U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Assess the Impact and Evaluate the Response to Cybersecurity Issues (AIERCI)

Brookhaven National Laboratory (BNL)

Meng Yue

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

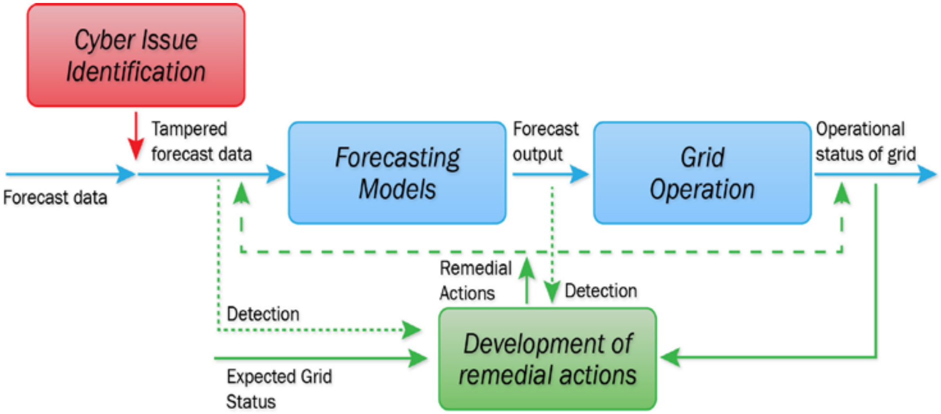
Summary: Assess the Impact and Evaluate the Response to Cybersecurity Issues (AIERCI)

Objective

- Develop an online AIERCI tool to detect and mitigate anomalies due to cyber attacks targeting essential forecasting data for load and renewables, and evaluate their impacts on grid scheduling functions for operation.

Schedule

- Project started 02/2016 and will end in 09/2020.
- Key deliverables: An online AIERCI tool based on a cybersecure forecasting scheme and grid scheduling functions, and a demonstration by 2020.
- Will ensure cybersecure forecasting for grid operation via the protection of data integrity and robust forecasting model against cybersecurity vandalism.



Total Value of Award:	$ 3.04M
Funds Expended to Date:	30%
Performer:	Brookhaven National Laboratory
Partners:	Argonne National Laboratory Idaho National Laboratory University of North Carolina – Charlotte University of Connecticut Orange and Rockland Utilities

Advancing the State of the Art (SOA)

- State of the art
  - Solely rely on information technology (IT) based solutions to protect data from being tampered with.
  - A lack of understanding of how adversaries perform cyberattacks on forecasting data and impact evaluation.
  - No online tool is available to detect, deter, evaluate, and mitigate impacts of cyberattacks on forecasting data.
    - Existing handling methods to detect bad data focus on detection of point and contextual anomalies and are inadequate for coordinated cyberattacks.
- Technical approach
  - **Cyber Layer**: identification and mitigation of potential vulnerabilities, exploit potential, and exposure in data input streams of energy management and control systems.
  - **Application Layer**: Detecting and mitigating anomalies in forecast data.
    - o Identify the potential means for compromising the forecasting input and output data, detection and mitigation of anomalies.
    - o Evaluate the effectiveness of detection/mitigation methods by feeding the tampered data into the forecasting model(s).
  - **Impact Assessment**: Determining the impacts on the scheduling functionalities.

Advancing the State of the Art (SOA, cont'd)

- Features of the technical approach
  - Complementing existing IT-based solutions by adding another layer of defense, as a commonly adopted defense-in-depth strategy.
  - Ensuring a cybersecure forecasting using advanced model- and data analytics-based anomaly detection and mitigation and robust ensemble models to effectively deal with coordinated attacks.
  - Developing a platform for evaluation of cyberattack impacts and performance of detection and mitigation means.

Challenges to Success

Challenge 1: Seamless integration with energy forecasting systems and scheduling functions being used by utilities

- Solution: BNL is using systems and data that are the same as or similar those being used by our utility partner (ORU) for realistic assessment and development. This is expected to make the tool compatible with other utility systems.

Challenge 2: Industry acceptance

- Solution: Creation of IAB for providing guidance for the tool development.
- Solution: Demonstration of the tool under an environment as close as possible to the utilities' operation.

