Data-driven Security Monitoring System for Cyberattacks on SSDCs in DFIG-Based Wind Parks

Zeinab Oladi

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 (Quality Systems Engineering) at

Concordia University

Montréal, Québec, Canada

January 2025

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Zeinab Oladi**

Entitled: **Data-driven Security Monitoring System for Cyberattacks on SSDCs in DFIG-Based Wind Parks**

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

Master of Applied Science (Quality Systems Engineering)

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. Farnoosh Naderkhani

______________________________ Examiner
Dr. Suryadipta Majumdar

______________________________ 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 System for Cyberattacks on SSDCs in DFIG-Based Wind Parks

Zeinab Oladi

The massive integration of wind parks (WPs) in the modern power grid resulted in a significant concern regarding the security of the entire grid. These concerns are more important in the presence of WPs with inherent stability issues, e.g., when doubly-fed induction generators (DFIGs) are connected to series-compensated transmission systems. This thesis presents a novel real-time, data-driven security monitoring system to detect false data injection (FDI) and denial of service (DoS) cyberattacks targeting the subsynchronous damping controller (SSDC) in DFIG-based WPs.

A detailed and realistic electromagnetic transient (EMT) model of a DFIG-based WP is developed, along with the design of an SSDC to mitigate the subsynchronous control interaction (SSCI) phenomenon. The cyber vulnerabilities within the WP system, based on IEC 61400 standards, are analyzed to identify potential attack vectors in its cyber layer. It is demonstrated that such attacks can render the performance of SSDC ineffective, resulting in instability and sustained oscillations. To counter these issues, a real-time security monitoring system leveraging a customized recurrent neural network (RNN)-long short-term memory (LSTM) networks model is proposed to identify FDI and DoS attacks against the SSDC. The performance of the developed RNN-LSTM model is benchmarked against well-known classifiers, including random forest (RF), k-nearest neighbors (KNN), and multilayer perceptron (MLP), demonstrating superior detection accuracy. The effectiveness of the proposed model is further validated using unseen data, ensuring its effectiveness and generalization capability. Additionally, the proposed model exhibits low latency, making it suitable for near real-time operations in WPs.

Acknowledgments

I sincerely thank everyone who has supported and encouraged me throughout my academic journey. First and foremost, I extend my deepest thanks to my supervisor, Dr. Mohsen Ghafouri, for his invaluable guidance, support, and insightful advice, which have shaped the direction of my research. Beyond academics, his positive attitude and open-mindedness have taught me valuable life lessons and been a profound source of inspiration.

I am deeply thankful to my parents for their unconditional love, encouragement, and belief in me, which have been the foundation of my achievements. I am truly grateful to my husband, Omid, for his unwavering support and love, which have been integral to my success and our shared journey.

To my older sister, Najmeh, I owe immense gratitude for being my motivation to embark on this journey. Her constant presence and belief in me have been a source of strength throughout my life. To my younger sister, Maryam, thank you for being my constant motivation during challenging times and for your invaluable artistic support in drawing figures—you are truly a lifesaver in more ways than one.

I sincerely thank my friend, Hossein, for his valuable technical assistance and guidance, which greatly contributed to the progress of my project. I am also deeply grateful to my friend, Afshar, for his support and expertise in machine learning tasks, which greatly contributed to the success of this work.

Contents

List of Figures vii

List of Tables viii

List of Acronyms . . . xii

1 Introduction **1**

1.1 Problem Definition . . . 1

1.2 Objectives . . . 2

1.3 Methodology . . . 3

1.4 Contributions . . . 3

1.5 Thesis Structure . . . 4

2 Literature Review **6**

2.1 Subsynchronous Phenomenon . . . 7

2.2 Mitigation Techniques for SSCI . . . 7

2.3 Cyberattacks on SSDC . . . 8

2.4 Cyberattack Detection Methods . . . 10

2.5 Research Gap . . . 13

3 Cyber-Physical Modeling and Control of DFIG-Based WPs **15**

3.1 Physical Layer . . . 16

3.1.1 Simplified WP Model for SSDC Design . . . 19

3.1.2 Linearization and SSDC implementation . . . 22

3.2 WP Cyber Layer with the Designed SSDC 23

4 Threat Modeling and Data-Driven Security Monitoring Framework 25

4.1 Threat model 25

4.1.1 FDI and DoS attack models 27

4.2 Motivation for using RNN-LSTM architecture 30

4.3 Data generation for training and validation of the model 31

4.4 Designing the RNN-LSTM network detection model 32

4.4.1 Structure of customized RNN-LSTM network 33

4.4.2 Hyperparameter Tuning 35

5 Simulation Results and Analysis 37

5.1 Data Generation for Training and Validation 37

5.2 Hyperparameter tuning 39

5.3 Benchmark Classifiers for Comparative Analysis 39

5.3.1 Hyperparameter Optimization for Benchmark Classifiers 40

5.4 Performance of customized RNN-LSTM model 41

5.4.1 Model Validation on Unseen Data 46

5.4.2 ROC and AUC Analysis 47

5.5 Real-Time Security Monitoring System Implementation 48

6 Conclusion 50

Bibliography 51

List of Figures

Figure 3.1 Physical layer connection of a WP grid-connected system. 16

Figure 3.2 Simplified model of a radially compensated WP in eigenvalue analysis. . . . 19

Figure 3.3 Control architecture of DFIG wind turbine incorporating SSDC. 20

Figure 3.4 Cyber layer connection of a WP grid-connected system. 23

Figure 4.1 Cyberattack on the designed SSDC. 26

Figure 4.2 POI active power, reactive power, and voltage in S1 and S2. 28

Figure 4.3 POI active power, reactive power, and voltage in S2 and S3. 29

Figure 4.4 POI active power, reactive power, and voltage in S2 and S4. 29

Figure 4.5 RNN-LSTM model structure for the security monitoring system under different uncertainties in WP system. 32

Figure 4.6 LSTM cell architecture. 34

Figure 5.1 Accuracy and loss function for training and testing dataset plot. 42

Figure 5.2 Confusion matrices for different classification methods. 44

Figure 5.3 Confusion matrix for RNN-LSTM model on the unseen dataset. 46

Figure 5.4 ROC curves for normal, FDI, and DoS classes. 47

Figure 5.5 Time-domain detection of DoS attack using RNN-LSTM model. 48

List of Tables

Table 3.1 Wind park parameters in the EMTP model. 17

Table 3.2 Internal wind park parameters. 17

Table 3.3 Cables data. 18

Table 4.1 Analysis of the SSDC performance under normal and attack conditions . . . 28

Table 5.1 Comparison of different methods for classification performance 44

List of Acronyms

API Application Programming Interface

DC Direct Current

DFIG Doubly Fed Induction Generator

DL Deep Learning

DoS Denial of Service

DT Decision Tree

EMT Electromagnetic Transient

EMTP Electromagnetic Transients Program

FDI False Data Injection

FN False Negative

FP False Positive

FRT Fault Ride Through

HVDC High Voltage Direct Current

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

LSTM Long Short-Term Memory

ML Machine Learning

MLP Multilayer Perceptron

MITM Man-in-the-Middle

MPPT Maximum Power Point Tracking

PI Proportional-integral

POI Point of Interconnection

RNN Recurrent Neural Network

ReLU Rectified Linear Unit

RF Random Forest

RTU Remote Terminal Unit

SCADA Supervisory Control and Data Acquisition

SSI Subsynchronous Interaction

SSCI Subsynchronous Control Interaction

SSDC Subsynchronous Damping Controller

SVM Support Vector Machine

TCP/IP Transmission Control Protocol/Internet Protocol

TN True Negative

TP True Positive

VSC Voltage Source Converter

WP Wind Park

WPC Wind Park Control

WT Wind Turbine

WTC Wind Turbine Controller

Chapter 1

Introduction

1.1 Problem Definition

Among various renewable energy sources, wind-based units have gained significant attention in recent decades. Wind energy production has emerged as a fundamental component of renewable energy solutions globally, playing a critical role in reducing greenhouse gas emissions and combating climate change. According to the global wind Energy council (GWEC), wind power is essential for achieving international commitments to triple renewable energy capacity by 2030, contributing to energy security, economic growth, and job creation. Canada's wind energy sector exemplifies this potential, leveraging its vast wind resources to transition to a sustainable energy future. Between 2024 and 2028, North America is projected to add approximately 71.5 gigawatts (GW) of onshore wind capacity, with 91% of this expansion occurring in the United States and 9% in Canada [1]. Additionally, statistics from the international energy agency (IEA) predict that global wind capacity will nearly double between 2024 and 2030 compared to 2017-2023 [2].

The increasing integration of renewable energy into modern power grids has made wind-based energy systems, particularly wind parks (WPs), a cornerstone of sustainable energy development. A WP typically comprises wind turbines (WTs), medium voltage (MV) feeders, transformers, and a wind park controller (WPC).

Numerous technologies have been established to effectively capture wind energy. Among the various WT technologies, types 3 and 4 are the most widely utilized due to their ability to maximize wind energy utilization by operating in the maximum power point tracking (MPPT) mode [3], [4]. The doubly-fed induction generator (DFIG) technology (type 3) is particularly favored for its ability to operate under variable wind speeds and its reduced converter size, making it economically efficient [5]. To efficiently deliver the maximum power generated by DFIG-based WPs, series-compensated transmission lines have been adopted. These lines enhance transient stability, increase transmission capacity, enable load-sharing control, and accommodate voltage drops. However, they can impose resonance conditions on the power system, potentially leading to stability issues. Despite the advantages of DFIG-based systems, integrating WPs into power grids poses challenges, particularly subsynchronous control interactions (SSCI).

To mitigate SSCI, techniques such as passive damping, FACTS-based devices, and active damping controllers like subsynchronous damping controllers (SSDCs) have been proposed. SSDCs are widely adopted due to their cost-effectiveness and ability to provide efficient damping. Their integration within the WP supervisory control and data acquisition (SCADA) system— SCADA system, along with the energy management system (EMS), is essential for monitoring, operating, and safeguarding both WP generators and the power system[6]—involves the extensive use of the cyber layer and information and communications technology (ICT) [5]. However, this dependence on cyberinfrastructure introduces significant vulnerabilities to cyberattacks, such as false data injection (FDI) and denial of service (DoS). These threats underscore the critical need for advanced attack detection mechanisms to ensure the resilience and security of WP-integrated grids.

This thesis presents a data-driven security monitoring system designed to detect FDI and DoS cyberattacks targeting SSDCs in DFIG-based WPs, aiming to enhance system resilience.

1.2 Objectives

The main objectives of this thesis are as follows:

- To identify FDI and DoS cyberattacks on SSDC and analyze the impact of these cyberattacks on the WP operation system.

- To demonstrate the performance degradation of SSDC during the FDI and Dos cyberattacks

- To propose a real-time security monitoring system based on a customized recurrent neural network (RNN)-long short-term memory (LSTM) architecture to detect FDI and DoS cyber-attacks on SSDC in DFIG-based WPs.

1.3 Methodology

This thesis employs a data-driven approach to develop a security monitoring system for DFIG-based WPs operating in series-compensated transmission lines. The methodology is structured into the following key steps:

- System modeling: A state-space model is developed to represent the detailed and realistic electromagnetic transient (EMT) model of the DFIG-based WP. This state-space model is used to design an SSDC based on the linear quadratic regulator (LQR) technique to mitigate SSCI.

- Cyber vulnerability analysis: Attack vectors are identified in the WP cyber layer based on the IEC 61400-25 standard. The impacts of FDI and DoS attacks are simulated to demonstrate their disruptive effects on SSDC operation.

- Development of the data-driven security monitoring system: a real-time security monitoring system based on the proposed RNN-LSTM model is developed to detect FDI and DoS attacks. The model is trained on datasets representing various operating conditions, including fluctuating wind speeds, varying in-service WTs, and changing grid impedances.

- Performance evaluation: The RNN-LSTM model is benchmarked against other well-established classifiers. The effectiveness of the proposed system is also validated using an unseen dataset.

1.4 Contributions

The main contributions of this thesis are as follows:

- Developing models for FDI and DoS cyberattacks targeting the SSDC in WPC,

- Proposing an RNN-LSTM-based security monitoring system to identify and classify DoS and FDI cyberattacks targeting the SSDC in WPC, and
- Benchmarking the performance of the developed RNN-LSTM model against other commonly used classifiers, such as random forest (RF), k-nearest neighbors (kNN), and multilayer perceptron (MLP).

1.5 Thesis Structure

The thesis is structured into six chapters, each addressing a specific aspect of the research. The second chapter reviews the related works in the field of existing techniques for mitigating SSCI in DFIG-based WPs. It also examines various detection methods for identifying cyberattacks such as FDI and DoS in WP control systems.

The third chapter develops a cyber-physical model of a DFIG-based WP, focusing on mitigating SSCI through a designed SSDC. It includes detailed modeling of the physical layer, such as the WP configuration, system parameters, and fault scenario, using EMTP-RV simulations. The cyber layer addresses SCADA system architecture, communication protocols, and related cyber vulnerabilities. The SSDC is designed using a linearized model with an LQR controller and observer, integrated into the WT control loops via communication links.

Chapter four presents a threat model highlighting cyberattacks on SSDC communication links, with a particular focus on FDI and DoS attacks. It underscores vulnerabilities in the communication protocols of WP SCADA systems, emphasizing the susceptibility of SSDC signals to cyber threats and the critical need for advanced cybersecurity measures to ensure system security and stability. This chapter proposes an RNN-LSTM-based framework for real-time security monitoring system to detect these cyberattacks. The data generation process includes simulating various operational scenarios and cyberattacks, and capturing time-series features from WP telemetry data for model training and validation. The design of the RNN-LSTM network is detailed, including its architecture, sliding window approach, and hyperparameter tuning using Bayesian optimization to enhance detection accuracy.

The fifth chapter includes a detailed analysis of the performance metrics, latency, and comparison with well-known classifiers such as RF, kNN, and MLP. It presents the results of the simulation studies, validating the performance of the proposed security monitoring system under various normal and cyberattack scenarios by an unseen dataset.

The final chapter, chapter six, concludes the thesis by summarizing the key contributions and findings. It outlines potential directions for future research.

Chapter 2

Literature Review

This chapter reviews the challenges of subsynchronous control interactions (SSCI) and cybersecurity in DFIG-based WPs. It explores SSCI mitigation techniques, emphasizing subsynchronous damping controllers (SSDCs), and examines cyberattack detection methods, categorized into model-based and data-driven approaches. The chapter highlights vulnerabilities in WP-integrated power systems, particularly targeting SSDCs, and identifies key research gaps, setting the stage for developing a robust, data-driven security monitoring framework.

This chapter analyzes the DFIG-based WP challenges and solutions. It begins by exploring the susceptibility of DFIG-based WPs to SSCI when connected to series-compensated transmission lines. Various mitigation strategies for addressing SSCI are critically reviewed. Next, it examines the cybersecurity vulnerabilities in the communication links and supervisory control and data acquisition (SCADA) networks of WPs, highlighting how these systems are exposed to potential cyberattacks, including DoS and FDI attacks. The chapter further compares model-based and data-driven methods for detecting such cyber threats, evaluating their effectiveness and limitations. Finally, it identifies existing research gaps, emphasizing the need for advanced real-time security monitoring systems to ensure the secure and stable operation of wind-integrated power systems.

