U.S. DEPARTMENT OF ENERGY

OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Watching Grid Infrastructure Stealthily through Proxies (WISP)

Raytheon Technologies Research Center
Dr. Lingyu (Lynn) Ren

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

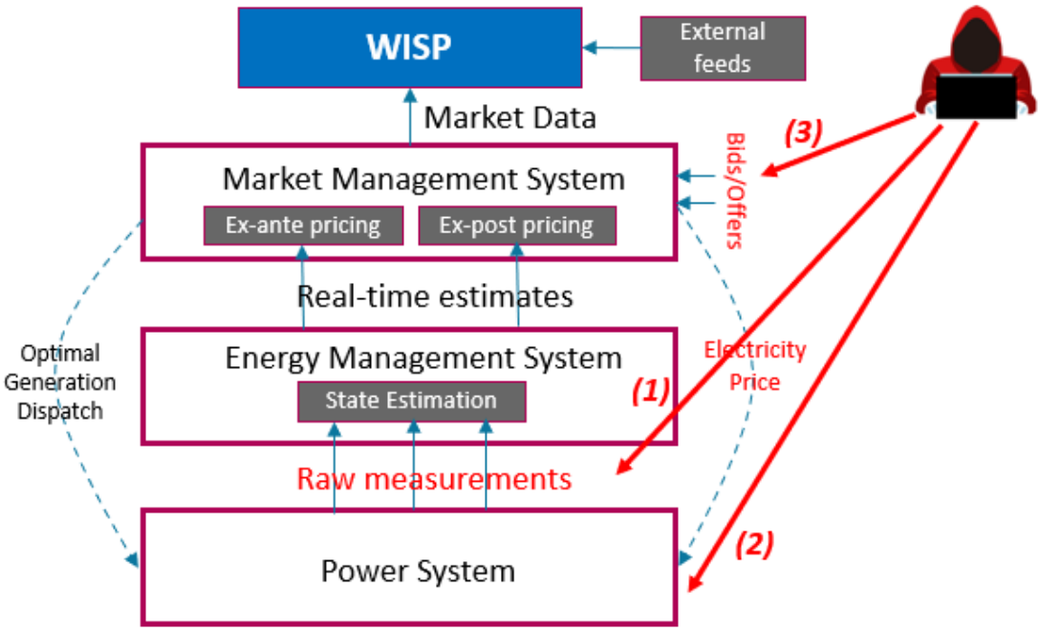
Project Overview

Objective

- **Develop a non-intrusive, data-driven energy market monitoring tool, named WISP.**
  - Use only publicly available electricity market data and relevant metadata.
  - Detect and distinguish cyber-attacks from normal power system events.
  - Localize the region of interest for potential cyber attacks.
- **Demonstrate the WISP technology using realistic electricity market simulators.**

Schedule

- **Project Timeline: Mar.2019 – Sept. 2021 (30m)**
- **Key Deliverables:**
  - Reports on threat and attack classification for energy markets. ✓
  - Simulation models and datasets. ✓
  - Library of attack and normal signatures. ✓
  - Architecture and design document for anomaly detection system. ➲
  - Red team testing report.
  - Final report.



Total Value of Award:	**$ 2.8M**
Funds Expended to Date:	**% 50**
Performer:	**RTRC**
Partners:	**UTK, PNNL**

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Advancing the State of the Art (SOA)

SCADA System

Intrusion Detection System:

- Network behavior anomaly detection
- Critical-state tracking
- Physics model-based detection

Drawbacks:

- False alarms
- Domain knowledge
- Lack of attack models

State Estimation

Attacks:

- False data injection attacks
- Lead to non-optimal/unsecure power operation

Countermeasures:

