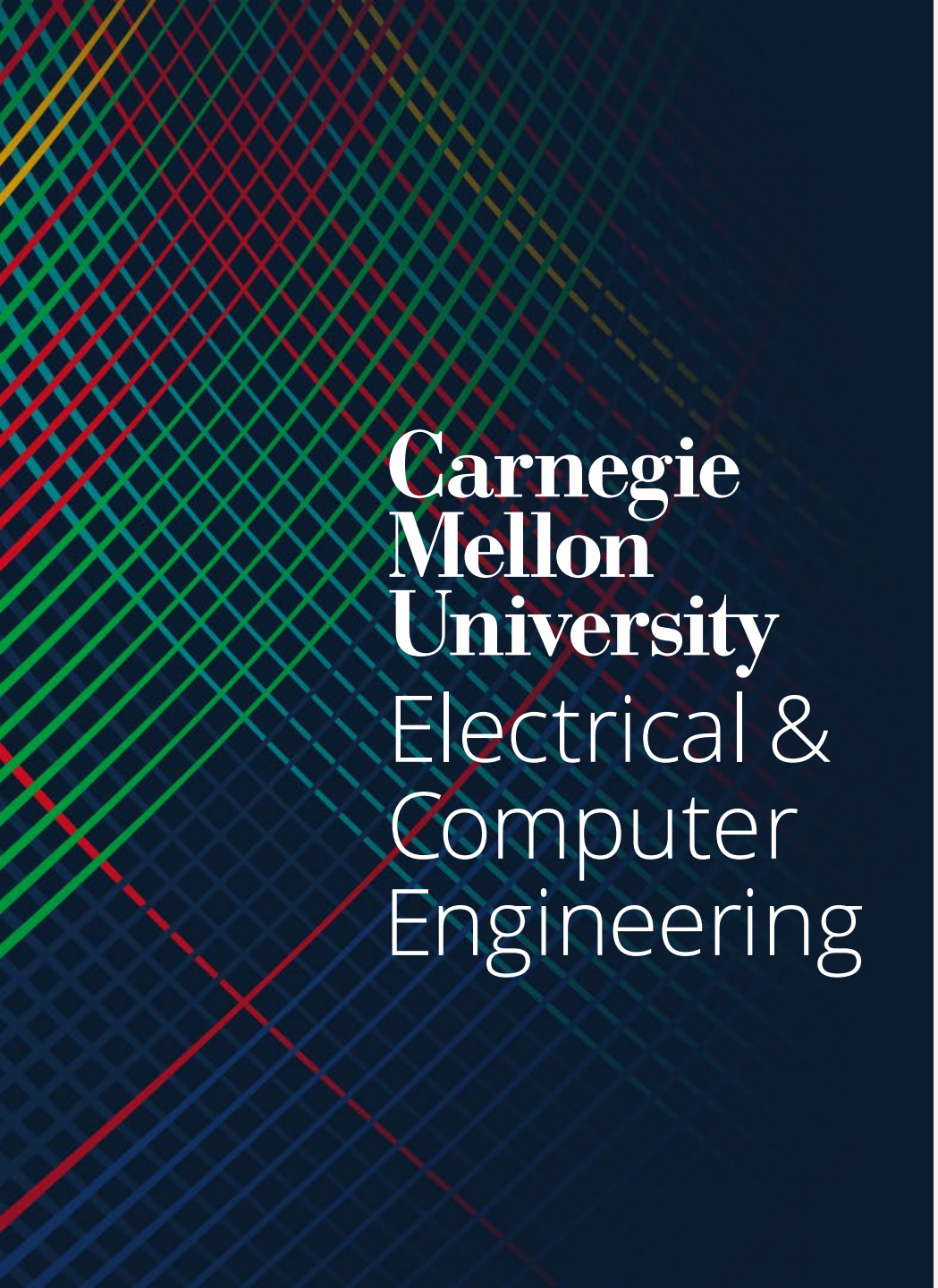


Data-assisted Physics-based Modeling and Simulation for Grid Cybersecurity

AUGUST 16TH, 2022

Amritanshu Pandey
amritanshu.pandey@uvm.edu

My Journey

- **Academic Experience**
  - Special Faculty at Carnegie Mellon – **2020-2022**
  - Incoming Asst. Professor at the University of Vermont – **2023-**
- **Industry Experience**

ISO-NE
Summer 2013

Analyzing critical systems in nuclear stations
2012-mid 2015

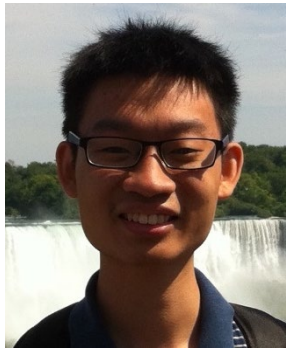
Pearl Street
TECHNOLOGIES

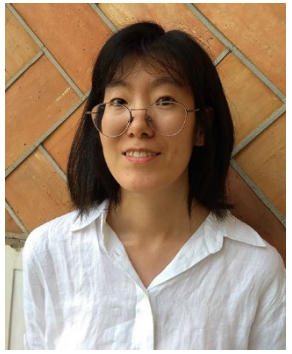
Commercializing PhD research
2019-2020

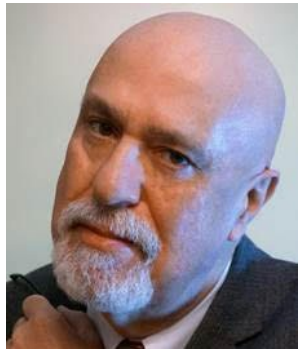
Collaborators


Lujo Bauer


Christos Faloutsos


Bryan Hooi


Shimiao Li


Craig Miller


Larry Pileggi

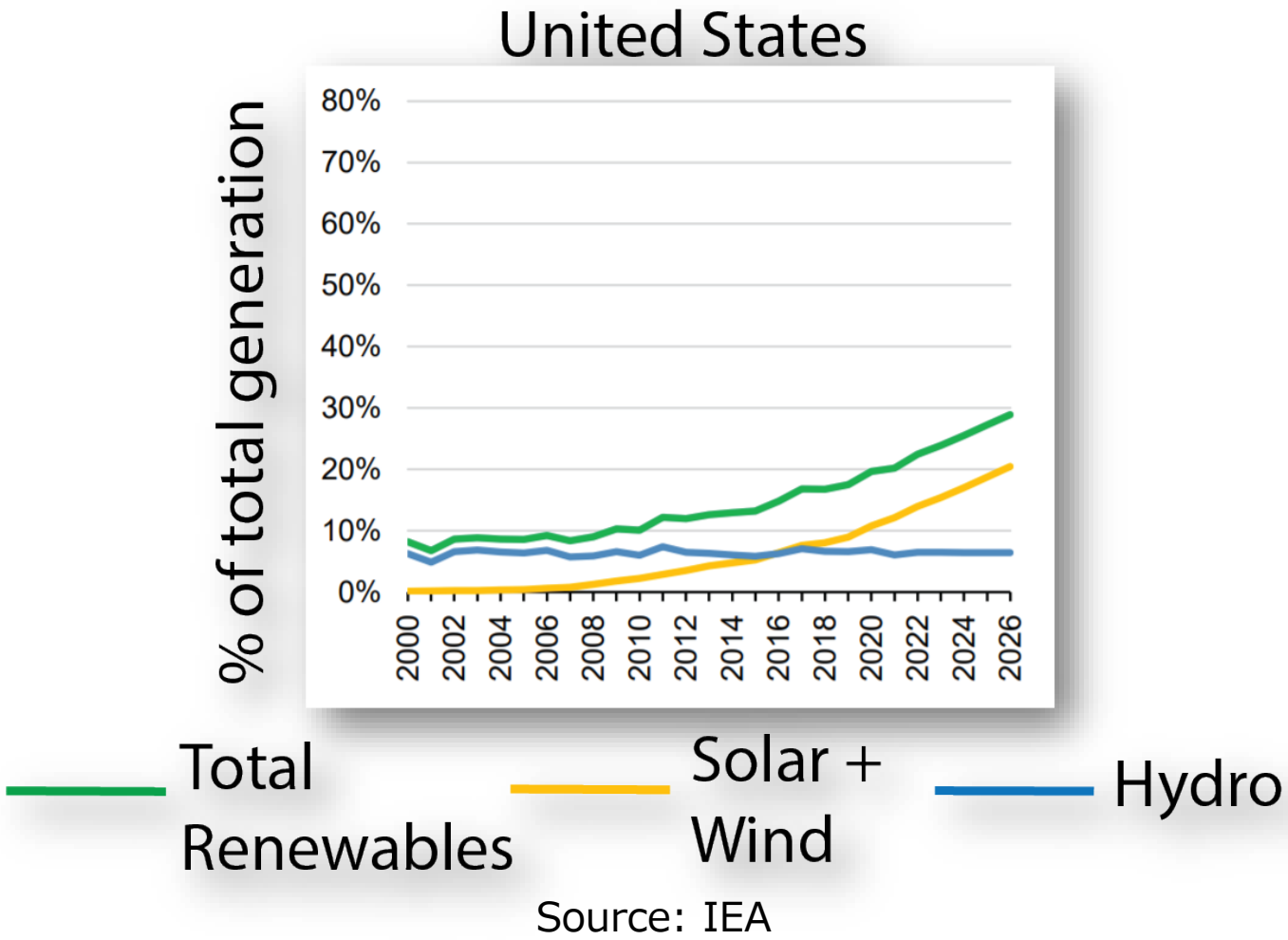

Vyas Sekar


Brian Singer

Evolving Grid → Real Cybersecurity Concerns

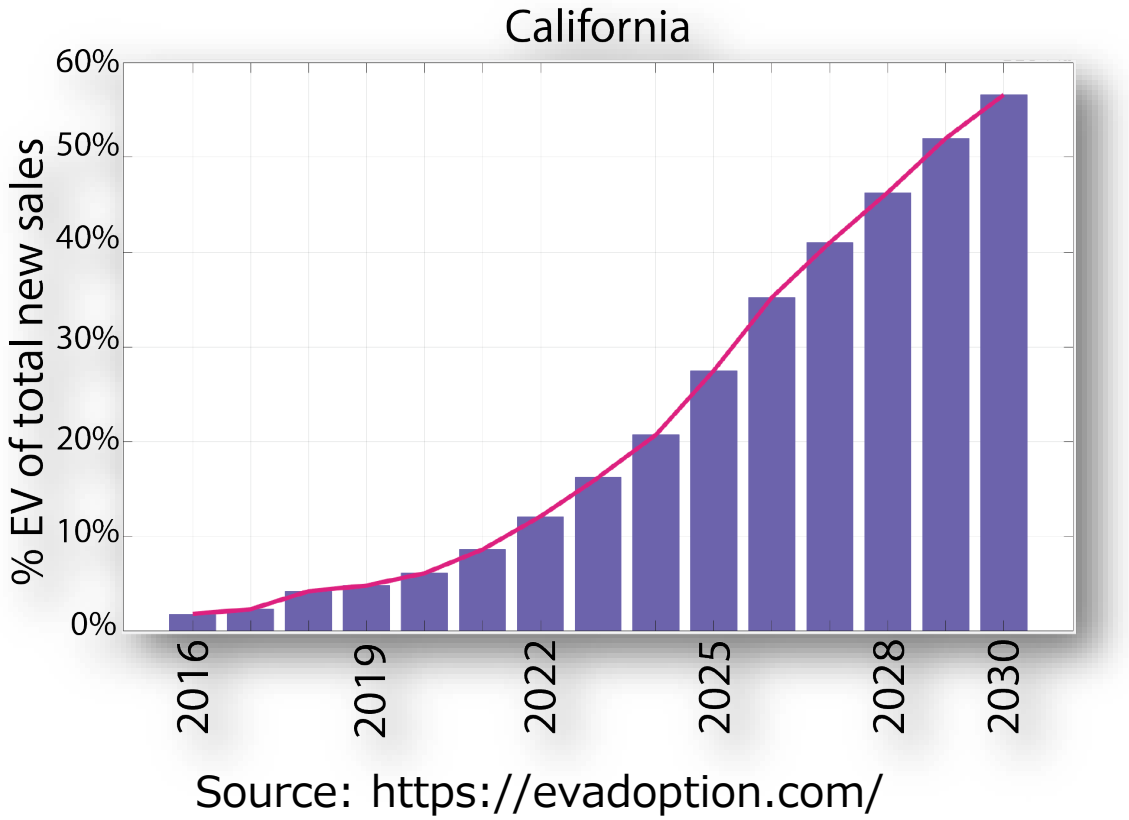
The Electric Grid is at an Inflection Point

- Decarbonization



Source: IEA

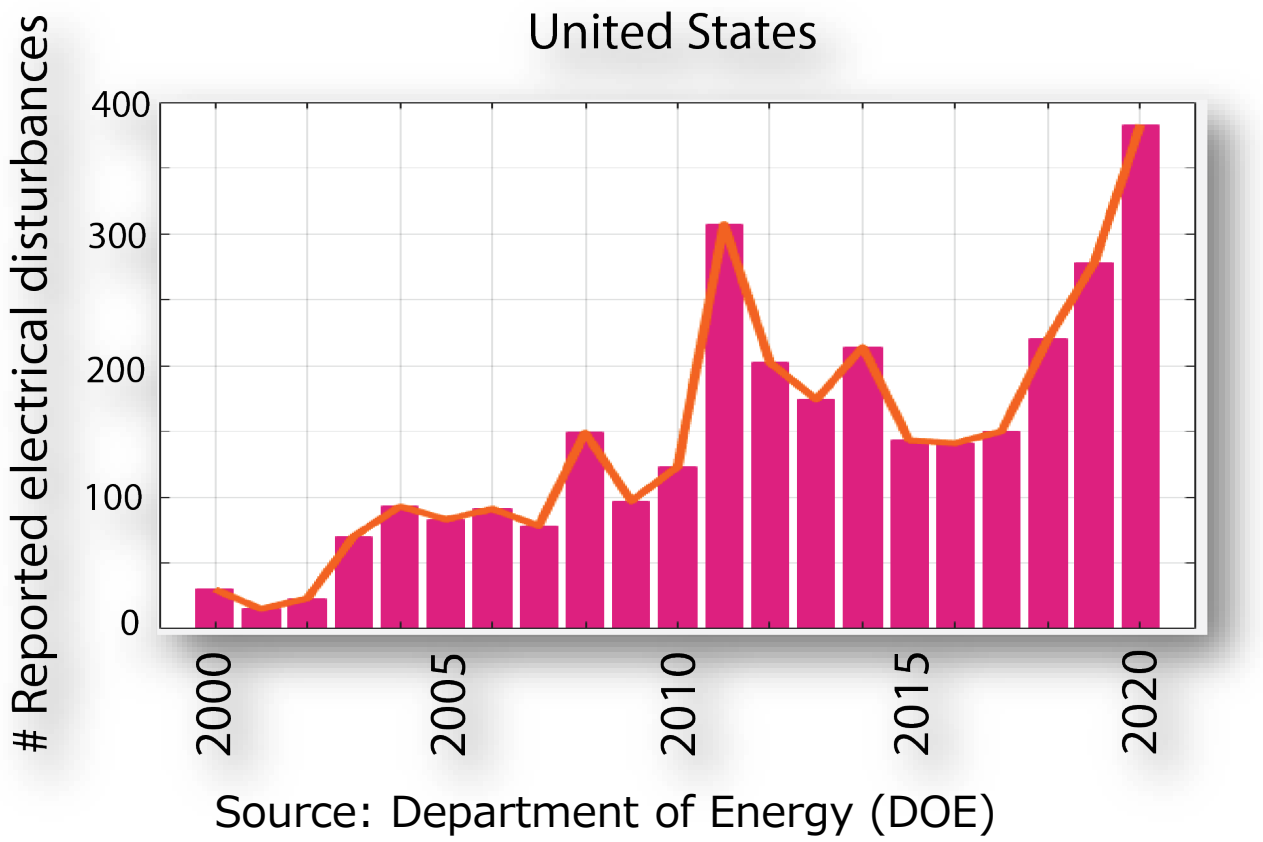
The Electric Grid is at an Inflection Point



Source: https://evadoption.com/

- Decarbonization
- Electrification

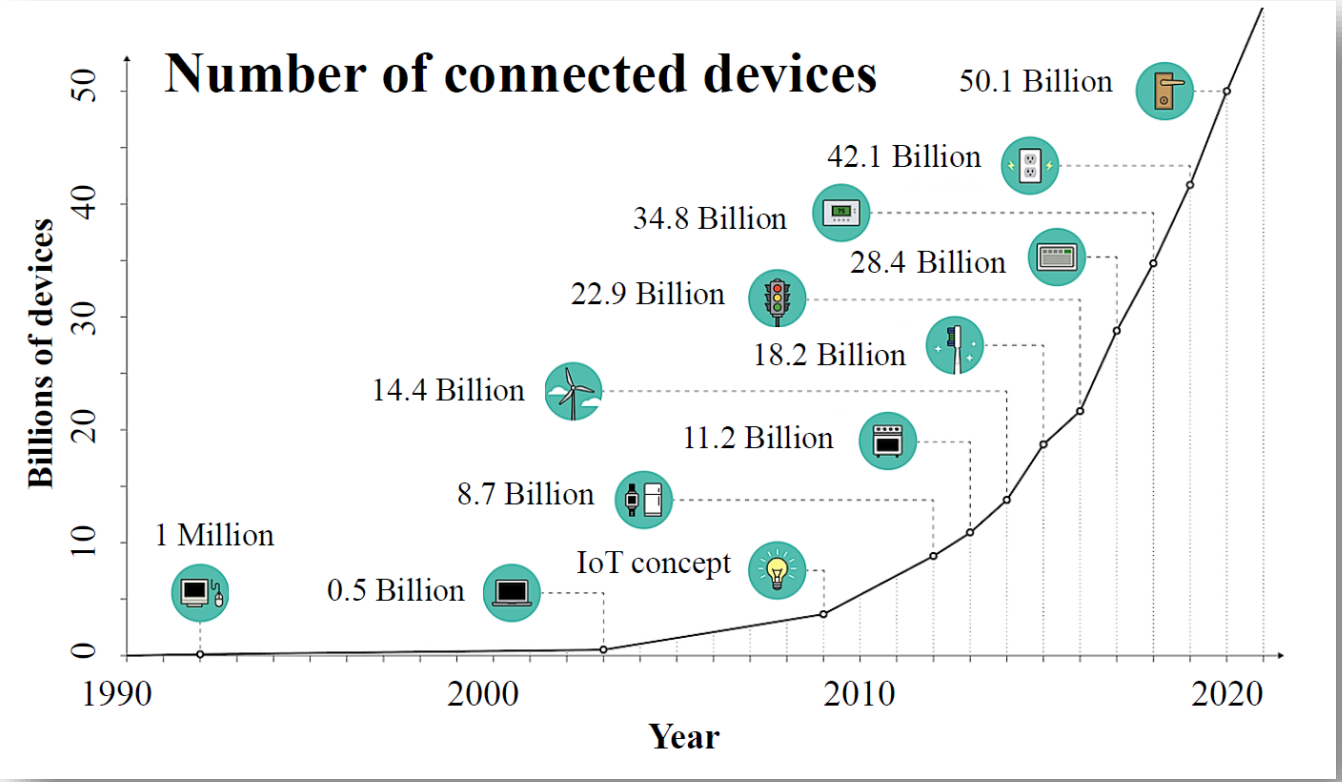
The Electric Grid is at an Inflection Point



Source: Department of Energy (DOE)

- Decarbonization
- Electrification
- Deteriorating resilience

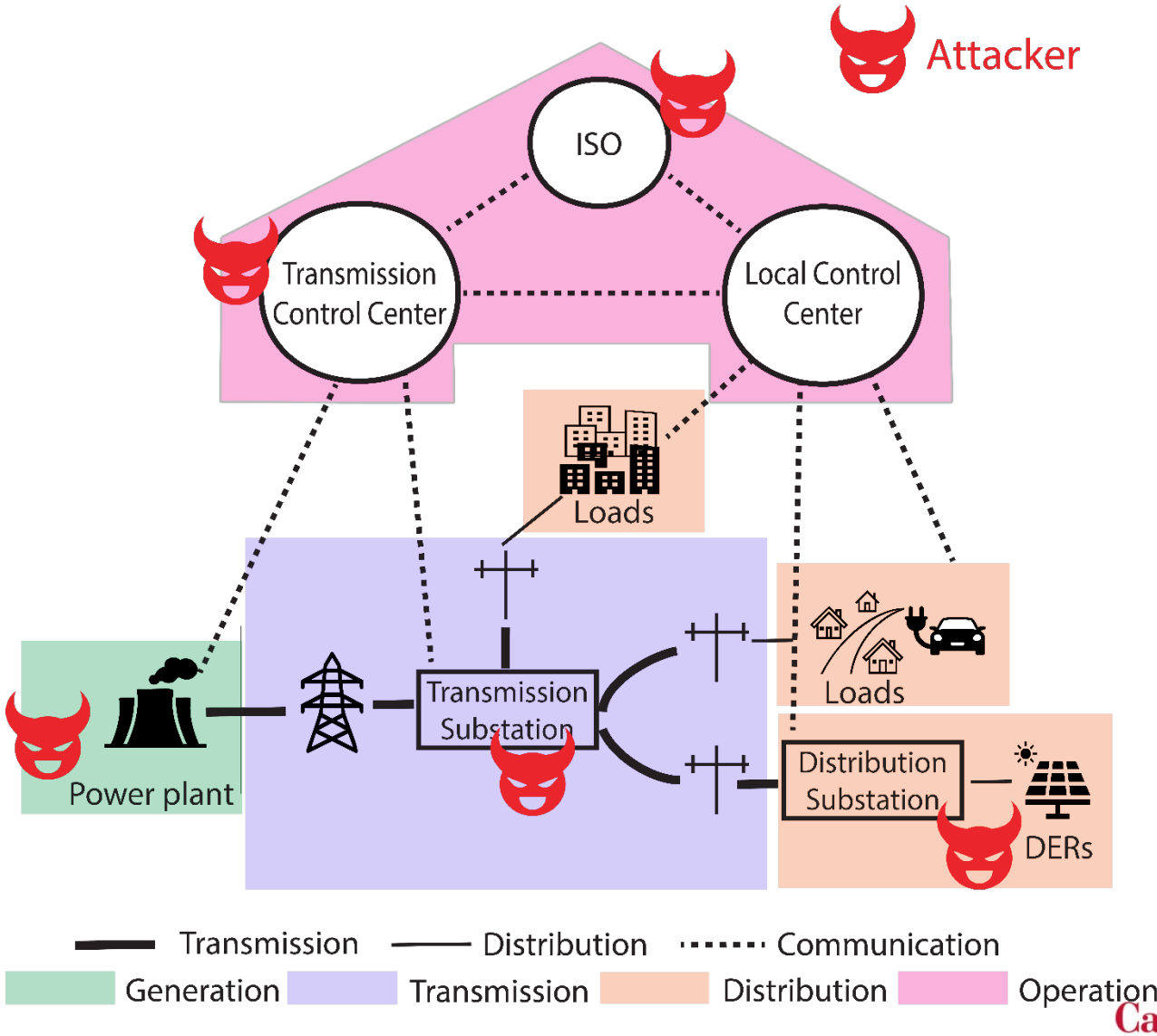
The Electric Grid is at an Inflection Point



