Impact of False Data Injection Attacks in Wide Area Damping Control

Abhishek Saini
Dept. of Electrical Engineering
IIT Dharwad
Dharwad,Karnataka, India
202021007@iitdh.ac.in

Pratyasa Bhui
Dept. of Electrical Engineering
IIT Dharwad
Dharwad,Karnataka, India
pbhui@iitdh.ac.in

Abhinav Kumar Singh
Electronic and Computer Science
University of Southampton, Southampton, Hampshire, GB
London,UK
A.K.Singh@soton.ac.uk

Faheem Ul Haq
Dept. of Electrical Engineering
IIT Dharwad
Dharwad,Karnataka, India
201081002@iitdh.ac.in

Chakravarthi Kotakonda
Dept. of Electrical Engineering
IIT Dharwad
Dharwad,Karnataka, India
193081001@iitdh.ac.in

***Abstract*—Wide area measurement based damping controllers are used to mitigate the inter-area oscillations in a large geographically distributed power system. The performance of wide area damping control (WADC) heavily relies on cyber and physical infrastructure. As the measured input signals used in WADC are transferred to the controller location via a communication channel, it is prone to cyber-attacks. The attacker can inject malicious data into the WADC measurements and/or control signals. This paper focuses on modeling and analyzing the impact of different types of false data injection (FDI) attacks on the WADC control signals, namely, sinusoidal attack, triangular attack, sawtooth attack, ramp attack, pulse attack, random attack, and replay attack. The control architecture for analyzing these attacks consists of power system stabilizers placed on each generator for damping of local modes and an H_2/H_∞ based WADC controller for damping of inter-area modes in Kundur's 4-machine 2-area test system. Different types of attacks were compared for their severity, and it has been found that a sinusoidal attack has the highest severity of all the analyzed FDI attacks. The results obtained in this paper will be useful in implementing the cyber-attack detection and mitigation algorithms.**

***Index Terms*—Wide area damping control, low frequency oscillation, phasor measurement units**

I. Introduction

A modern power system is a large scale multi-area system, in which real-time measurement data are transmitted from various substations via phasor measurement units (PMUs) to phasor data concentrators (PDCs) [1]. The PDCs send data to the main remote control center, where estimation and control signals are generated for real-time monitoring and dynamic control of the system. However, in a wide area power system, electro-mechanical low-frequency oscillations can cause instability and impose restrictions on transmission lines' power transfer capability. Such low frequency inter-area oscillations are primarily caused by poorly damped modes or eigenvalues of the system which have frequencies in the range of 0.2 to 0.8 Hz and also have high participation from electromechanical states of generators in two or more areas [2].

The local measurement-based power system stabilizer designed using phase compensation or residue method is used for damping out local mode of oscillations as they lack global observation capability. In contrast, the wide area measurement system provides global modal observability using PMUs to damp inter-area oscillations through wide area damping control (WADC) [3].

WADC is generally implemented in the main control center. As shown in the Fig.1, it takes measurement signals (line power flow, bus voltages, speed deviation, etc.) as input and generates control signals as output which are transmitted to the plant actuators (Flexible AC transmission system (FACTS) controller, Automatic voltage regulators (AVRs), High-voltage direct current (HVDC) controllers). The operation of the WADC is impacted by both the cyber system (consisting of the control and communication infrastructure) and the physical system (consisting of the actuators and the rest of the power system). The different attack locations are also shown in the diagram. The attacker can manipulate the measurement signal, control signal, or both. The stealthy cyber attack can bypass the bad data detection algorithm and disrupt the performance of WADC operations. For example, a false data injection attack at the measurement signals results in generating an inaccurate control signal by WADC, which causes serious damage to grid stability.