- Harden the physical sensors
- Improve bad data detection algorithms

Electricity Market

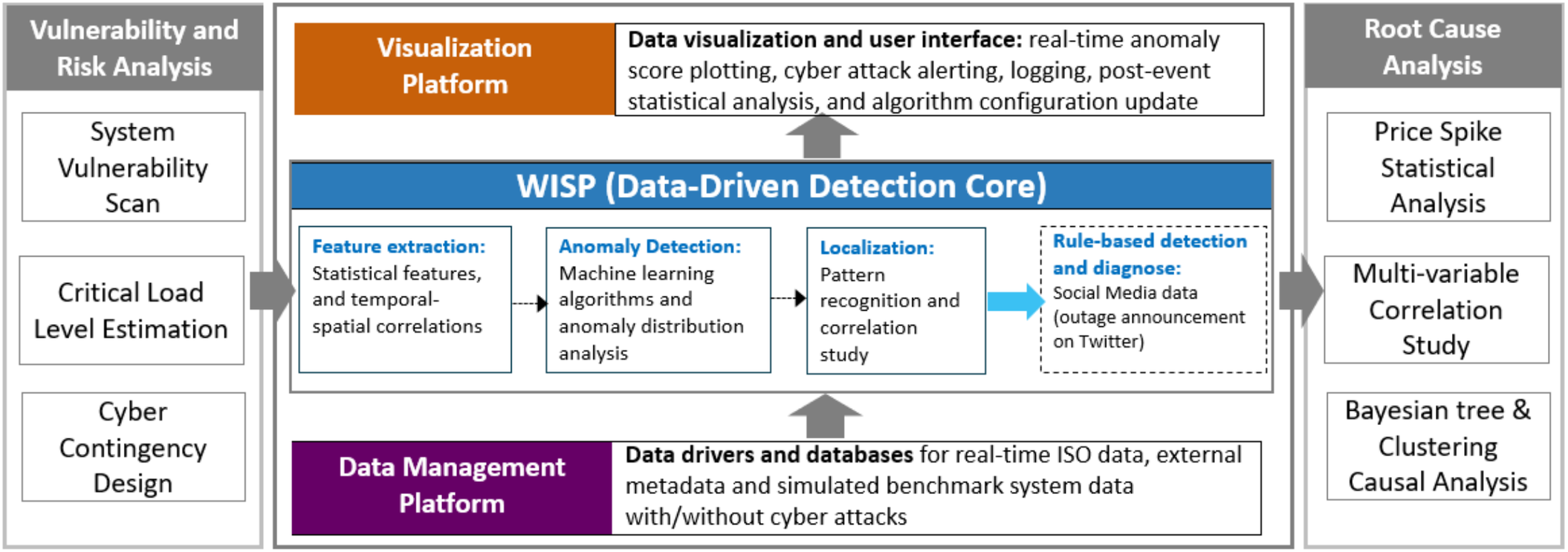
Attacks:

- Market manipulation through false data injection in state estimation
- Financial arbitrage through virtual bidding at selected buses
- Financial gains by fabricating fake transmission congestion patterns

Research Gaps:

Cyber threats occur at physical layer, energy management layer, market management layer and internal and external interfaces. Currently there is no system level protection on detecting cyber attacks and identifying region of interest.

Advancing the State of the Art (SOA)



Features

WISP is a cyber security monitoring tool which will be deployed as ***a service in the Cloud or on premise*** and provides reliable information to system operators for enhanced situational awareness, without impeding energy delivery functions.

Benefits

- WISP is a ***non-intrusive*** software application that provides additional cyber situational awareness.
- WISP provides ***diagnose results*** of the cyber alerts which facilitates the post-event decision-making process.
- WISP leverages the ***big data statistic and analytic technologies*** associated with the electricity market mechanism and rules to protect the soundness of the system which has never been achieved before.

Progress to Date

Major Accomplishments

- **DOE Deliverables (Technical Reports and Milestones):**
  - Technical Report on "Threat and Attack Classification for Energy Markets", Sept. 2019.
  - Technical Report on "Dataset Generation and Signature Derivation", April 2020.
  - Technical Milestone 1: development of machine learning algorithms to identify anomalous prices (detection rate > 85%, false alarm rate < 1%) , April 2020.
  - Technical Milestone 2: development of detection models to identify region of interest and attack target (detection rate > 85%), July 2020.
- **Outreach to potential customers:**
  - ISO New England on-site visit on Jan. 17th 2020.
  - PJM remote technical presentation and review on March 27th 2020.
- **Outreach to Raytheon commercialization team:**
  - Technical presentations and internal discussions with Raytheon Cyber Physical System Security Team, in July and Aug. 2020.
- **Four journal and conference papers:**
  - Title: "Market-Level Defense against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations", Journal: "IEEE Transactions on Power Systems", Status: accepted.
  - Title: "Profit-Oriented False Data Injection on Energy Market: Reviews, Analysis and Insights", Journal: "IEEE Transactions on Industrial Informatics", Status: second round review.
  - Title: "Cyber-Vulnerability Analysis for Real-time Market Operations", Journal: "IEEE Transactions on Smart Grid", Status: under review.
  - Title: "Data-Driven Probabilistic Anomaly Detection for Electricity Market under Cyber Attacks", Conference: 2021 American Control Conference (ACC), Status: invited paper.

Challenges to Success

Challenge 1: develop the right set of attack scenarios to test the efficiency of the proposed detection algorithms.

- Three months have been dedicated to build the attack scenarios for electricity markets. Besides consultation with industry experts, we also leveraged the simulation studies and published research results to guide the development of attack classes and their characterization.

Challenge 2: perform detection validation on large-scale power systems.

- The team created simulation test cases for Polish Power Network and Texas Power Grid, both contain over 2000 buses. The team is using RTRC high performance computing platform for parallel computing in dataset generation and model training.

Challenge 3: continuously use and update of models in adversarial environments.

- WISP will be designed to detect new data streams and display decisions (anomalous/normal, potential region of interest and attack target) in the Market Monitoring Tool, where operators can classify the decision as suspicious/normal; the decision made by operators will be pushed back to WISP allowing it to update the learned models pertaining to the new data streams.
- WISP is currently using a detection lock on the time period subsequent to a detected anomaly.

Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user

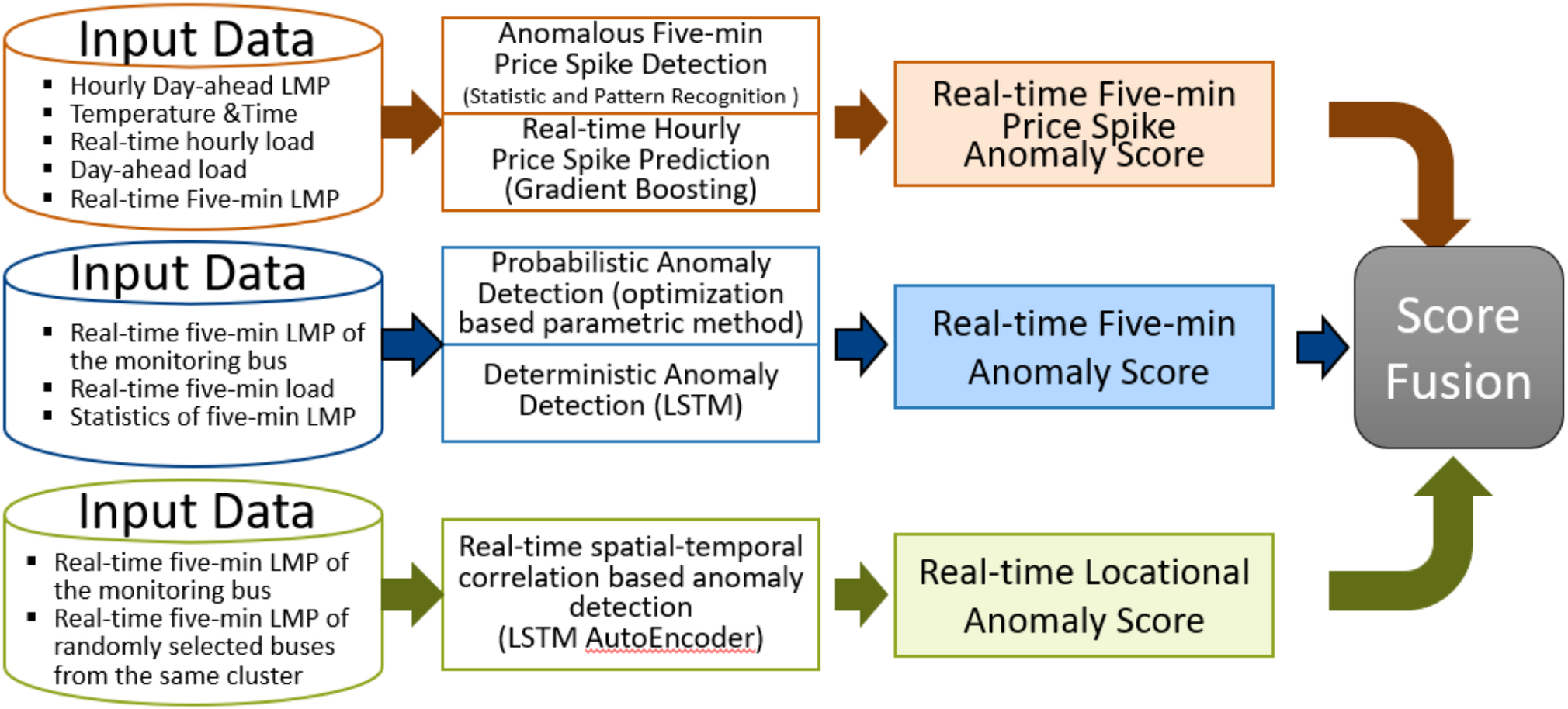
- Most of the research results are published as journal or conference papers for knowledge transfer to the academia and the general public.
- The targeted end user and customers are utilities and ISO/RTOs.
- Plans for industry acceptance and demonstration:
  - WISP will be demonstrated at UTK's CURENT research center, using the Large-scale Test Bed (LTB) platform, under the guidance from industry consultants. The demonstration will be performed at Phase II starting Mar. 2021, conditional to the approval of Phase I report.
  - WISP is currently tested on ISO NE, PJM, and California ISO datasets. Due to lack of attack data, the current testing is limited to spike detection and root cause analysis.
  - The team's industry consultant is joining regular team meetings and giving valuable feedbacks for easier industry acceptance. The team is also reaching out to major ISOs for technical review and potentials of on-site deployment.
  - The Raytheon Cyber Physical System Security Team is currently reviewing the project and looking for commercial use cases.

Next Steps for this Project

Approach for the next year or to the end of project

- Integration of data-driven detection core with the ancillary modules.
  - Vulnerability scan and risk analysis tool will help filter out the high-risk time periods based on the load patterns and the high-risk buses based on the vulnerability level of the attack targets.
  - The root cause analysis will provide diagnose information of potential reasons for anomalous price behavior based on cooccurrence of rare events from various observations.
- Software architecture design and development.
  - An integrated cyber monitoring tool will be developed using open source real-time visualization software and data management software. The final product will be self-contained and easy-configurable for deployment in major industry environment.
- Red team testing and Large-scale system demonstration.
  - The WISP cyber monitoring tool will be tested by an independent red team. Both cyber attacks and operational events will be applied to test the robustness of the WISP tool.
  - Large-scale power system test cases will be used in the demonstration phase.

