Machine Learning-based Cyber-Physical Anomaly Detection in Wide Area Voltage Control Systems

Burhan Hyder, *Student Member, IEEE*, Vivek Kumar Singh, *Member, IEEE*, Manimaran Govindarasu, *Fellow, IEEE*, and Reynaldo Nuqui, *Senior Member, IEEE*

2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) | 978-1-6654-3775-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISGT50606.2022.9817484

***Abstract*—Wide-area voltage control systems (WAVCS) are widely deployed in power grid to improve the voltage stability in transmission system using Flexible AC Transmission System (FACTS) devices. The WAVCS relies on wide-area measurement and control signals for closed-loop control of FACTS devices to improve the transient voltage stability in power grid in real-time. Since the WAVCS utilizes a cyber-layer communication during its normal operation, they are susceptible to cyber attacks from adversaries which can lead to a voltage collapse if the attacks go undetected and unmitigated. This paper proposes a supervised machine learning (ML)-based anomaly detection algorithm for detecting various stealthy cyber attacks in the context of WAVCS cybersecurity. In particular, a fuzzy logic-based wide-area controller, as proposed by the Bonneville Power Administration (BPA), is implemented on the Kundur's four machine two-area system that is integrated with a static var compensator (SVC) to improve voltage profile on sensitive buses. Later, different types of data integrity attacks, including pulse and ramp attacks, are considered on the wide-area measurement and control signals to analyze the performance of the proposed anomaly detector. Our experimental evaluation shows a promising performance with a high true-positive rate (more than 99%) and low false-negative rate (less than 1%) while exhibiting a small prediction time.**

***Index Terms*—Anomaly detection, FACTS, Fuzzy Logic Control, Machine Learning, wide-area voltage control system.**

I. Introduction

With the ever increasing demand of electric loads, reliable operation of the power grid faces new challenges everyday especially given the uncertain and extreme weather conditions and a shift from conventional power sources to the distributed energy resources (DERs). Voltage security is one of the most crucial areas of concern when it comes to reliable operation of the grid. The North American Electric Reliability Corporation (NERC) recommends the application of wide-area monitoring systems using the synchrophasor technology necessary to identify and prevent major voltage collapses [1]. This implies that wide-area voltage control systems (WAVCS), one of the critical applications within Wide-Area Control System (WACS), are now a priority for power utilities to control, protect, and ensure reliable operations of the bulk power system [2]. A wide variety of literature shows new and innovative techniques being adopted for achieving the goal of voltage stability and security in bulk power systems using wide-area monitoring and control [3]–[6].

The North American Transmission Forum (NATF) recommends use of FACTS devices, such as Static VAR Compensator and Static Synchronous Compensator (STATCOM) for improving voltage stability [7]. The WACS design and implementation, proposed in [5], using fuzzy-logic control for SVC is deployed in the North-Western region of the US power grid implying the use of FACTS devices for wide-area voltage control as feasible and pragmatic in the modern grid.

Since the WAVCS relies on the wide-area network (WAN) for monitoring and control, it is susceptible to cyber attacks that exploit the vulnerabilities in the system. Successful cyber attacks on these systems can be catastrophic and can lead to voltage collapse of the grid [8], [9]. It has, thus, become imperative to design, develop, and deploy defense-in-depth measures that can fend off stealthy cyber attacks when the traditional IT cybersecurity systems fail to do so. There is a plethora of work which deals with the cybersecurity of wide-area measurement, protection, and control (WAMPAC) systems in the smart grid [10]–[15] but only a few deal with the cybersecurity of wide-area voltage control systems. In [16], the authors propose a model-based temporal prediction method for detecting false-data injections in WAMCS.

In this paper, we propose an ML-based anomaly detection system (MLADS) for WAVCS. This paper contributes towards development of a data-driven algorithm for detecting stealthy cyber attacks in WAVCS. We develop a centralized fuzzy logic-based wide-area voltage control system (FL-WAVCS) on the modified two-area four-machine Kundur power system equipped with a static VAR compensator (SVC) using phasor measurement units (PMU). We carry out various stealthy cyber attacks on the measurement and control signals exploiting the attack surfaces to emulate anomalies in the system. Using datasets generated from the FL-WAVCS, we develop the proposed MLADS using supervised ML-algorithms with physics- and entropy-based feature extraction and compare its performance using various supervised ML-algorithms.