Some practical examples of WADC application in real-world power systems are the centralized adaptive WADC-HVDC system through the modulations of multiple HVDC link for damping inter-area oscillations and generator exciter control, which has implemented in China Southern Grid and Central China Grid. [4], and a similar WADC-HVDC system for the Pacific DC intertie in the North American Western Interconnection [5]. Unfortunately, in recent years numerous cyber-attacks have happened on power systems around the globe. For instance, in 2015, a coordinated cyber-physical attack

This is the author's accepted manuscript (AAM) version of
DOI: 10.1109/NPSC57038.2022.10069455

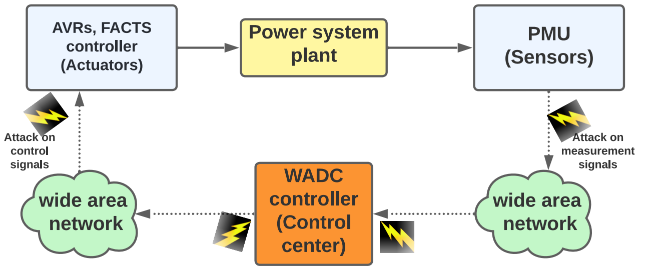

AVRs, FACTS controller (Actuators)
Power system plant
PMU (Sensors)
Attack on control signals
Attack on measurement signals
wide area network
WADC controller (Control center)
wide area network

Fig. 1: Structure of wide area power system with different attack locations.

jeopardized the Ukraine power grid and caused its blackout [6]. This attack resulted in approximately 2,25,000 consumers losing power across regions. Thus, it is vital for the power system's security to analyze how false data injection attacks (FDIA), replay attacks, denial of service (DoS) attacks, and other attacks affect the security of supply and stability of a power system.

This paper provides an impact-analysis of different types of FDI attacks on control signals, modelled using both existing and new models proposed in this paper, with varying attack parameters. To the best of our knowledge, this is the first effort to analyze the impact of various FDI attacks on inter-area oscillations, such that the attacks that yield maximum damage through WADC can be identified.

The significant contributions of this paper can be abbreviated as follows:

- Different FDI attacks template are proposed and replay attack is modeled and implemented on the WADC control signals.
- The impact of various attack cases for different attacks signal frequency and magnitude are analyzed on inter area oscillations.
- The attack impact study is validated by demonstrating various attack scenarios on Kundur's benchmark systems with H_2/H_∞ based WADC controller.
- Results obtained from the simulation study are compared with the different attacks cases.

The rest of the paper is organized as follows. Section II presents the wide-area power system modeling, and different models of existing and proposed FDI attacks. Section III provides a brief description of the test system. Section IV presents experiments and simulation results. Finally, Section V provides concluding remarks.

II. Modeling of Power System with WADC and Cyber Attacks

The practical power system is inherently nonlinear, and the dynamical behavior of the system is described from differential algebraic equations (DAE). Further, the reduced-order linearized model is obtained from the DAEs to analyse small-signal stability. Control design further requires model-order reduction of the linearized system [7]. The linearized power system model can be expressed with a state space model as follows.

$$\begin{aligned}\dot{x}(t) &= Ax(t) + Bu(t)\\ y(t) &= Cx(t)\end{aligned} \tag{1}$$

where $x \in \mathbb{R}^n$, are the state vector (e.g. generator speed deviation, rotor angle etc.), u is the control vector to generators' exciters or AVRs. y is the remote signal transmitted via PMU to the main control center, which can be the speed difference of generators in two areas, deviation in line power flow, bus voltage etc. **A** represents the system state matrix, **B** and **C** are input and output matrices of appropriate dimensions. For studying the impact of cyber-attacks in the case of wide area damping controller, various data integrity attacks (power system integrity is compromised through manipulating transmission data) are considered here for modeling, namely random attack, sinusoidal attack, replay attack, ramp attack, pulse attack, triangular attack and saw-tooth attack. The attack modeling mainly focuses on manipulating measurement and control signals. These attacks manipulate the control and measurement signals by compromising the communication network or the control center, which affects the authenticity of true adjustment commands produced by the control center, due to which the power system becomes unstable. The modeling of cyber attacks for the WADC system pertains to the three-dimensional attack space proposed in [8]. The attack locations can be compromised, and a malicious attack vector can be injected into the actuator and sensor channels of the power system model in (1) can be characterized as follows.