WISP - Data-driven Detection Core



ISO-NE data
Spike Information

Spike	DR	FAR
>$100	66%	16%

IEEE 39 Simulation Data
Milestone 1 results

Attacks	DR	FAR
FDIA	85%	1%

PJM Data
Milestone 2 results

Clusters	DR	FAR
c1	88%	13%

FDIA: False Data Injection Attacks; PRA: Price Responsive Attacks;
LRA: Load Redistribution Attacks; DR: Detection Rate; FAR: False Alarm Rate.

WISP - Data-driven Detection Core

Fig. 1 Five-min LMP Anomaly Detection

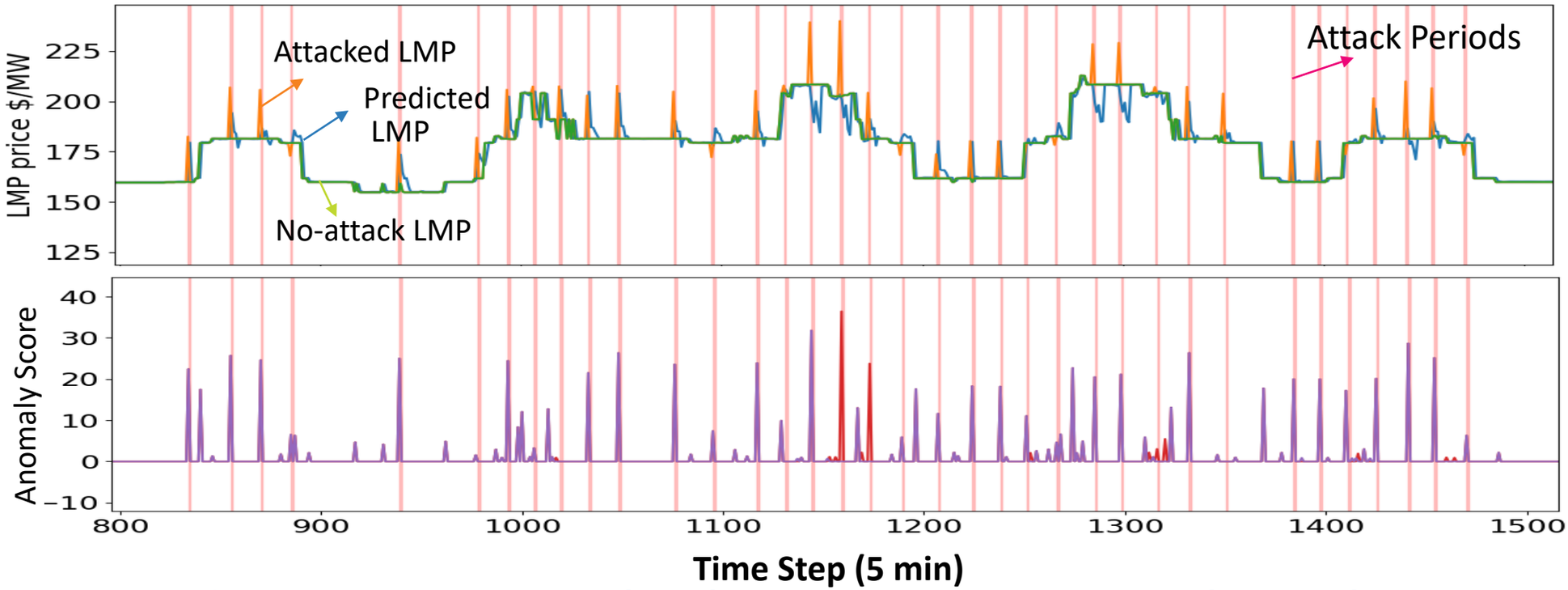


Fig. 2 ROC for Detection Threshold (0-30)

