

Cyber-security Enhancement of Wide-area Monitoring, Protection, and Control Systems

Masoud Zadsar

A Thesis

in The Department of

Concordia Institute for Information and Systems Engineering (CIISE)

Presented in Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy (Information and Systems Engineering) at

Concordia University

Montréal, Québec, Canada

August 2024

© Masoud Zadsar, 2024

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Masoud Zadsar**

Entitled: **Cyber-security Enhancement of Wide-area Monitoring, Protection, and Control Systems**

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

Doctor of Philosophy (Information and 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:

Dr. Xiaozhe Wang External Examiner

Dr. Chunyan Lai Examiner

Dr. Amr Youssef Examiner

Dr. Chadi Assi Examiner

Dr. Mohsen Ghafouri Supervisor

Approved by

Dr. Michel Trudeau, Chair
Department of Chemical and Materials Engineering

Date of Defence August 6, 2024

Prof. Mourad Debbabi, Dean
Faculty of Engineering and Computer Science

Abstract

Cyber-security Enhancement of Wide-area Monitoring, Protection, and Control Systems

Masoud Zadsar, Ph.D.

Concordia University, 2024

Wide-area monitoring, protection and control (WAMPAC) systems have emerged as a promising solution to improve situational awareness of power grid operators. WAMPAC systems collect system-wide measurements through communication infrastructure, synchronize using global positioning system (GPS) in phasor measurement units (PMUs), and utilize them to evaluate the system operation condition and make appropriate real-time protection and control decisions. Despite the provided advantages, the reliance of WAMPAC systems on information and communication technologies (ICTs) makes them prone to various cyber attacks. The socioeconomic impacts of the real-world cyber-attacks on power grids such as the 2015 Ukraine power grid attack have prompted the national level institutions to initiate several road-maps emphasizing the necessity of new adoptions toward cyber security enhancement in the North America power grids. To take step toward this adaptation, this thesis initially investigates the vulnerability of wide-area applications in integrated power and gas systems (IPGSs) and proposes a preventive defense strategy and online neural network detection scheme. Afterward, this thesis emphasizes on the vulnerability of data aggregation standards and protocols in WAMPAC systems to time-synchronization attacks (TSAs). During prevention phase, this thesis proposes a robust optimization model to obtain communication configuration between PMUs and control centers in order to minimize TSA consequences. Following the prevention phase, this thesis proposes an integrated TSA detection and mitigation scheme. The TSA detection scheme is a convolutional neural network (CNN) model which captures the temporal correlation of data quality information to identify and localize TSAs. In the

mitigation phase, a new robust state observer mitigation scheme is proposed for wide-area control applications. Eventually, this thesis emphasizes on vulnerability of grid supporting functions in inverter-based resources (IBRs) to a resonance cyber-attack. As a countermeasure, this thesis proposes a new wavelet-enabled wide neural network model which not only detects resonance FDIAs on grid-connected IBRs, but also distinguishes them from normal system events. Numerical results from multiple test benchmarks demonstrate that the proposed prevention, detection, and mitigation schemes in this thesis not only improve the security of wide-area control applications but also do not compromise normal system performance.

Acknowledgments

I would like to extend my deepest gratitude to my family for their unwavering support and encouragement throughout my academic journey. Their belief in me has been a constant source of motivation.

I am profoundly grateful to my supervisor, Dr. Mohsen Ghafouri, for his invaluable guidance, insightful feedback, and continuous support, which have been instrumental in the completion of this work. I also wish to express my sincere appreciation to my colleagues and co-authors at Concordia University for their collaborative efforts, stimulating discussions, and dedicated contributions. Eventually, I want to thank all technical supports of Dr. Amir Ameli from Lakehead University and Dr. Bassam Moussa from Hydro-Québec Research Institute (IREQ), as without their assistance and camaraderie, this thesis would not have been possible. Thank you all for your significant roles in this endeavor. Eventually, I would like to express my gratitude for the financial support provided by Fonds de recherche du Québec (FRQ) for this thesis.

Contents

List of Figures	x
List of Tables	xiv
Nomenclature	xvi
1 Introduction	1
1.1 Cyber-physical Architecture of WAMPAC Systems	1
1.1.1 Standards for Implementation of WAMPAC systems	3
1.2 WAMPAC Applications	4
1.2.1 Wide-Area Monitoring Applications	4
1.2.2 Wide-Area Protection Applications	6
1.2.3 Wide-Area Control Applications	7
1.3 Scope of the Work	8
1.4 Research Contributions	9
2 Security Enhancement of EMS	12
2.1 Problem Statement	12
2.2 Literature Review and Research Gaps	12
2.3 Attack Model	15
2.3.1 Cyber Vulnerabilities of IPGSSs	15
2.3.2 First stage: FDIA on EMS	16
2.3.3 Second stage: FDIA on pipeline monitoring system	21
2.3.4 Methodology for Solving the Bi-level Optimization Problems	26

2.4	Proposed Countermeasures	28
2.4.1	Preventive Defense Strategy	29
2.4.2	Online Learning-based Detection Scheme	31
2.5	Results and Discussion	34
2.5.1	Consequences of the Attack Model	34
2.5.2	Effectiveness of the Preventive Defense Strategy	38
2.5.3	Performance of the Online Learning-based Detection	39
2.5.4	Performance Evaluation on a Large-Scale IPGS	43
3	Security Enhancement of WADC- Part I	47
3.1	Problem Statement	47
3.2	Literature Review and Research Gaps	48
3.3	Attack Model	50
3.3.1	Assumptions of The Attack	50
3.3.2	Implementation of The Attack	52
3.4	Proposed Countermeasure	58
3.4.1	Model to Optimize Preventive Countermeasure	60
3.4.2	Methodology to solve Preventive Countermeasure Model	61
3.5	Results and Discussion	63
3.5.1	Case-I: Two-Area Kundur Test System	64
3.5.2	Case-II: IEEE 39-Bus Test System:	67
3.5.3	Sensitivity Analysis	71
3.5.4	Impact of the Proposed Preventive Countermeasure on Other Wide Area Applications	73
4	Security Enhancement of WADCs- Part II	76
4.1	Problem Statement	76
4.2	Literature Review and Research Gaps	77
4.3	Attack Model	79
4.3.1	Attack Surface, Intrusion Path, and Vulnerability	79

4.3.2	Attack Vector Optimization Model	84
4.4	Proposed Countermeasure	87
4.4.1	Deep Learning Based Detection Scheme	88
4.4.2	Robust State Observer Mitigation Scheme	92
4.5	Numerical Results and Discussions	96
4.5.1	Case-I: Two-Area Kundur Test System	99
4.5.2	Case-II: IEEE 39-Bus Test System	100
4.5.3	Performance Comparison of the Detection Scheme	102
4.5.4	Performance Comparison of the Mitigation Scheme	104
4.5.5	Solution Scalability	108
5	Security Enhancement of Grid-Supporting Functions in Inverter-Based Resources	111
5.1	Problem Statement	111
5.2	Literature Review and Research Gaps	112
5.3	Attack Model	113
5.3.1	Attacker's Objective	113
5.3.2	Intrusion Path	114
5.3.3	Attack Vector Construction	115
5.4	Proposed Countermeasure	118
5.4.1	Wavelet-Enabled Resonance Attack Detection Scheme	118
5.4.2	Frequency Features Extracted by DWT	119
5.4.3	Statistical Features	122
5.4.4	Optimized Wide Neural Network Classifier	123
5.5	Numerical Results and Discussion	124
5.5.1	Impact of Resonance Attack	124
5.5.2	Performance of the Proposed Resonance Attack Detection Scheme	127
5.5.3	Impact of Integration Statistical Features	130
5.5.4	Performance of the Optimized Wide Neural Network model	130
5.5.5	Detection Model's Robustness to Imbalanced Real-World Data	131

6 Conclusion and Future Work	137
Bibliography	143

List of Figures

Figure 1.1	Overall structure of WAMPAC systems.	2
Figure 2.1	The proposed attack model against IPGS.	14
Figure 2.2	FDIA against the EMS in power networks.	17
Figure 2.3	FDIA against pipelines monitoring system.	22
Figure 2.4	Defense strategy on a sample power system.	26
Figure 2.5	Utilized MLP neural network structure.	31
Figure 2.6	IEEE 24-Bus 20-Node IPGS and its most critical measurements.	35
Figure 2.7	FDIA vectors on measurements of IEEE 24-Bus system at Peak Load.	37
Figure 2.8	SCED solution in IEEE 24-Bus system affected by the designed attack vectors.	37
Figure 2.9	Effectiveness of the preventive defense strategies S1-S9.	40
Figure 2.10	Performance of the detection scheme on the 24-Bus-20-Node IPGS without the preventive measures (S0) and during different preventive defense strategies S1- S9 in Table 2.4.	42
Figure 2.11	IEEE 118-Bus 135-Node IPGS and its most critical measurements.	43
Figure 2.12	FDIA against the EMS of IEEE 118-Bus power system during the peak load (a) attack vector on measurements (b) output of SCED.	45
Figure 2.13	Performance of the detection scheme on the IEEE 118-Bus-135-Node IPGS for the different preventive strategies.	45
Figure 3.1	Overall PMU-enabled WADC scheme.	49
Figure 3.2	TSA impacts on PMUs data aggregation at PDC using relative time-alignment: (a) pre-attack condition, (b) post-attack condition I, (c) post-attack condition II.	51

Figure 3.3	Attack implementation steps.	54
Figure 3.4	The proposed preventive countermeasure.	59
Figure 3.5	Two-Area Kundur test system.	62
Figure 3.6	PMU-PDC data forwarding trees in Two-Area Kundur for Scenarios (a) S1, (b) S2, and (c) S3.	63
Figure 3.7	Post-attack dropout status of the critical PMUs u_3 and u_4 in Two-Area Kun- dur during Scenarios (a) S1: $\tau_c=40$ ms, (b) S2: $\tau_c=40$ ms, and (C) S3: $\tau_c=33$ ms or 40 ms	65
Figure 3.8	Post-attack Two-Area Kundur's WADC performance for generators (a) G1 and (b) G3.	66
Figure 3.9	IEEE 39-Bus test system.	66
Figure 3.10	(a) Targeted modes and (b) GMO of PMU measurements in IEEE 39-Bus. .	67
Figure 3.11	PMU-PDC data forwarding trees in IEEE 39-Bus for Scenarios (a) S1, (b) S2, and (c) S3.	68
Figure 3.12	Post-attack 39-bus WADC performance for Generators (a) G2, (b) G5, and (c) G9 during single TSA.	70
Figure 3.13	Post-attack 39-bus WADC performance for Generators (a) G2, (b) G5, and (c) G9 during multiple TSAs.	72
Figure 3.14	Sensitivity analysis of the presented TSA on IEEE 39-Bus: (a) blind attack, (b) optimal attack.	73
Figure 4.1	Threat model.	79
Figure 4.2	Attack surface.	80
Figure 4.3	TSA impacts on PMU data collection in RTA.	81
Figure 4.4	TSA impacts on PMU data collection in ATA.	83
Figure 4.5	Overall architecture of the proposed integrated TSA detection and mitigation scheme.	87
Figure 4.6	Architecture of the proposed deep CNN detection scheme.	88
Figure 4.7	Post-attack speed deviation of G3 in Case-I during (a) attack free scenario S0 and TSA scenarios (b) S1, (c) S2, (d) S3, and (e) S4.	98

Figure 4.8	TSA detection performance indices in Case-I.	98
Figure 4.9	Post-attack speed deviation of G3 in Case-I during (a) attack free scenario S0 and TSA scenarios (b) S1, (c) S2, (d) S3, and (e) S4.	100
Figure 4.10	Post-attack speed deviation of G2 in Case-II during attack free scenario S0 and TSA scenarios (b) S1, (c) S2, (d) S3, and (e) S4.	101
Figure 4.11	TSA detection performance indices in Case-II.	102
Figure 4.12	Eigenvalue analysis of observer error dynamic model in Case-II for various optimal TSAs (a) LQR, (b) SDDR [1], and (c) proposed observer.	104
Figure 4.13	Sample optimal TSA Events 1-5 and blind TSA Events 6-10 in Case-II: (a) location of TSAs, and (b) PMUs' dropout probability.	105
Figure 4.14	Estimation error of the observers in Case-II during (a) worst-case optimal TSA Event 4, (b) Optimal TSA Event 2, and (c) Blind TSA Events 7, 9, and 10. . .	107
Figure 4.15	Test Case-III: Simplified 14-Generator Model of the Southeastern Australian Power System.	108
Figure 4.16	Post-attack speed deviation of Generator TPS-5 in Case-III during attack free scenario (a) S0 and TSA scenarios (b) S2 and (c) S4.	109
Figure 4.17	TSA Detection Performance Indices in Case-III.	109
Figure 5.1	The overall scheme of LCL-type inverter and attack surface.	114
Figure 5.2	Diagram of LCL-type inverter under resonance FDIA.	115
Figure 5.3	Equivalent circuit of grid-connected LCL-type inverter.	117
Figure 5.4	Overview of applying a DWT on a chirp signal, its approximation and details levels.	121
Figure 5.5	Bode plots of output impedance of the inverter.	125
Figure 5.6	Resonance FDIA with frequency of 1500 Hz (a) Voltage at PCC and (b) inverter current.	126
Figure 5.7	Resonance FDIA with frequency of 3500 Hz (a) Voltage at PCC and (b) inverter current.	127
Figure 5.8	Resonance FDIA with frequency of 2500 Hz (a) Voltage at PCC and (b) inverter current.	128

Figure 5.9 Overview of applying a DWT on PCC's voltage signal during normal and attack conditions.	129
Figure 5.10 Two first levels of DWT of normal operation, step change, and attack. . . .	130
Figure 5.11 Results of various detection methods by using extracted features from DWT.	133
Figure 5.12 Results of various detection methods after improving in features extraction.	134
Figure 5.13 The performance of the wide neural networks optimized Bayesian optimizer.	135
Figure 5.14 Classification and hyperparameters error, as well as best point of hyperparameter for the proposed detection method.	135
Figure 5.15 Robust performance of proposed detection method across varying B-ratios. .	136

List of Tables

Table 2.1	Case Studies on 24-Bus 20-Node IPGS	35
Table 2.2	Injection Value to the Pipelines' Flow Measurements of 24-Bus 20-Node IPGS During Peak Load (MBtu/h)	37
Table 2.3	Post-attack System Results During Peak Load in Cases I-IV Where no De- fense Strategy is Performed.	38
Table 2.4	The Preventive Defense Strategies	39
Table 2.5	TP, FN, TN, and FP Parameter for the IEEE 24-Bus 20-Node IPGS	41
Table 2.6	FDIA on the Pipeline Flow Measurements of IEEE 118-Bus 135-Node IPGS During Peak Load and Consequent Outage of GFPPs	44
Table 2.7	TP, FN, TN, and FP Parameter for the IEEE 118-Bus 135-Node IPGS	45
Table 3.1	Expected PMU-PDC Delay in Two-Area Kundur (ms).	63
Table 3.2	Optimal Attack Vector in Two-Area Kundur	64
Table 3.3	Expected PMU-PDC Delay in IEEE 39-Bus (ms)	69
Table 3.4	Optimal Attack Vector in IEEE 39-Bus for Single TSA Condition	69
Table 3.5	Optimal Attack Vector in IEEE 39-Bus for Multiple TSA Condition	71
Table 3.6	Performance of AC State Estimation In IEEE 39-Bus	74
Table 4.1	TSA Detection Approaches in The Literature	78
Table 4.2	Optimal TSA Vectors in Case-I	97
Table 4.3	TSA Detection Performance in Case-I	98
Table 4.4	Optimal TSA Vectors in Case-II	100
Table 4.5	TSA Detection Performance in Case-II	102

Table 4.6	Detection Performance comparison with ANN-based Model in [2]	103
Table 4.7	Stabilization Time (T_s [s]) During The Optimal and Blind TSA Events. . . .	106
Table 4.8	Optimal TSA vectors in Case-III	108
Table 5.1	The poor performance of well-known machine learning models when used time-domain features.	119
Table 5.2	The Parameters of The Test Case Gird-Connected LCL-Type Inverter	124

Nomenclature

Sets and indices:

$\{i, j\} \in \Omega^b$ Buses

$g \in \Omega^g, d \in \Omega^d$ Targeted power plants and electrical loads

$l \in \Omega^l, \Omega^{TG} \subset \Omega^g$ Lines, targeted gas-fired power plants

$w \in \Omega^w, q \in \Omega^q$ Gas wells and gas loads

$n \in \Omega^n, p \in \Omega^p$ Gas nodes and pipelines

Λ Attackable subset of system

$k \in \Omega^k$ Pieces in linearization method

$c \in \Omega^C$ PDCs

$l \in \Omega^L$ Communication links

$u \in \Omega^U$ PMUs

$m \in \Omega^m$ Measurements of PMUs

$\omega \in \Omega^\omega$ Uncertainty scenarios of communication latency

Parameters:

A_{ig}, A_{id} Connection status of power plant g and electrical load d to bus i

A_{nw}, A_{np} Connection status of gas well w and pipeline p to gas node n

A_{ng}, A_{nq}	Connection status of power plant g and demand q to gas node n
B_{ij}, H_{li}	Bus to bus and line to bus admittance matrix
B_a^{PS}, B_a^{GN}	Adversary's capability to launch attack against the power system and the gas network
c_g, c_d^{sh}	Operational cost of power plant g and interruption cost of electrical load d [\$/100MWh]
c_w, c_q^{sh}	Operational cost of gas well w and interruption cost of gas demand q [\$/MBtu]
P_d, P_l^0	Pre-attack load d and power flow of line l [p.u]
$P_l^{\max}$	Maximum power flow of line l [p.u]
R_g^D, R_g^U	Ramp-rate up/down of power plant g [p.u/h]
$P_g^{\min}, P_g^{\max}$	Minimum/maximum power of power plant g [p.u]
τ_d, τ_q, τ^t	Maximum injection to measurements of electrical/gas loads and temperature
ψ_g, φ_q	Gas consumption rate of gas-fired power plant g [MBtu/100MWh] and gas demand q [MBtu]
$\theta^{\min}, \theta^{\max}$	Floor and cap of nodal gas pressure [bar]
$\Delta\varphi_p, \Delta\theta$	Pieces steps in linearization method for pipeline p and nodal pressure
A_{nl}, A_{ll}	Connection matrices of node-link and link-link
B^{max}	Maximum number of compromised PMUs
$D^{\max}$	Maximum negative timestamp manipulation of PMUs
M_{1-4}	Big values
T^s	Sampling time of PMUs
π_ω	Communication delay probability in Scenario ω
$\delta_{l\omega}$	Data transferring latency of Link l in Scenario ω

δ^{max} Latency requirement of WADC for data aggregation

Variables:

y_u Binary attack status of PMU u

$v_{uc\omega}$ Binary aggregation status of PMU u in the buffer of PDC c in Scenario ω

$\tau_{c\omega}^{trig}$ Buffer trigger time of PDC c in Scenario ω

$w_{uc\omega}$ Relative auxiliary buffer window of PDC c respecting PMU u in Scenario ω

α_u Timestamp manipulation of PMU u

$\delta_{uc\omega}$ Communication latency for data transferring from PMU u to PDC c in Scenario ω

P_g, P_d^{sh} Power generation of power plant g and power shedding of electrical load d [p.u]

u_g Power plant binary status (equal to 1 if power plant g is online)

u_p^a Fake leakage binary variable (equal to 1 if an fake leakage is portrayed at pipeline p)

δ_i Voltage angle of bus i [rad]

$\beta_{pk}^{pip}, \Omega_{pk}^{pip}, \Omega_{nk}^\theta$ Auxiliary binary variable in linearization method for pipeline p and pressure of node n

$\varphi_w, \varphi_q^{sh}$ Gas produced by gas well w and Gas shedding of load q [MBtu]

$\Omega_{pk}^{pip}, \Omega_{nk}^\theta$ Auxiliary binary variable in linearization method for pipeline p and pressure of node n

μ, λ Lagrangian coefficients of inequality and equality constraints

x_{luc} Binary deployment status of Link l for communication tree between PMU u and PDC c

τ_c^w Buffer waiting time of PDC c

Chapter 1

Introduction

Modern communities place a high priority on the safe and reliable operation of the power grid since the nation's economy, industry, social well-being, and other critical infrastructures all strongly rely on the sustainability of this energy delivery system. To enhance the overall power grid security and reliability, wide-area applications have opened up new opportunity for the operation, protection, and control of power systems with the combination of synchrophasor measurements, high-speed communication networks, and digital signal processing technologies [3].