This paper is organized as follows: Section II shows the architecture and design of the WAVCS, Section III details the proposed algorithm, Section IV shows the experimental setup and performance evaluation, and Section V concludes the work.

II. FACTS-based WAVCS: Architecture & Design

A. System Architecture

In this section, we discuss a high-level system architecture, as shown in Fig. 1, of the fuzzy logic-based wide-area voltage control system (FL-WAVCS). It consists of a fuzzy logic controller (FLC) that receives phasor measurements from different sensitive buses and sends an optimal voltage setpoint (V_{ref}) every 0.2 seconds to the deployed static VAR compensator (SVC) device of rating 300 MVAR to inject or absorb reactive power as required to improve the voltage profile during disturbances. This architecture is implemented on

This work is funded in part by the US DOE Cybersecurity for Energy Delivery System program

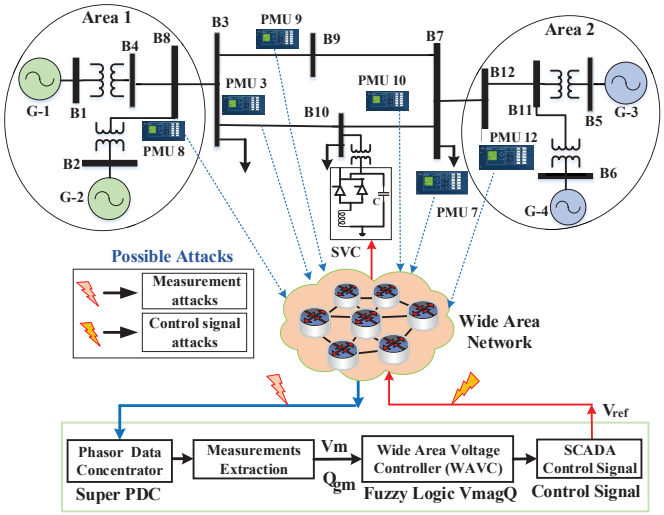

Fig. 1. High-level system architecture of WAVCS with its attack surfaces

the modified Kundur's four-machine two-area system, which consists of four generators, and an additional PQ load (60 MW, 30 Mvar) is connected to the bus 10 to create a voltage stress in the selected system. Fig. 1 also illustrates attack surfaces on measurement and control signals, as highlighted by lightning bolt symbols, that can be exploited to inject severe disturbances in the grid network. In our previous work [9], we assessed the impact of different data integrity attacks and also perform quantitative assessment using voltage profile index.

B. Design of FLC

We have developed a control center-based FLC, as discussed by the Bonneville Power Administration (BPA) [5], [6]. The design of this controller is discussed in several steps here.

Step 1 (Voltage stability analysis): For developing this controller, we have initially computed sensitive voltage nodes using the static voltage stability analysis [17] based on the Jacobian matrix, J, as shown in (1). ΔP and ΔQ represent the incremental changes in active and reactive powers. $\Delta\theta$ and ΔV are incremental changes in bus voltage angle and magnitudes. Assuming change in real power is zero, Q-V analysis can be performed using (2) and (3).

$$J = \begin{bmatrix} J_{P\theta} & J_{PV} \\ J_{Q\theta} & JQV \end{bmatrix} = \begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} \cdot \begin{bmatrix} \Delta\theta \\ \Delta V_{PQ} \end{bmatrix}^{-1} \tag{1}$$

$$\Delta Q = \left[J_{QV} - J_{Q\theta}.J_{P\theta}^{-1}.J_{PV}\right].\Delta V_{PQ} \tag{2}$$

$$\Delta Q = J_R.\Delta V_{PQ} \tag{3}$$

$$\Delta V = J_R^{-1}.\Delta V_{PQ} \tag{4}$$

For the given Kundur system, the computed reduced Jacobian matrix, J^{-1}, is a square matrix; and hence singlular value approach can be applied for the static voltage stability analysis. Fig. 2 illustrates the computed magnitude of the output singular vector for all buses for a maximum singular value of 0.135. Bus 10 represents the most sensitive node with a computed magnitude of 0.65734 and SVC is deployed