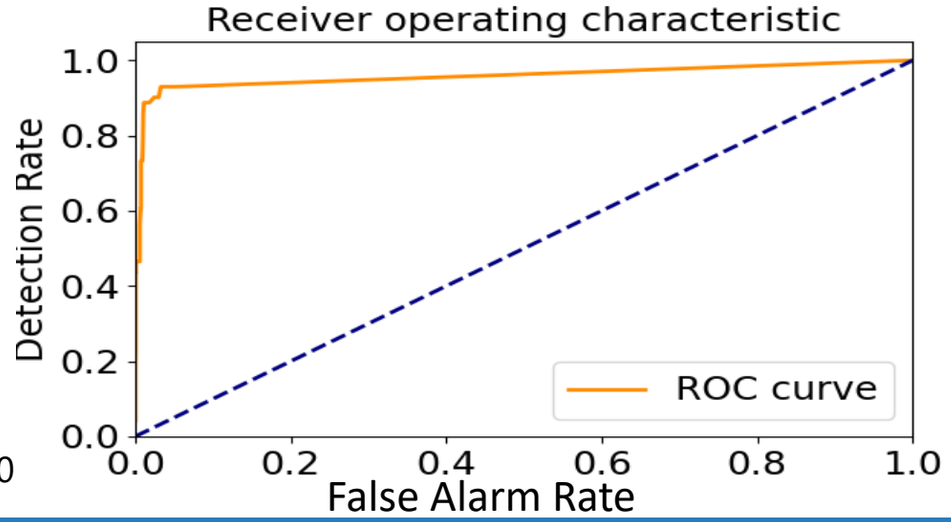
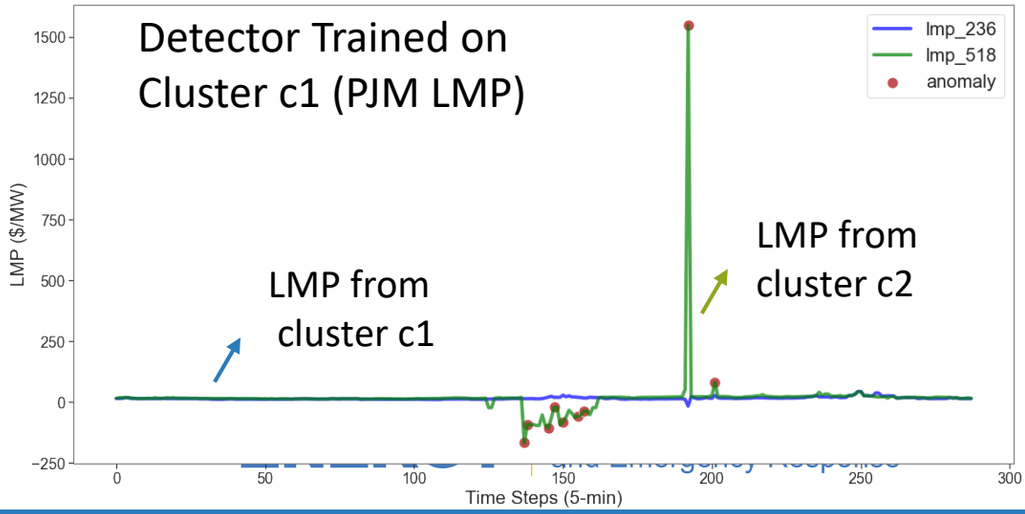
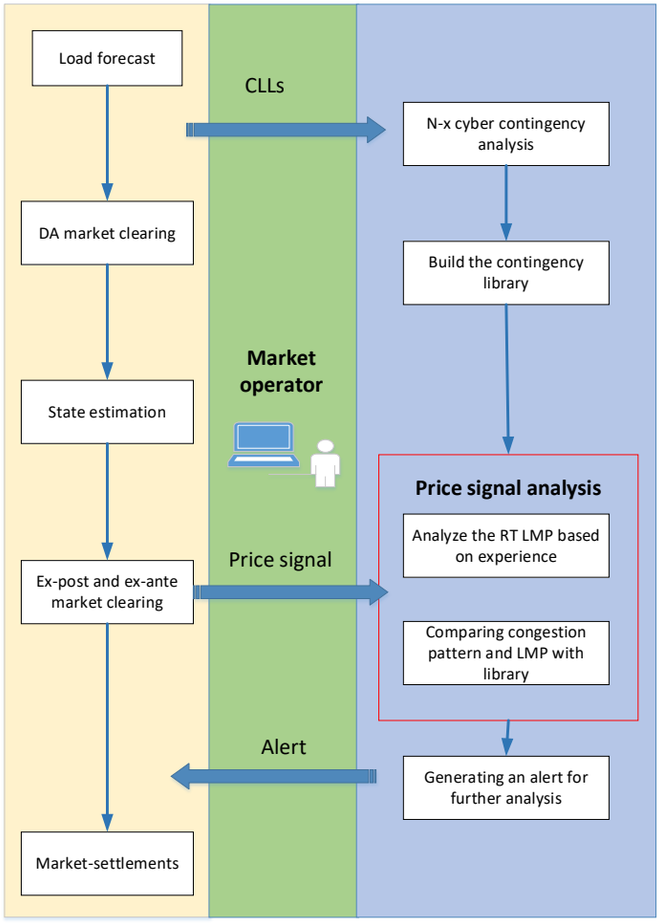