Source: www.ncta.com

- Decarbonization
- Electrification
- Deteriorating resilience
- Increasing remote automation

Evolving Attack Surface

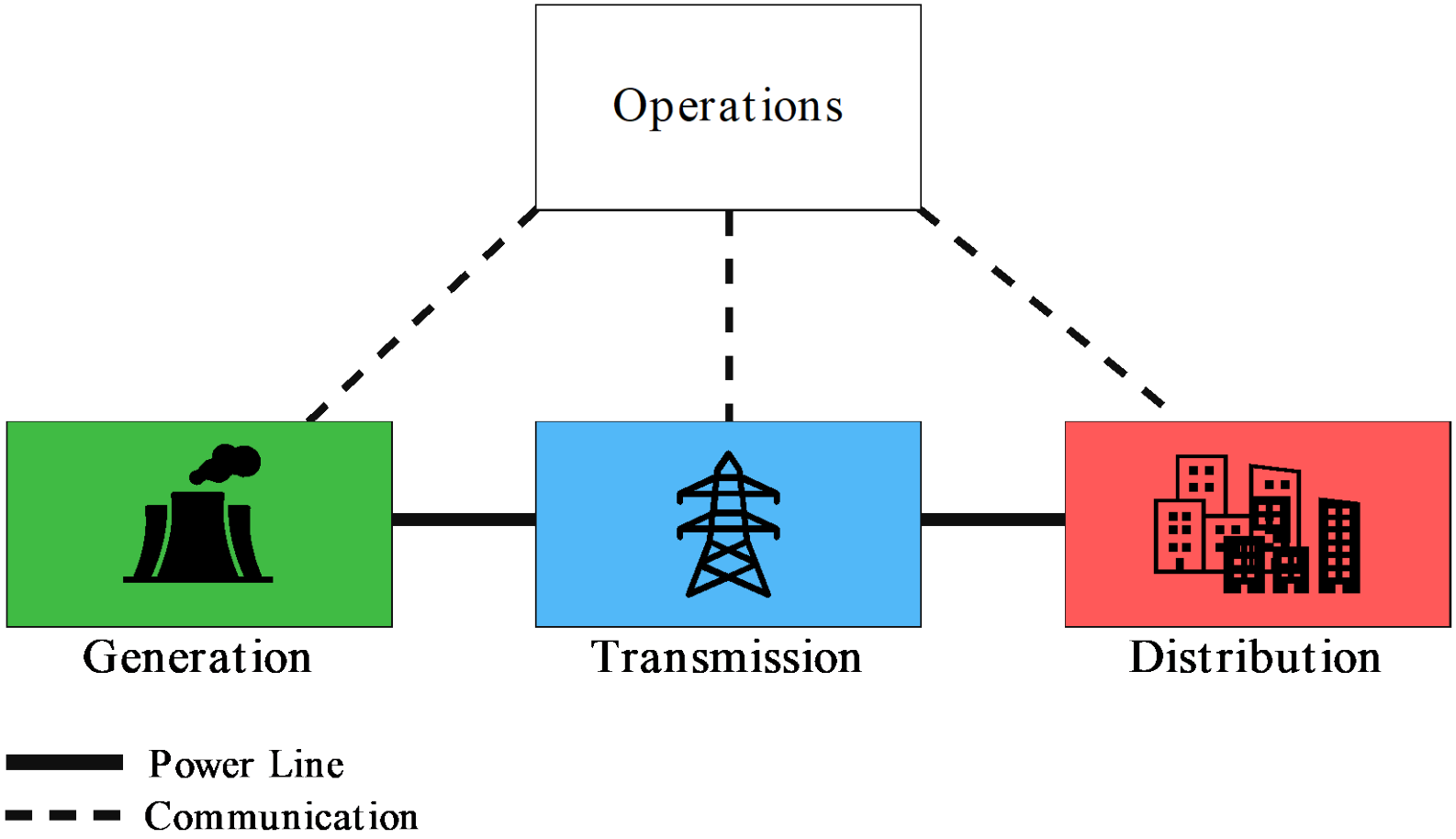


Grid Cybersecurity is a Real Threat Now

Cyberthreats Discussed in this Talk

- MadIoT threat
- False-data injection attack (FDIA)
- Anomalous Topology Threat

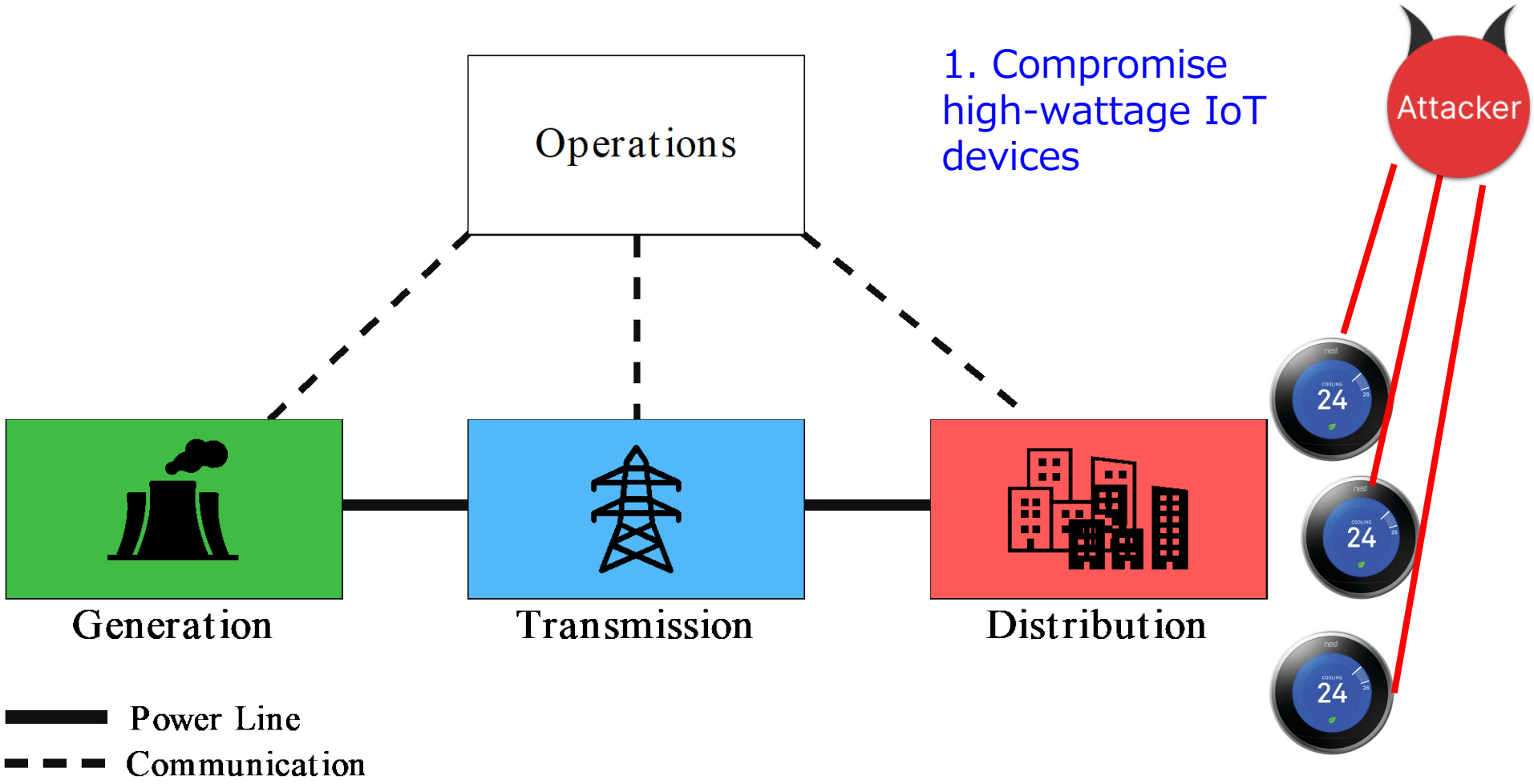
Introduction to MadIoT Threat



Saleh, Prateek Mittal, and H. Vincent Poor. "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid." In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 15-32. 2018.

Fig. Ackn. Brian Singer, ECE, CMU

Introduction to MadIoT Threat



Saleh, Prateek Mittal, and H. Vincent Poor. "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid." In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 15-32. 2018.

Fig. Ackn. Brian Singer, ECE, CMU

Introduction to MadIoT Threat

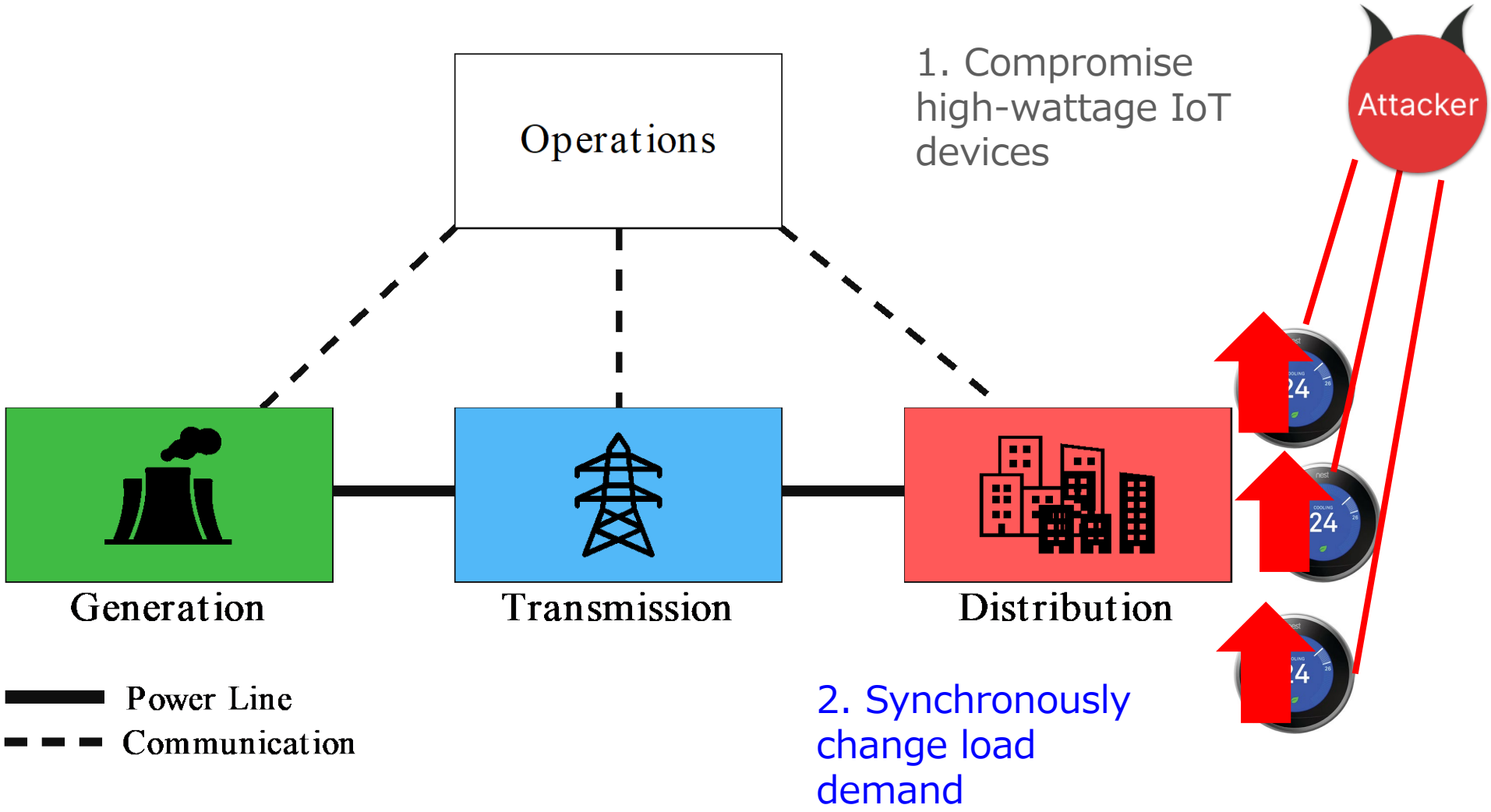


Fig. Ackn. Brian Singer, ECE, CMU

Introduction to MadIoT Threat

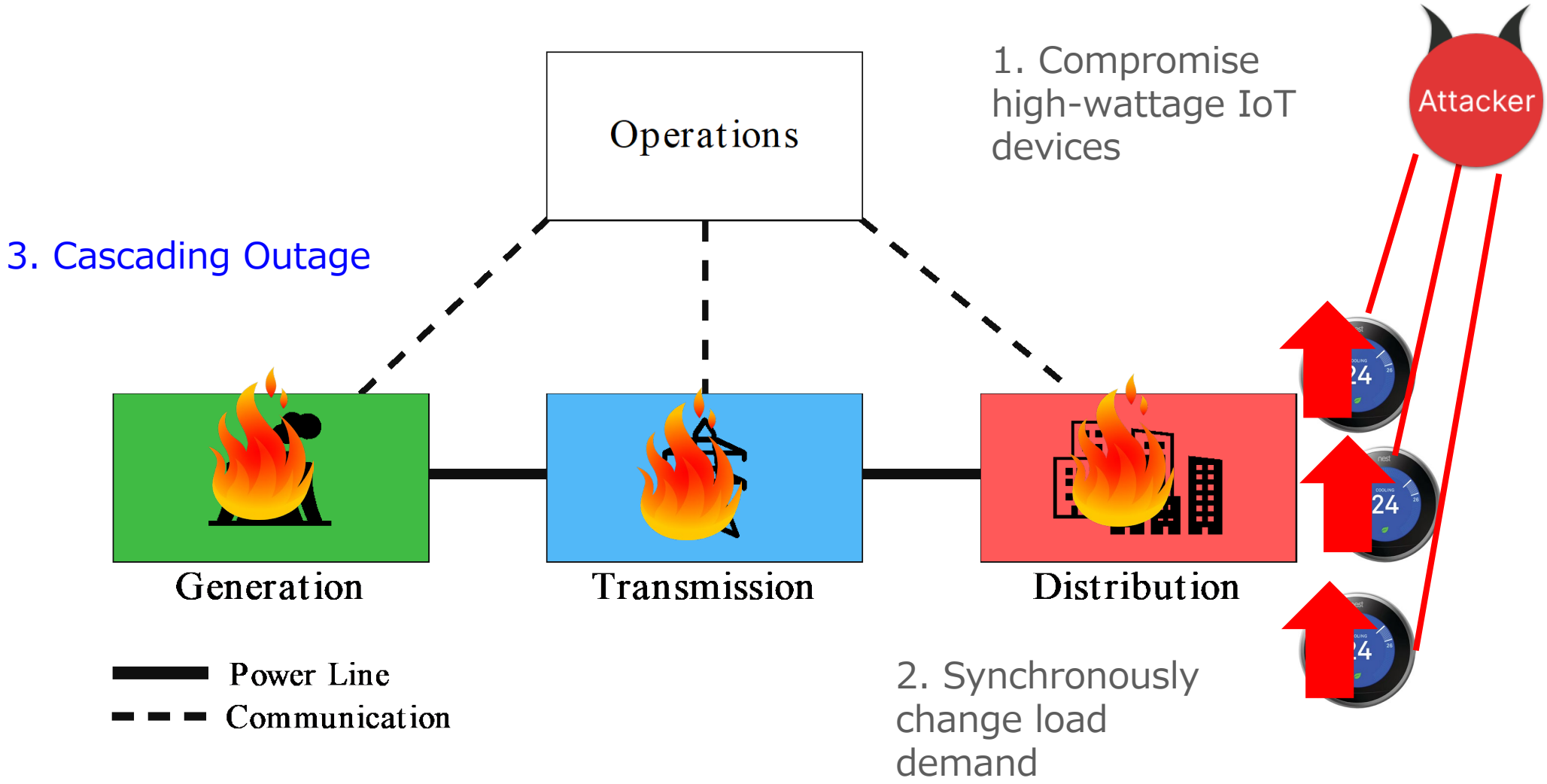
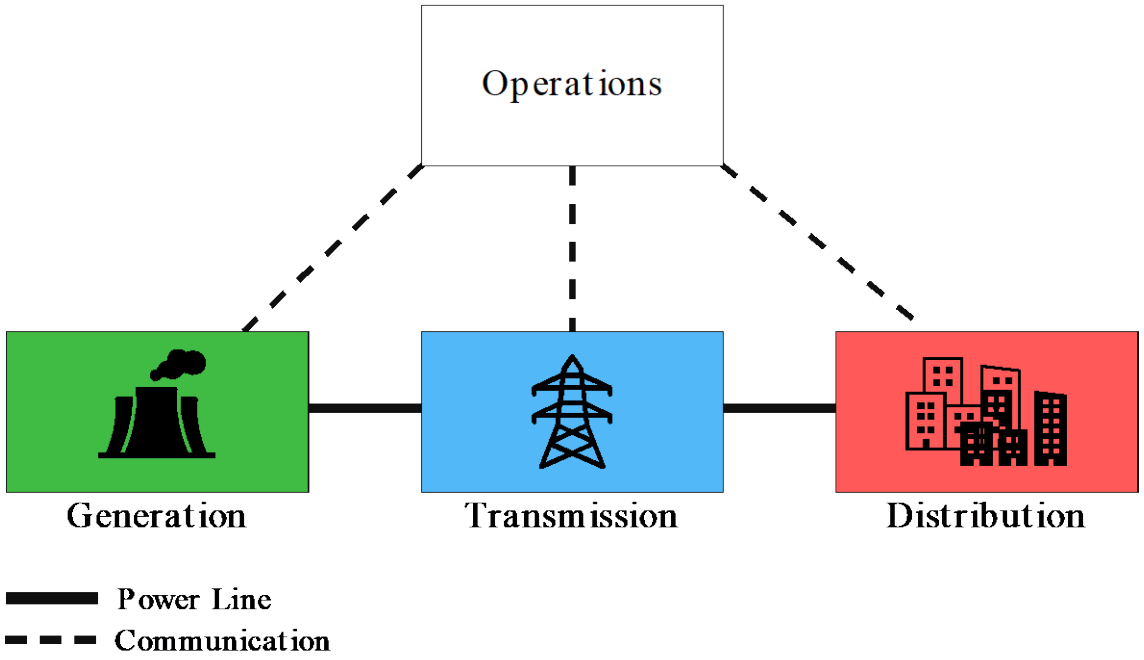


Fig. Ackn. Brian Singer, ECE, CMU

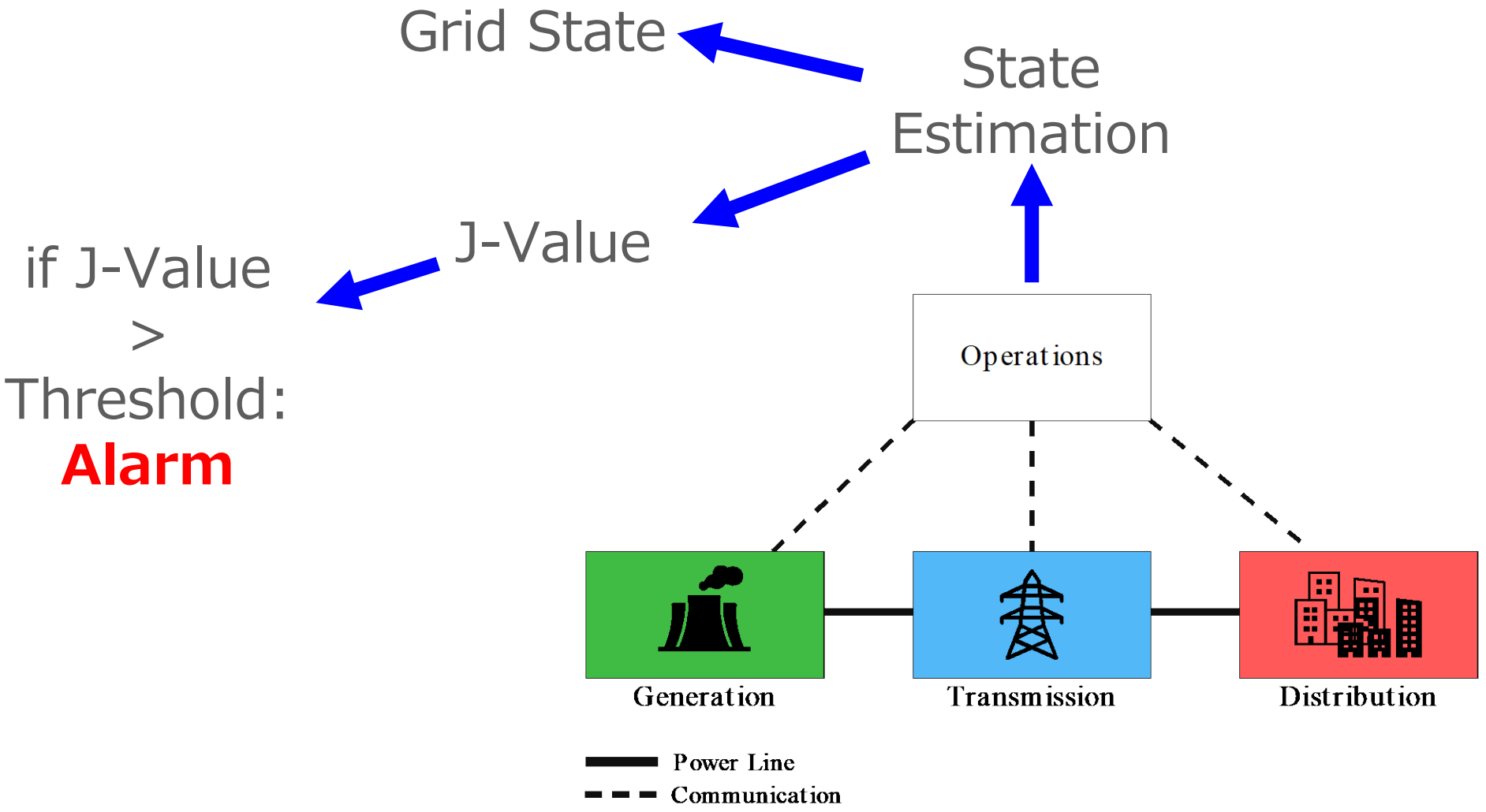
Introduction to False Data Injection Attack

- False Data Injection Attack (FDIA) spoofs sensor data to cause grid malfunction
  - Key idea: strategically spoof measurement data to bypass existing detection algorithms

