Anomaly Detection and Mitigation for Dynamic Frequency Regulation in Hydropower-Battery Systems

Preprint

Vivek Kumar Singh, Rakib Hossain, and Ethan Tucker

National Renewable Energy Laboratory

Presented at the 2024 IEEE Power & Energy Society General Meeting
Seattle, Washington
July 21-25, 2024

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5R00-87869
April 2024

Anomaly Detection and Mitigation for Dynamic Frequency Regulation in Hydropower-Battery Systems

Preprint

Vivek Kumar Singh, Rakib Hossain, and Ethan Tucker

National Renewable Energy Laboratory

Suggested Citation
Singh, Vivek Kumar, Rakib Hossain, and Ethan Tucker. 2024. *Anomaly Detection and Mitigation for Dynamic Frequency Regulation in Hydropower-Battery Systems: Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5R00-87869. https://www.nrel.gov/docs/fy24osti/87869.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5R00-87869
April 2024

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Water Power Technologies Office. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

NREL prints on paper that contains recycled content.

Anomaly Detection and Mitigation for Dynamic Frequency Regulation in Hydropower-Battery Systems

Vivek Kumar Singh, Rakib Hossain, Ethan Tucker
National Renewable Energy Laboratory
Golden, Colorado
Email: vivekkumar.singh@nrel.gov, rakib.hossain@nrel.gov, ethan.tucker@nrel.gov

***Abstract*—Hydropower operators and energy storage providers are increasingly interested in participating in frequency regulation services, driven by the incentives offered by independent system operators, such as the PJM Interconnection. This transition, however, unfolds against the backdrop of a modernizing and rapidly digitizing power grid, exposing the integrated legacy infrastructure to a multitude of cybersecurity threats. This work presents an approach for developing an anomaly detection and mitigation system to address cybersecurity challenges during the participation of a hydropower-integrated battery energy storage system (BESS) in a frequency regulation market. The applied anomaly detector utilizes machine learning algorithms to provide detailed classification of cyber-physical events. Later, the applied mitigation system triggers predefined corrective actions to minimize the impact of data integrity attacks on the regulation market and system stability. We evaluated the proposed approach on a hydropower-integrated BESS topology, specifically analyzing the slow regulation signal (Reg A) coming from the PJM market. Our simulation results demonstrate that the proposed approach performs well in detecting data integrity attacks within the allocated time frame and also minimizes the system's transient instability during the participation of hydropower and BESS in the regulation market.**

***Index Terms*—battery energy storage system, hydropower, regulation market, cybersecurity, machine learning.**

I. Introduction

The traditional power grid comprises centralized power generation facilities that supply enough electricity and related services to satisfy grid demands. However, as the grid evolves toward incorporating more smaller-scale power sources, especially wind and solar installations, there is a growing need for additional resources to enhance flexibility and meet ancillary service requirements. Many hydropower owners and energy storage providers are interested in participating in regulation services markets because of the additional incentives provided by independent system operators. For example, the PJM market utilizes hydropower with other distributed energy resources, such as battery energy storage systems (BESS), to provide frequency regulation in a competitive electricity market by minimizing small mismatches between load and generation [1]. This allows PJM to ensure the availability of adequate capacity at the most economic price point. In particular, the PJM regulation market generates two types of regulation signals: (1) Regulation A (Reg A) signal and (2) Regulation D (Reg D) signal, which are computed from the area control error (ACE). The Reg A is a slower signal that is generally met by conventional diesel generators and hydropower plants with limited ramping capability to recover from larger fluctuations in power grid. However, the Reg D signal is fast, dynamic, and requires energy storage systems, such as batteries and ultracapacitors, which can respond rapidly as needed to regulate frequency [2].

These regulation signals rely on the Distributed Network Protocol (DNP3), for exchanging information between PJM's control center and generation units, which is a clear text protocol and is protected using the Transport Layer Security (TLS) encryption [3]. The authors of [4] discussed nine common types of cyber-physical configurations of legacy hydroelectric plants that could be targeted by adversaries as the advanced operational capabilities are developed for managing and operating these hydropower facilities. Several machine learning algorithms were proposed in the past with the aim of detecting and classifying cyber-attacks within the grid network [5], [6]. A path mining-based classification approach is proposed in [5] that leveraged system parameters, including voltage, power, and frequency, to identify and categorize cyber threats. Further, the study presented in [6] highlights the efficacy of a supervised learning approach, specifically employing decision trees, in proficiently discerning cyber-attacks, physical events, and normal operation within the power grid.