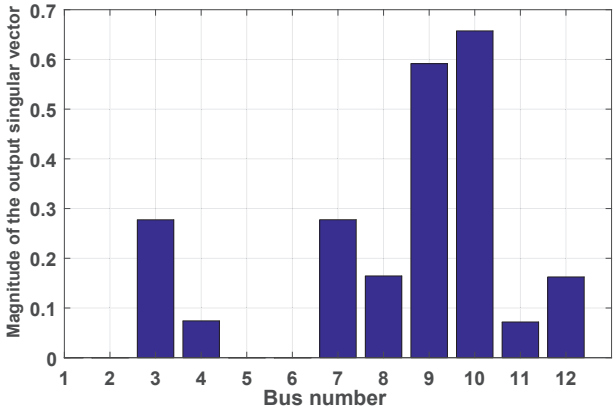

Fig. 2. Output singular vector plot for the static voltage stability analysis.

on this bus to improve the transient voltage stability during disturbances.

Step 2 (Apply VmagQ algorithm): We have applied the rules-based VmagQ algorithm [5] to calculate V_{ref} to the local SVC (FACTS) device. Fig. 3 illustrates the VmagQ

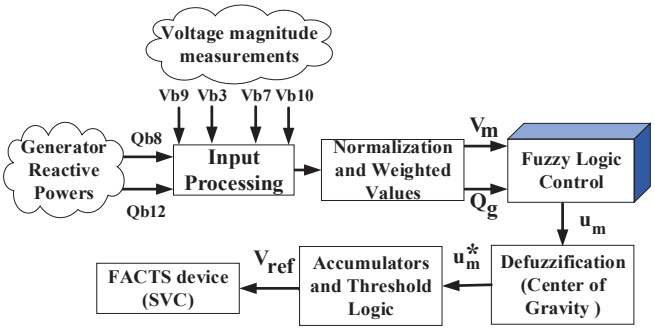

Fig. 3. VMagQ algorithm-based FLC scheme of FL-WAVCS

algorithm-based control scheme for FL-WAVCS. This algorithm utilizes voltage magnitude measurements (Vb9, Vb3, Vb7, and Vb10) of top four sensitive buses — bus 9, bus 3, bus 7, and bus 10, based on their rankings on the magnitude of the output singular vector. Also, reactive powers (Qb8 and Qb12) of area 1 and area 2 using bus 8 and bus 12 are considered for input features as they provide the accumulative power injection for these four sensitive buses. The overall scheme is categorized into four major stages.

Stage 1: Performs an input processing to validate input phasor signals and later compute V_m and Q_g as normalized and weighted values as input features for FLC. In this case, different weights for selected buses are assigned based on their magnitudes of output singular vector. We have performed offline analysis to compute weights of 0.58 to bus 8 and 0.42 to bus 12 for reactive power measurements based on the reactive power injection during physical disturbances.

Stage 2: Applies a set of fuzzy rules, as defined in [5], and provides an output u_m using membership functions. For example, if Q_g is positive large and V_m is low, then u_m is positive large so that SVC can inject more reactive power to improve voltage profile.

We have considered triangular membership functions, where isosceles triangle membership functions are applied for small

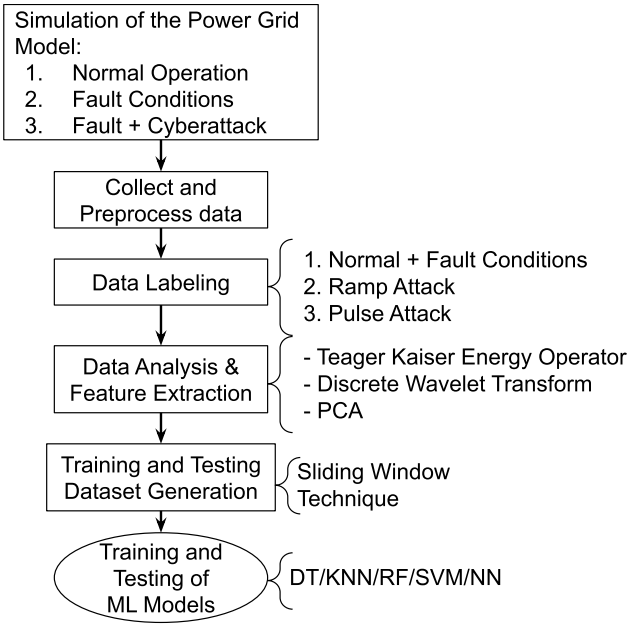

Fig. 4. Flowchart depicting MLADS Algorithm

and medium values and end functions are considered for large values while the output is residing between 1 to -1. Further, we have considered min-max logic during fuzzy inference where maximum value is selected when multiple rule conflicts the output variable.

