This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2020.2995313, IEEE Transactions on Smart Grid

Anomaly Detection and Mitigation for Wide-Area Damping Control using Machine Learning

Gelli Ravikumar, *Member, IEEE*, and Manimaran Govindarasu, *Fellow, IEEE*

***Abstract*—In an interconnected multi-area power system, wide-area measurement based damping controllers are used to damp out inter-area oscillations, which jeopardize grid stability and constrain the power flows below to their transmission capacity. The effect of wide-area damping control (WADC) significantly depends on both power and cyber systems. At the cyber system layer, an adversary can inflict the WADC process by compromising either measurement signals, control signals or both. Stealthy and coordinated cyber-attacks may bypass the conventional cybersecurity measures to disrupt the seamless operation of WADC. This paper proposes an anomaly detection (AD) algorithm using supervised Machine Learning and a model-based logic for mitigation. The proposed AD algorithm considers measurement signals (input of WADC) and control signals (output of WADC) as input to evaluate the type of activity such as *normal*, *perturbation* (small or large signal faults), *attack* and *perturbation-and-attack*. Upon anomaly detection, the mitigation module tunes the WADC signal and sets the control status mode as either wide-area mode or local mode. The proposed anomaly detection and mitigation (ADM) module works inline with the WADC at the control center for attack detection on both measurement and control signals and eliminates the need for ADMs at the geographically distributed actuators. We consider coordinated and primitive data-integrity attack vectors such as *pulse*, *ramp*, *relay-trip* and *replay* attacks. The performance of the proposed ADM algorithms was evaluated under these attack vector scenarios on a testbed environment for 2-area 4-machine power system. The ADM module shows effective performance with 96.5% accuracy to detect anomalies.**

***Index Terms*—Anomaly detection, oscillations, PMU, Machine Learning, wide-area damping control and measurement system.**

I. Introduction

THE electromechanical low-frequency oscillation (LFO) modes [1], a manifestation of relative movement of rotor angle position of generators [2], in an interconnected multi-area power system affect the system stability margins and impose constraints on the inter-tie power transfer capability. Typically, there are two significant sets of LFO modes (frequency components) present in the multi-area power systems, which are inter-area oscillation (IAO) modes ($0.1-1\ Hz$) and local modes ($1-2\ Hz$). In addition to the traditional damping torque analysis and modal analysis, various model-based deterministic and measurements-based probabilistic methods have been developed for oscillation modal analysis and robust controller designs for damping LFO modes [2]–[7]. It is evident from these techniques that local measurement system based actuators provide effective damping to the local oscillation modes as they constrained (limited) to local modal observability [8] whereas the wide-area measurement system (WAMS) based actuators provide effective damping to the IAO modes as they have global modal observability.

The wide-area damping control (WADC) is one of the critical wide-area control system (WACS) applications in modern power systems. A wide-area damping controller, typically located at the control center, synthesizes a set of remote measurement signals to generate WADC signals to dispatch to the geographically distributed actuators. The performance of WACS applications significantly depends on the dynamics of both power and cyber systems.

The significant challenges to design WADC application include selection of wide-area measurements and actuators that receive wide-area control signals to modulate the power system components such as generators, high voltage DC transmission (HVDC) devices [9]–[12] and flexible AC transmission system (FACTS) devices [12]. The dynamics due to the cyber systems on the WADC application include quality of services (QoS) such as low latency, less packet-drop and high reliability. In addition to these system dynamics, the stochastic nature of cyber-attacks on both power and cyber systems may severely impact the performance of WACS applications such as WADC, which may endanger power system operations and affect grid stability. Stealthy and coordinated cyber-attack vectors may bypass the conventional cybersecurity measures to disrupt the seamless operation of WACS applications. Adversaries deploy these cyber-attack vectors to modify the compromised data channels (either measurement signals, control signals or both), which manifests the cyber-attack anomalies to the actual data, of the WACS applications. Therefore, it is essential to build an attack-resilient system, which can detect, mitigate and prevent the cyber-attack anomalies, for the WACS applications.

Recently, HVDC-based WADC system is designed and demonstrated [9]–[11] for the Pacific DC Intertie (PDCI) in the North American Western Interconnection (WI). The controller prototype synthesizes real-time synchrophasor feedback signals to generate a control signal that modulates the parallel Pacific HVDC Intertie to damp Pacific AC Intertie (PACI) oscillations. The China Southern and Central Grids (CSG and CCG) have established a centralized adaptive WADC system that modulates multiple HVDC systems to damp out dominant IAO modes exhibiting in the range of 0.3 Hz and 0.8 Hz [13]–[15]. On the other hand, the cyber-attacks on the Ukrainian power grid [16] witness that adversaries can take control of SCADA systems to inflict the system operation. It shut down the power supply for more than 200,000 consumers. Therefore, it is crucial to consider the attack resiliency for the secure operation of the wide-area control system, which is sensitive to the cyber-attacks, particularly the data-integrity attacks.

Gelli Ravikumar and Manimaran Govindarasu are with the Department of Electrical and Computer Engineering, Iowa State University, USA. (e-mail: gelli@iastate.edu and gmani@iastate.edu)

Over the recent decade, there has been an extensive research on off-line-based AD [17], [18] and ML-based online AD using the synchrophasor measurements to detect anomalies on the frequency, voltage, power oscillations [19]–[22]. All of these detection methods monitor synchrophasors on the measurement-signal segment, which limits the scope to the wide-area monitoring and measurement system based applications. The cyber-physical control system of the power grid includes attack surface on both measurement-signal and control-signal segments. Therefore, it is required to build an attack-resiliency for WACS applications such as WADC against both the attack surface segments. On the other hand, various resilient wide-area control designs have been developed against cyber system events such as communication failures and delay tolerance [23]–[28]. These methods are limited to modeling cyber system events under the control system perspective to achieve resiliency for WADC system operation. Therefore, there is a substantial need to develop models and algorithms for attack-resilient WACS operation against stealthy cyberattacks on both measurement-signal and control-signal segments.

In this paper, we propose, an attack-resilient wide-area damping control system using Machine Learning-based anomaly detection and model-based mitigation (ADM) algorithms executed in a control center environment.

Contribution: The ***key*** contributions of our research are:

- Propose an anomaly detection (AD) algorithm using supervised Machine Learning and Model-based mitigation.
- Propose physics-based and signal-entropy based feature extraction to increase the detection accuracy and robustness of the trained ML model.
- Propose a combined power system operating conditions and cyberattack events-based dataset generation model using parallel execution approach so that to use for any large-scale power grid models.
- Testbed-based demonstration using hardware-in-the-loop (HIL) WADC integrated with ADM for a cyber-physical closed-loop test power system.

The paper is organized as follows: Section II elucidates the proposed approach for the attack-resilient WADC system. Sections III proposes the anomaly detection using Machine Learning (ML) and a suitable mitigation technique. Section IV demonstrates and evaluates the proposed ADM for the WADC application.

II. Proposed Framework for the AR-WADC System

A schematic diagram of the proposed ADM methodology for the attack-resilient WADC (AR-WADC) system is shown in Fig. 1. The geographically distributed PMUs compute the synchrophasor measurements from the current transformers (CTs) and potential transformers (PTs) and transfer them to the configured local and super phasor data concentrators (PDCs). The local PDCs are typically deployed at the substations when they comprise of multiple PMUs whereas the super PDCs operated at the control centers for the collection of synchrophasors from the system-wide PMUs and PDCs. The suitability of existing synchrophasor networks [29] can be configured based on the time-critical wide-area applications and the quality of services (QoS) such as low latency, high bandwidth, and less packet-drop. We use the IEEE-C37.118 protocol for the synchrophasor data communication, and the DNP3 and IEC-61850 protocols for the SCADA data and control signal communication across the control center, actuators, intelligent electronic devices (IEDs) and remote terminal units (RTUs).

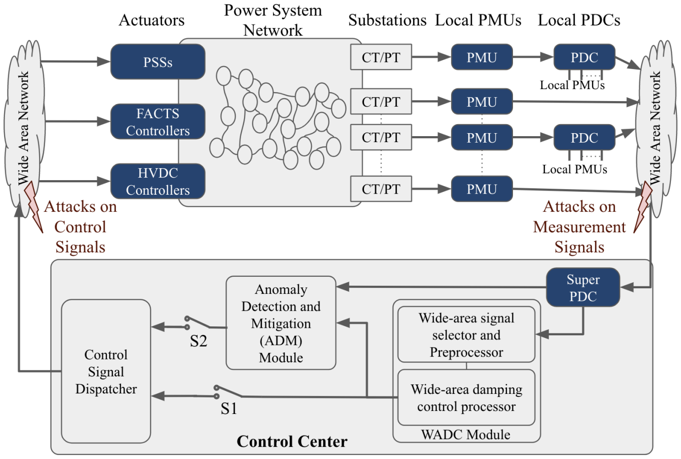
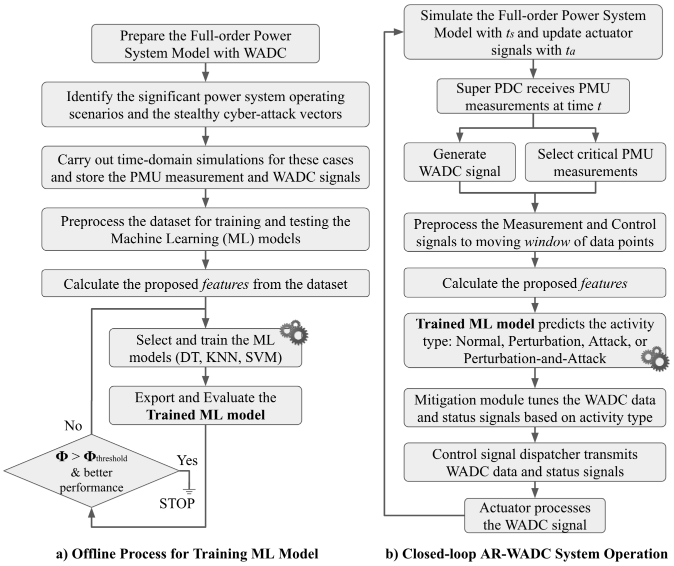


Fig. 1. Schematic Diagram for Proposed Attack-Resilient WADC System

It is inevitable that the adequate damping of IAO by the WADC system significantly depends on the selection of wide-area input measurements, actuators, and the latency. Various approaches have been devised to build robust and delay-tolerant WADC system for ensuring better performance during the high-latency scenarios. However, besides to the typical cyber-attacks like malware-based and denial-of-service (DoS)-based, adversaries can deploy stealthy and coordinated data-integrity cyber-attack vectors such as *Pulse-attacks*, *Ramp-attacks* and *Switching-attacks* on the measurement signals, control signals or both. These can severely affect the operation of the WADC system. Further, it may also lead to system instability with the effect of negative damping. This paper proposes an AR-WADC system operation by the integration of the Machine Learning and model-based ADM to the WADC processor as shown in Fig. 1. The S_1 or S_2 switch operates WADC system without or with ADM respectively.