This paper presents a novel approach for developing an anomaly detection and mitigation system (ADMS) for hydropower-integrated BESS that can detect data integrity attacks on a regulation signal (Reg A) in real time. Once these attacks are detected, corrective actions are triggered based on the duration of these attacks to minimize their impact on grid operation. We tested the proposed approach using an IEEE 2-bus test system in which the incoming Reg A signal

[1] Acknowledgement: This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Water Power Technologies Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

is split into two input power signals, one for hydropower and another for battery resources. Finally, we have evaluated the performance of the proposed approach using performance metrics, processing time, and dynamic power flow simulations.

II. Related Works and Overview

In [7], the Pacific Northwest National Laboratory discussed a road map to improve the cybersecurity of U.S. hydropower fleets and identified existing challenges related to peer-to-peer information sharing between facility owners, asset management, and patch management. The authors of [8] presented the impact of false data injection and denial-of-service attacks on hydropower plants by modifying local signals that impacted system stability through increased oscillation. The authors of [9] developed a cybersecurity platform that detects network-specific attacks and deploys honeypots, which simulate the vulnerable programmable logic controller and Internet of Things devices to disguise these devices from potential threats. Although great efforts, the platform presented in [9] might fail to detect stealthy cyberattacks that could have initiated through internal threats, malware injection, and other evasion techniques. This paper presents the potential solution to address internal threats that will not be detected by the aforementioned approach.

A. Frequency Regulation Market

Fig. 1 shows a high-level architecture that closely fits into the PJM-based frequency regulation market, which utilizes a Reg A signal and provides an efficient participation of BESS and hydropower to meet the required power response. It is divided into three major steps, as discussed here:

Step 1 (Reg A communication): The normalized Reg A, $(r_1(t))$, calculated from the ACE, is forwarded to the field site using the DNP3 communication. Also, we assume that the DNP3 traffic is secured with the TLS virtual private network tunnel, as discussed in [3].

Step 2 (Allocate input-power response to hydropower): Within the substation network, $r_1(t)$ is decrypted, and the actual regulation power signal, $R(t)$, is computed by multiplying $r_1(t)$ with a regulation participation factor (k). The input power allocation for the hydropower, $P_{hi}(t)$, is computed based on the assigned weight, w, as shown in Eq. (1). Note that w is decided based on the capacity and power limits of hydropower and BESS. Later, the power error, $e_r(t)$, is computed based on the difference between the hydropower output, $P_{ho}(t)$, and hydropower input, $P_{hi}(t)$.

$$P_{hi}(t) = w \times R(t) \tag{1}$$

$$e_r(t) = P_{hi}(t) - P_{ho}(t) \tag{2}$$

Step 3 (Allocate input-power response to BESS): The total input power, $P_{bi}(t)$, for the BESS is computed in Eq. (3) by adding $e_r(t)$ and the remaining Reg A component, $(1-w) \times R(t)$.