Wide-area monitoring, protection, and control (WAMPAC) system is a set of technologies and applications, which centralises system-wide data to track, analyse, and estimate the steady-state and dynamic states of the power system and make appropriate protection and control decisions in a real-time manner. In the other hand, interconnection of the power grids and integration of inverter-based technologies across the entire grid have made WAMPAC as an essential tool for operation of modern power system [4]. To shed lights on this important tool in the modern power systems, this section aims to explain the architecture of WAMPAC systems by presenting the deployed cyber-physical layers and applications.

1.1 Cyber-physical Architecture of WAMPAC Systems

WAMPAC systems can be highlighted as the foundation of future power system, which enable more flexible and adaptive protection and control strategies to improve system reliability and

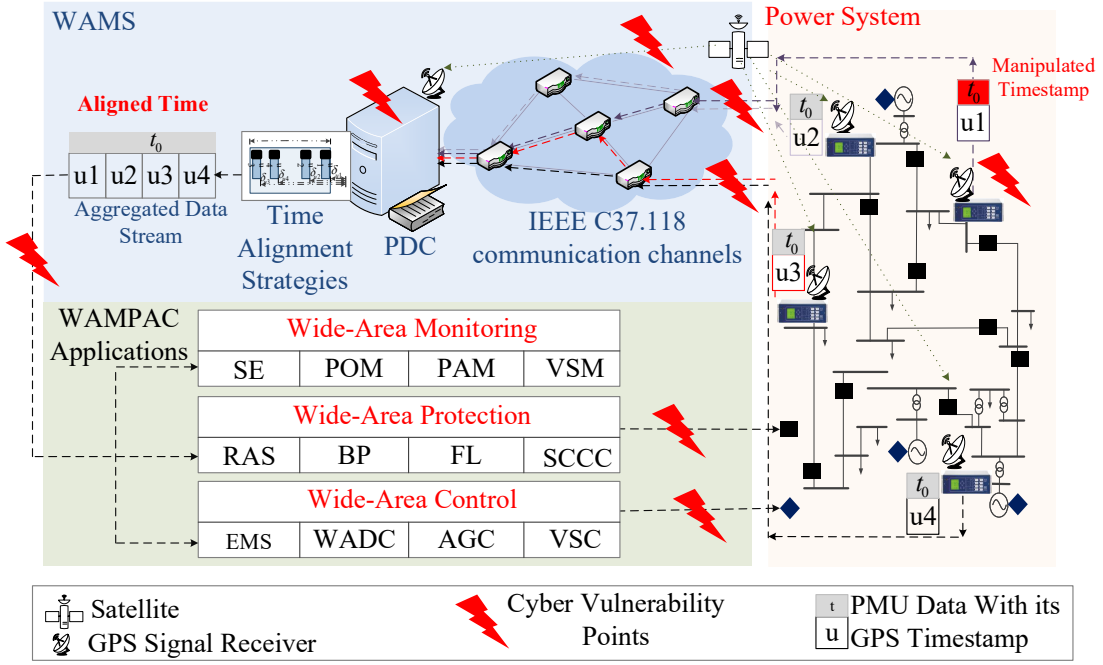


Figure 1.1: Overall structure of WAMPAC systems.

stability. WAMPAC systems utilize a set of system-wide and local information, aiming at counteracting the propagation of large-scale disturbance propagation and system blackout. Deployment of wide-area measurements in WAMPAC systems results in more efficient and reliable application of remedial measures for system-wide concerns. Meanwhile, since the operational data measured in entire physical layers and substations, they need to be time-synchronized before being used for monitoring, protection, and control purposes. As a result, time-synchronized measurement technology is a critical component of WAMPAC systems, which are provided by phasor measurement units (PMUs). PMUs measure real-time voltage and current phasor as well as frequency, which are synchronized with highly precision universal time reference provided by global positioning system (GPS). PMUs also enable high sampling rate up to 120 samples per second, which are suitable for real-time applications, in particular for those applications which require the highly accurate dynamic states of the power system [5].

A overall configuration of WAMPAC systems is shown in Fig. 1.1. Using wide-area measurement system (WAMS), the synchronized data is hierarchically transferred between PMUs and

super PDC via wide range of data communication protocols. PMUs provide system-wide time-synchronized measurement data and send it to phasor data concentrators (PDCs) through IEEE C37.118 communication channels [6]. PDCs collect the data based on their timestamp through time-alignment strategies outlined in IEEE Std C37.247-2019 [7]. Each utility in a WAMPAC system with several electrical lines, transformers, substations, and generators can have its own PDC. A super PDC can be also established to collect chosen synchronized operational data for the control center. Furthermore, all data collected in super PDC can be transferred to each power utility's PDC, enabling each power utility to comprehend the condition of the power grid outside its regional control area. The super PDC is linked to the control center, where WAMPAC applications will be executed directly based on the collected data [6].

1.1.1 Standards for Implementation of WAMPAC systems

Thanks to the development of standards dedicated to WAMPAC systems, wide-area applications have recently been deployed in real-world power systems. This section briefly reviews the technical standards developed regarding WAMPAC systems.

High availability and low latency are among key requirements for the communication architecture dedicated for WAMPAC system. To meet these requirements, the IEEE C37.118 standard is mostly utilized in wide-area measurement systems to transfer synchrophasor PMU data across the communication networks [8]. This standard elaborates on the synchrophasor PMU data format and requirements to transfer it. This standard has not adopted to deal with cyber-security concerns. Therefore, to address lack of security features in the IEEE C37.118 standard, IEC 61850-90-5 has been developed. The IEC 61850-90-5 standard describes the specifications and requirements for transmitting synchrophasor data based on IEEE C37.118 in accordance with IEC 61850 which is used in substation automation schemes. On the other hand, despite the fact that IEC 61850 and IEEE C37.118 were initially developed separately, they are now on the path to integration in accordance with IEC 61850-90-5. Thanks to this integration, data collection from PMUs in substations may be carried out in an integrated manner, which enables the sharing of synchrophasor measurements from PMUs (IEEE C37.118) under the information model and the exchange information model of IEC 61850. These allow faster communications to be sent across a wide-area network beyond the

substations for deployment of WAMPAC applications. Despite the benefits provided, commercially available device producers have not yet adopted this standard in very large numbers. In other words, because of the cost and complexity that adopting IEC 61850-90-5 imposes on the network, it is still difficult to incorporate it into existing power grids. Using the Hash-based Message Authentication Code, this standard verifies the authenticity of data. In a recent research, IEEE C37.118 and IEC 61850-90-5 were compared for features, capabilities, and attack resistance. IEC 61850-90-5 was shown to be more resilient to different cyber-attacks, including reconnaissance, authentication / access, replay / reflection, and denial of service, and Man-in-the-middle attack [8].

One of the important standards in wide-area measurement systems IEEE C37.244-2019, which provides the requirements for PMUs data stream aggregation at PDC level. The IEEE C37.244-2019 standard outlines the criteria for implementing PDC capability in WAMPAC systems, with a focus on synchronisation, synchrophasor data processing, and real-time access. This standard defines several time alignment strategies to aggregate the PMUs' data stream while guaranteeing the time-synchronization and latency requirements of WAMPAC applications [7].

1.2 WAMPAC Applications

As shown in Fig. 1.1, the collected synchronized operational data are utilized to execute WAMPAC applications to monitor the system in real-time and obtain the appropriate protection and control decisions. From functionality point of view, the applications of WAMPAC systems can be grouped into three categories, (i) wide-area monitoring applications, (ii) wide-area protection applications, and (iii) Wide-area control applications. The subsequent subsections explain the most common WAMPAC applications belonging to these three categories.

1.2.1 Wide-Area Monitoring Applications

Utilizing wide-area measurements for power system monitoring offers distinct insights into system operations, component statuses, and the grid's stability margin for operators. Furthermore, the data generated by these wide-area monitoring applications can be integrated into protective and control applications, or serve as alerts for the power system operator in emergency situations. The most

common wide-area monitoring applications are highlighted as follows:

- **State Estimation (SE):** One of the most significant online applications required for control applications and operational security awareness is power system SE. Based on available redundant measurements in the system, the estimator delivers the optimum solution of the system states (voltage angles and magnitudes) using the nonlinear least square approach [9]. In addition, since the measurements are exposed to the measuring device error, bad data detection scheme is also utilized to isolate the measurements with high residual error and ensure the accuracy of SE application. The SE performance can be affected by network observability, measurement precision, and redundancy levels [10].
- **Power oscillation monitoring (POM):** The electrical grid encounters various disturbances resulting in variations in voltage, frequency, power, and rotor angle, among other parameters. POM detects these oscillations as they offer vital information regarding the stability of the underlying system, its current modes, and the source of power system disturbances [11].
- **Phase Angle Monitoring (PAM):** PAM provides real-time access to the precise phase angle difference between any two buses. PAM provides for the early detection of possible issues on a local and regional scales. Despite its simplicity, PAM may help system operators in various real-time operational conditions to identify system stress [12].
- **Voltage stability monitoring (VSM):** Voltage stability incidents occur when the power system fails to maintain an appropriate voltage magnitude at substations due to inadequate reactive power support. The WAMPAC systems utilize the collected operational data to compute several instability indices, aiming at evaluating the system voltage stability state, detecting possible dangers, and warning control and protection applications. In case of voltage instability incidents, this application of WAMPAC may trigger the control applications to modify reactive power generation and retrieve voltage, and protective applications to undertake load shedding and enhance the voltage instability margin [13].

1.2.2 Wide-Area Protection Applications

The power system disturbance cascades gradually, while, depending on the type of disruptive incident, the time scale between initial outage/fault to system collapse can vary from several minutes to milliseconds. In all circumstances, it is crucial to classify and localize the disturbance and make actions to prevent incident propagation by isolating the disturbance and ensure a secure system recovery. WAMPAC systems supported by high-speed communication networks and synchrophasor data empower power system to more effectively deal with large-scale disturbances by implementing sophisticated protection logic. WAMPAC systems is also equipped with computer-based and internet of things (IoT) relays which help the system operator to develop communication-assisted wide-area protection schemes using various protocols, e.g., IEC 61850.

- **Remedial action scheme (RAS):** This application aims to promptly and automatically address identified abnormalities through corrective measures, e.g., shedding loads/generators, rescheduling generation, and tripping lines. The implementation of these measures minimize the impact of faults, avert cascading events, and ensure the reliable operation of the power system [14].
- **Backup protection (BP):** In content of protection coordination, different protection zones are intentionally designed to overlap, with some relays acting as backups to ensure no fault goes unnoticed. However, in real-world systems, due to conditions of operation with less stress, such a local backup protection system may trigger incorrectly. Consequently, comprehensive backup protection schemes, which leverage PMU data and facilitate communication between the relays/control centers, can be implemented. This application ensures swift fault resolution and offers backup protection for crucial sections of the system in the event of any relay malfunction [15].
- **Fault localization (FL):** This application leverages PMU data to precisely localize the fault in long-distance transmission lines. Accurately pinpointing the fault's location is highly crucial, as it allows the power system operator to promptly address or replace the problematic components and restore the line to regular operation [16].

- **Short circuit current calculation (SCCC):** As the configuration of the power system may change, this application provides the rapid calculation of the short circuit current in accordance with the changes power system configuration. This application also facilitates the corresponding modification of relay settings [17].

1.2.3 Wide-Area Control Applications

Given that PMUs support high-sampling rate measuring, the control center is able to monitor the dynamic behaviour of power systems and identify the wide-area oscillation patterns. On this basis, wide-area control applications are employed to make a wide-area close loop control system aiming at operating the system economically, improving the system stability performance by damping the post-contingency oscillations, and maintaining the system voltage and frequency within acceptable range. The most privileged wide-area control applications are further elaborated as follows:

- **Energy management system (EMS):** This application is a sophisticated software suite that monitors, controls, and optimizes the operation of an electrical grid over a large geographic area. It integrates real-time data from various PMUs to issue optimal control command via various sub-applications, e.g., security constrained economic dispatch (SCED), optimal power flow (OPF), and generation rescheduling. This application mainly optimizes the economic dispatch while ensuring that the grid operates securely under various contingencies [18].
- **Wide-Area Damping Controller (WADC):** The occurrence of dominant low-damping oscillations can jeopardize the reliability and stability of modern power systems [19]. To alleviate the detrimental impacts of these oscillations, wide-area damping controllers (WADCs) have been widely utilized. WADCs in control center provide appropriate control signals to power system actuators, e.g., synchronous generators, static VAR compensators (SVCs), and flexible alternating current transmission system (FACTS) technologies to effectively damp the observed wide-area oscillations [20].
- **Automatic generation control (AGC):** This application is a control system used to regulate

and maintain the nominal frequency of the system and the power interchange with neighboring systems within acceptable limits. AGC achieves this by adjusting the power output of generators in real-time based on the deviation of system frequency from its nominal value. This helps in maintaining the balance between generation and load and ensures the stability of the power grid [21].

- **Voltage stability control (VSC):** Voltage stability is a critical issue in many power outages worldwide, often stemming from an overloaded system and a deficiency of generated reactive power, leading to notably low voltage levels. By leveraging PMU data and calculating proximity indicators to the stability threshold, the wide-area controller of the power network can identify the risk of this stability concern. Consequently, adjustments can be made to the reactive power output of synchronous generators or FACTS equipment, based on the gathered data, thus guaranteeing voltage stability within the system [22].

1.3 Scope of the Work

As shown in Fig. 1.1, PMU, PDC, and IEEE C37.118 communication channels are key components of WAMPAC systems. However, the real-world incidents, e.g., [23, 24], and experimental experiences, e.g., [12], have demonstrated that all these components are vulnerable to cyber attacks, which put the entire power grid at risk. PMUs rely on accurate time synchronization, making them susceptible to time synchronization attacks (TSAs) [25]. Additionally, their communication links to the PDC can be potential points of entry for cyber threats. Furthermore, the internal firmware of PMUs must be secure to prevent unauthorized access or tampering [25]. The communication channels connecting the PDC lack encryption, leaving them open to various security risks. Within the PDC system, several vulnerabilities can give rise to potential issues. These encompass the possibility of unnecessary traffic flow through network interfaces, excessive privileges granted to the PDC, making unauthorized alterations difficult to detect, and allowing straightforward access to the configuration and programming software of PDCs [26]. These weaknesses have the potential to empower an insider to compromise or misconfigure the PDC, leading to an incomplete transmission of measurement data up the WAMPAC applications [26]. The prevailing communication protocol in

WAMPAC systems is IEEE C37.118, widely adopted for its compatibility and efficiency. However, it lacks inherent security features or robust transmission protocols, rendering it vulnerable to an array of cyber threats. These encompass potential risks like IP spoofing, packet interception, unauthorized data injection, overwhelming data buffer, exploit of buffer limits, Denial-of-Service (DoS) attacks, reconnaissance maneuvers, breaches in authentication/access, Man-in-the-Middle (MITM), false data injection attacks (FDIAs), and replay attacks [27]. For example, network infrastructure elements such as routers and switches could be manipulated to interfere with critical measurements used in protection and control algorithms or to distort commands destined for PMUs or PDCs [27].

The vulnerabilities in the cyber realm pose a significant threat to the functionality of WAMPAC applications. These cyber vulnerabilities can have far-reaching consequences, ranging from substantial financial losses to the potential for system instability and large-scale outages. It's worth noting that the unique characteristics of WAMPAC applications, including their input-output structures, configurations, and algorithms, may necessitate distinct approaches for prevention, detection, and mitigation tailored to each application. Therefore, this research primarily focuses on the cyber vulnerabilities within two critical wide-area control applications, i.e., EMS and WADC. The subsequent chapter will delve deeper into the vulnerabilities specific to each application, outlining potential cyber attack scenarios, and proposing a comprehensive set of measures for prevention, detection, and mitigation.

1.4 Research Contributions

This research takes a bold step towards improving the security of society and industry by reinforcing WAMPAC systems which are the backbone of future power grids against various stealthy cyber-threats. The society and general public are beneficiaries of the outcomes of this research, which directly or indirectly are in line with four sustainable development goals (SDGs), i.e., sustainable cities and communities, affordable and clean energy, climate action, and decent work and economic growth. Cyber-resilient WAMPAC systems guarantee the sustainability of electric energy which is needed to construct sustainable cities and communities. They also enable large-scale integration of clean energy sources by improving the situational awareness of the system operator,

which boosts affordable and clean energy and climate action goals. Furthermore, secure WAMPAC systems pave the way for the economic growth by diminishing the probability of large-scale black-outs and reducing the economic losses caused by unreliable electricity. This research also benefits the electric utilities and operators, e.g., Hydro-Québec and Independent Electricity System Operator, as well as manufacturers of IoT devices deployed in WAMPAC by providing comprehensive guidelines as well as effective prevention, detection, and mitigations tools to respond against malicious cyber threats. Furthermore, various interdisciplinary researchers in fields of energy, control of industrial process, and cyber security will benefit from outcomes on this research through knowledge and technology transfer to build a resilient society. The findings of this research have been published in top conference and journals as highlighted in the following:

- Masoud Zadsar, Ahmadreza Abazari, Mohsen Ghafouri, Jun Yan, "*Prevention and Detection of Coordinated False Data Injection Attacks on Integrated Power and Gas Systems*", **IEEE Transactions on Power Systems**, vol. 38, no. 5, pp. 4252-4268, 2022.
- Masoud Zadsar, Mohsen Ghafouri, Amir Ameli, Bassam Mousa, "*Preventing Time-Synchronization Attacks on Synchrophasor Measurements of Wide-Area Damping Controllers*", **IEEE Transactions on Instrumentation & Measurement**, vol. 72, pp. 1-14, 2023.
- Masoud Zadsar, Mohsen Ghafouri, Amir Ameli, Bassam Mousa, "*Integrated Deep Learning-Based Detection and Robust State Observer Mitigation of Time-synchronization Attacks: A WADC Case Study*", **IEEE Transactions on Smart Grid**, Early Access, pp. 1-14, 2024.
- Masoud Zadsar, Masoud Babaei, Mohsen Ghafouri, and Amir Ameli, "*Wavelet-Enabled Data-Driven Approach for Detection of Resonance Attack on Inverter-based Resources*", **IEEE Transaction of Industrial Application**, Under Preparation.
- M. Zadsar, A. Abazari, M. Ansari, M. Ghafouri, S. Muyeen, and F. Blaabjerg, "*Central Situational Awareness System for Resiliency Enhancement of Integrated Energy Systems*", in **2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON)**. IEEE, 2021, pp. 1–6.

