Anomaly Detection and Mitigation in FACTS-based Wide-Area Voltage Control Systems using Machine Learning

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

***Abstract*—With the increasing deployment of Flexible AC Transmission System (FACTS) devices in wide-area voltage control systems (WAVCS) for achieving improved voltage stability of bulk power systems, the possibility for cyber attacks on these systems is also increasing. Successful stealthy cyber attacks that are difficult to detect by traditional informational technology (IT)-based cybersecurity solutions or threshold-based bad data detectors can lead to a voltage collapse in power grid. This paper presents the testbed-based attacks implementation and real-time evaluation of machine learning (ML) algorithm for detecting and mitigating stealthy cyber attacks on FACTS-based WAVCS on a hardware-in-the-loop (HIL) testbed. Initially, we discuss the implementation of a fuzzy logic controller (FLC) that controls a Static VAR Compensator (SVC) device deployed in a two-area four-machine Kundur power system for improving transient voltage stability. Later, the ML-based Anomaly Detection and Mitigation (ADM) system is implemented on the cyber-physical HIL testbed to detect and mitigate various stealthy cyber attacks, which are injected in real-time over the wide-area network (WAN). The experimental results show accurate and effective performance of ADM system in detecting and mitigating anomalies while keeping the grid stable and within the system operating limits, as defined by the North America Electric Reliability Corporation (NERC).**

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

2022 IEEE Power & Energy Society General Meeting (PESGM) | 978-1-6654-0823-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/PESGM48719.2022.9916839

I. Introduction

Over the recent years, with the increase in electric power demand and extreme weather events, organizations like NERC and The North American Transmission Forum (NATF) have recommended use of FACTS devices for wide-area control of power grids to improve voltage stability and prevent voltage collapses [1], [2]. To this end, there has been increasing deployment of FACTS-based wide-area voltage control schemes as well as extensive research in this field [3]–[6]. At the same time, there is an increasing threat of cyber-attacks on power grid applications that utilize wide-area communications.

Traditionally, most of the wide-area monitoring, protection, and control (WAMPAC) applications that have been researched and developed for achieving reliable operations in the smart grid have been developed without consideration for cybersecurity. This calls for the development of efficient and accurate cyber security solutions that can defend the wide-area communication system, specifically, measurement and control signals necessary for WAMPAC applications, against stealthy cyber-attacks. In the recent years, there has been a significant growth in research literature on cyber attack-resilient algorithms that focuses on securing WAMPAC applications against stealthy cyber attacks that bypass traditional cybersecurity measures. A data-driven algorithm and a physics model-based method are proposed in [7] for false data injection attack detection in WAMPAC-based HVDC systems. A machine-learning-based methodology for detection of stealthy cyber attacks in wide-area protection systems is proposed in [8]. Some research has also been focused on the implementation and evaluation of attack-resilient algorithms for WAMPAC applications on real-time testbeds [8]–[10]. But there still exists a need for development and HIL testbed-based evaluation of attack-resilient methodologies and algorithms for various WAMPAC applications like FACTS-based WAVCS. Previously, we performed the impact analysis of different data integrity attacks and showed their impact using the voltage profile index (VPI) [11].

This work involves the implementation and evaluation of anomaly detection and mitigation system for WAVCS on a hardware-in-the-loop (HIL) testbed which closely emulates real-world grid characteristics. This allows for the evaluation of offline trained ML model (*Fine KNN*), proposed by us in [12] in a close to real-world environment. Additionally, the cyber attacks that introduce anomalies in the system are injected in the live environment with a realistic response from the system. The results show high accuracy in anomaly detection with small time-delays followed by the mitigation of the cyber attacks to minimize the impact of the attack. The mitigation successfully prevents the propagation of impacts of the anomalies till they persist in the system, stabilizing the grid to operate within the System Operation Limits (SOL) as dictated by NERC for bulk power systems.

This paper is organized as follows: Section II shows the architecture and design of the WAVCS, Section III delineates the proposed algorithm methodology and implementation, Section IV shows the HIL Testbed-based implementation and performance evaluation, and Section V concludes the work.