$$P_{bi}(t) = e_r(t) + (1-w) \times R(t) \tag{3}$$

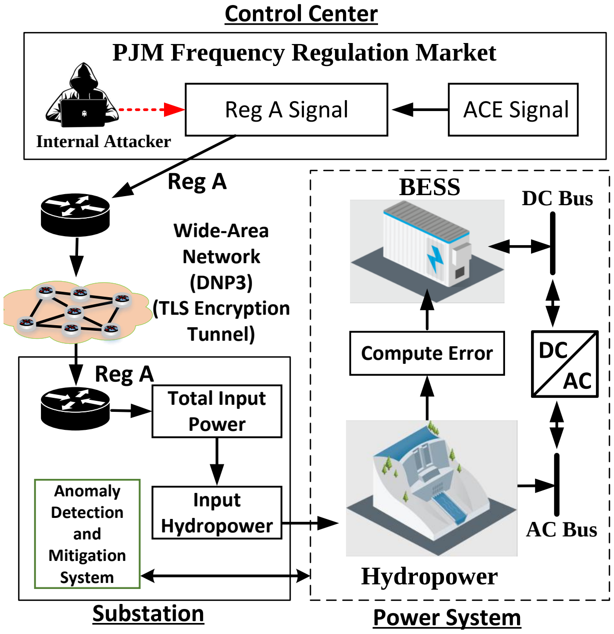


Fig. 1: High-level architecture

B. Cyberattack Vectors

Considering the integration of TLS encryption-based secure DNP3 traffic and the intent to execute stealthy attacks, we assume that the attacker is able to access the control center network and perform either of two types of data integrity attacks:

1) **Load/line tripping attack**: This attack vector includes unauthorized tripping of a physical relay to disconnect the transmission line or load [6].

2) **Signal-altering attack**: This attack vector involves modifying the incoming Reg A signals using attack templates, including pulse, ramp, and scaling attacks [6].

III. Proposed Methodology

A. Anomaly Detection Methodology

The proposed anomaly detector, deployed in the substation (see Fig. 1), utilizes measurements collected from the plant facility, which include time series of hydro output power, battery output power, active power of bus 1, active power of bus 2, and battery state of charge (SOC), to train classification models (see Fig. 2). Different types of machine learning algorithms, including support vector classifier (SVC), decision tree (DT), random forest (RF), logistic regression (LR), k-nearest neighbors (KNN), and artificial neural network (ANN), were applied to develop classification models. We have generated a dataset encompassing cyberattacks and normal operation and labeled it during the offline process to improve computational efficiency of the applied supervised machine learning algorithms. The labeled dataset is preprocessed to support data cleaning and normalization, and 70% of the dataset is utilized for training different machine learning algorithms. During the offline testing of the remaining 30% dataset, the most efficient machine learning algorithm is selected based on its performance and is integrated with rules-based mitigation system (RBMS) during real-time testing.

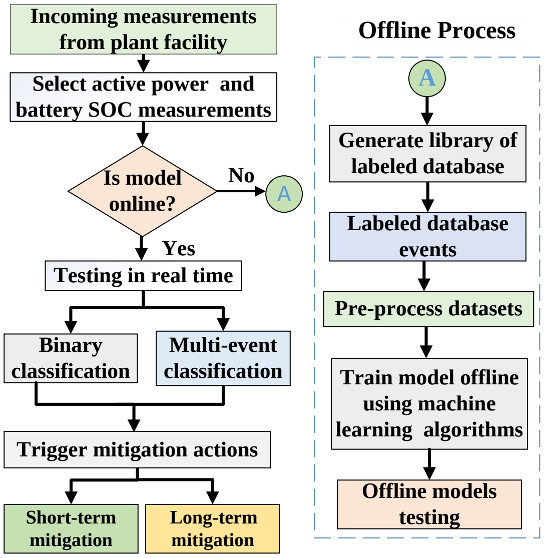

Incoming measurements from plant facility
Select active power and battery SOC measurements
Is model online?
No
A
Yes
Testing in real time
Binary classification
Multi-event classification
Trigger mitigation actions
Short-term mitigation
Long-term mitigation
Offline Process
A
Generate library of labeled database
Labeled database events
Pre-process datasets
Train model offline using machine learning algorithms
Offline models testing

Fig. 2: Proposed anomaly detection and mitigation approach

B. RBMS

The RBMS applies corrective actions depending on the duration of signal-altering attacks detected by the anomaly detector. Note that we assume that the system can withstand a $N-1$ contingency, which could happen during a load or tripping attack, obviating the need for mitigation actions in such cases. Meanwhile, it is crucial for the anomaly detector to accurately differentiate between signal-altering attacks and other types of events for developing a robust multiclass classification model. For signal-altering attacks, we have defined an attack duration threshold, λ, that could be defined by grid operators or substation engineers during offline analysis based on grid topology, operation devices, and other factors. Based on λ, we have considered two types of mitigation.

1) **Mitigation against short-term attack**: In this scenario, we compute the sliding average from the previous l number of historical measurements that are not corrupted for the Reg A signal and use the computed average instead of the live, corrupted signal during the attack duration until the attack is resolved.