Progress to Date

Major Accomplishments

- **FY 2016 Milestones**
  - Creation of Advisory Board: Completed
    - Industrial Advisory Board (IAB) has been created and meets annually, or as needed
      - Orange and Rockland Utility (POC: Keith Brideweser), Nevermore Security (POC: Annabelle Lee), New England ISO (POC: Jonathan Black), and SAS (Statistical Analysis Systems, POC: Jingrui Xie).
  - Identify and Justify Detection/Mitigation Methods: Completed
    - Developed new cyberattack templates and identified various detection and mitigation methods for different types of anomalies.
- **FY 2017 Milestones***
  - Develop Data Flow Requirements and Design Review: Completed
    - Developed internal and external threat scenarios based on ORU's data.
  - Develop short-term/very-short-term forecasting techniques/schemes: Completed
    - Developed and implemented both model- and data analytic-based anomaly detection (MBM and DABM) and mitigation methods, and the model assisted hybrid implementation of an integrated solution (HIIS)
    - Quantitatively validated the performance of the proposed solution using a Monte Carlo approach

: To address one of peer reviewers' comment in 2016, an ensemble approach is being developed to further enhance the performance of the forecasting

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

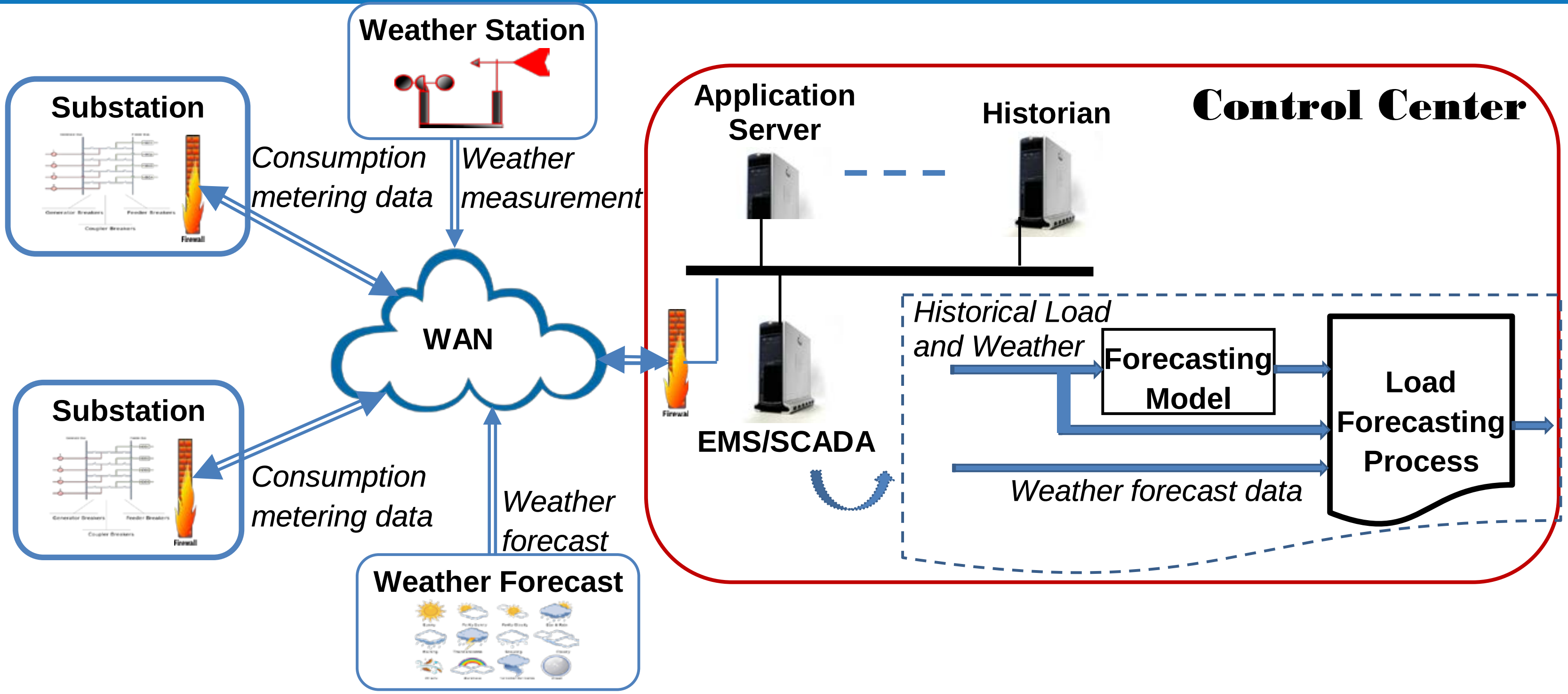
- The targeted end users for the technology or knowledge include both utilities and vendors.
- To gain industry acceptance
    - Development of the tool will be performed with close consultation and input from the IAB members.
    - The prototype Matlab-based AIERCI tool is being converted to a Python-driven web service for easy access by forecast practitioners.
    - A separate task is scheduled for a demonstration of the developed AIERCI tool.
        - Testing environment of the developed tool is vital.
        - The tool demonstration will be performed in an environment as close as possible to the real operational environment.
            - A control room or test bed mimicking the real-time operation based on utilities' datasets.