Fig. 3 Locational Anomaly Detection

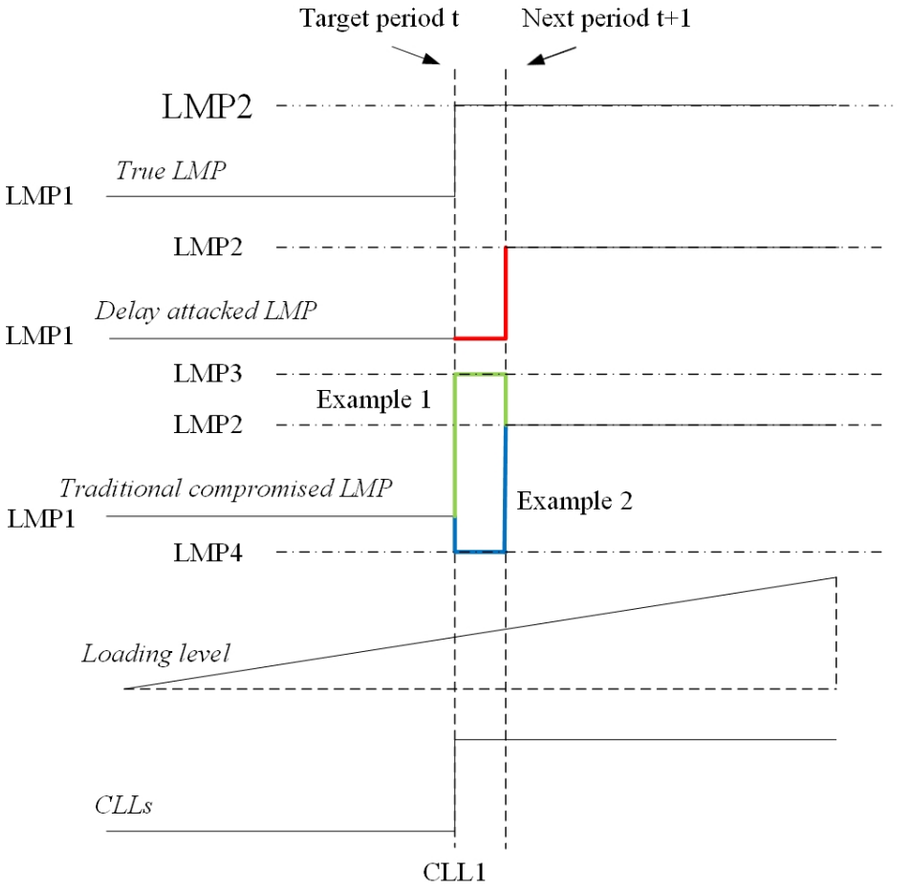


FDIA: Market-level defense and LMP Disguising Attack

- **Traditional market FDIAs easily induce abnormal price spikes. Based on this observation, we have developed a market-level defense strategy and a new LMP-disguising attack.**



Detection procedures



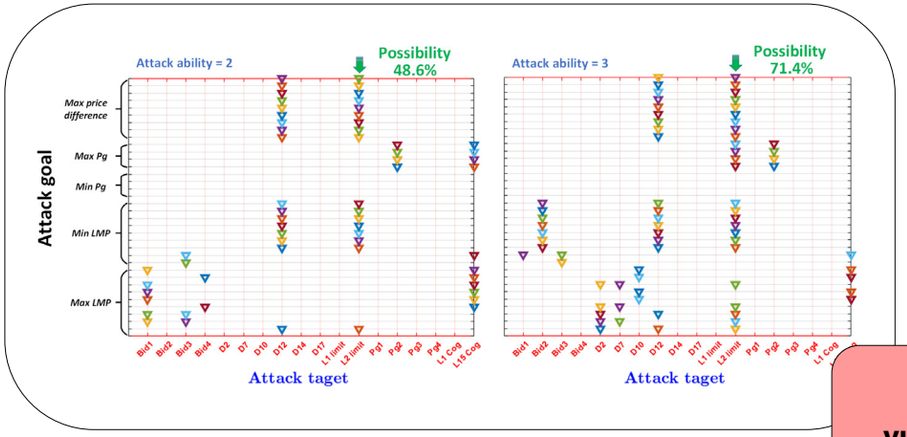
LMP-disguising attack

Q. Zhang, F. Li, H. Cui, R. Bo, L. Ren, "Market-Level Defense against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations," *IEEE Transactions on Power Systems*, In-Press.

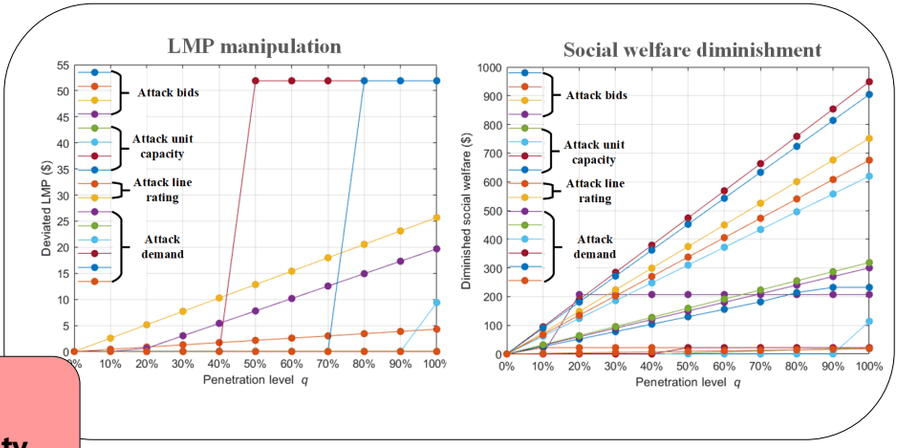
Cyber Vulnerability Assessment

- **Generally, potential attack targets, risky operating conditions, and the effectiveness of the defense are the most vital elements in developing a defense strategy and assessing the cyber vulnerability.**