- M. Zadsar, M. Ghafouri, A. Ameli, and B. Moussa, “*Time-synchronization Attack on Data Aggregation in Wide-area Damping Controllers*”, in **2022 IEEE Electrical Power and Energy Conference (EPEC)**. IEEE, 2022, pp. 368–373.
- M. Zadsar, M. Ghafouri, and A. Ameli, “*Cyber Attack-Aware Security Hardening of Time Synchronization Technologies in WAMPAC Systems*,” in **2023 IEEE 2nd Industrial Electronics Society Annual On-Line Conference (ONCON)**. IEEE, 2023, pp. 1–5.
- M. Zadsar, M. Babaei, M. Ghafouri, and A. Ameli, “*Cyber Induced Harmonic Instability of Inverter-Based Renewable Generators*,” in **24 IEEEIC International Conference on Environment and Electrical Engineering**. IEEE, 2024, pp. 1–5.

This research was also recognized by Fonds de recherche du Québec as the second-ranked research project in the field of energy in Quebec during 2022-2023 competition.

Chapter 2

Security Enhancement of EMS

2.1 Problem Statement

The extensive deployment of gas-fired power plants (GFPPs) in power systems escalates the interdependencies between smart grids and gas networks (GNs) [28]. Such a strong interdependency enhances the operation flexibility and the reliability of resultant integrated power and gas systems (IPGSs) [29]. To operate an IPGS in a reliable and efficient manner, fast and accurate transfer of data through information and communication technologies (ICTs) is required [30]. This improved reliability and efficiency, however, is achieved at the expense of exposing IPGSs to various threats emanating from the cyber space [31–33]. For instance, cyber-attacks against the supervisory control and data acquisition (SCADA) system of the Ukrainian power grid in 2015 [23] and U.S. pipeline firms in 2018 [34] are examples of such cyber threats, which resulted in prolonged service interruptions for thousands of customers. As a result, identifying potential cyber-attacks, analyzing their possible impacts, and developing effective defense strategies against them are crucial for IPGSs.

2.2 Literature Review and Research Gaps

Among various cyber threats against energy infrastructure, false data injection attacks (FDIAs) have received significant attention due to their complex nature and severe implications [35]. Not only do FDIAs falsify the observability of a system by concealing/portraying changes in the system

behaviors, but also they mislead operators into making wrong decisions [36]. So far, a significant number of studies have been dedicated to devising FDIAs and defending against them. The aim of the first category is to reveal system vulnerabilities and investigate the ability of adversaries to craft successful FDIAs, while bypassing bad data detection (BDD) mechanisms. For instance, the authors of [37] have developed an FDIA against SE by manipulating the network parameters and measurements with a reduced number of attack points. The proposed model in [38] enables an adversary to retrieve the parameters of a system by eavesdropping phasor measurement units and construct attack vectors. In [39], an FDIA is developed to mislead the operator into identifying a wrong grid topology. Additionally, a family of coordinated cyber-physical attacks is developed in [40,41] to create cascading outages by physically disconnecting transmission lines and masking it by FDIAs. The second category of studies is focused on detecting and mitigating FDIAs [13,42–48]. For instance, a graph-based approach is proposed in [42] to detect FDIAs against AC SE. Using interdependencies between components, the authors of [43] have developed a preventive defense strategy against the FDIAs that result in cascading outages. To defend against FDIAs on smart grids, the authors of [13] have developed detection and mitigation strategies for FDIAs that target the voltage stability of the grid. The authors of [44] and [45] leverage machine-learning-based approaches to identify and localize falsified data. To improve the performance of SE under FDIAs, two model-based approaches, i.e., extended Kalman filter and k -smallest residual similarity, have been proposed in [46] and [47], respectively. To defend against FDIAs, data packet encryption strategies are deployed in [48] to secure the communication between measurement devices and the EMS. In addition, three new SE methods are proposed in [10,49,50] to facilitate distinguishing between normal and portrayed topology changes in large-scale power systems. Although all these studies are effective in defending against FDIAs, they only focus on power systems and overlook the interdependencies between power and natural gas networks. In fact, all these studies ignore the propagation of cyber-attacks from power systems to GNs, and vice versa. This issue, however, is of paramount importance as proved by the 2021 Texas blackout, in which a disturbance in the GN propagated in the entire IPGS [51].

Despite the significance of IPGSs' cyber-security, a limited number of studies, e.g., [52–54],

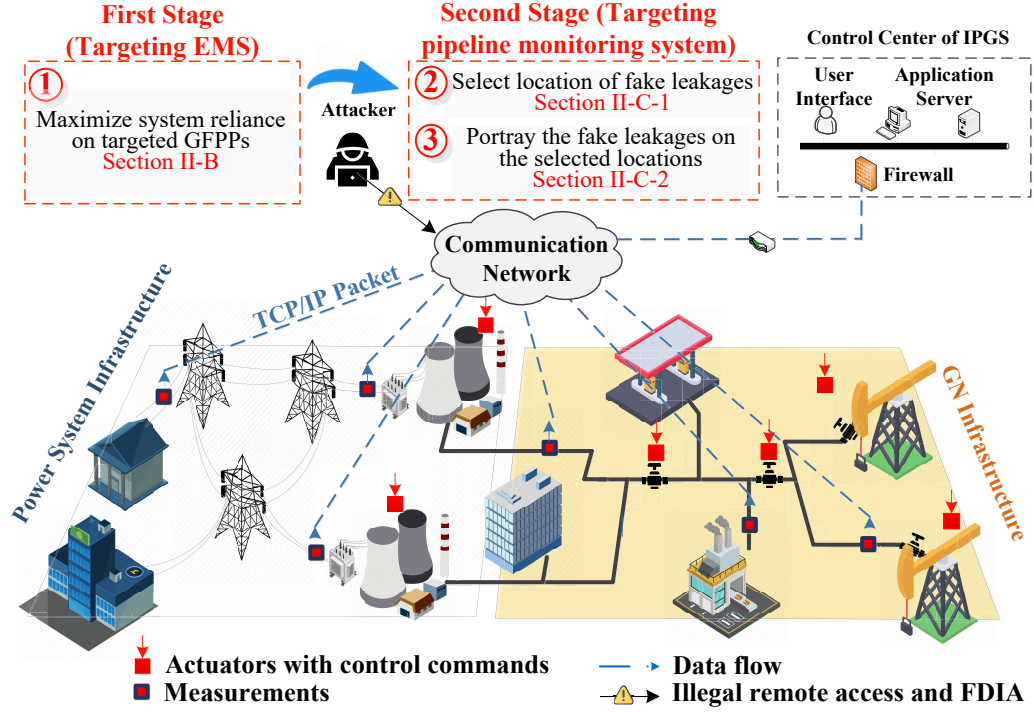


Figure 2.1: The proposed attack model against IPGS.

have been published on this topic. In [52, 53], risk mitigation frameworks are proposed considering operational data violation caused by FDIAs on electrical and gas measurements, as well as the uncertainties of renewable energy sources. The authors of [54] developed a data-driven attack detection scheme that identifies falsified data of power-to-gas facilities. Although these studies sparked off a new research direction to build more-resilient IPGSs against FDIAs, they (i) are developed based on simple attack models that can be detected by the currently-deployed monitoring systems, (ii) overlook the ability of adversaries to coordinate FDIAs against both power systems and GNs, and (iii) do not propose any solution (i.e., preventive defense strategies or online detection mechanisms) for coordinated FDIAs against IPGSs. Thus, a comprehensive research work that studies the cyber vulnerability of IPGSs and develops effective countermeasures against coordinated FDIAs is still missing in the literature.

2.3 Attack Model

This section presents the attack model developed in this thesis by elaborating on the cyber-physical model of IPGSs, attackers' objective and the procedure for launching the proposed FDIA, and the mathematical formulation for constructing stealthy attack vectors.

2.3.1 Cyber Vulnerabilities of IPGSs

A typical cyber-physical model of IPGSs is shown in Fig 2.1. To operate an IPGS efficiently and securely, operational data are needed to be gathered from physical layers and monitored in real-time. To this aim, modern IPGSs utilize an SCADA system to transmit operational data from measurements to control center, and send control signals to actuators. The control center uses the received data to monitor, control, and protect the system through various modules preserved in applications server.

One of the important online monitoring modules in control center of IPGSs is leakage detection, whose necessity is emphasized by the gas industry regulators in several countries, e.g., American Petroleum Institute and International Organization for Standardization in the U.S. [55]. The commonly-used leakage detection module in gas industries are developed based on volume/mass balance method [55]. In this method, the leakage detection module localizes the gas leakage by comparing the measured inlet and outlet gas flow across pipelines. When the leakage detection module is triggered, the system operator isolates the corresponding pipeline by sending shut-off command to the controllable valves through the SCADA system. Since the pipeline network is mostly buried underground, this attack could remain hidden until the repair crew are dispatched, and consequently can impose a high cost on IPGSs.

Since the leakage detection module of pipeline monitoring system relies on SCADA infrastructure, it can be targeted by adversaries to intentionally disconnect critical pipelines for malicious purposes. Cyber attacks against pipeline monitoring system can affect the operation of power systems due to deployment of GFPPs in power networks. On this basis, this thesis develops a two-stage attack model on IPGSs (Fig. 2.1). In the first stage of the attack, an adversary launches an FDIA against the EMS to increase the reliance of the system on targeted GFPPs. Afterward, in the second

stage, the main attack on leakage detection module is launched, aiming at disrupting the supply of gas fuel of the GFPPs. It should be mentioned that the only goal of the first stage is to intensify the impacts of the second stage. For example, if for an operating point GFPPs lightly participate in supplying the demand, targeting the gas network during does not significantly impact the electric grid, and might not achieve the attackers' goals. As a result, the second stage must be complimented with the first stage of the attack to increase the participation of target GFPPs to the desired level.

To perform the two stages of the proposed coordinated FDIAs, the measurements of gas and power networks are targeted. Due to deployment of firewalls and other security mechanisms in the control center of IPGSs, attacking directly on the EMS and the leakage detection module of pipeline monitoring system might be practically difficult [56]. However, manipulating the measurements of these two systems is more feasible due to deployment of Mod-bus, DNP3, and TCP/IP communication protocols for gathering the measurements, and the vulnerabilities of these protocols to cyber-attacks [57]. Additionally, the security mechanisms implemented for securing measurement devices is lighter than the ones used in control centers [56]. To perform the proposed coordinated FDIAs in this thesis, adversaries should first penetrate into the SCADA network to gather the required information. For instance, an attacker with insider-level access can use virtual private network (VPN) to access SCADA devices and measurements. Additionally, eavesdropping the data is another way of gathering information, which is easier to implement when wireless communication is used [58]. Once the adversaries succeed to access the SCADA network and learn data exchange protocols and TCP/IP packet format, they can launch Man-In-The-Middle (MITM) attack, which is a type of FDIA [59]. In this attack, the adversaries interrupt an existing data transfer between the control center and measurement devices, and make them believe they are talking directly to each other. Additionally, compromising measurement devices, e.g., by malware contamination, is another alternative to tamper with the authentic measurements.

2.3.2 First stage: FDIA on EMS

This subsection mathematically models the first stage of coordinated FDIAs against IPGSs, and shows how stealthy attack vectors can be constructed against EMS to intensify the attack severity by increasing the reliance of the system on GFPPs. As Fig. 2.2 shows, the EMS runs SE by using

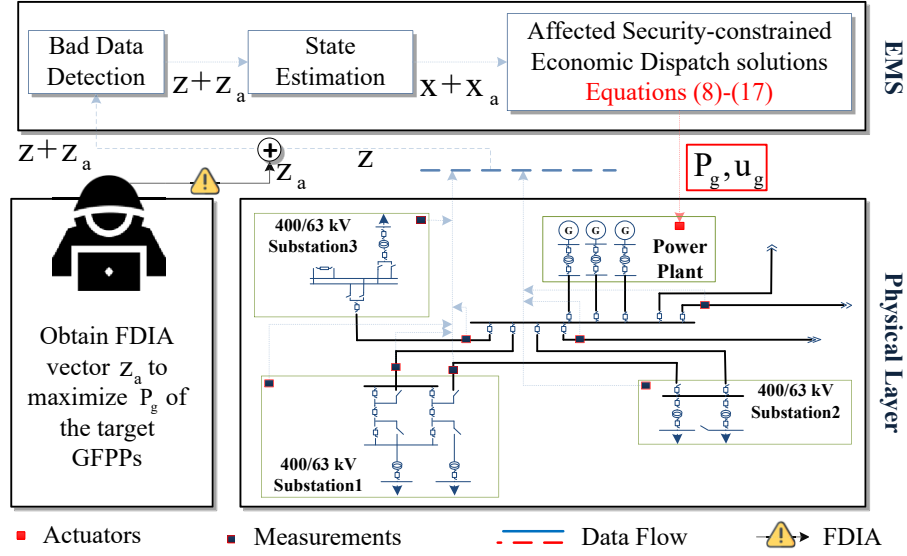


Figure 2.2: FDIA against the EMS in power networks.

the measurement vector z to derive grid's states x , and accordingly, determines the optimal power (i.e., P_g) and on/off status (i.e., binary variable u_g) of generating units using the security-constraints economic dispatch (SCED) module. In addition, the EMS deploys the BDD mechanism to identify and eliminate the abnormal measured data before they are used by the SCED module.

The attack vector z_a must be designed through an optimization problem with respect to the attacker's capability to increase the generation of targeted GFPPs, while bypassing BDD mechanism. Meanwhile, because the adversary can not directly manipulate the power of GFPPs, designing an attack vector is subjected to the solution of the SCED problem. Therefore, to construct the attack vector, this thesis proposes a bi-level optimization problem, in which the attacker level, i.e., (2.1)-(2.7), represents the objective function and constraints from the adversary's point of view, while the operator level, i.e., (2.8)-(2.17), are associated with the SCED problem. The attacker's objective function is to maximize the power generation of the targeted GFPPs, as follows:

$$\underset{z_a := \{z_{a|d}, z_{a|l}\}}{\text{maximize}} \quad \sum_{g \in \Omega^{TG}} P_g(z_a) \quad (2.1)$$

This optimization problem is subjected to constraints (2.2)-(2.7). Constraint (2.2) represents the

attacker's ability limitation, where $u_{a|l}$ and $u_{a|d}$ are binary variables that indicate whether the measurements of line l and load d are compromised (equal to 1) or not (equal to 0), respectively.

$$\sum_{l \in \Lambda^l} u_{a|l} + \sum_{d \in \Lambda^d} u_{a|d} \leq B_a^{PS} \quad (2.2)$$

The second constraint of the attacker-level problem is associated with bypassing the BDD mechanism. To construct a stealthily attack vector, the adversary must first bypass the BDD mechanism, as shown in Fig. 2.2. It is worth noting that although most real-world EMSs use AC SE, this thesis—for the sake of simplicity and conveying the main remarks more clearly—leverages the DC SE for constructing the attack vector. This assumption, however, results in an acceptable error from the adversary's point of view since this thesis deals with transmission systems in the steady-state—where the conditions of DC SE and power flow, e.g., high X/R ratio, voltage magnitudes of 1 p.u., and small phase angles for all busses, are often met. The acceptable error of DC SE is also proven in [9] using several case studies. In DC SE, the states are the voltage angles of all buses, and the measurement vector is the real power injections of all load buses and real power flows of all lines. As proven in [60] and [52], the adversary can bypass the BDD mechanism of DC SE if the following equation is met:

$$\left[\mathbf{H}(\mathbf{H}^T \mathbf{H})^{-1} \mathbf{H}^T - \mathbf{I} \right] \mathbf{z}_a = 0 \quad (2.3)$$

where $\mathbf{z}_a$ and $\mathbf{H}$ denote the injected vector and system Jacobian matrix, respectively. If a higher accuracy is needed, (2.3) should be replaced with corresponding residual error of the AC model. As such, the Jacobian matrix H is no longer linear and a linearization techniques must be adopted. More details can be found in [61]. Constraint (2.3) also guarantees that the zero-injection buses remain unchanged after FDIA. The next attacker-level constraints denote the range in which the measurements can be manipulated to keep the attack stealthy:

$$-P_l^{\max} \leq P_l^0 + z_{a|l} \leq P_l^{\max} \quad \forall l \in \Lambda^l \quad (2.4)$$

$$-u_{a|l} M \leq z_{a|l} \leq u_{a|l} M \quad \forall l \in \Lambda^l \quad (2.5)$$

$$-\tau_d u_{a|d} P_d \leq z_{a|d} \leq \tau_d u_{a|d} P_d \quad \forall d \in \Lambda^d \quad (2.6)$$

in which, subscripts d and l denote power system loads and lines, respectively. Accordingly, subscripts $a|d$ and $a|l$ signify the attack sub-vectors associated with power measurements of loads and lines, respectively. As a result, $z_{a|l}$ and $z_{a|d}$ are injected values to the measurements of line l and load d [62]. Additionally, sets Λ^d and Λ^l indicate loads and lines whose measurements are attackable, respectively. In this thesis, set Λ^d includes all loads, while set Λ^l contains all lines except for those whose measurements are obtained inside power plants. The reason for this exception is that power plants are often highly secure and are difficult to be attacked [52]. Finally, the last attacker-level constraints ensures that the sum of the injected values into the load measurements remains equal to zero:

$$\sum_{d \in \Lambda^d} z_{a|d} = 0 \quad (2.7)$$

This constraint also helps to keep the attack stealthy [52].

In the attacker-level optimization problem of (2.1), generators' power $P_g(z_a)$ is a subset of the operator decision $\mathbf{X}_o$, which will be obtained in the operator-level problem described in (2.8)-(2.17). This level runs the SCED from the operator's perspective to dispatch power plants. Given that DC power flow model is adopted in most EMS software packages [63], this thesis also utilizes the DC SCED. The objective function of the DC SCED in a IPGS can be formulated as an operation cost minimization problem, as follows:

$$P_g(z_a) \in \arg\{\underset{\mathbf{X}_o}{\text{minimize}} \underbrace{\sum_{g \in \Omega^g} c_g P_g + \sum_{d \in \Omega^d} c_d^{sh} P_d^{sh} + \sum_{w \in \Omega^w} c_w \varphi_w + \sum_{q \in \Omega^q} c_q^{sh} \varphi_q^{sh}}_{f_{SCED}}\} \quad (2.8)$$

where, f_{SCED} signifies the objective function of SCED problem whose first and second terms, respectively, denote the operation costs of non-GFPPs (c_g is one for non-GFPPs, and is zero for GFPPs) and electrical load shedding costs; the third term represents the production costs of gas wells;

and the last term indicates the gas load shedding costs. This objective function is subjected to the SCED's constraints, i.e., (2.9)-(2.17). Constraints (2.9)-(2.12) denote ramp-up/-down constraints of power plants, as well as the feasible range for the generation of power plants, power through lines, and load shedding, respectively.

$$-u_g(R_g^D - P_g^0) \leq P_g \leq u_g(R_g^U + P_g^0) \quad \forall g \in \Omega^g \quad (2.9)$$

$$u_g P_g^{\min} \leq P_g \leq u_g P_g^{\max} \quad \forall g \in \Omega^g \quad (2.10)$$

$$-P_l^{\max} \leq \sum_{i \in \Omega^b} H_{li} \delta_i \leq P_l^{\max} \quad \forall l \in \Omega^l \quad (2.11)$$

$$0 \leq P_d^{sh} \leq P_d \quad \forall d \in \Omega^d \quad (2.12)$$

Moreover, (2.13) represents the power balance for each bus:

$$\begin{aligned} \sum_{g \in \Omega^g} A_{ig} P_g &= \sum_{j \in \Omega^b} B_{ij} \delta_j \\ &+ \sum_{d \in \Omega^d} A_{id} (P_d - P_d^{sh} + z_{a|d}) \quad \forall i \in \Omega^b \end{aligned} \quad (2.13)$$

In addition to power network constraints, the constraints of the GN should be considered as well.