$$\begin{aligned}\dot{x}(t) &= Ax(t) + Bu(t) + B_a\chi_u(t)\\ y(t) &= Cx(t) + C_s y_s(t)\end{aligned} \tag{2}$$

where $\mathbf{B_a}$ and $\mathbf{C_s}$ are two gain matrices and $\chi_u(t)$ and $y_s(t)$ represents the actuator and sensor attack signals, respectively. The actuator channels produce response by acknowledging control signals for damping low-frequency oscillation, [9], [10]. Considering only actuator attacks (or control signal attacks) in the attack model, (2) can be represented as follows.

$$\begin{aligned}\dot{x}(t) &= Ax(t) + B\left(u(t) + \chi_u(t)\right)\\ y(t) &= Cx(t)\end{aligned} \tag{3}$$

The malicious attack signal which manipulates the actuator channel can be modeled as

$$\chi_u(t) = \Psi^u u_\chi(t) = \begin{bmatrix} \eta_1 & & 0\\ & \ddots & \\ 0 & & \eta_n \end{bmatrix} \begin{bmatrix} u_{\chi_1}(t)\\ \vdots \\ u_{\chi_n}(t)\end{bmatrix} \tag{4}$$

where the fabricated data injected into the actuator channels is mapped by binary incidence matrix represented as Ψ^u and the compromised actuators' fabricated data is described by $u_\chi(t)$. The malicious data $u_\chi(t)$ applied for implementing various FDI attacks at the actuator channels is modelled as in (5).

$$u_\chi(t) = \begin{cases} 0 & \text{for } t \notin \tau_a\\ \lambda \cdot \mathcal{K}(.) & \text{for } t \in \tau_a \end{cases} \tag{5}$$

where, λ represents attack signal magnitude, the function $\mathcal{K}(.)$ represents the nature of the attack signal, and τ_a denotes the duration of the attack.

1) Pulse attack: In the case of the pulse attack, the attack vector is injected in the form of a pulse signal, and it can be additive or subtractive to the true data signal. The pulse attack signal can be modeled with different period T_p and the width of the pulse t_w can be altered using using a positive integer n. The magnitude of pulse attack signal is varied using λ. The model of a pulse attack is given as follows.

$$u_{\chi}(t) = \begin{cases} 0 & \text{for } t \notin \tau_a \\ \lambda_p \cdot \mathcal{K}_p & \text{for } t \in \tau_a \end{cases} \tag{6}$$

$\mathcal{K}_p$ in (7) represents the pulse signal.

$$\mathcal{K}_p = \begin{cases} 1 & \text{for } 0 < t_w < T_p/n \\ 0 & \text{for } T_p/n < t_w < T_p \end{cases} \tag{7}$$

Other types of attack modeling are discussed below, and are given in (8).

$$u_{\chi}(t) = \begin{cases} 0 & \text{for } t \notin \tau_a \\ \lambda_s \cdot \mathcal{K}_s(\omega_s) & \text{for } t \in \tau_a \\ \lambda_{sa} \cdot \mathcal{K}_{sa}(T_{sa}) & \text{for } t \in \tau_a \\ \lambda_t \cdot \mathcal{K}_t(T_t) & \text{for } t \in \tau_a \\ \lambda_{ra} \cdot \mathcal{K}_{ra}(\lambda_{sra}) & \text{for } t \in \tau_a \\ \lambda_r \cdot \mathcal{K}_r & \text{for } t \in \tau_a \end{cases} \tag{8}$$

2) Sinusoidal attack: For sinusoidal attack modeling, the significant parameters are λ_s and frequency ω_s. The appropriate selection of signal frequency can cause large oscillation. According to the nature of the sinusoidal signal, it causes a sinusoidal variation in accurate data. The magnitude of the attack signal can be varied by varying λ_s. The system knowledge can be used to select the signal magnitude and makes an attack hard to detect [10].