2.1 Subsynchronous Phenomenon

The subsynchronous interaction (SSI) phenomenon is a frequent stability issue for wind-integrated power systems that can result in substantial power generation losses. The subsynchronous phenomenon can generally be classified into three types:

(1) subsynchronous resonance (SSR) occurs when a series-compensated system oscillates at the natural frequencies of the power system, potentially causing mechanical failures [7], [8].

(2) subsynchronous torsional interaction (SSTI) arises from interactions between the turbine-generator mechanical system and devices like compensated lines and HVDC systems [9], [10].

(3) subsynchronous control interaction (SSCI) a purely electrical interaction between type 3 WTs and series-compensated lines, can result in rapidly growing oscillations due to negative damping from control systems, leading to potential equipment damage [11]. SSCI frequency of oscillations is below the nominal frequency of the power system. SSCI events have caused global instability incidents, such as in the U.S. and China [12, 13, 14]. This interaction, if not mitigated, can result in damaging oscillations that lead to power system stability.

Unstable SSCI between the power system and the current control loops of the WP control system can be triggered by various faults or disturbances [15]. If adequate preventive actions are not implemented, SSCI can cause significant consequences, including equipment damage from transient overvoltages, power generation loss due to generator trips and oscillating voltages, and degraded power quality [16], [17]. Consequently, several SSCI mitigation strategies have been proposed in the literature, aimed at ensuring grid stability and protecting system components. These methods emphasize enhancing control mechanisms, implementing supplementary damping controllers, and exploring advanced power electronic solutions.

2.2 Mitigation Techniques for SSCI

The major techniques used in the literature to mitigate SSCI can be summarized as follows: (i) passive damping components such as resistors, damping circuits, and tunable filters. However, they have limitations such as cost and adaptive tuning complexity [18]. (ii) FACTS and converter-based devices such as static var compensators (SVC) [17], static synchronous compensators (STATCOM) [19], and shunt-voltage sourced converters (SVSC) [20]. These methods also suffer from high installation costs and grid integration complexity; (iii) Subsynchronous damping controllers (SSDCs) which are deployed in DFIG or WP control schemes to provide damping in frequency of oscillations [21]. For instance, linear quadratic regulator (LQR) [22], μ-synthesis [23], multiple-model adaptive control (MMAC) [24], PD controller [25], feedback linearization theory and sliding mode control (SMC) [26], active disturbance rejection control (ADRC) [27], model-free adaptive control (MFAC) [28], Energy-Shaping Controller [29], a generalized harmonic compensation control strategy [30], partial feedback linearization [31], two-degree-of-freedom damping control loops [32], and lead-lag scheme [33] are used among others to mitigate SSCI. Due to the low cost of deployment and effectiveness, these schemes are the preferred solution in the literature and industry.

2.3 Cyberattacks on SSDC

As large-scale WPs grow, cybersecurity for their integrated control systems has become a paramount concern. The deployment of mitigating controllers in a WP heavily relies on the integration of internet of things (IoT) devices within the WP's SCADA system, ICTs, and communication links, making it susceptible to cyberattacks [5]. The main reason for this integration is to transfer the measurements from the DFIGs to the WPC and send the control commands back to the WTs. Moreover, the use of various communication protocols, e.g., IEC 61400-25, IEC 60870-5, DNP 3.0, Modbus, and IEC 61850-7, as well as multi-level control loops make the WP even more dependent on its cyber layer. This reliance, on the other hand, makes the WP prone to cyberattacks, such as FDI and DoS. In [6] cyberattack scenarios concerning cyber components or networks within the integrated WP SCADA/EMS system architecture are investigated, focusing on the vulnerabilities in the communication network of WPs. According to attack targets, the cyberattack against power systems can be classified into destroying the availability, integrity, and confidentiality of information. The availability destruction is embodied in unavailable information resulting from communication interruption, whose typical methods are DoS attacks, black hole attacks, and attacks modifying network topology. The integrity destruction is embodied in incorrect information resulting from FDI, man-in-the-middle (MITM) attack, and replay attack[34]. Among the existing cyberattacks, FDI and DoS attacks have received a high level of attention in the literature due to their ease of implementation and severe consequences on the operation of power systems.

Over the past decade, adversaries have exploited these vulnerabilities, leading to significant WT outages in several incidents. A DoS attack in 2019 targeted the communication between a control center and wind generation sites, in Utah, USA. This attack exploited vendor firewall vulnerabilities, causing unexpected device reboots [35]. Another cyberattack in 2022 disrupted approximately 30,000 satellite communication terminals, affecting modems in 5,800 turbines operated by ENERCON, with a combined capacity of over 10 gigawatts [36]. Moreover, in 2022, the Nordex Group SE was hit by a ransomware attack, prompting the precautionary shutdown of IT systems across various locations and suspending remote communication with the turbines [37]. Additionally, in 2022, Deutsche Windtechnik faced a comparable cyberattack, resulting in the loss of remote connectivity and control for 2,000 WTs throughout Germany [38]. These events emphasize the critical need for effective security monitoring systems and advanced attack detection mechanisms to safeguard WP-integrated grids.

Despite its significance, only a limited number of studies have specifically addressed the security analysis of WPs. These approaches can be divided into model-based and data-driven techniques. Regarding the model-based approaches, in [39], [6] WP cyber and physical layers are discussed and various attack entry points that can result in sending false shutdown commands to the WTs are studied. Moreover, in [40], [41], the FDI attacks against the setpoint of WT controllers are discussed and possible implications of such attacks on WP operation are investigated. The performance of such model-based techniques is dependent on the operating condition of the system and their deployment requires detailed parameters of the system, which may not be fully available. For data-driven approaches, in [42], a time-sequence machine learning (ML)-based methodology was proposed to detect DoS, signal tampering, and stealthy data injection attacks in voltage source converters (VSCs) used in combination with WP. These discussed research works are, however, general and do not focus on attacks targeting SSDCs. In the case of attacks against SSDCs, there are only a few studies in the literature. For instance, reference [43] presents a mitigation scheme for attacks that target an SSDC that stabilizes a series compensated DFIG-based WP. In that study, attacks aiming to create SSCI instability are classified into (i) internal attacks in which internal WP cyber layers are compromised and (ii) external attacks where the cyber layer of the neighbor substation is compromised. Then, a robust static-output-feedback observer and an adaptive mechanism are designed for attack detection and mitigation. A cyber-resilient event-triggered control framework for large-scale WPs is proposed in [5] to mitigate DoS and FDI attacks against SSDC by utilizing an observer-based fuzzy control scheme. Moreover, a model-based mitigation technique based on the Smith predictor is developed in [44] for delay attacks targeting SSDC in DFIG-based WPs. Similar to general attacks on WPs, current countermeasures for threats against SSDCs are limited to identifying cyberattacks at a single operating point of the system and often require precise grid and WP parameters. This information may not always be available for security monitoring schemes. Additionally, existing data-driven methods focus solely on attacks targeting setpoints, neglecting those against measurements. Thus, there is a need to develop detection techniques capable of identifying attacks on SSDC measurements under various operating conditions. To the best of the authors' knowledge, developing such a data-driven security monitoring system remains an open gap in the literature.

2.4 Cyberattack Detection Methods

Despite its significance, only a limited number of studies have specifically addressed the security analysis of WPs. In securing WP-integrated power systems, cyberattack detection methods are generally classified into two main categories: model-based and data-driven techniques. Model-based approaches use detailed mathematical models to identify deviations, making them effective when system parameters are well-defined but less adaptable in dynamic scenarios. In contrast, data-driven methods employ ML-based methods to analyze real-time data, offering flexibility and adaptability to evolving cyberattacks. These methods utilize data from SCADA systems to detect subtle anomalies, making them ideal for complex and variable environments in the presence of WP uncertainties. This section provides an in-depth description of these two categories.

- Model-based methods use mathematical models to detect cyberattacks by relying on a cyber-physical system (CPS) model that captures the normal behavior of the system. This understanding allows these methods to identify deviations that may signal potential cyber threats. For example, in [39], [6] WP cyber and physical layers are discussed and various attack entry points that can result in sending false shutdown commands to the WTs are studied. Moreover, in [40], [41], the FDI attacks against the setpoint of WT controllers are discussed and possible implications of such attacks on WP operation are investigated. The performance of such model-based techniques is dependent on the operating condition of the system and their deployment requires detailed parameters of the system, which may not be fully available. A cyber-resilient event-triggered control framework for large-scale WPs is proposed in [5] to mitigate DoS and FDI attacks against SSDC by utilizing an observer-based fuzzy control scheme. Moreover, a model-based mitigation technique based on the Smith predictor is developed in [44] for delay attacks targeting SSDC in DFIG-based WPs. Similar to general attacks on WPs, current countermeasures for threats against SSDCs are limited to identifying cyberattacks at a single operating point of the system and often require precise grid and WP parameters. This information may not always be available for security monitoring schemes. A study [45] explores a nonlinear virtual inertia control (VIC) method to mitigate the impact of FDI, hijack attack (HjA), and DoS attacks on DFIGs, improving active power and frequency stability. The authors of [46] proposed an adaptive control approach based on a fuzzy reference model to mitigate the effects of FDI attacks on the active power profile in WPs. The detection mechanism incorporates real-time monitoring and a firewall. In the case of attacks against SSDCs, there are only a few studies in the literature. For instance, reference [43] presents a mitigation scheme for attacks that target an SSDC that stabilizes a series compensated DFIG-based WP. In that study, attacks aiming to create SSCI instability are classified into (i) internal attacks in which internal WP cyber layers are compromised and (ii) external attacks where the cyber layer of the neighbor substation is compromised. Then, a robust static-output-feedback observer and an adaptive mechanism are designed for attack detection and mitigation. A cyber-resilient event-triggered control framework for large-scale WPs is proposed in [5] to mitigate DoS and FDI attacks against SSDC by utilizing an observer-based fuzzy control scheme. Moreover, a model-based mitigation technique based on the Smith predictor is developed in [44] for delay attacks targeting SSDC in DFIG-based WPs.

- Data-driven techniques have emerged as a powerful approach to enhancing cybersecurity in modern power systems, effectively addressing various uncertainties. These techniques are widely favored for their ability to efficiently scale to larger systems while maintaining low computational costs. Reference [47] discussed data-driven techniques that are more flexible and can adapt to changes in the system being monitored. They leverage their ability to learn from patterns in large datasets, making them particularly effective in dynamic environments like power grids with increasing WP integration, where conditions and potential threats can vary frequently. Advancements in data processing technology have increased the focus on data-driven methods for detecting cyberattacks in smart grid systems [48]. The review [49] highlights the importance of data-driven techniques in detecting cyberattacks in power systems, especially as WPs become more integrated. It notes that the digitalization and complexity of such integration introduce new cybersecurity challenges, necessitating advanced methods like ML and deep learning (DL) to identify anomalies and secure the power grids. These techniques' ability to adapt to evolving conditions and process real-time data makes them effective in maintaining the stability and security of power systems with renewable energy sources. These methods leverage ML and advanced neural network (NN) architectures to detect and mitigate various cyber threats. For instance, a hybrid power system study [50] highlights the use of a transformer NN-based (TNN-based) classifier for detecting FDI cyberattacks targeting frequency sensors of the hybrid electric system. The method outperforms traditional classifiers like support vector machine (SVM) and KNN based on performance metrics, emphasizing the effectiveness of data-driven approaches for securing WP-integrated power systems. A study on the Sri Lankan power system proposes data-driven detection of cyberattacks, leveraging NN models like convolutional neural networks (CNNs), transformer models, and LSTMs. Synthetic datasets were generated using solar farm models and demand-supply curves, analyzing attacks such as data injection and spoofing. The approach aims to mitigate energy theft and grid destabilization, emphasizing enhanced cybersecurity for renewable energy-integrated systems [51]. Additionally, a study on cyber-physical power systems (CPPS) emphasizes the importance of detecting data integrity attacks (DIAs) for grid security. The impact of DIAs on wide area control (WAC) applications is analyzed, with a focus on data-driven detection methods. RF outperforms SVM and KNN in anomaly detection, highlighting its effectiveness in enhancing CPPS resilience [52]. The authors of [53] proposed a detection approach for FDI attacks in grid-connected WPs. The detection process utilizes a margin setting algorithm (MSA). The experimental results indicated that the proposed MSA outperformed traditional SVM and ANN algorithms in detecting FDI attacks, delivering superior accuracy with minimal error. The authors in [42] proposed a time-sequence ML-based methodology to detect DoS, signal tampering, and stealthy data injection attacks in voltage source converters (VSCs) used in combination with WP. These discussed research works are, however, general and do not focus on attacks targeting SSDCs.

2.5 Research Gap

Despite significant advancements in the literature on detecting cyberattacks and stability issues in WP-integrated power grids, several critical gaps remain, particularly in the context of cyberattacks targeting SSDCs. Similar to general attacks on WPs, current countermeasures for threats against SSDCs are limited to identifying cyberattacks at a single operating point of the system and often require precise grid and WP parameters. Data-driven techniques are widely favored for their ability to efficiently scale to larger systems while maintaining low computational costs. This information may not always be available for security monitoring schemes. Additionally, existing data-driven methods focus solely on attacks targeting setpoints, neglecting those against measurements. Thus, there is a need to develop detection techniques capable of identifying attacks on SSDC measurements under various operating conditions. The application of data-driven security monitoring systems for detecting cyberattacks on SSDCs in WP-integrated power grids has not been studied, representing a significant gap in the existing literature.

This thesis seeks to address these gaps by developing a data-driven, real-time security monitoring framework based on the RNN-LSTM model, explicitly focusing on FDI and DoS cyberattacks targeting SSDCs in DFIG-based WPs.

Chapter 3

Cyber-Physical Modeling and Control of DFIG-Based WPs

This chapter presents a comprehensive cyber-physical model of a DFIG-based WP, emphasizing the role of SSDCs in mitigating SSCI. The chapter begins with a detailed exploration of the physical layer including the configuration and parameters of the WP, transmission lines, and control systems. This benchmark system based on a realistic WP model will be developed using the EMTP-RV simulation software.

A simplified model of the WP is then developed for SSDC design, incorporating linearization and state-space representations to capture the system's dynamic behavior. The SSDC is implemented using an LQR controller and an observer, which enhance SSCI mitigation by adapting to WT outages and improving damping performance.

The cyber layer is subsequently addressed, focusing on the SCADA system architecture. It outlines the hierarchical control level, communication protocols, and vulnerabilities associated with the integration of ICTs and communication links in the WP control system. The chapter underscores the importance of robust cyber-physical modeling for ensuring the secure and stable operation of WP-integrated power grids, particularly in the context of growing cybersecurity threats.