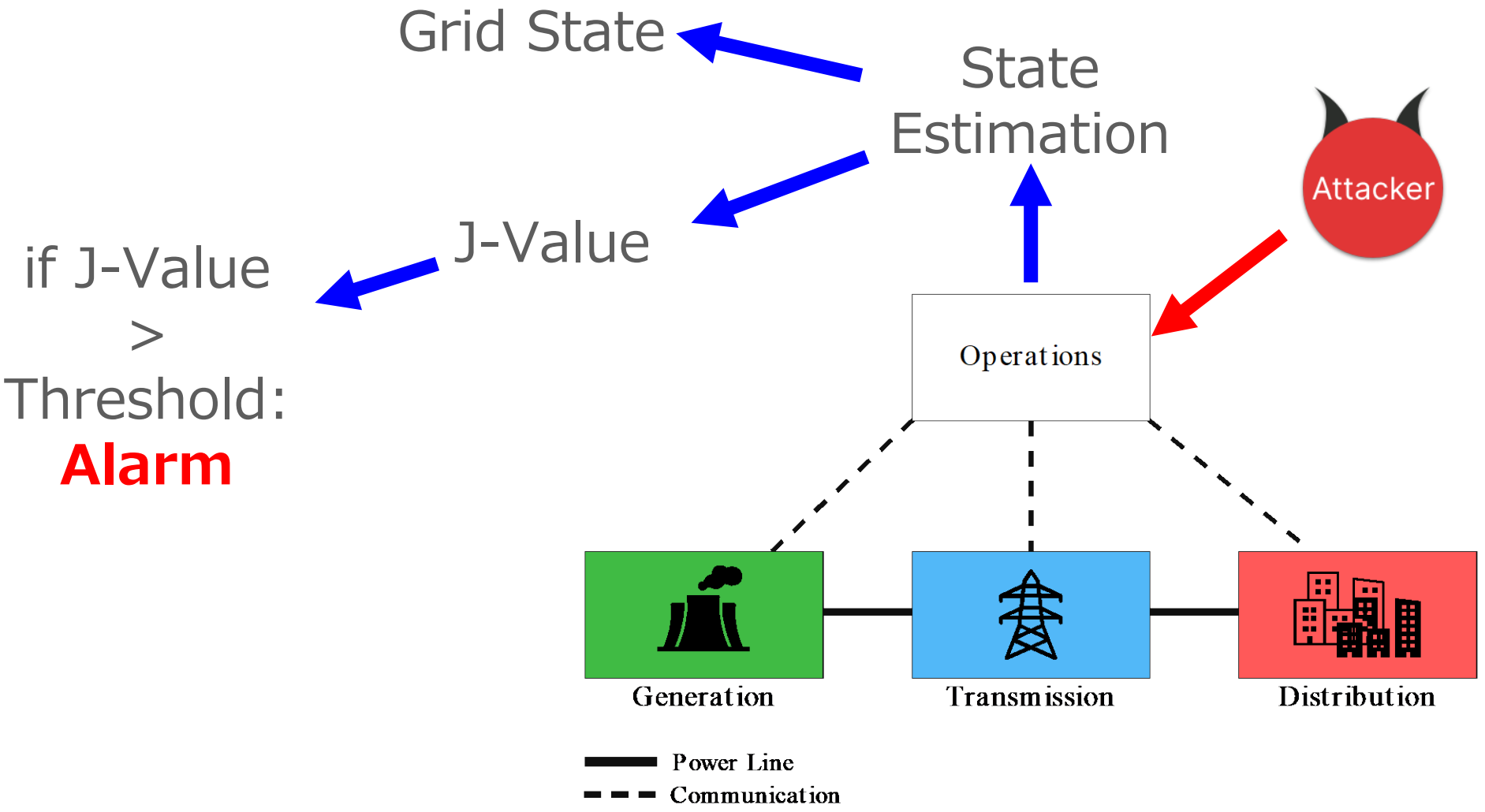


Liu, Yao, Peng Ning, and Michael K. Reiter. "False data injection attacks against state estimation in electric power grids." ACM Transactions on Information and System Security (TISSEC) 14, no. 1 (2011): 1-33.

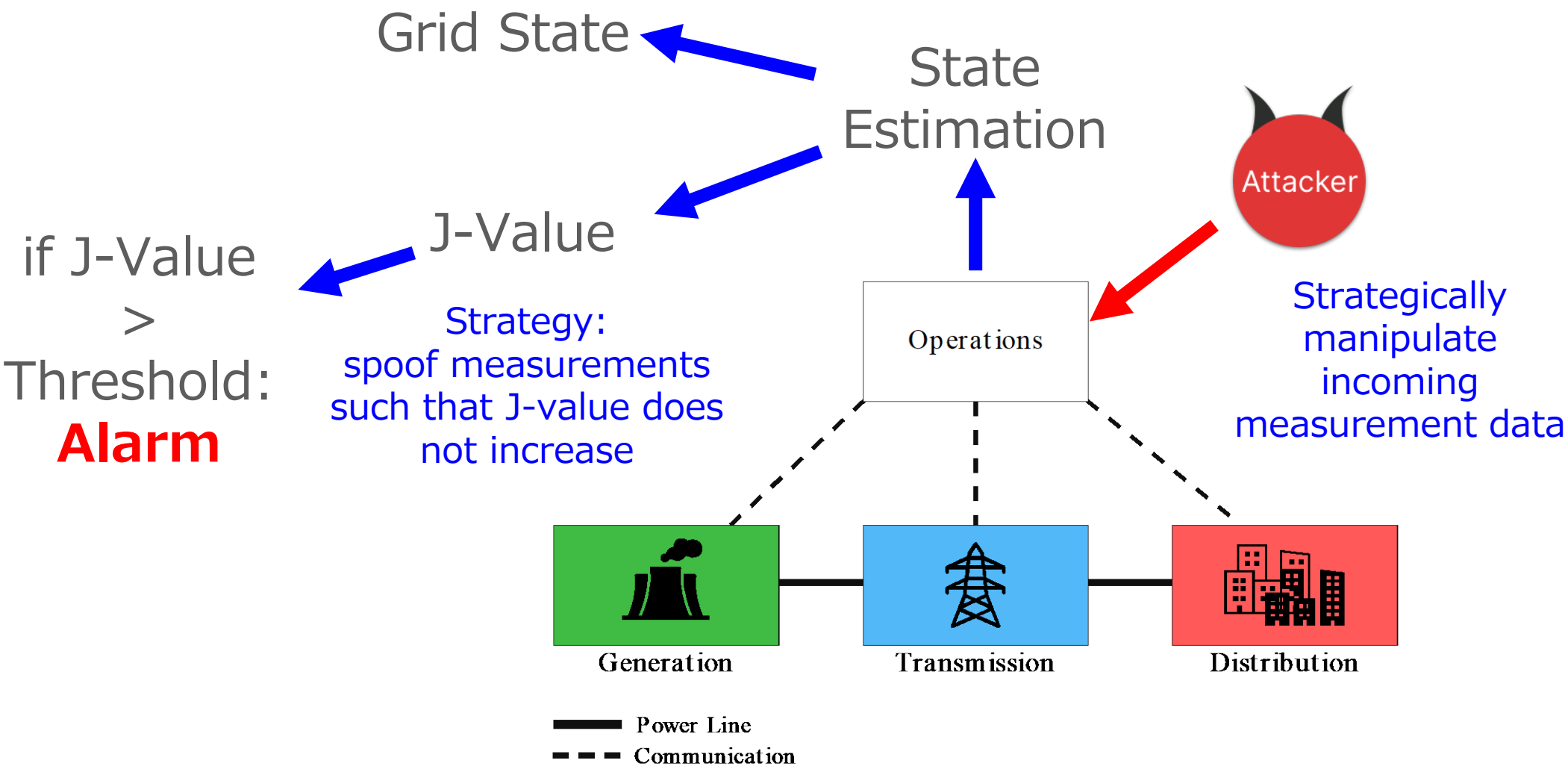
Introduction to False Data Injection Attack



Introduction to False Data Injection Attack

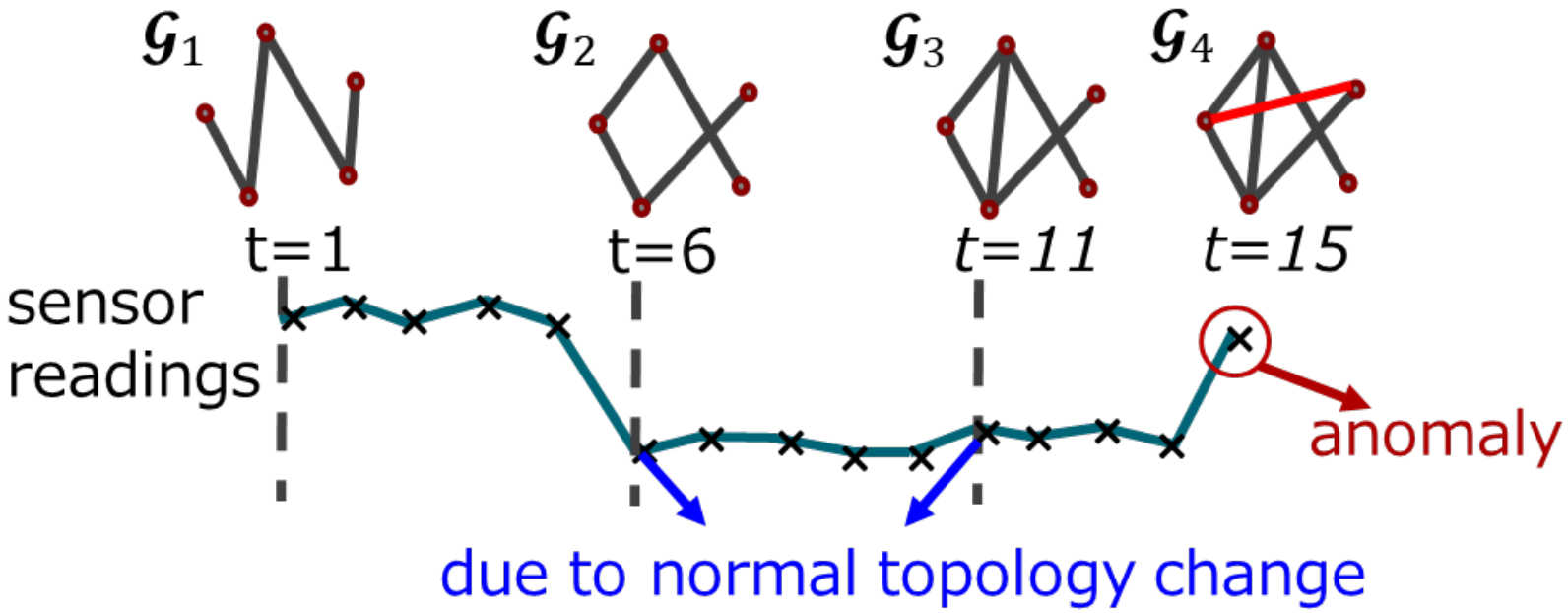


Introduction to False Data Injection Attack



Introduction to Anomalous Topology Threat

- In this threat, an attacker's goal is to change the grid topology
  - E.g., Toggle the circuit breaker for one of two parallel transmission lines



Modeling and Simulation Framework for Cyber-Threat Evaluation

Carnegie Mellon University
Electrical & Computer Engineering

Status Quo in Threat Evaluation - MadIoT

BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid

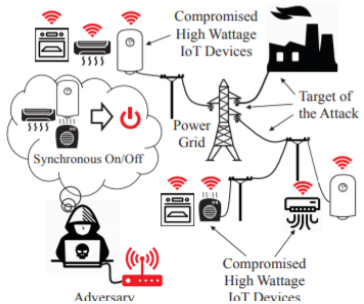
Saleh Soltan
Department of Electrical Engineering
Princeton University
ssoltan@princeton.edu

Prateek Mittal
Department of Electrical Engineering
Princeton University
pmittal@princeton.edu

H. Vincent Poor
Department of Electrical Engineering
Princeton University
poor@princeton.edu

Abstract

We demonstrate that an Internet of Things (IoT) botnet of high wattage devices–such as air conditioners and heaters–gives a unique ability to adversaries to launch large-scale coordinated attacks on the power grid. In particular, we reveal a new class of potential attacks on power grids called the Manipulation of demand via IoT (MadIoT) attacks that can leverage such a botnet in order to manipulate the power demand in the grid. We study five variations of the MadIoT attacks and evaluate their effectiveness via state-of-the-art simulators on real-world power grid models. These simulation results demonstrate that the MadIoT attacks can result in local power outages and in the worst cases, large-scale blackouts. Moreover,



Not Everything is Dark and Gloomy:
Power Grid Protections Against IoT Demand Attacks

Bing Huang
The University of Texas at Austin
binghuang@utexas.edu

Alvaro A. Cardenas
University of California, Santa Cruz
alvaro.cardenas@ucsc.edu

Ross Baldick
The University of Texas at Austin
baldick@ece.utexas.edu

Abstract

Devices with high energy consumption such as air conditioners, water heaters, and electric vehicles are increasingly becoming Internet-connected. This new connectivity exposes the control of new electric loads to attackers in what is known as Manipulation of demand via IoT (MadIoT) attacks. In this paper we investigate the impact of MadIoT attacks on power transmission grids. Our analysis leverages a novel cascading outage analysis tool that focuses on how the protection equipment in the power grid as well as how protection algorithms react to cascading events that can lead to a power blackout. In particular, we apply our tool to a large North American regional transmission interconnection system consisting of

work proposed a novel form of attack called Manipulation of demand via IoT (MadIoT) [47], and showed that if an attacker compromised hundreds of thousands of high-energy IoT devices (such as water heaters and air conditioners), the attacker could cause various problems to the power grid, including (i) frequency instabilities, (ii) line failures, and (iii) increased operating costs. These attacks paint a dire picture of the security of the power grid as they show that a 30% increase in demand can trip all the generators in the US Western interconnection causing a complete system blackout, and a 1% increase of demand in the Polish grid results in a cascade of 263 transmission line failures, affecting 86% of the load in the system.

(left) Soltan, Saleh, Prateek Mittal, and H. Vincent Poor. "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid." In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 15-32. 2018.
(right) Huang, Bing, Alvaro A. Cardenas, and Ross Baldick. "Not everything is dark and gloomy: Power grid protections against IoT demand attacks." In 28th {USENIX} Security Symposium ({USENIX} Security 19), pp. 1115-1132. 2019.

Status Quo in Threat Evaluation - MadIoT

BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid

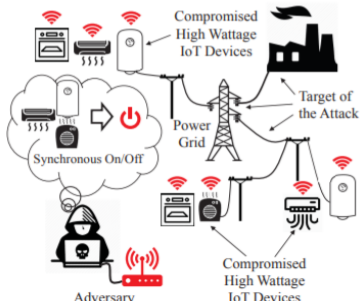
Saleh Soltan
Department of Electrical Engineering
Princeton University
ssoltan@princeton.edu

Prateek Mittal
Department of Electrical Engineering
Princeton University
pmittal@princeton.edu

H. Vincent Poor
Department of Electrical Engineering
Princeton University
poor@princeton.edu

Abstract

We demonstrate that an Internet of Things (IoT) botnet of high wattage devices–such as air conditioners and heaters–gives a unique ability to adversaries to launch large-scale coordinated attacks on the power grid. In particular, we reveal a new class of potential attacks on power grids called the Manipulation of demand via IoT (MadIoT) attacks that can leverage such a botnet in order to manipulate the power demand in the grid. We study five variations of the MadIoT attacks and evaluate their effectiveness via state-of-the-art simulators on real-world power grid models. These simulation results demonstrate that the MadIoT attacks can result in local power outages and in the worst cases, large-scale blackouts. Moreover,



Not Everything is Dark and Gloomy:
Power Grid Protections Against IoT Demand Attacks

Bing Huang
The University of Texas at Austin
binghuang@utexas.edu

Alvaro A. Cardenas
University of California, Santa Cruz
alvaro.cardenas@ucsc.edu

Ross Baldick
The University of Texas at Austin
baldick@ece.utexas.edu

Abstract

Devices with high energy consumption such as air conditioners, water heaters, and electric vehicles are increasingly becoming Internet-connected. This new connectivity exposes the control of new electric loads to attackers in what is known as Manipulation of demand via IoT (MadIoT) attacks. In this paper we investigate the impact of MadIoT attacks on power transmission grids. Our analysis leverages a novel cascading outage analysis tool that focuses on how the protection equipment in the power grid as well as how protection algorithms react to cascading events that can lead to a power blackout. In particular, we apply our tool to a large North American regional transmission interconnection system consisting of work proposed a novel form of attack called Manipulation of demand via IoT (MadIoT) [47], and showed that if an attacker compromised hundreds of thousands of high-energy IoT devices (such as water heaters and air conditioners), the attacker could cause various problems to the power grid, including (i) frequency instabilities, (ii) line failures, and (iii) increased operating costs. These attacks paint a dire picture of the security of the power grid as they show that a 30% increase in demand can trip all the generators in the US Western interconnection causing a complete system blackout, and a 1% increase of demand in the Polish grid results in a cascade of 263 transmission line failures, affecting 86% of the load in the system.

Widely varying perceptions on whether comprised IoT devices can cause cascading failure in the electric grid!

(left) Soltan, Saleh, Prateek Mittal, and H. Vincent Poor. "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid." In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 15-32. 2018.
(right) Huang, Bing, Alvaro A. Cardenas, and Ross Baldick. "Not everything is dark and gloomy: Power grid protections against IoT demand attacks." In 28th {USENIX} Security Symposium ({USENIX} Security 19), pp. 1115-1132. 2019.

Status Quo in Threat Evaluation - FDIA

False Data Injection Attacks against State Estimation in Electric Power Grids

Yao Liu, Peng Ning
Department of Computer Science
North Carolina State University
Emails: {yliu20, pning}@ncsu.edu

Michael K. Reiter
Department of Computer Science
University of North Carolina, Chapel Hill
Email: reiter@cs.unc.edu

***Abstract*—A power grid is a complex system connecting electric power generators to consumers through power transmission and distribution networks across a large geographical area. System monitoring is necessary to ensure the reliable operation of power grids, and *state estimation* is used in system monitoring to best estimate the power grid state through analysis of meter measurements and power system models. Various techniques have been developed to detect and identify bad measurements, including the *interacting bad measurements* introduced by *arbitrary, non-random* causes. At first glance, it seems that these techniques can also defeat malicious measurements injected by attackers, since such malicious measurements can be considered as interacting bad measurements.**

In this paper, we present a new class of attacks, called *false data injection attacks*, against state estimation in electric power grids. We show that an attacker can take advantage of the configuration of a power system to launch such attacks to successfully bypass the existing techniques for bad measurement detection. Moreover, we look at two realistic attack scenarios, in which the attacker is either constrained to some specific meters (due to the physical protection of the meters), or limited in the resources required to compromise meters. We show that the attacker can systematically

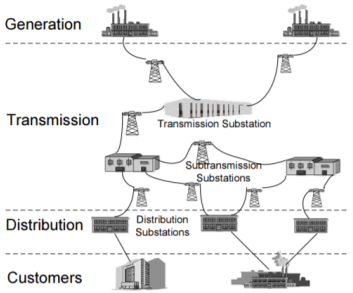


Fig. 1. A power grid connecting power plants to customers via power transmission and distribution networks (revised from [2])

- Grid operators and researchers[1]:
  - "We do not believe false data injection is a real threat to grid security"
  - "Realistic grid settings must be considered to evaluate the efficacy of this attack"

Liu, Yao, Peng Ning, and Michael K. Reiter. "False data injection attacks against state estimation in electric power grids." ACM Transactions on Information and System Security (TISSEC) 14, no. 1 (2011): 1-33.
1. Paraphrased based on discussions with the U.S. grid operators and other researchers in the domain.

Status Quo: Challenges with Threat Evaluation

- Cyber threats are not studied on realistic grid setups
  - E.g., Did the MadIoT evaluation consider an N-1 secure grid setup?

B. Singer, A. Pandey, S. Li, L. Bauer, C. Miller, L. Pileggi, and V. Sekar, "Shedding light on inconsistencies in grid cybersecurity: Disconnects and recommendations," IEEE Security and Privacy, 2023. (To appear)

Status Quo: Challenges with Threat Evaluation

- Cyber threats are not studied on realistic grid setups
  - E.g., Did the MadIoT evaluation consider an N-1 secure grid setup?
- Threat space is not comprehensively explored
  - E.g., Did it consider both hot weather and extreme winter scenarios?

B. Singer, A. Pandey, S. Li, L. Bauer, C. Miller, L. Pileggi, and V. Sekar, "Shedding light on inconsistencies in grid cybersecurity: Disconnects and recommendations," IEEE Security and Privacy, 2023. (To appear)

Status Quo: Challenges with Threat Evaluation

- Cyber threats are not studied on realistic grid setups
  - E.g., Did the MadIoT evaluation consider an N-1 secure grid setup?
- Threat space is not comprehensively explored
  - E.g., Did it consider both hot weather and extreme winter scenarios?
- Simulation tools do not capture the true processes of the grid
  - E.g., Did MadIoT evaluation consider droop, AGC control, and fast reserves?
  - E.g., Did FDIA construction assume ACSE in control rooms?

B. Singer, A. Pandey, S. Li, L. Bauer, C. Miller, L. Pileggi, and V. Sekar, "Shedding light on inconsistencies in grid cybersecurity: Disconnects and recommendations," IEEE Security and Privacy, 2023. (To appear)

Status Quo: Challenges with Threat Evaluation

- Evaluation of cyber threats on unrealistic grid setups
- Threat space is not comprehensively explored
- Simulation tools do not capture the true processes of the grid

Lack of a single universal framework where all grid threats can be analyzed sufficiently accurately!

B. Singer, A. Pandey, S. Li, L. Bauer, C. Miller, L. Pileggi, and V. Sekar, "Shedding light on inconsistencies in grid cybersecurity: Disconnects and recommendations," IEEE Security and Privacy, 2023. (To appear)

Inspiration from NERC Standards?

- NERC standard TPL-001-4[1] tells system planners how to analyze future systems under a wide range of contingencies:

> "Establish Transmission system planning performance requirements within the planning horizon to develop a Bulk Electric System (BES) that will operate reliably over a broad spectrum of System conditions and following a wide range of probable Contingencies."

1. "NERC Reliability Standards for the Bulk Electric Systems of North America, Standard TPL-001-4 - Transmission System Planning Performance Requirements"

Inspiration from NERC Standards?

- NERC standard TPL-001-4[1] tells system planners how to analyze future systems under a wide range of contingencies:

> "Establish Transmission system planning performance requirements within the planning horizon to develop a Bulk Electric System (BES) that will operate reliably over a broad spectrum of System conditions and following a wide range of probable Contingencies."

- Would a similar methodology help with standardizing the evaluation of cyber threats?