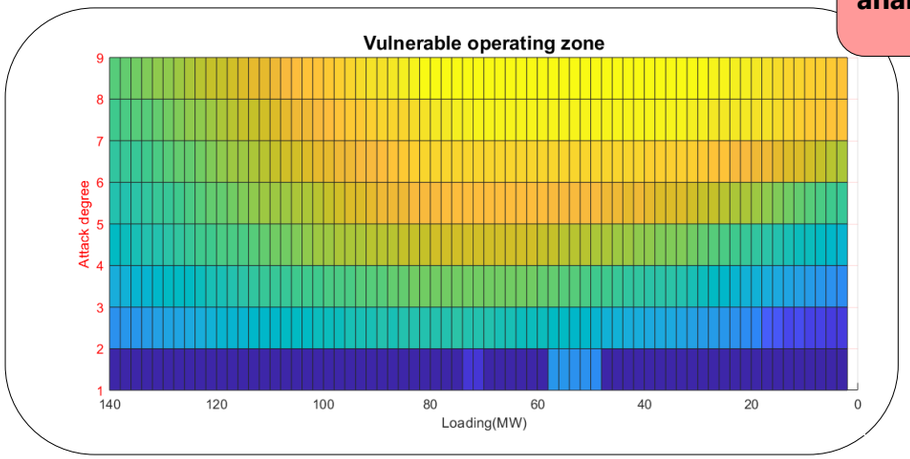
Highly probable cyberattack targets



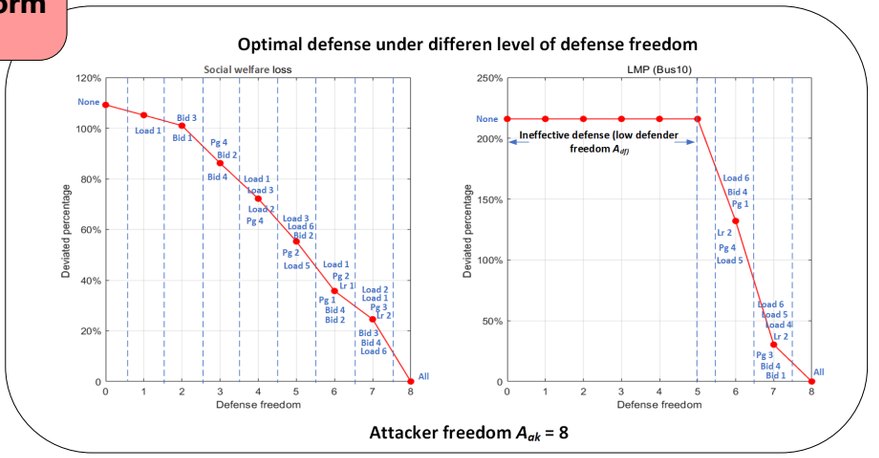
Devastating attack targets



Cyber-vulnerability analysis platform



Risky load levels



Mitigation ability under different degrees of defense

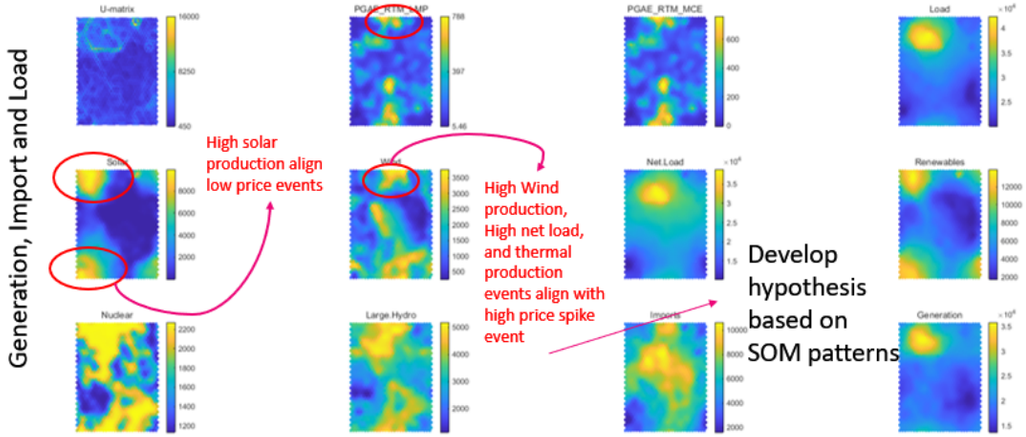
cyber-vulnerability analysis platform

Price Spike Root Cause Analysis

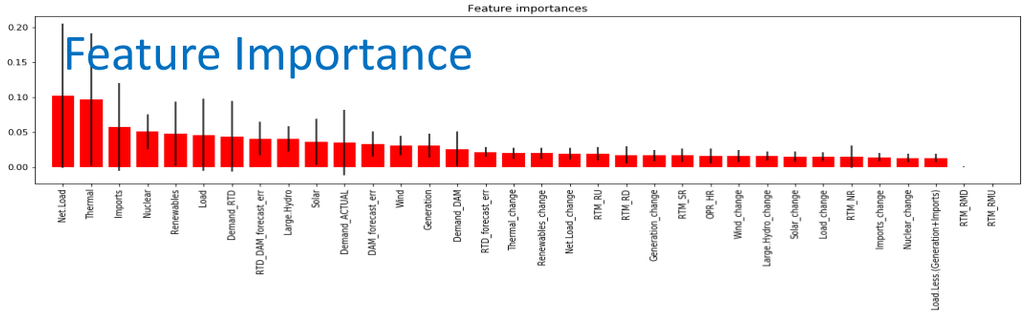
Objective:

- Identify root causes/system conditions or combination of root causes that lead to spikes.
- However, price-spikes in real-time can be caused by various factors that affect the state space of the system.
- A data-driven approach using machine learning models is implemented to identify the primary drivers behind price-spike events.

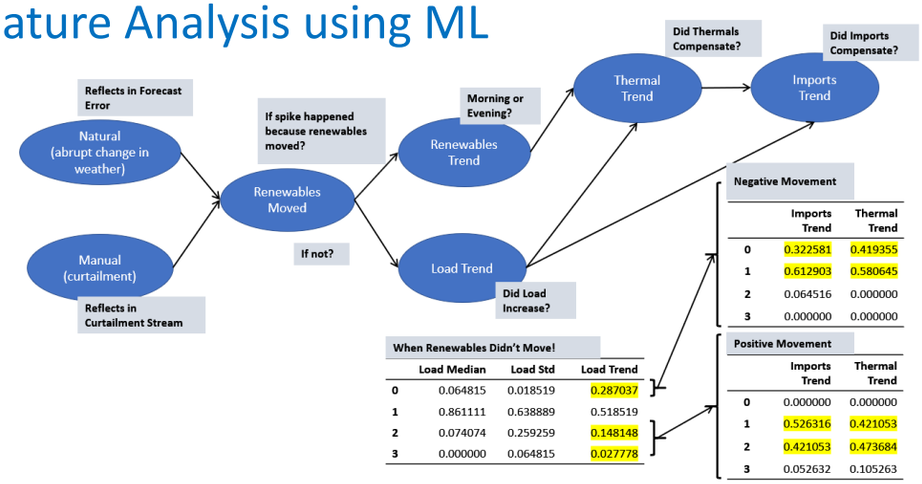
State Space using Self-Organizing Map



Feature Importance



Feature Analysis using ML