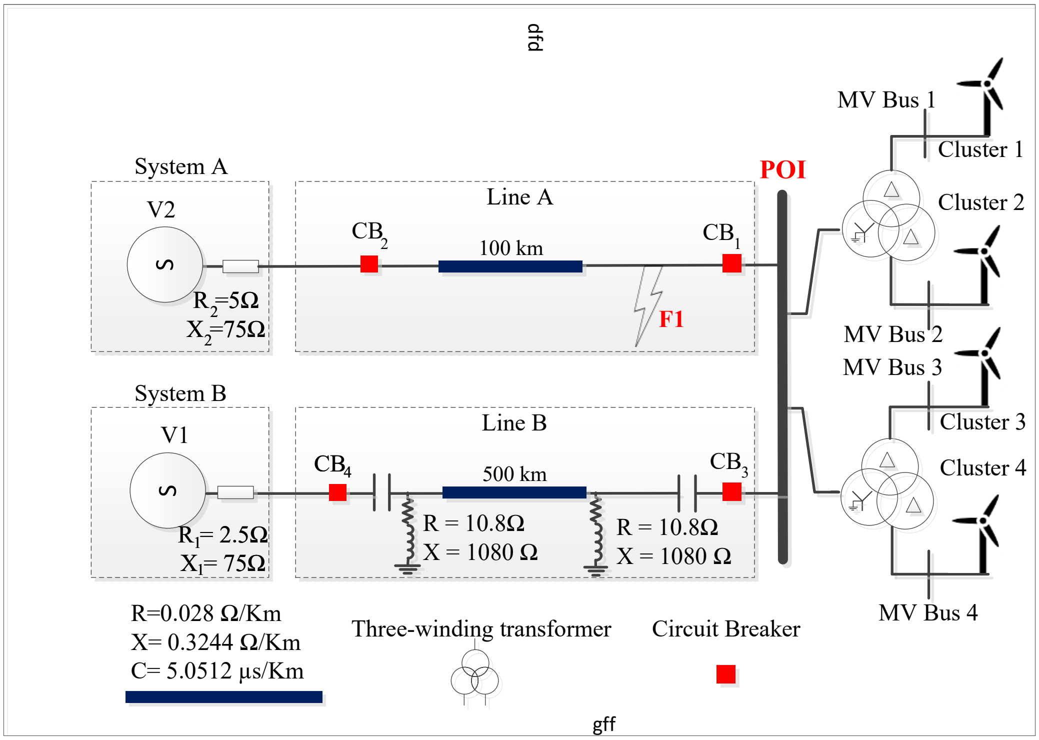


Figure 3.1: Physical layer connection of a WP grid-connected system.

3.1 Physical Layer

The physical layer of the WP-integrated power system under study is depicted in Fig. 3.1. It comprises a WP with a maximum of 268 low-voltage DFIG WTs with 1.5 MW capacity each operating at 575 V and 60 Hz. The WP is subdivided equally into four clusters, with each cluster comprising a maximum of 67 WTs. In this WP, the WTs are connected through step-up transformers to the medium voltage (MV) 34.5 kV collector grid. The WTs of each cluster and their internal transformers are represented using their aggregated model behind an RLC branch. At the point of interconnection (POI), each cluster is connected to the power system through a 500/34.5/34.5 kV delta-delta-grounded star three-winding transformer. The WPC monitors the current and voltage at the POI and regulates the reactive power, voltage, or power factor depending on the operator's selected function. This study examines the WPC operating under the reactive power control function, which independently controls the injected reactive power.

The power system includes two transmission lines, line A and line B, which link the WP to other parts of the power grid, designated as systems A and B. Line A is a 100 km short transmission line,

Table 3.1: Wind park parameters in the EMTP model.

Parameter	value	Description
Mean wind speed	$11.24\frac{m}{s}$	Nominal mean wind speed
WPC mode select	1	1(Q-control) 2(V-control) 3(PF control)
Q_{POI}	0	Reactive power at POI
PF_{POI}	1	Power-factor at POI
f_n	60	Nominal frequency
N_{gen}	268	Number of WTs in the Wind park
N_{gen} in service	268	Number of WTs in service
P_{gen}	1.5 MW	Rated active power of one wind generator
S_{gen}	1.667 MVA	Rated apparent power of one wind generator
$V_{gen_{KVRMSLL}}$	0.575 kV	Generator nominal voltage kV RMS line to line
$V_{collector_{KVRMSLL}}$	34.5 kV	Collector grid nominal voltage kV RMS line to line
$V_{POI_{KVRMSLL}}$	500 kV	Transmission grid voltage kV RMS line to line
$S_{dfig_{trans}}$	1.75 MVA	Rated apparent power of DFIG transformer
$X_{dfig_{trans}}$	0.06 pu	DFIG transformer inductance in pu
$R_{dfig_{trans}}$	0.002 pu	DFIG transformer resistance in pu
$R_{collector}$	0.083Ω	Equivalent collector resistance in Ohms
$L_{collector}$	2.39×10^{-4} H	Equivalent collector inductance in H
$C_{collector}$	2.55×10^{-6} F	Equivalent collector capacitance in F
$S_{WP_{trans}}$	224 MVA	Rated apparent power of wind park transformer
$X_{WP_{trans}}$	0.12 pu	Wind park transformer inductance in pu
$R_{WP_{trans}}$	0.003 pu	Wind park transformer resistance in pu
$Tap_{WP_{trans}}$	1	Wind park transformer tap ratio
$f_{sampling_{RSC}}$	11.25KHz	Sampling rate at RSC
$f_{sampling_{GSC}}$	22.5KHz	Sampling rate at GSC
$f_{PWM_{RSC}}$	2250Hz	PWM frequency at RSC
$f_{PWM_{GSC}}$	4500 Hz	PWM frequency at GSC
$T_{risetime_{RSC}}$	20ms	RSC rise time
$T_{risetime_{GSC}}$	10ms	GSC rise time
K_v	2	Voltage regulation gain
K_p	1	Proportional gain of P control loop
T_{ip}	0.1	Integral gain of P control $Ki = \frac{K_p}{T_{ip}}$

Table 3.2: Internal wind park parameters.

H_t	4 s	K_{tg}	1.2 pu
D_{tg}	1.5 pu	n_{pp}	3
H_{gen}	0.9 s	D_{gen}	0
R_s	0.033 pu	L_{ls}	0.18 pu
R_r	0.026 pu	L_{lr}	0.16 pu
L_m	2.9 pu	K_{tg}	1.2
R_{choke}	0.015 pu	L_{choke}	1.5 pu

Table 3.3: Cables data.

Cable	Resistance ($\frac{\Omega}{Km}$)	Inductance ($\frac{H}{Km}$)	Capacitance ($\frac{F}{Km}$)
3/0 AWG	0.3815	44×10^{-5}	8×10^{-8}
350 kcmil	0.164	38×10^{-5}	10.5×10^{-8}
500 kcmil	0.125	37×10^{-5}	11.5×10^{-8}
750 kcmil	0.0778	35×10^{-5}	14×10^{-8}

while line B spans 500 km and is 50% compensated [22, 54]. This benchmark is commonly used in the study of the SSCI phenomenon [5, 22, 23, 43, 44, 54]. In this system, a three-phase metallic fault (F1) occurs at t=1.2 s and is cleared by circuit breaker CB_1 at t=1.26 s and CB_2 at t=1.28 s, resulting in the disconnection of line A. This disconnection can potentially trigger unstable SSCI between the power grid and the WP, providing an opportunity to evaluate the performance of the SSDC under different scenarios.

The benchmark system developed in Fig. 3.1 will reflect real-world power systems subject to SSCI phenomena. The WP is modeled with four clusters, corresponding to four MV feeders, which aligns with practical WP configurations. This detailed and realistic modeling approach not only enhances the applicability of the WP-based power system but also provides a foundation for localizing attack points in future studies. In future studies, telemetry data from each cluster can be analyzed independently, enabling the identification and isolation of specific clusters affected by FDI and DoS cyberattacks. This capability is essential for the development of WP advanced security monitoring frameworks capable of detecting and mitigating the impact of attacks while maintaining WP stability and security performance. Therefore, this configuration not only enhances the benchmark's realism but also facilitates the exploration of localized cybersecurity measures in future research, which are vital for safeguarding WP-integrated power systems.

The performance of the WP under normal operation and during cyberattack scenarios will be evaluated through detailed EMT simulations. This detailed modeling considers the fault-ride-through (FRT) function, the WPC, and all nonlinear functions required to obtain the precise transient behavior of the system. The input parameters of the EMTP-RV model and the WP parameters are summarized in Tables 3.1 and 3.2, 3.3.

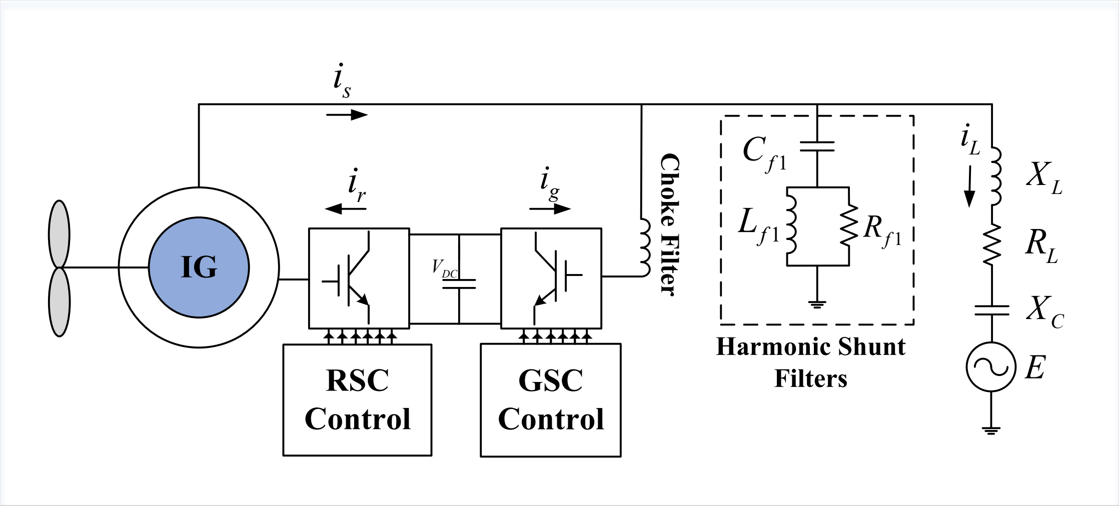


Figure 3.2: Simplified model of a radially compensated WP in eigenvalue analysis.

H_t and H_g represent the inertia constants of the turbine and the induction generator (IG), respectively. Similarly, D_t and D_g are the mechanical damping coefficients of the turbine and the IG, while D_{sh} and K_{sh} denote the damping coefficient and shaft stiffness of the flexible coupling between the turbine and the IG. Additionally, L_s, L_r, and L_m represent the stator, rotor, and mutual inductance matrices, respectively. Detailed information regarding the control system of DFIG WTs can be found in [55].

3.1.1 Simplified WP Model for SSDC Design

A simplified model of a series compensated WP is shown in Fig. 3.2. In this figure, the wound rotor is connected to a back-to-back converter allowing bidirectional power flow, while the stator is directly connected to the grid. This converter comprises two VSCs, namely, the rotor side converter (RSC) and the grid side converter (GSC). By utilizing a DC bus, the back-to-back converter effectively decouples the RSC and the GSC. To protect the RSC from over-currents and the DC capacitor from over-voltages, a crowbar, and a chopper are respectively, placed in the model. When the crowbar is activated, the RSC is blocked, and the WT begins to consume reactive power. Additionally, a DC resistive chopper is used to keep the DC voltage within acceptable limits during faults, preventing unnecessary crowbar operation [56]. The power quality of the GSC is enhanced by one choke filter and two shunt harmonic filters as depicted in Fig. 3.2 [56]. The collector grid, WT transformer, WP transformer, and series compensated transmission line are modeled with a series

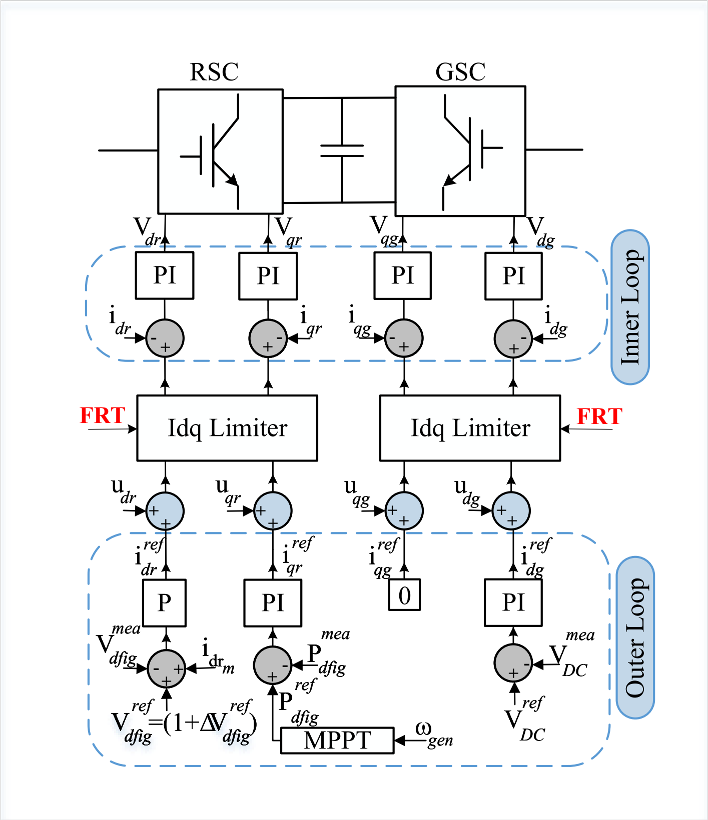


Figure 3.3: Control architecture of DFIG wind turbine incorporating SSDC.

RLC impedance, i.e., R_L, X_L, and X_C. Both the RSC and the GSC are controlled using vector control techniques—in the dq-frame based on either the AC flux or the AC voltage—allowing for the decoupled control of active and reactive powers. Currents and voltages are projected onto a rotating reference dq-frame based on either the AC flux or the AC voltage. The DFIG WT control scheme is illustrated in Fig. 3.3, where i_{dr}, i_{qr} are RSC currents in d- and q-axes, respectively. Moreover, i_{dg} and i_{qg} indicate the d-axis and q-axis currents of the GSC, respectively. The currents used in the current control loops are $I_{Conv} = [i_{dr}, \quad i_{qr}, \quad i_{dg}, \quad i_{qg}]$. The positive-sequence component of the DFIG terminal voltage (V^{mea}_{dfig}) and the active power output of the DFIG (P^{mea}_{dfig}) are controlled using i_{dr} and i_{qr}, respectively. Meanwhile, i_{dg} regulates the DC bus voltage (V^{mea}_{DC}), and i_{qg} provides the necessary reactive power to the grid during faults. Additionally, V^{mea}_{DC} is the DC bus voltage and the superscript 'ref' indicates reference values. Both the RSC and GSC feature two control loops, namely the outer loop and the inner loop. The slow outer loop generates reference signals for the currents $I^{\text{ref}}_{\text{Conv}} = [i^{\text{ref}}_{dr}, \quad i^{\text{ref}}_{qr}, \quad i^{\text{ref}}_{dg}, \quad i^{\text{ref}}_{qg}]$. The fast inner loop control generates the control signals that align with the converter's terminal voltages, which are then used to generate the modulated switching pattern. The reference signals for the DFIG's active power output P_{dfig}^{ref} is determined by the maximum power point tracking (MPPT) algorithm and its reference positive-sequence voltage $(1 + \Delta V_{dfig}^{ref})$ is calculated by the WPC. At the primary level, the WTC monitors and controls its own positive sequence terminal voltage (V_{dfig}^{mea}) with a proportional (P) voltage regulator. The WP reactive power control is based on the secondary voltage control concept. At the secondary level, the WPC modifies the WTC reference voltage values (ΔV_{dfig}^{ref}) via a proportional-integral (PI) reactive power regulator to achieve the desired reactive power flow at POI when operating under reactive power control function [57], [58]. In Fig. 3.3, i_{drm} is the compensating term for the reactive current absorbed by the IG and approximated by

$$i_{drm} = \frac{V_{dfig}^{mea}}{X_m} \tag{1}$$

where X_m is the IG magnetizing reactance. During normal operation, GSC operates at unity power factor $(i_{qg}^{ref} = 0)$ and the RSC controller gives the priority to the active current, i.e.,

$$\begin{aligned} &i_{dr}^{\mathrm{ref}} < I_{dr}^{\mathrm{lim}}, \quad I_{dr}^{\mathrm{lim}} = 1\,\mathrm{pu}, \\ &i_{qr}^{\mathrm{ref}} < I_{qr}^{\mathrm{lim}} = \sqrt{\left(I_r^{\mathrm{lim}}\right)^2 - \left(i_{dr}^{\mathrm{ref}}\right)^2}, \quad I_r^{\mathrm{lim}} = 1.1\,\mathrm{pu} \end{aligned} \tag{2}$$

where I_{dr}^{lim}, I_{qr}^{lim} and I_r^{lim} are the limits for d-axis, q-axis and total RSC currents, respectively [22]. For more details on DFIG-based WP modeling, readers may refer to [22]. Grid code requirements stipulate that WTs must sustain a stable response to sudden voltage changes, requiring the integration of a fault ride-through (FRT) function to adjust the active and reactive current references generated by the WTC's outer loop to comply with grid codes [59]. This paper considers the DFIG WT equipped with an FRT function that adheres to the grid code requirements and when the FRT function is activated, the RSC controller gives the priority to the reactive current by reversing the d- and q-axis current limits given in (2).

