Data-Driven Security Monitoring for False Data Injection Attacks on Subsynchronous Damping Controllers in PMSG-based Wind Farms

Mehri Mirzahosseini

A Thesis

in

The Department

of

Concordia Institute for Information Systems Engineering (CIISE)

Presented in Partial Fulfillment of the Requirements

for the Degree of

Master of Applied Science (Information Systems Security) at

Concordia University

Montréal, Québec, Canada

June 2025

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Mehri Mirzahosseini**

Entitled: **Data-Driven Security Monitoring for False Data Injection Attacks on Subsynchronous Damping Controllers in PMSG-based Wind Farms**

and submitted in partial fulfillment of the requirements for the degree of

Master of Applied Science (Information Systems Security)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the Final Examining Committee:

_____ Chair
Dr. Suryadipta Majumdar

_____ External Examiner
Dr.

_____ Examiner
Dr. Anjali Awasthi

_____ Supervisor
Dr. Mohsen Ghafouri

Approved by _____
Chun Wang, Chair
Department of Concordia Institute for Information Systems Engineering (CIISE)

_____ 2025

_____
Mourad Debbabi, Dean
Faculty of Engineering and Computer Science

Abstract

Data-Driven Security Monitoring for False Data Injection Attacks on Subsynchronous Damping Controllers in PMSG-based Wind Farms

Mehri Mirzahosseini

The integration of Permanent Magnet Synchronous Generator (PMSG) Wind Turbines (WTs) into the power grid requires advanced control strategies to maintain stability and damp oscillations, particularly under weak grid conditions. These strategies, along with wind farm control loops, often rely on data transfer and information provided by communication networks.

However, the cyber layers used for such data transfer make the entire network prone to various cyber threats, such as False Data Injection Attacks (FDIAs). These attacks can compromise power grids' stability and operational integrity and result in blackouts. On this basis, we highlight the vulnerability of communication links of PMSG-based WF to FDIAs and propose a data-driven detection system developed based on a Convolutional Neural Network (CNN) to identify threats.

First, FDIAs are introduced in the simulation by manipulating the communicated signals between the SCADA system of the wind farm and WT controllers. Second, the CNN model is trained using grid and wind farm data in various operating conditions to detect FDIAs, distinguishing them from normal operational variations. To evaluate the performance of the proposed detection method, it is tested in a wind farm connected to a power system and compared with traditional data-driven detection methods based on K-Nearest Neighbors (KNN), Random Forest (RF), and Extreme Gradient Boosting (XGBoost). The results demonstrate that CNN achieves high detection rates with minimal false positives, validating its efficiency in detecting FDIAs in grid-connected wind farms.

Acknowledgments

I express my deepest gratitude to my supervisor, Dr. Mohsen Ghafouri, for his invaluable guidance, continuous support, and encouragement throughout this research. His patience, insightful feedback, and expertise have significantly shaped the direction of this thesis. I am especially grateful to him for providing me with the opportunity to be part of his research team.

I am deeply grateful to my parents for their love, patience, and belief in me. Their constant support has been the foundation of all my achievements, especially my mother, who has been my greatest source of strength, especially during difficult moments. I would like to express my deepest gratitude to my beloved husband, Peyman, for his support, patience, and encouragement throughout this research.

A heartfelt thank you to my younger brother, Ramin, whose wise and kind advice has always guided me through challenging times. His words have often brought clarity and strength when I needed them the most.

I would also like to thank my teammate, Masoud, for his valuable technical assistance. I sincerely thank my friend, Zeinab, for her encouragement and support throughout this journey.

To all those who supported me along this journey, thank you.

And last but not least, I thank myself for not giving up. You did it!

Contents

List of Figures viii

List of Tables ix

List of Acronyms xii

1 Introduction 1

1.1 Problem Definition 1

1.2 Objectives 2

1.3 Methodology 2

1.4 Contributions 4

1.5 Thesis Structure 5

2 Literature Review 6

2.1 Subsynchronous Phenomena in PMSG Wind Farms 6

2.2 SSCI Mitigation Techniques 7

2.3 Cyberattacks on Wind Farms 8

2.4 Cyberattack Detection Methods 10

2.5 Research Gap 12

3 Model of a Grid-Connected PMSG-based Wind Farm 13

3.1 Physical Layer 14

3.1.1 Control scheme of GSC 15

3.1.2 Weak Grid Conditions 16

3.1.3 Impact of Weak Grids on Wind Farms . . . 17
3.1.4 Mitigation Strategies for Weak Grid Conditions . . . 18
3.1.5 SSDC design . . . 18
3.1.6 SSDC Implementation . . . 20
3.2 Cyber Layer of PMSG-Based Wind Farms with SSDC . . . 21
3.2.1 Cyber-Physical Interactions and Communication Framework . . . 21
3.2.2 Cybersecurity Threats and Attack Scenarios . . . 22

4 Threat Modeling and Data-Driven Security Monitoring Framework 24
4.1 FDIAs on the Cyber Layer . . . 24
4.1.1 FDIA Threat Model and Attack Surface . . . 24
4.1.2 Impact of FDIAs on SSDC Stability . . . 25
4.1.3 Attack Scenario Simulation and Monitoring . . . 26
4.2 Motivation for Using CNN Architecture . . . 26
4.3 Model Capability Analysis: CNN vs. Traditional Models . . . 27
4.4 Data Generation for Model Training and Validation . . . 28
4.5 Signal Structure and Time Resolution of the Dataset . . . 29
4.5.1 Simulation Configuration and Time Step Estimation . . . 29
4.5.2 Recorded Signals and Dimensions . . . 29
4.6 Designing the CNN-Based Detection Model . . . 30
4.6.1 Structure of a CNN Network . . . 31
4.6.2 Hyperparameter Tuning . . . 34

5 Simulation Results and Analysis 36
5.1 Dataset Generation and Scenario Composition . . . 36
5.2 Hyperparameter tuning . . . 37
5.3 Benchmark Classifiers for Comparative Analysis . . . 37
5.3.1 Hyperparameter Optimization for Benchmark Classifiers . . . 39
5.4 Performance of customized CNN model . . . 40
5.5 Performance Evaluation of Classification Models . . . 43

6 Conclusion **45**

Bibliography **47**

List of Figures

Figure 3.1 The schematic of a Wind Farm including PMSG WTs connected to the power grid. 14
Figure 3.2 Control architecture of the grid-connected wind farm 16
Figure 3.3 System active power and reactive power, and voltage response to transition to weak grid at t=1s, without SSDC. 17
Figure 3.4 SSDC integration to the WFC 18
Figure 3.5 System active power and reactive power response to transition to weak grid at t=1s, with SSDC. 20
Figure 3.6 An overview for a cyber layer connection of a PMSG-Based Wind Farm . . 22
Figure 4.1 System response to an FDIA on Voltage measurement v_{dc}. 26
Figure 5.1 Accuracy and loss function for training and testing dataset plot. 41
Figure 5.2 Confusion matrices for different classification methods. 43

List of Tables

Table 3.1 PSO parameters for SSDC 20
Table 4.1 Logged Output Signals and Their Dimensions 30
Table 5.1 Classification performance comparison of different models 44

List of Acronyms

ADRC active disturbance rejection control

API Application Programming Interface

CPS Cyber-Physical Systems

DC Direct Current

DL Deep Learning

DT Decision Tree

EMT Electromagnetic Transient

FDIA False Data Injection Attack

FN False Negative

FP False Positive

ICT Information and Communication Technology

IEC International Electrotechnical Commission

IED Intelligent Electronic Devices

IEA International Energy Agency

IEEE Institute of Electrical and Electronics Engineers

KNN K-Nearest Neighbor

LQR Linear Quadratic Regulator

MFAC Model-Free Adaptive control

MITM Man-in-the-Middle

ML Machine Learning

MMAC Multiple Model Adaptive Control

MPPT Maximum Power Point Tracking

PCCs points of common coupling

PI Proportional Integral

PLL Phase-Locked Loop

PMSG Permanent Magnet Synchronous Generator

POI Point of Interconnection

PSO Particle Swarm Optimization

ReLU Rectified Linear Unit

RF Random Forest

RTU Remote Terminal Unit

SC Synchronous condensers

SCADA Supervisory Control and Data Acquisition

SCR Short Circuit Ratio

SDC Supplementary Damping Controller

SMC Sliding Mode Control

SSI Sub-synchronous Interaction

SSCI Sub-synchronous Control Interaction

SSDC Sub-synchronous Damping Controller

SSO Sub-synchronous oscillations

TCP/IP Transmission Control Protocol/Internet Protocol

TN True Negative

TP True Positive

VSC Voltage Source Converter

WF Wind Farm

WT Wind Turbine

WTC Wind Turbine Controller

XGBoost Extreme Gradient Boosting

Chapter 1

Introduction

1.1 Problem Definition

Wind energy plays a crucial role in modern power grids and nearly doubled its expansion in 2023 compared to 2019 [1]. By the end of 2024, the global wind energy capacity reached approximately 1,130 gigawatts [2], accelerating the move toward a low-carbon energy generation. This type of energy captures significant amounts of clean energy through Wind Turbines (WTs), aiding the replacement of fossil fuels and significantly reducing greenhouse gas emissions. Among various technologies, Permanent Magnet Synchronous Generator (PMSG) WTs are widely used due to various advantages, such as their ability to harvest energy at variable wind speeds, higher energy yield, less maintenance, and smaller size and costs, compared to WT with the gearbox [3],[4]. However, like other energy resources interfaced with the grid through inverters, integrating these PMSG WTs into weak grids presents stability challenges. One of the most critical issues is Sub-Synchronous Interaction (SSI) [5], an instability phenomenon that occurs at frequencies lower than the grid frequency. A common method to address SSI is to use Subsynchronous Damping Controllers (SSDC) at the wind farm level [6]. This auxiliary controller, which is often deployed in a wind substation, receives the measurements from WTs and sends the control commands back to local controllers of the turbines. These control signals are sent using the wind farm communication structure and the Supervisory Control and Data Acquisition (SCADA) systems [7]. As a result, wind farm operation demands extensive information exchange and data transfer, which makes them and the entire grid

prone to cyber threats. Multiple instances of cyberattacks targeting the wind farm SCADA system have been reported. For example, the first attack on sPower turbines occurred in the USA in 2019, and another incident involved ENERCON turbines in Germany, where a cyberattack on satellite communications disrupted SCADA access for 5,800 WTs [8]. On this basis, there is an urgent need to improve the security of PMSG Wind Farms, particularly when they are connected to weak power grids.

1.2 Objectives

The main objectives of this thesis are as follows:

- To identify FDI cyberattacks on SSDC and analyze the impact of these cyberattacks on the PMSG Wind Farm.
- To demonstrate the performance degradation of SSDC during the FDI cyberattacks
- To propose a security monitoring system based on a CNN architecture to detect FDIAs on SSDC in PMSG-based Wind Farms.

1.3 Methodology

In this study, we develop a data-driven detection framework based on CNN to identify FDIAs in the communication infrastructure of wind farms. The research methodology consists of three main stages:

- **System Modeling:** The first stage focuses on modeling a grid-connected Wind Farm in MATLAB Simulink, including the SCADA system and its communication links with the SSDC. To replicate the behavior of a weak grid, characterized by high source impedance and limited capacity to handle disturbances, the model is configured with elevated grid impedance values, reflecting the typical constraints of weak grids observed in real-world power systems. The SSDC is implemented using a fuzzy logic-based control approach, which dynamically adjusts its control parameters based on real-time system conditions. This allows for improved

adaptability compared to conventional Proportional-Integral (PI) controllers. To further enhance its performance, the SSDC parameters are optimized using the Particle Swarm Optimization (PSO) algorithm. The PSO framework iteratively adjusts the controller parameters to minimize the settling time of the DC-link voltage, ensuring optimal damping of subsynchronous oscillations under varying grid conditions. This combination of fuzzy logic control and PSO-based optimization enhances the SSDC's ability to stabilize Wind Farms connected to weak grids.

- **Attack Simulation:** To assess the impact of cyber threats on Wind Farm stability, multiple cyber vulnerabilities in the communication layer are identified and exploited in controlled attack simulations. FDIAs are introduced by manipulating the transmitted signals between the SCADA system and the SSDC, targeting critical control variables such as the DC-link voltage and reactive power reference signals. These attacks are implemented using predefined scaling factors and additive biases, mimicking real-world cyber threats to destabilize power grid operations. The simulation framework generates various attack patterns, including abrupt signal changes, gradual drifts, and sinusoidal disturbances, ensuring comprehensive evaluation under different adversarial conditions. The effectiveness of the SSDC in mitigating subsynchronous oscillations under attack conditions is also examined to highlight the potential vulnerabilities in the system.

- **Machine Learning-Based Detection:** Following the attack simulations, a dataset containing both normal and compromised operational states is generated through extensive time-domain simulations under varying wind power outputs and grid conditions. The dataset includes key system measurements such as active/reactive power, voltage, and current waveforms, all labeled according to whether they correspond to a normal state or an attack scenario. This dataset is then used to train and validate a CNN model, which autonomously extracts spatial and temporal features from the signal data to accurately classify attack instances. Unlike traditional machine learning approaches that require manual feature selection, CNNs excel at automatically learning patterns from raw data, improving classification accuracy. The CNN

model is evaluated against conventional data-driven classifiers, including K-Nearest Neighbors (KNN), Random Forest (RF), and Extreme Gradient Boosting (XGBoost). Performance metrics such as accuracy, precision, recall, and F1-score are used to ensure a comprehensive assessment of the detection framework.

The CNN-based detection model outperforms traditional approaches in identifying FDIAs, achieving high accuracy with minimal false positives. Feature engineering techniques such as normalization, data augmentation, and dropout regularization enhance its robustness. These improvements ensure reliable performance across various operating conditions, securing wind farm communication networks against cyber threats.