1. "NERC Reliability Standards for the Bulk Electric Systems of North America, Standard TPL-001-4 - Transmission System Planning Performance Requirements"

Threat - Definition

Threat = {Goals, Capabilities}

Cause cascading grid outage

Control 80% of the total IoT devices, synchronously

B. Singer, A. Pandey, S. Li, L. Bauer, C. Miller, L. Pileggi, and V. Sekar, "Shedding light on inconsistencies in grid cybersecurity: Disconnects and recommendations," IEEE Security and Privacy, 2023. (To appear)

Attack - Definition

Attack = {Goals, Capabilities, Strategy}

Cause cascading grid outage

Control 80% of the total IoT devices, synchronously

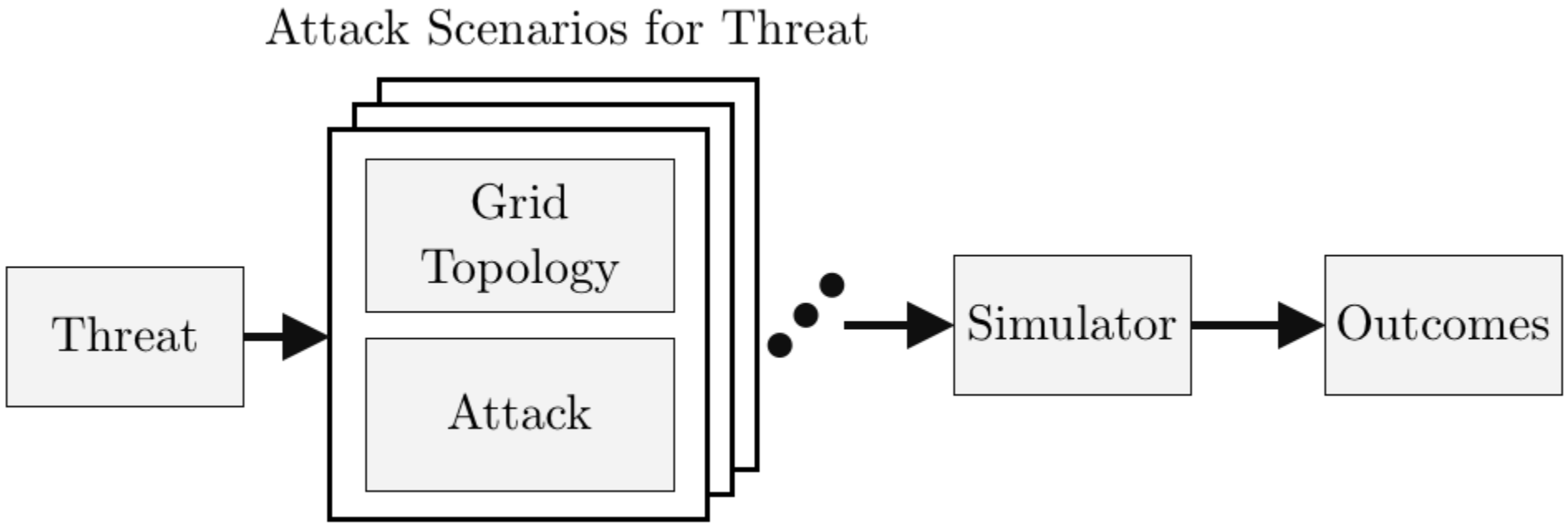
Crank up the power of all IoT-controlled devices

Attack Scenario - Definition

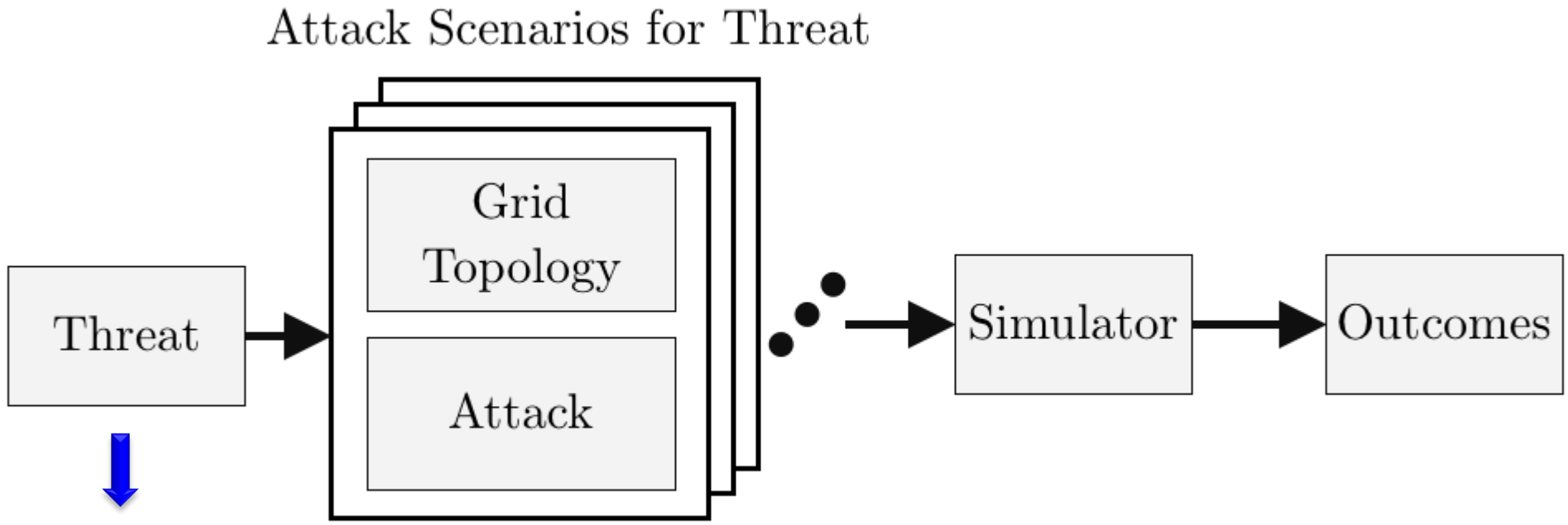
Attack Scenario = {Attack, Grid Topology}

Texas grid on a hot summer day!

A Methodology for Threat Evaluation

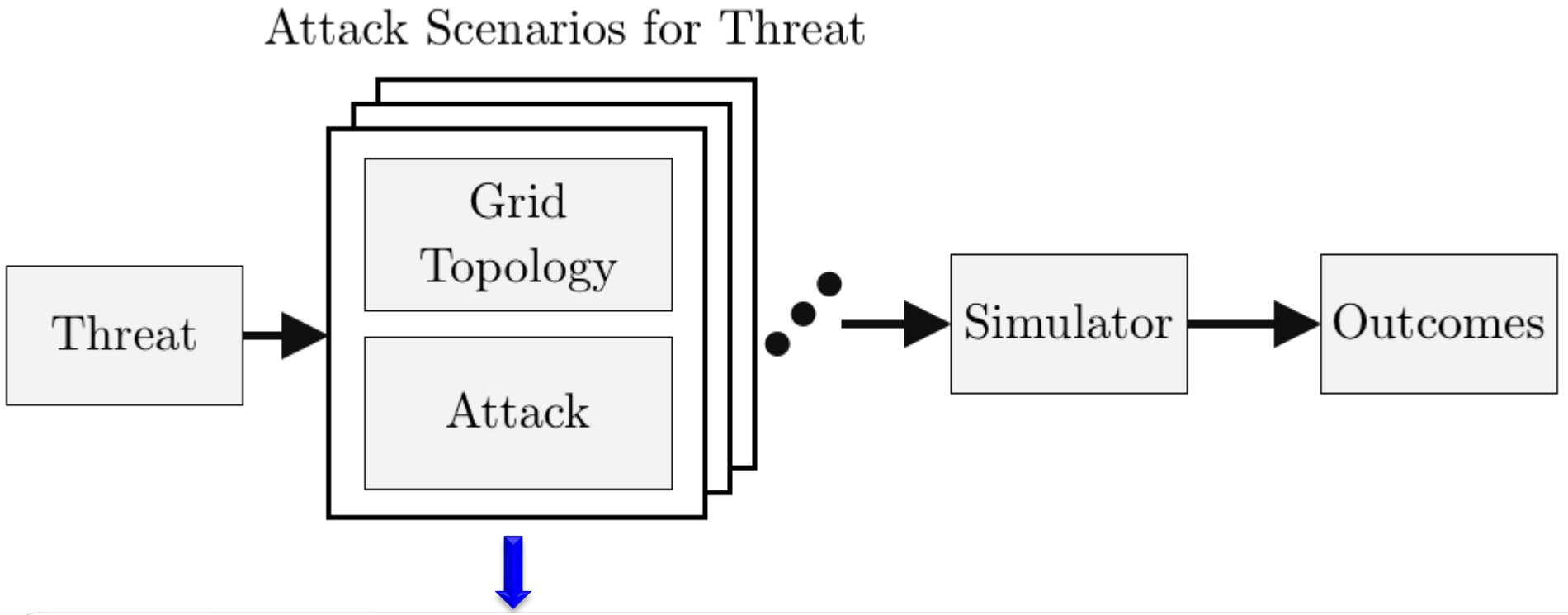


A Methodology for Threat Evaluation



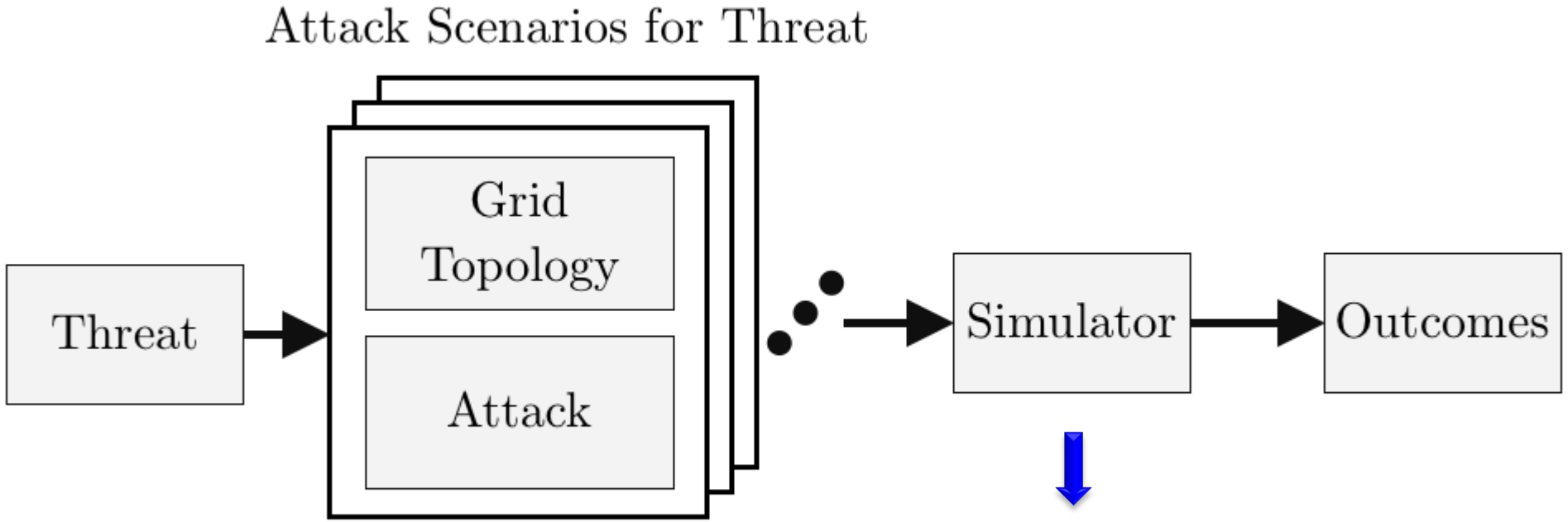
Define threat space for a given grid setting

A Methodology for Threat Evaluation



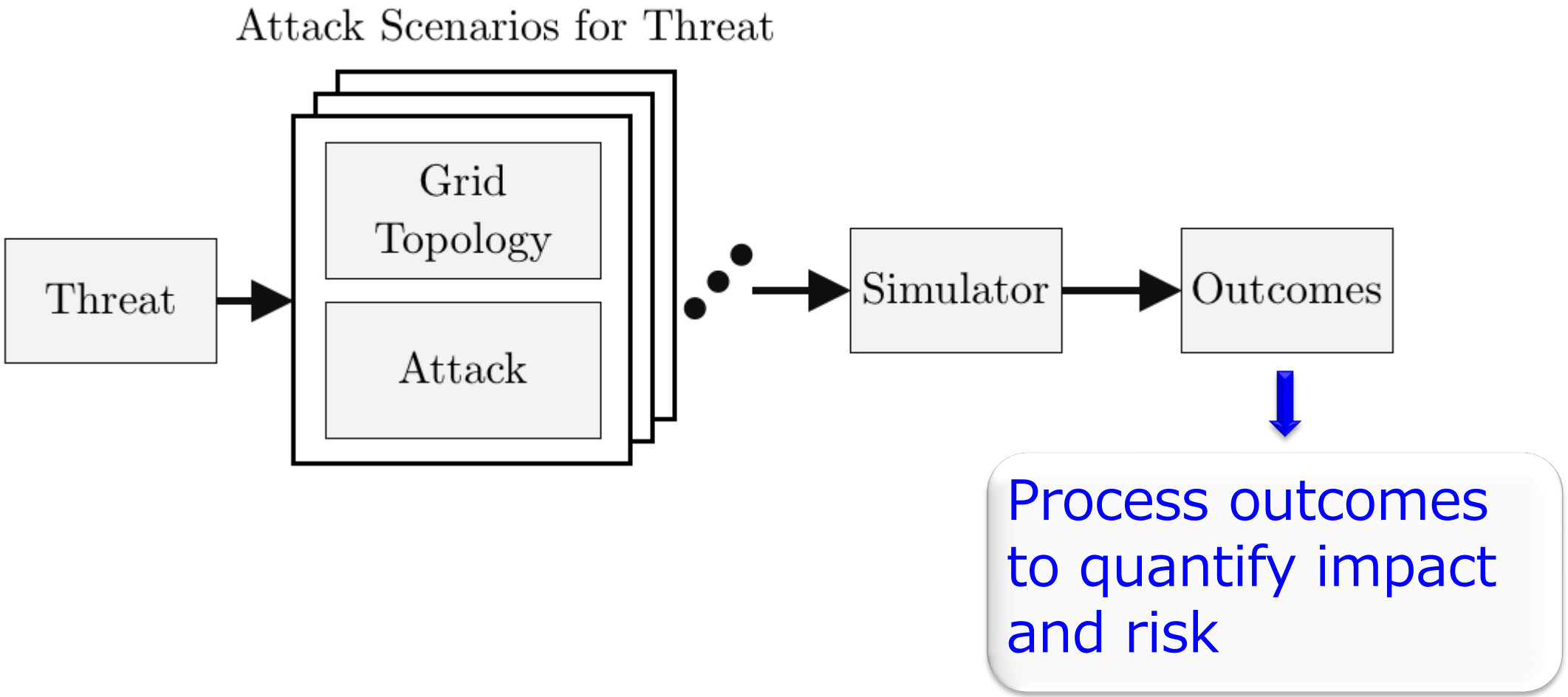
→ Consider realistic attack scenarios (e.g., N-1 secure)
→ Cover boundary attack scenarios