The RSC and GSC control systems play a crucial role in managing the DFIG under different operating conditions. However, in the presence of SSCI oscillations, relying solely on these controllers may not be sufficient to guarantee the stability of the system. Therefore, an SSDC should be designed and added to the control scheme of WP to mitigate the SSCI phenomenon.

3.1.2 Linearization and SSDC implementation

This section presents a brief overview of the linearized model for the proposed system, including the implementation of the SSDC in the WP-integrated power grid.

A simplified series compensated DFIG-based WP, as shown in Fig. 3.2, is linearized to design SSDC. The obtained linearized state-space equations can be expressed as:

$$\begin{aligned} \dot{x} &= Ax + Bu \\ y &= Cx + Du \end{aligned} \tag{3}$$

where x, u, and y represent the vectors of the system's states, inputs, and outputs, respectively. The matrices A, B, C, and D determine the small-signal behavior of the system. The state vector x is defined as:

$$\mathbf{x} = \begin{pmatrix} x_{\text{DC}}, & x_{\text{IG}}, & x_{\text{mech}}, & x_{\text{sys}}, & x_{\text{HF}}, & x_{\text{CNTL}}, & x_{\text{IVF}} \end{pmatrix}^T \tag{4}$$

In (4), x_{DC}, x_{IG}, x_{mech}, x_{sys}, x_{HF}, x_{CTNL}, and x_{IVF} represent the states of the DC link, the induction generator, the mechanical system, the power system, the harmonic filters, the control systems, and the voltage/current filters, respectively. The output vector of the system, which is the controller input, consists of the measurements of the converter currents, i.e., $y = [i_{dr}, \quad i_{qr}, \quad i_{dg}, \quad i_{qg}]$ as shown in Fig. 3.3.

The SSDC's output signals, $u = [u_{dr}, \quad u_{qr}, \quad u_{dg}, \quad u_{qg}]$, are transmitted back into the current control loops of the DFIGs as input signals of the WTC through the communication links between WPC and WTC. Finally, an LQR controller and its associated observer are designed using the developed linear model to dampen oscillations.

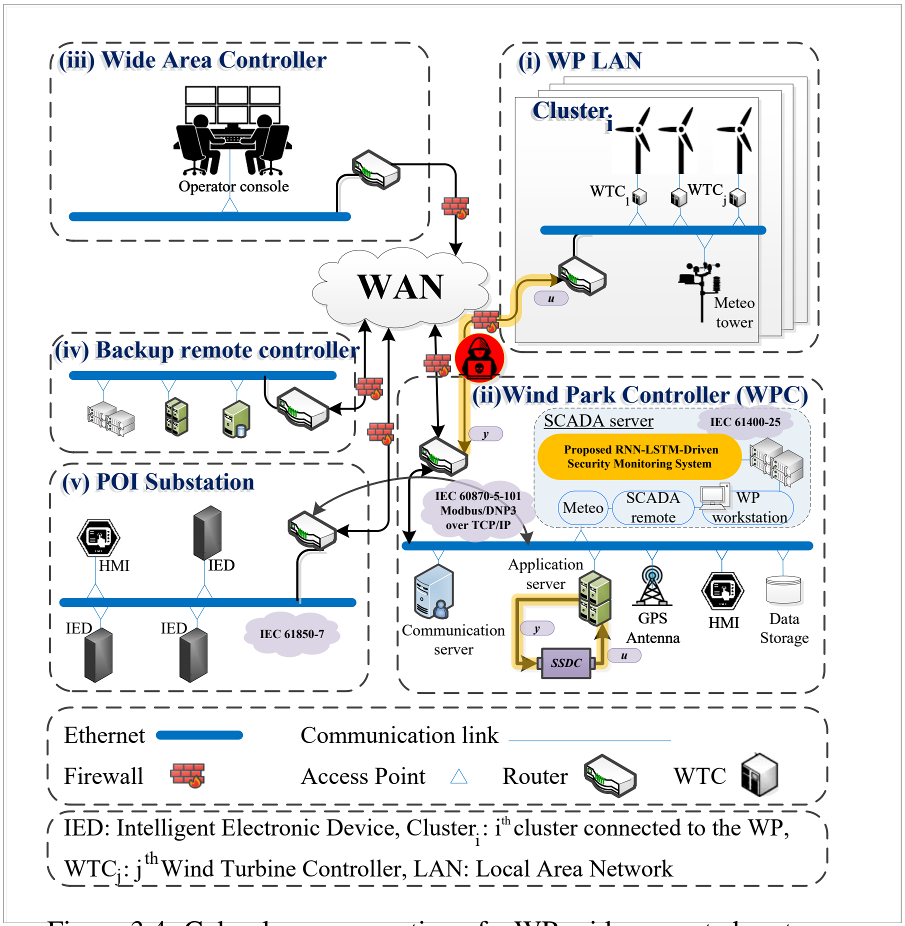

(iii) Wide Area Controller
Operator console
(i) WP LAN
Cluster$_i$
WTC$_1$
WTC$_j$
Meteo tower
u
WAN
(iv) Backup remote controller
(ii)Wind Park Controller (WPC)
y
SCADA server
IEC 61400-25
Proposed RNN-LSTM-Driven Security Monitoring System
Meteo
SCADA remote
WP workstation
IEC 60870-5-101 Modbus/DNP3 over TCP/IP
(v) POI Substation
HMI
IED
IED
IED
IEC 61850-7
Application server
Communication server
y
SSDC
u
GPS Antenna
HMI
Data Storage
Ethernet
Communication link
Firewall
Access Point
Router
WTC
IED: Intelligent Electronic Device, Cluster$_i$: ith cluster connected to the WP,
WTC$_j$: jth Wind Turbine Controller, LAN: Local Area Network

Figure 3.4: Cyber layer connection of a WP grid-connected system.

3.2 WP Cyber Layer with the Designed SSDC

The WP's SCADA system typically consists of monitoring and control mechanisms, along with a communication framework. These mechanisms are generally implemented across three hierarchical levels: (i) the primary level (WT level), (ii) the secondary level (WP level), and (iii) the tertiary level (grid level). Additionally, the communication architecture of the SCADA system, as illustrated in Fig. 3.4, manages the transmission of data and commands and is divided into five distinct subnetworks, as outlined below [5, 6]: (i) The WP LAN, connected to the WPC through ethernet, are set up using WTCs and other field devices, such as the METEO function, which collects meteorological data like wind speed and temperature. The WTC is responsible for managing and monitoring each WT, including its electrical and mechanical components. (ii) The WPC, which functions as a standalone SCADA network, performs monitoring and control tasks for the WTs. The communication protocols used in the WPC networks are based on the international electrotechnical commission (IEC) 61400-25 standard which enables the SCADA system to communicate with any device in a standardized manner. IEC 60870-5-101, DNP 3.0 over the TCP/IP framework, and Modbus are also used for communicating control commands and measurements between control rooms and substations. This integration enables measurement transfers from WTs to the WPC and sends control commands to WTs, relying on protocols such as IEC 61400-25, IEC 60870-5, DNP 3.0, Modbus, and IEC 61850-7. In the WP SCADA system, real-time command and measurement information are displayed on the workstation, while long-term data from measurement components is stored in a historian database. The SCADA system acquires grid data, including electrical variables from WTs and meteorological data like wind speed and temperature via the METEO function. The SCADA server processes this data and transmits it to the application server. The application server stores measurement data in the real-time database and sends control commands to the workstation. The communication server processes information exchanged with the control center and is restricted from directly communicating with the workstation [60]. Meanwhile, the application server stores measurement data in a real-time database and transmits control commands to the workstation. If an attacker gains control over the workstation, the WTs within the compromised WP can receive fabricated trip commands, forcing them to shut down. As shown in Fig. 3.4, the SSDC is implemented in the application server. Thus, the WTCs send the required signals (y) as the input of the SSDC through the routers and receive the control commands (u) from the SSDC to use in the inner control loop of the WTCs. (iii) The wide area controller manages multiple WPs across the grid, ensuring coordinated control and stability. (iv) The backup remote controller can provide redundancy for managing the SCADA system, offering backup capabilities in case the WPC is not functional. (v) POI Substation operates under the IEC 61850-7 standard, handling communications and automation for monitoring and controlling physical substation components. The human-machine interface (HMI) facilitates the operation and supervision of the substation [61]. The intelligent electronic devices (IEDs) in the substation communicate with the control center and can also be polled by local remote terminal units (RTUs). The data collected from the IEDs is then transmitted to the control center [62].

Chapter 4

Threat Modeling and Data-Driven Security Monitoring Framework

This study proposes an RNN-LSTM network for real-time security monitoring to detect the developed cyber threats targeting the SSDC. The proposed network utilizes a sliding window approach to analyze the time-dependent features of WP telemetry data, enabling the differentiation between normal operations, FDI attacks, and DoS attacks. By continuously monitoring data streams, the network provides timely alerts to the security monitoring framework within the WPC upon detecting any cyberattacks.

This section introduces a threat model to highlight potential cyberattacks, focusing on FDI and DoS attacks targeting SSDC control signals. The rationale behind selecting the LSTM architecture is then discussed, followed by an explanation of the dataset development process for training and validation. Finally, the design procedure for the RNN-LSTM network is presented.

4.1 Threat model

This study simulates FDI and DoS cyberattacks on the SSDC communication links, aiming to degrade SSDC performance in WP-integrated power systems. These attacks exploit vulnerabilities in the communication links between the WPC and WTs, specifically targeting the SSDC output/input signals.

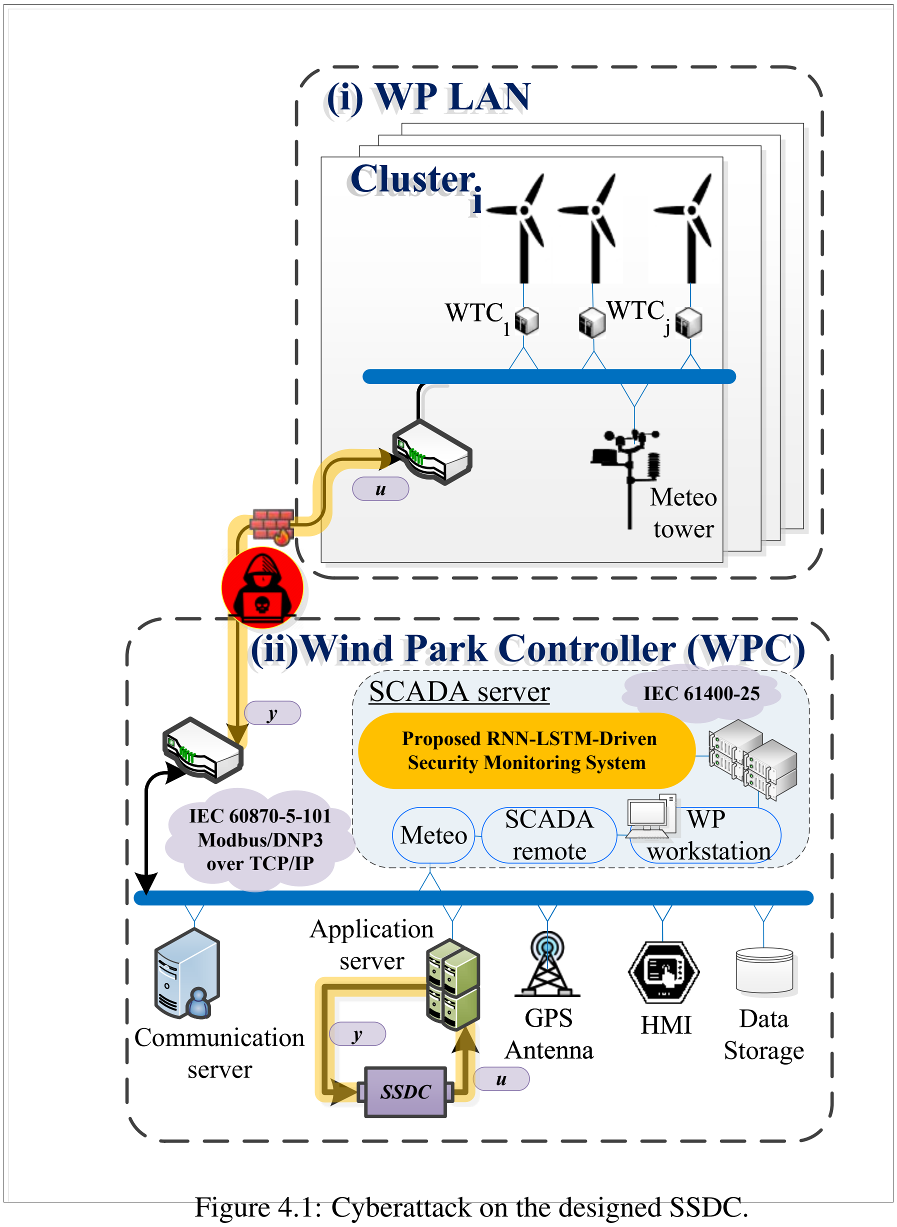


Figure 4.1: Cyberattack on the designed SSDC.

It is important to note that most communication protocols used in the WP SCADA systems, such as IEC 61400-25 [63], are designed for rapid data exchange but lack essential security features, as highlighted by the United States department of energy [35]. This reliance on real-time data exchange makes the communication links between the WTCs and the WPC, as illustrated in Fig. 4.1, particularly vulnerable to cyberattacks, including FDI and DoS attacks. Such vulnerabilities underscore the critical need for robust cybersecurity measures to protect the integrity and availability of the WP control system.