The Fig. 2 shows the two phases of the proposed AR-WADC operation. The first phase includes the training of ML model that detects cyber-attack anomalies, and the second phase comprises of its integration with the WADC and mitigation techniques in the closed-loop system operation. The proposed ADM module processes both the WADC signal and the wide-area measurements received from the super PDC. In the closed-loop AR-WADC system operation, the anomalies of the compromised measurement signals appear on the current cycle whereas the next cycle for the compromised control signals. The ADM module includes trained ML model to detect the activity type such as normal, perturbation (voltage perturbations at generators or faults), attack and attack-and-perturbation. If it detects cyber anomalies, then the mitigation sub-module modifies the WADC signal and sets the WADC status mode to 0. The control signal dispatcher (CSD) sends


Prepare the Full-order Power System Model with WADC
Identify the significant power system operating scenarios and the stealthy cyber-attack vectors
Carry out time-domain simulations for these cases and store the PMU measurement and WADC signals
Preprocess the dataset for training and testing the Machine Learning (ML) models
Calculate the proposed features from the dataset
Select and train the ML models (DT, KNN, SVM)
Export and Evaluate the Trained ML model
No
Φ > Φthreshold & better performance
Yes
STOP
Simulate the Full-order Power System Model with ts and update actuator signals with ta
Super PDC receives PMU measurements at time t
Generate WADC signal
Select critical PMU measurements
Preprocess the Measurement and Control signals to moving window of data points
Calculate the proposed features
Trained ML model predicts the activity type: Normal, Perturbation, Attack, or Perturbation-and-Attack
Mitigation module tunes the WADC data and status signals based on activity type
Control signal dispatcher transmits WADC data and status signals
Actuator processes the WADC signal

a) Offline Process for Training ML Model **b) Closed-loop AR-WADC System Operation**

Fig. 2. Proposed Methodology for Training ML model for Anomaly Detection and Closed-loop AR-WADC System Operation with ADM

both the control and status data to the wide-area actuator, which operates if the status mode set to 1. We consider designing the status signal besides the control data to set the operation of the actuator from the wide-area mode to local-mode or off. It plays an essential role to prevent the penetration of anomalies due to the compromised control signals to the wide-area actuators.

III. Proposed Anomaly Detection using ML

Machine Learning (ML) has evolved from the study of pattern recognition [30] and has explored for the construction of algorithms that utilizes data to learn and build models. These trained ML models overcome the static program instructions by making data-driven predictions, decisions, and classifications. We use ML algorithms to build trained models where it is infeasible or difficult to design algorithms explicitly for the data-driven applications. For instance, the detection of network intruders, stochastic nature of cyber-attack anomalies, recognition of patterns and computer vision. The essential modules to build trained models include dataset preparation, extraction of features from the dataset and the ML algorithms. Fig. 3 shows the systematic process of these three modules for building a trained ML model. Feature selection is essential in the ML algorithm to improve detection accuracy and eliminate inappropriate attributes. The following subsections discuss proposed robust set of feature vectors and a systematic method for the generation of the dataset including power system and cyber-attack events. Further, it discusses trained ML models using supervised ML algorithms [31] and demonstrate their accuracy for a power system using hardware-in-the-loop synchrophasor cyber-physical system (CPS) security testbed.

A. Preparation of Dataset Models

The dataset includes synchrophasor measurement data for various power system operating conditions (α_{psoc}) including perturbations and cyber system attack events (β_{csae}). A generic

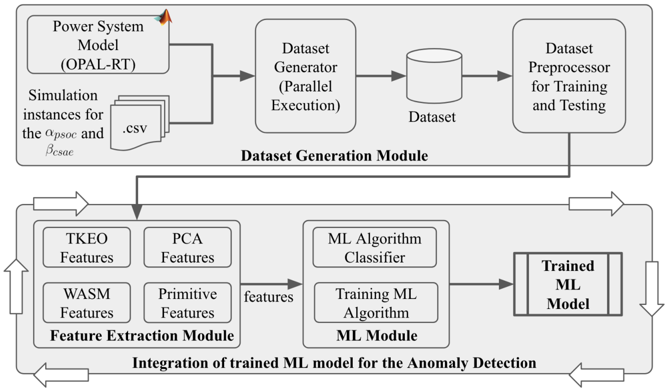

Power System Model (OPAL-RT)
Simulation instances for the α_{psoc} and β_{csae}
.csv
Dataset Generator (Parallel Execution)
Dataset
Dataset Preprocessor for Training and Testing
Dataset Generation Module
TKEO Features
PCA Features
WASM Features
Primitive Features
features
Feature Extraction Module
ML Algorithm Classifier
Training ML Algorithm
ML Module
Trained ML Model
Integration of trained ML model for the Anomaly Detection

Fig. 3. Proposed Anomaly Detection System using Machine Learning

configuration of the cyber-physical system (CPS) of WACS includes actuators, PMUs, cyber network devices and WACS application modules located at the control center as articulated in Fig. 1. We consider the CPS of WACS applications to prepare the dataset for training and testing the proposed ADM using ML. The performance of the ML relies significantly on the abundant dataset whereas it is important to observe the absence of a practical dataset comprising α_{psoc} and β_{csae}. Therefore, it is inevitable to devise a systematic methodology to generate the CPS dataset through a set of simulations. The dataset comprising of α_{psoc} and β_{csae} for a considered network is defined as follows:

$$Dataset = D = f(\alpha_{psoc}, \beta_{csae}) \tag{1}$$

$$\alpha_{psoc} = \{\alpha_{vp}, \alpha_f, \alpha_{ld}, \alpha_{gd}, \alpha_{lc}\} \tag{2}$$

$$\beta_{csae} = \{\beta_p, \beta_r, \beta_{rt}, \beta_{fd}, \beta_{ct}\} \tag{3}$$

We consider a set of α_{psoc} including possible perturbation scenarios, which include voltage perturbations (α_{vp}) at generators, faults (α_f), load (α_{ld}) and generation (α_{gd}) deviations, and line contingencies (α_{lc}). Each scenario may turn the selected power system to a stable, marginally stable or an unstable operating condition. In addition to these α_{psoc}, we consider a set of possible stealthy cyber-attack vectors that may impact the power system stability. The set of β_{csae} include pulse attack (β_p), ramp attack (β_r), relay-trip attack (β_{rt}), replay attack (β_{rp}), false-data injection attack (β_{fd}), and coordinated attacks with simultaneous or sequential timing vector (β_{ct}) on the measurement and control signals. As these cyber-attack vectors are stochastic in nature, we consider their presence on both ideal and α_{psoc} scenarios. The β_{csae} can be defined as follows:

$$\beta_{csae} = \begin{cases} \beta_p & = & f(\lambda_m, \lambda_p, \lambda_w, \lambda_t) & \forall t \in t_a \\ \beta_r & = & f(\lambda_m, \lambda_s, \lambda_t) & \forall t \in t_a \\ \beta_{rp} & = & f(\lambda_r, \lambda_{tc}, \lambda_t) & \forall t \in t_a \\ \beta_{fd} & = & f(\lambda_{fr}, \lambda_{pe}, \lambda_{md}, \lambda_t) & \forall t \in t_a \\ \beta_{ct} & = & f(\lambda_{av}, \lambda_{at}, \lambda_t) & \forall t \in t_a \end{cases} \tag{4}$$

where, λ_t defines duration of attack-time, t_a represents duration of attack period, and the other variables explained below in the corresponding subsections. We refer any of the following attack as stealthy whenever it poses difficult problem to the conventional bad-data detectors and increase its false positive rate.

Pulse Attack *(β_p):* Pulse attack is prepared with essentially three parameters, namely, attack magnitude (λ_m), duration of pulse period (λ_p), width of pulse ON duration (λ_w). A pulse attack applied on a true data signal can be inclusive (additive) or exclusive (subtraction). As the nature of pulse attacks, it injects an amplitude of frequency components to the true data signals. A stealthy pulse attack is constructed by a right choice of amplitude component (λ_m) and frequency component, which is defined by the λ_p and λ_w.

Ramp Attack *(β_r):* Ramp attack prepared with essentially two parameters, namely, attack magnitude (λ_m) and slope of the ramp signal (λ_s). A ramp attack applied on a true data signal can be inclusive (additive) or exclusive (subtraction). As the nature of ramp attack, it injects a continuous increase or decrease of amplitude to the true data signals. A stealthy ramp attack is constructed by a right choice of amplitude and slope. A ramp attack with small slope changes the true data signal at a slower rate, which means it can bypass the conventional bad-data detector.