Stage 3: The computed u_m is forwarded for defuzzification that produces a crisp output value u_m^* with domain ± 1 using the center of sums method [5].

Stage 4: Finally, V_{ref} is computed by re-scaling the output domain ± 1 to 0-1 range. Further manual tuning and testing is required to avoid frequent changes in output value, computing threshold logic for output updates, and analyze voltage profile for different V_{ref}.

III. Proposed ML-based Anomaly Detection System (MLADS)

Machine Learning algorithms are being extensively used for detection of anomalies in Cyber-Physical Systems (CPS) [18]. By making predictions, decisions, and classifications based on data, ML algorithms enable us to build models for applications that otherwise are challenging to design. We propose a ML-based Anomaly Detection System (MLADS) for accurate classification and detection of a broad range of anomalies that can exist in the WAVCS due to stealthy cyber attack injections. The essential components for building the MLADS include dataset generation, feature extraction from the generated dataset, and the ML algorithms for classification or regression. A flowchart depicting the MLADS algorithm is shown in Fig. 4.

A. Dataset Generation

Prior to creation of ML-based models, ensuring availability of sufficient data is vital for the design and optimal performance of any anomaly detector. In order to have enough data for highly accurate performance of the MLADS, we consider a combination of system faults and stealthy cyber-attack vectors for the dataset generation. Stealthy cyber-attacks are carried out on both measurement signals coming into the FLC from PMUs and control signals being forwarded by the FLC to the SVC over the wide-area network, as shown in Fig. 1. In particular, two types of data-integrity attacks are considered:

Ramp Attack: Ramp attack on the measurement or control signals involves either continuous increase or decrease of the amplitude of the signal being attacked by addition or subtraction of attack vector parameters, respectively, to the target signal. Ramp attack [19] involve adding a time-changing ramp signal with a ramp signal parameter, λ_{ramp} to the input signal, $P_i(t)$, as shown in (5).

$$P_{ramp}(t) = P_i(t) + \lambda_{ramp} \times t \tag{5}$$

Pulse Attack: Pulse attack on the measurement or control signals involves a usually high frequency (as compared to system frequency) pulse signal multiplication to the target signal, rapidly manipulating its magnitude. Pulse attack vector [19] periodically changes an input control signal, $P_i(t)$, by adding the pulse attack parameter, λ_{pulse}, for a small time interval, (t1) and retaining the $P_i(t)$ for a remaining interval, (T- t1), for the given time period, (T), as shown in (6).

$$P_{pulse} = \begin{cases} P_i(1 + \lambda_{pulse})(t = t_1) \\ P_i(t = T - t_1) \end{cases} \tag{6}$$

Appropriate adjustment of the parameters of the aforementioned attack vectors enable cyber attackers to bypass the conventional bad-data detectors. In order to generate a wide variety of data integrity attacks on the measurement and control signals, we use the combination of a wide range of parameters of the ramp and pulse signal attacks in addition to simulating system faults in the two-area Kundur system. These parameters will be discussed in more detail in the next section. Moreover, the impact analysis of these stealthy cyber attacks on the given system have been studied in [9].

Since MLADS uses supervised ML algorithms for detection of anomalies, the next stage after the collection of data from attack and fault simulations is labeling of the data. The labeling stage involves assignment of tags to each data point in the generated dataset for the corresponding event in the power system.