2) **Mitigation against long-term attack**: This case is considered when the attack is continued for a long period of time, exceeding the defined λ. At this point, hydropower and battery will switch to the local mode of operation that does not respond to the Reg A signal and ancillary services will not be provided by them.

IV. System Modeling and Datasets Generation

A. System Modeling

For a case study, we modeled an IEEE two-bus test system using the Python-integrated open-source Distribution System Simulator (OpenDSS). In this configuration (see Fig. 3), a battery of maximum capacity of 3.9 MW and rated voltage of 600 V was connected to a DC/AC boost converter to control charging and discharging of the battery [10]. The hydropower model of rating 30 MVA and 13.8 kV initially provided a total active power of around 15 MW to two static PQ loads (7.5 MW each) connected at bus 1. Also, a Python-based co-simulation framework, openDSS-wrapper [11], was utilized to perform dynamic simulation based on the incoming Reg A signal, dated May 4, 2014, as provided in [2].

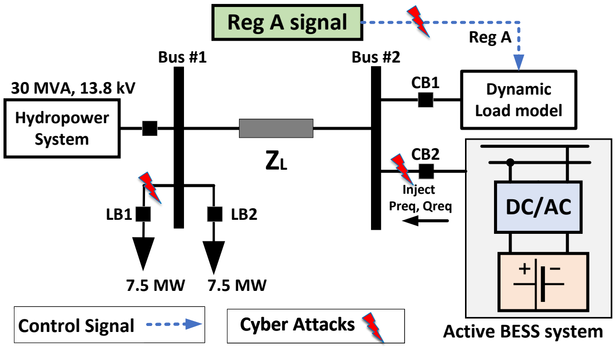


Fig. 3: System configuration

TABLE I: Scenarios for training and testing models

Cyberattacks	Parameters	Cases
Pulse attacks	duty cycle=[1, 2, 3] time period=[1, 2, 3, 4]	12
Ramp attacks	Slope=[1, 2, 3, 4] [-1, -2, -3, -4]	8
Scaling attacks	[-1, 1]	2
Load tripping	LB1	1
Line tripping	CB2	1

Note that we assumed that the battery had a sufficient power capacity to provide the required input response in a negligible ramping time. Further, we assigned $k = 10$ for the Reg A signal and $w = 7$ (70%) during this simulation. In this configuration, a dynamic PQ load model connected to bus 2 was assigned to mimic the required active power of the Reg A signal, and hydropower and battery provided output power, according to the calculated P_{ho} and P_{bi}.

1) Dataset generation

For generating datasets, we varied the total base load at bus 1 from 14 MW to 18 MW in a step increase of 0.2 MW to create 20 operating points while maintaining the balance of generation and load. During pulse attack, we considered a pulse signal with a unit magnitude with three duty cycles (1, 2, 3) and four time periods (1, 2, 3, 4). In case of ramp attack, four positive and negative ramping steps per second (slope) were considered to gradually increase or decrease the incoming Reg A signal. A load-tripping attack was simulated by disconnecting the circuit breaker, LB1, to remove 7.5 MW of load on bus 1. During a line-tripping attack, the battery was removed by disconnecting the circuit breaker, CB2, at bus 2. While utilizing these 24 cases (see Table I), we performed a binary classification with two labels: attack and normal. We created six labels for multiclassification that include normal operation, pulse attack, ramp attack, scaling attack, load tripping, and line tripping.

V. Results and Discussions

A. Detection Evaluation

We utilized the Python-based library Scikit-Learn and the TensorFlow platform for training and testing these machine learning algorithms. During binary classification (see Fig. 4) using 6,726 samples, we observed that the applied ANN showed a better performance with an accuracy of 96.17%, recall of 86.48%, precision of 97.86%, and F1 score of 91.10%. The RF and KNN showed a similar performance, with an accuracy of around 95.6% and F1 score of 90%. We also observed that the LR failed to detect cyberattacks during the testing phase and exhibited a poor performance with an accuracy of 85.69%, recall of 49.90%, precision of 42.91%, and F1 score of 46.14%. We also computed the fitting time during model training and prediction time during testing of these algorithms for binary classification (see Table II). Although the ANN takes a longer time, around 412 seconds, during model training, the computed prediction time is around 0.76 second/sample for the testing dataset. Note that the tested ANN model was trained for 100 epochs, consisted of 2 hidden layers with 128 neurons in each hidden, layer, with an initial learning rate set to 0.005.