The first constraint is associated with the gas flow of pipelines, which can be formulated as

$$\varphi_p^{pip} |\varphi_p^{pip}| = \left(\frac{\pi}{4}\right)^2 \frac{D_p^5}{Y_p F_p T_p R Z \rho_0^2} \sum_{n \in \Omega^n} A_{np} \left(\theta_n^{nod}\right)^2 \quad (2.14)$$

where φ_p^{pip} and θ_n^{node} present the gas flow through Pipeline p and gas pressure of Node n ; D_p , Y_p , F_p , and T_p signify diameter, length, fraction coefficient, and temperature of Pipeline p ; and R , Z , and ρ_0 refer to the specific gas constant, compressibility factor, and gas density in the standard condition, respectively. Constraint (2.14) is known as Weymouth equation, which is derived from

two isothermal differential equations, i.e., continuity and momentum [64]. To guarantee the global optimality of solution, the non-linear terms of (2.14), i.e., $\varphi_p^{pip} |\varphi_p^{pip}|$ and $(\theta_n^{nod})^2$, are linearized by deployment of piecewise linearization approach explained in Section 2.3.4. The second constraint of the GN represents the allowed range of nodal pressures, as follows:

$$\theta^{\min} \leq \theta_n^{nod} \leq \theta^{\max} \quad \forall n \in \Omega^n \quad (2.15)$$

Additionally, the feasible shedding range for gas loads is represented by the following constraint

$$0 \leq \varphi_q^{sh} \leq \varphi_q \quad \forall q \in \Omega^q \quad (2.16)$$

Eventually, (2.17) represents the nodal gas balance constraint:

$$\begin{aligned} \sum_{w \in \Omega^w} A_{nw} \varphi_w &= \sum_{p \in \Omega^p} \sum_{k \in \Omega^k} A_{np} \delta_{pk}^{pip} + \sum_{g \in \Omega^g} A_{ng} \psi_g P_g \\ &+ \sum_{q \in \Omega^q} A_{nq} (\varphi_q - \varphi_q^{sh}) \quad \forall n \in \Omega^n \end{aligned} \quad (2.17)$$

The developed bi-level optimization problem (2.1)-(2.17) is solved by recasting the operator level with corresponding KKT conditions as elaborated in Section 2.3.4. In the rest of the section, the parameters that are determined in the first stage are denoted by symbol “ $\hat{\cdot}$ ”.

2.3.3 Second stage: FDIA on pipeline monitoring system

This subsection models the second stage of the proposed attack model, where an FDIA on gas measurements maliciously trigger leakage detection module of pipeline monitoring system. As Fig. 2.3 illustrates, this module detects leakages from pipelines by calculating the following indicator [55]:

$$|\varphi_p^{in} - \varphi_p^{out}| \geq \varepsilon_L \hat{\varphi}_p^{pip} \quad (2.18)$$

where φ_p^{in} , φ_p^{out} denote the inlet and outlet flow measurements received through the SCADA system, and $\hat{\varphi}_p^{pip}$ is the average value of inlet and outlet flows of pipeline p . Additionally, $\varepsilon_L = a_f + 0.3(a_{c2} + 5a_p)$ is the leakage detection threshold, which accounts for (i) uncertainties of the natural gas transient

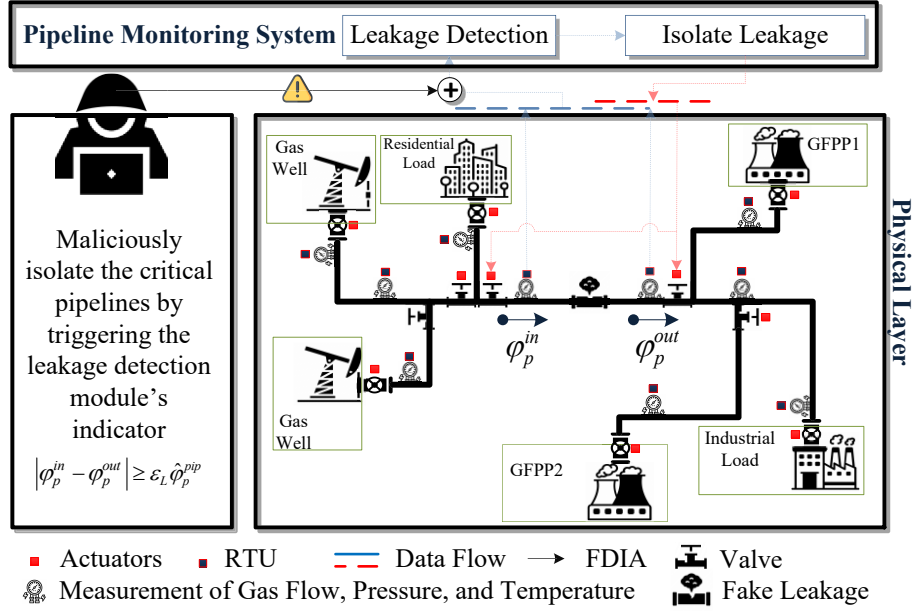


Figure 2.3: FDIA against pipelines monitoring system.

in pipelines ($a_{c,2}$), (ii) packing effect (a_p), and (iii) measurement error (a_f) [55]. In practice, this threshold is often about 4% [55]. If the indicator's condition is met for any pipeline, that pipeline is shut off by sending a command to its controllable valves through the SCADA. Thus, if an attacker manipulates the measurements of the GN such that the leakage detection modules of target pipelines detect a leakage, while the GN equations are met, those pipelines are shut off and the supply of gas to certain loads are disrupted. To perform this attack, first the adversary should determine the location of fake leakage(s), and then manipulate the measurements to portray them while satisfying the gas flow equations of the GN to bypass BDD module in GN. The two steps of the second stage are shown in Fig. 2.1 by ② and ③, respectively.

Determining the Location of Fake Leakage(s): In this sub-section, the adversary aims to find the best location of fake leakage(s) ($u_p^a = 1$) to maximize the disruption of GFPPs. Since the pipeline monitoring system shuts off the pipelines if it detects that they are leaking, this attack can significantly change the operating point and parameters of the GN. If, as a result of the attack, the GN becomes unable to supply all the loads and/or satisfy the operational constraints, load shedding schemes must be run by the operator to save the entire network from collapse, and/or to satisfy the operational constraint of the grid. Thus, the adversary should include the operator's decision making

process in his/her optimization while selecting the location of the fake leakage(s). As a result, determining the location of fake leakage(s) must be modeled as a bi-level optimization, where the upper-level denotes the attacker's objective function and constraints, and the lower-level expresses the IPGS operator's decision making and constraints. The objective function of the attacker-level problem (2.19) is to maximize the disruption of GFPPs, as shown below

$$\underset{u_p^a}{\text{maximize}} \quad \sum_{g \in \Omega^{TG}} (1 - u_g(u_p^a)) \hat{P}_g \quad (2.19)$$

In this equation, $\hat{P}_g$ denotes the redispatched power of generating unit g after launching the FDIA of the first stage, and is a constant value. In fact, in this equation, $\hat{P}_g$ is used as a weighting factor to determine the fake leakage(s) that disrupts the supply of gas to GFPPs with the largest power output. The attacker's objective function, i.e., (2.19) is subjected to the attacker's capability and limitations for portraying fake leakages, which is formulated by the following equation:

$$\sum_{p \in \Lambda^p} u_p^a \leq B_a^{GN} \quad (2.20)$$

In the attacker's level, u_g is the operator's decision variable, which should be determined in the operator's level using the following objective function

$$u_g(u_p^a) \in \arg\{\underset{\mathbf{x}_o}{\text{minimize}} \quad f_{SCED}\} \quad (2.21)$$

where f_{SCED} was defined in (2.8). In fact, this level models the reaction of the operator in response to fake leakage(s). The optimization problem of (2.32) should be solved subject to the operational constraints of the IPGS (i.e., (2.9)-(2.17)), as well as the following constraint

$$-(1 - u_p^a)M \leq \varphi_p^{pip} \leq (1 - u_p^a)M \quad \forall p \in \Lambda^p \quad (2.22)$$

which indicates that the gas flow of targeted pipelines is zero. In this equation, subscripts p refer to pipelines, and set Λ^p indicate attackable pipelines of the gas network except for those whose

measurements are obtained inside gas wells and gas-fired power plants. The reason for this exception is that gas wells and gas-fired power plants are often highly secure and are difficult to be attacked. Additionally, M is a large number that releases this constraint for non-attacked pipelines. The above-mentioned bi-level optimization is solved using the approach explained in Section 2.3.4.

Manipulating the Measurements: In the previous step, the location of fake leakages are obtained ($\Lambda_p^a \in \Lambda^p | u_p^a = 1$). To portray these fake leakages, the inlet and outlet gas flow measurements of corresponding pipelines must be manipulated such that (2.18) is met for them, so their leakage detection module picks up. In the mean time, other related measurements of pipelines—i.e., flow (φ_p^{pip}), nodal pressure (θ_n^{nod}), temperature (T_p), and gas loads (φ_q^a)—should be manipulated accordingly to satisfy the gas flow equations of the GN and keep the attack stealthy. Manipulation of measurements, however, should be performed such that the measurements received at the control center do not look suspicious. For instance, a large manipulation of a measurement may increase the risk of attack being detected. As such, the adversary should minimize the deviation of manipulated data from the original one as much as possible to keep the attack stealthy and avoid any suspicion. This goal can be achieved by using the following objective function

$$\underset{z_{a|m}}{\text{minimize}} \quad \sum_{m \in \{\Lambda^p, \Lambda^n, \Lambda^q\}} \left| \frac{z_{a|m} - \hat{z}_m}{\hat{z}_m} \right| \quad (2.23)$$

where subscript $a|m$ indicates the attack sub-vector against gas measurement m , which can target attackable gas loads Λ^q , pipelines Λ^p , or gas nodes Λ^n . Accordingly, $z_{a|m} = \left\{ \varphi_p^{pip}, T_p, \theta_n^{nod}, \varphi_q^a \right\}$ denotes the manipulated measurements of the GN, and $\hat{z}_m$ represents the actual measurements. In this thesis, set Λ^q includes all gas loads. Sets Λ^p and Λ^n , however, comprise all the pipelines and nodes of the gas network except for those whose measurements are obtained inside gas wells and gas-fired power plants. The reason for such an exception was explained in the previous subsection. The objective function represented by (2.23) should be minimized subject to constraint (2.18) for targeted pipelines, as well as constraints (2.14)-(2.16). Additionally, constraints (2.24)-(2.25) ensure that the leakage detection module of targeted pipelines pick up by manipulating their inlet and outlet

gas flow measurements:

$$(1 - \varepsilon_L) \hat{\varphi}_p^{pip} \leq \varphi_p^{in} \leq (1 + \varepsilon_L) \hat{\varphi}_p^{pip} \quad \forall p \in \Lambda_a^p \quad (2.24)$$

$$(1 - \varepsilon_L) \hat{\varphi}_p^{pip} \leq \varphi_p^{out} \leq (1 + \varepsilon_L) \hat{\varphi}_p^{pip} \quad \forall p \in \Lambda_a^p \quad (2.25)$$

where set Λ_p^a indicates the location of fake leakages, which was obtained in Section 2.3.3. Constraints (2.26) and (2.27) ensure that the measurements of gas loads and pipelines' temperature are manipulated within a certain range:

$$-\tau_q \varphi_q \leq \varphi_q^a \leq \tau_q \varphi_q, \sum_{q \in \Lambda^q} \varphi_q^a = 0 \quad \forall q \in \Lambda^q \quad (2.26)$$

$$-\tau^t T_p^0 \leq T_p \leq \tau^t T_p^0 \quad \forall p \in \Lambda^p \quad (2.27)$$

in which, subscripts q refers to loads of the gas network. Eventually, Constraint (2.28) guarantees that the nodal gas balance equations are met after manipulating the measurements

$$\begin{aligned} \sum_{w \in \Omega^w} A_{nw} \hat{\varphi}_w &= \sum_{p \in \Omega^p, p \notin \Lambda_a^p} \sum_{k \in \Omega^k} A_{np} \delta_{pk}^{pip} + \sum_{g \in \Omega^g} A_{ng} \psi_g \hat{P}_g \\ &+ \sum_{p \in \Lambda_a^p} A_{np}^+ \varphi_p^{in} + \sum_{p \in \Omega_a^p} A_{np}^- \varphi_p^{out} + \sum_{q \in \Omega^q} A_{nq} \left(\varphi_q + \varphi_q^a - \varphi_q^{sh} \right) \\ &\quad \forall n \in \Omega^n \end{aligned} \quad (2.28)$$

in which $\hat{\varphi}_w$ is the gas production of gas well w , and A_{np}^+ and A_{np}^- refer to the positive and negative array of node-pipeline connection matrix, respectively. Given that T_p is a decision variable in this problem, the non-linear term $(\theta_n^{nod})^2 / T_p$ appears in the Weymouth equation shown by (2.14). To reach a MILP model for the measurement manipulation problem, this non-linear term must be linearized as elaborated in Section 2.3.4.

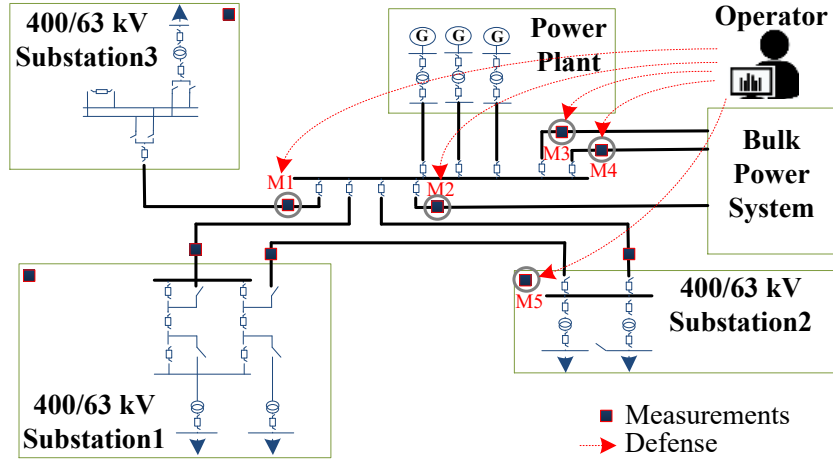


Figure 2.4: Defense strategy on a sample power system.

2.3.4 Methodology for Solving the Bi-level Optimization Problems

This section describes the adopted methodology for solving the two bi-level optimization problems stated in the first and second stages of the proposed coordinated attacks. To solve either problem, it must be written in the following standard compact form

$$\underset{\mathbf{Z}_a}{\text{maximize}} \quad f^U(\mathbf{X}_o^*) \quad (2.29)$$

s.t.

$$h^U(\mathbf{Z}_a) = 0 \quad (2.30)$$

$$g^U(\mathbf{Z}_a) \leq 0 \quad (2.31)$$

$$\mathbf{X}_o^* \in \arg \left\{ \underset{\mathbf{X}_o = \{\mathbf{X}_{o|c}, \mathbf{X}_{o|b}\}}{\text{minimize}} \quad k^T \mathbf{X}_{o|c} \right\} \quad (2.32)$$

s.t.

$$A\mathbf{Z}_a^* + B\mathbf{X}_{o|c} = b_1 \quad (2.33)$$

$$C\mathbf{X}_{o|c} + D\mathbf{X}_{o|b} \leq b_2 \quad (2.34)$$

where $\mathbf{Z}_a$ is the vector of attacker's decision obtained from attacker-level problem; $\mathbf{X}_{o|c}$ and $\mathbf{X}_{o|b}$ signify the vector of continuous and binary variables associated with the operator's decision obtained in the operator-level problem, respectively; $f^U(\cdot)$ is the leader level's objective function; $h^U(\cdot)$ and $g^U(\cdot)$, respectively, represent the set of equality and inequality constraints of attacker-level problem; k is the vector of coefficients multiplying the operator level's objective function; A , B , and C are the coefficient matrices defining the operator-level constraints; and b_1 and b_2 denote the constant vectors of the operator-level constraints. To extract the compact form, all equality and inequality constraints must be rewritten in the standard form. For instance, to solve the bi-level optimization problem of the first stage, the inequality constraints (9)-(12), (15)-(16), and (41)-(48) need to be reformulated as (56). The compact bi-level optimization model is solved by recasting it into a equivalent single-level model in which the operator-level problem is replaced by corresponding KKT conditions. However, the operator-level problem (2.32)-(2.34) contains binary variables $\mathbf{X}_{o|b}$, which violate the optimality of the KKT conditions. To address this problem, the proposed method in [18] is employed, where the binary variables are reformed with continuous representation $\mathbf{X}'_{o|b}$. Meanwhile, a penalty term, i.e., $[\mathbf{X}'_{o|b}]^T \text{diag}(k_f) \mathbf{X}'_{o|b} - k_f^T \mathbf{X}'_{o|b}$ where k_f denotes the penalty vector, is added to the objective function to force the corresponding continuous variables to be either 1 or 0. Therefore, the Lagrangian function associated with the operator-level problem is extracted as follows:

$$\begin{aligned} \mathbf{L} = & k^T \mathbf{X}_{o|c} + \mathbf{X}'_{o|b}{}^T \text{diag}(k_f) \mathbf{X}'_{o|b} - k_f^T \mathbf{X}'_{o|b} \\ & + \lambda^T [A\mathbf{Z}_a^* + B\mathbf{X}_{o|c} - b_1] + \mu^T [C\mathbf{X}_{o|c} + D\mathbf{X}'_{o|b} - b_2] \end{aligned} \quad (2.35)$$

where λ and μ present the vector of positive Lagrange multipliers corresponding to the equality and inequality constraints of operator-level problem, respectively. The optimal solution of problem (2.32)-(2.34) must satisfy the following KKT optimality conditions:

$$\nabla_{\mathbf{X}_{o|c}} \mathbf{L} = k + B^T \lambda + C^T \mu = 0 \quad (2.36)$$

$$\nabla_{\mathbf{X}'_{o|b}} \mathbf{L} = 2 \text{diag}(k_f) \mathbf{X}'_{o|b} - k_f + D^T \mu = 0 \quad (2.37)$$

$$A\mathbf{Z}_a^* + B\mathbf{X}_{o|c} = b_1 \quad (2.38)$$

$$C\mathbf{X}_{\mathbf{o}|\mathbf{c}} + D\mathbf{X}'_{\mathbf{o}|\mathbf{b}} \leq b_2 \quad (2.39)$$

$$\mu^T \perp \left[b_2 - C\mathbf{X}_{\mathbf{o}|\mathbf{c}} - D\mathbf{X}'_{\mathbf{o}|\mathbf{b}} \right] \geq 0 \quad (2.40)$$

where (2.36)-(2.37) and (2.38)-(2.39), respectively, represent the dual feasibility constraint and the primal feasibility constraints, while (2.40) denotes the slackness condition. Accordingly, the bi-level problem (2.29)-(2.34) can be reformulated as follow:

$$\begin{aligned} & \underset{\mathbf{Z}_a, \mathbf{X}_{\mathbf{o}|\mathbf{c}}, \mathbf{X}'_{\mathbf{o}|\mathbf{b}}, \lambda, \mu}{\text{maximize}} && f^U(\mathbf{X}_{\mathbf{o}|\mathbf{c}}) \end{aligned} \quad (2.41)$$

s.t.:

$$h^U(\mathbf{Z}_a) = 0 \quad (2.42)$$

$$g^U(\mathbf{Z}_a) \leq 0 \quad (2.43)$$

$$k + B^T \lambda + C^T \mu = 0 \quad (2.44)$$

$$2 \text{diag}(k_f) \mathbf{X}'_{\mathbf{o}|\mathbf{b}} - k_f + D^T \mu = 0 \quad (2.45)$$

$$A\mathbf{Z}_a^* + B\mathbf{X}_{\mathbf{o}|\mathbf{c}} = b_1 \quad (2.46)$$

$$C\mathbf{X}_{\mathbf{o}|\mathbf{c}} + D\mathbf{X}'_{\mathbf{o}|\mathbf{b}} \leq b_2 \quad (2.47)$$

$$0 \leq b_2 - C\mathbf{X}_{\mathbf{o}|\mathbf{c}} - D\mathbf{X}'_{\mathbf{o}|\mathbf{b}} \leq \chi M \quad (2.48)$$

$$\mu^T \leq (1 - \chi) M \quad (2.49)$$

where the slackness conditions in (2.40) is formulated as linear expressions in (2.48)-(2.49) using Big-M method. In these equations, χ is a binary auxiliary variable. This equivalent single-level model is MILP, which can be solved using commercial solvers.