A Methodology for Threat Evaluation

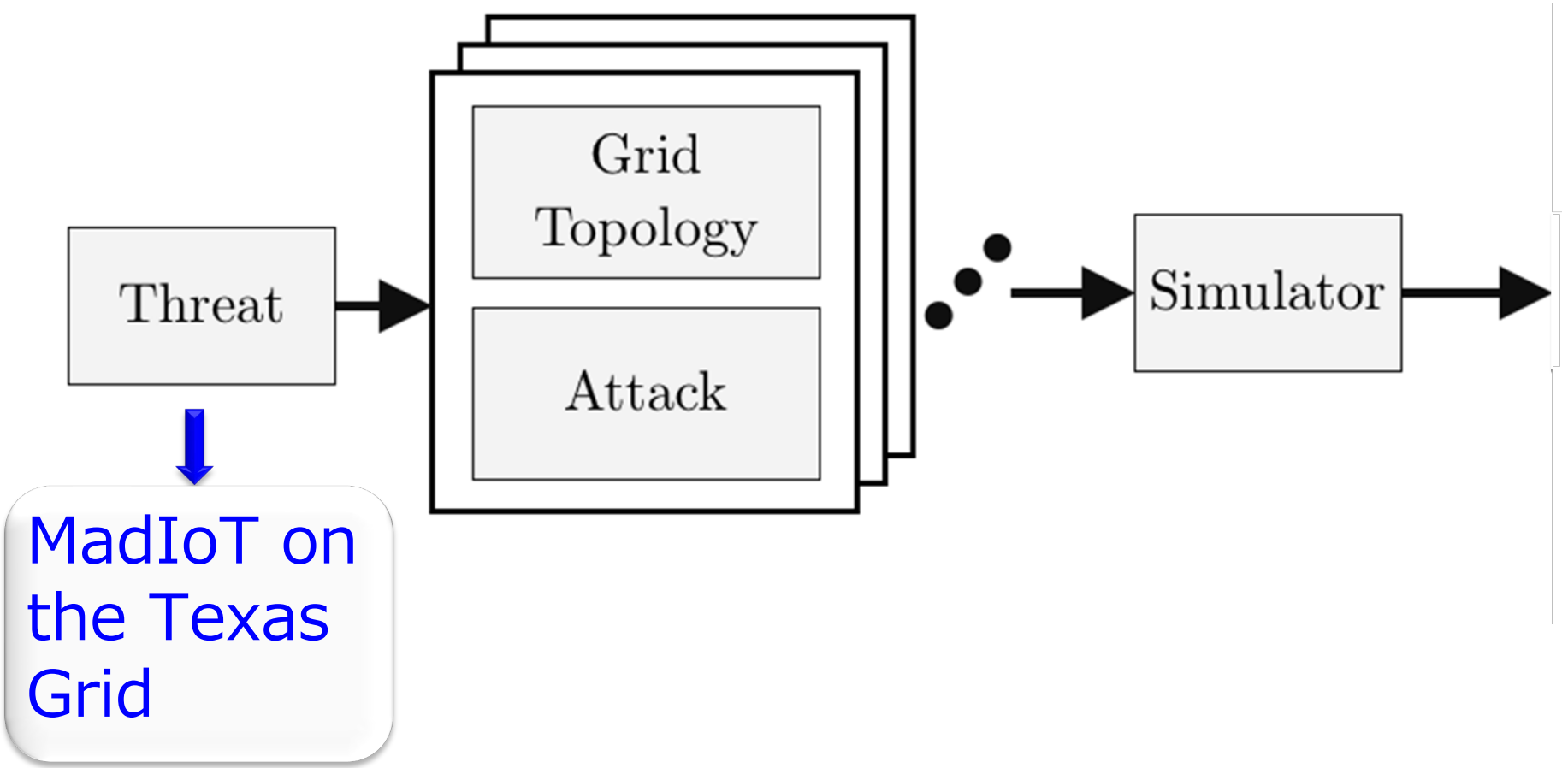


Use a simulator that mimics the real world *sufficiently* well

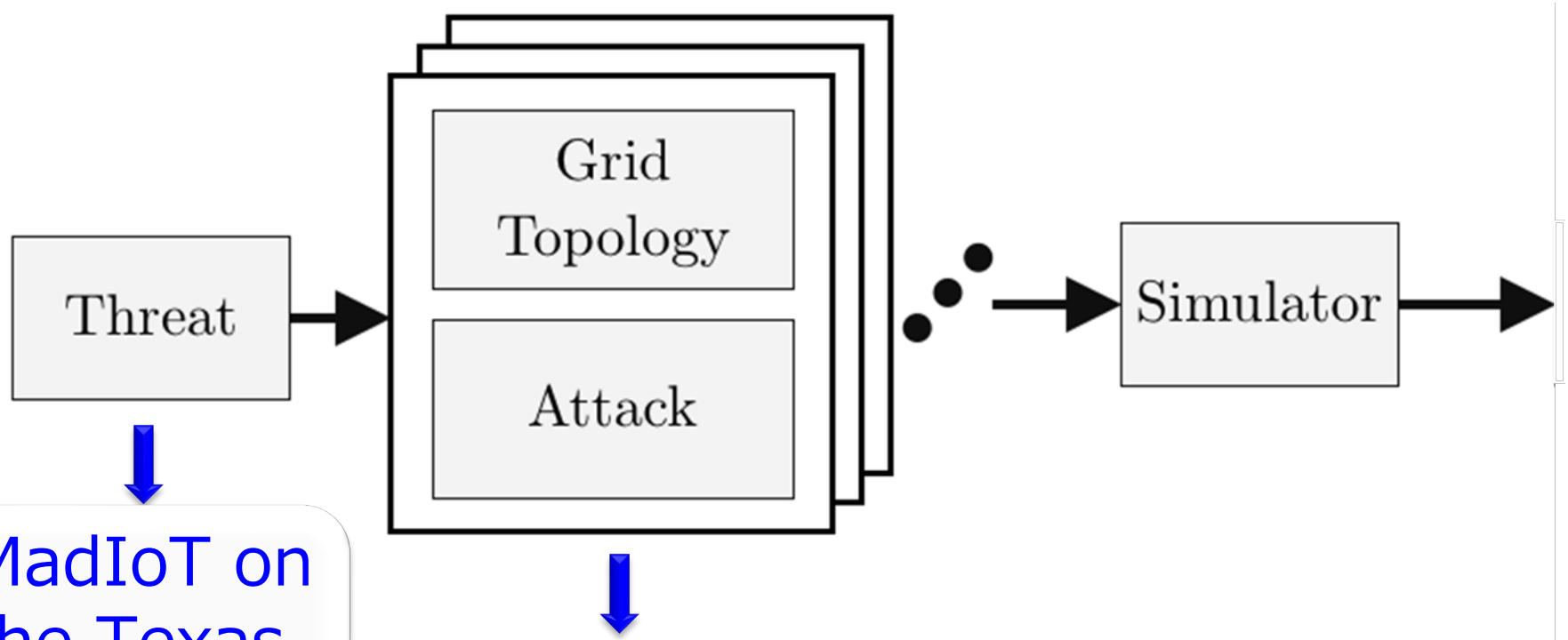
A Methodology for Threat Evaluation



MadIoT Example



MadIoT Example

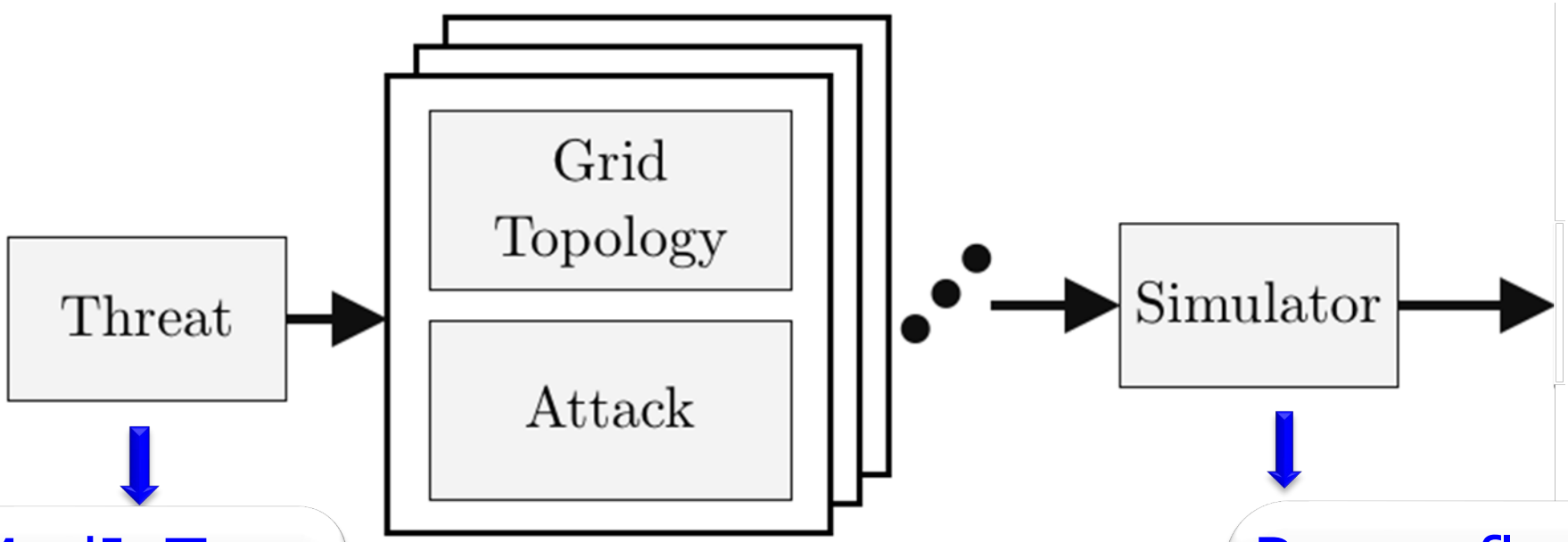


MadIoT on the Texas Grid

→Grid Topology: <Hot summer, Extreme winter>

→Attack: Ramp up power for 0 → ~1M IoT devices

MadIoT Example

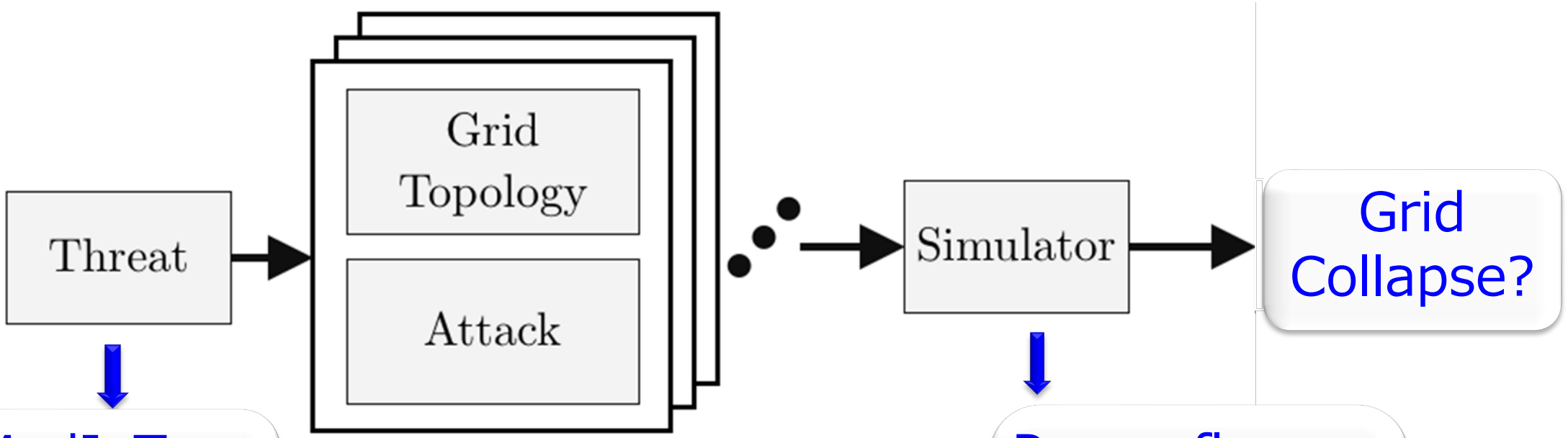


MadIoT on the Syn. Texas Grid

→Grid Topology: <Hot summer, Extreme winter>
→Attack: Ramp up power for 0 → ~1M IoT devices

Power flow + droop, AGC, and fast reserves

MadIoT Example

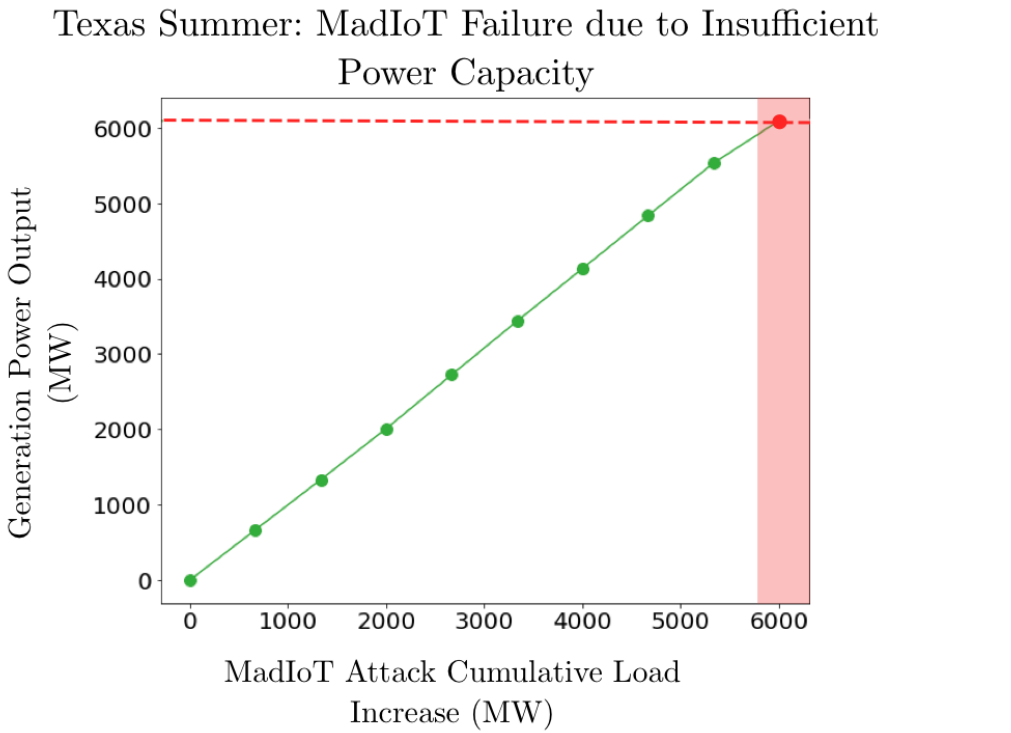


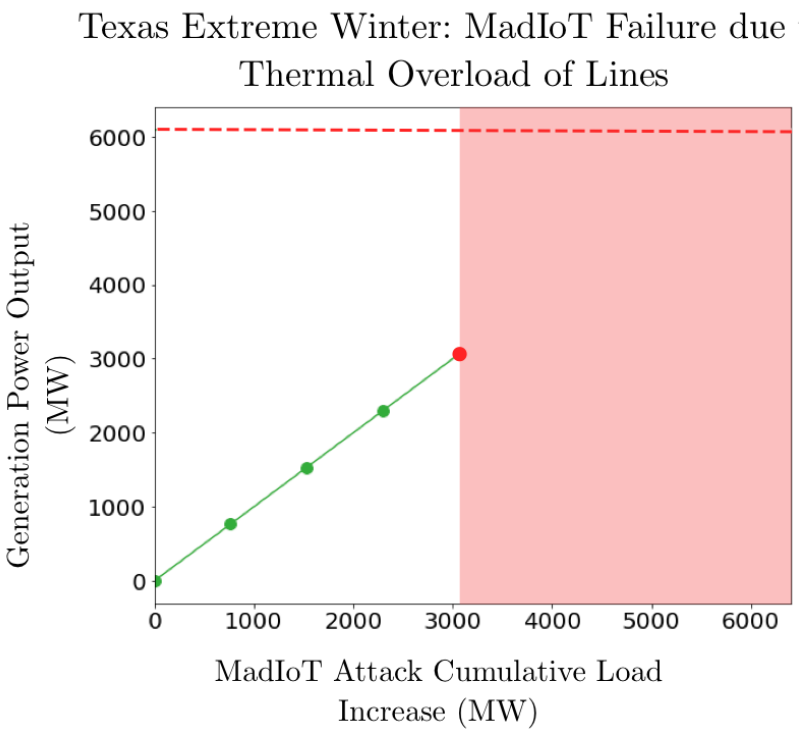
MadIoT on the Syn. Texas Grid

→Grid Topology: <Hot summer, Extreme winter>
→Attack: Ramp up power for 0 → ~1M IoT devices

Power flow + droop, AGC, and fast reserves

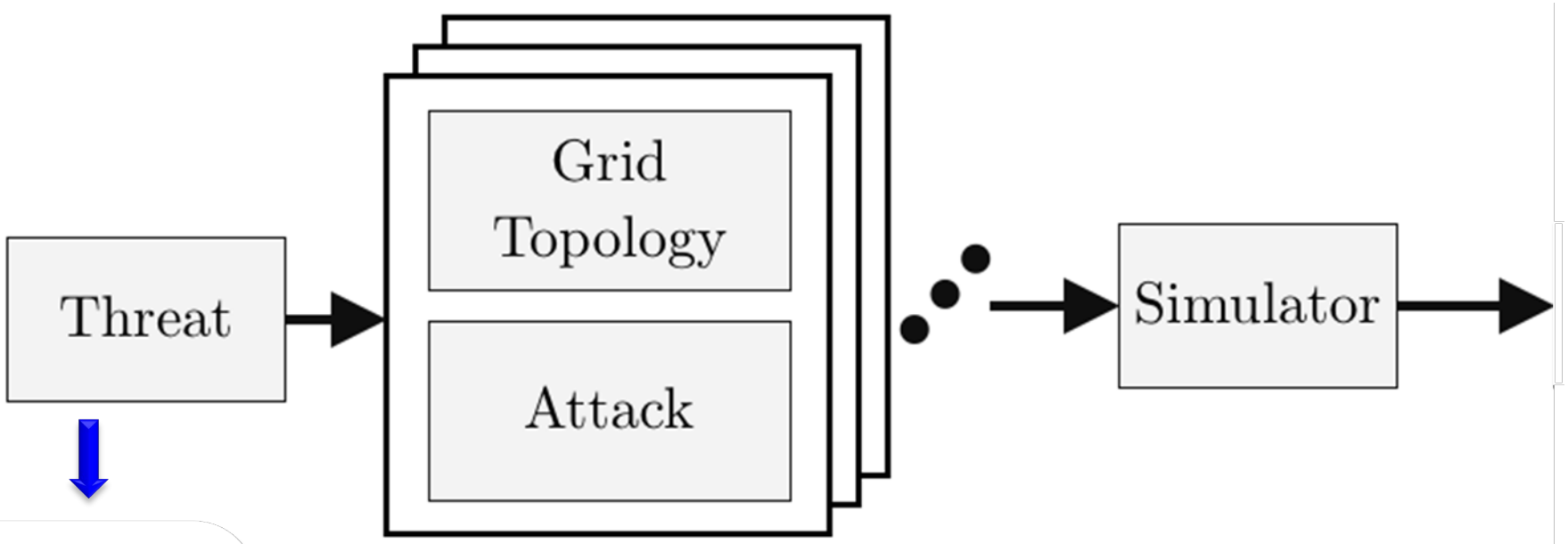
MadIoT Example (cont.)





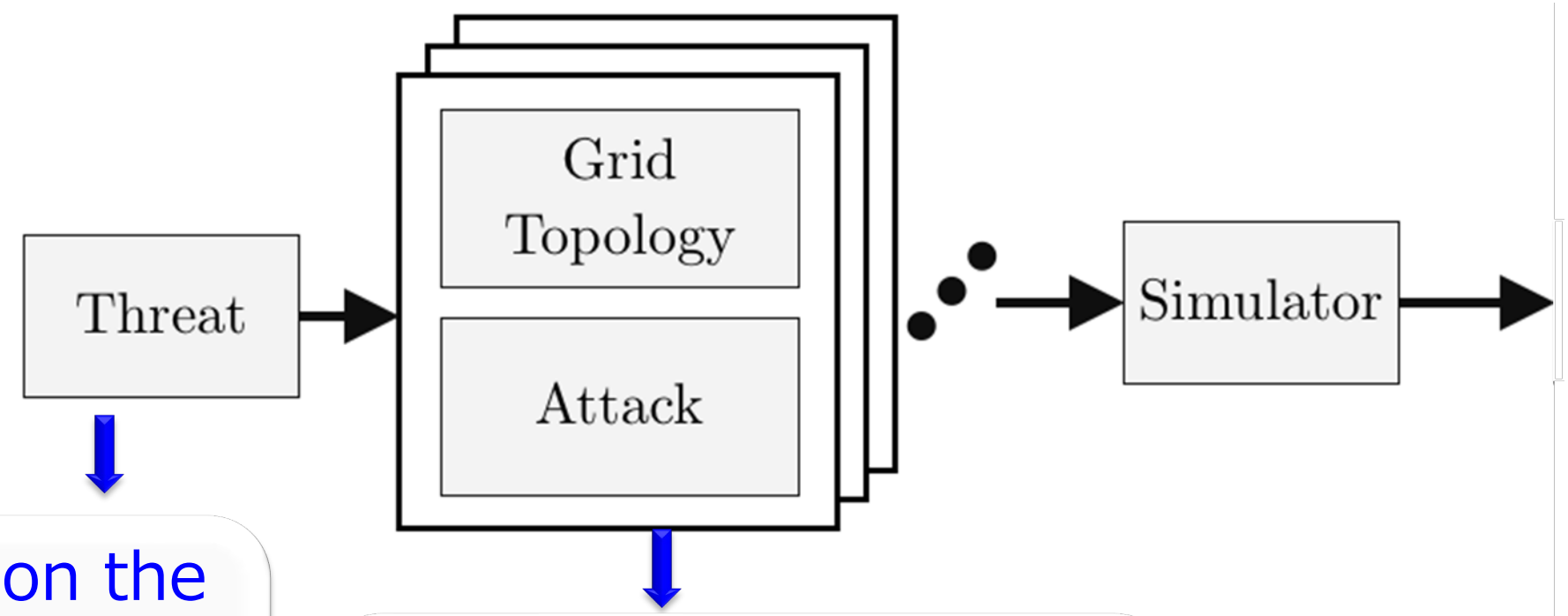
During the extreme winter scenario, model (syn. Texas network) predicts that synchronously turning on ~4% of the total load can cause a system failure.

FDIA Example



FDIA on the South Carolina Grid Setting

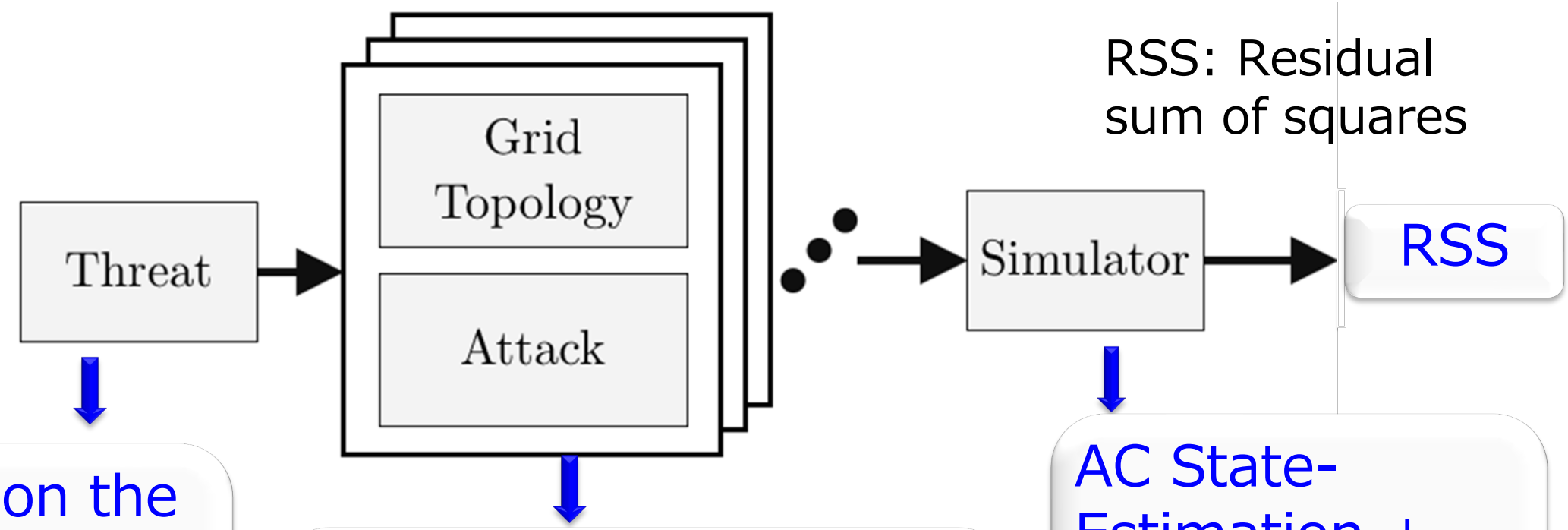
FDIA Example



FDIA on the Syn. South Carolina Grid

→Grid Topology: <normal grid setting, noisy meas.>
→Attack: Spoof a subset of grid measurements with system knowledge **K**

FDIA Example



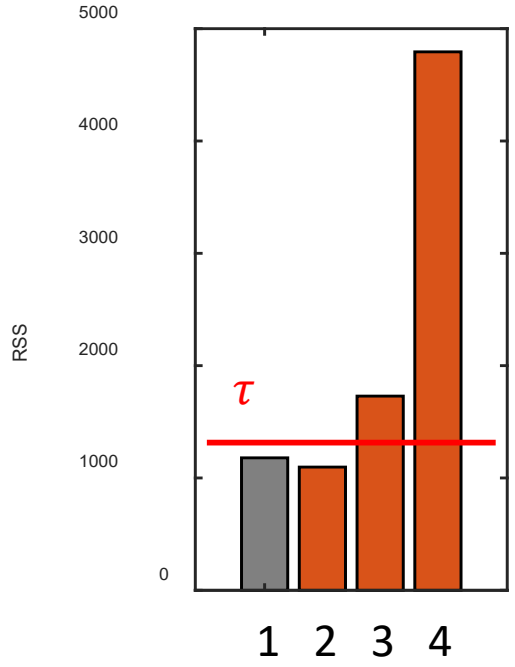
FDIA on the Syn. South Carolina Grid

→Grid Topology: <normal grid setting, noisy meas.>
→Attack: Spoof a subset of grid measurements with system knowledge **K**

AC State-Estimation + Bad-data Detection

FDIA Example (cont.)

- Ran 4 scenarios with varying system knowledge **K**
  - Key takeaway: the efficacy of the attack is dependent of attacker's knowledge of grid state



1 – No attack
2 – FDIA, (ideal) Attacker has perfect system knowledge
3 – FDIA, imperfect topology knowledge $K_{topo} = 50$
4 – FDIA, imperfect network parameter knowledge $K_{\sigma} = 0.02$

→ τ is the critical value of Chi-square distribution
→ With $RSS > \tau$, bad-data detection raises an alarm

RSS: Residual sum of squares
(also called the J-value)

DYNWATCH: Physics-driven Data Mining Technique for Anomaly Detection

Carnegie Mellon University
Electrical & Computer Engineering

Data Processing in High-voltage Grids

Source: ISO-New England

- Data processing in control rooms
  - AC State-Estimation (ACSE)
  - Topology Estimation (TE)

Data Processing in High-voltage Grids

Source: ISO-New England

- Data processing in control rooms
  - AC State-Estimation (ACSE)
  - Topology Estimation (TE)
- Fundamental in grid operation

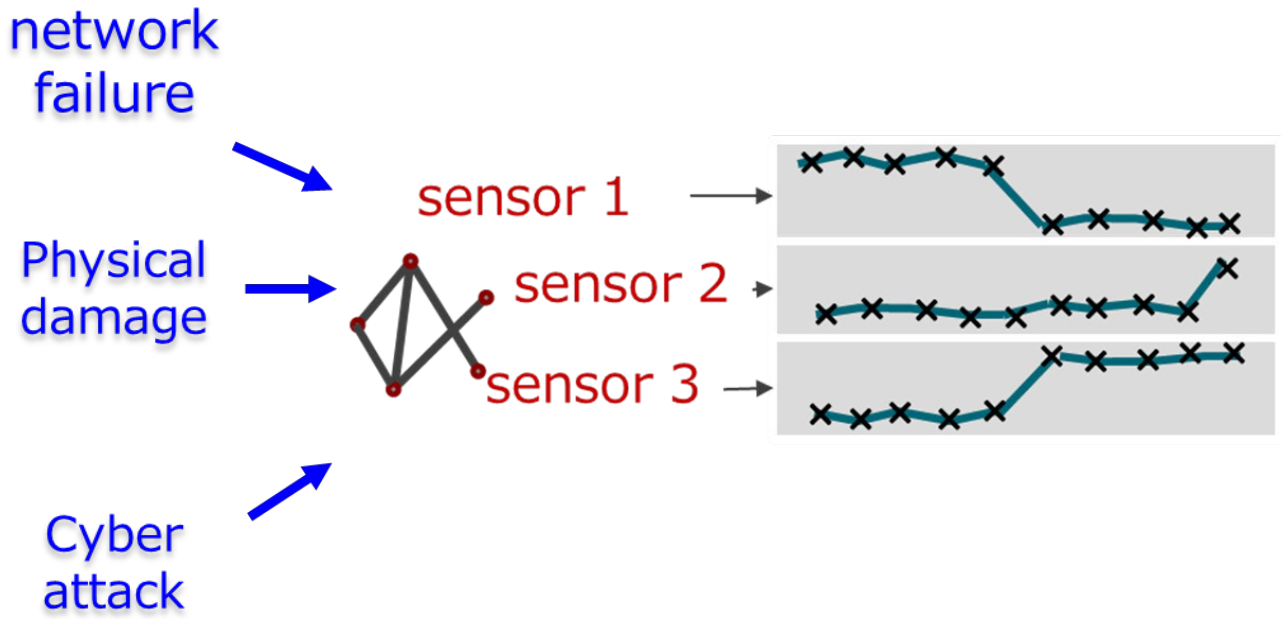
Data Processing in High-voltage Grids

Source: ISO-New England

- Any anomalous data can significantly hamper grid operation

Anomalies in ACSE and TE

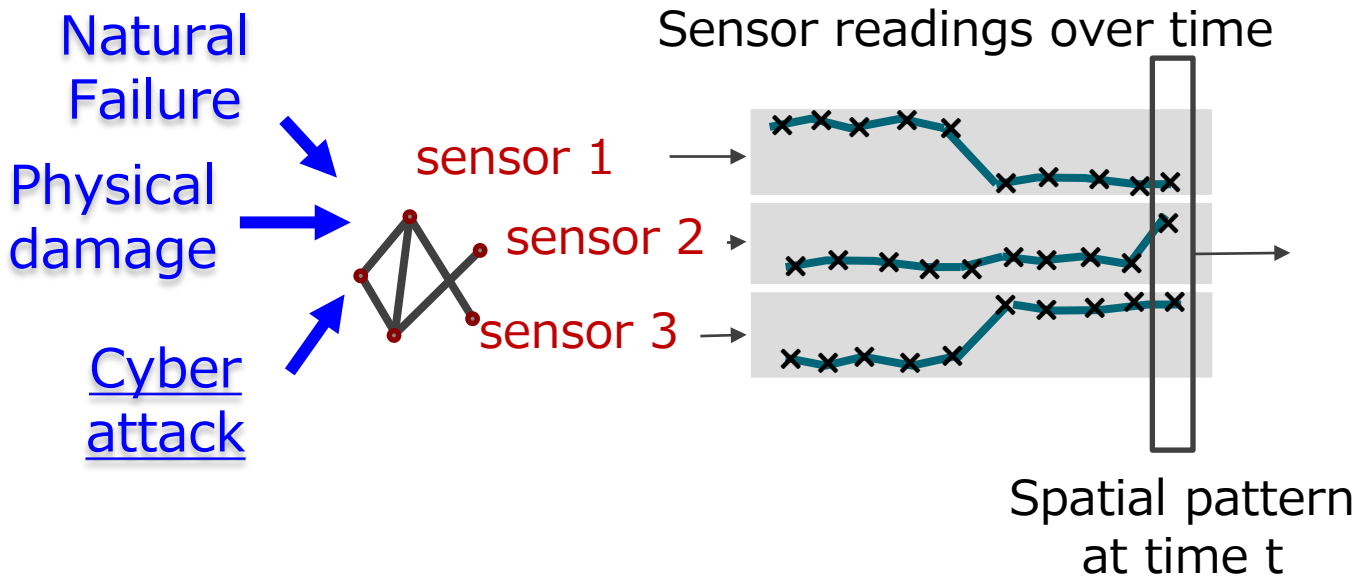
- Many known causes for anomalies in grid data