Since SSDC signals are crucial for the stability of the WP, attackers attempt to manipulate these signals to create undamped oscillations. In this threat model, it is assumed that the attackers possess sufficient knowledge of the WP communication network and its cyber infrastructure to modify or interrupt the SSDC control commands. This information could be obtained by the insiders with access to WP data, by external attackers compromising the system's database [6, 64] or by conducting reconnaissance activities [36]. The target of the attack in this study is the communication link between the WPC and WTC, where real-time measurement data and SSDC control commands are managed. Additionally, it is assumed that the attack was launched from outside networks of WP, similar to the Utah attack that occurred in 2019 [35]. In the threat model used in this thesis, as illustrated in Fig. 4.1, data transmitted between routers located in WP LAN and the WPC via internet protocol (IP) or transmission control protocol/internet protocol (TCP/IP) are considered vulnerable to man-in-the-middle (MITM) attacks, which can falsify or block the SSDC output control signals.

4.1.1 FDI and DoS attack models

The FDI attack is mathematically formulated as:

$$u'(t) = \alpha \cdot u(t) \tag{5}$$

where α determines the magnitude of the attack. $u'(t)$ and $u(t)$ are, respectively, the modified and original control signals.

On the other hand, the DoS attack can be modeled as:

$$u'(t) = u(t) \cdot (1 - H(t - t_1) + H(t - t_2)) \tag{6}$$

where $H(t)$ is the step function, t_1 is the start time of the DoS attack, and t_2 is its end time.

To illustrate the impact of the attacks, Table 4.1 presents different scenarios used to evaluate SSDC's performance with and without discussed attack scenarios. In all the scenarios, the wind speed is assumed to be minimum—where the SSCI is more severe—and 268 WTs are in service. Under normal conditions (Scenarios S1 and S2), Fig. 4.2 shows that without SSDC the system is unstable, whereas the designed controller can dampen the oscillations successfully. However, during

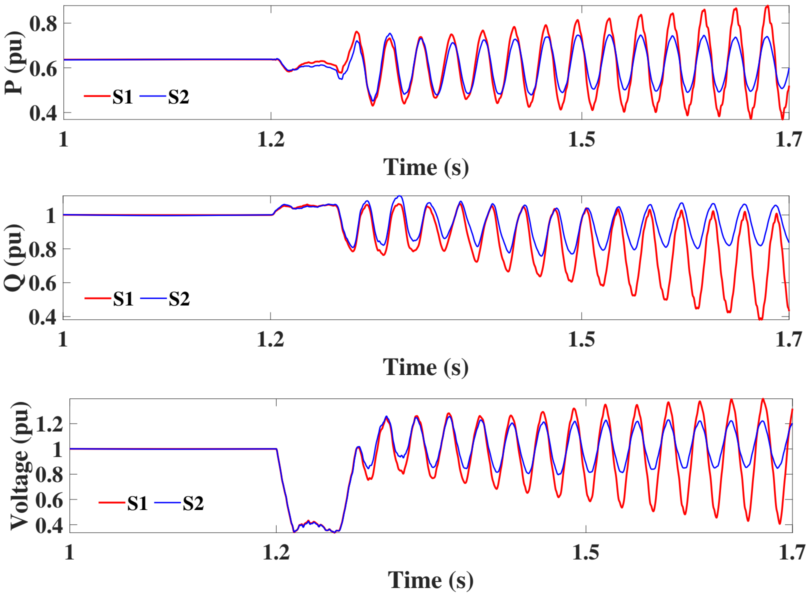


Figure 4.2: POI active power, reactive power, and voltage in S1 and S2.

the simulated FDI or DoS cyberattacks (Scenarios S3 and S4), the SSDC's performance deteriorates significantly, leading to sustained oscillations and system instability, as shown in Fig. 4.3 and Fig. 4.4, respectively. These results underscore that the designed SSDC, which effectively dampens oscillations under normal conditions, cannot stabilize the system in the presence of cyberattacks. Thus, robust cybersecurity measures, including advanced detection systems, are needed to effectively monitor and safeguard WP-integrated power systems. Moreover, Figs. 4.2-4.4 also illustrate the temporal dependencies of the data recorded during both normal and attack scenarios. Features such as park active power, reactive power, and voltage exhibit fluctuations over time, making it essential to capture the time-series nature of the data to identify evolving patterns of instability.

Table 4.1: Analysis of the SSDC performance under normal and attack conditions

Scenario	SSDC	Wind Speed	WT Numbers	System Condition
S1	No SSDC	0.6 pu	268	Normal
S2	With SSDC	0.6 pu	268	Normal
S3	With SSDC	0.6 pu	268	FDI attack
S4	With SSDC	0.6 pu	268	DoS attack

To show the impact of the attacks, Table 4.1 presents different scenarios that are used to evaluate SSDC's performance. In all the scenarios, the wind speed is assumed to be minimum—where the

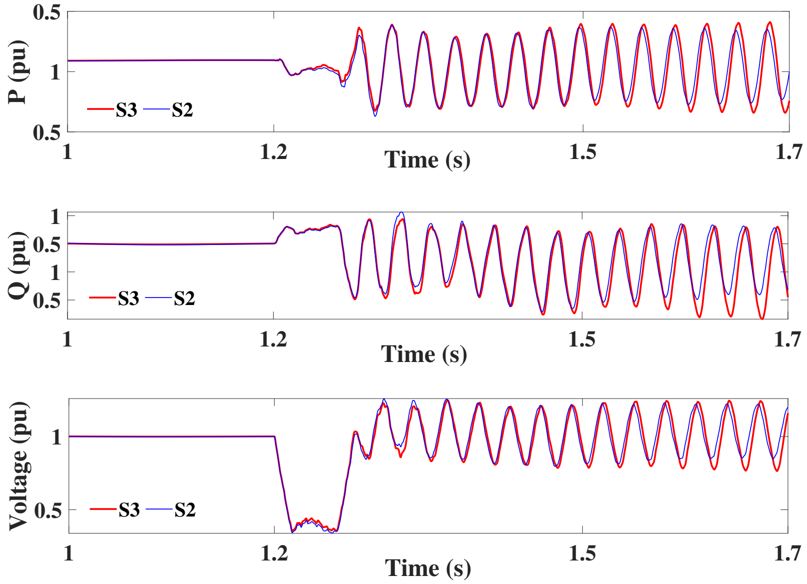


Figure 4.3: POI active power, reactive power, and voltage in S2 and S3.

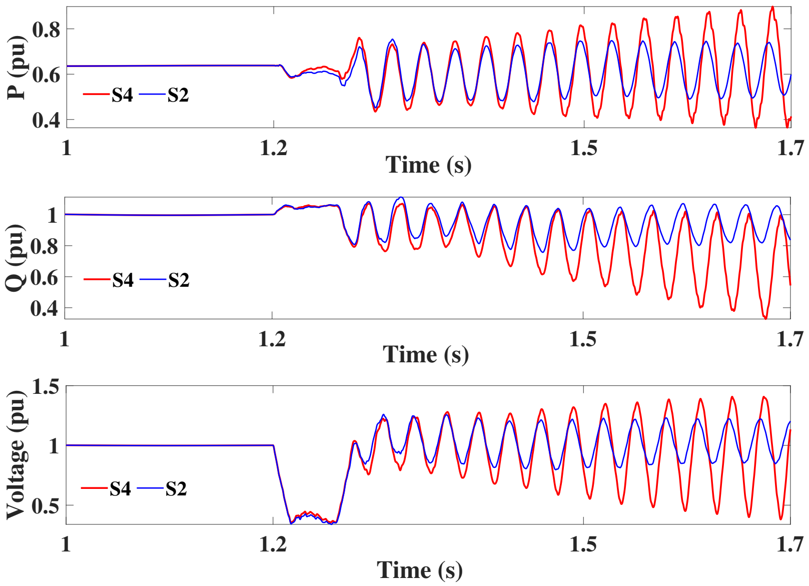


Figure 4.4: POI active power, reactive power, and voltage in S2 and S4.

SSCI is more severe—and 268 turbines are in service. Under normal conditions (S1 and S2), Fig. 4.2 shows that without SSDC the system is unstable, whereas the designed controller can dampen the oscillations. However, during the simulated FDI or DoS cyberattacks (S3 and S4), the SSDC's performance deteriorates significantly, leading to sustained oscillations and system instability as illustrated in Fig. 4.3- Fig. 4.4, respectively. For instance, in Fig. 4.3 SSDC's performance significantly degrades under FDI cyberattack, resulting in instability of the system due to sustained oscillation. Additionally, different instability patterns can be observed in the WP's waveforms in Fig. 4.4, where the WP is under a DoS attack targeting the SSDC control signals. These results underscore the importance of robust cybersecurity measures, including advanced detection systems, to effectively monitor and safeguard WP-integrated power systems against potential cyberattacks.

Figs. 4.2-4.4 show the temporal dependencies of the data recorded in both normal and attack scenarios. Features such as active power, reactive power, and voltage exhibit fluctuations over time. Therefore, capturing the time-series nature of the data is essential for identifying evolving patterns of instability.

Modern WP-integrated power systems exhibit highly dynamic behavior, driven by factors such as fluctuating wind speeds, varying numbers of in-service WTs, and shifting grid impedance. The inherent complexity of controlling such systems, combined with their reliance on communication links for real-time operation, renders them particularly susceptible to cyberattacks, including FDI and DoS attacks. Consequently, the development of advanced security monitoring and cyberattack detection systems has become increasingly attractive. These systems aim to ensure system integrity by continuously monitoring the security state of the power system and enabling real-time detection of potential cyber threats, thereby safeguarding the stability and reliability of WP-integrated power systems.

4.2 Motivation for using RNN-LSTM architecture

Unlike traditional model-based systems, ML-based methods excel in identifying sophisticated attacks by learning intricate patterns from datasets. ML algorithms are broadly categorized into supervised and unsupervised learning methods. Supervised learning relies on labeled datasets and feedback mechanisms to predict specific outcomes, while unsupervised learning operates on unlabeled data to uncover hidden patterns without external guidance. By leveraging these capabilities, ML methods offer a powerful means to identify subtle anomalies and evolving threats in modern power systems [65], [66].

WP-integrated power systems may exhibit time-sequential oscillatory behavior due to uncertainties in operating conditions—e.g., fluctuating wind speeds, varying numbers of WTs in service, and shifting grid impedance—as well as potential security issues. RNN-LSTM networks, a specialized variant of RNNs, are particularly well-suited for detection purposes when the data is time-sequential and oscillatory. Given the inherent uncertainties and the time-sequential nature of WP-integrated power systems, a method capable of handling sequential data and capturing long-term dependencies is essential. To address these needs, RNNs are well-suited for modeling sequential data as they retain information across time steps, enabling the capture of dependencies where past states influence future predictions. While RNNs can model sequential data by retaining information across time steps, they face limitations in capturing long-term dependencies due to the vanishing gradient problem [67]. To address this limitation, RNN-LSTMs incorporate memory cells and gating mechanisms that effectively manage relevant information over extended sequences, enabling the model to capture intricate temporal patterns.

Consequently, RNN-LSTMs are ideal for WP-integrated systems due to their ability to handle sequential data, capture long-term dependencies, and adapt to dynamic conditions. Additionally, their real-time processing capability ensures timely detection of cyberattacks, allowing for immediate interventions to maintain system stability and operational reliability.

4.3 Data generation for training and validation of the model

The data generation process is vital for effectively training the RNN-LSTM model under varying system conditions. To ensure comprehensive coverage of potential operational states, this study simulates system uncertainties in wind speed (W_s), number of WTs (N_{WT}) in-service, grid impedance (Z_{Grid}) under normal operation, FDI attacks, and DoS attacks. The data generation process involves multiple steps (i) system behavior is captured through EMT simulation of the understudy system in the presence of different uncertainties in W_s, N_{WT}, and Z_{Grid} under normal operation, FDI attacks, and DoS attacks. (ii) the feature set of the simulation results (F) are recorded including W_s, N_{WT}, park active power (P_{POI}), park reactive power (Q_{POI}), park voltage (V_{POI}), park current (I_{POI}),

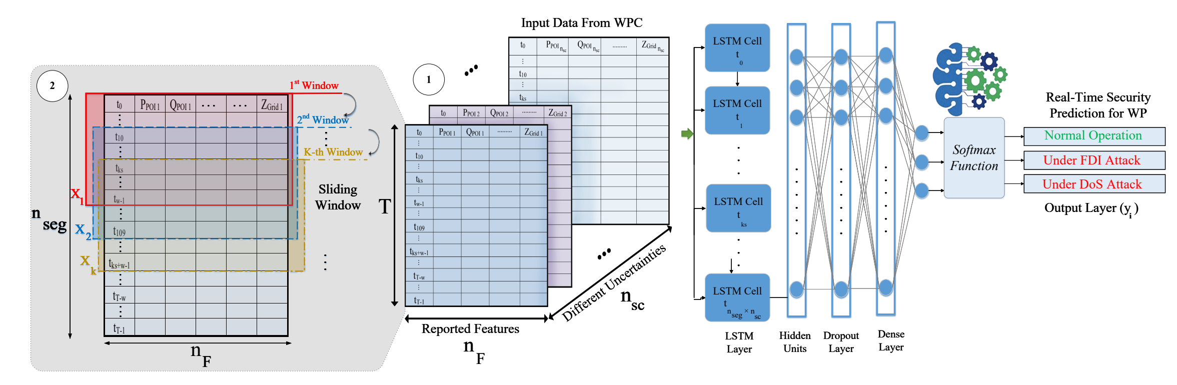


Figure 4.5: RNN-LSTM model structure for the security monitoring system under different uncertainties in WP system.

DC link voltage (V_{DC}), WPC reference signal (ΔV_{dfig}^{ref}), SSDC input signals (y), SSDC output signals (u), and grid impedance (Z_{Grid}). (iii) considering the assumption regarding the time of attack and disturbances, these features are extracted over a pre-determined period and stored in a dataset. (iv) The dataset is divided into two parts, one part is used for model training, while the other is reserved as an unseen dataset for validation. (v) The simulated data is processed for offline training of the RNN-LSTM model by cleaning, handling missing values, normalization, and scaling. Standardizing the data by removing the mean and scaling to unit variance ensures compatibility and enhances the model's efficiency [68].

This comprehensive dataset equips the RNN-LSTM model to effectively learn and detect patterns across varying operational states and cyberattack conditions, significantly enhancing the security monitoring and detection capabilities of the WP-integrated power system.

4.4 Designing the RNN-LSTM network detection model

In this section, we focus on designing an RNN-LSTM network by determining activation functions, selecting the optimization algorithm, and optimizing hyperparameters of the customized model (such as the number of hidden units, dropout rate, learning rate, batch size, and the number of training epochs) using Bayesian optimization [69]. This approach enables the model to effectively capture long-term dependencies in sequential data, crucial for identifying cyberattacks in WP-integrated power systems.