3) Saw-tooth attack: This attack involves the manipulation of the control signal by injecting the saw-tooth signal, which can be additive or subtractive. The attack signal can be designed with different periods. In this case $\mathcal{K}_{sa}$ can be modeled as a saw tooth signal by selecting appropriate λ_{sa} and distinct time period T_{sa},where T_{sa} represents triangular signal time period.

4) Triangular attack: A triangular signal is injected into the control signal. According to the nature of the triangular signal, it causes a rise in the true data signal in the first half period and a fall in the next half period. The attack signal can be exclusive (subtractive type) or inclusive (additive type) . The triangular attack signal $\mathcal{K}_t$ is designed using appropriate λ_t and T_t, where T_t represents triangular signal time period. Different triangular signals can be modeled by varying λ_t.

5) Ramp attack: The attacker can prepare a ramp signal with suitable magnitude λ_{ra} and slope λ_{sra} , which can be a positive ramp or negative ramp signal. It introduces a gradual rise or fall of amplitude in the original signal. The attacker can implement a stealthy ramp attack $\mathcal{K}_{ra}$ by selecting the appropriate slope and magnitude. A gradual change in slope causes stealth ramp attack which can bypasses bad data detector algorithms [3].

6) Random attack: A random signal is modeled using the true data signal's minimum and maximum limits as constraints. The data injected in a random attack is not easily detectable by a bad data detection algorithm because data lies in the allowable range. The attack signal can be injected with uniform random values without violating permissible data range constraints. The random attack signal is designed using appropriate $\mathcal{K}_r$ and λ_r.

7) Replay attack: In replay attack, the attacker records actual control data during normal operation or event scenario and injects this data in place of actual data during the attack, which misleads the controller. For example, when a three-phase fault occur in a power system, the attacker can replay normal operation data, which can amplify the fault impact. Furthermore, the attacker can replay event data when the power system is in a normal operating state, due to which an erroneous control signal is sent by the control center. The replay attack is severe because the attacker doesn't alter the data using fabricated values, instead the attacker replaces the real data with recorded data. The replay attack is implemented in two steps: first, recording the data either through attacking a cryptography algorithm or manipulating local conditions and second, replaying the recorded data until the end of the attack. The modeling of attack is shown in Eq. (9), where $u(t-k)$ represents the recorded data.

$$\dot{x}(t) = \begin{cases} Ax(t) + Bu(t) & \text{for } t \notin \tau_a \\ Ax(t) + Bu(t-k) & \text{for } t \in \tau_a \end{cases} \tag{9}$$

III. POWER SYSTEM DESCRIPTION

1) Test power system: Kundur's 4-machine 2-area test system is considered for attack study, and the system incorporates two identical areas [2]. Each generator is equipped with a power system stabilizer (PSS), and generator 4 is connected with a wide area damping controller (WADC). The WADC controller is placed at the control center. Mixed H$_2$/H∞ based controller is implemented to damp out the poorly damped inter area oscillation [11]. The input signal (measurement signal) transmitted via communication channels to the controller is the line power flow deviation of the line $5-6$, and the generated output signal (control signal) is transmitted to generator 4, via communication channels.

2) Mixed H_2/H_∞ controller: In a practical power system, the load is continuously changing, and it is significant to consider the various uncertainties and dynamic operating conditions during the design of the controller. The H_∞ control improves frequency domain performance but is not capable of improving transient response for the closed loop system. While

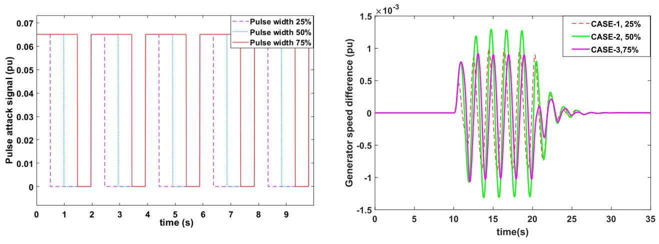
H_2 control's main goal is to improve the transient response and reject impulsive disturbance to ensure closed loop stability. The mixed H_2/H_∞ output feedback control is designed for maintaining trade off between conflicting requirements [11].