Next Steps for this Project

Approach for the next year or to the end of project

- Key Milestones to accomplish
  - Develop AIERCI tool (due in March 2019)
    - Finalized the layout of the online AIERCI tool and now converting the Matlab-based prototype tool of MBM and HIIS anomaly detection and mitigation tool to a Python-driven web service.
    - The ensemble approach will also be integrated.
  - Benchmark tool (Due in September 2019)
    - The AIERCI tool will be thoroughly tested, verified, and validated using utilities' real data and the tool will be continuously refined.
  - Demonstration design review and observations (Due in September 2019)
    - Review of tool design to assure its readiness.
  - Deploy AIERCI tool (Due in June 2020)
    - Interface the AIERCI tool with scheduling functionalities such as unit commitment (UC), power congestion and locational marginal price (LMP), and automatic generation control (AGC) based on ANL's development.

Data Flow and Communication Links for Load Forecasting

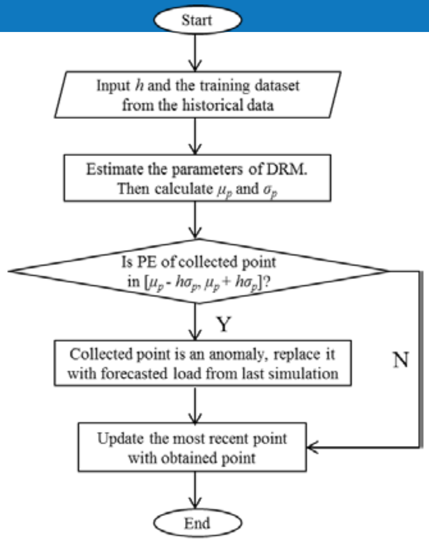


- The data include consumption metered data and data collected at substations/ feeders, historical weather measurements, and weather forecasts
  - **Internal threats** may be from disgruntled employees, employee mistakes, and contractors allowed within the facilities.
  - **External threats** can be carried out over the network, or by someone deliberately gaining unauthorized access to facilities (Cyber Criminals, Hacktivists, and State Sponsored Operations).

Real-time MBM and DABM for Anomaly Detection and Mitigation

Targeting detection and mitigation of various types of anomalies

- A model based method (MBM)
  - A dynamic regression model and an adaptive threshold for intervals of percentage error (PE) of the predicted load.
  - The thresholds for anomaly detection are updated on a rolling basis.



Start

Input h and the training dataset from the historical data

Estimate the parameters of DRM. Then calculate μ_p and σ_p

Is PE of collected point in $[\mu_p - h\sigma_p, \mu_p + h\sigma_p]$?