1.4 Contributions

This research presents a comprehensive approach to securing wind farm communication networks against FDIAs by integrating advanced control and machine learning techniques. The key contributions of this work are as follows:

- Developing a data-driven detection framework using CNN to identify FDIAs in wind farm communication networks.
- Designing a fuzzy logic-based SSDC optimized with PSO to enhance stability in weak grid conditions.
- Simulation various FDIA scenarios by manipulating SCADA control signals and evaluated their impact on wind farm stability.
- Comparing the proposed CNN-based detection system with traditional machine learning models including KNN, RF, and XGBoost, demonstrating superior accuracy and robustness against cyber threats.

1.5 Thesis Structure

This thesis comprises six chapters, each focusing on a fundamental component of detecting FDIAs in wind farm communication systems. The chapters are structured to provide a logical progression from background research to system modeling, attack simulation, machine learning-based detection, and final analysis.

Chapter 2 provides a comprehensive literature review, discussing previous research on wind farm cybersecurity, machine learning-based attack detection, and control strategies for mitigating stability issues in weak grids. Chapter 3 presents the physical modeling of a grid-connected wind farm and its cyber layers, detailing the SCADA system and the implementation of the SSDC. This chapter also explains the weak grid condition and the role of fuzzy logic-based SSDC optimized using PSO. Chapter 4 focuses on cybersecurity vulnerabilities and the methodology used for generating labeled datasets for training machine learning models. It covers the introduction of FDIAs into the communication network. Chapter 5 introduces machine learning-based detection models, with a primary focus on CNNs, and compares their performance with traditional classifiers such as KNN, RF, and XGBoost. This chapter details the model architecture, training process, and evaluation metrics. Finally, Chapter 6 summarizes the key contributions and findings of this research, highlighting the effectiveness of the CNN-based detection system compared with the other three classifiers.

Chapter 2

Literature Review

This chapter provides a structured review of the key challenges and emerging solutions associated with SSCI and cybersecurity in PMSG-based grid-connected Wind Farms. It begins by examining the root causes of SSCI, particularly under weak grid conditions, where dynamic coupling between converter control systems and grid impedance can lead to instability. The chapter further explores various SSCI mitigation strategies, including the deployment of subsynchronous damping controllers (SSDCs).

The second part focuses on the growing threat landscape in the cyber-physical layer of Wind Farms. It highlights the vulnerabilities of communication-dependent control components, such as SSDCs, to FDIAs, which can compromise system integrity and operational reliability. Then, Cyberattack detection techniques are introduced: model-based and data-driven approaches.

This chapter identifies research gaps by reviewing the state-of-the-art in SSCI mitigation and cyberattack detection. It underscores the need for a resilient, data-driven security monitoring framework to ensure the stability and security of grid-connected renewable energy systems.

2.1 Subsynchronous Phenomena in PMSG Wind Farms

With the growing integration of inverter-based resources (IBRs), such as wind and solar farms, subsynchronous oscillations (SSOs) have become a significant concern in power system stability.

In PMSG-based Wind Farms, particularly under weak grid conditions, various subsynchronous

phenomena can occur, manifesting as oscillatory behaviors at frequencies below the fundamental grid frequency. These include Subsynchronous Torsional Interaction (SSTI), caused by electrical excitation of mechanical shaft modes; Subsynchronous Control Interaction (SSCI), the interaction between the converter's internal control loops, such as phase-locked loop (PLLs), current regulators, and outer voltage loops, and a transmission line in sub-synchronous frequency; and Converter-Driven Subsynchronous Resonance (CD-SSR), which results from resonant behavior introduced by the converter's dynamic response in weak network conditions [9],[10], [6].

Among these, SSCI is considered the most relevant subsynchronous issue in PMSG-based Wind Farms. This phenomenon has been confirmed by several real-world SSCI events involving PMSG-based Wind Farms that have been reported under weak grid conditions. In 2011, a 4 Hz oscillation occurred in Texas following a 138-kV line outage [11]. Between 2011 and 2014, BPA reported the presence of oscillations, and a 450 MW PMSG-based wind power plant in Oregon was identified as the source [12]. In the summer of 2013, BPA's PMU monitoring system recorded 5 Hz oscillations in voltage as well as active and reactive power. By early 2014, 14 Hz oscillations were observed, with reactive power fluctuations reaching up to 80 Mvar peak-to-peak and active power output approaching 85% of the plant's rated capacity. In 2015 in Xinjiang, China, a serious SSO originated from the wind farms and propagated to the turbo generators more than 300 km away [6]. Similarly, in 2018–2019, 3.5 Hz oscillations were observed in Ontario, Canada, after a scheduled 230 kV bus outage that reduced grid strength, affecting both wind and solar units [11]. In 2019, a 9 Hz instability event in a 799 MW offshore wind farm in Great Britain triggered emergency de-loading due to SSCI caused by poor voltage control in a weak grid environment [13].

Given the increasing prevalence of such events, several SSCI mitigation strategies have been proposed in the literature, aimed at ensuring grid stability and protecting system components.

2.2 SSCI Mitigation Techniques

Numerous mitigation strategies have been proposed to enhance system stability and suppress SSCI, generally categorized into two main groups: converter-level techniques and grid-level techniques.

The first group includes converter-level strategies, particularly the implementation of Subsynchronous Damping Controllers (SSDCs) [6]. A wide range of SSDC designs has been developed in the literature, including linear quadratic regulator (LQR) [14], μ-synthesis [15], multiple-model adaptive control (MMAC) [16], PD controllers [17], feedback linearization theory and sliding mode control (SMC) [18], active disturbance rejection control (ADRC) [19], model-free adaptive control (MFAC) [20], Energy-Shaping Controllers [21], generalized harmonic compensation control strategies [22], partial feedback linearization [23], two-degree-of-freedom damping control loops [24], and traditional lead-lag damping schemes [25]. as an efficient mitigation approach within the wind farm control architecture [26], The integration of SSDCs directly within the converter control system without requiring major hardware modifications, makes them cost-effective, flexible, and highly suitable for retrofitting existing PMSG-based Wind Farms operating under weak grid conditions. Reference [27] implemented virtual inertia and grid-forming control strategies and enhanced the stability of power converters by actively regulating voltage and frequency. The SSDC in [5] was designed by optimizing inverter current control parameters to improve dynamic response, and adjusting voltage and reactive power control loops successfully prevented excessive oscillations.

The second group involves grid-level techniques, which include both passive and active methods. Passive damping elements, such as series-connected resistors or filters [28]. These are simple in structure but lack adaptivity and are often associated with high installation and thermal losses. On the other hand, active devices such as Synchronous Condensers (SCs), Static Synchronous Compensators (STATCOMs) [29], and Static Var Compensators (SVCs) [8] offer dynamic voltage and reactive power support to the grid. However, they are generally more expensive, require regular maintenance, and may pose integration challenges in complex wind farm topologies.

2.3 Cyberattacks on Wind Farms

The implementation of SSDCs in PMSG-based systems involves extensive communication between the wind farm SCADA systems, turbine controllers, and centralized supervisory devices. This makes the overall system inherently vulnerable to cyberattacks that can target either the availability or integrity of critical signals [30].

In practice, the SSDC depends on real-time access to voltage or frequency measurements, which are transmitted across potentially insecure communication networks. Common protocols used in wind farm SCADA systems, such as IEC 61400-25, IEC 60870-5, DNP 3.0, Modbus, and IEC 61850-7, were originally designed with a focus on interoperability, speed, and performance, rather than cybersecurity, and they suffer from critical security limitations. For instance, most of these protocols lack authentication, encryption, and integrity checks by default, making them vulnerable to spoofing, packet injection, and eavesdropping. Modbus and DNP 3.0 are particularly exposed to these attacks due to their plaintext communication and absence of session management. Even IEC 61850, although more modern, does not enforce secure key exchange or robust access control by default [31]. These shortcomings open the door to a wide range of cyberattacks, including false data injection (FDI), denial-of-service (DoS), replay, and man-in-the-middle (MITM) attacks [32].

Several real-world events illustrate the severity of these threats. A DoS attack in 2019 disrupted communication between a control center and multiple wind sites in Utah by exploiting firewall vulnerabilities, causing device reboots and unexpected outages [33]. In 2022, a cyberattack affected about 30,000 satellite terminals, disrupting over 5,800 ENERCON turbines and highlighting the vulnerability of remote communication links [34]. That same year, ransomware attacks targeted Nordex Group SE [35] and Deutsche Windtechnik [36], leading to widespread IT shutdowns and the suspension of turbine communication. Although these attacks did not specifically target SSDCs, they underline the urgent need to protect the entire wind farm cyber-physical infrastructure.

Most existing works, such as [37] and [38], analyze cyber-physical vulnerabilities and attack entry points in general SCADA systems, including the possibility of false shutdown commands to WTs. Other studies, such as [39] and [40], discuss FDI attacks against WT setpoints but do not focus on the SSDCs. Very few contributions explicitly consider attacks on SSDCs like [41], in which a communication delay Attack has been implemented in DFIG-based Wind Farm. This attack does not corrupt the content of the data but alters its timing, which can severely degrade the performance of the SSDC. [42] investigates two types of cyberattacks targeting a series-compensated DFIG-based Wind Farm. In the external attack, the adversary remotely trips a transmission line breaker, forcing the wind park to operate under weakened conditions that induce SSI. In the internal attack, the adversary injects false data into the SSDC's feedback loop, distorting control signals by

30–40%, which degrades damping performance and leads to prolonged SSOs.The most recent paper implements two cyberattacks on PMSG-based Wind Farm, the S_{PC} attack, which passively weakens grid strength by tripping transmission lines, and the S_{AC} attack, which disables STATCOMs to reduce active support. Both attacks destabilize converter control and trigger SSO [43].

2.4 Cyberattack Detection Methods

Cyberattack detection strategies are typically divided into model-based and data-driven approaches.

Model-based approaches rely on mathematical representations of cyber-physical systems (CPS) to detect cyberattacks by modeling normal system behavior. This enables the identification of anomalies that may indicate potential security threats. The model performs well when the system dynamics and parameters are fully known. However, their effectiveness declines in the highly variable and uncertain operating conditions common to PMSG-based Wind Farms. For instance, [38] and [37] analyze both cyber and physical layers of wind farm systems and investigate various potential attack entry points that could lead to issuing false shutdown commands to WTs. Additionally, [39] and [40] discuss FDI attacks targeting WT controller setpoints and examine their operational implications for wind farm systems. The effectiveness of these model-based methods heavily depends on system operating conditions, and their implementation requires precise knowledge of system parameters, which may not always be readily available.

On the other hand, data-driven methods apply machine learning algorithms to analyze real-time operational data, offering greater adaptability to evolving attack patterns. These methods can detect anomalies even in complex and dynamically changing grid environments by leveraging data from SCADA and control systems. Data-based detection methods outperform model-based approaches by eliminating the need for detailed physical modeling and enabling adaptive detection of unknown anomalies. They are more scalable, robust to system uncertainties, and suitable for real-time implementation in complex cyber-physical systems [44]. In reference [45], a model-free, data-driven framework based on high-dimensional statistical analysis was applied to detect and identify cyber and physical attacks in distribution power grids with high PV penetration. The approach operates

in real-time without requiring system modeling or prior training, making it suitable for practical deployment in noisy and dynamic smart grid environments. Recent advancements in deep learning have led to the development of intelligent cyberattack detection models tailored for power systems. A transformer-based model was proposed in [46], where a multi-head attention mechanism and embedded positional encoding were used to analyze frequency variations in hybrid power systems under FDIAs. This model outperformed conventional classifiers such as KNN [47] and SVM [48] and RF [49] by capturing subtle temporal anomalies in real-time signals. Similarly, a neural network approach combining Chebyshev graph convolutions and LSTM layers was introduced in [50] for FDIA detection in voltage stability monitoring. The method leveraged spatial–temporal relationships across the grid topology and demonstrated high detection accuracy, showing resilience against attacks. In [51], a Bidirectional Recurrent Neural Network (Bi-RNN) was integrated into an IEEE 1815.1-based cyber-physical architecture to identify anomalies arising from data manipulation and delay in substation communication. This sequential model effectively detected both short and long-term network anomalies, highlighting its suitability for real-time SCADA applications. These studies collectively illustrate the growing adoption of deep learning architectures for robust cyberattack detection in smart grid environments. However, it is important to note that most of these studies have focused on general cyberattacks and have not specifically addressed attacks targeting SSDCs in PMSG-based Wind Farms. Future work should prioritize developing hybrid detection frameworks that integrate model-based understanding with adaptive data-driven intelligence, capable of protecting internal control loops in the face of evolving cyber threats.

2.5 Research Gap

As the SSDC relies on accurate and timely data, any compromise in communication integrity can directly undermine system stability and control.Despite these contributions, no existing work has specifically investigated false data injection attacks (FDIAs) targeting the communication signals of SSDCs in PMSG-based Wind Farms. While some studies examine FDIAs on turbine-level setpoints, and others consider delay-based disruptions or command injections, the deliberate corruption of SSDC feedback signals, such as voltage or current measurements used as inputs of SSDCs, has not been addressed in the context of PMSG-based architectures. This gap is particularly critical given the increasing reliance of SSDCs on real-time, networked data, making them a vulnerable yet underexamined component in wind farm cybersecurity. To address these shortcomings, this work proposes a data-driven framework that leverages CNNs to learn complex spatiotemporal patterns in SSDC signal behavior without relying on explicit system models. CNNs are trained to identify anomalies in SSDC input signals under variable operating conditions, using raw signal features extracted from detailed simulation data. This system improves the detection of measurement-based FDIAs without requiring detailed system models. To the best of the authors' knowledge, no existing study in the literature offers such a unified solution capable of operating under varying grid conditions while maintaining high detection accuracy against signal-based FDIAs targeting SSDCs. This gap forms the basis of the present work.