3) Selecting Attack Signal Magnitude: : Arbitrary injected signals can be easily detected if the attack signal's magnitude or frequency is inconsistent with the signal's typical magnitude or frequency. As the FDI attacks are implemented in the WADC control signal, first the control signal (WADC output signal) frequency is estimated during a three-phase fault using prony analysis. As expected, it is nearly the same as inter-area mode frequency. To calculate the magnitude limits for the attack signals, numerous three phase faults of $0.2s$ duration were simulated at different buses. The maximum range of the WADC control signal was obtained as $[-0.13227, 0.1123]$ for fault at bus 6 for $0.2s$. These magnitude limits are considered for modeling the FDI attacks.

IV. Experiments and Results

In this section, data integrity attacks are implemented to highlight the impact on the WADC control signal. It has been assumed that the attacker has access to the desired signals and can inject inaccurate data.

1) Pulse attack: A pulse attack signal is injected at the control signal. Numerous pulse signal attack vector can be developed by varying pulse width and pulse period. In this experiment, the pulse signal frequency is kept the same as the inter area mode frequency. Then the width of the pulse signal is changed to 25%, 50%, and 75% of the pulse signal total period. The attack signal with different pulse widths is shown in Fig.2a, and the magnitude in pu (per unit) is kept within the permissible limits. The attack signal is implemented at 10s for an attack duration of 10s. The speed deviation of generator $G3$ with respect to generator $G1$, $(\omega_3 - \omega_1)$ in pu is shown in Fig.2b. It can be concluded from Fig.2b that maximum oscillation is produced when the attack signal width is 50%.

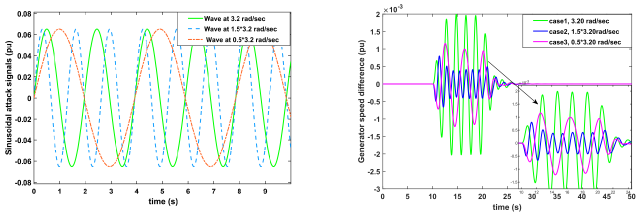


(a)

(b)

Fig. 2: The details of three types of pulse attack in pu for 10s is depicted in (a) and Speed deviation $(\omega_3 - \omega_1)$ in pu of generator $G3$ with respect to generator $G1$ for different pulse attacks is shown in (b).

2) sinusoidal attack: A sinusoidal attack signal can be added to the control signal at different frequencies. In an oscillation situation, the controller produces a signal in the interarea frequency range $(0.2 - 0.8)$ Hz. The attack signal is also injected at 50%, 100%, and 150% of the controller signal frequency. The attack signal at different frequencies is shown in Fig.3a. In three attack cases, the oscillation magnitude is highest when the attack signal and inter area mode are of same frequency and create a resonance, as shown in Fig.3b.

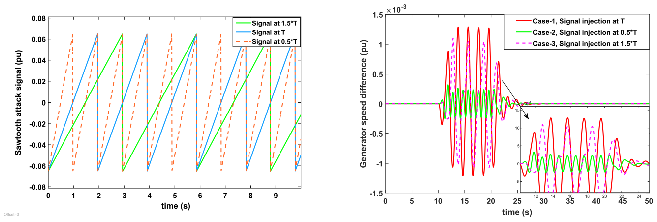


(a)

(b)

Fig. 3: Three types of sinusoidal attack signal for 10s is depicted in (a) and Oscillation comparison $(\omega_3 - \omega_1)$ in (b).

3) Saw-tooth signal: A saw-tooth signal of appropriate magnitude is injected into the control signal. Three cases for attack are considered, that is the fabricated signal time period varied as 0.5, 1.5, and kept the same as the inter area mode time period. The attack signal for different cases is shown in Fig.4a. The generator speed difference $(\omega_3 - \omega_1)$ is plotted for all attack cases and is shown in Fig.4b. The maximum oscillation was produced in the first case because the saw-tooth signal frequency was approximately identical to the inter area mode frequency, and the minimum amplitude of oscillation was produced in the second case, when the saw-tooth frequency is nearly double the inter-area mode frequency.