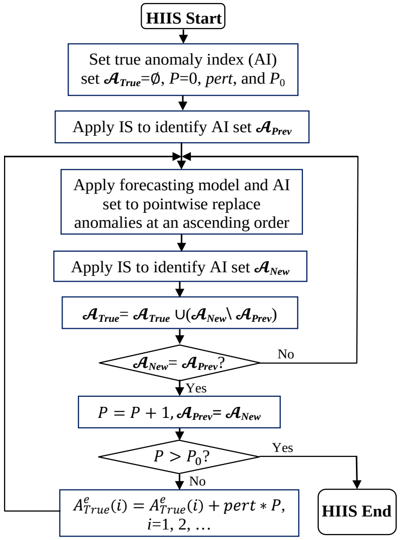
Y

N

Collected point is an anomaly, replace it with forecasted load from last simulation

Update the most recent point with obtained point

End



HIIS Start

Set true anomaly index (AI) set $\mathcal{A}_{True}=\emptyset$, P=0, *pert*, and P_0

Apply IS to identify AI set $\mathcal{A}_{Prev}$

Apply forecasting model and AI set to pointwise replace anomalies at an ascending order

Apply IS to identify AI set $\mathcal{A}_{New}$

$\mathcal{A}_{True}= \mathcal{A}_{True} \cup(\mathcal{A}_{New} \backslash \mathcal{A}_{Prev})$

$\mathcal{A}_{New}= \mathcal{A}_{Prev}$?

No

Yes

$P = P + 1, \mathcal{A}_{Prev}= \mathcal{A}_{New}$

$P > P_0$?

Yes

No

$A^e_{True}(i) = A^e_{True}(i) + pert * P$, i=1, 2, …

HIIS End

- An HIIS of data analytics based method (DABM)
  - o Apply the forecasting model to generate load points to replace the anomalies detected by the DABM, i.e., IS.
  - o By doing this, some of the undetected anomalies become boundary points and are easier to detect
  - o The IS and the load forecasting model can be alternatively applied for detecting and fixing the boundary anomalies until no more anomalies are detected.

- **Achieved preliminary results for adversarial training and robust regression model development**

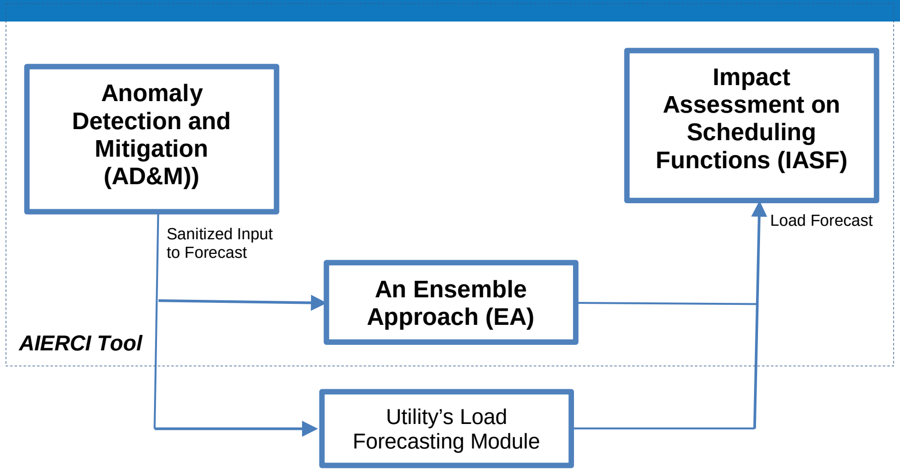
Publications:
1. M. Cui, J. Wang, and M. Yue, "Machine Learning Based Anomaly Detection for Load Forecasting under Cyberattacks," submitted to IEEE Transactions on Smart Grid, under review.
2. M. Yue, T. Hong, and J. Wang, "Data Analytics Based Anomaly Detection in Time Series Data for Online Cybersecure Load Forecasting," accepted by IEEE Transactions on Smart Grid.
3. J. Luo, T. Hong, and M. Yue, "Real-time Anomaly Detection for Very Short-Term Load Forecasting," Journal of Modern Power Systems and Clear Energy, Vol 6, No 2, March 2018.
4. M. Yue, "Evaluation of A Data Analytic Based Anomaly Detection Method for Load Forecasting Data," IEEE PES General Meeting, August 2018
5. M. Yue, "An Integrated Anomaly Detection Method for Load Forecasting Data under Cyberattacks," IEEE PES General Meeting, July 2017.