B. Feature Extraction

Appropriate feature extraction and selection from the raw dataset is an effective way of increasing efficiency and accuracy of trained ML-models [20]. For the purpose of accurately distinguishing cyber attacks from system faults and normal operation, it becomes necessary to extract physics- and entropy-based features apart from using the raw data. MLADS uses two such feature vectors extracted for each data point in the generated dataset to improve the accuracy of anomaly detection:

Discrete Wavelet Transform (DWT): This feature allows for accurate and fast decomposition of the given signals in the frequency domain both for short-period frequency components (transients) and for long-period frequency components (fundamental and harmonics). Such a decomposition is very

TABLE I
ATTACK VECTOR INJECTION PARAMETERS

Attack Vector	Parameters
Pulse Attack (Measurement & Control)	Duty Cycle (%) = [30, 50, 80] Period = [0.5, 1, 1.5, 2] Amplitude = 1 Start Time (seconds) = [4, 10]
Ramp Attack (Measurement & Control)	Slope = [1, 2, 3, 4, 5] Start Time (seconds) = [4, 10]
Fault Type	**Fault Duration**
L-L-L (A-B-C) at B9	Start Time (seconds) = 8 End Time (seconds) = 8.2

efficient in differentiation between short- and long-term faults and normal operation [21].

Teager Kaiser Energy Operator (TKEO): This feature represents instantaneous energy of the signal at any point of time and, thus, allowing for an accurate segregation of normal operation, fault, and attack scenarios where the instantaneous energy can differ significantly [14].

Post feature extraction, *Principal Component Analysis (PCA)* is carried out on the feature dataset. PCA helps in dimensionality reduction of the feature dataset by giving higher weightage to the highly uncorrelated features present in the data which explain majority of the variance (e.g. $> 95\%$ variance) in the output, thus, reducing the computational burden of the algorithm being used [22].

C. ML Algorithms

Once the dataset is generated with extracted features and PCA, training and testing datasets are extracted from this dataset for training and testing different ML algorithms, respectively. The proposed MLADS uses supervised ML algorithms for classification and detection of anomalies in the FL-WAVCS. Using the training dataset, multiple algorithms including Support Vector Machine (SVM), K-Nearest Neighbour (KNN), Decision Tree (DT), Neural Network (NN), and Random Forest (RF) algorithms are trained using the training dataset. The performance of these algorithms is compared using the test dataset. For the purpose of creating training and testing datasets, we use the sliding window technique in order to aggregate multiple data points from the originally generated time-series dataset which allows for improved performance of these algorithms. The sliding window technique aggregates multiple data points together based on the selected window size and uses a first-in first-out method to include the latest data point in the window while removing the oldest data point.

IV. EXPERIMENTAL SETUP AND PERFORMANCE EVALUATION OF THE MLADS

This section describes the (i) modeling platforms and parameters used for simulating the fuzzy logic controller-based wide-area voltage control system using SVC; and (ii) Performance evaluation of the proposed ML-based anomaly detection system comparing various ML algorithms.

A. FL-WAVCS Model Simulation for Dataset Generation

The two-area four-machine Kundur power system is implemented on OPAL-RT, a real-time digital simulator, using its ARTEMiS library which allows faster simulations at time-steps of the order of a few microseconds which is necessary for simulating the FACTS device (SVC) model. The simulation (refer to Fig. 1) includes a 3-Phase-to-Phase fault on one of the inter-tie buses (B9) and ramp and pulse attacks with varying parameters on the measurement signals from the PMUs and control signal sent to the SVC from the FLC. Various parameters for the attack vector injection are depicted in Table I. The dataset generated consists of 4 bus voltage magnitude signals ($Vb9$, $Vb3$, $Vb7$, and $Vb10$), 2 reactive power flow measurements ($Qb8$ and $Qb12$), $2 * 6$ (12) coefficients of TKEO, and $2 * 6$ (12) coefficients of DWT. The complete feature dataset thus consists of 30 features. For dimensionality reduction, we conduct PCA on the feature dataset which retained 16 features (explaining 99% variance) that are used for generating the training and testing datasets. The complete dataset contains 3.35 $Million$ data points. The training and testing datasets have 70% and 30% of the data points from the complete dataset, respectively, which are split randomly. The training and testing is performed in a MATLAB environment (Classification Learner App) on a Microsoft Windows Server 2016 with Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz, 4 Cores and 32 GB RAM.