Relay-trip Attack *(β_{rt}):* These are man-in-the-middle type of attacks. It essentially includes two tasks, namely, identification of vulnerable relay (λ_r), also known as intelligent electronic device (IED), and launching a trip or close (λ_{tc}) operation by SCADA protocols (DNP3, IEC-61850, Modbus).

False-data Injection Attack *(β_{fd}):* Adversaries use the system properties to manipulate the data. For instance, injection of signals from fault recordings (λ_{fr}, fault-reading based data injection), extracting a block of data from the past and repeat that in the transient condition (λ_{pe}, past-event-based replay attack), Missing data attack (λ_{md}).

Coordinated Attack *(β_{ct}):* These attacks are more stealthy as adversaries use any combination of attacks to launch an attack-vector (λ_{av}) comprising of different cyber-attack events and various attack-time sequence (λ_{at}) events.

A compromised signal ($x^*(t)$) with a data-integrity attack (β_{csae}) can be defined as

$$x^*(t) = (1 + \beta_{csae}) \times x(t) \quad \forall t \in t_a \tag{5}$$

where, the $x(t)$ can be either measurement or control signal of an operation condition defined in α_{psoc} and t_a represents duration of attack period.

As shown in Fig. 3, we prepare a power system model in a simulation environment, and a set of comma separated value (CSV) files, wherein each file represent a simulation instance variables comprising of system variables of the model and scenario variables from the α_{psoc} and β_{csae} operating conditions and attack events.

1) Dataset Generator (Parallel Execution): We consider isolating the simulation instance variables from the simulation model to facilitate optimal parallel execution of all the plausible simulation instances. This process is essential to prepare a rich dataset for a large-scale power system including the substantial size of actuators and measurements, where the number of possible attacks and possible combinations on various system operating conditions leads to a massive set of simulation scenarios. It is critical to use either high-performance computing (HPC) or parallel computing environment to execute all the simulation scenarios in parallel. In this module, we utilize parallel computing toolbox to dynamically auto-assign the simulation instances to the workers of the cluster in the Matlab environment. As of 2018, the maximum number of workers in a parallel computer cluster are 1024 [32] under Matlab cloud center environment, which means it can execute 1024 simulation instances in parallel. On the other hand, with a trade-off between accuracy and extensive computation, the total number of simulation scenarios can be reduced by a weighted-random selection on the number of combination of channels that may be exposed to attack. In ideal case, we consider all the combinations i.e., $\alpha_{psoc} \times \beta_{csae} \times 2^n$. However, $w_a \times 2^n$ combinations can be considered with a statistical threat analysis such that the w_a can vary between 0 and 1. The w_a represents a weight associated to select a number of combinations from whole set of 2^n. The number of power system operating conditions and cyber attack events defines the scope of detecting anomalies by the trained ML model with the 95% confidence interval rate of detection accuracy.

2) Dataset Preprocessor for Training and Testing: It includes two primary tasks. i) Assign labels: Supervised ML algorithms require labeled dataset as an input. In this module, we assign tags to the generated data of each simulation instance by their corresponding scenarios such as *normal*, *perturbation* (small or large signal disturbances like faults, generator outages, and line contingencies), *attack* and *perturbation-and-attack*. ii) Prepare window frames: We consider a suitable size of a window length on the labeled-dataset to prepare a vector of data points (window frame) to preserve the characteristics for a period of the window length. We consider a moving window method with a one-point deviation, which means every new window frame excludes oldest data point and includes the latest data point. This step is essential to execute trained-ML module in real-time, PMU data rate of 60 fps (frames per second), under closed-loop HIL simulation. These window frames of the labeled-dataset will be used to build a rich dataset of features to train ML algorithms.

B. Proposed Features for the Anomaly Detection

Raw input data such as measurements from PMUs can be directly used as features to train an ML model. However, it affects detection accuracy and performance of such trained ML models, mainly when there are multiple power system events in conjunction with attack-activity events. Therefore, physics-based and signal-entropy based feature extraction, a process of computing inherited patterns from the window frames of the labeled-dataset, is crucial to building a robust trained ML model for anomaly detection. These domain-specific features obeying physical laws of a complex power system reinforces the cohesiveness among the event patterns in the data streams. In addition to the features derived from statistical [33] techniques, these proposed domain-specific features improve detection accuracy for various subtly varying events, which may occur when adversaries deploy stealthy cyber-attack vectors that are in proximity to the natural power system events such as small-signal and large-signal perturbations. A single or a combination of these features specify an activity detection. The training process of a supervised ML model builds an associative weight map between these features and a labeled data. The trained ML model accuracy depends on the weight map accuracy, which relies on the voluminous of training dataset and robust extracted features. Algorithm 1 shows the extraction of following proposed features.

Algorithm 1 Feature Extraction

```
while (all $features$ are not processed) do
    - Define feature vectors: $f_v \in \{f_{tkeo}, f_{pca}, f_{wasm}, f_{primitive}\}$
    - Feature Extraction:
    while (all $i$ of $f_v$ are not processed) do
        - Define a new feature variable $i \in f_v$
        - Compute the $i$
    end while
    - Feature Selection: Exclude the redundancy/inappropriate feature variables in the $f_v$
end while
- Output the filtered feature variables, which feed through the trained ML model for anomaly detection.
```

1) Teager-Kaiser Energy Operator (TKEO): It is defined to estimate an instantaneous signal energy ($\Psi_{TK}[*]$) [34] for the discrete ($x(n)$) time signal and an example trajectory signal as

$$\Psi_{TK}[x(n)] = x_n^2 - x_{n-1}x_{n+1} \tag{6}$$

$$\Psi_{TK}[e^{-\alpha n}Acos(\omega n)] = e^{-2\alpha n}A^2\omega^2 \tag{7}$$

During the transient variations, the first component of the $\Psi_{TK}[*]$ becomes dominant and contributes to the impulsive responsive on the signal energy. The $\Psi_{TK}[*]$ produces negligible variations on the signal energy for the natural power system oscillations and the oscillatory modes such as IAO and LO. The TKEO acts as a better indicator to track the trajectory of the damped IAO and LO modes, where the trajectory of an exemplified signal can be obtained as in (7). As it provides a better estimate on the transient variations, the extraction of this feature on the raw input data signals can act as a better indicator to distinguish the transient variations between natural power system events and the stealthy cyber-attack vectors deployed by adversaries. It is also applied on the PMU data to predict the frequency and detection of power system oscillations [35]. As it provides a better estimate on the signal energy, it has been used widely in various signal processing techniques, and one of the significant application is tracking the envelope of Amplitude Modulation (AM) signals [36]. Further, we consider a correlative feature by deriving the interaction energy ($\Psi_{CTK}(x_n, y_n)$) between the two signals. This correlative feature strengths the accuracy of attack-activity detection. The interaction or cross-energy ($\Psi_{CTK}(x_n, y_n)$) and its normalization over a time-window (say 0 to N) by the Energy-based Similarity Measure (EbSM) [36]–[38] for continuous and discrete time signals can be defined as follows:

$$\Psi_{CTK}(x_n, y_n) = x_{n-1}y_{n-1} - \frac{x_n y_{n-2} + y_n x_{n-2}}{2} \tag{8}$$

$$EbSM(x_n, y_n) = \frac{\sqrt{2}\sum_{n=0}^{N}\Psi_{CTK}(x_n, y_n)}{\sum_{n=0}^{N}\sqrt{\Psi_{CTK}^2(x_n, x_n) + \Psi_{CTK}^2(y_n, y_n)}} \tag{9}$$

2) Principal Component Analysis (PCA): To obtain dimensionality reduction (without loss of significant information) and patterns identification over the high-dimensional data, we use PCA [39] in the process of feature extraction. It uses orthogonal transformation to convert a window (either temporal, spatial or both) of observations or measurements of possibly correlated variables into a set of linearly independent variables called principal components (PCs). A set of x variables with n measurements (higher-dimension) can have $min(n-1, x)$ distinct orthogonal PCs (lower-dimension), where each PC represents the data variability ($variance$) in the direction of its corresponding unit eigenvector. It is vital in the ML algorithm to use the PCs with relatively high variance that capture at least 95% variance of the input data set. It is essential to consider the dominant PCs as features to avoid over-fitting and to improve the accuracy and computation time of the activity detection. The PCA and its variants with computationally efficient algorithms for computing the PCs have been used widely in various ML applications [40]–[42].

3) Wide-Area System Measures (WASMs): We use WASMs based features in the ML algorithm to identify the anomalies by the stealthy cyber-attack vectors that are distinct from the natural power system events. The WASMs comprising of coherency and non-coherency based indices characterize the dynamics of power system events. We recently published the efficacy of the significant WASMs for angle-stability assessment [7]. These indices identify the event patterns over the PMU data streams and provide measures for the system stability and dynamic security assessments in real-time or near real-time. As these indices form a closed set of threshold values based on the system dynamics of the power system, we consider the indices to extract the features in the ML algorithm for improving the accuracy to the identification of power system events and the cyber-attack events. The mathematical models and detailed procedures of the WASMs are discussed in [7] to calculate the coherency and non-coherency based measures such as coherency sensitivity indicators, integral square generator angle (ISGA), wide-area severity index (WASI) and integral square bus angle (ISBA). For Ng generators in an i^{th} area of a multi-area power system, the COI of the area, system COI, the relative rotor angle deviation of a generator referred to the i^{th} area, and the i^{th} area referred to its system can be defined as:

$$\delta_{COI_i} = \frac{1}{M_i}\sum_{k=1}^{Ng_i} M_k\delta_k \tag{10}$$

$$\delta_{COI_{system}} = \frac{1}{\sum_{i=1}^{N_{area}} M_i}\sum_{i=1}^{N_{area}} M_i\delta_{COI_i} \tag{11}$$

$$\delta_k^{COI_i} = \delta_k - \delta_{COI_i} \tag{12}$$

$$\delta_i^{COI_{system}} = \delta_i - \delta_{COI_{system}} \tag{13}$$

Where, M_k and δ_k are inertia and rotor angle of the k^{th} generator. Ng_i and M_i are the number of generators and cumulative inertia of the i^{th} area respectively.