II. FACTS-based WAVCS: Architecture & Design

A. System Architecture

This subsection presents a high-level architecture for developing the response-based wide-area voltage control system (WAVCS) that has been developed through a joint effort of Bonneville Power Administration (BPA), Ciber Inc., and Washington State University (WSU) [5], [6]. In general, the WAVCS utilizes positive sequence PMU measurements from several substations and provides several corrective actions, including generator tripping and switching FACTS devices

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

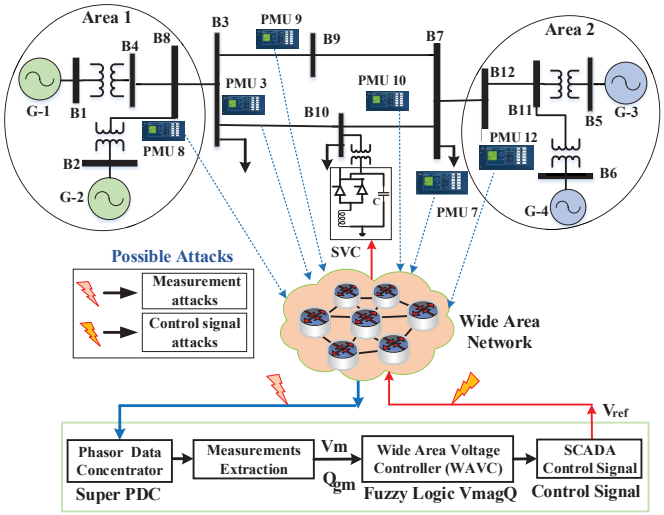

Fig. 1. High-level system architecture of WAVCS with its attack surfaces

that is decided through the rules-based fuzzy logic controller (FLC), operating between 0.15 to 0.3 seconds.

In this paper, one of our key contributions is to implement the FLC on the modified Kundur's four-machine two-area system, as shown in Fig. 1. This system consists of two symmetrical areas (Area 1 and Area 2) that are connected through two 230 kV lines of 220 km length and and each area consists of two generators of ratings (900 MVA, 20 kV). Note that the kundur system is well-known to study dynamic voltage stability [13], oscillation damping, power interchange, etc. In this test system, we have connected an additional PQ load (60 MW, 30 Mvar) to the bus 10 to create a voltage stress in the grid network.

In this architecture, the applied FLC 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. The SVC injects or absorbs reactive power as required to improve the voltage profile during disturbances. Based on the existing wide-area synchrophasor network, possible attack surfaces on measurement and control signals are also highlighted by lightning bolt symbols.

B. Design of FLC

The major steps involved in designing FLC include voltage stability analysis to select sensitive bus voltages and applying *V magQ* algorithm to calculate (V_{ref}) for the SVC. The details of these steps are discussed here.

Step 1 (Voltage stability analysis): The static voltage stability analysis [13] is performed by computing power flow jacobian matrix, J, during modal analysis. 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).

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

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

$$\Delta Q = J_R.\Delta V_{PQ} \quad (3)$$

$$\Delta V = J_R^{-1}.\Delta V_{PQ} \quad (4)$$

For the given Kundur system, the computed reduced Jacobian matrix, J^{-1}, is a square matrix; and hence both modal analysis and singular value approach can be applied for the voltage stability analysis. Fig. 2 shows the computed magnitude of the output singular vector for all buses for a maximum singular value of 0.135. In this case, with the computed magnitude of 0.65734, bus 10 represents the most sensitive node followed by bus 9, bus 7, and bus 3. This finding also supports the fact of optimal location of SVC in this system, i.e., bus 10.

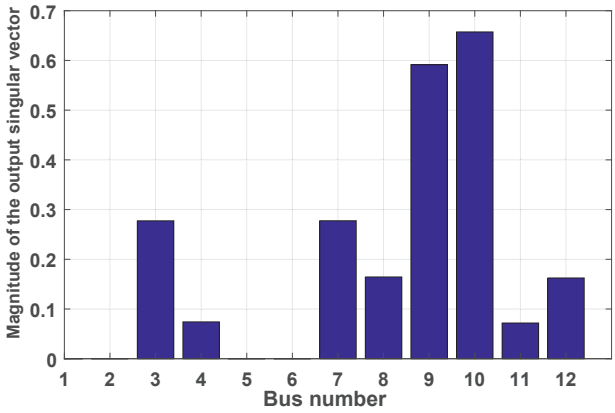

Fig. 2. Output singular vector plot for the static voltage stability analysis.