- Anomalous data must be identified and isolated for reliable operation

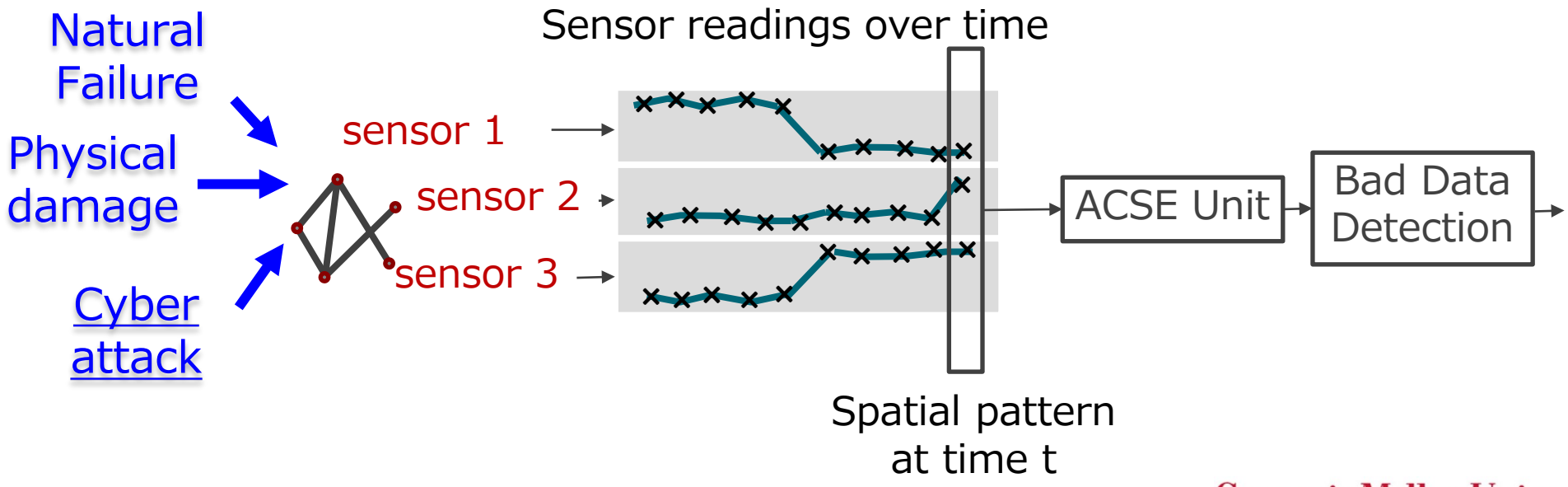
Status Quo for Anomaly Detection: Spatial Pattern

- Setting: spatial features at a single time snapshot



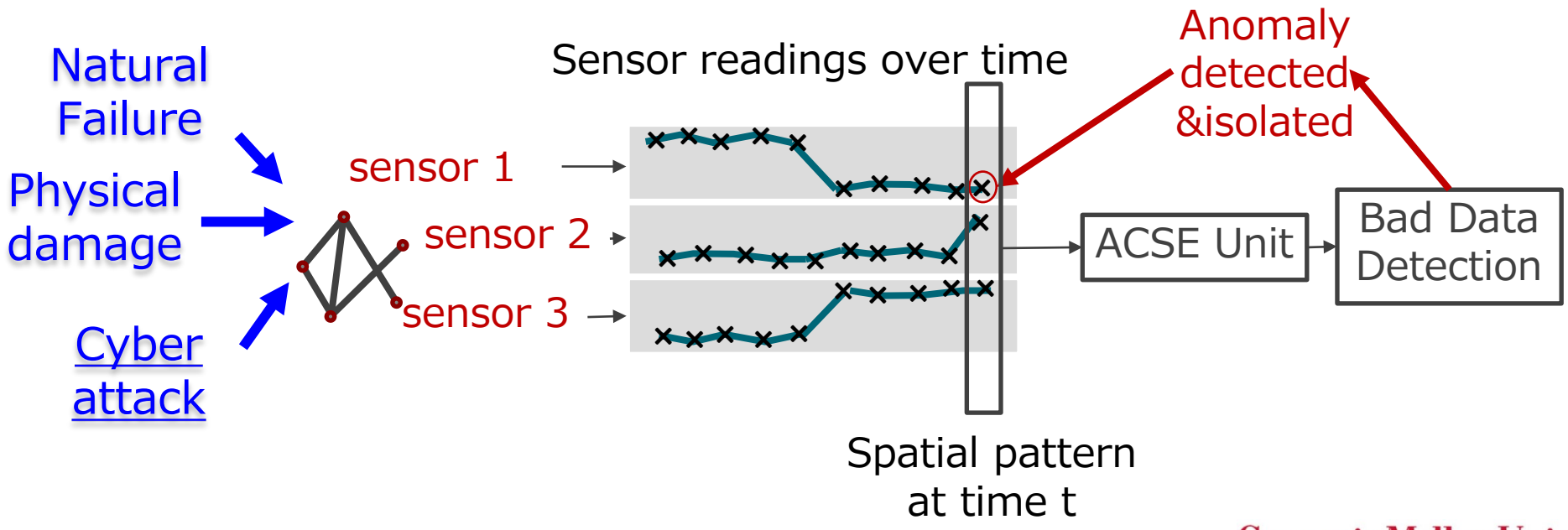
Status Quo for Anomaly Detection: Spatial Pattern

- Setting: spatial features at a single time snapshot
- Measurement data is processed by ACSE and BDD units



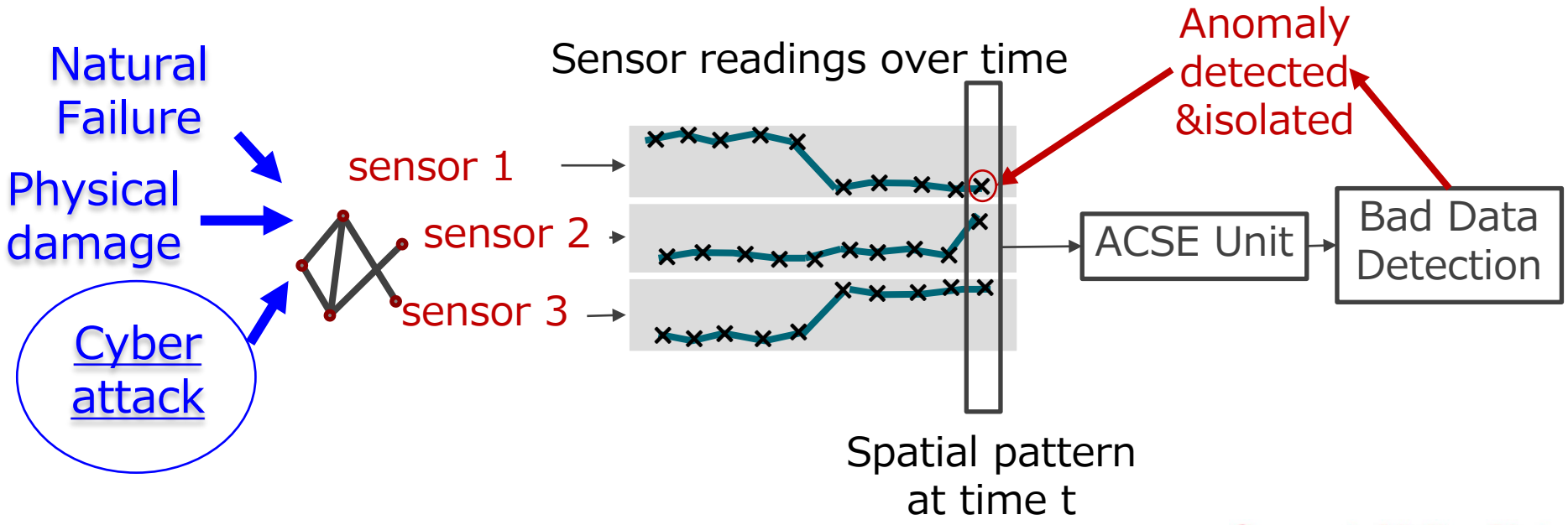
Status Quo for Anomaly Detection: Spatial Pattern

- Setting: spatial features at a single time snapshot
- BDD may trigger an anomaly based on the J-value from ACSE



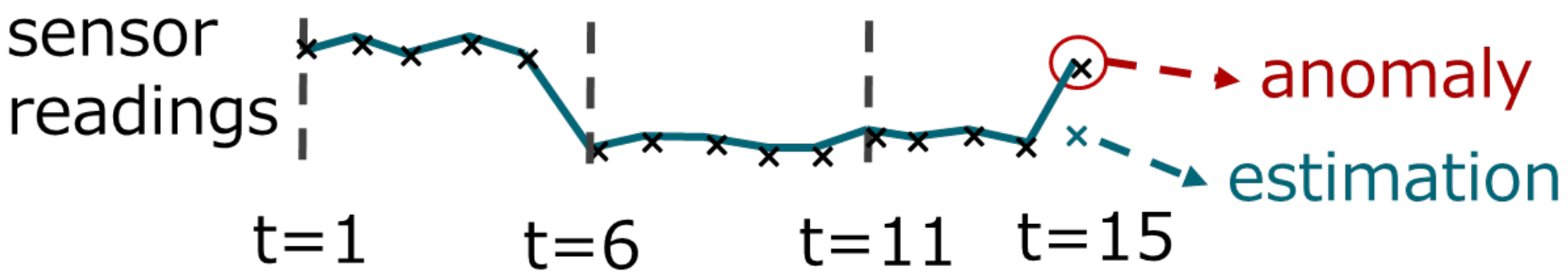
Status Quo for Anomaly Detection: Spatial Pattern

- Setting: spatial features at a single time snapshot
- Some anomalies are not detectable from analysis of spatial patterns alone



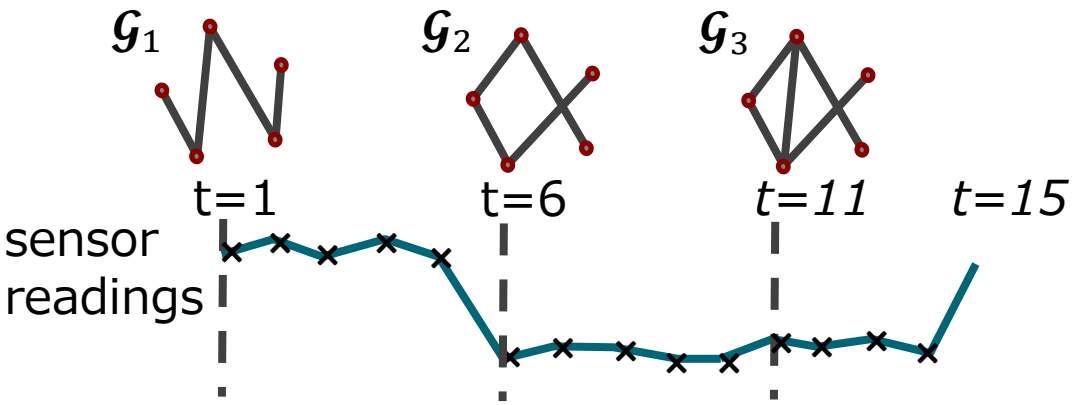
Status Quo for Anomaly Detection: Temporal Pattern

- Given sensor data over time, can we detect an anomalous data-point?
- Time-series processing can detect anomalies that violate temporal statistical consistency (see t = 15)



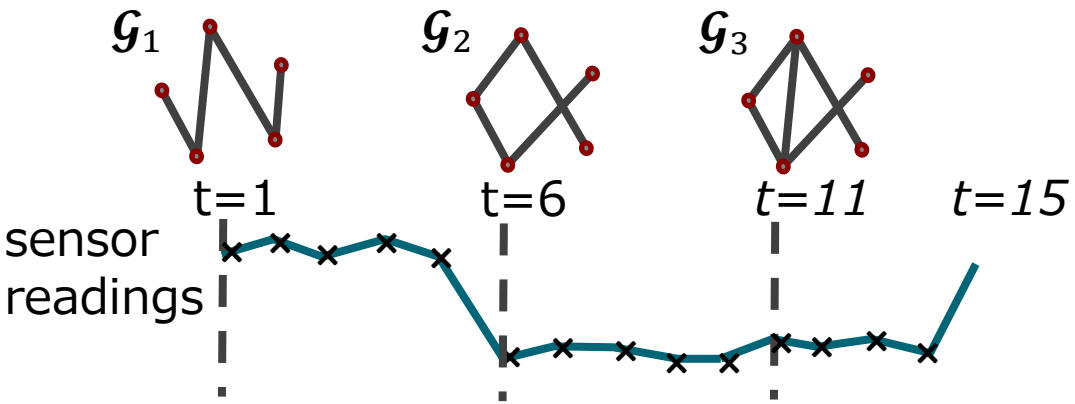
Topology Changes → False Positives

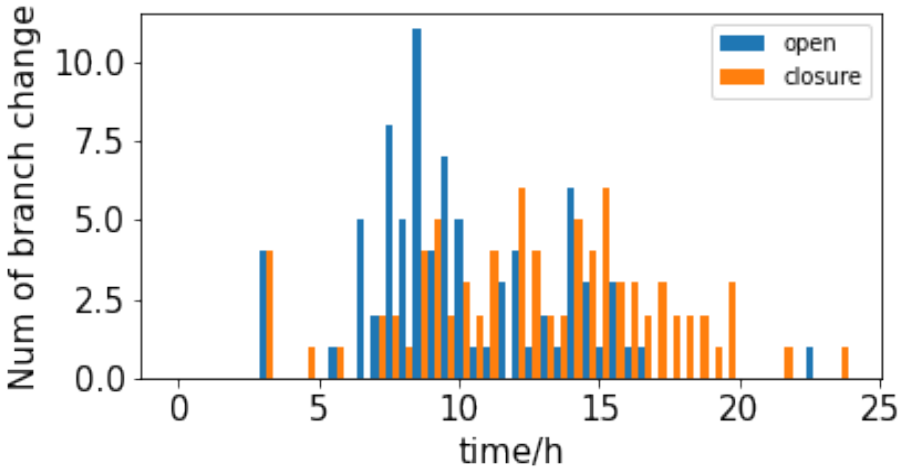
- Power grid topology changes frequently



Topology Changes → False Positives

- Power grid topology changes frequently

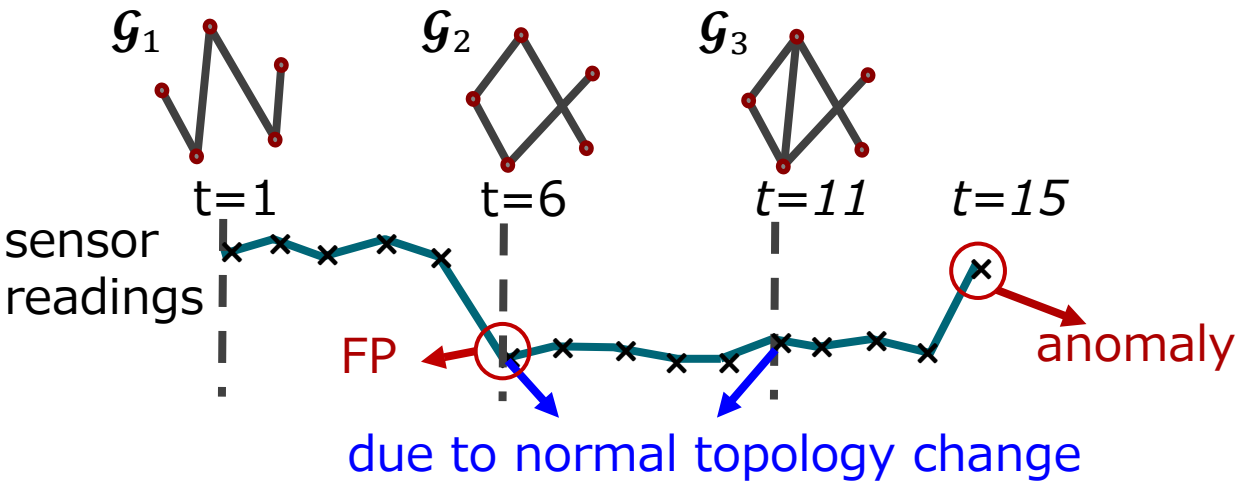


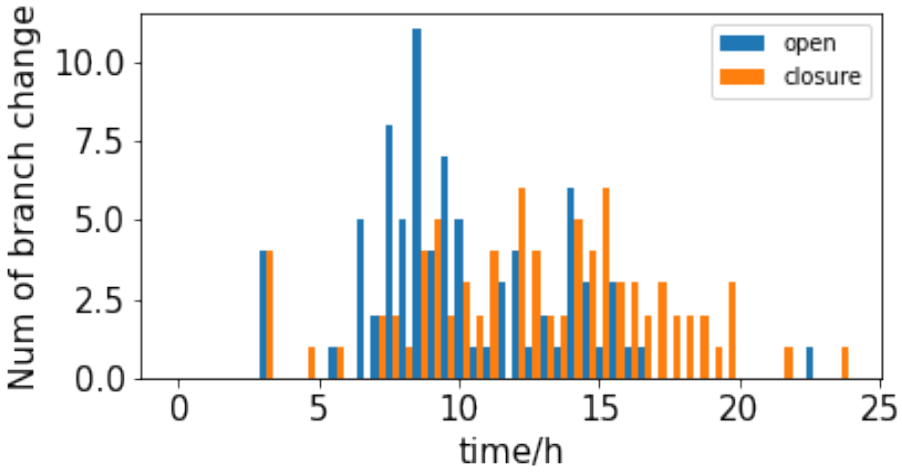


Records from a real utility in the Eastern Interconnection (>17,000 lines)

Topology Changes → False Positives

- Power grid topology changes frequently
  - Classical approaches can result in false positives (FP)

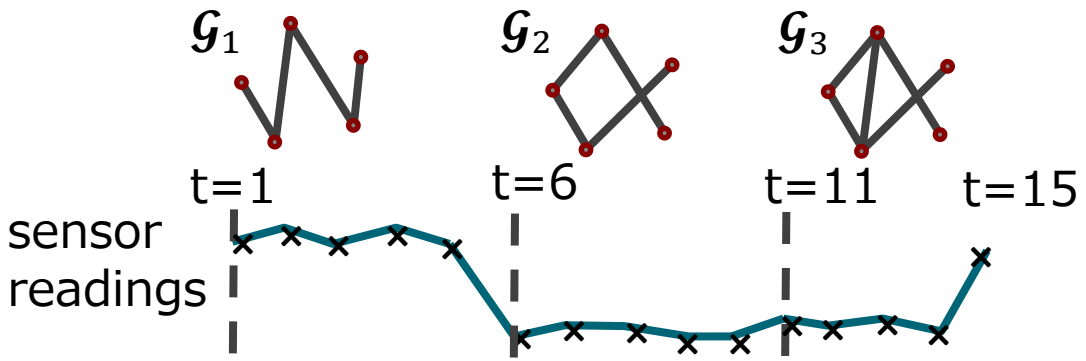




Records from a real utility in the Eastern Interconnection (>17,000 lines)

DYNWATCH: Temporal + Spatial-based Detection

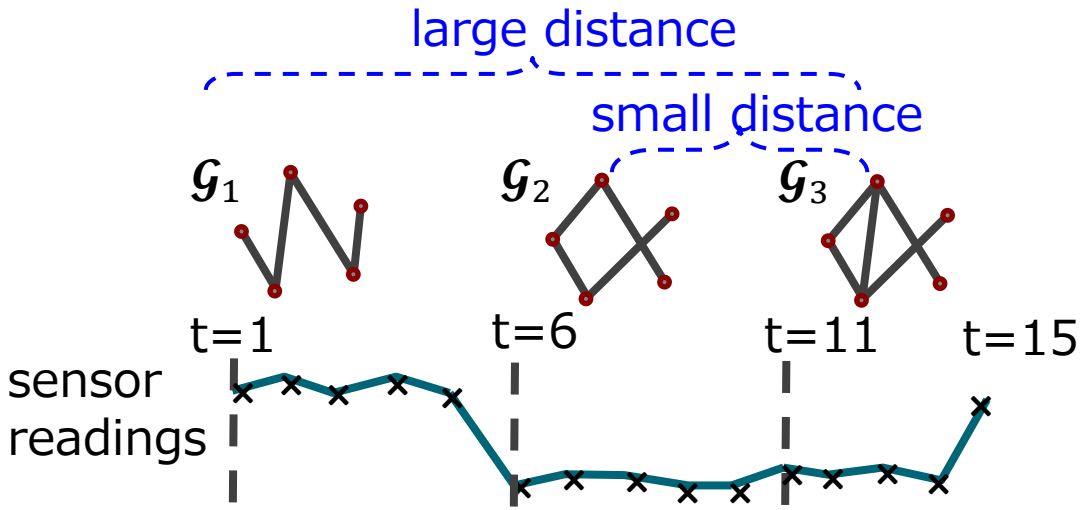
- The proposed approach on time-series data mining considers the impact of topology change
  - The algorithm has 3 steps