Chapter 3

Model of a Grid-Connected PMSG-based Wind Farm

The initial focus of this chapter is on the components of the wind power system, detailing its configuration, transmission line characteristics, and control system architecture. Matlab Simulink software serves as the primary tool for modeling and capturing the dynamic response of the PMSG-based Wind Farms to facilitate the design of Supplementary Damping Controllers (SDCs). This model employs linearized equations and state-space representations to portray system behavior under varying dynamic conditions, thus streamlining the design process.

The design of the SSDC is further enhanced through the application of Particle Swarm Optimization (PSO), an iterative algorithm that fine-tunes control parameters to effectively mitigate SSCI and maintain system stability during disturbances, such as generator outages or fluctuations in grid conditions. Transitioning to the cyber aspects, the chapter explores the architecture of the SCADA system, analyzing its hierarchical control structures, communication technologies, and integration challenges. It also addresses the vulnerabilities introduced by the reliance on Information and Communication Technologies (ICTs) in the operation of wind farm, highlighting the necessity for resilient and secure designs to protect against potential cyber threats.

By integrating advanced control strategies like PSO-based SDCs with robust cyber-physical modeling, this chapter underscores a comprehensive pathway to enhance the reliability and security

of PMSG-based Wind Farms. It emphasizes the critical need to address both physical and cyber vulnerabilities, ensuring stable grid operations in the face of increasingly complex power networks and evolving cybersecurity risks.

3.1 Physical Layer

Fig. 3.1 shows a simplified diagram of a wind farm, designed in [52], including PMSG WTs connected to the Thevenin equivalent of a power grid through two parallel transmission lines. The farm is modeled by an aggregated WT. This turbine is composed of mechanical sections, which are connected to a synchronous machine. The machine is connected to a back-to-back converter topology to convert the generator AC current to DC and then to AC to be injected into the grid. The control scheme of the Grid Side Converter (GSC) is shown in Fig. 3.2. It should be noted that since the DC link separates the dynamics of the machine and Machine Side Converter (MSC) from the rest of the system, a DC current source is used to model them. The wind farm is connected to the grid and PCC through a filter, which is represented by its RL impedance ($Z_f = R_f + jX_f$). Two parallel transmission lines are used to transfer the power generated by the wind farm to the grid. The grid is represented as a voltage source (V_g) behind an impedance (Z_g). At $t = t_0$, Line 1 is disconnected by opening the circuit breaker. This leaves the wind farm radially connected to a weak

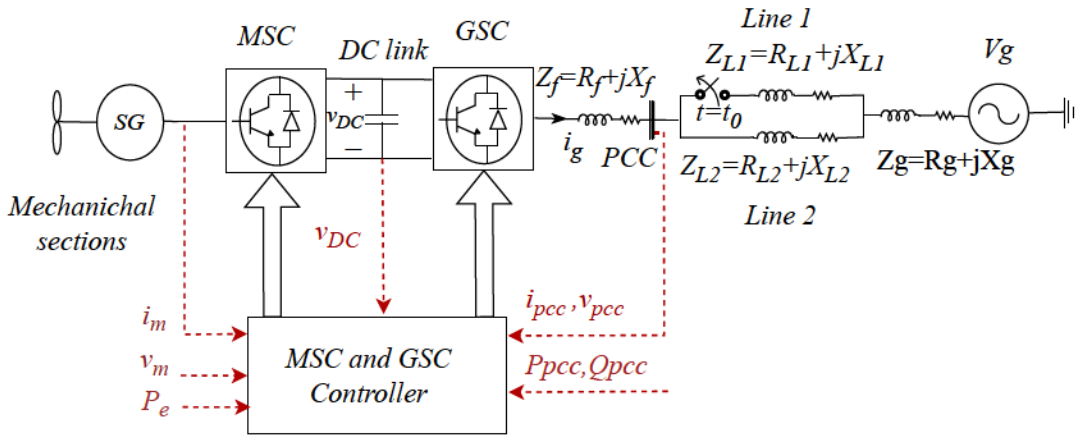

Figure 3.1: The schematic of a Wind Farm including PMSG WTs connected to the power grid.

grid. This simple representation of the grid is sufficient for discussion in this paper [53].

As depicted in Fig. 3.1, a PMSG-based Wind Farm is modeled as an aggregated WT, which is interfaced with a weak grid through a Voltage Source Converter (VSC). The model configuration and parameter values are adapted from the study presented in [52]. The total capacity of the turbine is 4 MW at a base voltage of 690V. The DC-link voltage is set at 1130 V, with a DC-link capacitance of 32.64 mF. The filter network consists of a resistance of $R_f = 0.471\ m\Omega$ and an inductance of L_f =30 μH, designed to smooth power flow and reduce harmonics. For grid connection, the grid resistance is R_g =1.84$ Ω, while the grid inductance is L_g =1.46$ mH, which indicates operation in a weak grid environment. The system regulates active power and reactive power using a dq-axis current control strategy, where P is mainly regulated through i_q, and Q is controlled through the i_d. A simplified PMSG-based Wind Farm, as shown in Fig. 3.1, should be linearized to design PI controllers in GSC. The obtained linearized state-space equations can be expressed as (1) and (2):

$$\dot{x} = Ax + Bu \tag{1}$$

$$y = Cx + Du \tag{2}$$

The matrices A, B, C, and D define the small-signal dynamics of the system. By simulating and analyzing the system's transient response, these state-space models enable the precise tuning of the PI controller coefficients within the GSC control loop.

3.1.1 Control scheme of GSC

In the GSC, the vector control technique is used to regulate the DC voltage and the reactive power production of the converter, as shown in Figure 3.2. The outer control loop in the q-axis is used to control the reactive power measured in the PCC (P_{PCC}). The reference reactive power (Q_{ref}) is compared with Q_{PCC} and the error signal is fed to a PI controller (PI_Q(s)) to determine the reference current for the inner loop i^{q}_{ref}. The inner loop compares i^{q}_{ref} with the measured q-axis current from the output of the GSC (i^{q}_g) and feeds it to another PI controller ((PI_i(s)) to determine $v^{*\mathrm{q}}_{GSC}$. In addition, feedforward terms are added to v^{q}_g to create v^{q}_{GSC}. The outer control loop in the d-axis is used to control v_{dc}. The reference DC voltage v_{dcref} is compared with v_{dc} and the error

signal is fed to a PI controller (PI_{dc}(s)) to determine the reference current for the inner loop (i^{d}_{ref}). The inner loop compares i^{d}_{ref} with the measured d-axis current from the output of the GSC (i^{d}_{g}) and feeds it to another PI controller (PI_i(s)) to determine $v^{*\mathrm{d}}_{GSC}$. Then the feedforward terms are added to v^{d}_{g} to create v^{d}_{GSC}.

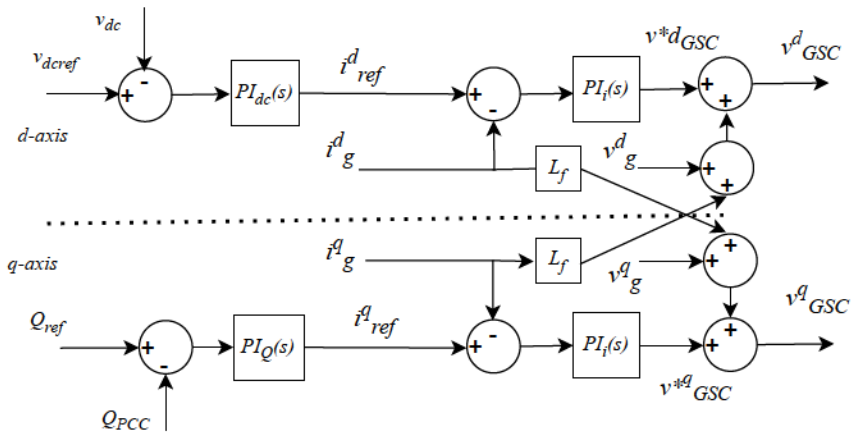

Figure 3.2: Control architecture of the grid-connected wind farm

3.1.2 Weak Grid Conditions

Grid strength at the PCC is measured by the Short Circuit Ratio (SCR), which is defined as (3):

$$SCR = \frac{S_{SC}}{MW_{WT}} \tag{3}$$

where MW_{WT} is the Wind Farm power capacity and S_{SC} is the system short circuit capacity, given by (4):

$$S_{SC} = \frac{U^2_{PCC}}{Z_g} \tag{4}$$

where U_{PCC} is the line nominal voltage at the PCC and Z_g is the grid impedance, as shown in Fig. 3.1. As seen from (3) and (4), grid strength is inversely proportional to the system impedance. A higher grid impedance results in a lower short-circuit capacity, leading to a weaker grid. Increased transmission line resistance and reactance make the system more sensitive to voltage fluctuations

and disturbances, which in turn lead to poor voltage regulation. The low short-circuit capacity of a weak grid reduces its ability to absorb disturbances, making the system more prone to instability. This limitation affects power quality and can cause excessive voltage deviations.

3.1.3 Impact of Weak Grids on Wind Farms

When an inverter-based resource, such as a PMSG-based Wind Farm, is radially connected to a weak grid, various stability issues arise. These oscillations are attributed to weak grid interactions, low SCR values, and inadequate damping in inverter control loops. Unlike strong grids, which naturally absorb fluctuations, low-SCR grids are highly sensitive to changes in power injection from wind farms.

Another critical issue in weak grid conditions is the interaction between grid impedance and Wind Farm controllers (WFC). Since wind farms operate using grid-following inverters, they rely on external grid conditions to regulate power injection. When grid impedance increases, the ability of the wind farm to control voltage and reactive power is significantly reduced. As a result, the stability margin of the system shrinks, making it more prone to oscillations. Fig. 3.3 presents the system response without the damping controller, illustrating severe oscillations in active power (P_{PCC}) and reactive power (Q_{PCC}), along with phase misalignment in three-phase voltage (V_{PCC}). These oscillations indicate instability in the weak grid configuration, which directly affects both i_g^{d} and v_{dc}, leading to power imbalances and system instability.

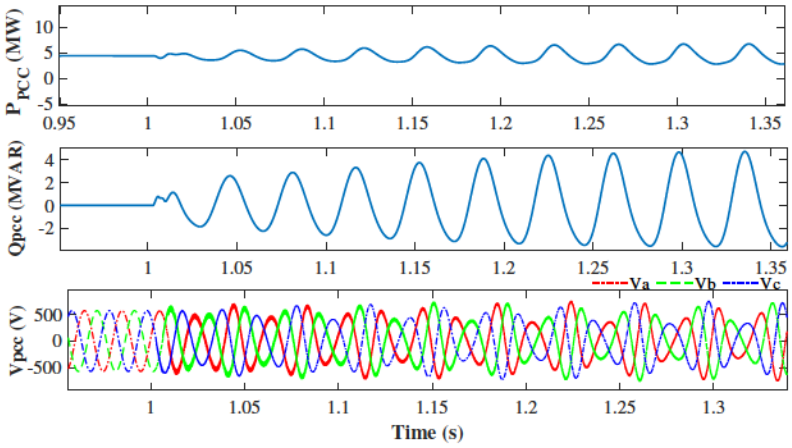

Figure 3.3: System active power and reactive power, and voltage response to transition to weak grid at t=1s, without SSDC.

3.1.4 Mitigation Strategies for Weak Grid Conditions

Several mitigation strategies have been proposed in both research and industry to enhance stability in weak grids. One of the most critical considerations for improving weak grid stability is that adaptive control mechanisms, such as self-tuning PI controllers, which can provide better stability by dynamically adjusting control gains based on real-time system conditions. In the next section, the development of an SSDC-based PI controller will be explored, focusing on real-time damping of oscillations in weak grids.

3.1.5 SSDC design

To address the SSOs that emerge under weak grid conditions, this study employs an SSDC embedded within the control architecture of a PMSG-based Wind Farm. As illustrated in Fig. 3.4, the SSDC receives the DC-link voltage error as its input and generates a corrective control signal to adjust the i^{d}_{ref} , thereby enhancing damping performance. The SSDC is implemented as a proportional–integral (PI) controller, with gains optimized using PSO.

The input to the SSDC is the DC-link voltage error as (5):

$$e(t) = v_{\mathrm{dcref}}(t) - v_{\mathrm{dc}}(t) \tag{5}$$

where v_{dcref} is the reference DC-link voltage and v_{dc} is the measured DC-link voltage of WTs.

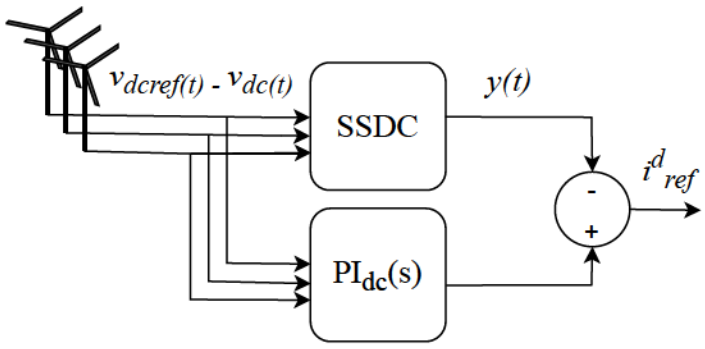

Figure 3.4: SSDC integration to the WFC

The control output is computed using the standard PI control law by (6):

$$y(t) = K_P \cdot e(t) + K_I \int_0^t e(\tau)\, d\tau \tag{6}$$

where K_P and K_I are the proportional and integral gains of the SSDC, respectively. The output $y(t)$ is added to thei_{ref}^{d} in the GSC's d-axis current control loop to enhance damping.