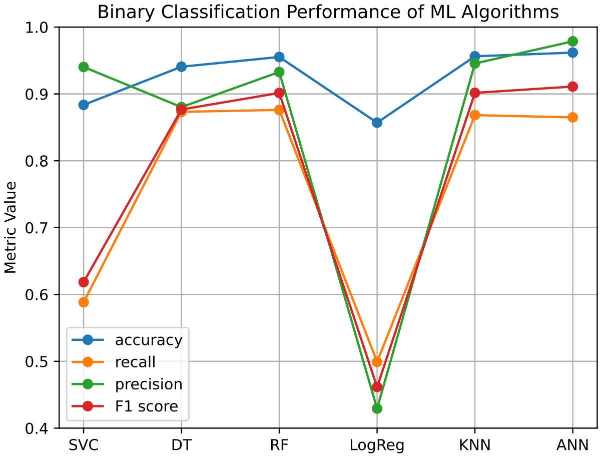


Fig. 4: Performance of machine learning during binary classification

During multiclass classification (see Fig. 5), the applied RF outperformed the other algorithms, especially ANN, with an accuracy of 82.39%, recall of 79.27%, precision of 84.25%, and F1 score of 81.50%. Note that the prediction time (see Table III) of the applied machine learning algorithms is within 1 second, except in the case of SVC, which is well within the timing requirement of Reg A signal coming every 2 seconds to the hydropower plant and BESS.

TABLE II: Processing time during binary classification

Time (sec)	ANN	KNN	RF	DT	SVC	LR
Prediction Time	0.764	0.243	.41	0.003	7.55	0.005
Fitting Time	411.82	0.058	13.42	0.12	96.16	1.976

B. Mitigation Evaluation

In the period prior to the attack, we observed that the hydropower and battery systems were able to provide the required input power response based on the incoming Reg A signal. In this case, data integrity attacks were initiated at the 238th second, and the RBMS was triggered in the next cycle (240th second). Fig. 6 shows the performance of RBMS during pulse, ramp, and scale attacks for a short-term duration of 14 seconds, between the 238th and 262nd seconds. In this case, we applied short-term mitigation, as we assumed $\lambda = 15$ seconds and the duration of attacks was within the defined threshold. In this scenario, the computed sliding average value ($l = 10$) was applied until the attack stopped at the 262nd second. This mitigation strategy minimized the transient instability that could be injected into the power grid due to these attacks.