When Renewables Didn't Move!

	Load Median	Load Std	Load Trend
0	0.064815	0.018519	0.287037
1	0.861111	0.638889	0.518519
2	0.074074	0.259259	0.148148
3	0.000000	0.064815	0.027778

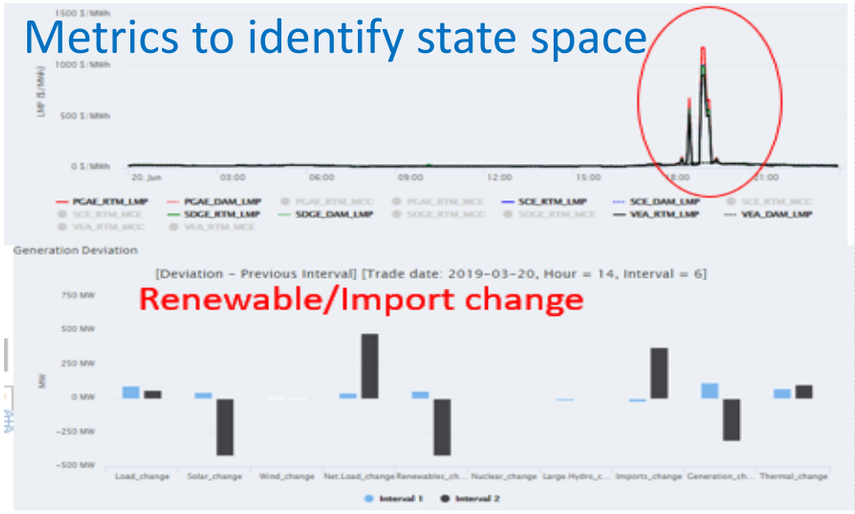
Negative Movement

	Imports Trend	Thermal Trend
0	0.322581	0.419355
1	0.612903	0.580645
2	0.064516	0.000000
3	0.000000	0.000000

Positive Movement

	Imports Trend	Thermal Trend
0	0.000000	0.000000
1	0.526316	0.421053
2	0.421053	0.473684
3	0.052632	0.105263

Metrics to identify state space



Impact:

1. Features identified in this analysis to be used to improve LMP prediction in the cyber-attack anomaly detection algorithms.
2. Identify vulnerable system conditions that can used for cyber-attacks.
3. Distinguish actual spikes vs. cyber-attack event spikes.

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

A. Somani, S. Datta, M. Jain, M. Halappanavar, PNNL