Step 2 (Apply *V magQ* algorithm): We have applied 11 rules, stated in [5], to calculate V_{ref} using weighted and normalized voltage and reactive power measurements.

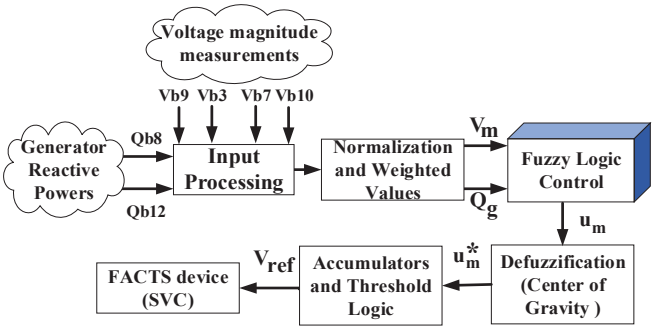

Fig. 3. *V magQ* algorithm-based FLC scheme of FL-WAVCS

Fig. 3 illustrates the *V magQ* 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. Also, reactive power measurements of area 1 and area 2 are collected using bus 8 (Qb8) and bus 12 (Qb12) for input features as they provide the accumulative power injection for these four sensitive buses. The overall scheme is categorized into four major stages.

978-1-6654-0823-3/22/$31.00 ©2022 IEEE

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 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 Anomaly Detection and Mitigation System: Methodology and Architecture

Machine Learning algorithms are being extensively used for detection of anomalies in Cyber-Physical Systems (CPS) [14]. ML-based algorithms help in the detection of cyber-attacks as well as in differentiating between non-cyber system events (like system faults) from cyber-injected anomalies, which otherwise are hard to model.

Fig. 4 shows the methodology adopted for the development and evaluation of the proposed Anomaly Detection and Mitigation (ADM) system. The methodology involves two broad steps, *offline process* and *real-time implementation process*. The *offline process* has been presented in [12], which shows a comparison of the performance evaluation of various ML models for the cyber-anomaly detection and mitigation in the FACTS-based WAVCS for the power system discussed in Section II. The *offline process* discussed in [12] yielded in the Machine Learning (ML) model *Fine KNN* with the best performance for detection of stealthy cyber attacks in the FACTS-based WAVCS having an overall detection accuracy of 99.99% and a false positive rate of less than 0.04%.

This paper deals with the *real-time implementation process* of the ADM system along with the testing and performance evaluation. The *real-time implementation process* involves three steps: (1) Implementation of trained KNN model in the HIL Testbed; (2) Simulation of system faults and injection of real-time stealthy cyber attacks through the communication network; and (3) Evaluating the performance of the ADM system using attack detection time and accuracy as well as monitoring power system stability after mitigation of cyber attacks.

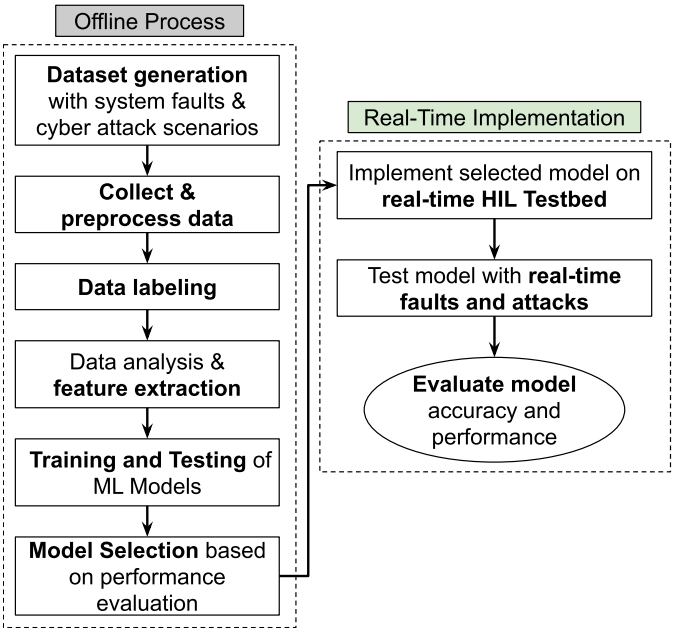

Fig. 4. Proposed anomaly detection and mitigation system methodology

We use the Voltage Profile Index (VPI) of the power grid given by (5) as a metric to monitor the voltage stability of the grid and to evaluate the performance of the ADM system. The VPI is the root-mean square deviation of the bus voltage magnitudes from the reference voltage, that is, 1 pu [15]. The VPI enables the performance evaluation of the proposed algorithm with respect to the NERC's SOL.