2.4 Proposed Countermeasures

This section describes two countermeasures, i.e., preventive defense strategy and online learning-based detection scheme, to deal with the coordinated FDIA against IPGSs. The former, which is

performed in advance to the FDIA, aims to reduce the attacker's ability in constructing an effective attack vector by protecting the critical measurements. The latter, however, is deployed during real-time operation of IPGSs, whose objective is to detect the developed coordinated FDIA using the trusted data sources and local information.

2.4.1 Preventive Defense Strategy

One of the most-effective defense strategies against potential cyber-attacks is to reduce attacker's ability to launch a FDIA on systems [18]. In line with the attacker's objectives (2.1) and (2.19) in two-stage model, the attacker's capability rate is assumed to be the total capacity of GFPPs outage caused by the coordinated FDIA to the total capacity of the targeted GFPPs. In this thesis, the operator aims to minimize the attacker's capability by improving the security of measurements in high-risk locations. Measurements in high-risk locations refer to those measurements that are highly probable to being targeted by attackers to construct a stealthy FDIA. The idea behind this defense strategy is that the attacker needs to simultaneously inject the false data into the set of measurements to satisfy power flow constraints and bypass BDD mechanism. For instance, in Fig. 2.4, if the attacker wishes to falsify the load measurements of Substation 3, the measurement M1 needs to be manipulated as well. Meanwhile, due to the balance flow constraint, the injected data to load measurements of Substation 3 needs to be distributed throughout the system by manipulating the measurements of Substation 1 and 2 and their associated lines or measurements of lines connected to the bulk power system, i.e., M2, M3, and M4. In such circumstances, if the operator prevents an attack on a subset of these measurements by improving their security, the attacker's ability to construct an effective attack vector significantly diminishes. For instance, in the exemplary system of Fig. 2.4, improving the security of measurements M1, M2, M3, M4, and M5 hinders the attacker to launch an FDIA on the load measurements located at Substation 1, 2, and 3. However, the operator's capability for improving the security of measurements throughout the system is limited. based on this limitation, the defense degree is defined as the maximum number of measurements that can be protected by the system operator.

To effectively allocate the limited budget of the operator, first, the critical measurements needs to be identified by analyzing the attack vectors under different attack parameters. For this purpose,

Algorithm 1: How to obtain the preventive defense strategies

Data: Set of attack parameters Ω^{AD} with different $B_a^{PS}, B_a^{GN}, \tau_d, \tau_q, \tau_t$ and defense degree

Result: Set of the critical measurements Ω^{CM} and the effective preventive defense strategies Ω^S

Initialized Ω^{CM} and Ω^S equal to $\emptyset$ **for each attack parameter do**

 Solve the developed two-stage attack model (Section 2.3) Record the optimal attack vector and compromised measurements Update Ω^{CM} based on index (2.50)

end

for each defense degree do

 Modify the sub-network $\Lambda = \{\Lambda^l \cup \Lambda^d \cup \Lambda^p \cup \Lambda^n \cup \Lambda^q\}$ based on the defense degree and Ω^{CM} Solve the two-stage attack model (2.1)-(2.28) Record the attacker's capability rate Update Ω^S based on the effectiveness of the defense strategy by Fussell–Vesely index (2.51)

end

this thesis uses Algorithm 1, whose aims are to (i) obtain the most critical measurements, (ii) define effective defense strategies as the security improvement of limited subset of the critical measurements, and (iii) investigate the effectiveness of several defense strategies on reducing the attacker's capability rate. To this end, first, Algorithm 1 solves the two-stage attack optimization model expressed in (2.1)-(2.28) with gradual increase of attack parameter $r = \{B_a^{PS}, B_a^{GN}, \tau_d, \tau_q, \tau_t\} \in \Omega^{AD}$. Afterward, it obtains the most critical measurements set Ω^{CM} based on the following index:

$$CMI_m = \frac{\sum_{r \in \Omega^{AD}} u_{a|m}^r \overline{z_{a|m}^r}}{\sum_{r \in \Omega^{AD}} \sum_{m \in \Lambda} u_{a|m}^r \overline{z_{a|m}^r}} \quad (2.50)$$

where $u_{a|m}^r$ and $\overline{z_{a|m}^r}$ denote the under attack status and normalized injection value (based on the actual value) to Measurement m under the attack parameter r , respectively. This index expresses the critical measurements for a system as ones that must be manipulated in order to conceal the majority of attacks against that system. Considering the critical measurement set Ω^{CM} , Algorithm 1 forms the defense strategies set with respect to the defense degree. Then, it solves the developed two-stage attack model iteratively while different defense strategies are taken in place, and the corresponding the attacker's capability rates are recorded. To determine the most effective preventive defense strategy, the system operator needs to make comparison between the extracted strategies. To this aim, this thesis utilizes Fussell–Vesely (FV) importance index defined as follows [65]:

$$FV_s = \frac{AI_0 - AI_s}{AI_0} \times 100\% \quad (2.51)$$

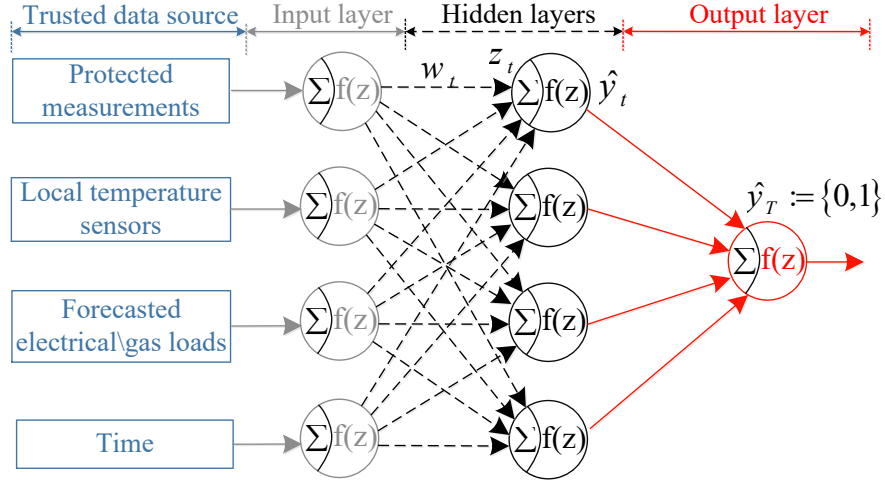


Figure 2.5: Utilized MLP neural network structure.

which represents the relative reduction of attacker's capability rate when the defense strategy s is performed (AI_s) compared to the system under no defense measure (AI_0). The main reasons behind using this index is its simplicity of interpretation and ease of calculation. Flexibility is another salient feature of this index, which enables the operator to easily replace the attacker's capability criterion with any other desired one, e.g., load shedding costs. There are other indices in the literature, e.g., conditional value at risk (CVaR) [66], that can be used instead of the FV index. However, these indices suffer from drawbacks, such as (i) having a complex nature, (ii) requiring the probability density function of parameters, which is difficult to obtain particularly in the case of cyber-attacks, and (iii) lack of flexibility.

2.4.2 Online Learning-based Detection Scheme

Since the designed attack vector respects the load/gas flow equations in IPGSs, the coordinated FDIA can successfully bypass BDD scheme in power systems and pipeline monitoring system in GNs. To tackle this problem, this thesis benefits from learning-based approaches to detect such coordinated cyber-attacks against IPGSs. Among learning-based approaches, neural networks can approximate any multi-input multi-output function, if there are no limitation on the number of neurons [67]. On this basis, as Fig. 2.5 depicts, this thesis utilizes a MLP neural network model to map the operational data of IPGSs, as a set of input features $F = [f_1, f_2, \dots, f_M]^T$ provided by the

trusted data source, to a binary classification label $\hat{y}_T := \{0, 1\}$, which indicates whether the system is operated in the normal mode or under-attack mode, respectively. The parameters of the developed MLP model is tuned using forward backward propagation algorithm. In forward propagation, the input data pass through T layers of the networked artificial neurons (i.e., input layer, multi-hidden layers, and output layer), where the input vector of each layer (z_t) can be obtained as follows:

$$z_t = w_t^T F + \beta_t \quad \forall t = 1 \quad (2.52)$$

$$z_t = w_t^T \hat{y}_{t-1} + \beta_t \quad \forall t \in \{2 : T\} \quad (2.53)$$

where w_t and β_t , respectively, denote the weight and bias vectors of layer t , and $\hat{y}_{t-1}$ represents the output vector of layer $t - 1$. The activation function, which determines the output of each hidden layer based on the corresponding input vector, is considered to be Sigmoid function expressed as follows:

$$\hat{y}_t = f(z_t) = \frac{1}{1 + e^{-z_t}} \quad (2.54)$$

This thesis utilizes Sigmoid function for the following reasons: (i) due to its non-linear nature, it is appropriate for detecting cyber-attacks against IPGSs, where the output layer of the neural network is non-linearly related to the input features, e.g., secured and local measured data; (ii) it produces an output in the range of $(0, 1)$ when it is fed with various inputs; and (iii) due to the large gradient of Sigmoid function in the proximity of zero, a small deviation in input values in this proximity results in a large deviation in the output [68]. In fact, the second and third reasons make Sigmoid function appropriate for binary classification, which is the main purpose for using the neural network in this thesis. Using Sigmoid function, the error vector in the output layer (e_T)—which indicates the difference between the actual and classified labels—and in the hidden layers (e_t) both can be represented by:

$$e_T = (y - \hat{y}_T) f'(z_T) = (y - \hat{y}_T) \hat{y}_T (1 - \hat{y}_T) \quad (2.55)$$

$$e_t = e_{t+1} w_{t+1} \hat{y}_t (1 - \hat{y}_t) \quad (2.56)$$

where y refers to the actual labels. Therefore, during the training process, the weights and biases vector of all layers can be learned to minimize the error vector in the output layer (2.55). To this aim, in the backward error propagation, the weight and bias in each layer is updated using gradient descent as follows:

$$w_t = w_t + \alpha_L e_t \hat{y}_{t-1} \quad (2.57)$$

$$\beta_t = \beta_t + \alpha_L e_t \quad (2.58)$$

in which α_L is learning rate. Therefore, the input data propagate in the MLP model using the updated weight and bias vectors, and new error vectors are computed. This forward backward propagation continues until the error vector in the output layer is minimized.

The data set utilized in the training process comprise of (i) the operational data of IPGSs, i.e., power generation of power plants, gas production of gas wells, real power of lines, gas flow and temperature of pipelines, nodal pressure, electrical and gas loads, provided either by the secure measurements or by the protected measurements, (ii) temperature sensors, (iii) forecasted electrical/gas loads, and (iv) time, which labeled by normal or under-attack operation mode. This training data set can be extracted from the system historical records during several real-world normal and attack scenarios. However, due to the scarcity of such a coordinated FDIA against IPGSs, synthetic normal and attack scenarios are conducted to enrich the training data set. Therefore, two data subsets, i.e., legitimate and under-attack, are constructed under different operational points, network configuration for N-1 contingencies, and attack parameters. The normal data determined by SCED problem (2.8)-(2.17) are recorded in the legitimate subset, while the falsified data obtained by the proposed two-stage coordinated FDIA (Section 2.3) are recorded to construct under-attack subset. Additionally, to ensure that the proposed detection scheme can differentiate between real incidents and attacks, the legitimate subset is extended by considering several real leakage with different severity.

2.5 Results and Discussion

This section presents the numerical analysis of the developed coordinated FDIA model and the effectiveness of the proposed countermeasures in IEEE 24-Bus 20-Node IPGS and large-scale IEEE 118-Bus 135-Node IPGS. As Fig. 2.6 shows, in IEEE 24-Bus 20-Node IPGS, the power system comprises of 38 lines, 24 buses, 17 loads, and 10 power plants which three of them, i.e., $g1$, $g4$, and $g5$, are GFPPs that are supplied by GN through $n5$, $n1$, $n2$, respectively. Additionally, 55 measurements are installed in the power system as illustrated by red foursquare in Fig. 2.6. Given that each node of the GN is equipped with measurements of pressure, gas flow, and temperature, 60 measurements are installed in the GN. The actuators corresponds to the power plants, gas well, pipeline valves, and electrical and gas loads which are shown by blue foursquare in Fig. 2.6. These actuators receive the control commands from operator using the solutions of the scheduling problem. Total electrical loads and gas demands are 2,385.45 MW and 4,232.11 MBtu, respectively. Furthermore, the interruption cost for electrical loads and NG demands are \$1000/MWh and \$5500/MBtu, respectively. The coefficients of pipeline leakage detection threshold, i.e., transient (a_{c2}), packing feature (a_p), and measurements accuracy (a_f), are considered to be 1%, 0.5%, and 1%, respectively [55]. Further details of this system could be found in [69]. The simulation was performed by CPLEX solver of GAMS software with 0.1% optimality gap on a PC with Intel Core i5 and 8GB RAM.

2.5.1 Consequences of the Attack Model

Four case studies are introduced in Table 2.1 to evaluate the consequences of the presented attack mechanism. The attack is launched during the peak load condition with different targeted GFPPs and maximum allowed rang of false data injection to the measurements of electrical/gas loads and pipelines' temperature. It is worth noting that the adversary is not able to target GFPP $g5$ because manipulating the gas measurements located at gas wells and GFPPs can be easily identified by the system operator. In all cases, it is assumed that the attacker is able to compromised at most 11 power measurements and cause one fake leakage in the GN.

By solving the first stage of the proposed attack model, the attack vector on the power system measurements is obtained, as shown in Fig. 2.7. According to this figure, to increase the power

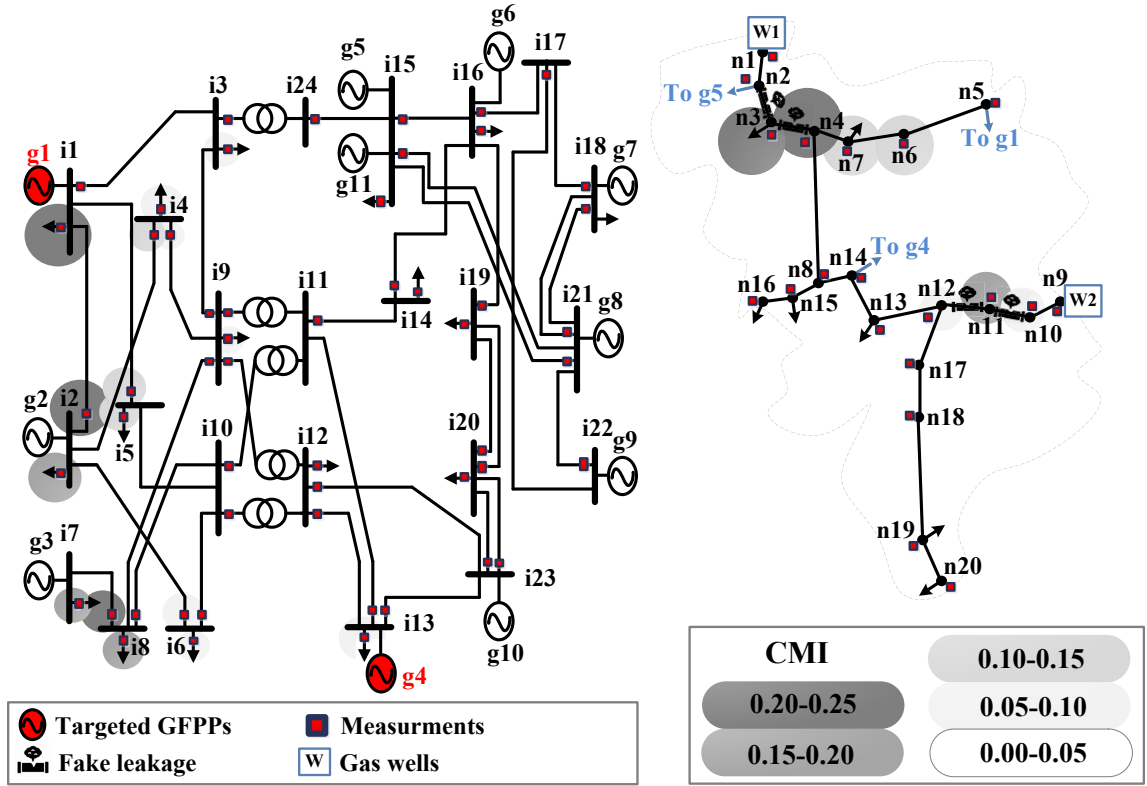


Figure 2.6: IEEE 24-Bus 20-Node IPGS and its most critical measurements.

Table 2.1: Case Studies on 24-Bus 20-Node IPGS

	Targeted GFPPs	Capacity (MW)	$\tau_d, \tau_q, \tau^t(\%)$
Case I	$g4$	152	0.25
Case II	$g4$	152	0.5
Case III	$g1, g4$	552	0.25
Case IV	$g1, g4$	552	0.5

generation of $g4$ in Cases I and II, the attacker injects negative value to the load measurements $d1$ and $d2$, and compensate it with positive values in $d3-d9$. Accordingly, to bypass the BDD mechanism, the measurements of lines $l1-l8$ and $l11$ are compromised. In contrast, in Cases III and IV, where both $g1$ and $g4$ are targeted by the attacker, the group of load measurements $d1-d2$ and $d3-d9$ are compromised with positive and negative injection values, respectively. In general, the attack vectors shown in Fig. 2.7 contribute to the greater amount of the injection value $z_{a|d}$ and $z_{a|l}$ to the load measurements $d1, d2, d7$, and $d8$ and the line measurements $l1$ and $l11$ compared to the other measurements. These attack vectors mislead the operator into redispatching the power plants

as illustrated in Fig. 2.8. As depicted in this figure, the increasing generation of power plants $g1$ and $g4$ are compensated by reducing the one of $g3$. Therefore, the attacker succeeds to reach the power generation of the targeted GFPPs to 81%, 100%, 83% and 99% of their total maximum capacity in Cases I-IV, respectively.