The PI gains are tuned using the PSO algorithm, which searches for optimal gain values that minimize a predefined objective function. In this work, the objective function is the settling time of the DC-link voltage, defined as (7):

$$J(K_P, K_I) = T_s \tag{7}$$

where T_s is the time taken for the v_{dc} to settle within 5% of its final value after a disturbance.

PSO is initialized with a swarm of candidate solutions, each representing a pair of (K_P, K_I) values. The particles update their positions using the following update rules (8), (9):

$$v_i^{(t+1)} = w \cdot v_i^{(t)} + c_1 r_1 \left(p_i^{\mathrm{best}} - z_i^{(t)}\right) + c_2 r_2 \left(g^{\mathrm{best}} - z_i^{(t)}\right) \tag{8}$$

$$z_i^{(t+1)} = z_i^{(t)} + v_i^{(t+1)} \tag{9}$$

where z_i and v_i are the position and velocity of particle i, p_i^{best} is the personal best position, g^{best} is the global best, and w, c_1, c_2, r_1, and r_2 are the inertia weight, cognitive and social parameters, and random numbers in [0,1], respectively.

The PSO algorithm is a population-based stochastic optimization method inspired by the collective movement of birds or fish [54]. Each particle evaluates its performance based on a fitness function that measures the system's settling time, overshoot, and steady-state error. During each iteration, particles adjust their positions based on their personal best solution, while the swarm converges towards the global best solution. As the parameters in Table 3.1 show, the optimization process is terminated after 10 iterations or when the particle velocity falls below a predefined threshold of 10^{-6}. This ensures rapid convergence while maintaining an optimal control response. The optimized PI gains directly affect i_g^{d}, ensuring that power injection remains stable and oscillations are mitigated.

Table 3.1: PSO parameters for SSDC

parameter	value
number of particles	10
maximum iterations	10
cognitive parameter c_1	2
social parameter c_2	2
inertia weight w	0.9
maximum velocity $w_{\max}$	0.1
tolerance ϵ	10^{-6}

In this study, we have utilized an adaptive PI controller to dampen the SSO and stabilize the grid. Unlike conventional PI controllers with fixed gains, the proposed controller dynamically adjusts its optimal proportional gain (K_P) and integral gain (K_I) based on system conditions. To adjust these optimal gains based on the system conditions, a fuzzy logic system is applied. The fuzzy logic controller processes the input and determines the required K_P and K_I as outputs. This ensures that the damping control action adapts to varying grid conditions, improving stability under weak grid scenarios.

3.1.6 SSDC Implementation

The adaptive PI controller is implemented to evaluate its performance in damping SSO. The controller is tested under varying weak grid conditions, where the system impedance is adjusted incrementally from 0.6 to 1 in 0.05 increments to analyze robustness. The response of i_g^{d} and v_{dc} is also observed to assess how the adaptive controller influences the current waveform, active power flow, and voltage stability.Fig. 3.5 shows the system response when the adaptive SSDC is activated.

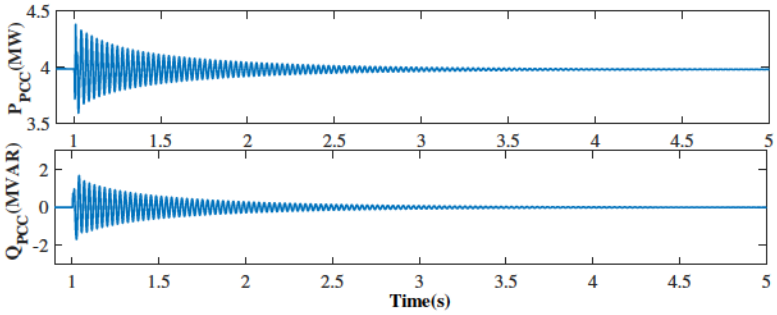

Figure 3.5: System active power and reactive power response to transition to weak grid at t=1s, with SSDC.

At $t = 1s$, the weak grid condition is introduced, but unlike the uncontrolled case, the oscillations in P_{PCC} and Q_{PCC} are significantly reduced. Additionally, the three-phase voltage and current signals maintain a stable phase alignment, demonstrating the controller's ability to mitigate instability. The dynamic adaptation of i_g^{d} directly stabilizes v_{dc}, ensuring efficient power exchange between the WT and the grid. As a result, voltage fluctuations are minimized, and the WT can continue injecting power without destabilizing the grid.

3.2 Cyber Layer of PMSG-Based Wind Farms with SSDC

The cyber layer of a PMSG-based Wind Farm is an interconnected network comprising several key components, including the SCADA system, the WFC, the Wide Area Controller (WAC), the Backup Remote Controller (BRC), the PCC Substation, and the Wide Area Network (WAN). The WFC integrates essential subsystems such as the SCADA server, application server, communication server, Human-Machine Interface (HMI), and data storage. The application server is responsible for processing computational tasks related to control algorithms and data analytics, while the communication server manages data exchange between various system components.

In this architecture, the SCADA system ensures real-time monitoring and control of WTs, facilitating bidirectional communication between field devices and control units. The SSDC module, hosted within the application server, processes the DC-link voltage signal (v_{dc}) and generates a control signal (y) to stabilize wind farm operations. The WAC provides centralized supervision of multiple wind farms across the grid, while the BRC ensures redundancy in case of system failures. The PCC substation serves as the interface between the wind farm and the main power grid, integrating Intelligent Electronic Devices (IEDs) and HMI interfaces to automate grid interconnection and control operations [55, 56].

3.2.1 Cyber-Physical Interactions and Communication Framework

The SCADA system is structured into three hierarchical levels: (i) The primary level, handling individual WT control, (ii) The secondary level, managing wind farm-level operations through the WFC, and (iii) The tertiary level, overseeing grid-level interactions via the WAC.

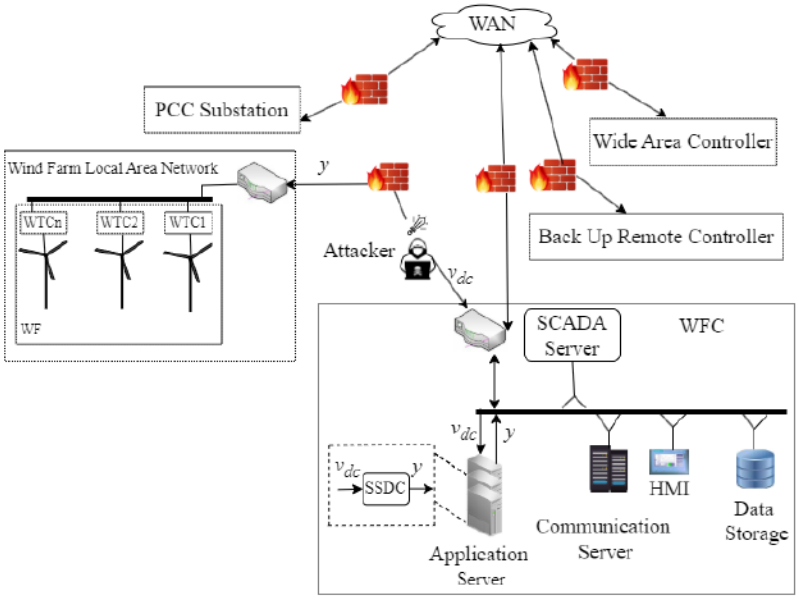

Figure 3.6: An overview for a cyber layer connection of a PMSG-Based Wind Farm

The communication architecture is divided into five distinct sub-networks [55, 56]: (i) The wind farm Local Area Network (Wind Farm LAN), which interconnects the WFC with field devices, including meteo sensors collecting meteorological data such as wind speed and temperature. (ii) The wind farm Controller (WFC) network, which operates as a standalone SCADA system managing the turbines using standard protocols such as IEC 61400-25, IEC 61850-7, and DNP 3.0 over TCP/IP [56]. (iii) The Wide Area Controller (WAC), which coordinates multiple wind farms to enhance grid stability. (iv) The Backup Remote Controller (BRC), which serves as a failover mechanism to maintain operational continuity in the event of WF failure. (v) The PCC Substation, which adheres to IEC 61850-7 standards for automation and communication, ensuring real-time control of physical components and interaction with the grid [55].

3.2.2 Cybersecurity Threats and Attack Scenarios

The increasing reliance on cyber-physical control systems introduces potential attack vectors that can compromise wind farm stability. Adversaries may exploit SCADA vulnerabilities to launch cyber attacks targeting the converter-driven stability of the grid [56]. The following attack scenarios are particularly relevant in the context of PMSG-based Wind Farms:

- **FDI Attacks:** Malicious alterations of measurements within the SCADA network can lead to erroneous control decisions, destabilizing wind farm operations [56].
- **MITM Attacks:** Cyber adversaries can intercept and modify control signals exchanged between the WF and WTs, disrupting system stability [55].
- **DoS Attacks:** Overloading the communication channels of the WF or WAC can lead to loss of control and delayed response times, resulting in severe grid instability [56].

In this work, we specifically focus on FDIAs by malicious alterations of v_{dc} measurement, which could significantly destabilize converter-based wind farms connected to weak grids.

Chapter 4

Threat Modeling and Data-Driven Security Monitoring Framework

4.1 FDIAs on the Cyber Layer

FDIAs pose one of the most significant threats to cyber-physical systems, especially those relying on SCADA infrastructure for real-time monitoring and control. In the context of wind farms employing PMSG, FDIAs can compromise control integrity by manipulating communicated signals within the SCADA environment. In particular, the SSDC module, which plays a vital role in stabilizing the system under weak grid conditions, becomes a key vulnerability when it receives manipulated measurement inputs such as the DC-link voltage (v_{dc}).

4.1.1 FDIA Threat Model and Attack Surface

The threat model considered in this thesis involves an adversary capable of intercepting and manipulating control signals within the cyber layer of the wind farm communication network. Specifically, the attacker targets the measurement signal $v_{dc}(t)$ that is transmitted to the SSDC module located in the application server of the WFC. By leveraging man-in-the-middle capabilities, attacker positions themselves between the measurement source and the application server. This allows real-time injection of a manipulated signal $z(t)$ that replaces the original measurement $x(t)$, thereby misleading the SSDC control logic and degrading damping performance. This constitutes a FDIA

executed via a compromised communication path by (10):

$$z(t) = \alpha \cdot x(t) + \beta \tag{10}$$

In this expression, $x(t)$ represents the original unmodified signal, while $z(t)$ denotes the attacker-manipulated signal. The parameter α is a scaling factor applied for proportional modification of the signal, and β is an additive offset introduced to further distort the signal. This formulation enables attackers to inject both amplitude-based and offset-based modifications to compromise the accuracy of control and monitoring functions in the power system. By carefully choosing α and β, the attacker can induce significant control misbehavior without triggering basic threshold alarms. For instance, α values slightly below 1 (e.g., 0.85–0.95) can suppress voltage amplitude without complete signal loss, mimicking degraded but plausible conditions. Similarly, non-zero β values can introduce sustained offsets that degrade SSDC response over time.

4.1.2 Impact of FDIAs on SSDC Stability

The SSDC relies on the accuracy of v_{dc} measurements to compute appropriate damping control commands y, which are sent to the inner control loops of the WTCs. Any distortion in this measurement chain directly affects the stability of power exchange between the PMSG units and the grid and degrades performance under weak grid scenarios. Figure 4.1 demonstrates the system response to the FDIA on the voltage measurement signal, where the values of α and β are, respectively, 0.8 and -0.1. The manipulated signal causes significant oscillations, which are transferred throughout the system, destabilizing the voltage and current waveforms. This disruption compromises the grid's stability and can lead to a cascade of failures. The results emphasize the importance of robust cybersecurity defense to safeguard the integrity of control systems in power networks against FDIAs. These impacts are especially severe in weak grid conditions, where real-time damping control is essential for maintaining synchronization and voltage regulation.

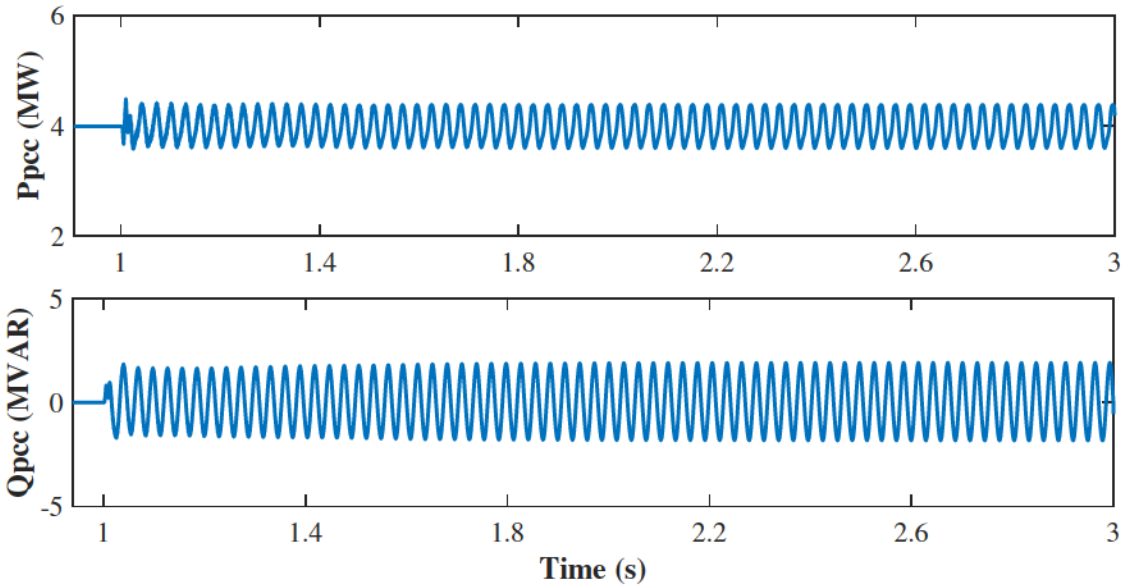

Figure 4.1: System response to an FDIA on Voltage measurement v_{dc}.