4.4.1 Structure of customized RNN-LSTM network

The structure of the customized RNN-LSTM network is shown in Fig. 4.5. As illustrated in this figure, the input of the proposed RNN-LSTM network model (① in Fig. 4.5) reshaped into a 3-D matrix containing n_{sc} 2-D matrices of dimensions $T \times n_F$ to accommodate multiple scenarios. Each 2-D matrix has T rows and n_F columns, representing the dataset of the number of features in the length of T time steps. A sliding window method (② in Fig. 4.5) is applied to capture temporal dependencies and patterns, with window size (W) and step size (S). This method creates overlapping segments, where the first segment includes time steps t_0 to t_{W-1}, and the k-th segment includes time steps t_{KS} to t_{KS+W-1}. Thus, the total number of segments n_{seg} is given by:

$$n_{\text{seg}} = \left\lfloor \frac{T - W}{S} \right\rfloor + 1 \tag{7}$$

Each segment is treated as an independent input X_i for training the RNN-LSTM model, enabling it to capture sequential patterns and classify different scenarios. When the input data is reshaped as discussed above, the next step is to send it to the LSTM layer, which is composed on $n_{\text{seg}} \ \times n_{\text{sc}}$ LSTM cells, each with a number of hidden units optimized through hyperparameter tuning. These cells are specifically designed to capture long-term dependencies and temporal patterns within the reshaped input data, enhancing the model's ability to detect subtle changes over time. The LSTM cell architecture as illustrated in Fig. 4.6 manages the flow of information through three main gates, which helps retain relevant information and discard unnecessary data at each time step. These gates allow the model to learn and remember important temporal patterns across the time steps, which are essential for detecting subtle attack-related changes in WP-based power system variables. The three gates are described as follows [70]:

- The forget gate helps the LSTM decide which information to discard from the cell state, based on the previous hidden state (h_{t-1}) and the current input (x_t). This ensures that the model keeps only the most relevant data. Mathematically, the forget gate is defined as:

$$f_t = \sigma(W_f \cdot [h_{t-1}, X_t] + b_f) \tag{8}$$

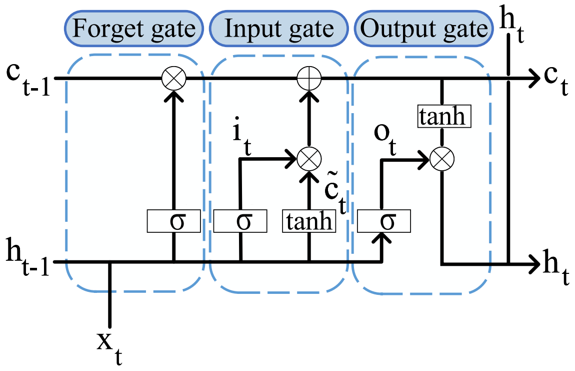


Figure 4.6: LSTM cell architecture.

The output f_t is multiplied with the previous cell state C_{t-1} to update the cell's memory.

- The input gate determines what new information to add to the cell state. It combines a sigmoid activation for input selection and a hyperbolic tangent function to generate the candidate cell state update:

$$i_t = \sigma(W_i \cdot [h_{t-1}, X_t] + b_i) \tag{9}$$

$$\tilde{C}_t = \tanh(W_c \cdot [h_{t-1}, X_t] + b_c) \tag{10}$$

$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t \tag{11}$$

This combination allows the LSTM to update the cell state (C_t) based on both past memory and new information. This process ensures that important new information is stored, while irrelevant information is discarded.

- The output gate controls what information from the updated cell state is passed to the next hidden state (h_t), enabling the network to propagate relevant information through time steps:

$$O_t = \sigma(W_o \cdot [h_{t-1}, X_t] + b_o) \tag{12}$$

$$h_t = O_t * \tanh(C_t) \tag{13}$$

It uses the current input and the previous hidden state to decide which parts of the cell state are relevant for the output. It should be noted that in Fig. 4.6, σ is the activation function.

To prevent overfitting, a dropout layer with a tuned dropout rate is then applied. During training, dropout randomly deactivates neurons, ensuring the model doesn't rely too heavily on any specific pattern, thereby improving its generalization ability across different scenarios. Following the LSTM layer, a dense layer or fully connected (FC) with a tuned number of units is added. FC layer is a type of neural network layer where each neuron is connected to every neuron in the previous layer. This layer takes the output of the LSTM layer and applies a weighted sum, followed by a rectified linear unit (ReLU) activation function. The ReLU function enables the model to learn nonlinear representations of the input data, which is crucial for distinguishing between normal operations and cyberattacks effectively. It should be noted that the output dataset of the RNN-LSTM model is a matrix with $n_{\text{seg}} \times n_{\text{sc}}$ rows and the three columns correspond to the predicted probabilities for considered three classes (i.e., normal, FDI, and DoS attacks) that classify each input using the last time step label in each window. Each row contains a probability distribution over these classes, with the predicted class determined by the highest probability. The output layer uses a softmax activation function, which converts the model's outputs into a probability distribution over the three classes. The softmax function ensures that the outputs sum to 1, allowing the model to predict the most likely class for each input.

4.4.2 Hyperparameter Tuning

The performance of DL models relies significantly on precise hyperparameter tuning, which influences the model's capacity to learn complex patterns and achieve high accuracy. Hyperparameters are the configurations that are set before the learning process begins, and finding the optimal values can significantly improve model accuracy and efficiency. To optimize the RNN-LSTM model, Bayesian optimization was used for its efficiency in exploring the hyperparameter search space [69]. This methodology uses a probabilistic model to estimate the performance of different hyperparameter configurations and uses an acquisition function to balance exploration (testing new hyperparameter values) and exploitation (refining promising configurations). Its iterative approach ensures an efficient search for optimal hyperparameters, particularly in complex models like LSTMs.

The tuned critical hyperparameters include the number of hidden units, dropout rate, learning rate, batch size, the number of training epochs, and optimizer. Hidden units were adjusted to improve the model's ability to capture long-term dependencies, while dropout was applied to prevent overfitting and enhance generalization. The learning rate, controlling the step size during optimization, and the batch size, determining the number of samples per update, were both fine-tuned for efficient training. The number of epochs balances training time and performance, and the optimizer's objective is to adjust weights and learning rates during the training of DL models, minimizing loss and enhancing accuracy.

The categorical cross-entropy loss function, which is detailed in [71], was utilized for our multiclass classification task. This function penalizes incorrect predictions, encouraging the model to assign high probabilities to the correct class. For three classes (normal, FDI, and DoS), the cross-entropy loss is:

$$L = -\frac{1}{N} \sum_{i=1}^{N} \sum_{c=1}^{3} y_{i,c} \log(\hat{y}_{i,c}), \tag{14}$$

where N is the number of training samples, $y_{i,c}$ is a binary indicator for whether class c is the correct label for sample i, and $\hat{y}_{i,c}$ is the predicted probability for class c.

In addition to hyperparameters, Bayesian optimization selected the Adam optimizer as the best-performing optimizer. Adam's adaptive learning rate, which adjusts dynamically based on the first and second moments of gradients, ensures efficient convergence and handles the nonlinear patterns in WP-integrated power system data effectively.

Integrating Bayesian optimization, categorical cross-entropy, and the Adam optimizer enables the RNN-LSTM model to achieve high accuracy and low latency. This configuration supports the continuous monitoring of incoming data streams, providing timely alerts to the WPC security monitoring system and ensuring the security of the WP-integrated power system.

Chapter 5

Simulation Results and Analysis

In this section, the simulations of the system under study (discussed in Section 3) were performed in EMTP-RV. The process of dataset generation and analysis of the collected results were performed in MATLAB. The SSDC is designed so that it can stabilize the system in the worst-case condition of the grid using the LQR technique. All simulations were performed on a Windows personal computer equipped with a 64-bit Intel i7 processor running at 2.9 GHz and 16 GB of RAM. Additionally, Google Colab with Python 3.8 was utilized to execute ML tasks. The RNN-LSTM model was developed using the TensorFlow library. Bayesian optimization was conducted using the Optuna framework for hyperparameter tuning.

5.1 Data Generation for Training and Validation

The dataset consists of 550 scenarios, with 480 scenarios allocated for training and 70 scenarios reserved as an unseen dataset for validation purposes. The training dataset comprises 160 scenarios each for normal, FDI, and DoS conditions and is divided into training and testing subsets using an 80:20 split. The unseen dataset consists of 30 normal, 20 FDI, and 20 DoS scenarios. This structured dataset generation ensures a comprehensive evaluation of the model's ability to generalize to new and unseen operational conditions.

To capture the normal behavior of the system, we changed operating conditions within a conventional range of wind speed, number of in-service WTs, and grid impedance. For instance, wind speed (W_s) was varied between 0.6 p.u. and 0.96 p.u., while the number of in-service WTs (N_{WT}) was changed from 161 (60%) to 268 (100%). Moreover, grid impedance (Z_{Grid}) was also varied across four levels to represent different grid operating conditions by multiplying the grid impedance by coefficients $\{0.8, 0.9, 1, 1.1\}$. It should be noted that such ranges are selected so that we have a diverse and possible operating range for the WP-integrated grid.

To create a wide range of attack scenarios and form the dataset, FDI and DoS attacks were simulated with varying severities.

For FDI attacks, the attack magnitudes (α) in the training and validation datasets were set to $\{0.95, 0.9, 0.85, 0.8, 0.75, 0.7, 0.65, 0.6\}$. Similarly, for DoS attacks, interruption durations ($t_2 - t_1$) were chosen as $\{0.5, 0.55, 0.6, 0.65, 0.7, 0.75, 0.8, 0.85\}$ seconds for training and validation datasets. In this study, the DoS attack is assumed to be launched concurrently with the occurrence of a fault (F1) and the activation of the FRT mechanism. This timing represents the worst-case scenario, as it blocks the SSDC precisely when it is most critical for damping oscillations and maintaining system stability.

All scenarios were simulated in EMTP-RV over a 0.5-second time window from t=1 s to t=1.5 s to capture the most relevant data for accurate attack detection. The data was sampled at a rate of 250 μs, producing 2001 time steps (T) per scenario.

The training dataset used in this study is inherently imbalanced, reflecting the attack timing. Moreover, considering the time steps T and the number of scenarios n_{sc}, we have 449,068 samples for normal operations, 320,160 for FDI attacks, and 191,252 for DoS attacks, all reported before applying the sliding window method. Similarly, the unseen dataset contains 76,050 samples for normal operations, 40,020 for FDI attacks, and 24,000 for DoS attacks, also before the employment of the sliding window method. This imbalance mirrors real-world conditions, where DoS attacks typically occur over shorter durations compared to normal operation or FDI scenarios.

A total of 91,680 inputs from normal and attack scenarios were generated for the training dataset after utilizing the sliding window method, while 13,370 inputs were created for the unseen dataset, considering the related n_{seg} and n_{sc}. The number of normal samples is higher than expected because the system's behavior before the initiation of a DoS attack is also considered normal operation, thereby contributing additional normal samples to the dataset.

5.2 Hyperparameter tuning

The hyperparameter tuning process focused on optimizing key parameters and selecting an appropriate optimizer from the defined search space using Bayesian optimization. The search space included LSTM layers with hidden units ranging from 32 to 128, dropout rates between 0.2 and 0.5, learning rates within the range of $[10^{-4}, 10^{-2}]$, number of epochs between 30 and 100, and batch sizes ranging from 16 to 32. Among the optimizers, RMSprop and Adam were evaluated. The best configuration included the Adam optimizer with 70 hidden units, a dropout rate of 0.37, a learning rate of 0.00077, a batch size of 32, and 60 epochs.

5.3 Benchmark Classifiers for Comparative Analysis

This section presents the reasons for choosing the other classifiers for benchmarking with the proposed RNN-LSTM model. The chosen classifiers are well-suited for the cyberattack classification task in the WP-based power system, which involves WP telemetry data and requires distinguishing intricate patterns. Each classifier brings unique strengths that make it applicable in this context:

- Random Forest:

  RF is a powerful ensemble learning method that combines the predictions of multiple decision trees (DTs), 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 [72]. As highlighted in [73], RF can handle large feature spaces effectively by constructing multiple DTs and aggregating their outputs. This makes it ideal for analyzing telemetry data from WP 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 WP-based power system.

- k-Nearest Neighbors:

kNN method, highlighted in [74], 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 being able to predict 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.

- Multilayer Perceptron:

  The references [75], [76] describes the MLP as a deep learning model capable of capturing complex, nonlinear data relationships, making it effective for analyzing intricate patterns in power systems. Its flexibility in learning intricate patterns makes it highly suitable for this task, particularly in capturing interactions between features influenced by WP-based system dynamics.

  These diverse strengths make them ideal benchmarks for evaluating the efficacy of the proposed model.

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): [5, 500].
  - Maximum depth: [10, 50].
  - Minimum samples split: [2, 10].
  - Minimum samples leaf: [1, 5].
  - Maximum features: [sqrt, log2].

The best RF parameters determined through Bayesian optimization are as follows: 167 estimators, a maximum depth of 34, a minimum of 2 samples required for a split, 5 samples per leaf node, and the square root of the total number of features considered for the best split.

- **kNN:**
  - Number of neighbors (k): [1, 30].
  - Weighting scheme: [Uniform, distance-based].
  - Distance metric: [Euclidean, Manhattan, Jaccard].

  The kNN classifier is tuned with 13 numbers of neighbors, using a distance-based weighting scheme, and the Euclidean distance metric to calculate distances.

- **Multilayer Perceptron (MLP):**
  - Hidden layer sizes: [32, 256].
  - Learning rate: [10^{-5}, 10^{-1}].
  - Activation functions: [ReLU, tanh]
  - Dropout rate: [0.2, 0.5].
  - Batch size: [16, 64]
  - Number of epochs: [20, 100]

  The MLP classifier is tuned, resulting in hidden layer sizes set to [64, 32], a learning rate of 10^{-3}, the ReLU activation function, a dropout rate of 0.3, a batch size of 32, and the number of epochs set to 50.

5.4 Performance of customized RNN-LSTM model

This section evaluates the performance of the proposed RNN-LSTM model in classifying cyber-attacks to monitor the security status of the WP-integrated power grid. The model's effectiveness is

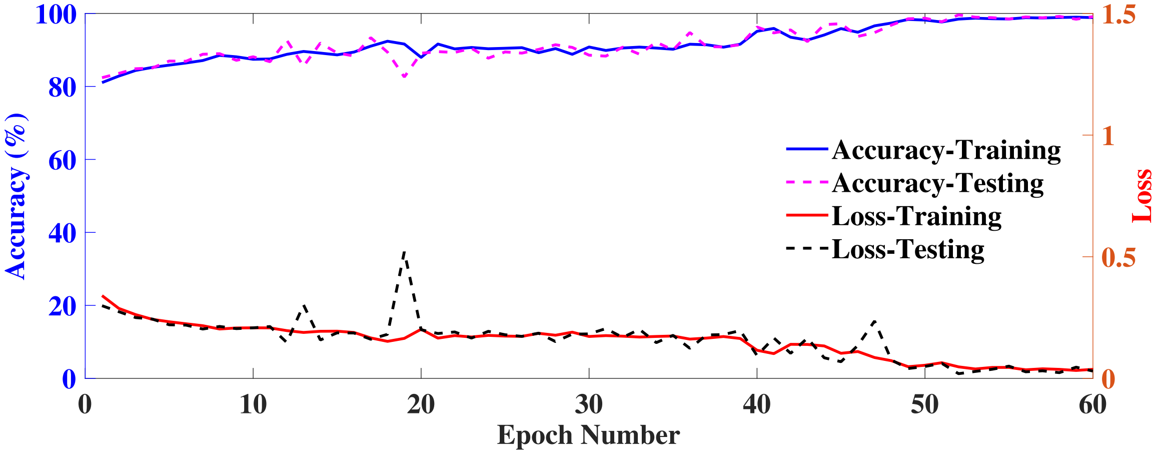


Figure 5.1: Accuracy and loss function for training and testing dataset plot.

assessed using multiple metrics. A comparative analysis with other well-established classifiers highlights the advantages of the proposed RNN-LSTM model for the WP security monitoring system. The model is also evaluated using a previously designed unseen dataset.