In the second stage of the developed attack, the adversary obtains the best location of fake leakage as reported in Table 2.2. As shown in this table, the attacker aims to portray a fake leakage on the pipelines that transfer the gas wells $w2$ and $w1$ to the GN, causing severe fuel shortage for the targeted GFPPs. Based on the location of fake leakage, the injection value to inlet/outlet gas flow measurements of the targeted pipelines are obtained based on the measurement manipulation problem (2.23)-(2.28). The attack vector on pipeline monitoring system in Cases I-IV demonstrates that the measurements located at nodes $n2-n4$ and $n10-n12$ are more exposed to the FDIA, whose aim is the outage of GFPPs $g1$ and $g4$. As Table 2.3 reports, the coordinated FDIA on the IPGS in Case I contributes to 124.3 MW generation outage and 81.8% attacker's capability rate. In Case II, the adversary succeeds to cause 152 MW generation outage with 100% attacker's capability rate because increasing the allowed injection value on the measurements of electrical/gas loads and temperature enables the attacker to design more impactful attack compared to Case I. In Cases III-IV, where 552 MW generation capacity are targeted, the designed attack vector results in 460.6 MW and 551.2 MW generation outage. The forced generation outage in Cases III and IV correspond to 83.4% and 99.8% attacker's capability rate, respectively. As Table 2.3 illustrates, the more the allowed range of injection on the measurements of electrical/gas loads and temperature, the higher the ability of the attacker, and the lower execution time in designing the data attack would be. To determine the minimum number of compromised measurements in the power system and GN, the two-stage model is iteratively run under descending value of B_a^{PS} and B_a^{NG} . Once the optimization problems of two-stage model fail to achieve a global optimal solution, the number of manipulated measurements in the previous iteration is recorded as the minimum number of compromised measurements. Results show that the number of compromised measurements in the power system and GN is reduced while the allowed range of injection on measurements of electrical/gas loads and pipelines' temperature increases. However, increasing the false data injection range to electrical/gas load measurements elevates the chance of anomaly detection by control center. Therefore, the attacker faces a trade off

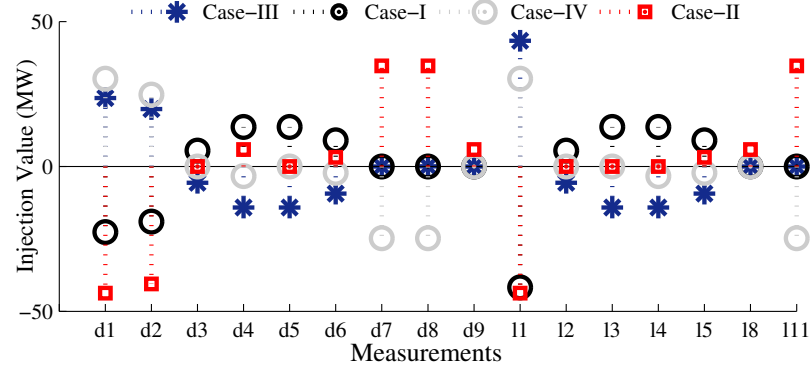


Figure 2.7: FDIA vectors on measurements of IEEE 24-Bus system at Peak Load.

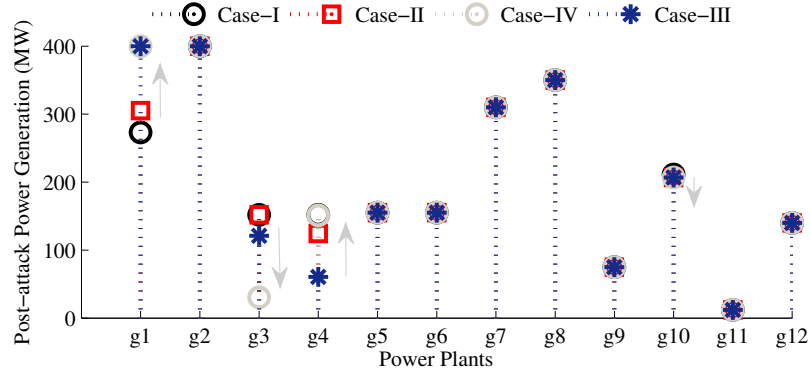


Figure 2.8: SCED solution in IEEE 24-Bus system affected by the designed attack vectors.

Table 2.2: Injection Value to the Pipelines' Flow Measurements of 24-Bus 20-Node IPGS During Peak Load (MBtu/h)

	Location of fake leakage	Injection value to the inlet measurement	Injection value to outlet measurement
Case-I	n11-n12	1203.8	1251.9
Case-II	n10-n11	1500.1	1560.1
Case-III	n3-n4	4019.5	4180.3
Case-IV	n2-n3	4032.2	4194.5

between the interest, execution time, and detection chance to build a malicious attack.

The forced generation power outages in Cases I-IV are, respectively, equivalent to loss of 5.2%, 6.4%, 19.3%, and 23.1% of total generation power, which can adversely impact the grid's frequency and cause cascading failure. In addition, since the pipeline monitoring system detects and isolates the leakage no longer than few minutes, the system operator fails to immediately recover the lost power generation due to the ramp-up constraints of available power plants. As a result, the load

Table 2.3: Post-attack System Results During Peak Load in Cases I-IV Where no Defense Strategy is Performed.

	Case I	Case II	Case III	Case IV
Total generation outage (MW)	124.3	152	460.4	550.9
Total load shedding (MW)	0	0	270.4	360.9
AI_0 (%)	81.8	100	83.4	99.8
Execution time (s)	53	24	89	31
Min number of compromised power system measurements (N.O)	9	6	9	7
Min number of compromised GN measurements (N.O)	7	5	7	5

shedding plan must taken in place to satisfy the short term load-generation balance. According to the ramp-up rate of the power plants, during first 10 minutes in post-attack period, the under-study IPGS is capable of increasing at most 236.7 MW and 190 MW in Cases I-II and III-IV, respectively. Therefore, in Cases I and II, the power generation outage of $g4$ is compensated by the other power plants during this horizon time. In contrast, the system operator fails to recover the severe generation mismatches caused in Cases III and IV, leading to 270.4 MW and 360.9 MW load shedding, respectively. Although, no load shedding occurs in Cases I and II, this FDIA can expose economic losses to the IPGS by violating the optimal operation solution. The resultant economic losses can be even considerable since the topology attack on the pipeline monitoring system could be hidden for several hours.

2.5.2 Effectiveness of the Preventive Defense Strategy

This subsection describes the results obtained by Algorithm 1 for identifying the critical measurements in the under-study IPGS and the mitigation ability of defense strategy. The most critical measurements are obtained, by following the first loop of Algorithm 1 with gradual increase of the attack parameters, i.e., $B_a^{PS} \in [6, 20]$, $B_a^{GN} \in [1, 2]$, and $\tau_d = \tau_q = \tau^t \in [10, 50]$, while targeting two GFPPs $g1$ and $g4$.

As Fig. 2.6 shows, power measurements $d1$, $d2$, $d3$, $d7$, $d8$, $l1$, $l3$, and $l11$ as well as NG measurements located at $n3$, $n4$, $n6$, $n7$, $n10$, $n11$, and $n12$ are more exposed to the FDIA. Accordingly, several defense strategies are extracted to protect these measurements. Table 2.4 identifies the most

Table 2.4: The Preventive Defense Strategies

	d1	d3	d7	l1	l11	n3	n4	n6	n7	n10	n11	n12
S1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
S2	✓	✓	✓	✓	✓	✓	✓	✓	✓			
S3	✓		✓	✓	✓	✓	✓	✓	✓			
S4	✓				✓	✓	✓	✓	✓			
S5						✓	✓	✓	✓			
S6	✓		✓		✓	✓	✓					
S7	✓				✓	✓	✓					
S8					✓	✓	✓					
S9						✓	✓					

effective defense strategies which are selected based on FV index (2.51). While the measurements $d7$, $d8$, and $l3$ are among the critical measurements, no defense measure is required to protect them. This means that the operator can hinder the attacker to build an effective attack vector by protecting a precise sub-group of the critical measurements. The effectiveness of the developed defense strategies against different attack parameters—here only the contribution of τ_d , τ_q , and τ_t are studied—is shown in Fig. 2.9. As can be seen in this figure, the more the defense degree, the lower attacker’s capability rate would be. By deploying defense strategies $S1$ and $S2$, where 26 and 17 measurements are protected, respectively, the operator can significantly reduces the attacker’s capability rate to bellow 10%, even though the attack parameters are increased up to 50%. If the defense strategies $S3$ and $S4$ are taken in place, the attacker’s capability rate decreases more than 80% even in the case of 50% increase in attack parameters. Eventually, in the defense strategies $S8$ and $S9$, in which just seven and six measurements are protected, the attacker’s capability rate is decreased more than 40% in average. These results demonstrate that improving the security of even small subset of measurements can considerably decrease the attacker’s ability to construct the effective attack vector.

2.5.3 Performance of the Online Learning-based Detection

This subsection evaluates the performance of the proposed online learning-based detection scheme. To enrich training data set, several operational points, network configuration for N-1 contingencies, and attack parameters are taken into account to ensure the accuracy of detection scheme

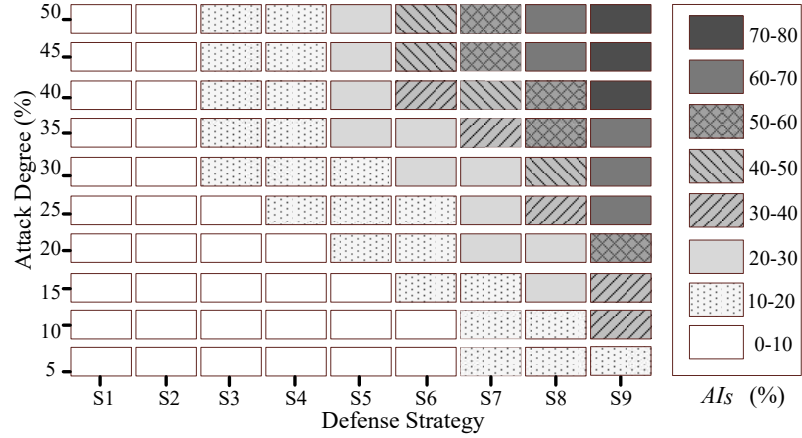


Figure 2.9: Effectiveness of the preventive defense strategies S1-S9.

during different conditions. To this aim, the recorded data of the PJM electricity market (RTO local area in 2020), e.g., normalized forecasted hourly load and temperature, are used to capture 8760 operational points. Moreover, in each operational point, Monte Carlo simulation with unique probability function is deployed to select network configuration during normal condition (no outage) and N-1 contingencies, the attack parameters $B_a^{PS} \in [6, 20]$, $B_a^{GN} \in [1, 2]$, and $\tau_d = \tau_q = \tau^t \in [10, 50]$. Afterward, in each operational point and network configuration, data of electrical/gas loads, temperature, and time, as well as the data corresponding to the protected measurements, e.g., power of lines, gas flow of pipelines, and nodal pressure, are obtained using normal SCED problem and the developed two-stage FDIA, being recorded in the legitimate and under-attack subsets, respectively. Additionally, the legitimate subset are extended by considering 100 real-leakage samples whose locations and leakage intensities are randomly selected on 11 pipelines and between 5% to 10% of normal gas flow, respectively. Therefore, there are 17,620 samples in total in the data set, which comprises of 8,760 under-attack samples, 8,760 normal operation samples, and 100 real leakage samples. To train the proposed method, 80% of the constructed data set is randomly selected, and the remaining 20% is used for testing. The appropriate number of the hidden layers and neurons in each layer are, respectively, selected to be 20 and 30, using the cross-entropy index and sensitivity analysis over 500 training iterations. This thesis uses the *MLPClassifier* function from *sklearn.neural_network* library in Python environment to create and learn the proposed MLP model.

Table 2.5: TP, FN, TN, and FP Parameter for the IEEE 24-Bus 20-Node IPGS

Preventive Strategy	TP	FN	TN		FP	
			Normal operation	Real leakage	Normal operation	Real leakage
S0	1578	174	1574	14	178	6
S1	1743	9	1748	19	4	1
S2	1737	15	1731	18	21	2
S3	1698	54	1690	18	62	2
S4	1684	68	1683	18	69	2
S5	1678	74	1676	18	76	2
S6	1658	94	1649	17	103	3
S7	1629	123	1626	17	126	3
S8	1607	145	1609	16	143	4
S9	1584	168	1591	16	161	4

To evaluate the performance of the proposed detection scheme, five statistical metrics are considered, i.e., Accuracy, Precision, Sensitivity, Specificity, and F1-Score. These metrics are calculated based on four parameters including: (i) true positive (TP): the number of under-attack samples that are correctly detected; (ii) true negative (TN): the number of the legitimate samples that are recognized; (iii) false positive (FP): the number of false alarm during the legitimate samples; and (iv) false negative (FN): the number of the under-attack samples which are not detected. Further information about these metrics is available in [70].

The performance of the proposed detection scheme in the case of different preventive defense strategies (Table 2.4) is illustrated in Table 2.5 and Fig.2.10. In Strategy *S0*, in which no preventive defense measure is taken in place, the MLP model is learned using data related to the generation of power plants, gas production of gas wells, forecasted electrical/gas loads, temperature, and time. In this case, the learned MLP model succeed to detect 1578 falsified data samples among 1752 under-attack data subset, and has 178 and 6 false alarms during 1752 and 20 samples of normal operation and real-leakage, respectively. Given that the attack vector in this thesis completely satisfies the gas/load flow equations of IPGSs (in oppose to [54] where the attack vector on IPGSs is statistically constructed), the performance of the proposed detection scheme is acceptable. Meanwhile, the results demonstrate that the proposed preventive defense strategy can significantly improve the detection performance. In Strategy *S1*, a higher number of measurements, i.e., 26 out of 115, are

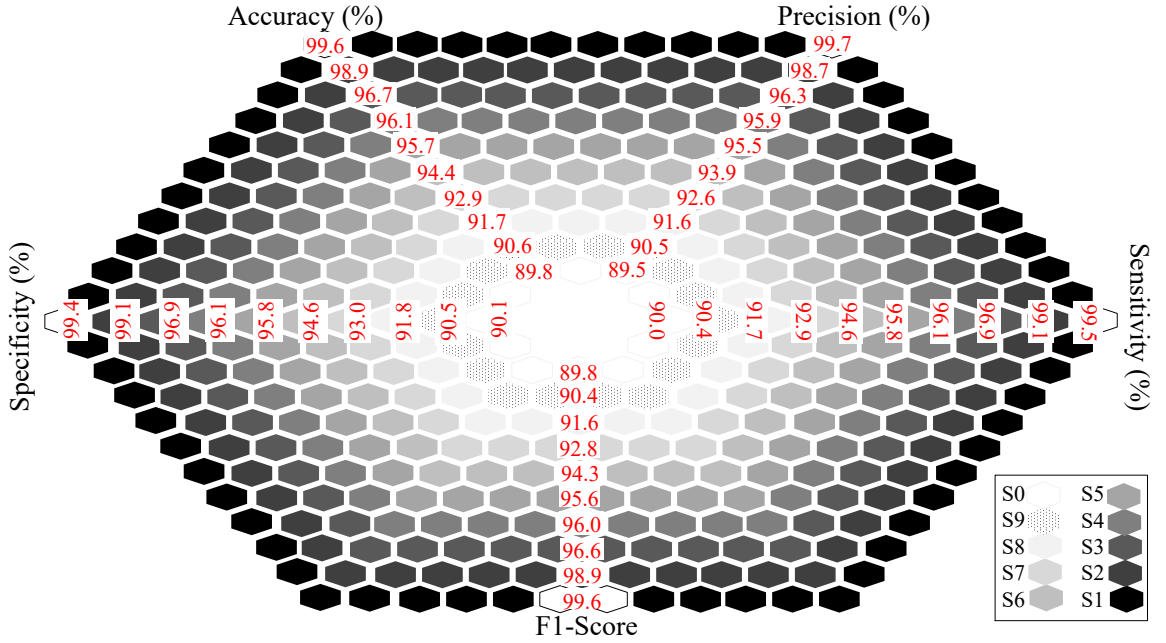


Figure 2.10: Performance of the detection scheme on the 24-Bus-20-Node IPGS without the preventive measures (S0) and during different preventive defense strategies S1-S9 in Table 2.4.

protected. This can be translated into having more features for training of the MLP model. As a result, this strategy comes with superior detection performance compared to the other strategies, i.e., 99.6%, 99.7%, 99.5%, 99.6%, and 99.4% for Accuracy, Precision, Sensitivity, Specificity, and F1-Score, respectively. As reported in Table 2.5, this performance is achieved by detecting 1743 out of 1752 attack samples and distinguishing 19 out of 20 real leakage samples. By reducing the number of the protected measurements in Strategies $S_2 - S_9$, the number of features used for training of the MLP model will decrease, resulting in continuously decreasing the performance of the detection scheme. In Scenario S_9 , where only six measurements are protected, number of TP and TN reduce from 1743 and 1764 in Scenario S_1 to 1584 and 1607, respectively. Therefore, Accuracy, Precision, Sensitivity, Specificity, and F1-Score metrics considerably decrease to 90.6%, 90.5%, 90.4%, 90.4%, and 90.5%, respectively. This results emphasize the importance of the proposed preventive defense strategy on the accuracy of the online detection scheme. Therefore, in order to defend against such a coordinated FDIA in IPGSs, a systematic approach is required which coordinates the selection of the critical measurements, the adoption of a preventive defense strategy to protect the critical measurements, and the online attack detection. In line with this crucial requirement,

Table 2.6: FDIA on the Pipeline Flow Measurements of IEEE 118-Bus 135-Node IPGS During Peak Load and Consequent Outage of GFPPs

Targeted GFPPs	Attack parameters	Location of fake leakages	Injected value to the gas flow measurements (MBtu/h)		Total outage (MW)
			inlet node	outlet node	
$g8, g9$	$B_a^{PS} = 30$ $B_a^{GN} = 1$ $\tau_d, \tau_q, \tau^t = 50$	n86-n3	2515.8	-	200
$g21, g26$	$B_a^{PS} = 30$ $B_a^{GN} = 2$ $\tau_d, \tau_q, \tau^t = 50$	n43-n44 n14-n33	4909.5 3782.1	4708.3 3592.9	343.1

EMS. In the case of portraying two fake leakages, i.e., $B_a^{NG} = 2$, the adversary can interrupt the supply of gas to GFPPs $g21$ and $g26$, as well as to other gas loads, by targeting Pipelines $n43 - n44$ and $n14 - n33$ simultaneously. In this case, however, $g21$ and $g26$ are not committed. Thus, the adversary needs to inject the attack vector shown in Fig. 2.12-(a) in the power system measurements to redistribute the electrical demands during peak load condition, and consequently, mislead the EMS to increase the generation of these two power plants. As Fig. 2.12-(b) shows, the launched FDIA affects the SCED's solution such that $g21$ and $g26$ are committed to generate 83.1 MW and 260 MW, while the generation of $g30$ and $g40$ are reduced to 0 MW and 93.2 MW, respectively. Therefore, the adversary succeeds to cut off 343.1 MW of power. This case proves that although the attack on the EMS and the pipeline monitoring system seems independent, coordinating them intensify the severity of the attack.

To develop and implement the proposed countermeasures, first possible attack vectors on power and gas measurements are extracted by running the two-stage attack model iteratively with different attack parameters, i.e., $B_a^{PS} \in [15, 30]$, $B_a^{GN} \in [1, 2]$, and $\tau_d = \tau_q = \tau^t \in [10, 50]$. To create a dataset for training of the proposed learning-based detection scheme, 8760 operation points from the historical data of PJM electricity market in 2020 are used. Additionally, to empower the detection scheme to distinguish between fake and real leakages, 500 real leakage incidents are considered. The location of these real leakages are randomly selected among 141 pipelines with leakage flow between 5%-10% of their normal gas flow.