4.1.3 Attack Scenario Simulation and Monitoring

To analyze the effects of FDIAs, we implemented a simulated SCADA cyber layer model incorporating the SSDC and communication delays. In the simulation setup, the attacker manipulates the v_{dc} signal using randomly chosen α and β values within defined ranges to represent varying levels of attack severity. The system's response is then evaluated in terms of active/reactive power deviations, voltage oscillations at the PCC, and the SSDC output command y. A security monitoring module integrated into the SCADA server continuously logs the real-time values of v_{dc}, y, and other critical signals. These logs are used for post-event analysis and anomaly detection using data-driven models in the next stage of the framework.

4.2 Motivation for Using CNN Architecture

The motivation for adopting a CNN in our attack detection framework stems from its ability to automatically learn and extract discriminative features from complex multivariate time-series data, without requiring manual feature engineering. CNNs are especially effective for recognizing local patterns such as signal distortions, oscillations, abrupt spikes, and frequency changes — all of which are key indicators of cyber-physical attacks like FDIAs.

Unlike traditional machine learning models that rely on handcrafted statistical features, CNNs process raw or minimally preprocessed signals through convolutional layers that identify temporal and spatial correlations between input variables. These learned hierarchical features enable the model to generalize across different scenarios and attack intensities.

Furthermore, CNNs are computationally efficient, benefit from parameter sharing and local connectivity, and are well-suited for real-time detection systems. Their robustness to noise and scalability across large datasets make them an ideal choice for detecting subtle, fast-changing anomalies in dynamic environments such as power grids or industrial control systems.

4.3 Model Capability Analysis: CNN vs. Traditional Models

While XGBoost, Random Forest, and KNN are well-established techniques for classification tasks on structured or tabular data, they cannot inherently capture temporal dependencies and localized patterns present in raw multivariate time-series signals. In contrast, CNNs are particularly well-suited for anomaly and attack detection frameworks involving dynamic electrical signals. Their ability to automatically learn robust feature representations from raw input, combined with their strong performance on both temporal and spatial data, makes them highly effective in cyber-physical system monitoring applications.

CNNs offer significant advantages, including scalability to large datasets, suitability for real-time detection, and superior generalization under noisy or imbalanced data conditions. These strengths make CNNs particularly well-suited for cyber-physical system security applications, where dynamic signal variations and attack patterns are often subtle and complex. Given these capabilities, CNN was selected as the foundational architecture for our attack detection framework, enabling fast, accurate, and reliable classification of potential threats in power systems. To further support the architectural choice of CNNs in our detection framework, this section presents a detailed performance comparison between CNNs and three commonly used machine learning models: XGBoost, RF, and KNN. The comparison focuses on five key dimensions relevant to cyber-physical anomaly detection, including feature extraction, temporal modeling, scalability, generalization, and support for multivariate time-series data.

The proposed CNN architecture directly learns complex temporal features from unprocessed signals, eliminating the need for manual feature engineering. Its ability to model local temporal dependencies enables it to detect early transients and abrupt anomalies effectively. The use of regularization techniques such as dropout and batch normalization enhances generalization and robustness against noise and data imbalance. Furthermore, CNNs scale efficiently with data size and maintain the structure of multichannel input signals (e.g., voltage, current, power), allowing for accurate and real-time detection in large-scale, weak-grid scenarios.

4.4 Data Generation for Model Training and Validation

To build a comprehensive dataset for training and validating the attack detection model, a MATLAB Simulink-based simulation environment was developed to represent both normal and attack conditions in a power grid system under varying WT power input levels (P_{in}). The simulation captured six critical system output signals: active power (P_{PCC}), reactive power (Q_{PCC}), voltage (V_{PCC}), current (I_{PCC}), frequency (w_{PCC}) at the PCC, and an additional control output (y). All these signals are already available in SCADA measurements in wind farms. Each scenario was labeled according to the presence or absence of FDIAs, enabling supervised learning for the classification task.

The attack dataset was constructed by injecting FDIAs using 21 different values of the attack magnitude parameter α and 10 distinct values of the offset parameter β, resulting in a total of 210 attack scenarios. In parallel, the dataset includes 270 normal scenarios representing various non-attack conditions. These were generated by modifying the operating conditions through 9 different values of P_{in}, 10 values of α, and 3 values of β.

Furthermore, to diversify the dataset and emulate grid variability, additional scenarios were generated by changing the grid impedance. This extension added 470 more scenarios, comprising 220 normal and 250 attack cases. In total, the full dataset consists of 950 labeled scenarios, which were split into training and testing subsets using an 80:20 ratio to evaluate the model's ability to generalize to previously unseen conditions. This structured simulation-based data generation approach ensures diversity in system operating states and attack patterns. It facilitates the model's exposure to

a wide range of normal and attack behaviors, which is essential for robust and accurate cyber-attack detection in modern grid-connected wind power systems.

4.5 Signal Structure and Time Resolution of the Dataset

In this study, each simulation scenario generates a structured set of output signals, which are saved in MATLAB as a struct with consistent field names across all cases. The recorded outputs represent time-series measurements of critical system variables and include both one-dimensional and multi-dimensional signals.

4.5.1 Simulation Configuration and Time Step Estimation

The Simulink model is configured to run for a total simulation time of 3 seconds, with the solver set to ode45, which is a variable-step solver. To ensure high-resolution output, the maximum allowable step size (MaxStep) is specified as 1×10^{-5} seconds. Under the assumption of a fixed-step solver, each signal would yield exactly 300,000 time samples over 3 seconds. However, since ode45 is a variable-step solver, the actual number of recorded samples is typically lower—generally ranging from tens of thousands to a few hundred thousand—depending on signal dynamics, transients, and model complexity. The adaptive solver adjusts its step size to ensure accuracy, especially during events such as faults or attacks.

4.5.2 Recorded Signals and Dimensions

Table 4.1 summarizes the expected signals recorded for each scenario, along with their corresponding dimensional formats. Here, N denotes the number of time steps collected in a given simulation.

The voltage and current signals are recorded in three phases and stored as $[N \times 3]$ matrices, while all scalar outputs are stored as $[N \times 1]$ arrays synchronized by the common time vector. The label field is a binary scalar that designates whether the scenario corresponds to a normal operation or an attack condition i.e., FDIA. This standardized struct format ensures that all scenarios yield temporally aligned multivariate time-series data for downstream processing. During preprocessing,

Table 4.1: Logged Output Signals and Their Dimensions

Field Name	Description	Dimension
Ppcc	Active power at the PCC	$[N \times 1]$
Qpcc	Reactive power at the PCC	$[N \times 1]$
Vpcc	Voltage at the PCC (3-phase)	$[N \times 3]$
Ipcc	Current at the PCC (3-phase)	$[N \times 3]$
Wpcc	Frequency (angular velocity) at the PCC	$[N \times 1]$
y	Output voltage of the SSDC	$[N \times 1]$
Time	Time vector corresponding to all recorded signals	$[N \times 1]$
Label	Class label for the scenario (Normal = 0, Attack = 1)	Scalar

a sliding window technique may be applied to segment these long time-series signals into smaller fixed-length frames (e.g., 100 points) suitable for input into CNN models.

4.6 Designing the CNN-Based Detection Model

In this section, a customized CNN model is developed for attack detection in wind farms. The model architecture is constructed by systematically selecting activation functions, optimization strategies, and key hyperparameters that govern training dynamics and generalization performance. These hyperparameters include the number of convolutional filters, kernel sizes, dropout rate, learning rate, batch size, and the number of training epochs.

To identify the optimal configuration, Bayesian optimization is employed as an efficient hyperparameter search strategy. This method enables a guided exploration of the hyperparameter space, maximizing model accuracy while reducing overfitting and training time.

The CNN architecture is specifically designed to extract spatial and temporal patterns directly from raw multivariate time-series data. Its convolutional layers are capable of detecting localized variations and transient anomalies that are indicative of cyberattacks, such as FDIAs. By leveraging its hierarchical feature learning capability, the model captures both low-level signal fluctuations and higher-level abstract representations of system behavior.

The network's structure is optimized to balance expressiveness and computational efficiency, ensuring that the model remains suitable for real-time implementation. Dropout layers are included

to enhance robustness against overfitting, and the ReLU activation function is used throughout the network to introduce non-linearity while preserving computational simplicity. The final classification is performed using a SoftMax output layer, providing probabilistic predictions of whether the system is in a normal or attack state.

This optimized CNN framework ensures accurate, scalable, and real-time detection of cyber-physical anomalies in complex energy systems.

4.6.1 Structure of a CNN Network

In a typical CNN-based modeling pipeline for multivariate time-series analysis, the input data is represented as a two-dimensional matrix of dimensions $T \times n_F$, where T denotes the number of time steps and n_F represents the number of input features or channels. This structure allows the representation of multivariate signals such as voltage, current, or power measurements from multiple system nodes. Each row of the input matrix corresponds to a time instant, while each column captures a distinct physical variable.

The CNN processing begins with the application of convolutional filters over the temporal dimension. Each filter acts as a learnable kernel that slides across the input, capturing local temporal features within short windows of time. These features include transient changes, trends, periodic behaviors, or abrupt anomalies. Mathematically, a one-dimensional convolution operation for a signal x with kernel w and bias b is defined by (11):

$$y_t = (x * w)_t + b = \sum_{i=0}^{k-1} w_i x_{t+i} + b \tag{11}$$

where k is the kernel size and y_t is the output at time t.

Multiple filters are used in each convolutional layer to extract different types of localized patterns. This is followed by a non-linear activation function such as the Rectified Linear Unit (ReLU), given by (12):

$$\text{ReLU}(z) = \max(0, z) \tag{12}$$

which introduces non-linearity into the model and enhances its capacity to learn complex mappings.

To reduce the dimensionality of the output and focus on the most salient features, pooling operations such as max-pooling or average pooling are applied. For instance, max-pooling with window size p and stride s is given by (13):

$$y_j = \max_{i=0}^{p-1}(x_{js+i}) \tag{13}$$

These layers downsample the feature maps, maintaining translation invariance and improving computational efficiency. This pooling operation not only simplifies the computation but also mitigates overfitting by enforcing a degree of abstraction.

The sequence of convolutional and pooling layers can be repeated multiple times to create a deep feature hierarchy, where early layers detect simple patterns (e.g., peaks or slopes), and deeper layers capture complex temporal dependencies and higher-level abstractions across channels.

Once the feature extraction phase is complete, the output tensor is flattened into a one-dimensional vector, which is then passed to one or more fully connected (dense) layers. These layers perform high-level reasoning and decision-making based on the extracted features. A dense layer with weights $W \in \mathbb{R}^{m \times n}$, bias $b \in \mathbb{R}^m$, and flattened input vector $z \in \mathbb{R}^n$ produces output (14):

$$y = Wz + b \tag{14}$$

Dropout regularization is often applied to prevent overfitting. Given a dropout rate r, the dropout mask is sampled independently for each neuron. The output after dropout becomes (15):

$$y_i^{\text{drop}} = m_i \cdot y_i \tag{15}$$

This technique helps prevent co-adaptation of neurons and improves generalization.

The final output layer typically uses a SoftMax activation function to provide a probability distribution across the possible output classes. In binary classification tasks (e.g., normal vs. attack), the output layer contains two neurons, each representing the probability of a given class. The SoftMax function is defined as (16):

$$\text{SoftMax}(z_i) = \frac{e^{z_i}}{\sum_{j=1}^{C} e^{z_j}}, \quad \forall i \in \{1, \ldots, C\} \tag{16}$$

where C is the number of classes. This function ensures that outputs are non-negative and sum to one, making them interpretable as probabilities.

Training of the CNN is performed by minimizing a loss function using gradient-based optimization. For classification, the categorical cross-entropy loss is typically used which is defined by (17):

$$\mathcal{L} = -\sum_{i=1}^{C} y_i \log(\hat{y}_i) \tag{17}$$

where y_i is the ground truth label and $\hat{y}_i$ is the predicted probability for class i. The backpropagation algorithm is used to compute gradients, and weights are updated via the Adam optimizer, an adaptive learning rate optimization algorithm by (18):

$$\theta_{t+1} = \theta_t - \eta \cdot \frac{\hat{m}_t}{\sqrt{\hat{v}_t} + \epsilon} \tag{18}$$

where $\hat{m}_t$ and $\hat{v}_t$ are bias-corrected first and second moment estimates of the gradient.

CNNs are particularly effective in modeling spatially or temporally correlated data. They are widely used not only in image and speech recognition, but also in signal-based anomaly detection tasks due to their ability to learn spatial-temporal features directly from raw data. This advantage eliminates the need for manual feature extraction and enables the model to generalize across various operating conditions.

The general CNN structure also supports efficient parallelization and scalability. Due to the localized nature of convolutional operations, CNNs are computationally efficient and benefit from GPU acceleration, which is critical for real-time implementation in practical monitoring systems. Furthermore, CNNs naturally handle multichannel signals and learn patterns jointly across different variables, making them suitable for detecting cyber-physical threats in critical infrastructure environments.

In the proposed system, we adopt a customized CNN architecture tailored to detect FDIAs in a PMSG-based power grid. The input signals include P_{PCC}, Q_{PCC}, V_{PCC}, I_{PCC}, and y, all sampled from the MATLAB/Simulink simulation platform. These inputs are concatenated into a multi-channel time-series input with dimensions $T \times n_F$, where $T = 300{,}000$ for a 3-second window, and $n_F = 9$ when including three-phase signals.

The customized CNN architecture consists of two convolutional layers (with filter sizes $[5 \times 1 \times 32]$ and $[3 \times 1 \times 64]$), each followed by max-pooling and dropout layers to suppress overfitting. A flattening layer transforms the extracted features into a one-dimensional array, which is then passed to a fully connected layer with ReLU activation. The final classification is performed using a SoftMax output layer, distinguishing between normal and attack classes.