4) Primitive Measures: The rate of change, mean, standard deviation and root mean squared (RMS) functions over a window of raw synchrophasor input data provide a primary relationship between the signals. We consider these primitives as features to preserve the primary variations on the input signals and provide better measures in stable system operation.

C. Supervised ML Algorithms for Trained Models

Extensive research on ML algorithms for the data-intensive complex domain applications have led to the development of TensorFlow [43], an open-source ML platform, to train ML models. On the other hand, Matlab has provided ML toolbox [44] for plug-and-play of various supervised and unsupervised ML algorithms. We use supervised ML algorithms, namely, support vector machine (SVM), decision trees, k-nearest neighbor, Naive Bayes, discriminant analysis, logistic regression, and neural networks for the classification of data. The SVM and KNN exhibit greater performance for the classification of anomalies; on the other hand, the KNN and DT converge more quickly and shortens the training time [45]. Hence, we consider DT and KNN ML algorithms for anomaly detection. In particular, we consider three variants (*Fine Tree*, *Medium Tree* and *Coarse Tree*) of the Decision Tree (DT), and six variants (*Fine KNN*, *Medium KNN*, *Coarse KNN*, *Cosine*, *Cubic KNN* and *Weighted KNN*) of K-Nearest Neighbor (KNN) supervised ML models for the detection of cyber-attack anomalies. We consider ML toolbox [44] available in the Matlab environment to build a trained model, which is then integrated with the WADC module to work in real-time on HIL CPS testbed.

D. Mitigation Technique

We have two segments of attack surfaces, namely, attacks on the measurement signals and attacks on the control signals. We consider deploying the ADM module at the control center to detect anomalies on both measurement and control data. The ADM detects the attack anomalies and the corresponding channel indices of the compromised signals. Accordingly, the ADM performs suitable mitigation techniques for AR-WADC operation as follows: i) If there is an attack on a measurement signal, then it passes through the ADM on the current cycle. Subsequently, the ADM detects and sends a tuned WADC signal to wide-area actuators. ii) If there is an attack on a control signal, then it passes through the ADM only in the next control cycle loop. Subsequently, the ADM detects the anomalies and compromised channels. However, in this case, a tuned WADC signal would not be sufficient as the attacks are happening on the control signal side that affects the tuned control signal again. Two possible mitigation methods, Only-PSS mode and Reconfiguration mode, are as follows:

Only-PSS mode: It considers operating the system using local signals to sustain the stable operation until the exclusion of attacks. As the ADM module detects the attacks on the control signal side, it issues the WADC status mode zero (0) to the actuators so that they operate with local signals. The process to switch between the wide-area control signals and local signals explained in [25].

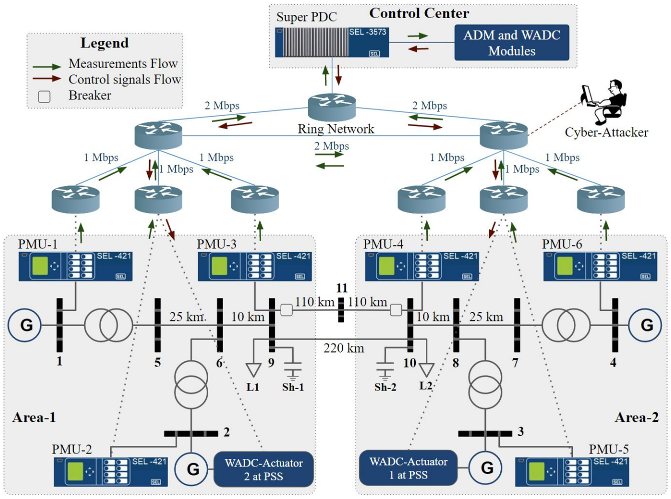


Fig. 4. Schematic Diagram of the AR-WADC for Two-Area Power System

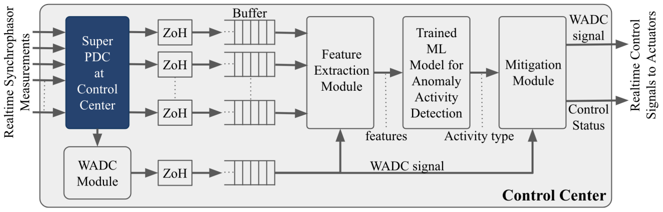

Realtime Synchrophasor Measurements
Super PDC at Control Center
ZoH
Buffer
Feature Extraction Module
Trained ML Model for Anomaly Activity Detection
Mitigation Module
WADC signal
Control Status
Realtime Control Signals to Actuators
features
Activity type
WADC Module
WADC signal
Control Center

Fig. 5. Integration of ADM and WADC for Attack-Resilient WACS Operation

Reconfiguration mode: It is useful when a system has WADC with redundant input and output signals. In this case, reconfiguration of WADC can be carried out with reliable data channels to avoid only-PSS mode of operation. The hybrid WADC design [26]–[28] by reconfiguration of input and output communication channels enhances the resiliency of the WADC closed-loop operation.

IV. Testbed-Based Implementation

We consider the four-machine two-area power system network shown in Fig. 4 for the demonstration of AR-WADC application. The ADM module monitors all the PMU measurements to detect anomalies, and WADC module uses the required PMU data and synthesizes a control signal. Fig. 5 shows a detailed view of the ADM and WADC Modules and their integration in the closed-loop operation. The selected power system is implemented on the OP5600 OPAL-RT real-time digital simulator integrated with the hardware setup available at the PowerCyber [46] lab in the Iowa State University. We integrate the model with the virtual PMUs provided by the ARTEMiS-SSN of the OPAL-RT. We use the SEL-3373 hardware PDC to collect and transfer the synchrophasors from the PMUs to the WADC module. The WADC module uses the selected wide-area measurements from the super PDC to synthesize a control signal to dispatch to geographically distributed actuators. The subsequent sections discuss the implementation and evaluation of the WADC operation and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2020.2995313, IEEE Transactions on Smart Grid

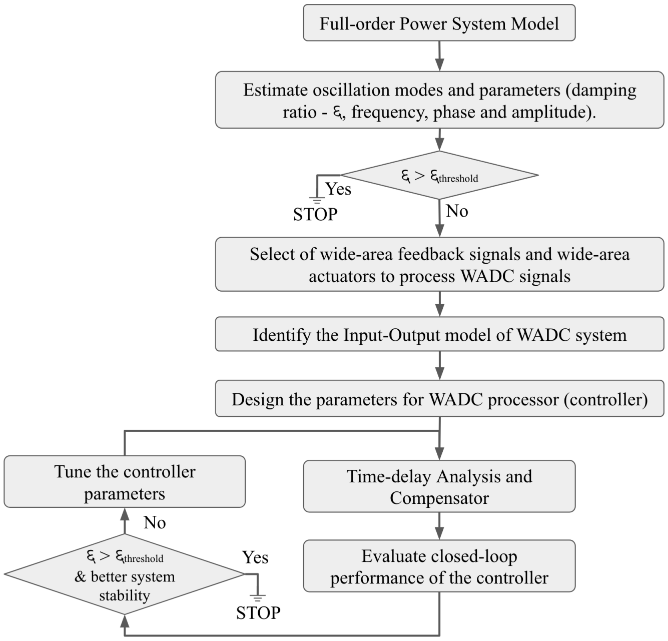

Full-order Power System Model
Estimate oscillation modes and parameters (damping ratio - ξ, frequency, phase and amplitude).
ξ > ξthreshold
Yes
STOP
No
Select of wide-area feedback signals and wide-area actuators to process WADC signals
Identify the Input-Output model of WADC system
Design the parameters for WADC processor (controller)
Tune the controller parameters
Time-delay Analysis and Compensator
No
ξ > ξthreshold & better system stability
Yes
STOP
Evaluate closed-loop performance of the controller

Fig. 6. WADC Design and Tuning the Controller Parameters

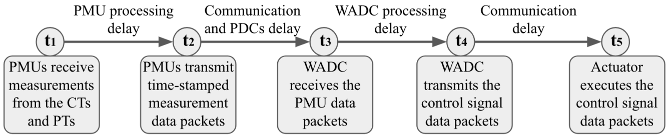

PMU processing delay
Communication and PDCs delay
WADC processing delay
Communication delay
t1
t2
t3
t4
t5
PMUs receive measurements from the CTs and PTs
PMUs transmit time-stamped measurement data packets
WADC receives the PMU data packets
WADC transmits the control signal data packets
Actuator executes the control signal data packets

Fig. 7. Time-Delay Sequence of WADC System Operation

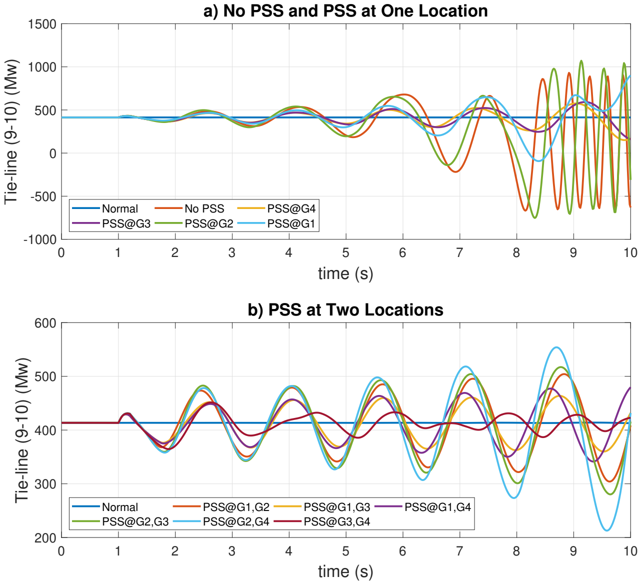


Fig. 8. PSS Performance during Voltage Perturbation

its integration with the proposed ADM algorithm for the demonstration AR-WADC system operation.