Based on the extracted possible attack vectors, the most critical measurements, i.e., 23 for the

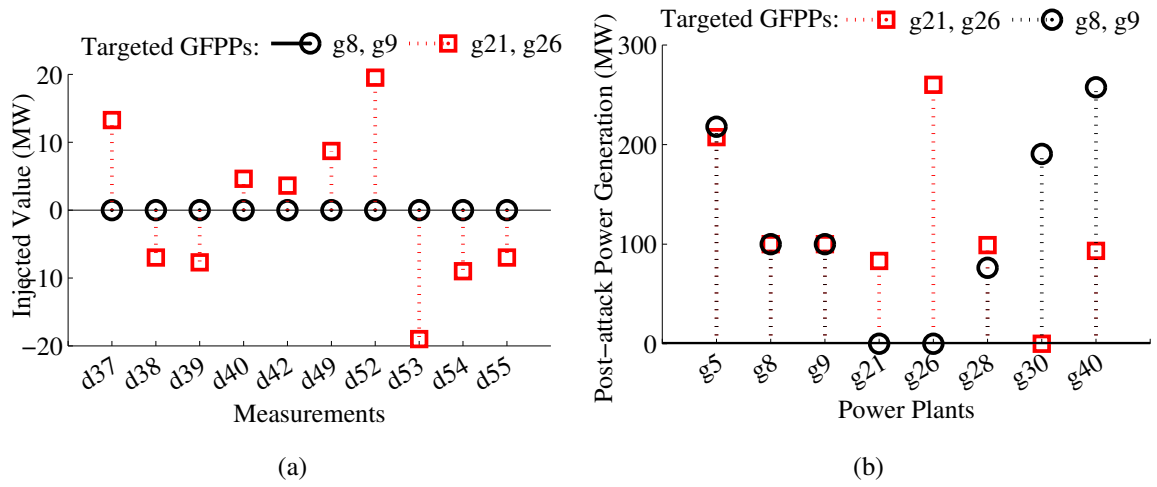


Figure 2.12: FDIA against the EMS of IEEE 118-Bus power system during the peak load (a) attack vector on measurements (b) output of SCED.

Table 2.7: TP, FN, TN, and FP Parameter for the IEEE 118-Bus 135-Node IPGS

Preventive Strategy	TP	FN	TN		FP	
			Normal operation	Real leakage	Normal operation	Real leakage
S0	1570	182	1574	81	178	19
S1	1745	7	1746	98	6	2
S2	1538	14	1539	96	13	4
S3	1575	177	1577	84	175	16

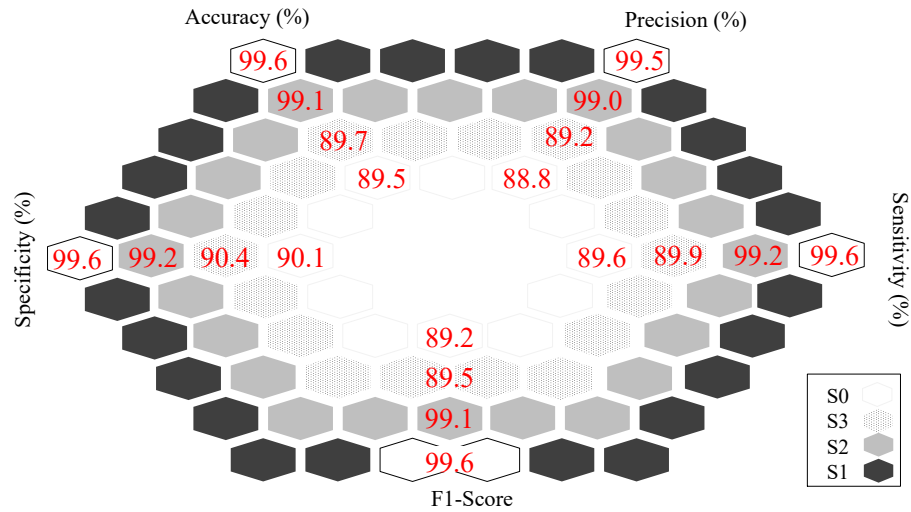


Figure 2.13: Performance of the detection scheme on the IEEE 118-Bus-135-Node IPGS for the different preventive strategies.

power network and 12 for the GN, are identified using CMI index (2.50). These measurements are shown in Fig. 2.11. Afterward, to better evaluate the performance of the proposed method, the following preventive strategies are considered and compared:

- S_0 : No measurement in the gas and power networks are protected.
- S_1 : Both critical power and gas measurements are safeguarded.
- S_2 : Only critical gas measurements are protected.
- S_3 : Only critical power measurements are protected

For each strategy, the features corresponding to the protected measurements and the local sensors, as well as the forecasted data are given to the deployed neural network classifier as its input. Similar to Section 2.5.3, 80% and 20% of the dataset are used for training and evaluating the detection scheme, respectively. The performance of the detection scheme is reported in Table 2.7, which are further used to calculate the statistical metrics shown in Fig. 2.13. As Fig. 2.13 illustrates, for Strategy S_0 , detection accuracy reaches 89.46% by identifying 1570 attacks out of 1752, and having 197 false positive alarms during 1752 normal operation and 100 real leakage samples. For S_3 , the accuracy is slightly improved to 89.79%, with 1575 TP and 191 FP alarms. In contrast, for Strategy S_2 , the accuracy is considerably enhanced to 99.14%, with 1738 TP and 17 false positive alarms. Further improvement in the accuracy (i.e., 99.59%) can be achieved by protecting both power and gas measurements in Strategy S_1 . In Strategy S_1 , the learning-based detection scheme succeeds to identify 1745 out 1752 attack samples and distinguish 98 out 100 real leakage from FDIAs. The reason for such high accuracies is that after implementing the proposed method, only a portion of measurements can be manipulated during cyber-attacks, since (i) the critical ones are reinforced against intrusions and thus are unattackable, and (ii) the attacker's ability is bounded, so a limited number of measurements can be compromised. As a result, the developed learning-based framework can detect cyber-attacks, by recognizing the inconsistencies or contradictions among measurements. Note that by reinforcing critical measurements these inconsistencies/contradictions cannot be hid anymore. However, in the case of a real fault or disturbance (e.g., a real leakage), all the measurements are consistent, so it can be distinguished from cyber-attacks.

Chapter 3

Security Enhancement of WADC- Part I

3.1 Problem Statement

The occurrence of dominant low-damping oscillations (DLOs) can jeopardize the reliability and stability of modern power systems [19]. To alleviate the detrimental impacts of these oscillations, wide-area damping controllers (WADCs) have been widely utilized in power grids around the world, e.g., in the U.S. [4] and China [72]. As Fig. 4.5 depicts, in a WADC scheme, the timestamped and highly-sampled synchrophasor data—up to 120 measurements per second—from several phasor measurement units (PMUs) are transmitted to local phasor data concentrators (PDCs) using IEEE C37.118 communication channels. Through time-alignment strategies, which are discussed in IEEE Std C37.247-2019, local PDCs aggregate PMU data into a single data stream based on their timestamp [73]. Aiming to dampen the oscillations, these data are then transmitted to WADC to generate the appropriate control signals, which are sent back to grid actuators, e.g., synchronous generators [73].

Since the WADC needs to have time-synchronized data of PMUs, it is crucial to ensure that accurate, authenticated, and coordinated universal timing signals are available for all wide geographical scattered PMUs [74]. To achieve this goal, two major time synchronization technologies are often used in wide area systems: (i) space-based, such as global positioning system (GPS) [75], and (ii) network-based, e.g., precision time protocol (PTP) [76]. However, both technologies are proven to be prone to time synchronization attacks (TSAs) which puts the entire grid at risk as

demonstrated theoretically and experimentally [3, 12, 77–79]. For instance, GPS receiver of PMUs can be compromised by spoofing or replay attacks [3], and PTP time reference can be maliciously altered by launching deception or delay attacks on broadcasting synchronization messages [77]. Moreover, it has been demonstrated that TSAs can result in catastrophic degradation of power system performance, particularly its control schemes [12, 78, 79]. The experimental studies in [12] and [80] demonstrated that manipulation of PMU data timestamp can appear as an error in phasor angle, which consequently can degrade WADC performance and even destabilize the grid. Additionally, TSAs can compromise PMU data aggregation procedure in the PDC, exposing WADCs to loss of PMU data packet or delay [79]. The TSAs can also remain hidden and undetectable from commonly-used bad data detection schemes in power systems, as proven in [81]. Thus, it is of paramount importance to identify the potential repercussions of TSAs and prepare effective countermeasures against them.

3.2 Literature Review and Research Gaps

Extensive scholarly works exist in the literature for detection, e.g., [82–84] and mitigation, e.g., [85, 86], of TSAs against wide-area applications. For instance, the authors in [82] proposed a Kalman filter-based anti-GPS spoofing attack scheme, which detects the post-attack violated phasor angle error using PMU data. Given the correlation between the information from the PMU clock and the power system, a data-driven TSA detection approach has been developed in [83]. More recently, a GPS spoofing attack detection scheme was proposed in [84] by the deployment of a redundant GPS antenna. Aiming at mitigating TSAs, the authors in [85] proposed a robust PMU angle deviation correction approach, which can be used to compensate for the manipulated phase angles after TSAs. To deal with the abnormal delay caused by TSAs, the authors in [86] proposed a delay-aware variable loop gain WADC scheme. Although detection and mitigation approaches for TSAs are well-studied, limited research, e.g., [87–89], has been conducted to prevent TSAs. In space-based time synchronization schemes, a GPS spoofing attack prevention was presented in [87] using key encryption, drift monitoring, and signal geometry approach. For network-based time synchronization schemes, the authors in [88] proposed a new extension that improves the security of

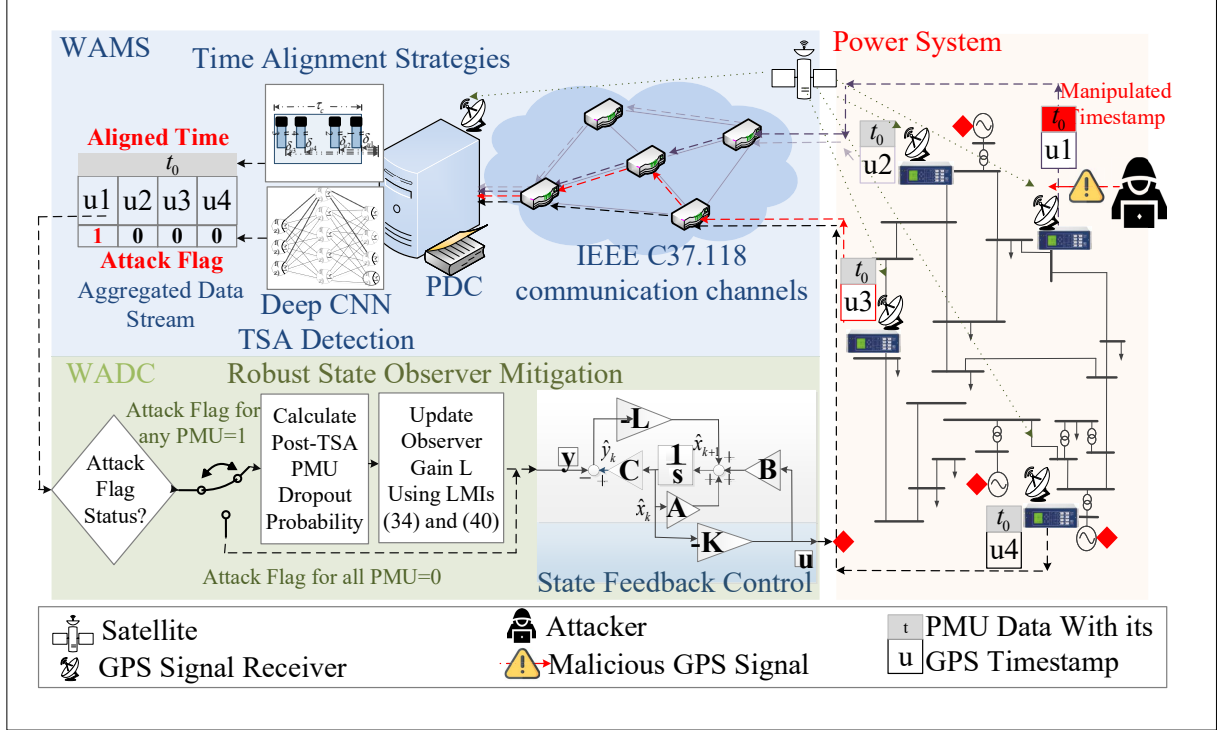


Figure 3.1: Overall PMU-enabled WADC scheme.

the PTP scheme by collecting time messages from slave clocks and accessing the clock synchronization status. Moreover, to improve the security of data aggregation against TSA, blockchain's inherent advantages, e.g., distributed storage, consensus mechanism, and avoidance of single-point of failure, were employed in [89]. These developed prevention approaches, however, reinforce the information and communication infrastructure of time-synchronization schemes without considering wide-area applications, particularly WADCs. Moreover, current studies in the literature suffer from at least one of the following drawbacks: they (i) require hardware/software modification or network device/scheme aggregation in PMU-enabled WADCs, which increases overall system complexity, (ii) ignore the adversary's capability to construct a stealthy malicious TSA vector targeting WADCs' observability performance, (iii) do not fully investigate the impacts of TSAs against PMU data aggregation procedure and their effects on WADC performance, and (iv) do not propose any prevention strategy against TSAs targeting PMU data aggregation in WADC schemes.

3.3 Attack Model

PMU-enabled WADCs is a recent paradigm in modern power systems, which not only counteracts large-scale contingency propagation and cascading failures but also enables higher power transfer capacity [90]. In contrast to local controllers, WADCs empower power grids to observe system-wide oscillations behaviors and make real-time appropriate control decisions. To this aim, as Fig. 4.5 shows, WADCs leverage the highly-sampled synchronized PMU measurements that are aggregated by PDCs. Based on IEEE Std C37.247-2019, PDCs utilize the timestamps of PMU data to aggregate the measurements into a single stream using relative or absolute time-alignment strategies [7]. In the case of relative time alignment, a new time-stamped buffer is created following the first PMU data arrival at PDC. The PDC is expected to receive data from all other PMU data with the same timestamp during a relative waiting time, accounting for communication delay. The waiting time guarantees the complete aggregation of all PMU data tagged with the same timestamp in a single data stream. Once the waiting time is over, the PDC will close the buffer that was initiated, generate an output data stream, and transmit it to the control center. On the other hand, the absolute time alignment approach uses the PDC's local clock as a reference time to start time-stamped buffers. In this situation, the PDC collects all PMU data with the timestamp same as the time-stamped buffer before an absolute buffer waiting time runs out. It is worth noting that, there is no direct relationship between the PDC buffer waiting time and PMU sampling time. In fact, this statement implies that the PDC can have concurrent open data stream buffers associated with different sampling times [7]. Regardless of the time-alignment strategy deployed by PDC, any PMU data that arrives after the PDC buffer waiting time will be dropped [7]. These time alignment strategies open new windows for attackers to compromise the data collection functionality of PDCs and deliberately drop PMU data by manipulating their timestamps [91].

3.3.1 Assumptions of The Attack

In this thesis, the attack surface is the time-synchronization technologies of PMUs. A PMU receives measurement sample value from potential/current transformers (PT/CT) in substations and calculates the associated phasor data using the converted digital form of the measurement sample

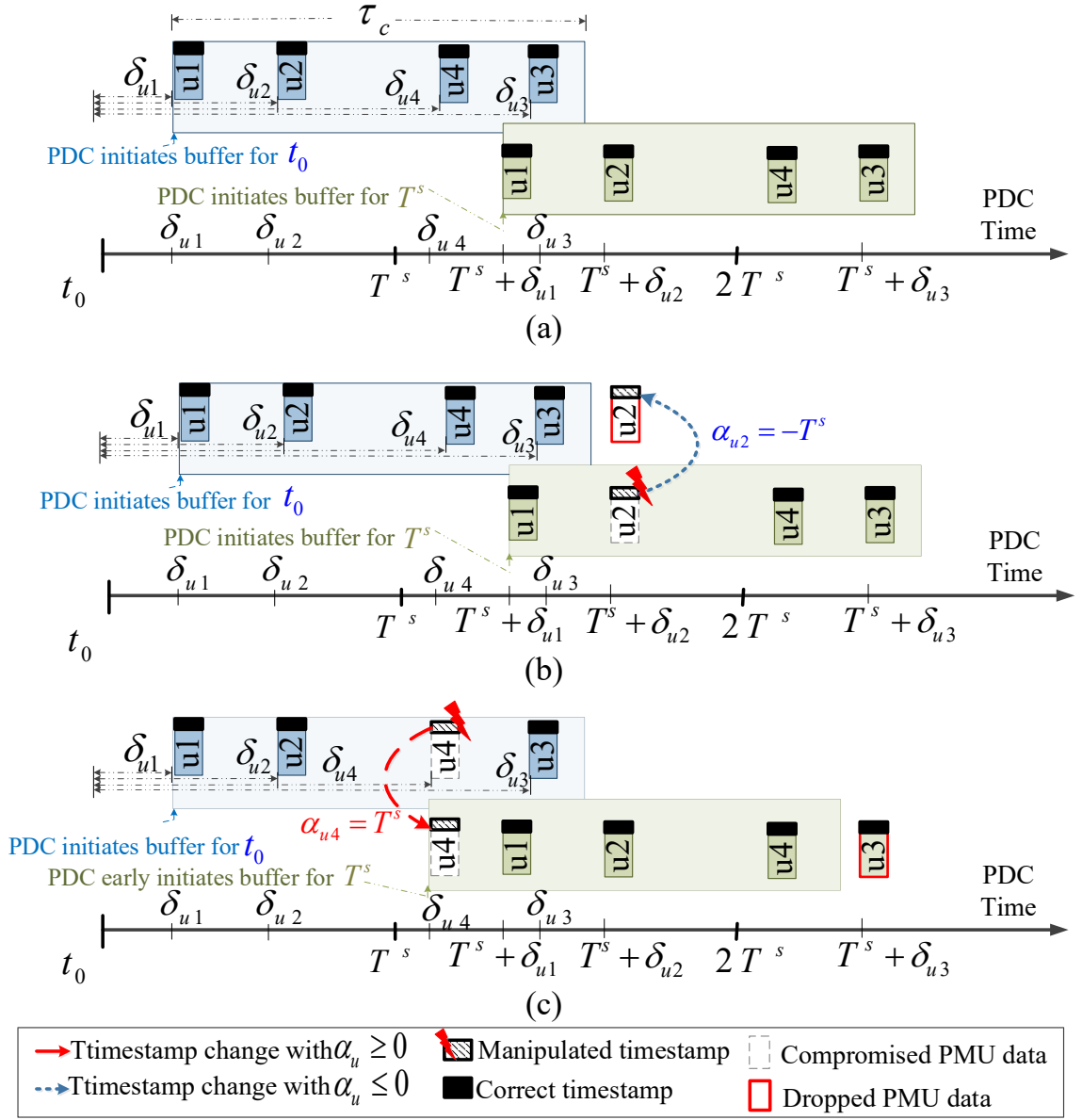


Figure 3.2: TSA impacts on PMUs data aggregation at PDC using relative time-alignment: (a) pre-attack condition, (b) post-attack condition I, (c) post-attack condition II.

and a time reference provided by the time synchronization schemes [25]. On this basis, the TSA modifies the time reference signal which is used in PMU during the sampling (not during data transmission). For space-based time-synchronization technologies, the adversary can launch a GPS spoofing attack by misleading the GPS receiver to follow a malicious signal. This signal is similar to the legitimate one in terms of phase, delay, and encoded data, but has more intensity. Alternatively, the adversary can perform GPS spoofing using a replay attack, in which he/she sends time-shifted

copies of legitimate GPS signals with a higher strength to the PMU receiver to disrupt the real GPS signal. [3]. For network-based time-synchronization technologies, the adversary can compromise the PTP broadcasting synchronization message by launching deception or delay attacks [88]. In this attack, the false time is ensured once the time synchronization schemes are compromised. Regardless of the time-synchronization technology used for the execution of the attack, Fig. 3.2 shows two ways that can result in the data drop in the PDC.