4.6.2 Hyperparameter Tuning

The performance of deep learning models such as CNNs depends heavily on the appropriate tuning of hyperparameters, which govern the model's learning behavior, capacity, and generalization. Hyperparameters are set prior to training and include architectural choices and training configurations that significantly impact the network's ability to detect attacks with high accuracy and low latency. To optimize the CNN architecture for our detection task, Bayesian optimization was employed due to its efficiency in exploring complex hyperparameter spaces.

Bayesian optimization uses a surrogate probabilistic model to approximate the objective function (e.g., validation loss or accuracy) and guides the search process through an acquisition function. This function balances exploration (trying less certain configurations) and exploitation (refining promising ones), leading to a more efficient discovery of optimal hyperparameters. This approach is especially useful for high-dimensional search spaces such as those arising in CNN design.

For the CNN model, the key hyperparameters tuned via Bayesian optimization include the number of convolutional filters in each layer, filter (kernel) sizes, dropout rates, learning rate, batch size, number of epochs, and the choice of optimizer. The number of filters controls the network's ability to extract rich hierarchical features. Kernel size determines the receptive field of each convolutional neuron, affecting how local patterns are detected across the time series. Dropout was optimized to enhance generalization and prevent overfitting, while learning rate and batch size were adjusted to ensure stable and efficient convergence. The number of training epochs was tuned to balance learning capacity with training time and to avoid both underfitting and overfitting.

The categorical cross-entropy loss function was employed to evaluate the discrepancy between the predicted and actual labels in this binary classification task (Normal vs. Attack). The loss is defined by (19):

$$\mathcal{L} = -\frac{1}{N}\sum_{i=1}^{N}\sum_{c=1}^{2} y_{i,c}\log(\hat{y}_{i,c}) \tag{19}$$

where N is the number of training samples, $y_{i,c}$ is the binary indicator (0 or 1) if class c is the correct classification for sample i, and $\hat{y}_{i,c}$ is the predicted probability for class c. This function penalizes incorrect classifications and encourages the model to assign high probability to the true class.

Through Bayesian optimization, the Adam optimizer was selected as the most effective optimizer for training. Adam dynamically adjusts the learning rate during training using estimates of the first and second moments of the gradients, allowing for faster convergence and improved stability. This is particularly beneficial in handling the non-linear and high-dimensional nature of signals in wind-power integrated power systems. By integrating Bayesian hyperparameter optimization, categorical cross-entropy loss, and the Adam optimizer, the proposed CNN model achieves high detection accuracy, fast convergence, and robustness to noise and signal variability. These characteristics are essential for secure and real-time monitoring in cyber-physical systems such as wind farm-integrated power grids.

Chapter 5

Simulation Results and Analysis

All simulations were performed in MATLAB R2023b using a detailed Simulink model representing normal and attack scenarios in a wind power-integrated system. During each simulation run, key system signals were recorded in a timeseries format via "To Workspace" blocks. These signals were then extracted using custom MATLAB M-files and structured into labeled datasets for CNN training. The CNN model was developed by modifying standard layers from MATLAB's Deep Learning Toolbox, allowing seamless integration between the simulation and learning pipeline. All simulations were executed on a workstation with an Intel(R) Xeon(R) E-2144G CPU @ 3.60 GHz and 32 GB RAM.

5.1 Dataset Generation and Scenario Composition

The simulations were conducted by varying WT operating conditions and applying FDIAs to emulate realistic system behavior under both normal and compromised states. For each scenario, six critical system output signals were recorded at PCC: active power (P_{PCC}), reactive power (Q_{PCC}), three-phase voltage (V_{PCC}), three-phase current (I_{PCC}), voltage frequency (ω_{PCC}), and the damping controller output (y). These signals were exported in a timeseries format.

The normal scenarios were constructed by modifying wind speed and the number of in-service WTs. A set of scaling (P_{in}) coefficients ranging from 0.93 to 1.2 was applied to emulate varying wind conditions and partial turbine availability, resulting in 270 unique normal scenarios under

different operating conditions.

Attack scenarios were created by injecting false data into the voltage measurement signal using a linear transformation. A combination of 21 values of α and 10 values of β was used, producing 210 FDIA cases.

To further expand attack variability, by altering grid impedance Z_g, changing R_g by 20% to 40% and L_g by 5% to 25%, 250 more FDIA scenarios were developed, yielding a total of 470 scenarios, including 220 Normal and 250 Attacks.

Altogether, the dataset comprises 950 labeled scenarios, including 490 normal and 460 attack instances. These were split into training and testing sets using an 80%–20% ratio to evaluate the model's generalization ability. This simulation-based data generation framework provides a comprehensive representation of both operational diversity and cyberattack conditions in wind-integrated power systems, supporting the development of robust FDIA detection models.

5.2 Hyperparameter tuning

To enhance the classification performance of the CNN model, a hyperparameter tuning process was performed. The finalized architecture employed two fully connected layers with 64 and 32 neurons, each followed by batch normalization, ReLU activation, and a dropout rate of 0.5 to mitigate overfitting. Training was conducted over 100 epochs using the Adam optimizer, with a learning rate of 0.00005 and a mini-batch size of 32. A 5-fold stratified cross-validation was applied to ensure reliable performance evaluation across different data subsets. Additionally, data augmentation using Gaussian noise and class balancing through oversampling were implemented to improve generalization.

5.3 Benchmark Classifiers for Comparative Analysis

This section presents the reasons for choosing the other classifiers for benchmarking with the proposed CNN model. Each classifier brings unique strengths that make it applicable in this context:

- RF:

RF is a powerful ensemble learning method that combines the predictions of multiple decision trees, using techniques like bootstrap aggregation and random feature selection, making it particularly effective for classification tasks in intrusion detection systems due to its ability to handle high-dimensional data, imbalanced datasets, and categorical features efficiently [57]. As highlighted in [58], RF can handle large feature spaces effectively by constructing multiple DTs and aggregating their outputs. This makes it ideal for analyzing telemetry data from wind farm systems, where numerous parameters such as voltage, current, and wind speed contribute to system behavior. Its ability to manage nonlinearity and decision boundary complexities makes it an effective baseline for distinguishing cyberattacks in the wind farm-based power system.

- kNN:

  kNN method, highlighted in [59], is known for its simplicity and classifies data points based on the majority of their nearest neighbors, making it ideal for easily interpretable applications. kNN has the flexibility of predicting multiclass target variables. While it lacks an explicit mechanism for modeling temporal dependencies, its strength lies in identifying localized patterns, which can serve as a complementary baseline for detecting cyberattacks in such systems.

- XGBoost:

  XGBoost is a highly efficient and scalable implementation of gradient boosting decision trees, designed to improve classification accuracy by introducing a regularization term into its objective function, which helps prevent overfitting and simplifies the final model structure [60]. Unlike traditional boosting algorithms that rely solely on first-order derivatives, XGBoost leverages second-order derivatives to enhance the precision of model fitting [61]. Additionally, it supports advanced features like missing value handling, sparsity-aware training, and column sampling to reduce variance and computational cost [62]. These characteristics make XGBoost particularly suitable for tasks involving high-dimensional data with nonlinear and imbalanced patterns [63].

5.3.1 Hyperparameter Optimization for Benchmark Classifiers

To ensure a fair and rigorous comparison, the hyperparameters of all the above-mentioned classifiers were fine-tuned using Bayesian optimization. This approach efficiently explores the search space to identify the optimal configuration for each model, enhancing their performance on the given dataset. The specific hyperparameters tuned for each classifier are as follows:

- **RF:**
  - Number of estimators (trees): 50
  - Maximum number of splits per tree: 10
  - Base learner: Decision tree
  - Ensemble method: Bagging

  The RF classifier is trained using the Bag ensemble method with 50 decision trees. Each tree is constrained to a maximum of 10 splits to limit its depth and enhance generalization. The base learners are decision trees configured via a template, ensuring consistent structure across the forest.

- **kNN:**
  - Number of neighbors (k): 5
  - Weighting scheme: Uniform
  - Distance metric: Euclidean

  The kNN classifier is trained with $k = 5$ neighbors, using a *uniform* weighting scheme and the *Euclidean* distance metric to compute the distances between feature vectors. Feature selection involved normalization, removal of low-variance and highly correlated features, and optional noise addition.

- **XGBoost:**
  - Number of learning cycles (trees): 20
  - Learning rate: 0.05

- Base learner: Decision tree
- Maximum number of splits per tree: 3
- Minimum leaf size: 20
- Cross-validation: 10-fold (enabled)

The XGBoost-inspired ensemble classifier is trained using the LogitBoost method with 20 shallow decision trees to avoid overfitting. Each weak learner is limited to 3 splits and a minimum of 20 samples per leaf to enhance generalization. A low learning rate of 0.05 ensures gradual model convergence and 10-fold cross-validation is applied to validate performance and reduce variance.

5.4 Performance of customized CNN model

A comparative analysis with other well-established classifiers highlights the advantages of the proposed CNN model for the wind farm security monitoring system. The model is also evaluated using a previously designed unseen dataset.

This section presents an evaluation of the customized CNN model's performance in identifying cyberattacks, aimed at ensuring the security of the wind-farm-integrated power grid. The model's effectiveness is measured using several performance metrics, and a comparative analysis is conducted against other well-established classifiers to underline the strengths of the proposed CNN architecture within the context of wind farm security monitoring.

In addition to standard performance testing, the model is validated using an unseen dataset previously designed to test generalization capabilities. Figure 5.1 illustrates the training and testing accuracy and loss curves over the course of 50 epochs. These plots highlight the model's strong performance, showing high accuracy and consistently low loss for both training and testing phases. The minimal gap between training and testing accuracy indicates that the model is not suffering from overfitting and is capable of generalizing effectively to new, unseen data. Notably, during the final 10 epochs (from epoch 40 to 50), both accuracy curves maintain a stable and elevated level without notable variations, demonstrating the robustness and stability of the model's performance.

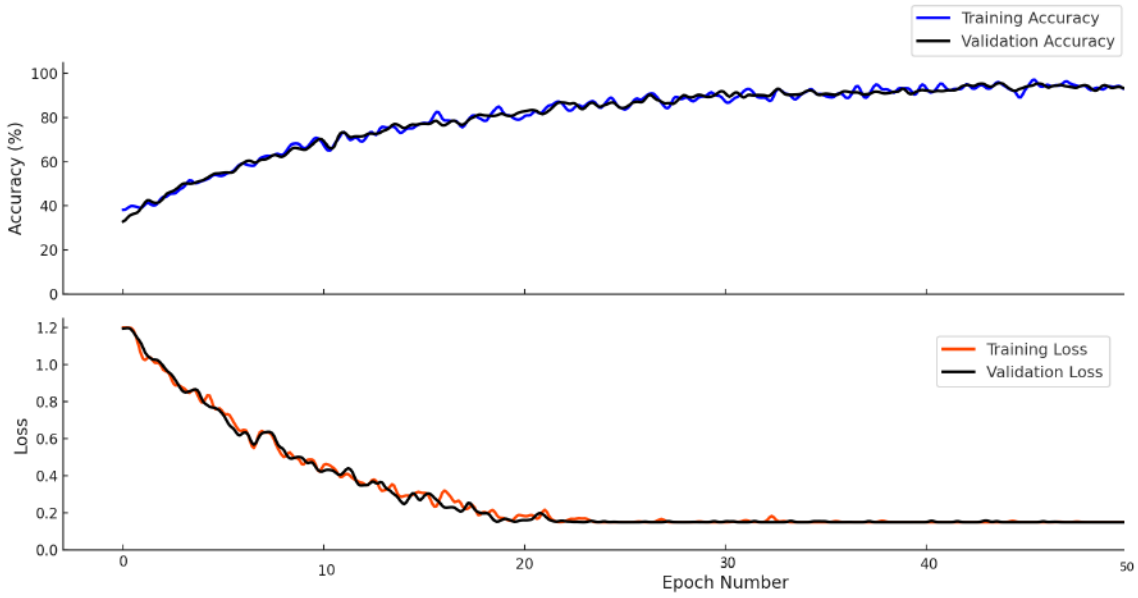

Figure 5.1: Accuracy and loss function for training and testing dataset plot.

Furthermore, the proposed CNN model is benchmarked against other prominent classifiers, RF [64, 58, 57], kNN [59], and XGBoost [60], to provide a comprehensive understanding of its relative advantages.

The proposed CNN model's classification performance is assessed based on multiple evaluation metrics, such as balanced accuracy (BACC), precision, recall, F1 score, and the confusion matrix. For this multiclass classification task, these metrics are computed according to the definitions provided in [65].

- Balanced accuracy is particularly effective in scenarios with class imbalance, as observed in our simulation dataset. It ensures that the evaluation gives equal importance to both normal and cyberattack classes. This metric is crucial for assessing the model's ability to accurately detect attacks without being biased toward the majority class. In the context of our binary classification task, it provides a fair and comprehensive assessment of the CNN's performance by (20):

$$\mathrm{BACC} = \frac{1}{2}\left(\frac{\mathrm{TP_{FDI}}}{\mathrm{TP_{FDI}} + \mathrm{FN_{FDI}}} + \frac{\mathrm{TP_n}}{\mathrm{TP_n} + \mathrm{FN_n}}\right) \tag{20}$$

Here, TP_{FDI} and TP_n represent the number of correctly classified FDI and normal instances, respectively. FN_{FDI} denotes FDI samples misclassified as normal, and FN_n indicates normal samples misclassified as FDI. The balanced accuracy metric reflects the average recall of each class, mitigating the influence of any class imbalance.