A. Design of WADC

The Fig. 6 shows the process followed for the design of the WADC processor. We use the Matlab for calculating the full-order nonlinear model of the considered power system. We consider the detailed models for all the synchronous generators that includes the governor, two-axis model with exciter, and PSS with lead-lag phase compensation blocks. We linearize the systems of equations of the nonlinear model around a selected operating point, which is a well proven systematic approach to build a general solution to the complex non-linear power systems and is instrumental in the applications such as small signal analysis, stability and security margins, and controller designs. We convert the linear model into state-space representation. It provides the system dynamics as a set of input, output and state variables (a minimum set of internal variables whose values evolve through time in response to their system dynamics) that form coupled first-order differential equations. We carry out the small-signal analysis on the state-space model for estimating the parameters characterizing the IAO modes such as damping ratio, frequency, phase, and amplitude.

We consider the eigenvalue modal analysis and the residue methods for the study of observability and controllability of IAO modes. We consider the right half-plane zeros (RHP-zeros) method for the identification of zeros on the right-half plane that specifies the instability margins. The observability analysis is used to identify the wide-area feedback signals that inherit the dominant IAO modes. We select the candidate feedback signals from the PMU dataset that includes positive-sequence voltage and current signals, phase angle, frequency and the derived signals such as active and reactive power on the lines, rotor speed and its deviation, and generator state variables. The observability analysis shows that IAO modes are observable on the PMUs connected to the tie-line and the PMUs connected to the generators 2 and 3. We select the phasor measurements of PMU-2, PMU-3, PMU-4 and PMU-5 from the super PDC and estimate the deviation of rotor speed of generators to use as wide-area feedback signals to the WADC processor.

The controllability analysis is used to identify the wide-area actuators that process WADC signals to damp the IAO modes. The actuators can integrate with the three types of devices such as PSS, HVDC, and FACTS, which controls the active and reactive power to increase the damping ratio of the power system. We consider two wadc-actuators (wide-area power system stabilizer - WA-PSS), one at the generator-3 and the other at the generator-2 as shown in Fig. 4. These WA-PSS process the control signals received from the WADC. In addition to the local-signal based PSS, the WA-PSS further supplements the excitation control to the generator to contribute to damp the IAO modes and increase the system stability. The high amplify gain of the PSS can provide a relatively better control efficiency with low amplified signals. As the power system includes more PSS devices compared to the FACTS and HVDC, the flexibility to select and integrate the wide-area actuators with PSS is relatively high. However, the actuator integrated with HVDC system can provide faster and direct control to the active power transmitted over the inter-tie lines to damp IAO modes. The field tests on the HVDC based WADC in the China Southern Power Grid (CSG) [13]–[15] have shown an increase of the damping ratio from 7.551% to 20.459% on an IAO mode. Though the primary application of the FACTS devices is to modulate active power flow to enhance power transfer capacity, it is witnessed that the

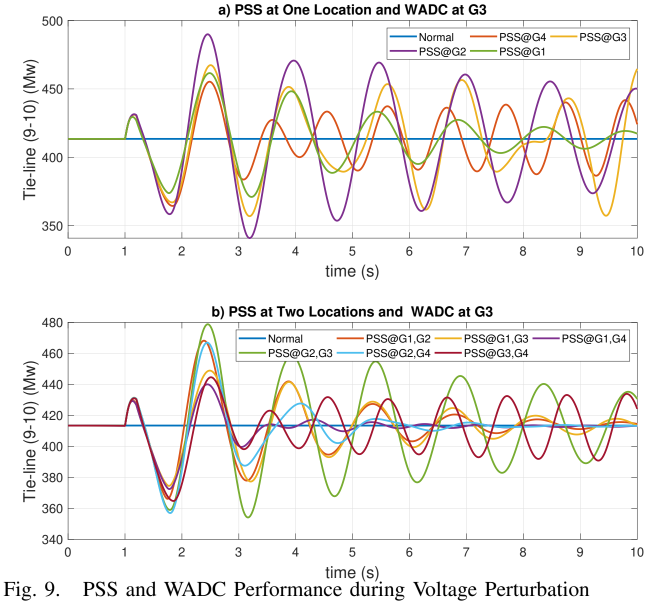


Fig. 9. PSS and WADC Performance during Voltage Perturbation

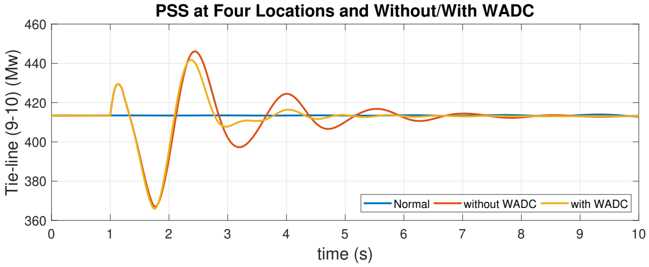


Fig. 10. WADC Performance with Four PSSs during Voltage Perturbation

FACTS-based WADC can also exhibit effective performance even under the effect of network latency [47].

1) State-space Modeling and Parameter Selection for WADC: Over three decades, there has been an extensive research delved into the state-space modeling and optimal design of gain and parameters for the WADC [48], [49]. Various simulation and hardware designs of wide-area damping controllers can be found at [12]. In this section, we brief out the state-space modeling and considered WADC design for the implementation. To identify LO and IAO modes of N_g generator system, the state space model [48] is defined as –

$$\dot{x} = Ax + Bu = Ax + \sum_{j=1}^{N} B_j u_j \qquad (14)$$
$$y_j = C_j x$$

where $x' = [\Delta\delta' \quad \Delta\omega']$; B_j is input matrix (column vector) and C_j is output matrix (row vector) for j^{th} generator. The A includes $2{*}N_g$ eigenvalues, wherein $N_g - 1$ complex conjugate pairs represent LO and IAO modes. The derivation and design of these parameters can be found at [12].

The synthesis of the selected wide-area feedback signals is defined by the robust mixed H_2/H_∞ output-feedback control with regional pole placement constraints. It is evaluated using the linear matrix inequality (LMI) method employed by the $h2hinfsyn$ [50] function of the Matlab for the calculation of parameters of the WADC processor. The WADC implementation design and the time constants are defined as follows. The state space model of WADC is defined as –

$$\begin{aligned} \dot{X}_k &= A_k X_k + B_k U_k \\ Y_k &= C_k X_k + D_k U_k \end{aligned} \qquad (15)$$

Where $U_k = [\Delta\omega']$. The theorems for deriving these design parameters including delay tolerance using the LMI methods can be found at [49]. The result of LMI method consists of optimal gain and $H_i(s)$ of the WADC. A detailed derivation for gain matrix for PSS using LMI is provided in [51] and scheduling of WADC K_{WADC} in relation with PDCs is provided in [52]. The selected WADC for the implementation is defined as –

$$H_{WADC}(s) = K_{WADC}\frac{sT_w}{1+sT_w}\left(\frac{1+sT_{lead}}{1+sT_{lag}}\right)^n \qquad (16)$$
$$= K_{WADC}H_i(s) \qquad (17)$$
$$\phi_c = \pi - argR_j \qquad (18)$$
$$\theta = \frac{T_{lead}}{T_{lag}} = \frac{1-sin(\phi_c/n))}{1+sin(\phi_c/n))} \qquad (19)$$
$$T_{lag} = \frac{1}{\omega_n\sqrt{\theta}}, T_{lead} = \theta T_{lag} \qquad (20)$$

where K_{WADC} - WADC gain; T_w - washout constant (e.g., 5 to 10 s); T_{lead} and T_{lag} - parameters for phase compensation; n - number of lead-lag blocks (usually two blocks); ϕ_c - phase required compensation; $argR_j$ - phase angle of residue R_j; ω_n - dominant oscillation mode frequency; The design parameters considered in the WADC are K_{WADC} = 30, T_w = 10, T_{lead} and T_{lag} = $[63.244e^{-3} \quad 44.516e^{-3}]$, output saturation limits = $[-0.15 \quad 0.15]$, and sensor time constant = $15e^{-3}$.

2) Time-domain Evaluation of WADC: It is essential to evaluate the transient response and stability of the designed controller for better performance on the nonlinear time-domain simulation. The WADC processor is evaluated and tuned on the HIL closed-loop the full-order model of the test system.

Fig. 7 shows the significant time delays involved from the capture of measurements to the moment that actuator executes the control signal to damp IAO modes. We configure the PMUs to transmit the data at 60 fps. It is observed that the mean processing time of each frame by the PMU is 2.865 ms and the WADC processing time is 1.28 ms.

We have applied 5%-magnitude pulse for 12 cycles at the voltage reference of the Generator 1. We have tuned the PSS for different scenarios such as one-PSS in the system and two-PSSs in the system using the same design approach used for WA-PSS i.e., LMI method. Figs. 8a and 8b show the effect of IAO damping by having a PSS at one location in the system during the normal operation and voltage perturbation accordingly. In this case, PSS at two locations shows relatively more damping but insufficient to damp IAO. We have executed the same exercise but modeled a WADC actuator, WA-PSS, at Generator 3 in the system. Figs. 9a and 9b show the effect of IAO damping by having a PSS at one location in the system during the normal operation and voltage perturbation accordingly along with the WADC at Generator 3. In this case, both the scenarios provide sufficient damping to the IAO. It draws the significant performance by WADC to damp IAO in the system.