B. Performance evaluation of the MLADS

Table II shows the performance comparison of the four ML algorithms in terms of overall accuracy, true positive rates (TPR) for each class, training time, and prediction time. The overall accuracy is the overall percentage of observations that are correctly classified for all classes, the TPR is the proportion of correctly classified observations per true class, the training time is time taken for the algorithm to train using the training dataset, and the prediciton time is the time taken by the trained algorithm to classify test data. We have defined three classes or labels for the dataset used: (i) **Label-1** defines *Normal Operation* and/or *System Fault*; (ii) **Label-2** defines *Pulse Attack* on eihter the measurement or the control signals; and (iii) **Label-3** defines *Ramp Attack* on the measurement or control signals. Evidently, the fine KNN algorithm outperforms the other algorithms that have been tested, namely, Support Vector Machine (Fine Gaussian SVM), Decision Tree (Fine DT), 3-layered Neural Network (NN), and Random Forest (RF). We have also shown detailed results for the Fine KNN algorithm. Table. III shows the Confusion Matrix for Fine KNN with the total number of correctly and incorrectly classified observations from the test dataset with an overall accuracy of 99.99%. Table. IV shows the TPR and the False Negative Rate (FNR) for Fine KNN for each class as is summarized in Table II as well. A 100% TPR for **Label-1** in case of Fine KNN shows that the algorithm has no false negatives in terms of classifying and detecting anomalies (i.e., 100% detection accuracy). The negligible inaccuracy ($\sim$ 0.04%) in classification for this algorithm exists only within the correct classification of the type of attack within the dataset (**Label-2** and **Label-3**), highlighting the highly accurate attack detection performance of Fine KNN.

TABLE II
PERFORMANCE COMPARISON OF VARIOUS ML ALGOTRITHMS

Algorithm	Overall Accuracy	TPR - 1	TPR - 2	TPR - 3	Training Time(sec)	Prediction Time (obs/sec)
Fine KNN	99.99%	100.0%	99.96%	100.0%	44.58	∼330000
Fine Gaussian SVM	94.1%	99.9%	90.3%	85.9%	19112	∼350
Fine DT	91.3%	99.7%	84.3%	82.1%	23.42	∼530000
NN	90.9%	100.0%	78.4%	83.7%	4775.1	∼880000
RF	87.7%	99.1%	48%	90.9%	247.58	∼100000

TABLE III
CONFUSION MATRIX FOR FINE KNN

True↓ /Predicted →	Label-1	Label-2	Label-3
Label-1	503415	0	0
Label-2	0	179979	74
Label-3	0	10	324118

TABLE IV
TPR AND FNR FOR FINE KNN FOR ALL THREE CLASSES

	Label-1	Label-2	Label-3
TPR	100.0%	99.96%	100.0%
FPR	0.0%	0.04%	0.0%

V. CONCLUSION AND FUTURE WORK

This paper proposed a supervised machine learning (ML)-based anomaly detection algorithm for detecting various stealthy cyber attacks on the WAVCS. For the dataset generation and validation of the algorithm, a Fuzzy Logic Controller (FLC)-based wide-area control scheme on a two-area four-machine Kundur power system equipped with a Static VAR Compensator (SVC) was considered. Different types of stealthy data integrity attack vectors were simulated on this model including pulse and ramp attacks on both measurement and control signals to analyze the performance of the proposed anomaly detection algorithm. Performance of various supervised ML algorithms were compared for classification of anomalies. The experimental results showed high detection accuracy (100%) and TPR ($> 99.9\%$) for anomaly detection and classification using the Fine KNN algorithm. This work serves as a preliminary step towards implementation of MLADS in a real-time environment for anomaly detection and mitigation for the WAVCS. The future work includes implementation of the MLADS module in a quasi-realistic WAVCS environment on the PowerCyber Testbed at the Iowa State University [23] with industry grade communication protocols like DNP3 and IEEE C37.118 over a wide-area network. This would allow for real-time red team testing of the proposed algorithm with real-world attack injections, allowing for validation of the algorithm for field deployment in the near future.

REFERENCES

[1] M. Patel, S. Aivaliotis, E. Ellen and et al, "NERC Real-Time Application of Synchrophasors for Improving Reliability," 2010. [Online]. Available: https://www.naspi.org/reference-documents

[2] M. Perron, E. Ghahremani, A. Heniche, I. Kamwa, C. Lafond, M. Racine, H. Akremi, P. Cadieux, S. Lebeau, and S. Landry, "Wide-area voltage control system of flexible ac transmission system devices to prevent voltage collapse," *IET Generation, Transmission & Distribution*, vol. 11, no. 18, pp. 4556–4564, 2017.