- Precision and Recall are particularly useful for assessing model performance where the dataset is imbalanced. Precision quantifies the proportion of TPs among all positive predictions made by the model, while recall quantifies the proportion of TPs instances that the model correctly identified. High precision means the model has few FPs, making it accurate in its predictions. High recall indicates the model effectively captures the most relevant instances, minimizing FNs.The Precision and Recall are given by (21) and (22):

$$\text{Precision} = \frac{\sum_{j=1}^{2} \text{TP}_j}{\sum_{j=1}^{2} \text{TP}_j + \text{FP}_{\text{n, FDI}} + \text{FP}_{\text{FDI, n}}} \tag{21}$$

$$\text{Recall} = \frac{\sum_{j=1}^{2} \text{TP}_j}{\sum_{j=1}^{2} \text{TP}_j + \text{FN}_{\text{FDI, n}} + \text{FN}_{\text{n, FDI}}} \tag{22}$$

where $j = 1, 2$, corresponds to the classes FDI, and normal.

- F1 Score combines the precision and recall scores by calculating their harmonic mean, providing a single metric that balances both precision and recall. It is given by (23)::

$$\text{F1 Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{23}$$

The confusion matrices for our proposed CNN model and other well-known classifiers are illustrated in Fig. 5.2. They provide a detailed breakdown of classification results for each model, illustrating their ability to distinguish between normal, FDI attacks.

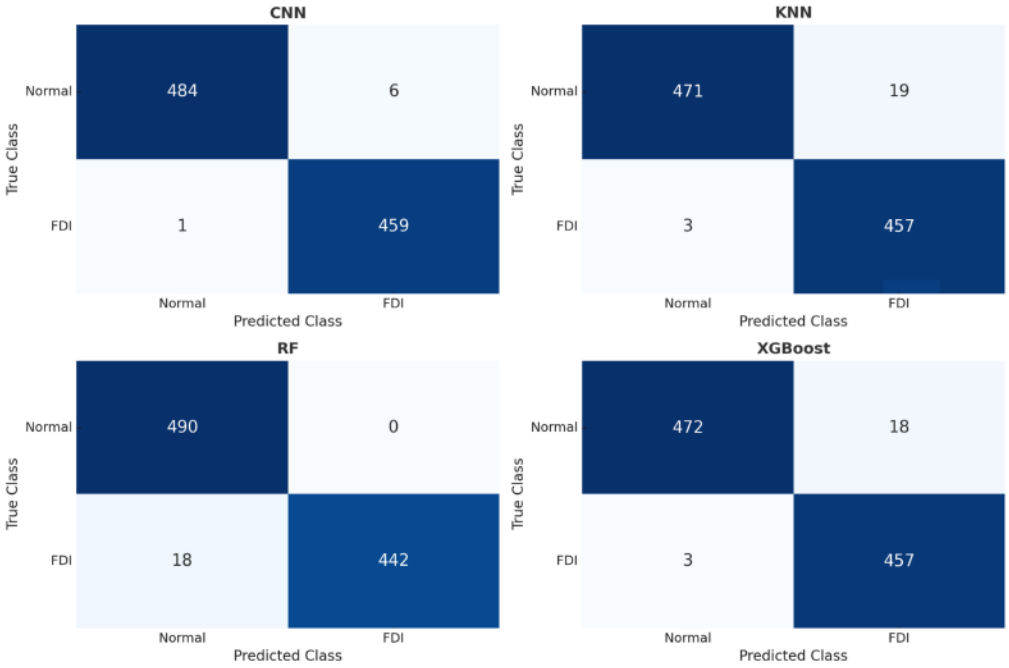

Figure 5.2: Confusion matrices for different classification methods.

5.5 Performance Evaluation of Classification Models

The proposed CNN model demonstrates outstanding performance in all evaluated metrics. As shown in Figure 5.2, the CNN achieves a test accuracy of 98.68%, with only 1 false negative and 6 false positives. This results in a balanced accuracy of 99.28%, the highest among all evaluated models. The CNN's ability to maintain a low misclassification rate across both classes reflects its strong generalization capability. Furthermore, its high recall score of 99.87% indicates excellent sensitivity in identifying cyberattacks, which is critical for ensuring the reliability and security of the wind farm-integrated power grid.

In comparison, the RF model also performs well, achieving the highest precision (99.90%) and a perfect classification of normal instances (no false positives). However, it misclassifies 18 FDI cases as normal, leading to a lower recall than CNN and a balanced accuracy of 98.07%. This suggests that while RF is highly reliable in confirming normal behavior, it may underperform slightly in detecting all attack instances.

The XGBoost model achieves a test accuracy of 96.08% and a balanced accuracy of 97.77%.

Despite correctly classifying most FDI cases, it registers 18 false positives and 3 false negatives, indicating some difficulty in clearly separating the class boundaries, especially in more ambiguous samples.

Similarly, the kNN classifier shows the lowest performance among the four, with a balanced accuracy of 97.76%, a test accuracy of 96.00%, and the highest number of false positives for the normal class (19 instances misclassified as FDI). Although it maintains a good F1 score of 97.96%, this model shows greater sensitivity to noise and overlapping data points in the feature space, which affects its robustness in real-world scenarios.

Overall, Figure 5.2 and Table 5.1 summarize the comparative performance of all four models. The proposed CNN model consistently outperforms the others across all critical evaluation metrics. Table 5.1 highlights the CNN's superior generalization and robustness to class imbalance, as evidenced by its highest recall (99.87%), strong F1 score (99.34%), and top balanced accuracy (99.28%).

Table 5.1: Classification performance comparison of different models

Model	**Test Accuracy**	**Precision**	**Recall**	**F1 Score**	**Balanced Accuracy**
CNN	98.68%	98.68%	99.87%	99.34%	99.28%
RF	97.87%	99.90%	96.15%	98.04%	98.07%
XGBoost	96.08%	96.08%	99.55%	98.00%	97.77%
KNN	96.00%	96.00%	99.55%	97.96%	97.76%

Chapter 6

Conclusion

The increasing penetration of PMSG-based Wind Farms into weak grid environments presents a dual challenge of ensuring dynamic stability and safeguarding control systems against cyber threats. This study tackles these concerns by developing a CNN-based detection framework for identifying FDIAs targeting the performance of the SSDC within cyber-physical wind energy systems. A detailed model of an aggregated PMSG-based wind farm connected to a weak grid is first constructed, where small-signal instability phenomena caused by SSOs are observed. SSDCs are employed to mitigate these instabilities, but their reliance on communication channels exposes the system to data manipulation risks.

To detect such threats, a CNN model is trained on time-series data derived from simulation scenarios representing both normal operation and various cyberattack cases, including signal injection and impedance manipulation. Feature engineering techniques are applied to extract meaningful patterns from the voltage, current, and power signals. The trained CNN model demonstrates superior performance in binary classification of attack and normal scenarios when compared to traditional ML classifiers, including XGBoost, KNN, and RF. The CNN achieved a test accuracy of 98.92%, with high precision and recall, validating its ability to learn temporal and spatial patterns critical for FDIA detection.

This performance gain is largely attributed to the CNN's capability to extract hierarchical features without manual intervention, which is essential for complex, high-dimensional system dynamics. The model operates efficiently with low latency, making it suitable for near real-time monitoring

in grid-connected wind farms. Future work will extend this framework to accommodate evolving multi-vector cyber threats and adaptive countermeasures. Additionally, by leveraging a benchmark scenario susceptible to SSI and FDIAs, future studies can explore localized attack detection strategies and reinforce cyber-resilience in renewable energy systems.

Bibliography

[1] International Renewable Energy Agency (IRENA). "World Adds Record New Renewable Energy Capacity in 2020", 2021. URL https://www.irena.org/publications/2021/Apr/World-Adds-Record-New-Renewable-Energy-Capacity-in-2020. Abu Dhabi, UAE, Apr. 2021.

[2] International Renewable Energy Agency (IRENA). "Renewable Energy Capacity Statistics 2025". https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2025/Mar/IRENA_DAT_RE_Capacity_Statistics_2025.pdf, 2025. [Online; accessed May 16, 2025].

[3] H. Du, J. Yan, M. Ghafouri, R. Zgheib, M. Kassouf, and M. Debbabi. "Modeling of Cyber Attacks Against Converter-Driven Stability of PMSG-Based Wind Farms with Intentional Subsynchronous Resonance". In *Proc. of the IEEE Int. Conf. on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pages 391–396, Aachen, Germany, 2021.

[4] Mohammad Kamruzzaman Khan Prince, Mohammad Taufiqul Arif, Ameen Gargoom, Muhammad Waseem Altaf, Ifte Khairul Amin, Aman Maung Than Oo, Kashem M Muttaqi, and Md Enamul Haque. "Coordinated Control of Grid-Connected PMSG Based Wind Energy System With STATCOM and Supercapacitor Energy Storage". *IEEE Transactions on Industry Applications*, 60(3):5108–5118, 2024. doi: 10.1109/TIA.2024.3371407.

[5] Jiabing Hu, Qi Hu, Bo Wang, Haiyan Tang, and Yongning Chi. "Small Signal Instability

of PLL-Synchronized Type-4 Wind Turbines Connected to High-Impedance AC Grid During LVRT". *IEEE Transactions on Energy Conversion*, 31(4):1676–1687, 2016. doi: 10.1109/TEC.2016.2577606.

[6] H. Liu, Y. Liu, Q. Yang, J. Wen, and J. M. Guerrero. "Subsynchronous Interaction Between Direct-Drive PMSG-Based Wind Farms and Weak AC Networks". *IEEE Transactions on Power Systems*, 32(6):4708–4720, 2017. doi: 10.1109/TPWRS.2017.2678562.

[7] Y. Zhang, Y. Xiang, and L. Wang. "Power System Reliability Assessment Incorporating Cyber Attacks Against Wind Farm Energy Management Systems". *IEEE Transactions on Smart Grid*, 8(5):2343–2357, 2017. doi: 10.1109/TSG.2016.2523922.

[8] Rajiv K. Varma, Soubhik Auddy, and Ysni Semsedini. "Mitigation of Subsynchronous Resonance in a Series-Compensated Wind Farm Using FACTS Controllers". *IEEE Transactions on Power Delivery*, 23(3):1645–1654, 2008. doi: 10.1109/TPWRD.2008.917699.

[9] G. D. Irwin. "Sub-synchronous Interactions with Wind Turbines". In *Proc. Tech. Conf. - CREZ System Design and Operation*, pages 1–6, Taylor, Texas, USA, January 2010. [Online]. Available: http://www.ercot.com/calendar/2010/01/20100126-TECH.

[10] L. C. Gross. "Sub-synchronous Grid Conditions: New event, New Problem, and New Solutions". In *Proc. Western Protective Relay Conference*, pages 1–5, October 2010.

[11] H. Zhang, Y. Liu, Z. Miao, and L. Fan. "Real-World Subsynchronous Oscillation Events in Power Grids With High Penetrations of Inverter-Based Resources". *IEEE Transactions on Power Systems*, 38(5):4170–4184, 2023. doi: 10.1109/TPWRS.2023.3265892.

[12] J. Zhu, Y. Li, S. Yang, L. Fan, and F. Blaabjerg. "Virtual Series Impedance Damping Control for SSR Suppression of MMC-HVDC Interconnected With PMSG-Based Wind Farm". *IEEE Transactions on Power Delivery*, 40(1):530–541, 2025. doi: 10.1109/TPWRD.2024.3285671.

[13] National Grid ESO. "Technical Report on the GB 9 August 2019 Power Outage Event", 2019. URL https://www.nationalgrideso.com/document/153346/download. Accessed online.

[14] Mohsen Ghafouri, Ulas Karaagac, Houshang Karimi, Simon Jensen, Jean Mahseredjian, and Sherif O. Faried. "An LQR Controller for Damping of Subsynchronous Interaction in DFIG-Based Wind Farms". *IEEE Transactions on Power Systems*, 32(6):4934–4942, 2017. doi: 10.1109/TPWRS.2017.2669260.

[15] Mohsen Ghafouri, Ulas Karaagac, Houshang Karimi, and Jean Mahseredjian. "Robust Subsynchronous Interaction Damping Controller for DFIG-based Wind Farms". *Journal of Modern Power Systems and Clean Energy*, 7(6):1663–1674, 2019. doi: 10.1007/s40565-019-0545-2.

[16] Hooman Ghaffarzdeh and Ali Mehrizi-Sani. "Mitigation of Subsynchronous Resonance Induced by a Type III Wind System". *IEEE Transactions on Sustainable Energy*, 11(3):1717–1727, 2020. doi: 10.1109/TSTE.2019.2938014.

[17] Jan Shair, Xiaorong Xie, Yunhong Li, and Vladimir Terzija. "Hardware-in-the-Loop and Field Validation of a Rotor-Side Subsynchronous Damping Controller for a Series Compensated DFIG System". *IEEE Transactions on Power Delivery*, 36(2):698–709, 2021. doi: 10.1109/TPWRD.2020.2989475.

[18] Bingbing Shao, Shuqiang Zhao, Yongheng Yang, Benfeng Gao, Liyuan Wang, and Frede Blaabjerg. "Nonlinear Subsynchronous Oscillation Damping Controller for Direct-Drive Wind Farms With VSC-HVDC Systems". *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 10(3):2842–2858, 2022. doi: 10.1109/JESTPE.2020.3025081.

[19] Yanhui Xu and Shimeng Zhao. "Mitigation of Subsynchronous Resonance in Series-Compensated DFIG Wind Farm Using Active Disturbance Rejection Control". *IEEE Access*, 7:68812–68822, 2019. doi: 10.1109/ACCESS.2019.2919561.

[20] Xi Wu, Shanshan Xu, Xingyu Shi, Mohammad Shahidehpour, Mengting Wang, and Zhiyi Li. "Mitigating Subsynchronous Oscillation Using Model-Free Adaptive Control of DFIGs". *IEEE Transactions on Sustainable Energy*, 14(1):242–253, 2023. doi: 10.1109/TSTE.2022.3209305.