$$VPI = \frac{1}{n}\sum_{i}^{n}\sqrt{\frac{1}{T}\sum_{i=1}^{T}(|V_{i,ref}| - |V_i|)^2} \tag{5}$$

where T is the simulation time-step, V_i is the voltage magnitude at bus i, and $V_{i,ref}$ is 1 pu for all the buses. The bus voltages taken into consideration for calculating the VPI are V_{B3}, V_{B7}, V_{B8}, V_{B9}, V_{B10}, and V_{B12} ($n = 6$).

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
Ramp Attack (Measurement & Control)	Slope = [1, 2, 3, 4, 5]
Fault Type	**Fault Duration**
L-L-L (A-B-C) at B9	Start Time (seconds) = 8 End Time (seconds) = 8.2

Various stealthy cyber attacks injected in the system are summarized in Table I.

The methodology used for mitigating the cyber attacks is depicted in fig. 5. The FACTS device (SVC)-controlled power system sends wide-area measurements to the FLC and the

978-1-6654-0823-3/22/$31.00 ©2022 IEEE

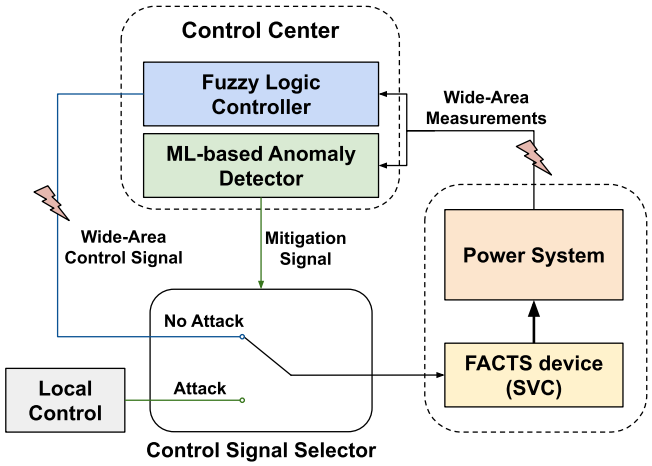

Fig. 5. Overview of anomaly detection and mitigation methodology

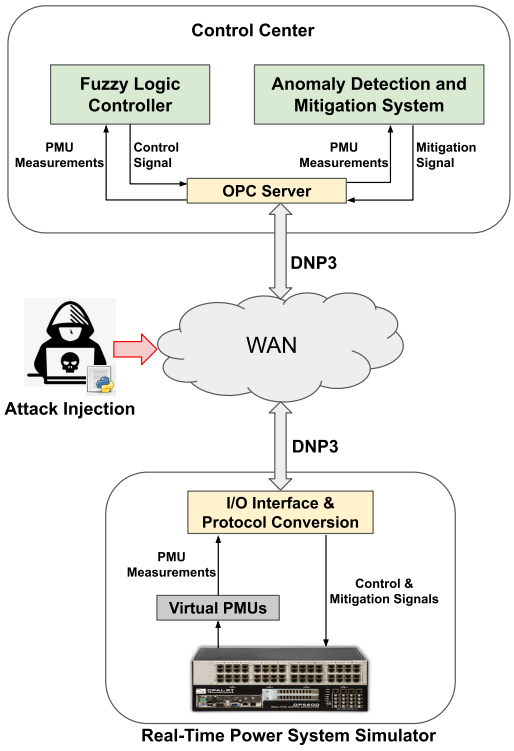

Fig. 6. HIL Testbed-based architecture for anomaly detection and mitigation

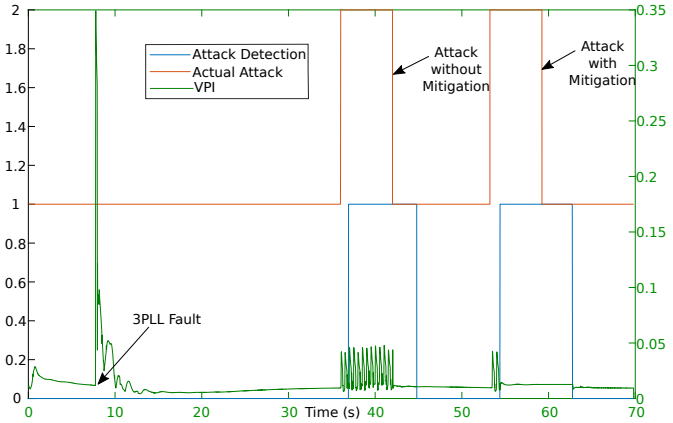

Fig. 7. VPI and attack detection by ADM algorithm for pulse attack on control signal

ADM system situated in the control center. The FLC calculates a control signal based on the input measurements and sends an appropriate control signal (V_{ref}) to the SVC. The ADM system constantly monitors the power system for anomalies using the input measurements. In case the ADM system detects an anomaly, it sends a mitigation signal to the *Control Signal Selector* which switches the control signal of the SVC from *wide-area control* to *local control*. The *Local Control* provides a constant V_{ref} to the SVC affecting the optimal operation of the power system. When the cyber attack is stopped, the ADM system resets the mitigation signal and subsequently, the input control signal to the SVC is switched back to the wide-area control signal sent by the FLC to allow for wide-area voltage control of the power system for optimal operation of the grid.

IV. HIL Testbed-based Real-Time Evaluation

A. HIL Testbed Architecture and Implementation