The WADC performance during voltage perturbation when PSS deployed at all the generator locations is shown in Fig. 10. We observed that the oscillations settle down for the small-signal disturbance. We conducted eigenvalue analysis and obtained IAO mode parameters, namely, damping ratio – 0.0612 and oscillation frequency – 0.6436 Hz. We considered this mode as a critical IAO mode. When we deploy either one PSS or two PSSs in a system, we observed their contribution of the damping ratio to the local modes is more compared to the IAO mode. However, when we install PSS at four generators in the two areas, the damping ratio increased to 0.313. When we tested the system with one WADC and one PSS, the damping ratio increased to 0.156, and in the case of one WADC and two PSS, it increased to 0.243. When we deploy all the four PSS and one WADCs in the system, the damping ratio increased to 0.378. Finally, we tested the system with four PSS and two WADCs, and the damping ratio increased to 0.396. Thus, we evaluated significant damping by WADC to the IAO modes.

B. Preparation of Dataset for Machine Learning Models

In accordance with the Section III-A, we consider the α_{psoc} and β_{csae} as follows. We consider $\alpha_{vp} = 5 * 4 = 20$ scenarios, which includes five voltage perturbations ($2 - 10\%$ magnitude pulse at an interval of 2%), applied for 12 cycles at the voltage reference of the four generators. We consider $\alpha_f = 10$ scenarios, which includes three unsymmetrical faults, namely, Single line-to-ground fault (LG), Line-to-line fault (LL) and Double Line-to-ground fault (LLG), and two symmetrical faults, namely, Three-phase short circuit fault (LLL) and Three-phase-to-ground fault (LLLG). We have applied these faults at two tie-line buses and fault cleared in 8 cycles. We consider 20 generation-load (α_{ld} and α_{gd}) dispatched scenarios, which includes a load variation from 70% to 110% at an interval of 2%. We consider $\alpha_{lc} = 2$ scenarios, which includes line contingencies on the critical two tie-lines. Thus, we consider $\alpha_{psoc} = 20 + 10 + 20 + 2 = 52$ scenarios. We consider $\beta_p = 6 * 5 * 5 = 150$ scenarios, which includes six pulse magnitude variables $(0.0040, 0.0030, 0.0025, 0.0020, 0.0015, 0.0010)$, five pulse period variables $(1/0.5, 1/0.9, 1/1.2, 1/1.4, 1/1.8)$ and five pulse width percentage ON variables $(90, 60, 30, 20, 10)$. These values are considered based on the empirical analysis of the considered test system. We consider $\beta_r = 10$ scenarios, which includes ten different slope values of the ramp signal. We also consider $\beta_{fd} = 10$ false-data injection attack scenarios. Thus, we consider $\beta_{csae} = 150+10+10 = 170$ scenarios. As the WADC module uses six measurement signals and two control signal, we consider applying these stealthy cyber-attack vectors on the combination of the eight signals, i.e., $2^8 = 256$. We consider $w_a = 0.125$ such that we dynamically select only 12.5% of the combinations of the eight signals. Therefore, the new combination set has $0.125*256 = 32$. The complete set of attack scenarios are $170*32 = 5440$. Thus, we consider a dataset of $D = 5440 * 52 + 52 = 282932$ different simulation scenarios. Each scenario includes 20 seconds of data, which means $20 * fps = 20 * 60 = 1200$ data points, and is labeled with reference to one of the four activity scenarios. Labeled data is essential for training supervised ML model. We have prepared a computational environment on the PowerCyber testbed available at Iowa State University. The computational set up for the experiment includes 100 cores with 2.3 GHz and 128 GB RAM. We have used Windows 2016 server environment to setup Matlab R2019a. We use the latest parallel computing toolbox that assigns a worker to a core with an upper cap of 512 simultaneous workers in a cluster. Each active worker executes simulation instance and archives the data. Thus, we have prepared a dataset that includes a combined power system operating conditions and cyberattack events-based activities. The total execution time of the data generation set is approximately 23 hrs under the testbed environment.

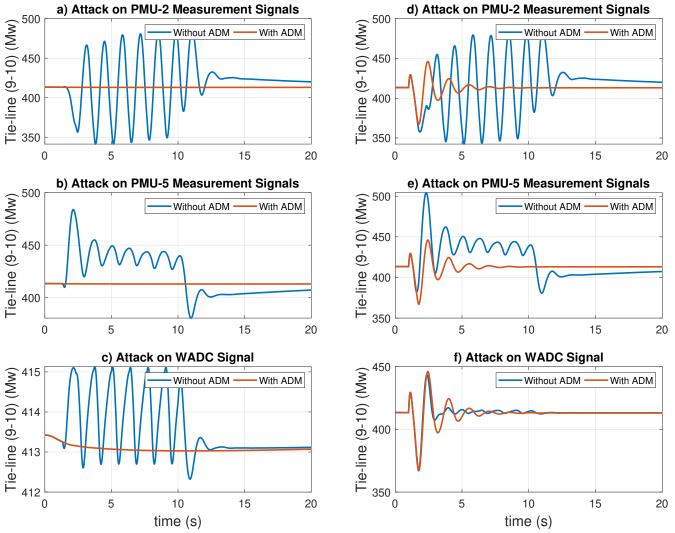


Fig. 11. Performance of ADM for Pulse Attack during the Normal (a-c) and Voltage Perturbation (d-f) Scenarios

C. Feature Extraction and Training ML Algorithms

We consider applying the process of extracting features as defined in the Section III-B on the dataset, D. The dataset is processed as a set of data points, which we refer as a window of dataset. With the empirical evaluation of different simulation test cases, we observe that $1/5*fps$=$1/5*60$=12-point window size provide better set of data patterns to compute the features. We consider moving window with 1-point step size so that the Feature Extraction module computes the selected features at the signal data rate. We consider 60% of the dataset for training the ML model and 40% of the dataset for the process of testing.

As discussed in Section III-B, we consider the TKEO, WASM, and primitive measures, as standalone features, and compute PCA on a subset of primitive measures for dimensionality reduction. We preserve linearly independent TKEO, and WASM measure features to capture the physics-based grid dynamics and characteristics. While in the implementation of the algorithms, we have followed an iterative approach to select the required subset of primitive measures to be used for PCA for dimensionality reduction. Subsequently, the window frames of the labeled-dataset are used as an input to prepare a rich dataset of features to train ML algorithms. These

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2020.2995313, IEEE Transactions on Smart Grid

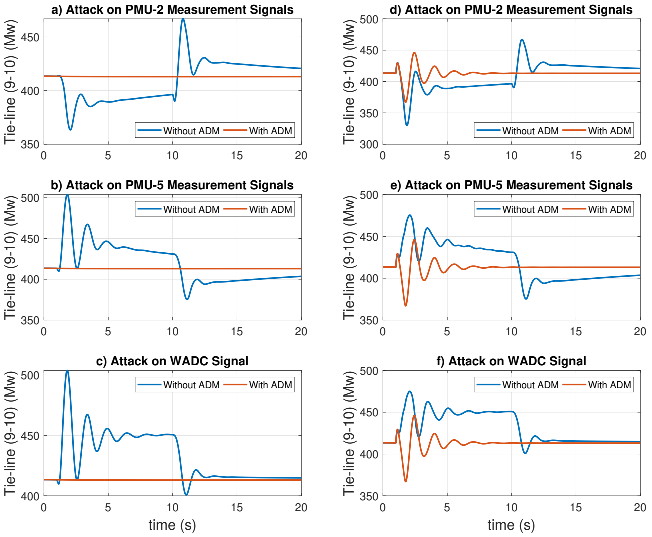


Fig. 12. Performance of ADM for Ramp Attack during the Normal (a-c) and Voltage Perturbation (d-f) Scenarios

window frames, for example, a length of 12 points (12/60 s window), feed to the proposed feature functions, namely, TKEO, WASM, primitive measures and PCA (on a subset of primitive features). The feature extraction algorithm computes all of these feature functions to prepare a vector of feature values. The feature values of the entire training dataset are used for training ML algorithms, while the feature values of the whole testing dataset used for testing the ML algorithms to determine false positives and false negatives. It is an iterative process, and consequently, we consider a trained ML model that exhibited better detection accuracy.

We consider different Decision Tree (DT) and KNN ML models for the training. We observe that the Fine KNN ML model exhibits better accuracy with 96.5% compared to other ML models as shown in Fig. 13. We use the Euclidean distance metric with one neighbor in the KNN. The model is trained to detect the designed significant activities such as *Normal*, *Perturbation*, *Attack* and *PerturbationAndAttack* from the measurement and control signal streaming data.

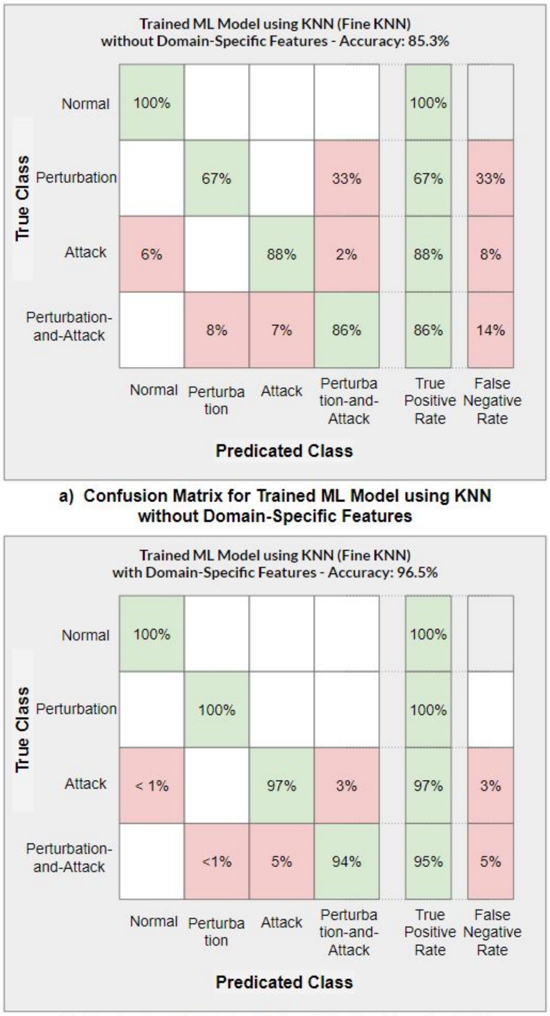
D. Integration of ADM and WADC

The KNN-based AD and the mitigation module are integrated with the WADC as shown in Fig. 5 for the demonstration and evaluation in the closed-loop simulation. We use the zero-order hold (ZOH) for preserving the input at the time-step of signal data rate (60 fps) and transfer the values to buffer to hold for a 12-point window. The trained ML model uses the features as input and predicts the activity type. Mitigation module uses the activity type and the WADC signal to generate the attack-resilient WADC signal and status data, which fed to the wide-area actuator deployed at Generator-3.