[21] Penghan Li, Jie Wang, Linyun Xiong, Sunhua Huang, Meiling Ma, and Ziqiang Wang. "Energy-Shaping Controller for DFIG-Based Wind Farm to Mitigate Subsynchronous Control Interaction". *IEEE Transactions on Power Systems*, 36(4):2975–2991, 2021. doi: 10.1109/TPWRS.2020.3048141.

[22] Andres E. Leon and Juan Manuel Mauricio. "Mitigation of Subsynchronous Control Interactions Using Multi-Terminal DC Systems". *IEEE Transactions on Sustainable Energy*, 12(1): 420–429, 2021. doi: 10.1109/TSTE.2020.3001907.

[23] M. A. Chowdhury and G. M. Shafiullah. "SSR Mitigation of Series-Compensated DFIG Wind Farms by a Nonlinear Damping Controller Using Partial Feedback Linearization". *IEEE Transactions on Power Systems*, 33(3):2528–2538, 2018. doi: 10.1109/TPWRS.2017.2752805.

[24] Po-Hsu Huang, Mohamed Shawky El Moursi, Weidong Xiao, and James L Kirtley. "Subsynchronous Resonance Mitigation for Series-Compensated DFIG-Based Wind Farm by Using Two-Degree-of-Freedom Control Strategy". *IEEE Transactions on Power Systems*, 30(3): 1442–1454, 2015. doi: 10.1109/TPWRS.2014.2348175.

[25] Ulas Karaagac, Sherif O. Faried, Jean Mahseredjian, and Abdel-Aty Edris. "Coordinated Control of Wind Energy Conversion Systems for Mitigating Subsynchronous Interaction in DFIG-Based Wind Farms". *IEEE Transactions on Smart Grid*, 5(5):2440–2449, 2014. doi: 10.1109/TSG.2014.2330453.

[26] Andres E. Leon and Jorge A. Solsona. "Sub-Synchronous Interaction Damping Control for DFIG Wind Turbines". *IEEE Transactions on Power Systems*, 30(1):419–428, 2015. doi: 10.1109/TPWRS.2014.2327197.

[27] Wenjia Si, Jingyang Fang, Xingyou Chen, Tao Xu, and Stefan M. Goetz. "Transient Angle and Voltage Stability of Grid-Forming Converters with Typical Reactive Power Control Schemes". *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pages 1–1, 2024. doi: 10.1109/JESTPE.2024.3477492.

[28] Jianqiao Ye, Shenghu Li, Peiru Feng, and Xuli Wang. "Passive Control Strategy to Mitigate Sub-synchronous Control Interaction of DFIG-Based Integrated Power Systems". In *2023 International Conference on Power System Technology (PowerCon)*, pages 1–6, 2023. doi: 10.1109/PowerCon58120.2023.10331555.

[29] Akshaya Moharana, Rajiv K. Varma, and Ravi Seethapathy. "SSR Alleviation by STATCOM in Induction-Generator-Based Wind Farm Connected to Series Compensated Line". *IEEE Transactions on Sustainable Energy*, 5(3):947–957, 2014. doi: 10.1109/TSTE.2014.2311072.

[30] Amir Amini, Mohsen Ghafouri, Arash Mohammadi, Ming Hou, Amir Asif, and Konstantinos Plataniotis. "Secure Sampled-Data Observer-Based Control for Wind Turbine Oscillation Under Cyber Attacks". *IEEE Transactions on Smart Grid*, 13(4):3188–3202, 2022. doi: 10.1109/TSG.2022.3159582.

[31] Robert Czechowski, Paweł Wicher, and Bernard Wiecha. "Cyber security in communication of SCADA systems using IEC 61850". pages 1–7, 2015. doi: 10.1109/MEPS.2015.7477223.

[32] Nima Abdi, Abdullatif Albaseer, and Mohamed Abdallah. "The Role of Deep Learning in Advancing Proactive Cybersecurity Measures for Smart Grid Networks: A Survey". *IEEE Internet of Things Journal*, 11(9):16398–16421, 2024. doi: 10.1109/JIOT.2024.3354045.

[33] Anuj Sanghvi, Brian Naughton, Colleen Glenn, Jake Gentle, Jay Johnson, Jeremiah Stoddard, Jonathan White, Nicholas Hilbert, Sarah Freeman, Shane Hansen, and Shawn Sheng. "Roadmap for Wind Cybersecurity". 7 2020. doi: 10.2172/1647705.

[34] Michael Mccarty, Jay Johnson, Bryan Richardson, Craig Rieger, Rafer Cooley, Jake Gentle, Bradley Rothwell, Tyler Phillips, Beverly Novak, Megan Culler, and Brian Wright. "Cybersecurity Resilience Demonstration for Wind Energy Sites in Co-Simulation Environment". *IEEE Access*, 11:15297–15313, 2023. doi: 10.1109/ACCESS.2023.3244778.

[35] Lawrence Abrams. "Wind Turbine Firm Nordex Hit by Conti Ransomware Attack". Online: https://www.bleepingcomputer.com/ news/security/wind-turbine-firm-nordex-hit-by-conti-ransomware-attack/, 2022.

[36] Megan Egan. “A Retrospective on 2022 Cyber Incidents in the Wind Energy Sector and Building Future Cyber Resilience”. *Boise State University*, 2022.

[37] Yichi Zhang, Yingmeng Xiang, and Lingfeng Wang. “Power System Reliability Assessment Incorporating Cyber Attacks Against Wind Farm Energy Management Systems”. *IEEE Transactions on Smart Grid*, 8(5):2343–2357, 2017. doi: 10.1109/TSG.2016.2523515.

[38] Asal Zabetian-Hosseini, Ali Mehrizi-Sani, and Chen-Ching Liu. “Cyberattack to Cyber-Physical Model of Wind Farm SCADA”. In *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, pages 4929–4934, 2018. doi: 10.1109/IECON.2018.8591200.

[39] Jie Yan, Chen-Ching Liu, and Manimaran Govindarasu. “Cyber intrusion of wind farm SCADA system and its impact analysis”. In *2011 IEEE/PES Power Systems Conference and Exposition*, pages 1–6, 2011. doi: 10.1109/PSCE.2011.5772593.

[40] M. Ansari, M. Ghafouri, and A. Ameli. “Cyber-Security Vulnerabilities of the Active Power Control Scheme in Large-Scale Wind-Integrated Power Systems”. In *2022 IEEE Electrical Power and Energy Conference (EPEC)*, pages 79–84, 2022. doi: 10.1109/EPEC56903.2022.10000140.

[41] Mohsen Ghafouri, Ulas Karaagac, Ilhan Kocar, Zhao Xu, and Evangelos Farantatos. “Analysis and Mitigation of the Communication Delay Impacts on Wind Farm Central SSI Damping Controller”. *IEEE Access*, 9:105641–105650, 2021. doi: 10.1109/ACCESS.2021.3096331.

[42] Mohsen Ghafouri, Ulas Karaagac, Amir Ameli, Jun Yan, and Chadi Assi. “A Cyber Attack Mitigation Scheme for Series Compensated DFIG-Based Wind Parks”. *IEEE Transactions on Smart Grid*, 12(6):5221–5232, 2021. doi: 10.1109/TSG.2021.3091535.

[43] H. Du, J. Yan, M. Ghafouri, R. Zgheib, and M. Debbabi. “Modeling and Assessment of Cyber Attacks Targeting Converter-Driven Stability of Power Grids With PMSG-Based Wind Farms”. *IEEE Transactions on Power Systems*, 39(5):6716–6728, 2024. doi: 10.1109/TPWRS.2024.3365416.

[44] Markos Markou and Sameer Singh. "Novelty Detection: A Review—Part 2:: Neural Network Based Approaches". *Signal Processing*, 83(12):2499–2521, 2003. ISSN 0165-1684. doi: https://doi.org/10.1016/j.sigpro.2003.07.019.

[45] Fangyu Li, Rui Xie, Bowen Yang, Lulu Guo, Ping Ma, Jianjun Shi, Jin Ye, and Wenzhan Song. "Detection and Identification of Cyber and Physical Attacks on Distribution Power Grids With PVs: An Online High-Dimensional Data-Driven Approach". *IEEE Journal of Emerging and Selected Topics in Power Electronics*, PP:1, 01 2020. doi: 10.1109/JESTPE.2019.2943449.

[46] Subal Beura and Bibhu Prasad Padhy. "A Transformer Neural Network-Based Cyberattack Detection Technique in Hybrid Power System". In *2023 IEEE 3rd International Conference on Sustainable Energy and Future Electric Transportation (SEFET)*, pages 1–6, 2023. doi: 10.1109/SeFeT57834.2023.10245890.

[47] J. Wang, L. Wang, and Y. Zhang. "Enhanced KNN-Based Anomaly Detection for Cyber-Physical Systems". *IEEE Access*, 8:123456–123465, 2020. doi: 10.1109/ACCESS.2020.2999999.

[48] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze. "Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors*, 21(18):6225, 2021. doi: 10.3390/s21186225.

[49] S. Sharma and P. Kumar. "Random Forest-Based Intrusion Detection in Power Grids". *IEEE Transactions on Industrial Informatics*, 17(3):2001–2012, 2021. doi: 10.1109/TII.2021.3056789.

[50] X. Pan, X. Lu, Y. Liu, and L. Wu. "Graph Neural Network-Based Approach for Detecting False Data Injection Attacks on Voltage Stability". *IEEE Transactions on Smart Grid*, 14(5):3695–3707, 2023. doi: 10.1109/TSG.2022.3232724.

[51] M. R. Haider, B. A. Shaw, B. Khan, T. R. Ayodele, S. A. Malik, and M. A. Mahmud. "IEEE 1815.1-Based Power System Security With Bidirectional RNN-Based Network Anomalous Attack Detection for Cyber-Physical Systems". *IEEE Transactions on Industry Applications*, 59(2):1835–1847, 2023. doi: 10.1109/TIA.2022.3226984.

[52] Tao Xue, Ulas Karaagac, Haoyan Xue, and Jean Mahseredjian. "Re-examination of small-signal instability in weak grid-connected voltage source converters". *Electric Power Systems Research*, 189:106700, 2020. doi: 10.1016/j.epsr.2020.106700.

[53] L. Fan. "Modeling Type-4 Wind in Weak Grids". *IEEE Transactions on Sustainable Energy*, 10(2):853–864, 2019. doi: 10.1109/TSTE.2018.2888978.

[54] M. H. P. Swari, I. P. S. Handika, I. K. S. Satwika, and H. E. Wahani. "Optimization of Single Exponential Smoothing using Particle Swarm Optimization and Modified Particle Swarm Optimization in Sales Forecast". In *2022 IEEE 8th Information Technology International Seminar (ITIS)*, pages 292–296, Surabaya, Indonesia, 2022. doi: 10.1109/ITIS57155.2022.10010034.

[55] A. Kondabathini D. Ishchenko J. Hong, R. F. Nuqui and A. Martin. "Cyberattack resilient distance protection and circuit breaker control for digital substations". *IEEE Trans. Ind. Informat.*, 15(7):4332–4341, 2019.

[56] A. Ameli J. Yan M. Ghafouri, U. Karaagac and C. Assi. "A cyberattack mitigation scheme for series compensated DFIG-based wind parks". *IEEE Trans. Smart Grid*, 12(6):5221–5232, 2021.

[57] Paulo Angelo and André Drummond. "A Survey of Random Forest Based Methods for Intrusion Detection Systems". *ACM Computing Surveys*, 51, 05 2018. doi: 10.1145/3178582.

[58] Shijin Liu, Hiroaki Fukuda, and Paul Leger. "An RF-based Low Rate DDoS Attack Real-time Detection System". In *2023 33rd International Telecommunication Networks and Applications Conference*, pages 304–309, 2023. doi: 10.1109/ITNAC59571.2023.10368543.

[59] Frank Acito. "Predictive Analytics with KNIME: Analytics for Citizen Data Scientists". *Springer Nature Switzerland*, 2023.

[60] A. B. Parsa, A. Movahedi, H. Taghipour, S. Derrible, and A. Mohammadian. "Toward safer highways: Application of XGBoost and SHAP for real-time accident detection and feature analysis". *Accident Analysis & Prevention*, 136:105405, 2020. doi: 10.1016/j.aap.2019.105405.

[61] A. Samat, E. Li, W. Wang, S. Liu, C. Lin, and J. Abuduwaili. "Meta-XGBoost for hyperspectral image classification using extended MSER-guided morphological profiles". *Remote Sensing*, 12(12):1973, 2020. doi: 10.3390/rs12121973.

[62] H. Li, Y. Li, and F. Porikli. "DeepTrack: Learning discriminative feature representations online for robust visual tracking". *IEEE Transactions on Image Processing*, 25(4):1834–1848, 2015.

[63] K. Zhou, J. Zhang, Y. Ren, Z. Huang, and L. Zhao. "A gradient boosting decision tree algorithm combining synthetic minority oversampling technique for lithology identification". *Geophysics*, 85(4):WA147–WA158, 2020. doi: 10.1190/GEO2019-0429.1.

[64] Grzegorz Dudek. "A Comprehensive Study of Random Forest for Short-Term Load Forecasting". *Energies*, 15(20):7547–7547, 2022. doi: 10.3390/en15207547.

[65] Andre M. Carrington, Douglas G. Manuel, Paul W. Fieguth, Tim Ramsay, Venet Osmani, Bernhard Wernly, Carol Bennett, Steven Hawken, Olivia Magwood, Yusuf Sheikh, Matthew McInnes, and Andreas Holzinger. "Deep ROC Analysis and AUC as Balanced Average Accuracy, for Improved Classifier Selection, Audit and Explanation". *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 45(1):329–341, 2023. ISSN 1939-3539. doi: 10.1109/tpami.2022.3145392.