Fig. 6 shows the overall architecture for implementation of the ADM system in the HIL testbed present at the Iowa State University [16]. The SVC-based two-area Kundur power system is implemented in the real-time power system simulator (RTPSS) The PMU measurements from the virtual PMUs within OPAL-RT are converted to DNP3 communication protocol and sent over the wide-area network (WAN) to the OPC server in the control center. The control center is implements the FLC and the ADM system in real-time environment. The FLC and the ADM system receive wide-area measurement signals from the OPC server. The FLC sends the control signal to the SVC in RTPSS over the WAN through the OPC Server. Pulse and ramp attack signals are injected by the attacker through the WAN. After injection of attacks, the ADM system detects and classifies the attacks and sends an appropriate mitigation signal back to the power grid (as depicted in fig. 5) through the OPC server over the WAN. The control signal and the mitigation signal are also sent using DNP3 communication protocol to the RTPSS.

B. Real-Time Performance Evaluation

Figs. 7 and 8 show the VPI of the system under fault conditions (3-phase line-to-line (3PLL) fault) and for pulse and ramp attacks on the control signal. The plots also show the time of actual attack injections and time of detection (with and without mitigation) of attack by the ADM system. These results also show the action of the control signal of the FLC which is able to damp the transient oscillations within a few seconds (up to 5 seconds) after the fault is injected and cleared. The red plots show the attack injection by the attacker and the blue plots show the attack detection (with and without mitigation) by the ADM system. During the attack (left y-axis value is 2 for pulse attack and 3 for ramp attack), when the mitigation is turned off, the impact of the attack on the VPI of the system can be seen for the entire duration of the attack even though the attack is detected by the ADM system (left y-axis value is 1 for attack detected and 0 for

978-1-6654-0823-3/22/$31.00 ©2022 IEEE

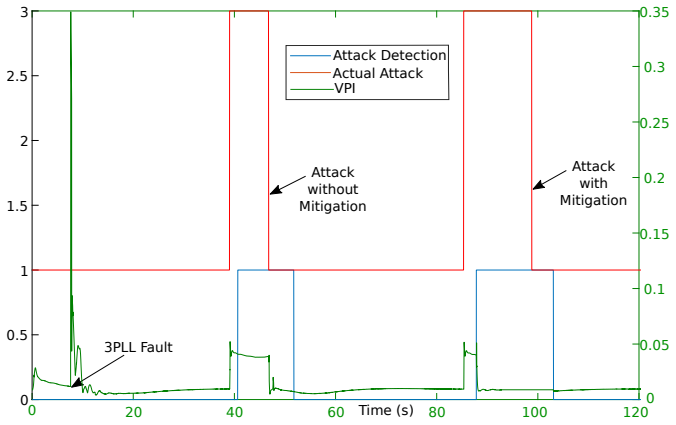

Fig. 8. VPI and attack detection by ADM algorithm for ramp attack on control signal