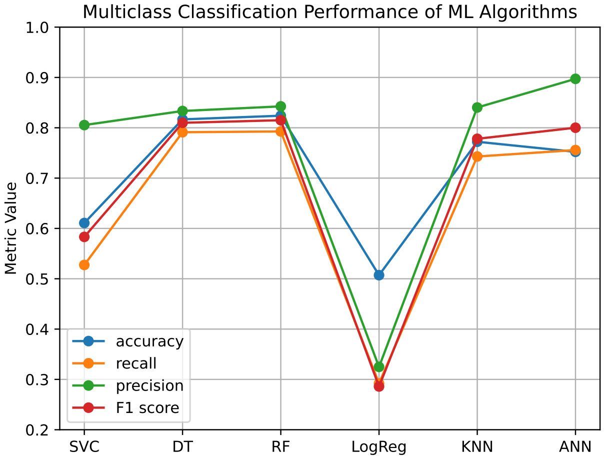


Fig. 5: Performance of machine learning during multiclass classification

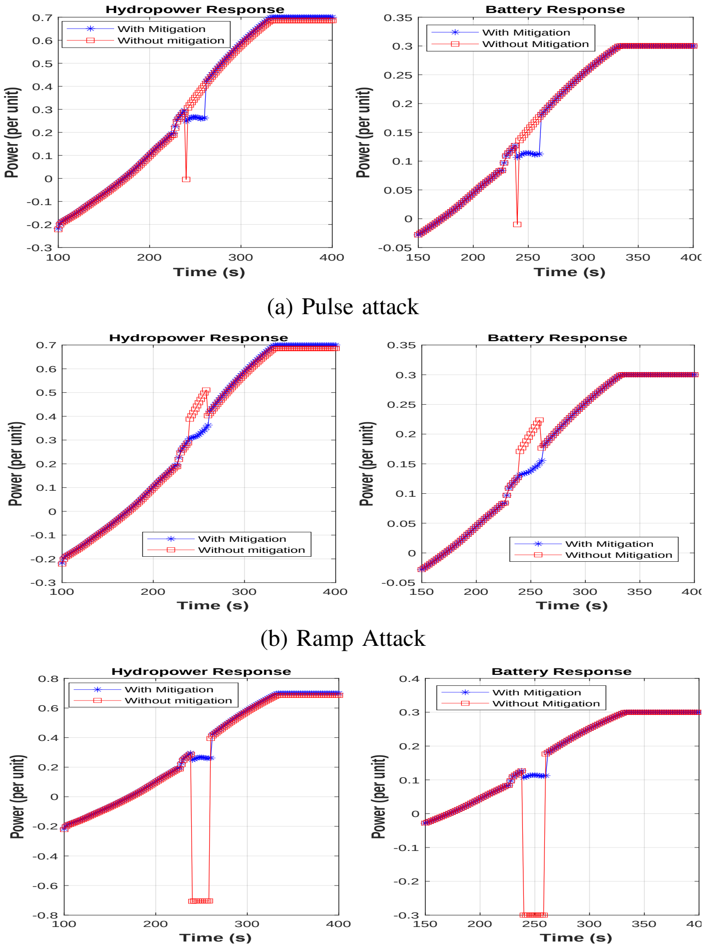
TABLE III: Processing time during multiclass classification

Time (sec)	ANN	KNN	RF	DT	SVC	LR
Prediction Time	0.594	0.29	0.5	0.0029	20.393	0.0054
Fitting Time	381.32	0.061	16.186	0.18	242.38	1.25

During the long-term scenario (see Fig. 7), these attacks continued throughout the simulation, exceeding the defined λ. In this case, hydropower and battery provided the same responses initially, as discussed in the previous scenario, and later switched to a local mode after the 262nd second and did not provide any output response to the incoming Reg A signal. Without mitigation, both hydropower and battery followed the compromised Reg A signal that can affect the reliability and economics of localized generation resources.

VI. Conclusion

This paper presented the machine-learning-based anomaly detection system and RBMS to address data integrity attacks during the participation of a hydropower-integrated battery system in the PJM-based frequency regulation market. This research does not include existing security measures employed by PJM to counter these attacks. The proposed anomaly detector utilizes incoming measurements from a plant facility to train different machine learning algorithms for both binary and multiclass classifications and identify different types of cyberattacks. The applied RBMS offers short-term and long-