A Detailed Performance Evaluation

A Monte Carlo simulation was performed using 500 samples for different attack templates.

Metrics	Detection Methods	Attack Parameters [a,b]				
		[0.0,0.1]	[0.1,0.2]	[0.2,0.3]	[0.3,0.4]	[0.4,0.5]
False Negative Ratio	SOD-method	99.98%	98.5%	93.7%	84.1%	81.0%
	CI-method	100%	99.6%	97.1%	89.8%	86.0%
	SAX-method	67.2%	43.1%	28.7%	20.8%	16.4%
	Integrated Solution	67.1%	42.5%	27.4%	19.6%	15.7%
	HIIS (w_s=5)	61.3%	45.5%	20.1%	8.4%	3.8%
	HIIS (w_s=6)	62.5%	30.8%	6.9%	2.8%	1.5%
False Positive Ratio	SOD-method	9.1E-4	0.05%	0.11%	0.06%	0.06%
	CI-method	9.5E-3	0.05%	0.11%	0.07%	0.04%
	SAX-method	3.97%	4.6%	4.8%	5.7%	6.6%
	Integrated Solution	4.9%	4.7%	5.0%	5.8%	6.6%
	HIIS (w_s=5)	1.3%	1.5%	2.0%	1.9%	2.0%
	HIIS (w_s=6)	2.1%	3.0%	3.1%	3.9%	4.7%
Mean Absolute Percentage Error	HIIS (w_s=5)	1.85%	2.51%	2.35%	1.98%	1.96%
	HIIS (w_s=6)	1.84%	2.14%	2.0%	1.94%	1.86%

AIERCI Tool Development

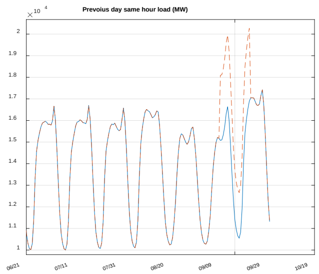

Anomaly Detection and Mitigation (AD&M))
Sanitized Input to Forecast
An Ensemble Approach (EA)
Impact Assessment on Scheduling Functions (IASF)
Load Forecast
AIERCI Tool
Utility's Load Forecasting Module

Architecture of the AIERCI Tool

- AD&M module: MBM and HIIS of DABM
- EA module: Adversarial training and Huber's robust regression
- IASF module: UC, congestion and LMP, and load frequency control

The Python-driven web service for AD&M module

- Can be easily accessed by utility personnel for dealing with data integrity issues
- Can be easily integrated into forecasting tools being used by utilities



Client

OAuth2 token

Input JSON (timeseries for location & date range)

- Historic load
- Input weather data
- Independent weather data
- Parameters

deserializer

Web Service

MVC: Model-View-Controller Design

- **Model:** models.py (interface to the data/database)
- **View:** urls.py, settings.py, templates (User Interface)
- **Controller:** views.py, glues the model and view
- **Compute:** anomaly detection for all time series

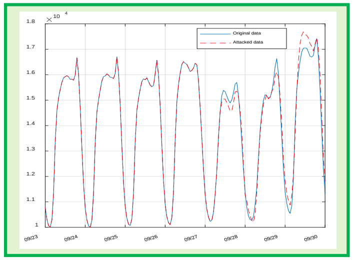
serializer

Output JSON (timeseries for location & date range)