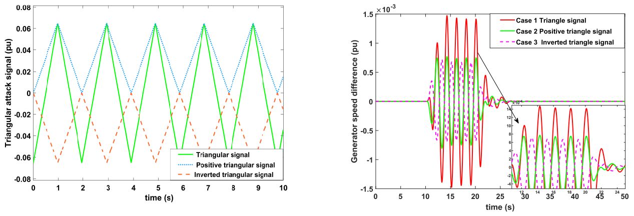
(a)

(b)

Fig. 4: Three types of saw-tooth attack signal for different time period is depicted in (a) and Speed deviation $(\omega_3 - \omega_1)$ for the different saw-tooth attack cases in (b).

4) Triangular attack signal: A triangular attack signal with different slopes is injected into the true signal. The modeled triangular attack signals are shown in Fig.5a. The oscillations produced due to distinct types of attack signals are shown in Fig.5b. The maximum oscillation is produced in case-1 when the attack signal is rising from -0.06 to 0.06 as shown in Fig.5a.

5) Ramp attack: A ramp signal is injected into the control signal with different slope values. Two cases are considered, the attack signal is injected at 10s with slope values 0.00651 and 0.00451 for attack duration of 10s. As the signal slope rises gradually, the oscillation doesn't appear instantly; fluctuations occur in the system after a few seconds. The oscillation produced is plotted in Fig.6 and demonstrates that Case-1 has a higher magnitude of fluctuation than Case-2.



(a) (b)

Fig. 5: Triangular attack signals for different cases are shown in (a) and Speed deviation $(\omega_3 - \omega_1)$ for distinct triangular attacks in (b).

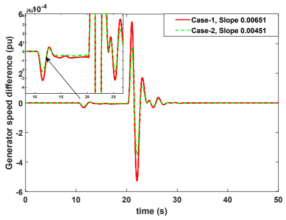
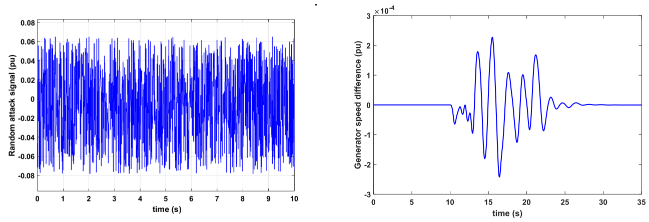


Fig. 6: The oscillation $(\omega_3 - \omega_1)$ comparison between two ramp attacks.

6) Random attack: A random signal is added to the control signal, injecting arbitrary values between the allowable minimum and maximum limits values of the control signal. The generated random signal is shown in Fig.7a, for which the values lie in $[-0.0784, 0.0651]$. The oscillation produced in the power system is shown in Fig.7b.



(a) (b)

Fig. 7: The random attack signal is shown in (a) and Speed deviation by random attack in (b).

7) Replay attack: For executing the replay attack, the data is recorded during a three-phase short circuit fault at bus number 10, for a duration of 10s, and replayed later until the attack is finished. The oscillation produced in the system is shown in Fig.8.

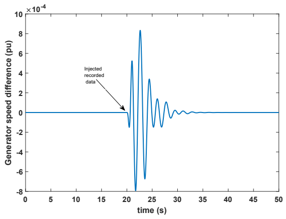


Fig. 8: Oscillation $(\omega_3 - \omega_1)$ due to replay attack.

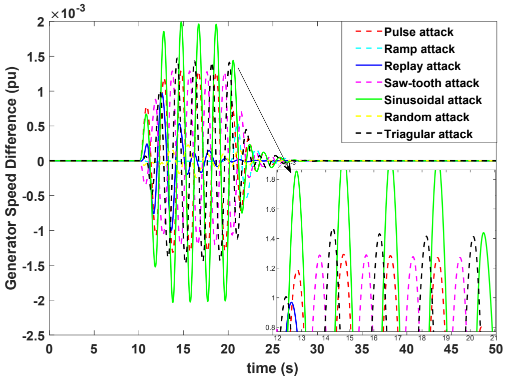


Fig. 9: The comparison result of different attack signals.