The accuracy and loss function plots for the training and testing data in the proposed model are illustrated in Fig. 5.1. These plots show the accuracy of training/testing and loss curves over 60 epochs. The model demonstrates a high level of accuracy on both the training and testing data, with a low and stable loss for both. The difference between training and testing accuracy is negligible, suggesting that the model is not overfitting and generalizes well to unseen data. From epochs 50 to 60, both training and testing accuracy remain consistently high without significant fluctuations, indicating stability in the model's performance.

The performance of the proposed model is evaluated in comparison with other established classifiers, such as RF [77, 73, 72], kNN [74], and MLP [75, 76].

The classification performance of the proposed RNN-LSTM model is evaluated using several criteria, including balanced accuracy (BACC), precision, recall, F1 score, and confusion matrix. These metrics for the multiclass classification task in this study are calculated as follows [78]:

- Balanced accuracy is particularly well-suited for addressing the class imbalance observed in our simulations, ensuring a fair evaluation across all classes. This metric highlights the model's performance in detecting normal and cyberattack scenarios and provides a comprehensive measure of its effectiveness, especially given the imbalanced dataset structure where interactions between classes are critical.

$$\text{BACC} = \frac{1}{3}\left(\frac{\text{TP}_{\text{DoS}}}{D_{\text{DoS}}} + \frac{\text{TP}_{\text{FDI}}}{D_{\text{FDI}}} + \frac{\text{TP}_{\text{n}}}{D_{\text{n}}}\right) \tag{15}$$

Where TP_{DoS}, TP_{FDI}, TP_{n} is true positives (TPs) for DoS, FDI, and normal, respectively. The denominators are defined as follows:

$$D_{\text{DoS}} = \text{TP}_{\text{DoS}} + \text{FN}_{\text{FDI, DoS}} + \text{FN}_{\text{n, DoS}} \tag{16}$$

$$D_{\text{FDI}} = \text{TP}_{\text{FDI}} + \text{FP}_{\text{DoS, FDI}} + \text{FN}_{\text{n, FDI}} \tag{17}$$

$$D_{\text{n}} = \text{TP}_{\text{n}} + \text{FP}_{\text{DoS, n}} + \text{FP}_{\text{FDI, n}} \tag{18}$$

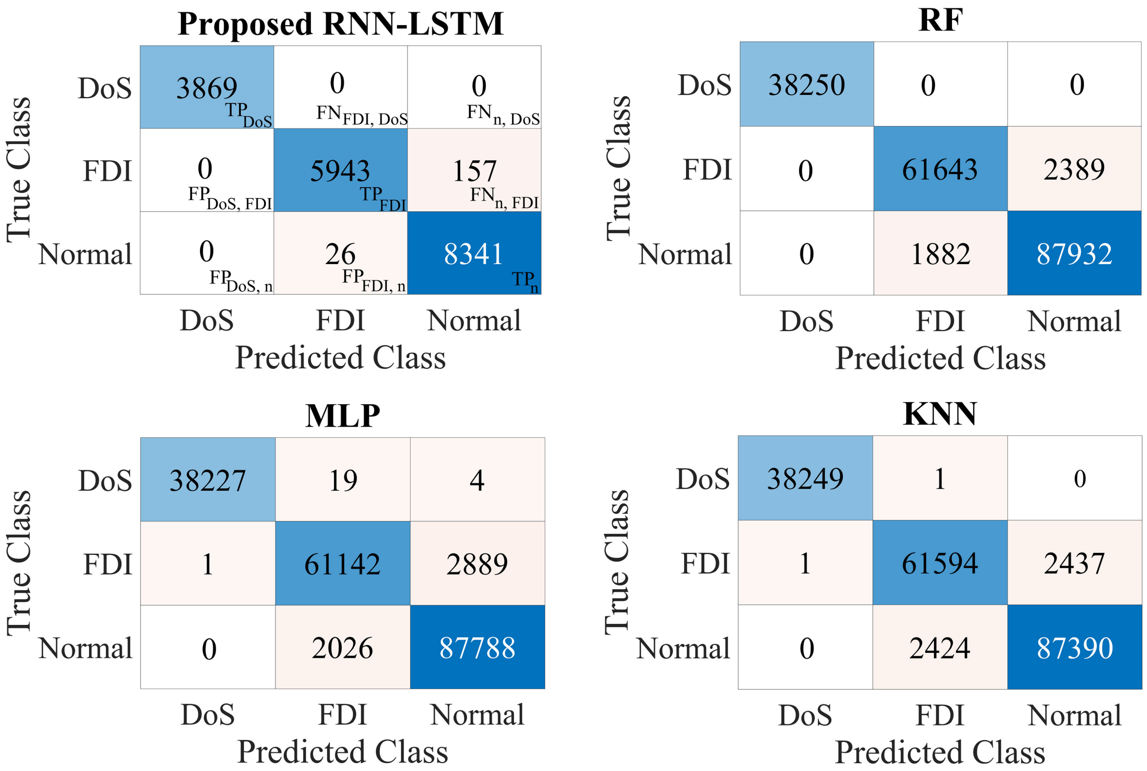
In these equations, D_{DoS} represents the sum of TPs for the DoS class and false negatives (FNs) where DoS is misclassified as FDI or normal. D_{FDI} is the sum of TPs for the FDI class and false positives (FPs) where DoS instances were incorrectly classified as FDI, as well as FNs where FDI instances were misclassified as normal. D_{n} includes the TPs for the normal class along with the FPs where other classes (DoS or FDI) were incorrectly classified as normal.

- 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.

$$\text{Precision} = \frac{\sum_{j=1}^{3} \text{TP}_j}{\sum_{j=1}^{3} \text{TP}_j + \text{FP}_{\text{DoS, FDI}} + \text{FP}_{\text{DoS, n}} + \text{FP}_{\text{n, FDI}}} \tag{19}$$

$$\text{Recall} = \frac{\sum_{j=1}^{3} \text{TP}_j}{\sum_{j=1}^{3} \text{TP}_j + \text{FN}_{\text{FDI, DoS}} + \text{FN}_{\text{n, DoS}} + \text{FN}_{\text{FDI, n}}} \tag{20}$$

where $j = 1, 2, 3$ corresponds to the classes DoS, FDI, and normal.



Proposed RNN-LSTM

True Class \ Predicted Class	DoS	FDI	Normal
DoS	3869 TP_{DoS}	0 $FN_{FDI, DoS}$	0 $FN_{n, DoS}$
FDI	0 $FP_{DoS, FDI}$	5943 TP_{FDI}	157 $FN_{n, FDI}$
Normal	0 $FP_{DoS, n}$	26 $FP_{FDI, n}$	8341 TP_{n}

RF

True Class \ Predicted Class	DoS	FDI	Normal
DoS	38250	0	0
FDI	0	61643	2389
Normal	0	1882	87932

MLP

True Class \ Predicted Class	DoS	FDI	Normal
DoS	38227	19	4
FDI	1	61142	2889
Normal	0	2026	87788

KNN

True Class \ Predicted Class	DoS	FDI	Normal
DoS	38249	1	0
FDI	1	61594	2437
Normal	0	2424	87390

Figure 5.2: Confusion matrices for different classification methods.

- 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:

$$\text{F1 Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{21}$$

The confusion matrices for our proposed RNN-LSTM 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, and DoS attacks.

Table 5.1: Comparison of different methods for classification performance

Classifier	Balanced Accuracy	Precision	Recall	F1 Score
kNN	97.83%	98.72%	98.71%	98.71%
MLP	97.85%	98.92%	98.46%	98.69%
RF	98.13%	99.00%	98.74%	98.87%
Proposed RNN-LSTM	99.23%	99.85%	99.14%	99.49%

The proposed RNN-LSTM model demonstrates outstanding classification performance across all three classes. Notably, it achieves zero FPs and FNs for the DoS class, reflecting its superior ability to capture temporal dependencies and accurately detect the unique characteristics of DoS attacks. Similarly, the FDI and normal classes exhibit minimal misclassifications, with only a small fraction of FDI samples being misclassified as normal. This highlights the model's strength in handling imbalanced datasets and distinguishing between closely related classes. Additionally, the ability of the proposed method to accurately distinguish between DoS and FDI attacks is particularly valuable, enabling WP operators to take timely preventive actions based on the specific type of detected attack. Among the classifiers, the RF model demonstrates high accuracy across all classes, particularly excelling in the classification of the DoS class. However, the MLP and kNN classifiers exhibit notable misclassification errors, particularly in distinguishing between the FDI and normal classes with higher FN and FP instances. Table. 5.1 summarizes the comparative performance of the proposed developed model against kNN, MLP, and RF. The proposed RNN-LSTM model achieves the highest BACC of 99.23%, indicating its superior ability to correctly classify instances across all classes, even under the dataset's inherent imbalance. This is a significant improvement over the RF, which exhibits a BACC of 98.13%, and the MLP and kNN, which show balanced accuracies of 97.85% and 97.83%, respectively.

In terms of precision, the RNN-LSTM model outperforms the other classifiers with a precision score of 99.85%. While RF follows closely with a precision of 99.00%, both MLP and kNN show slightly lower values of 98.92% and 98.72%, respectively.

The recall metric, which measures the model's ability to identify TPs, also highlights the RNN-LSTM's dominance with a recall score of 99.14%. This suggests that the model can effectively detect even the less frequent cyberattack scenarios (e.g., DoS attacks), minimizing the risk of FNs. In comparison, RF achieves a recall of 98.74%, whereas MLP and kNN show recalls of 98.46% and 98.71%, respectively.

Finally, F1 score further underscores the RNN-LSTM model's superiority. Achieving an F1 score of 99.49%, the proposed model balances high precision and recall, making it suitable for this classification task. RF, MLP, and kNN achieve F1 scores of 98.87%, 98.69%, and 98.71%, respectively, reflecting their comparatively lower consistency in handling the complex temporal and

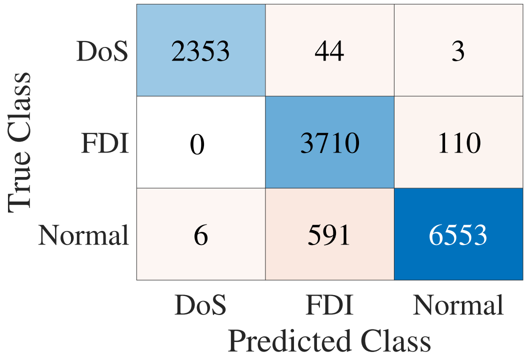


Figure 5.3: Confusion matrix for RNN-LSTM model on the unseen dataset.

class-dependent patterns present in the dataset.

The performance metrics collectively highlight the effectiveness of the customized RNN-LSTM model, which enables it to capture intricate temporal dependencies in the data. This capability proves critical in achieving high classification accuracy, particularly in distinguishing between the DoS and FDI classes, where temporal features play a significant role.

5.4.1 Model Validation on Unseen Data

The developed RNN-LSTM model was validated using the described unseen dataset, demonstrating strong generalization capabilities. The model achieved a BACC of 94.48%, recall of 98.77%, precision of 95.48%, and an F1 score of 97.09%. It effectively detected DoS attacks, correctly classifying 2,353 out of 2,400 samples, with only 3 and 44 misclassifications as normal and FDI as illustrated in Fig. 5.3. However, the model faced difficulty distinguishing between FDI and normal classes, as 591 normal samples were misclassified as FDI. This reflects the challenge of separating these two classes due to their similar behavior.

The model exhibited particularly high precision, especially for DoS attacks, achieving a near-perfect score of 99.74%, indicating its ability to identify TPs and minimize FPs—a critical feature for security monitoring. However, precision for the FDI class is lower at 86.25% compared to DoS and normal, indicating more FPs where normal instances are incorrectly classified as FDI. The recall for FDI (96.01%) was slightly lower than DoS and normal classes, likely due to overlapping patterns or subtler differences between FDI and normal classes. This performance suggests that the model can reliably identify FDI attacks, even with subtle data manipulations and variations in the

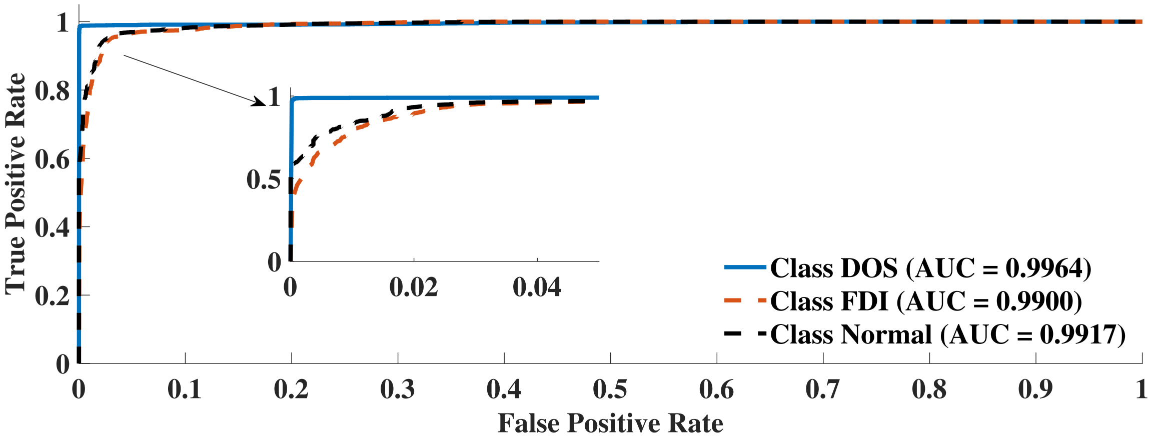


Figure 5.4: ROC curves for normal, FDI, and DoS classes.

mentioned WP-based uncertainties along with different attack vectors within the unseen dataset. Despite this, the model excels at distinguishing DoS attacks from FDI, ensuring that WP operators receive timely and reliable alerts for preventive actions.

5.4.2 ROC and AUC Analysis

To further evaluate the model's performance on the unseen data, receiver operating characteristic (ROC) curves and their corresponding area under the curve (AUC) metrics were analyzed. The AUC is a critical metric, particularly in imbalance datasets, as it provides a robust measure of model performance by summarizing the trade-off between the TP rate and FP rate across different threshold values [78].

A higher AUC value suggests a stronger performance, as it indicates the model's ability to maintain a high TP rate while minimizing a low FP rate across all decision thresholds. As illustrated in Fig. 5.4, the AUC values for the DoS, normal, and FDI classes were 0.9964, 0.9917, and 0.99, respectively. The high AUC score of 0.9964 for DoS indicates exceptional accuracy in detecting these attacks, with minimal risk of FPs. The slightly lower AUC for the FDI class is due to the inherent challenges of distinguishing FDI from normal operations. FDI attacks often exhibit patterns that closely resemble normal behavior, resulting in feature overlap, and they introduce only subtle deviations in system parameters, making detection more challenging compared to the more disruptive DoS attacks.