no attack detected). On the other hand, when the mitigation is turned on, the impact of the attack is briefly seen on the system VPI due to the short delay in detection (referred to as detection time). Post the detection of the attack, the mitigation signal immediately mitigates the attack impact and stabilizes the system voltage using *local control* instead of *wide-area control*. The mitigation signal resets the system to *wide-area control* as soon as the ADM system detects the removal of attack, further improving the voltage profile. For the plots in Figs. 7 and 8, the pulse attack duty cycle is 50% and the period is 0.5, and the ramp attack slope is 1.

TABLE II
REAL-TIME PERFORMANCE OF THE ADM SYSTEM FOR VARIOUS ATTACKS

Attack Type	**Average Detection Time** (s)	**Average VPI during Attack - with mitigation** (% deviation from $1pu$)
Pulse: Control	1.17	1.39%
Ramp: Control	2.5	1.51%
Pulse: Measurement	1.55	1.14%
Ramp: Measurement	1.02	1.18%

TABLE III
NERC SOL FOR BULK POWER SYSTEMS

System Voltage Limits (% deviation from $1pu$)	**System State**
$\pm 5\%$	Normal State (24 hours)
$\pm 8\%$	Emergency State ($\leq$4 Hours)
$\pm 10\%$	15-minute Emergency State ($\leq$15 minutes)

The results for the real-time performance of the ADM system for all the attack parameters mentioned in Table I are summarized in Table II, averaged for each attack type. The results show that the power system operating limits are well within the SOL set by NERC for bulk power systems which are summarized in Table III.

V. CONCLUSION AND FUTURE WORK

This work presents the HIL testbed-based implementation and evaluation of ML algorithm in WAVCS cybersecurity using local FACTS device in real-time. In particular, this work shows the efficient performance of Fine-KNN in detecting and mitigating anomalies in a realistic cyber-physical environment. The experimental results show an efficient performance of the proposed algorithm in presence of stealthy cyber-attacks on the WAN by keeping the system stable and within the system operating limits, as stated by NERC. The future work includes red-team testing of this platform by third party with new attack parameters that are not included in the training phase of this algorithm. This testing will improve the robustness of ADM system and will also facilitate the subsequent development for field deployment.

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] North American Transmission Forum (NATF), "Transient Voltage Criteria Reference Document," 2016. [Online]. Available: https://www.natf.net/documents
[3] 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 GT&D*, 2017.
[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] B. Chen, S.-i. Yim, H. C. Kim, and R. Nuqui, "Cyber attack detection for wampac-based hvdc applications," in *2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, 2020, pp. 1–5.
[8] 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.
[9] 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.
[10] M. S. Almas, L. Vanfretti, R. S. Singh, and G. M. Jonsdottir, "Vulnerability of synchrophasor-based wampac applications' to time synchronization spoofing," *IEEE Transactions on Smart Grid*, 2018.
[11] 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.
[12] B. Hyder, V. K. Singh, M. Govindarasu, and R. Nuqui, "Machine learning-based cyber-physical anomaly detection in wide area voltage control systems," in *IEEE ISGT-NA [Accepted]*, 2022.
[13] L. Cai, "Dynamic voltage stability analysis in multi-machine power systems," *15th Power System Computation Conf.*, 2005.
[14] 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.
[15] A. S. Musleh, S. M. Muyeen, A. Al-Durra, I. Kamwa, M. A. S. Masoum, and S. Islam, "Time-delay analysis of wide-area voltage control considering smart grid contingences in a real-time environment," *IEEE Transactions on Industrial Informatics*, 2018.
[16] G. Ravikumar and M. Govindarasu, "On-Premise Cloud-based HIL CPS Security Tesbted for Smart Grid," 2020. [Online]. Available: https://powercybertestbed.ece.iastate.edu/

978-1-6654-0823-3/22/$31.00 ©2022 IEEE