[3] A. S. Musleh, S. M. Muyeen, A. Al-Durra, and H. M. Khalid, "Pmu based wide area voltage control of smart grid: A real time implementation approach," in *IEEE ISGT - Asia*, 2016.

[4] A. Ashrafi and S. M. Shahrtash, "Dynamic wide area voltage control strategy based on organized multi-agent system," *IEEE Transactions on Power Systems*, vol. 29, no. 6, pp. 2590–2601, 2014.

[5] C. Taylor, D. Erickson, K. Martin, R. Wilson, and V. Venkatasubramanian, "Wacs-wide-area stability and voltage control system: R amp;d and online demonstration," *Proceedings of the IEEE*, vol. 93, 2005.

[6] R. Wilson and C. Taylor, "Using dynamic simulations to design the wide-area stability and voltage control system (wacs)," in *IEEE PES Power Systems Conference and Exposition*, 2004, pp. 100–107 vol.1.

[7] North American Transmission Forum (NATF), "Transient Voltage Criteria Reference Document," 2016. [Online]. Available: https://www.natf.net/documents

[8] B. Chen, K. L. Butler-Purry, S. Nuthalapati, and D. Kundur, "Network delay caused by cyber attacks on svc and its impact on transient stability of smart grids," in *IEEE PES General Meeting*, 2014.

[9] V. K. Singh, M. Govindarasu, and R. Nuqui, "Impact analysis of data integrity attacks on facts-based wide-area voltage control system," in *IEEE PES ISGT*, 2021.

[10] 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.

[11] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE*, vol. 105, pp. 1389–1407, 2017.

[12] B. Chen, S.-i. Yim, H. Kim, A. Kondabathini, and R. Nuqui, "Cybersecurity of wide area monitoring, protection, and control systems for hvdc applications," *IEEE Transactions on Power Systems*, vol. 36, 2021.

[13] M. Chenine, J. Ullberg, L. Nordström, Y. Wu, and G. N. Ericsson, "A framework for wamcs interoperability and cybersecurity analysis," *IEEE Transactions on Power Delivery*, 2014.

[14] G. Ravikumar and M. Govindarasu, "Anomaly detection and mitigation for wide-area damping control using machine learning," *IEEE Transactions on Smart Grid*, pp. 1–1, 2020.

[15] V. K. Singh and M. Govindarasu, "A novel architecture for attack-resilient wide-area protection and control system in smart grid," in *2020 Resilience Week (RWS)*, 2020, pp. 41–47.

[16] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in wamcs applications," *IEEE Systems Journal*, vol. 13, pp. 710–719, 2019.

[17] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.

[18] F. S. Mozaffari, H. Karimipour, and R. M. Parizi, *Learning Based Anomaly Detection in Critical Cyber-Physical Systems*. Cham: Springer International Publishing, 2020, pp. 107–130.

[19] V. K. Singh, E. Vaughan, J. Rivera, and A. Hasandka, "Hides: Hybrid intrusion detector for energy systems," in *2020 IEEE Texas Power and Energy Conference (TPEC)*, 2020, pp. 1–6.

[20] S. Singh and S. Silakari, "An ensemble approach for feature selection of cyber attack dataset," *CoRR*, vol. abs/0912.1014, 2009. [Online]. Available: http://arxiv.org/abs/0912.1014

[21] T. S. Abdelgayed, W. G. Morsi, and T. S. Sidhu, "Fault detection and classification based on co-trainingofsemisupervisedmachine learning," *IEEE Transactions on Industrial Electronics*, vol. 65, 2018.

[22] S. Wold, K. Esbensen, and P. Geladi, "Principal component analysis," *Chemometrics and Intelligent Laboratory Systems*, 1987.

[23] G. Ravikumar and M. Govindarasu, "On-Premise Cloud-based HIL CPS Security Tesbted for Smart Grid," 2020. [Online]. Available: https://powercybertestbed.ece.iastate.edu/