S. Li, A. Pandey, B. Hooi, C. Faloutsos and L. Pileggi, "Dynamic Graph-Based Anomaly Detection in the Electrical Grid," in *IEEE Transactions on Power Systems.*

DYNWATCH: Temporal + Spatial-based Detection

- The proposed approach on time-series data mining considers the impact of topology change

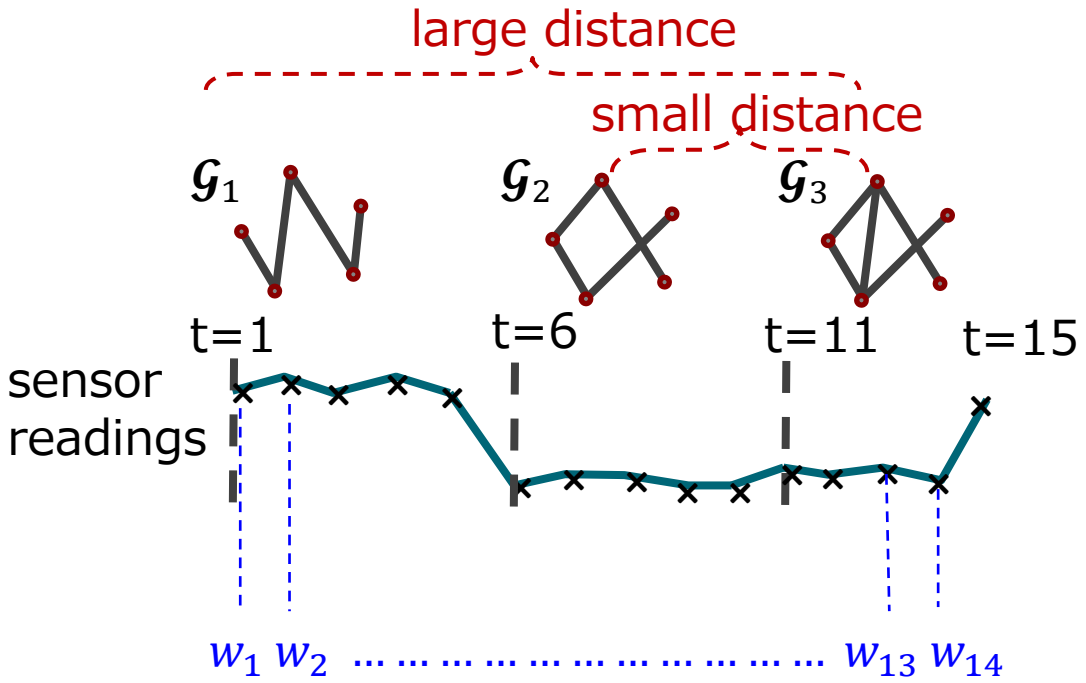


1) Define graph distance

S. Li, A. Pandey, B. Hooi, C. Faloutsos and L. Pileggi, "Dynamic Graph-Based Anomaly Detection in the Electrical Grid," in *IEEE Transactions on Power Systems.*

DYNWATCH: Temporal + Spatial-based Detection

- The proposed approach on time-series data mining considers the impact of topology change

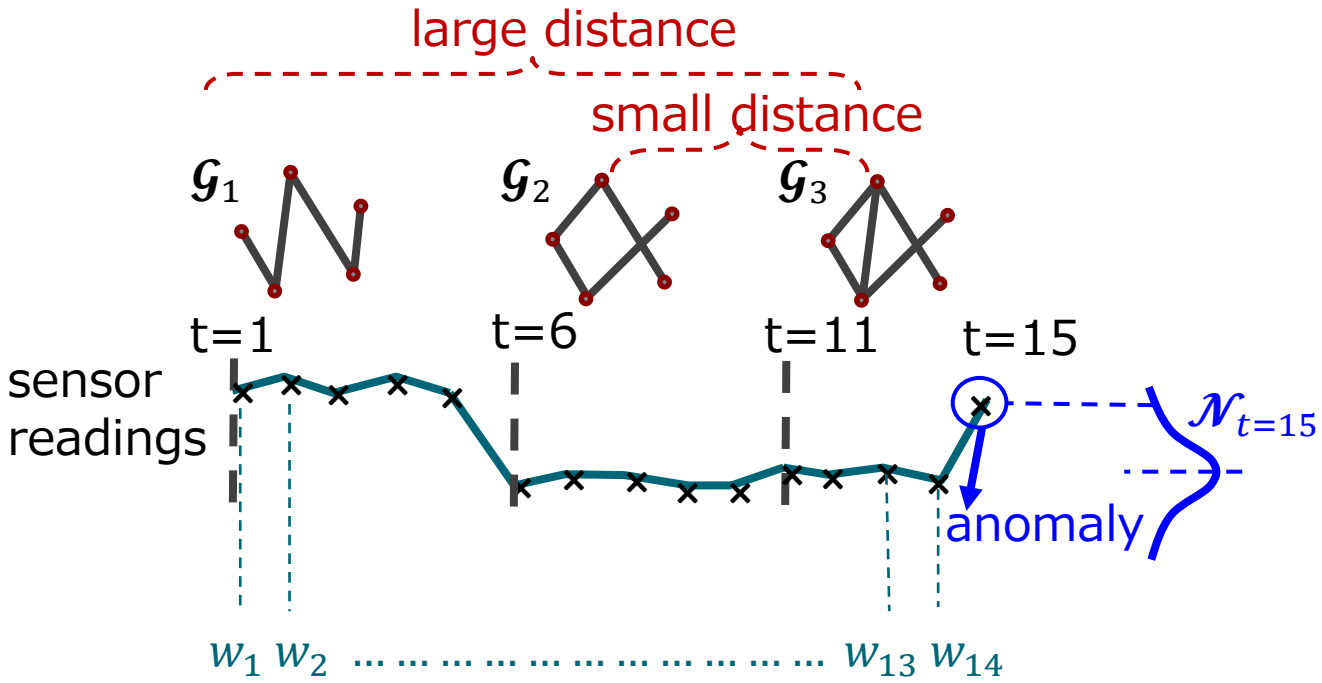


1) Define graph distance
2) Temporal weighting

S. Li, A. Pandey, B. Hooi, C. Faloutsos and L. Pileggi, "Dynamic Graph-Based Anomaly Detection in the Electrical Grid," in *IEEE Transactions on Power Systems.*

DYNWATCH: Temporal + Spatial-based Detection

- The proposed approach on time-series data mining considers the impact of topology change

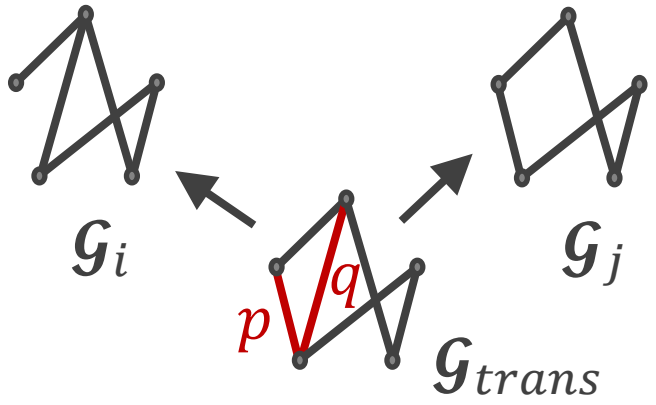


1) Define graph distance
2) Temporal weighting
3) Anomaly detection

S. Li, A. Pandey, B. Hooi, C. Faloutsos and L. Pileggi, "Dynamic Graph-Based Anomaly Detection in the Electrical Grid," in *IEEE Transactions on Power Systems.*

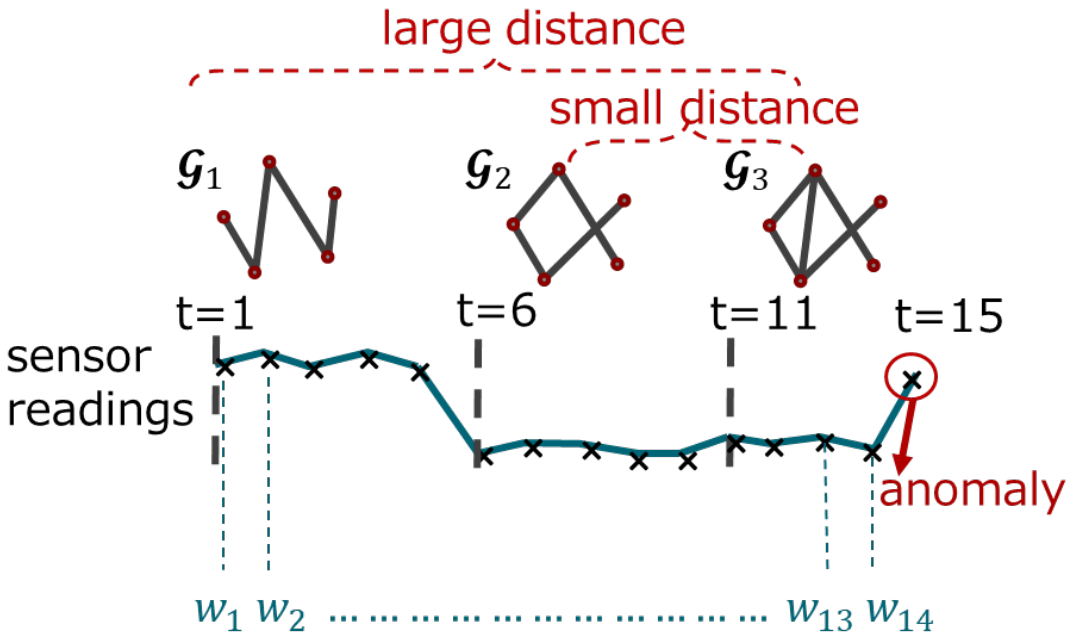
Domain-informed Graph Distance

- The difference between two graphs can be seen as different line outages on the union graph
- Impact of line outage is quantified by line outage distribution factor (LODF)
- Graph distance is the sum of line outage impacts



Temporal Weighting by Bias-variance Trade-off

- Weigh the past sensor data using a bias-variance trade-off
  - Bias: data from very different topology will increase bias
  - Variance: only using data from the most similar topology will increase variance



$$\min_w \sum_t w_t d_t + \frac{c}{2} w^T w$$

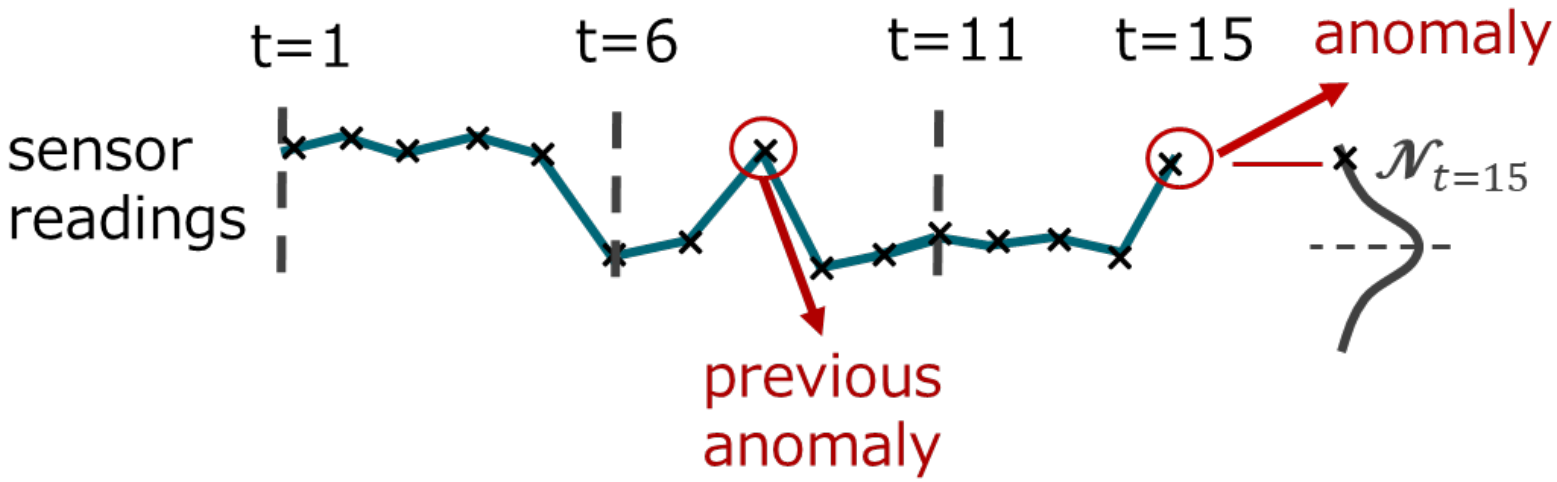
s.t.

$$w_t \geq 0, \forall t;$$

$$\sum_t w_t = 1,$$

Anomaly Score - Idea

- Learn a distribution of normal behavior while ignoring previous anomalous data
  - Median and IQR are more robust statistics



Anomaly Score - Construction

- Anomaly score measures the deviation from distribution center

For sensor s at time t:

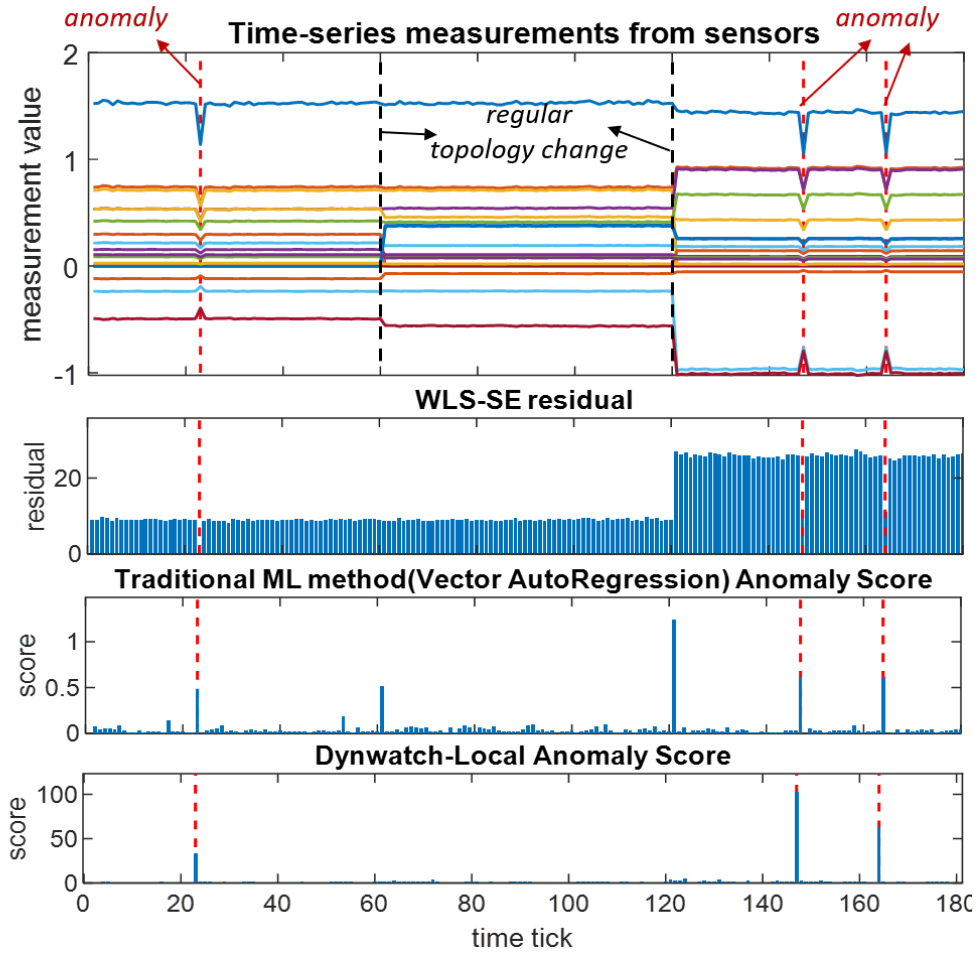
$$a_s(t) = \frac{x(t) - \mu(t)}{IQR(t)}$$

Final score for time t:

$$A(t) = \max_s a_s(t)$$

$\mu(\mathrm{t})$ = Weighted Median; $IQR(\mathrm{t})$ = Weighted IQR

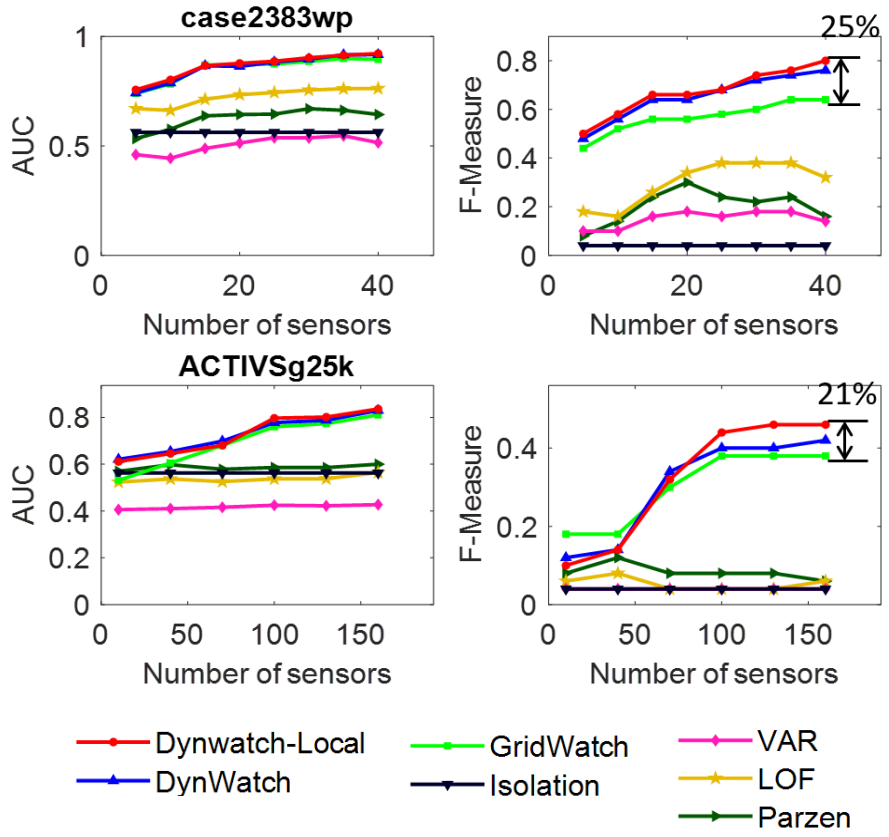
DYNWATCH has Lower False Positives

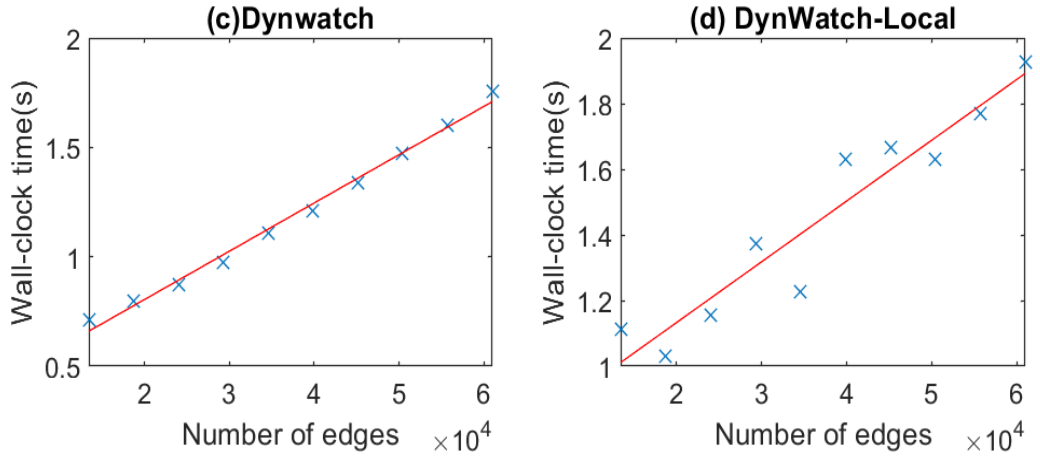


- False data injection attack (FDIA) is a coordinated attack on grid measurements
- With a constructed FDIA attack, only DYNWATCH is shown to detect all anomalies without False Positives (FP)

High Performance with Scalability

- DYNWATCH outperforms other classical approaches based on AUC and F-measure





The proposed method scales (almost) linearly with grid size.