- Quantitative anomaly detection summary
- Mitigated time series

OAuth2 token

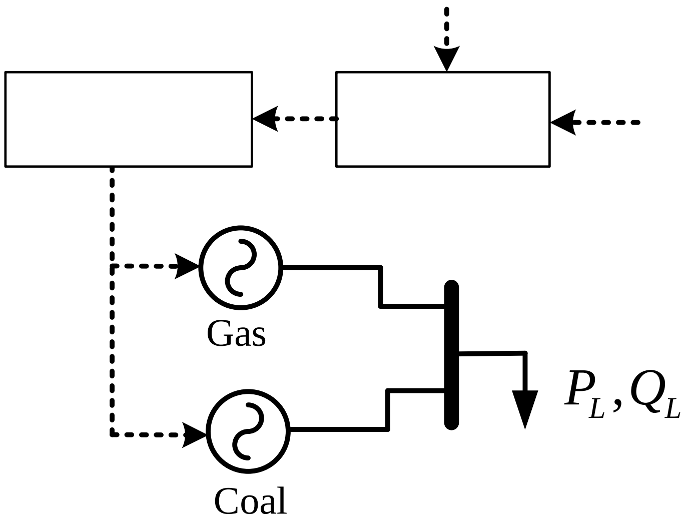
Client



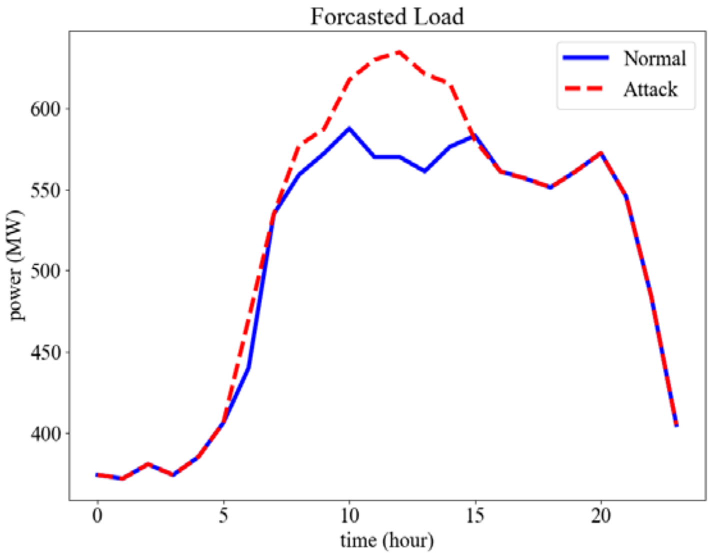
- Django RESTful Framework
- Written in Python
- SQLite database
- OAuth2 (industry standard protocol for authorization)

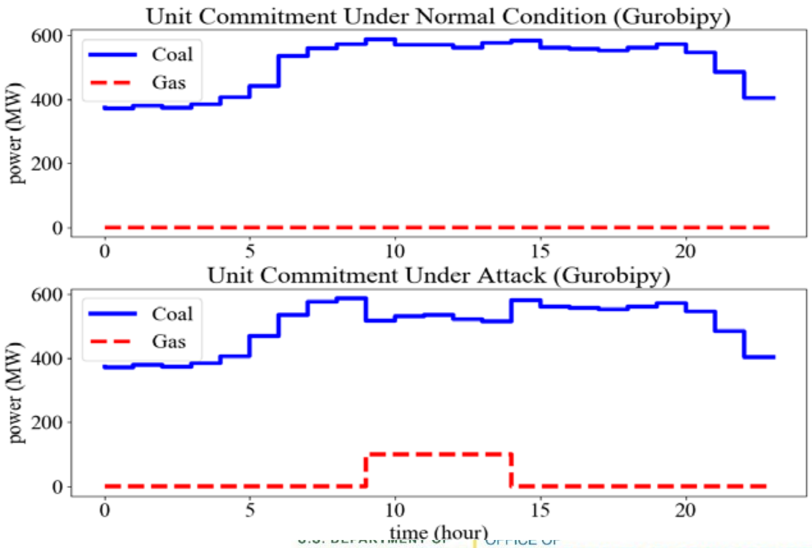
- Simple RESTful web services has been developed thus far
- Next steps are to build in complexities and incorporate anomaly detection algorithms

Impact Assessment of Scheduling Functions (IASF) – Unit Commitment Study



- Using an example two machine system for illustration
- Assessing the impacts on UC and the associated costs under cyberattack, especially the start-up and shut-down times
- Spinning reserve requirement is considered in the study
- Python scripts have been developed


Forcasted Load
Normal
Attack
power (MW)
time (hour)


Unit Commitment Under Normal Condition (Gurobipy)
Coal
Gas
power (MW)
Unit Commitment Under Attack (Gurobipy)
Coal
Gas
power (MW)
time (hour)