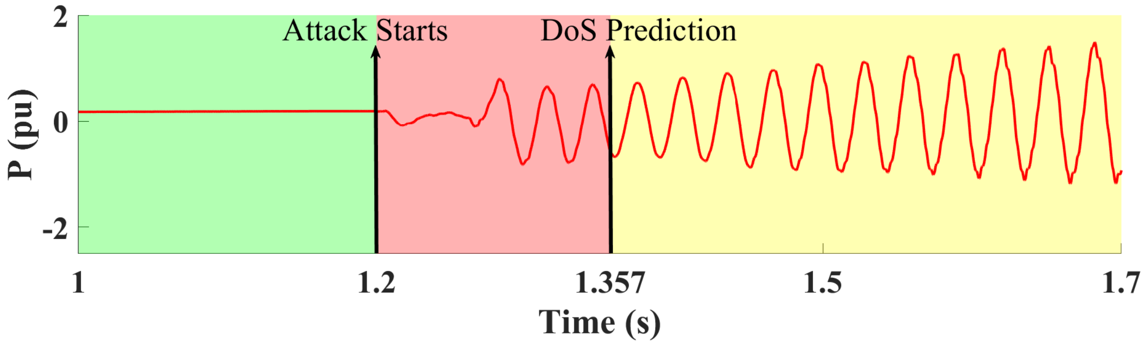


Figure 5.5: Time-domain detection of DoS attack using RNN-LSTM model.

5.5 Real-Time Security Monitoring System Implementation

This section evaluates the feasibility of implementing the developed RNN-LSTM-based security monitoring system for real-time operations in WP-based power grids. The timely detection of cyberattacks is critical for WP operators to issue alerts and initiate protective measures.

The average inference time of the RNN-LSTM model is approximately 132 ms per prediction over 100 iterations. This low latency allows the system to provide frequent updates, meeting the dynamic operational requirements of WP-based systems. As illustrated in Fig. 5.5, the proposed system effectively detect the evolving DoS cyberattack in near real-time. The slight prediction delay of 132 ms remains well within the acceptable operational thresholds for WP-integrated power systems, allowing operators to take rapid action to maintain system stability and security.

The proposed security monitoring system is integrated within the WPC, utilizing the WP SCADA architecture to access real-time WP operational data through secure interfaces, such as application programming interfaces (APIs) or shared databases. The real-time security monitoring system retrieves the required data via this interface. Initially, the data is preprocessed and reshaped into a 3-D format with a 250 μs sampling rate to ensure compatibility with the trained RNN-LSTM model. Subsequently, a sliding window approach, with a window size of 100 and a step size of 10, generates overlapping input segments every 25 ms, which allows the system to effectively capture temporal patterns essential for real-time analysis.

The trained RNN-LSTM model classifies the WP's security status as either normal, FDI, or DoS, and generates alerts accordingly. In the event of a detected cyberattack, the system promptly notifies WP operators, enabling them to respond with appropriate countermeasures. Predictions are refreshed approximately every 132 ms, ensuring that the system provides timely and accurate security updates that align with the operational needs of WP-based power grids.

Chapter 6

Conclusion

The growing integration of DFIG-based WPs into modern power grids highlights the dual challenge of addressing inherent stability issues and detecting rising cybersecurity threats. This study addresses these challenges by proposing a data-driven framework based on an RNN-LSTM model for detecting FDI and DoS attacks targeting the performance of SSDC in WP-integrated power systems. The proposed RNN-LSTM model was trained on a simulated dataset that captured diverse normal operating conditions and various cyberattack scenarios, accounting for uncertainties in the operation of wind-integrated power grids.

This trained model demonstrated superior classification performance compared to well-known ML models, including RF, KNN, and MLP. Specifically, the RNN-LSTM model achieved a BACC of 99.23% on test data and 94.48% on unseen data, significantly outperforming the other classifiers. The model's superiority is attributed to its ability to capture long-term dependencies and temporal patterns essential in distinguishing between normal operations and cyberattack conditions. Furthermore, the proposed model yields low latency, which makes it a suitable option for near real-time operation of WPs. Future research will focus on extending this framework to address multi-vector cyberattacks and developing adaptive mitigation strategies to enhance the robustness of WP-integrated power systems. Moreover, by utilizing the proposed benchmark prone to the SSCI conditions, future studies can develop detection methods to accurately localize cyberattack points, enabling more effective preventive measures in WP-based power grids.

Bibliography

[1] GWEC. “global wind report 2024”. *Global Wind Energy Council,*, Online: https://gwec.net/global-wind-report-2024, 2024.

[2] IEA. “renewables 2024: Analysis and forecast to 2030”. *International Energy Agency,*, Online: https://www.iea.org, 2024.

[3] Anissia Beainy, Chantal Maatouk, Nazih Moubayed, and Fouad Kaddah. “comparison of different types of generator for wind energy conversion system topologies”. pages 1–6, 2016. doi: 10.1109/REDEC.2016.7577535.

[4] Adil Mansouri, Abdelmounime El Magri, Rachid Lajouad, Ilyass El Myasse, El Khlifi Younes, and Fouad Giri. “wind energy based conversion topologies and maximum power point tracking: A comprehensive review and analysis”. *Advances in Electrical Engineering, Electronics and Energy*, 6:100351, 2023. ISSN 2772-6711. doi: https://doi.org/10.1016/j.prime.2023.100351.

[5] 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.

[6] 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.

[7] "terms, definitions and symbols for subsynchronous oscillations". *IEEE Transactions on Power Apparatus and Systems*, PAS-104(6):1326–1334, 1985. doi: 10.1109/TPAS.1985.319152.

[8] "proposed terms and definitions for subsynchronous oscillations". *IEEE Transactions on Power Apparatus and Systems*, PAS-99(2):506–511, 1980. doi: 10.1109/TPAS.1980.319686.

[9] Hailian Xie and M. de Oliveira. "mitigation of ssr in presence of wind power and series compensation by svc". *2014 International Conference on Power System Technology*, pages 2819–2826, 2014.

[10] Dawei Sun, Xiaorong Xie, Yuquan Liu, Ke Wang, and Meng Ye. "investigation of ssti between practical mmc-based vsc-hvdc and adjacent turbogenerators through modal signal injection test". *IEEE Transactions on Power Delivery*, 32(6):2432–2441, 2017. doi: 10.1109/TPWRD.2016.2636165.

[11] Garth D. Irwin, Amit K. Jindal, and Andrew L. Isaacs. "sub-synchronous control interactions between type 3 wind turbines and series compensated ac transmission systems". In *2011 IEEE Power and Energy Society General Meeting*, pages 1–6, 2011. doi: 10.1109/PES.2011.6039426.

[12] John Adams, Venkata Ajay Pappu, and Anuj Dixit. "ERCOT experience screening for sub-synchronous control interaction in the vicinity of series capacitor banks", 2012.

[13] Liang Wang, Xiaorong Xie, Qirong Jiang, Hui Liu, Yu Li, and Huakun Liu. "investigation of ssr in practical dfig-based wind farms connected to a series-compensated power system". *IEEE Transactions on Power Systems*, 30(5):2772–2779, 2015. doi: 10.1109/TPWRS.2014.2365197.

[14] Huakun Liu, Xiaorong Xie, Chuanyu Zhang, Yu Li, Hui Liu, and Yinghong Hu. "quantitative ssr analysis of series-compensated dfig-based wind farms using aggregated rlc circuit model". *IEEE Transactions on Power Systems*, 32(1):474–483, 2017. doi: 10.1109/TPWRS.2016.2558840.

[15] Babak Badrzadeh, Mandhir Sahni, Yi Zhou, Dharshana Muthumuni, and Aniruddha Gole. “general methodology for analysis of sub-synchronous interaction in wind power plants”. *IEEE Transactions on Power Systems*, 28(2):1858–1869, 2013. doi: 10.1109/TPWRS.2012.2225850.

[16] Kanghui Gu, Feng Wu, and Xiao-Ping Zhang. “sub-synchronous interactions in power systems with wind turbines: a review”. *IET Renewable Power Generation*, 13(1):4–15, 2019. doi: https://doi.org/10.1049/iet-rpg.2018.5199.

[17] 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.

[18] 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.

[19] 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.

[20] Jan Shair, Xiaorong Xie, Jianjun Yang, Jingyi Li, and Haozhi Li. “adaptive damping control of subsynchronous oscillation in dfig-based wind farms connected to series-compensated network”. *IEEE Transactions on Power Delivery*, 37(2):1036–1049, 2022. doi: 10.1109/TPWRD.2021.3076053.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] Megan Egan. “a retrospective on 2022 cyber incidents in the wind energy sector and building future cyber resilience”. *Boise State University*, 2022.

[39] 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.

[40] 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.

[41] 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.

[42] Mohammad Ashraf Hossain Sadi, Dongbo Zhao, Tianqi Hong, and Mohd. Hasan Ali. “time sequence machine learning-based data intrusion detection for smart voltage source converter-enabled power grid”. *IEEE Systems Journal*, 17(2):2477–2488, 2023. doi: 10.1109/JSYST.2022.3186619.

[43] 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.

[44] 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.

[45] Hossein Mahvash, Seyed Abbas Taher, and Josep Guerrero. “a new nonlinear virtual inertia approach to mitigate destructive effects of cyber attacks on active power and rotor speed profiles of wind turbine dfig sustainable energy production”. *Smart Grids and Sustainable Energy*, 9, 03 2024. doi: 10.1007/s40866-024-00201-9.

[46] Hamed Badihi, Saeedreza Jadidi, Ziquan Yu, Youmin Zhang, and Ningyun Lu. “smart cyber-attack diagnosis and mitigation in a wind farm network operator”. *IEEE Transactions on Industrial Informatics*, 19(9):9468–9478, 2023. doi: 10.1109/TII.2022.3228686.

[47] 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.

[48] 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.

[49] Naveen Tatipatri and S. L. Arun. “a comprehensive review on cyber-attacks in power systems: Impact analysis, detection, and cyber security”. *IEEE Access*, 12:18147–18167, 2024. doi: 10.1109/ACCESS.2024.3361039.

[50] 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.

[51] M. A. S. P. Dayarathne, M. S. M. Jayathilaka, R. M. V. A. Bandara, V. Logeeshan, S. Kumarawadu, and C. Wanigasekara. “deep learning-based cyber attack detection in power grids with increasing renewable energy penetration”. In *2024 IEEE World AI IoT Congress (AIIoT)*, pages 521–526, 2024. doi: 10.1109/AIIoT61789.2024.10578979.

[52] G. Varshini and S. Latha. “detection of data integrity attack in cyber physical power system using data-driven method”. pages 1–9, 12 2023. doi: 10.1109/ICEMCE57940.2023.10434053.

[53] Yi Wang, Mahmoud M. Amin, Jian Fu, and Heba B. Moussa. “a novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids”. *IEEE Access*, 5: 26022–26033, 2017. doi: 10.1109/ACCESS.2017.2769099.

[54] Mohsen Ghafouri, Ulas Karaagac, Jean Mahseredjian, and Houshang Karimi. “ssci damping controller design for series-compensated dfig-based wind parks considering implementation challenges”. *IEEE Transactions on Power Systems*, 34(4):2644–2653, 2019. doi: 10.1109/TPWRS.2019.2891269.

[55] Mohsen Ghafouri. *“Subsynchronous Resonance in DFIG-Based Wind Farms”*. PhD thesis, École Polytechnique de Montréal, 2018.

[56] Ulas Karaagac, Jean Mahseredjian, Simon Jensen, Richard Gagnon, Martin Fecteau, and Ilhan Kocar. “safe operation of dfig based wind parks in series compensated systems”. In *2018 IEEE Power Energy Society General Meeting (PESGM)*, pages 1–1, 2018. doi: 10.1109/PESGM.2018.8586524.

[57] Jorge Martinez Garcia. Voltage control in wind power plants with doubly fed generators, 2010.

[58] U Karaagac, H Saad, J Peralta, and J Mahseredjian. “doubly-fed induction generator based wind park models in emtp-rv”. *Polytechnique Montréal, Canada*, 2015.

[59] “grid code—high and extra high voltage”. *E.ON Netz GmbH*, 2006.

[60] Jared Verba and Michael Milvich. “idaho national laboratory supervisory control and data acquisition intrusion detection system (scada ids)”. In *2008 IEEE Conference on Technologies for Homeland Security*, pages 469–473, 2008. doi: 10.1109/THS.2008.4534498.

[61] Hamze Hajian-Hoseinabadi. “reliability and component importance analysis of substation automation systems”. *International Journal of Electrical Power & Energy Systems*, 49:455–463, 2013.

[62] Yichi Zhang, Lingfeng Wang, Yingmeng Xiang, and Chee-Wooi Ten. “power system reliability evaluation with scada cybersecurity considerations”. *IEEE Transactions on Smart Grid*, 6 (4):1707–1721, 2015. doi: 10.1109/TSG.2015.2396994.

[63] “international-electrotechnical-commission standards”. Online: https://webstore.iec.ch/home.

[64] 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.

[65] Oyeniyi Akeem Alimi, Khmaies Ouahada, and Adnan M. Abu-Mahfouz. “a review of machine learning approaches to power system security and stability”. *IEEE Access*, 8:113512–113531, 2020. doi: 10.1109/ACCESS.2020.3003568.

[66] Christopher Bishop. *“Pattern Recognition and Machine Learning”*, volume 16, pages 140–155. 01 2006. doi: 10.1117/1.2819119.

[67] Junzhe Wang and Evren M. Ozbayoglu. “application of recurrent neural network long short-term memory model on early kick detection”. *International Conference on Offshore Mechanics and Arctic Engineering*, 10:1–10, 2022. doi: 10.1115/OMAE2022-78739.

[68] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and É. Duchesnay. “scikit-learn: Machine learning in python”. *CoRR*, abs/1201.0490, 2012.

[69] Uphar Singh, Sanghmitra Tamrakar, Kumar Saurabh, Ranjana Vyas, and O.P. Vyas. “hyper-parameter tuning for lstm and arima time series model: A comparative study”. In *2023 IEEE 4th Annual Flagship India Council International Subsections Conference (INDISCON)*, pages 1–6, 2023. doi: 10.1109/INDISCON58499.2023.10270325.

[70] Chen Liu. “long short-term memory (lstm)-based news classification model”. *PLOS ONE*, 19 (5):1–23, 05 2024. doi: 10.1371/journal.pone.0301835.

[71] Yaoshiang Ho and Samuel Wookey. “the real-world-weight cross-entropy loss function: Modeling the costs of mislabeling”. *IEEE Access*, 8:4806–4813, 2020. doi: 10.1109/ACCESS.2019.2962617.

[72] 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.

[73] 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.

[74] Frank Acito. “predictive analytics with knime: Analytics for citizen data scientists”. *Springer Nature Switzerland*, 2023.

[75] Bongsoo Yi, Yao Li, and Thomas C. M. Lee. *“Multilayer Perceptrons: An Introduction”*, pages 1–10. John Wiley Sons, Ltd, 2023. ISBN 9781118445112. doi: 10.1002/9781118445112.stat08394.

[76] Lucas Costa, Márcio Guerreiro, Erickson Puchta, Yara de Souza Tadano, Thiago Antonini Alves, Maurıcio Kaster, and Hugo Valadares Siqueira. “multilayer perceptron”. *Introduction to Computational Intelligence*, 105, 2023.

[77] Grzegorz Dudek. “a comprehensive study of random forest for short-term load forecasting”. *Energies*, 15(20):7547–7547, 2022. doi: 10.3390/en15207547.

[78] 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.