Warm Starter for Cyberthreats-based Contingencies

Carnegie Mellon University
Electrical & Computer Engineering

Intro: Contingency Analysis

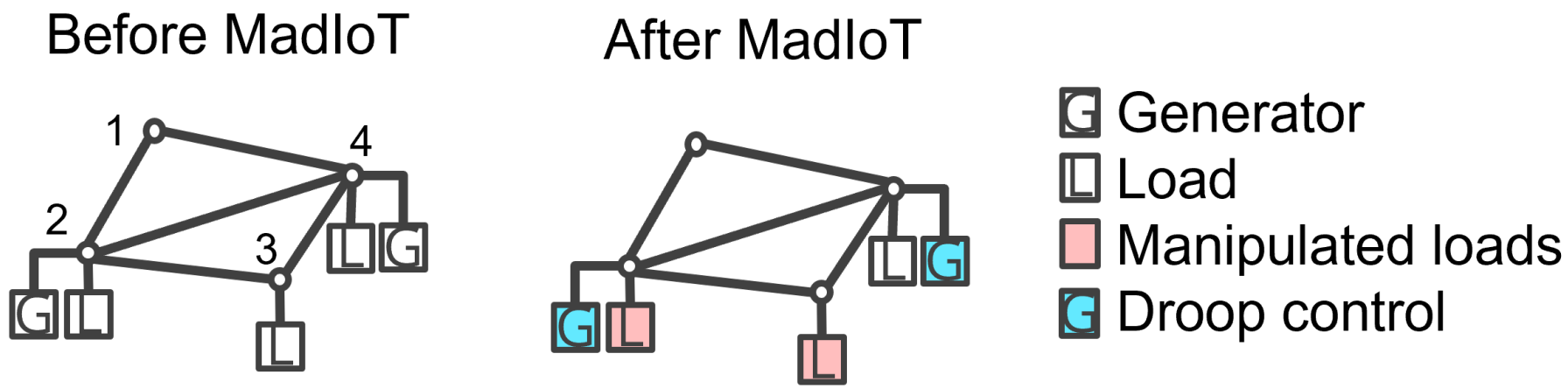
- Contingency analysis (CA) is pivotal for grid reliability
  - Evaluates N-1 security: Loss of any 1 device should not cause grid failure
  - Make necessary adjustments if the grid fails N-1 security

Intro: Contingency Analysis

- Contingency analysis (CA) is pivotal for grid reliability
  - Evaluates N-1 security: Loss of any 1 device should not cause grid failure
  - Make necessary adjustments if the grid fails N-1 security
- CA Requirement: A tool that can solve 10k+ power flow networks within minutes robustly
  - Current tools utilize the pre-contingency solution as the initial condition due to the vicinity to the final solution

Moving beyond N-1 security for Cyber Resiliency

- Many cyberthreats (MadIoT, substation takeover, etc.) represent N-x events
  - Necessitates that we move beyond N-1 to N-x security
  - Current methods for CA may not work



Moving beyond N-1 security for Cyber Resiliency

- Many cyberthreats (MadIoT, substation takeover, etc.) represent N-x events
  - Necessitates that we move beyond N-1 to N-x security
  - Current methods for CA may not work

CA Requirement for cyberthreats: Robust and fast power flow method for evaluating N-x events

A Novel Warm Starter Method

- Unlike N-1 contingency evaluation, the N-x contingency solution is not close to the pre-contingency solution
- Tradeoff between robustness and speed
  - Physics-based tools can be made robust but are slow
  - Pure data-driven methods can be fast but may lack robustness

Li, Shimiao, Amritanshu Pandey, and Larry Pileggi. "GridWarm: Towards Practical Physics-Informed ML Design and Evaluation for Power Grid." *arXiv preprint arXiv:2205.03673* (2022).

A Novel Warm Starter Method

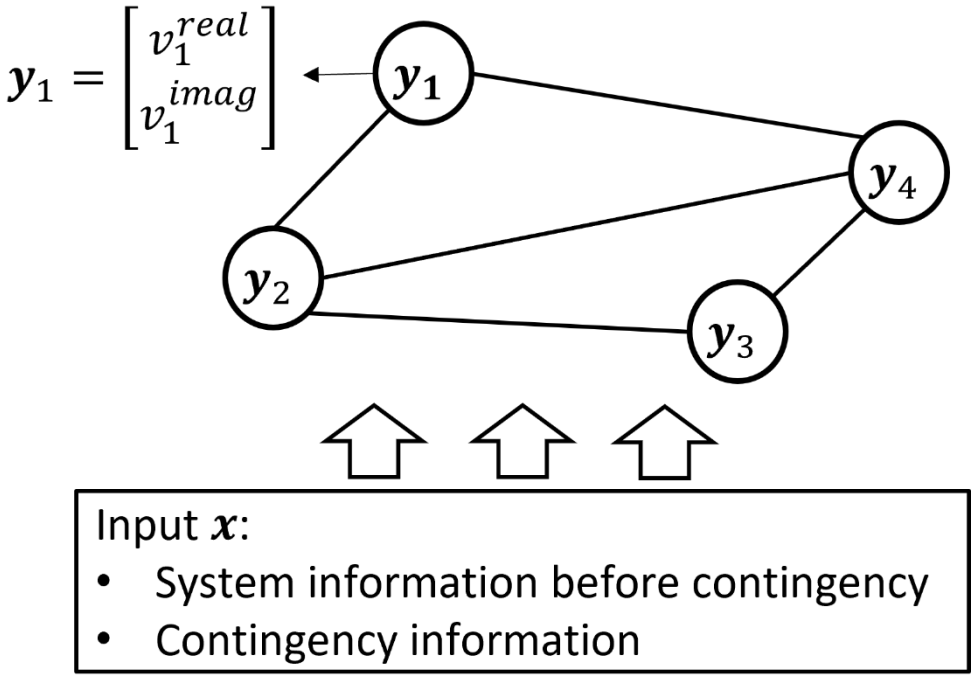
- Unlike N-1 contingency evaluation, the N-x contingency solution is not close to the pre-contingency solution
- Tradeoff between robustness and speed
- A warm starter can combine the benefits of both physics-based and data-driven methods

Use ML to learn good initial conditions for N-x events and feed them into the physics-based solver for fast convergence!

Li, Shimiao, Amritanshu Pandey, and Larry Pileggi. "GridWarm: Towards Practical Physics-Informed ML Design and Evaluation for Power Grid." *arXiv preprint arXiv:2205.03673* (2022).

Graph-based Warm Starter Model

- Power grid is an interconnected graph
  - Voltages at a node are a function of neighboring node voltages

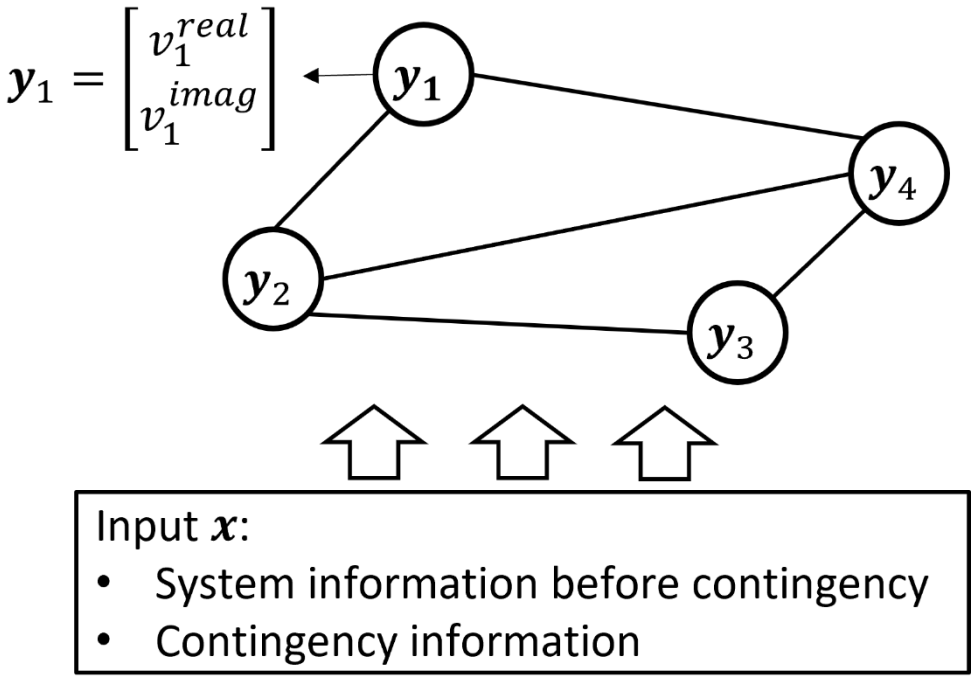


Li, Shimiao, Amritanshu Pandey, and Larry Pileggi. "GridWarm: Towards Practical Physics-Informed ML Design and Evaluation for Power Grid." *arXiv preprint arXiv:2205.03673* (2022).

Graph-based Warm Starter Model

- Power grid is an interconnected graph
- The joint distribution of post-contingency voltages conditioned on contingency & system information can be described via a pairwise Markov Random Field (cMRF) model:

$$P(y|x,\theta) = \frac{1}{Z(\boldsymbol{\theta},\boldsymbol{x})}\prod_{i=1}^{n}\psi_i(\boldsymbol{y_i})\prod_{(s,t)\in \boldsymbol{E}}^{n}\psi_i(\boldsymbol{y_s},\boldsymbol{y_t})$$



Li, Shimiao, Amritanshu Pandey, and Larry Pileggi. "GridWarm: Towards Practical Physics-Informed ML Design and Evaluation for Power Grid." *arXiv preprint arXiv:2205.03673* (2022).

Conditional Gaussian Random Field (cGRF) Model

- Assume the cMRF model to be Gaussian (cGRF)

$$P(y|x,\theta) = \frac{1}{Z(\boldsymbol{\theta},\boldsymbol{x})} \prod_{i=1}^{n} \psi_i(\boldsymbol{y_i}) \prod_{(s,t)\in \boldsymbol{E}}^{n} \psi_i(\boldsymbol{y_s},\boldsymbol{y_t})$$

if $P(y|x,\theta)$ is Gaussian then:

$$\psi_i(\boldsymbol{y_i}) = exp\left(-\frac{1}{2}\boldsymbol{y_i^T}\boldsymbol{\Lambda_i}\ \mathbf{y_i} + \boldsymbol{\eta_i^T}\boldsymbol{y_i}\right)$$

$$\psi_i(\boldsymbol{y_s},\boldsymbol{y_t}) = exp(-\frac{1}{2}\boldsymbol{y_s^T}\boldsymbol{\Lambda_{st}}\mathbf{y_t})$$

Conditional Gaussian Random Field (cGRF) Model

- Assume the cMRF model to be Gaussian (cGRF)
  - Use local neural nets to model parameters in Λ and η
  - Apply domain knowledge to choose the feature space

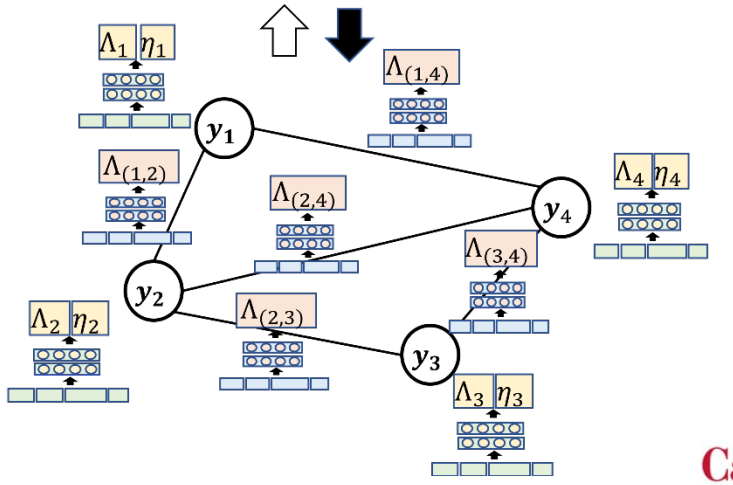
$$P(y|x,\theta) = \frac{1}{Z(\boldsymbol{\theta}, \boldsymbol{x})} \prod_{i=1}^{n} \psi_i(\boldsymbol{y_i}) \prod_{(s,t)\in \boldsymbol{E}}^{n} \psi_i(\boldsymbol{y_s}, \boldsymbol{y_t})$$

if $P(y|x,\theta)$ is Gaussian then:

$$\psi_i(\boldsymbol{y_i}) = exp\left(-\frac{1}{2}\boldsymbol{y_i^T \Lambda_i}\ \mathbf{y_i} + \boldsymbol{\eta_i^T y_i}\right)$$

$$\psi_i(\boldsymbol{y_s}, \boldsymbol{y_t}) = exp(-\frac{1}{2}\boldsymbol{y_s^T \Lambda_{st} y_t})$$

$$\Lambda = \begin{bmatrix} \boldsymbol{\Lambda_1} & \frac{1}{2}\boldsymbol{\Lambda_{(1,2)}} & \mathbf{0} & \frac{1}{2}\boldsymbol{\Lambda_{(1,4)}} \\ \frac{1}{2}\boldsymbol{\Lambda_{(1,2)}^T} & \boldsymbol{\Lambda_2} & \frac{1}{2}\boldsymbol{\Lambda_{2,3}} & \frac{1}{2}\boldsymbol{\Lambda_{(2,4)}} \\ \mathbf{0} & \frac{1}{2}\boldsymbol{\Lambda_{(2,3)}^T} & \boldsymbol{\Lambda_3} & \frac{1}{2}\boldsymbol{\Lambda_{(3,4)}} \\ \frac{2}{2}\boldsymbol{\Lambda_{(1,4)}^T} & \frac{1}{2}\boldsymbol{\Lambda_{(2,4)}^T} & \frac{1}{2}\boldsymbol{\Lambda_{(3,4)}^T} & \boldsymbol{\Lambda_4} \end{bmatrix}, \eta = \begin{bmatrix} \boldsymbol{\eta_1} \\ \boldsymbol{\eta_2} \\ \boldsymbol{\eta_3} \\ \boldsymbol{\eta_4} \end{bmatrix}$$



Conditional Gaussian Random Field (cGRF) Model

- Assume the cMRF model to be Gaussian (cGRF)
  - Use local neural nets to model parameters in Λ and η
  - Apply domain knowledge to choose the feature space

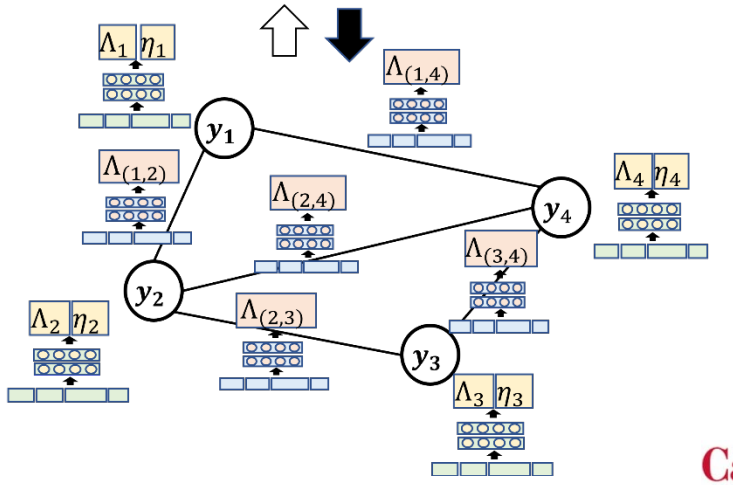
$$P(y|x,\theta) = \frac{1}{Z(\boldsymbol{\theta}, \boldsymbol{x})} \prod_{i=1}^{n} \psi_i(\boldsymbol{y_i}) \prod_{(s,t)\in \boldsymbol{E}}^{n} \psi_i(\boldsymbol{y_s}, \boldsymbol{y_t})$$

if $P(y|x,\theta)$ is Gaussian then:

$$\psi_i(\boldsymbol{y_i}) = exp\left(-\frac{1}{2}\boldsymbol{y_i^T \Lambda_i}\ \mathbf{y_i} + \boldsymbol{\eta_i^T y_i}\right)$$

$$\psi_i(\boldsymbol{y_s}, \boldsymbol{y_t}) = exp(-\frac{1}{2}\boldsymbol{y_s^T \Lambda_{st} y_t})$$

$$\Lambda = \begin{bmatrix} \Lambda_1 & \frac{1}{2}\Lambda_{(1,2)} & 0 & \frac{1}{2}\Lambda_{(1,4)} \\ \frac{1}{2}\Lambda_{(1,2)}^T & \Lambda_2 & \frac{1}{2}\Lambda_{2,3} & \frac{1}{2}\Lambda_{(2,4)} \\ 0 & \frac{1}{2}\Lambda_{(2,3)}^T & \Lambda_3 & \frac{1}{2}\Lambda_{(3,4)} \\ \frac{2}{2}\Lambda_{(1,4)}^T & \frac{1}{2}\Lambda_{(2,4)}^T & \frac{1}{2}\Lambda_{(3,4)}^T & \Lambda_4 \end{bmatrix}, \eta = \begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \\ \eta_4 \end{bmatrix}$$



$$\min_{\theta} -\sum_{j=1}^{N} l(\theta)^j$$

where:

$$l(\theta)^j = P\left(y^j \middle| x^j, \theta^j\right)$$

cGRF Model Inference

- With a trained model parameters $\hat{\theta}_x = [\hat{\theta}_\Lambda, \hat{\theta}_\eta]$, given x_{test}, $\hat{y}_{test}$ can be inferred:

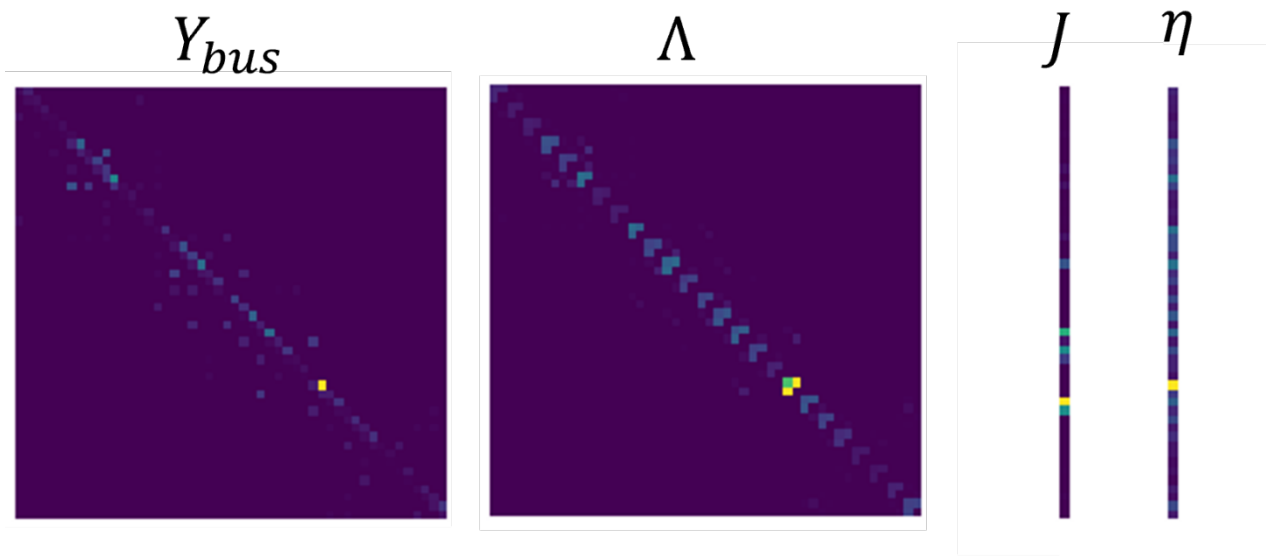
$$\hat{\Lambda} = f_\Lambda\left(x_{test}, \hat{\theta}_\Lambda\right)$$

$$\hat{\eta} = f_\eta\left(x_{test}, \hat{\theta}_\eta\right)$$

$$\hat{\Lambda}\,\hat{y}_{test} = \hat{\eta}$$

Physical Interpretability

- The proposed warm starter provides a linear proxy for grid operation post-contingency
- The linear proxy (Λ, η) is structurally similar to post-contingency admittance matrix at solution Y_{bus}, J

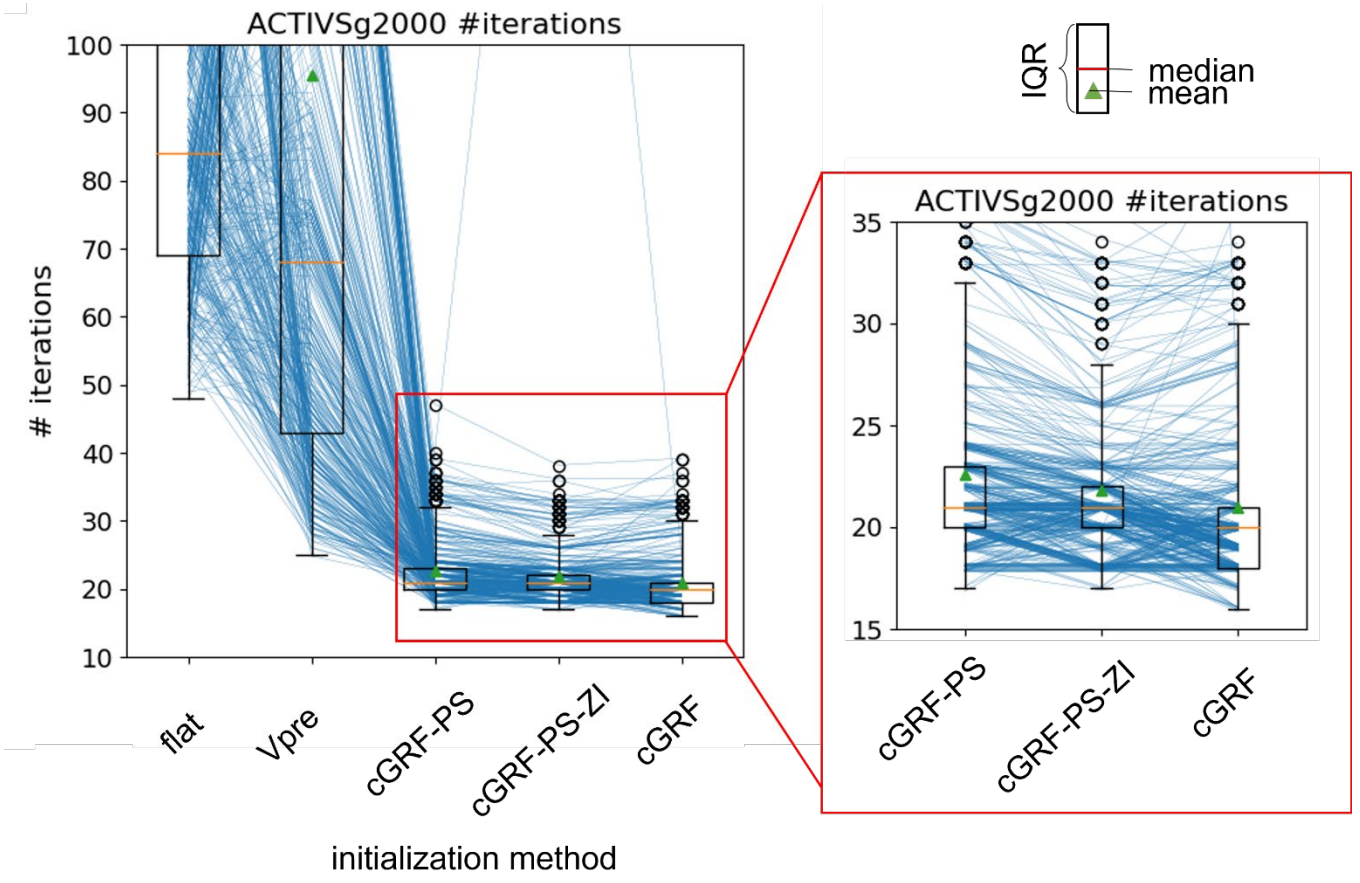


Including Domain Knowledge

- Developed three variants of graphical model-based warm starter: cGRF, cGRF-PS, cGRF-ZI

Domain Knowledge	cGRF	cGRF-PS	cGRF-ZI
Graphical Nature of the Grid	Y	Y	Y
Parameter Sharing	N	Y	Y
Zero Injection Nodes	N	N	Y

Results: Proposed Warm starter (cGRF)



(b) 2000-bus case.

On average, we observe a 5x speed improvement over traditional initialization methods

Conclusions

- Research goal: Develop analytical tools for grid cybersecurity
  - Special focus on combining data-driven and physics-based techniques
- Very interested in collaborations to maximize the impact