A. Comparison of Different FDI Attacks

Different types of FDI attacks and replay attack are compared here to identify the most severe FDI attacks in WADC. For each type of FDI attack, the most severe case is considered for comparison with other types of FDI attacks. For example, in the case of pulse attacks, the oscillation magnitude is highest when the pulse width is 50% and hence this case is selected. Further, the signal's peak magnitude is considered the same for all types of FDI attacks. Finally, the chosen attacks are compared with one another. It was observed that the amplitude of oscillation produced is largest for the sinusoidal attack, as depicted in Fig.9, because the component of the attack signal at inter-area mode is highest in this case which causes resonance. The highest oscillation is produced when sinusoidal attack signal is injected at the inter-area mode frequency. In general, closer the shape of the attack signal to a sinusoidal signal, and closer is its frequency to the inter-area frequency, the higher is the amplitude of the produced oscillation, and, hence, higher is the severity of the FDI attack.

V. CONCLUSION

This paper presents a procedure to design various FDI attacks and replay attack. Furthermore, it analyzes the impact of FDI attacks in WADC control signal on the power system. The attacks are implemented on Kundur's 4-machine 2-area test system. The simulation results demonstrate that a sinusoidal attack of inter-area mode frequency with appropriate magnitude causes the highest oscillation in the power system as compared to other FDI attacks. The future works include developing unsupervised and deep learning-based algorithms for detecting various data integrity attacks, DoS attacks, and coordinated attacks for WADC measurement and control signals.

ACKNOWLEDGEMENT

This work was supported by the project RSOP/21-26/TR/11 funded by CPRI and the Ministry of Power, India.

REFERENCES

[1] W. Qiu, K. Zhu, Z. Teng, Q. Tang, W. Yao, Y. Dong, and Y. Liu, "Cyber-attack identification of synchrophasor data via vmd and multi-fusion svm," *IEEE Transactions on Industry Applications*, 2022.

[2] P. Kundur, “Power system stability,” *Power system stability and control*, vol. 10, 2007.

[3] G. Ravikumar and M. Govindarasu, “Anomaly detection and mitigation for wide-area damping control using machine learning,” *IEEE Transactions on Smart Grid*, 2020.

[4] Y. Zhao, C. Lu, P. Li, and L. Tu, “Applications of wide-area adaptive hvdc and generator damping control in chinese power grids,” in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, IEEE, 2016.

[5] 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 wide area damping controller,” in *2017 IEEE Power & Energy Society General Meeting*, pp. 1–5, IEEE, 2017.

[6] M. Tian, M. Cui, Z. Dong, X. Wang, S. Yin, and L. Zhao, “Multilevel programming-based coordinated cyber physical attacks and countermeasures in smart grid,” *IEEE Access*, vol. 7, pp. 9836–9847, 2019.

[7] Y. Zhao, W. Yao, C.-K. Zhang, X.-C. Shangguan, L. Jiang, and J. Wen, “Quantifying resilience of wide-area damping control against cyber attack based on switching system theory,” *IEEE Transactions on Smart Grid*, 2022.

[8] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “A secure control framework for resource-limited adversaries,” *Automatica*, vol. 51, pp. 135–148, 2015.

[9] T. S. Ayyarao and I. R. Kiran, “A two-stage kalman filter for cyber-attack detection in automatic generation control system,” *Journal of Modern Power Systems and Clean Energy*, 2021.

[10] A. M. Mohan, N. Meskin, and H. Mehrjerdi, “A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems,” *Energies*, vol. 13, no. 15, 2020.

[11] Y. Zhang and A. Bose, “Design of wide-area damping controllers for interarea oscillations,” *IEEE transactions on power systems*, vol. 23, no. 3, pp. 1136–1143, 2008.