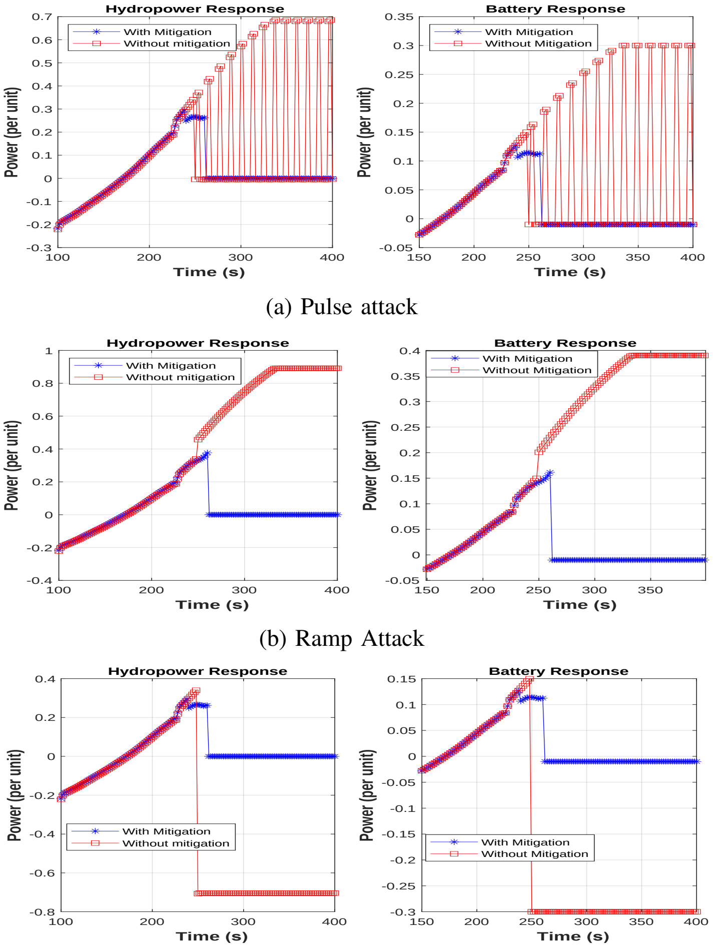


(a) Pulse attack

(b) Ramp Attack

(c) Scale Attack

Fig. 6: Mitigation against pulse, ramp, and scale attacks for short-term duration



(a) Pulse attack

(b) Ramp Attack

(c) Scale Attack

Fig. 7: Mitigation against pulse, ramp, and scale attacks for long-term duration

term mitigation actions tailored to the duration of applied data integrity attacks. Simulation-based testing and evaluation showed that the applied ANN showed a better performance during binary classification; however, for multiclass classification, RF proved to be the more efficient choice. The integrated mitigation strategies effectively minimize transient system instability during cyberattacks, ensuring that the hydropower and BESS are no longer able to participate in the regulation market during prolonged data integrity attacks on incoming regulation signals. Future efforts include: (1) testing the proposed methodology in a large-scale power system to further evaluate its efficiency, and (2) applying unsupervised approaches to detect unknown attacks and advanced persistent threats in the grid network.

References

[1] T. Wang, "Battery assisted conventional generator in pjm frequency regulation market," *2019 IEEE Power & Energy Society General Meeting (PESGM)*, pp. 1–5, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:210992800

[2] PJM, "Ancillary services." [Online]. Available: https://www.pjm.com/markets-and-operations/ancillary-services.aspx

[3] P. Interconnection, "Jetstream guide dnp scada over internet with tls security," 11 2022. [Online]. Available: https://www2.pjm.com/-/media/etools/jetstream/jetstream-guide.ashx

[4] K. D. Ham, C. R. Eppinger, D. E. Thorsen, C. Powell, P. A. Boyd, A. Somani, M. Ingram, and V. S. Koritarov, "Hydropower cyber-physical configurations." [Online]. Available: https://www.osti.gov/biblio/1893701

[5] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104–3113, 2015.

[6] V. K. Singh and M. Govindarasu, "A cyber-physical anomaly detection for wide-area protection using machine learning," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3514–3526, 2021.

[7] M. V. Whyatt, D. E. Thorsen, M. D. Watson, K. D. Ham, P. A. Pederson, A. D. McKinnon, and K. R. DeSomber, "Toward a resilient cybersecure hydropower fleet: Cybersecurity landscape and roadmap 2021." [Online]. Available: https://www.osti.gov/biblio/1899145

[8] R. Kumari and T. R. Chelliah, "Impact analysis of sensor cyber-attacks on grid-tied variable speed hydropower plants," *IEEE Transactions on Industry Applications*, pp. 1–10, 2023.

[9] V. Mladenov, V. Chobanov, P. Sarigiannidis, P. I. Radoglou-Grammatikis, A. Hristov, and P. Zlatev, "Defense against cyber-attacks on the hydro power plant connected in parallel with energy system," in *2020 12th Electrical Engineering Faculty Conference (BulEF)*, 2020.

[10] V. K. Singh, A. Banerjee, S. M. Shafiul Alam, and T. M. Mosier, "Dynamic frequency regulation improvement in hydropower-hybrid system using variational mode decomposition," in *2022 IEEE/PES Transmission and Distribution Conference and Exposition (TD)*, 2022, pp. 1–5.

[11] M. Blonsky, H. V. Padullaparti, F. Ding, S. Veda, and U. O. of Electricity, "Opendss-wrapper (distribution system co-simulator with distributed energy resource controls)," 6 2021.