E. Results and Observation of ADM with WADC

Figs. 11-12 show the performance of the proposed ADM with WADC for the Pulse and Ramp stealthy cyber-attack vectors during the normal operation and voltage perturbation scenario. We apply the Pulse attack vector (0.0036, 1/0.75 and 75%) and the Ramp attack vector for the duration of the $1-10$ seconds. It is observed that impact on the tie-line power flow persist even after the completion of attack for around $1-2$ seconds. We observed that the Pulse attacks introduce frequency components and impact the power flow to a low steady-state value during the attack period. It also injects overshoots at the start of attack. We observe that the Ramp attacks impact the power flow to high steady-state value during the attack period. It also injects high amplitude overshoots at the start of attack.

In addition to the stability and system operation impact on the power system, to evaluate the impact trajectory characteristics on the tie-line power flows affected due to the attack vectors, we have computed characteristic parameters such as peak overshoot, settling time, rise time, and oscillation components. In the case of normal power system operation, as shown in Fig. 11a, when pulse attacks launched on either PMU-2 signal or WADC signal, the tie-line power flow experienced an increased oscillation trajectory. However, when the pulse attack launched on the PMU-5 signal, the tie-line power flow experienced high overshoot and relatively decreased oscillation trajectory. In the case of normal power system operation, as shown in Fig. 12a, when ramp attacks


Trained ML Model using KNN (Fine KNN)
without Domain-Specific Features - Accuracy: 85.3%

True Class	Normal	Perturbation	Attack	Perturbation-and-Attack	True Positive Rate	False Negative Rate
Normal	100%				100%	
Perturbation		67%		33%	67%	33%
Attack	6%		88%	2%	88%	8%
Perturbation-and-Attack		8%	7%	86%	86%	14%

Predicated Class

a) Confusion Matrix for Trained ML Model using KNN without Domain-Specific Features

Trained ML Model using KNN (Fine KNN)
with Domain-Specific Features - Accuracy: 96.5%

True Class	Normal	Perturbation	Attack	Perturbation-and-Attack	True Positive Rate	False Negative Rate
Normal	100%				100%	
Perturbation		100%			100%	
Attack	< 1%		97%	3%	97%	3%
Perturbation-and-Attack		<1%	5%	94%	95%	5%

Predicated Class

b) Confusion Matrix for Trained ML Model using KNN with Domain-Specific Features

Fig. 13. Detection Accuracy of Trained ML Model using KNN without & with Proposed Domain-Specific Features

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2020.2995313, IEEE Transactions on Smart Grid

launched on either WADC signal or PMU-2, the tie-line power flow experienced positive peak overshoot. However, when the ramp attack launched on the PMU-2 signal, the tie-line power flow experienced negative peak overshoot with relatively less amplitude. It is observed that the ADM sets the WADC status to local-signal mode, as shown in Fig. 11, where the inter-tie line power flow exhibits the same damping characteristics as if the system works on local-signal based actuators.

F. Evaluation of Anomaly Detection

Figs. 13a and 13b show True Positive and False Negative rates for the trained ML models without and with domain-specific features accordingly. We observed that the trained ML model with domain-specific features had exhibited an enhanced detection accuracy at all the activities. The trained KNN ML model (Fig. 13b) has shown better performance with 96.5% accuracy. The model predicts less than 1% of *Attack* activity as *Normal* and 3% of *Attack* activity as *PerturbationAndAttack* activity. The model predicts the *PerturbationAndAttack* as *Perturbation* with 1%, as *Attack* with 5%, and as *PerturbationAndAttack* with 94% accuracy. The characteristic patterns of *Attack* and *PerturbationAndAttack* can be in proximity to *Perturbation* characteristics by stealthy cyber-attack vectors. It results in a significant challenge to ML for the activity detection with higher accuracy. The inclusion of domain features such as TKEO and WASMs provided better measures to train the ML model to detect the *PerturbationAndAttack* activity with 94% accuracy. It can be further improved by fine-tuned parameter settings of the ML models and dynamic window length.

G. Evaluation of Mitigation Technique

In accordance with the model-based mitigation technique defined in the Section III-D, the Figs. 11 and 12 show the effective performance of the mitigation operation in response to the Pulse and Ramp stealthy cyber-attack vectors during *Normal* and *Voltage Perturbation* operating conditions. Though it works in most of the scenarios, the rule three poses a limitation to switch to local-signal based actuators during the perturbation of the *PerturbationAndAttack* scenario. We envision to address the limitation of the mitigation module by devising a statistical or model-based technique to synthesize an approximate WADC signal to use as a mitigation operation. However, the approximated signal can only be sent in the case of attacks on the compromised measurement signals. If there is an attack on the control signal, then it must switch to the local mode for seamless operation of centralized ADM located at the control center. This limitation can further be addressed by deploying an ADM at each actuator with the trade-off to the increased complexity in the management, security and computational processing of the decentralized ADM operation.

V. Conclusion

This paper proposed anomaly detection using Machine Learning and model-based mitigation for ensuring secure and attack-resilient WADC system operation. We have proposed physics-based and signal-entropy based feature extraction to increase the accuracy and robustness of the trained ML model. These domain-specific features have increased the efficacy of the ADM module in detecting anomalies that are in proximity to the characteristics of natural power system events. We have demonstrated the proposed ADM integrated with WADC on the HIL synchrophasor CPS security testbed for the two-area four-machine power system. The test results witnessed ADM module with 96.5% accuracy including low false positive and negative rates for the data-integrity attacks. As the proposed ADM module executes at the control center and eliminates the need for ADMs at sensors, it can be adopted seamlessly by the utilities for the resilient operation of WACS application. Our future work includes devising deep learning-based attack resilient control algorithms for WAMPAC applications.

VI. Acknowledgement

This research is funded in part by US NSF Grant # CNS 1446831, and US DOE Grant # DE-OE0000830.

References

[1] G. Rogers, “Demystifying power system oscillations,” *Computer Applications in Power, IEEE*, vol. 9, no. 3, pp. 30–35, Jul 1996.

[2] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. McGraw-hill New York, 1994, vol. 7.

[3] T. Dy-Liacco, “Enhancing power system security control,” *Computer Applications in Power, IEEE*, vol. 10, no. 3, pp. 38–41, Jul 1997.

[4] K. R. Padiyar, *Power System Dynamics, Stability & Control*, 2nd ed. B.S. Publications, Hyderabad, 2008.

[5] I. Kamwa, A. Pradhan, G. Joos, and S. Samantaray, “Fuzzy partitioning of a real power system for dynamic vulnerability assessment,” *Power Syst., IEEE Trans. on*, vol. 24, no. 3, pp. 1356–1365, Aug 2009.

[6] G. Liu, J. Quintero, and V. Venkatasubramanian, “Oscillation monitoring system based on wide area synchrophasors in power systems,” in *Bulk Power System Dynamics and Control*, Aug 2007, pp. 1–13.

[7] G. Ravikumar and S. A. Khaparde, “Taxonomy of pmu data based catastrophic indicators for power system stability assessment,” *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–13, 2016.

[8] J. H. Chow, J. J. Sanchez-Gasca, H. Ren, and S. Wang, “Power system damping controller design-using multiple input signals,” *IEEE Control Systems*, vol. 20, no. 4, pp. 82–90, Aug 2000.

[9] B. J. Pierre, F. Wilches-Bernal, R. T. Elliott, D. A. Schoenwald, J. C. Neely, R. H. Byrne, and D. J. Trudnowski, “Simulation results for the pacific dc intertie wide area damping controller,” in *IEEE PESGM*, 2017.

[10] D. Trudnowski, B. Pierre, F. Wilches-Bernal, D. Schoenwald, R. Elliott, J. Neely, R. Byrne, and D. Kosterev, “Initial closed-loop testing results for the pacific dc intertie WADC,” in *IEEE PESGM*, 2017.

[11] F. Wilches-Bernal, B. J. Pierre, R. T. Elliott, D. A. Schoenwald, R. H. Byrne, J. C. Neely, and D. J. Trudnowski, “Time delay definitions and characterization in the PDCI WADC,” in *IEEE PESGM*, 2017.

[12] Y. Li, D. Yang, F. Liu, Y. Cao, , and C. Rehtanz, *Interconnected Power Systems - Wide-Area Dynamic Monitoring and Control Applications*, 1st ed. Springer-Verlag Berlin Heidelberg, 2016.

[13] J. He, C. Lu, X. Wu, P. Li, and J. Wu, “Design and experiment of wide area hvdc supplementary damping controller considering time delay in china southern power grid,” *IET GTD*, vol. 3, no. 1, pp. 17–25, 2009.

[14] C. Lu, X. Wu, J. Wu, P. Li, Y. Han, and L. Li, “Implementations and experiences of wide-area hvdc damping control in china southern power grid,” in *IEEE PESGM*, July 2012, pp. 1–7.

[15] Y. Zhao, C. Lu, P. Li, and L. Tu, “Applications of wide-area adaptive hvdc and generator damping control in chinese power grids,” in *IEEE PESGM*, July 2016, pp. 1–5.

[16] E-ISAC SANS Report, *Analysis of Cyber Attack on the Ukrainian Power Grid*. E-ISAC, 2016.

[17] H. Ren, Z. Hou, H. Wang, D. Zarzhitsky, and P. Etingov, “Pattern mining and anomaly detection based on power system synchrophasor measurements,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, no. PNNL-SA-131425. Pacific Northwest National Lab.(PNNL), Richland, WA (United States), 2018.

[18] S. Pal, B. Sikdar, and J. H. Chow, “Classification and detection of pmu data manipulation attacks using transmission line parameters,” *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 5057–5066, Sep. 2018.

[19] S. Brahma, R. Kavasseri, H. Cao, N. R. Chaudhuri, T. Alexopoulos, and Y. Cui, "Real-time identification of dynamic events in power systems using pmu data, and potential applications—models, promises, and challenges," *IEEE Transactions on Power Delivery*, vol. 32, no. 1, pp. 294–301, Feb 2017.

[20] H. Ren, Z. Hou, and P. Etingov, "Online anomaly detection using machine learning and hpc for power system synchrophasor measurements," in *2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, June 2018, pp. 1–5.

[21] M. Zhou, Y. Wang, A. K. Srivastava, Y. Wu, and P. Banerjee, "Ensemble-based algorithm for synchrophasor data anomaly detection," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2979–2988, May 2019.

[22] S. Matthews and A. St. Leger, "Leveraging mapreduce and synchrophasors for real-time anomaly detection in the smart grid," *IEEE Transactions on Emerging Topics in Computing*, pp. 1–1, 2019.

[23] Y. Shen, W. Yao, J. Wen, H. He, and C. Luo, "Resilient wide-area damping control for interarea oscillation considering communication failure," in *2017 IEEE Power Energy Society General Meeting*, July 2017, pp. 1–5.

[24] S. Zhang and V. Vittal, "Design of wide-area power system damping controllers resilient to communication failures," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4292–4300, Nov 2013.

[25] ——, "Design of wide-area power system damping controllers resilient to communication failures," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4292–4300, Nov 2013.

[26] M. E. Raoufat, K. Tomsovic, and S. M. Djouadi, "Virtual actuators for wide-area damping control of power systems," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4703–4711, Nov 2016.

[27] S. Khosravani, I. N. Moghaddam, A. Afshar, and M. Karrari, "Wide-area measurement-based fault tolerant control of power system during sensor failure," *Electric Power Systems Research*, vol. 137, pp. 66 – 75, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378779616300712

[28] M. E. Bento, "A hybrid procedure to design a wide-area damping controller robust to permanent failure of the communication channels and power system operation uncertainties," *International Journal of Electrical Power & Energy Systems*, vol. 110, pp. 118 – 135, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0142061518331247

[29] J. D. Taft, *Assessment of Existing Synchrophasor Networks*, 1st ed. Pacific Northwest National Laboratory, 2018.

[30] A. L. Samuel, "Some studies in machine learning using the game of checkers," *IBM Jour. of R&D*, vol. 3, no. 3, pp. 210–229, July 1959.

[31] S. J. Russell and P. Norvig, *Artificial intelligence: a modern approach*. Malaysia; Pearson Education Limited,, 2016.

[32] Matlab, "Cloud Center Parallel Computing - 1024 Workers." [Online]. Available: https://www.mathworks.com/help/cloudcenter/ug/cloud-center-release-notes.html

[33] S. Huang, K. Chen, C. Liu, A. Liang, and H. Guan, "A statistical-feature-based approach to internet traffic classification using machine learning," in *Int. Conf. on Ultra Modern Telecom. Workshops*, Oct 2009, pp. 1–6.

[34] P. Maragos, J. F. Kaiser, and T. F. Quatieri, "On separating amplitude from frequency modulations using energy operators," in *IEEE Int. Conf. on Acoustics, Speech, and Signal Processing*, vol. 2, 1992, pp. 1–4.

[35] I. Kamwa, A. K. Pradhan, and G. Joos, "Robust detection and analysis of power system oscillations using the teager-kaiser energy operator," *IEEE Tran. on Power Systems*, vol. 26, no. 1, pp. 323–333, Feb 2011.

[36] E. Kvedalen, "Signal processing using the teager energy operator and other nonlinear operators," *Uni. of Oslo Dept. of Informatics*, 2003.

[37] A.-O. Boudraa, J.-C. Cexus, M. Groussat, and P. Brunagel, "An energy-based similarity measure for time series," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, p. 1, 2008.

[38] W. Zhang, C. Liu, and H. Yan, "Gene time series data clustering based on continuous representations and an energy based similarity measure," in *Int. Conf. on Machine Learning and Cybernetics*, vol. 4, July 2010.

[39] H. Hotelling, "Analysis of a complex of statistical variables into principal components." *Journal of educational psychology*, vol. 24, no. 6, 1933.

[40] Y. Xu, D. Zhang, F. Song, J.-Y. Yang, Z. Jing, and M. Li, "A method for speeding up feature extraction based on kpca," *Neurocomputing*, vol. 70, no. 4, pp. 1056 – 1061, 2007.

[41] F. Song, Z. Guo, and D. Mei, "Feature selection using principal component analysis," in *Int. Conference on System Science, Engineering Design and Manufacturing Informatization*, vol. 1, Nov 2010, pp. 27–30.

[42] A. Lasisi and N. Attoh-Okine, "Principal components analysis and track quality index: A machine learning approach," *Transportation Research Part C: Emerging Technologies*, vol. 91, pp. 230 – 248, 2018.

[43] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard, M. Kudlur, J. Levenberg, R. Monga, S. Moore, D. G. Murray, B. Steiner, P. Tucker, V. Vasudevan, P. Warden, M. Wicke, Y. Yu, and X. Zheng, "Tensorflow: A system for large-scale machine learning," in *12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16)*. Savannah, GA: USENIX Association, 2016, pp. 265–283. [Online]. Available: https://www.usenix.org/conference/osdi16/technical-sessions/presentation/abadi

[44] Matlab, "Machine Learning Package." [Online]. Available: https://www.mathworks.com/solutions/machine-learning.html

[45] M. Jung, O. Niculita, and Z. Skaf, "Comparison of different classification algorithms for fault detection and fault isolation in complex systems," *Procedia Manufacturing*, vol. 19, pp. 111 – 118, 2018, proceedings of the 6th International Conference in Through-life Engineering Services, University of Bremen, 7th and 8th November 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2351978918300167

[46] A. Ashok, S. Krishnaswamy, and M. Govindarasu, "Powercyber: A remotely accessible testbed for cyber physical security of the smart grid," in *IEEE PES ISGT Conference*, Sept 2016, pp. 1–5.

[47] W. Yao, L. Jiang, J. Wen, Q. Wu, and S. Cheng, "Wide-area damping controller of facts devices for inter-area oscillations considering communication time delays," *IEEE Tran. on Power Systems*, vol. 29, 2014.

[48] M. E. Aboul-Ela, A. A. Sallam, J. D. McCalley, and A. A. Fouad, "Damping controller design for power system oscillations using global signals," *IEEE Transactions on Power Systems*, vol. 11, no. 2, pp. 767–773, May 1996.

[49] Hongxia Wu and G. T. Heydt, "Design of delayed-input wide area power system stabilizer using the gain scheduling method," in *2003 IEEE Power Engineering Society General Meeting (IEEE Cat. No.03CH37491)*, vol. 3, July 2003, pp. 1704–1709 Vol. 3.

[50] Matlab, "h2hinfsyn - H_2/H_∞ synthesis." [Online]. Available: https://www.mathworks.com/help/robust/ref/h2hinfsyn.html

[51] Y. Zhou, J. Liu, Y. Li, C. Gan, H. Li, and Y. Liu, "A gain scheduling wide-area damping controller for the efficient integration of photovoltaic plant," *IEEE Transactions on Power Systems*, vol. 34, no. 3, pp. 1703–1715, May 2019.

[52] G. Sánchez-Ayala, V. Centeno, and J. Thorp, "Gain scheduling with classification trees for robust centralized control of psss," *IEEE Transactions on Power Systems*, vol. 31, no. 3, pp. 1933–1942, May 2016.

Gelli Ravikumar (SM'2010, M'2017) is an Assistant Research Professor in the Department of Electrical and Computer Engineering, Iowa State University (ISU), USA. He received a Ph.D. degree in the Department of Electrical Engineering at the Indian Institute of Technology Bombay, India, in 2016. His research expertise is in the areas of Power system control and analysis, System stability, AI and Machine Learning, Attack-resilient control algorithms, Cyber-physical system security for the smart grid, and Cloud computing. He is active in 4 research projects sponsored by NSF and DOE research grants. He has contributed to 15+ research grant-writing proposals for funding, including the Department of Energy (DOE), National Science Foundation (NSF), and Power Systems Engineering Research Center (PSERC).

Manimaran Govindarasu (Fellow) is currently the Mehl Professor of Computer Engineering in the Department of Electrical and Computer Engineering at Iowa State University (ISU). His research expertise include CPS security for the smart grid, cyber security, and real-time systems. He is the Founding Chair of the Cybersecurity Task Force/Working Group within IEEE PES CAMS Subcommittee. He currently serves as an Associate Editor for IEEE Transactions on Smart Grid and IEEE Transactions on Mobile Computing. His research program is funded by NSF, DOE, DHS, and PSERC.