Post-Attack Condition I- dropout in the targeted PMU data ($\alpha_u < 0$): In this case, the adversary maliciously alters the timestamp of a PMU data to a time whose corresponding buffer has ended when the data arrives at the PDC. To put it in an example, as Fig. 3.2-(b) depicts, if the adversary changes the data timestamp of PMU u_2 from T^s to t_0 , the PDC receives this data at time $T^s + \delta_{u_2}$ when the buffer corresponding to t_0 has collapsed. Consequently, the manipulated PMU data will be dropped. Both relative and absolute time alignment strategies are subject to this attack.

Post-Attack Condition II- dropout in the other PMU data ($\alpha_u > 0$): In this case, the manipulated PMU data early triggers the PDC buffer such that the other PMU data arrive after the PDC waiting time expiry. As Fig. 3.2-(a) illustrates, during the pre-attack condition, PMU u_1 triggers the PDC buffer and all other PMU data arrive at the PDC before expiring the initiated buffer. In contrast, in the post-TSA condition shown in Fig. 3.2-(b), the compromised PMU u_4 triggers the PDC buffer associated with T^s at time δ_{u_4} . As a result, the data of PMU u_3 , which arrives after the waiting time, will be dropped. This case only happens when a relative time alignment strategy is performed by the PDC.

This thesis assumes that PDCs employ the relative time-alignment strategy to not only investigate the worst-case TSAs but also include both the above-mentioned conditions in the formulation and implementation.

3.3.2 Implementation of The Attack

Considering the vulnerability introduced in Section 3.3, this thesis presents a TSA model against PMUs data aggregation in PDC associated with the WADC. To launch the presented attack, the attacker should be capable of (i) capturing the parameters of the under-attacked power grid to obtain the state-space representation of the entire system; (ii) estimating the expected communication delay

between PMUs and PDCs; and (iii) compromising time synchronization technologies employed by PMUs. Fig. 3.3 shows the attack implementation steps, which are elaborated in the subsequent subsections.

Obtaining state-space representation of power system: In the attack model studied in this thesis, the manipulation in the PMU measurement layer propagates throughout the system by jeopardizing the modal observability of WADCs to issue incorrect control commands to the actuators. However, the adversary does not need to obtain the control commands themselves to assess the effectiveness of the attack. Instead, to maximize the impact of the attack, the adversary aims to construct an optimal attack vector that maximizes the post-TSA dropout in PMU measurements that are critical for WADCs. On this basis, the adversary first needs to determine the critical PMU measurements. To this aim, he/she should obtain the state-space representation of the grid, i.e.,

$$x_{k+1} = Ax_k + Bu_k \quad (3.1)$$

$$y_k = Cx_k + Du_k \quad (3.2)$$

where x_k , u_k , and y_k , respectively, denote the vectors of system's states, control signals, and measurements during sampling time k ; while A , B , C , and D represent matrices of state, input control, output measurement, and feed-forward, respectively. This model is the linearized form of a set of differential-algebraic equations (DAEs) of power systems including differential equations of synchronous generators and algebraic equations of power flow around an equilibrium point [92]. In this model, system's states vector x_k can be, for instance, internal voltage, stator current, rotor angle, speed deviation, and torque of synchronous generators. Additionally, in PMU-enabled WADC schemes, y_k includes measurements of PMUs collected from the physical layer by PDCs during sampling time of k . Based on the measurements, WADCs derive control signal u_k which is sent back to the physical layer actuators, e.g., the excitation system of synchronous generators [92]. All other matrices A , B , C , and D present the relation between the system's states, measurements, and control signals based on DAEs of power system [92]. To calculate this model, the attacker can retrieve the power grid's parameters using the following techniques: (i) leveraging insiders [93], (ii) performing reconnaissance activities [94], (iii) compromising the power grid's databases [95],

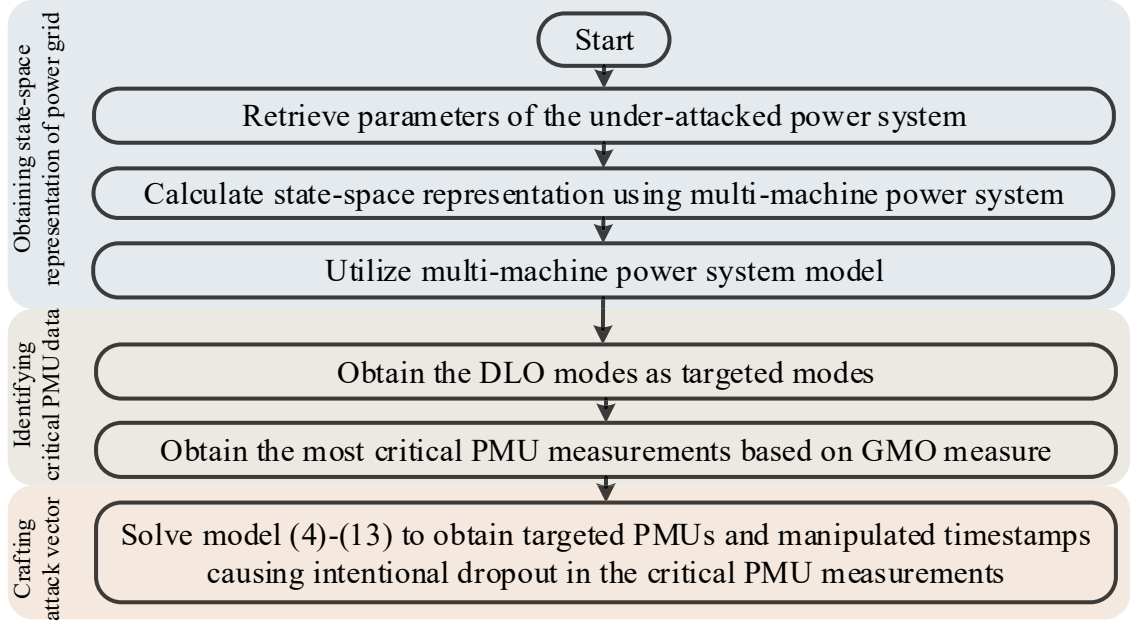


Figure 3.3: Attack implementation steps.

or (iv) using publicly available data [95]. Once the system parameters are extracted, the adversary can use multi-machine power system models in [92] to obtain (3.1)-(3.2). Although obtaining the state-space model (3.1)-(3.2) for a power grid is a challenging multi-stage task, it has been proven in several studies that adversaries can acquire this model for malicious purposes in real-world power systems. For example, the researchers in [95] demonstrated that using publicly available data circulated by the U.S. Energy Information Administration, New York Independent System Operator, and the local utility in New York, an adversary can obtain the power system's state-space of Manhattan city, USA.

Identifying critical PMU data: Once the state-space model is obtained, the adversary will be able to calculate DLO modes by conducting an eigenvalue analysis. Afterward, the adversary utilizes geometric measure of observability (GMO) to calculate the contribution of PMU measurements on the observability of DLO modes [96]. GMO is an index based on control engineering literature, which has been widely utilized to select a small subset of PMU measurements for WADCs, aiming at optimizing observability performance and streamlining the complexity of controller design [96]. The GMO for measurement signal m of PMU u associated with a targeted DLO mode o

can be calculated as follows:

$$GMO_u^m = \frac{|C_m \phi_o|}{\|C_m\| \|\phi_o\|} \quad (3.3)$$

where C_m refers to a row of the output measurement matrix C corresponding to measurement signal m , ϕ_o denotes the right eigenvectors of mode o , and $|\cdot|$ and $\|\cdot\|$ signify modulus and euclidean norms of a vector, respectively. The greater GMO for a measurement signal, the higher modal observability by that signal would be [96]. In other words, the dropout of a PMU measurement with a higher GMO, even in the presence of redundancy, can compromise the observability of oscillation modes by the WADC. This can result in incorrect control commands being sent to the system actuators, potentially impacting system stability. Therefore, the adversary aims to hinder WADC to observe the targeted DLO modes by causing intentional dropout in PMU measurements with higher GMO.

Crafting Attack Vector: To construct the TSA vector against WADCs, a stochastic MIL model is formulated from an adversary perspective considering the latency uncertainties of data transferring between PMUs and PDCs. Generally speaking, TSA vector construction approaches in the literature can be broadly categorized into two groups. The first group is a subset of false data injection attacks (FDIAs) that focus on the phase error introduced in measurement phasors due to TSAs and aims to construct attack vectors to bypass bad data detection (BDD) schemes in control centers [80, 81]. In contrast, the second group of approaches investigates the impact of TSAs on PMU data dropout by compromising the data aggregation strategies employed by PDCs [91, 97]. The TSA model proposed in this thesis aligns with the second group of approaches. What sets the proposed TSA model apart from other existing approaches is its ability to target multiple PMUs simultaneously in both attack conditions I and II in Section 3.3.1. This capability is crucial for conducting sensitivity analysis to comprehensively assess the potential consequences of TSAs. Furthermore, to the best of our knowledge, this model represents the first attempt to construct optimal TSAs specifically targeting WADCs, which are crucial PMU-enabled wide-area applications. In the presented model, the attack vector includes the targeted PMUs and their corresponding manipulated timestamp. Accordingly, the adversary's objective function is presented as follows:

$$\max_{\alpha_u, y_u} \sum_{u \in \Omega^u} \sum_{m \in \Omega^m} \sum_{c \in \Omega^c} \sum_{\omega \in \Omega^\omega} \pi_\omega (1 - v_{uc\omega}) GMO_u^m \quad (3.4)$$

which maximizes the expected data dropout in the critical PMU data identified in Section 3.3.2. This optimization is governed by Constraints (3.5)-(3.13). Constraint (3.5) presents adversary's budget limitation as he/she is able to target a limited number of PMUs [91].

$$\sum_{u \in \Omega^U} y_u = B^{max} \quad (3.5)$$

The attacker must compromise the time-synchronization mechanism of a PMU to alter its data timestamp ($y_u = 1$), which is met in Constraint (3.6).

$$-M_1 y_u \leq \alpha_u \leq M_1 y_u \quad \forall u \in \Omega^U \quad (3.6)$$

To keep the attack stealthy, the timestamp manipulation must be a factor of sampling time, as represented in (3.7).

$$\alpha_u = k_u T^s \quad \forall u \in \Omega^U \quad (3.7)$$

Meanwhile, Constraint (3.8) restricts the negative integer factor k_u in order to avoid abnormal packet duplication at PDC caused by negative timestamp manipulation ($\alpha_u < 0$).

$$k_u \geq -D^{max} \quad \forall u \in \Omega^U \quad (3.8)$$

Additionally, the data timestamp manipulation of PMU u should not exceed its minimum arrival delay to the PDC as presented in (3.9).

$$\alpha_u \leq \delta_{uc\omega} \quad \forall u \in \Omega^U, c \in \Omega^C, \omega \in \Omega^\omega \quad (3.9)$$

Based on the PMU-PDC data forwarding trees, the data transferring latency between PMU u to PDC c is calculated through Constraint (3.10).

$$\delta_{uc\omega} = \sum_{l \in \Omega^L} x_{luc} \delta_{l\omega} \quad \forall u \in \Omega^U, c \in \Omega^C, \omega \in \Omega^\omega \quad (3.10)$$

It is worth noting that, since this model approaches the problem from an adversary's standpoint, a model that adequately captures the overall network behavior and dominant trends, even with minor discrepancies in the details, is sufficient for calculating the expected latency between PMUs and PDCs. Additionally, based on a research survey, the wide-area communication network services in 26 out of 40 power utilities in the North American electric power industry are provided by independent telephone companies, third-party private networks, or private internet service providers [6]. Given that, incorporating the real-time internal data traffic of these independent/private service providers into the latency model presents significant practical challenges from an adversary standpoint. Meantime, these providers commonly use Traffic Engineering (TE) applications and protocols to control the network traffic in communication channels in a real-time manner [6]. As a result, this thesis assumes that the network traffic in the wide-area communication network is properly distributed and the latency primarily depends on data forwarding trees rather than fluctuations in network traffic. Nevertheless, assuming all detailed information of wide-area communication network is available for an adversary, the latency equation (3.10) can be replaced with the corresponding traffic-dependent one in the literature, e.g., [98]. Given that the relative time alignment strategy is deployed at PDC, the time-stamped PDC buffer is triggered while receiving the first PMU data, as presented in Constraint (3.11).

$$\tau_{c\omega}^{trig} = \min(\delta_{uc\omega} - \alpha_u) \quad \forall c \in \Omega^c, \omega \in \Omega^\omega \quad (3.11)$$

Constraint (3.12) formulates PDC relative buffer window for PMU u .

$$w_{uc\omega} = \tau_{c\omega}^{trig} + \tau_c - \delta_{uc\omega} + \alpha_u, \forall u \in \Omega^u, c \in \Omega^c, \omega \in \Omega^\omega \quad (3.12)$$

If PMU data comes after the buffer waiting time expiry, the PDC relative buffer window $w_{uc\omega}$ for that PMU becomes negative. Therefore, negative $w_{uc\omega}$ is interpreted as data loss of PMU u at PDC c in latency Scenario ω . On the contrary, positive $w_{uc\omega}$ means that the associated PMU data will be collected in the PDC buffer during Scenario ω . This thesis uses Big-M method to satisfy these

conditions as follows:

$$\frac{-w_{uc\omega}}{M_2} + \varepsilon \leq v_{uc\omega} \leq 1 + \frac{w_{uc\omega}}{M_2}, \forall u \in \Omega^U, c \in \Omega^C, \omega \in \Omega^\omega \quad (3.13)$$

in which ε signifies a small positive value. To recast the optimization model (3.4)-(3.13) into a stochastic MIL problem, Constraint (3.11) must be linearized. To this aim, a new ancillary variable $\sigma_{uc\omega}$ is defined as follows:

$$\sigma_{uc\omega} = \delta_{uc\omega} - \alpha_u \quad (3.14)$$

Accordingly, (3.15) enforces the binary ancillary variable $\gamma_{u,u'}$ associated with minimum $\sigma_{uc\omega}$ to be equal to zero.

$$\frac{\sigma_{uc\omega} - \sigma_{u'c\omega}}{M_3} \leq \gamma_{uu'} \leq 1 + \frac{\sigma_{uc\omega} - \sigma_{u'c\omega}}{M_3} \quad (3.15)$$

$$\forall u \in \Omega^u | u \neq u', c \in \Omega^c, \omega \in \Omega^\omega$$

Therefore, as presented in (3.16), trigger time of PDC buffer is equal to $\sigma_{uc\omega}$ when all $\gamma_{uu'}$ are equal to zero.

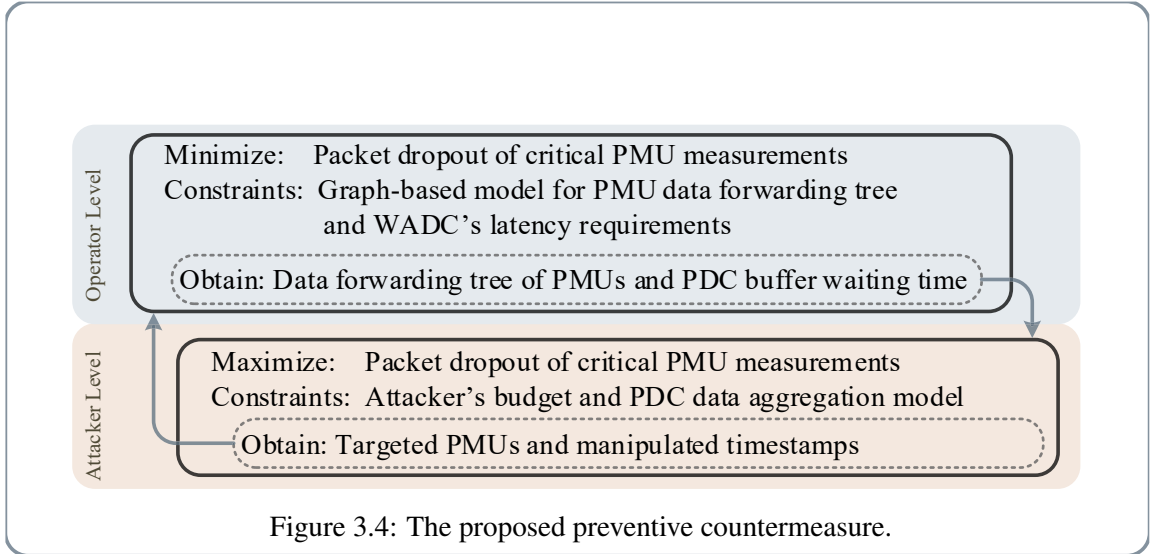
$$M_4 \sum_{u' \in \Omega^u} \gamma_{uu'} \leq \tau_{c\omega}^{trig} - \sigma_{uc\omega} \leq M_4 \sum_{u' \in \Omega^u} \gamma_{uu'} \quad (3.16)$$

$$\forall u \in \Omega^u, c \in \Omega^c, \omega \in \Omega^\omega$$

By replacing Constraint (3.11) with a set of Constraints (3.14)-(3.16), the attack model is recast to a stochastic MIL problem. The presented model (3.4)-(3.16) can be a generic TSA construction model while changing the purpose of the attack objective (3.4). Therefore, the TSA model can be solved for different purposes, grid operations, PMU-PDC communication structures, and sampling times, to name a few.

3.4 Proposed Countermeasure

Based on the introduced attack model in Section 3.3, data dropout after TSA heavily relies on (i) PDC time-alignment strategy, (ii) PDC buffer waiting time, and (iii) PMUs data arrival time at PDCs, which depends on PMU-PDC data forwarding trees. As a simple defense security approach,



PDCs can randomly switch between time-alignment strategies to reduce the post-TSA data dropout. However, this defense approach alone cannot provide comprehensive security, as both relative and absolute time-alignment strategies remain vulnerable to the post-attack Condition I presented in Section 3.3.1. As a result, additional defense approaches must be employed to ensure the secure data aggregation process at the PDC level against TSAs. Apparently, the longer PDC buffer waiting time, the less data dropout after TSA would be. However, increasing the PDC buffer waiting time stretches the overall end-to-end delay for PMUs data aggregation, affecting WADC performance detrimentally. In addition, reconfiguring the PMU-PDC data forwarding trees can rearrange PMU data arrival at PDCs in order to avoid data dropout in critical PMU measurement even after launching a well-designed stealthy TSA. Therefore, PDC buffer waiting time τ_c and PMU-PDC data forwarding trees x_{luc} are considered as two operator's defense decision variables in this thesis. To co-optimize these two variables, the operator needs to be aware of the attacker's decision including targeted PMUs y_u and manipulated timestamps α_u . This interaction between the operator and the attacker is formulated as a min-max robust optimization model, as described in Fig. 3.4. It is worth noting that, in practice, the PDC buffer waiting time is a fixed parameter that is adjusted based on the quality and completeness of the PMU data, taking into account the communication latency and wide-area applications' latency requirements. The proposed preventive countermeasure also aligns with the common practice in the industry, since it calculates a fixed waiting time for the entire PDC operation. In fact, this preventive countermeasure goes a step further by considering the presence of TSAs and models the interaction between the operator and attacker to determine the appropriate PDC buffer waiting time.

3.4.1 Model to Optimize Preventive Countermeasure

The operator's objective function is to minimize the expected data dropout of critical PMU measurement after launching the worst TSA, as formulated in (3.17). This objective function is subjected to the attacker constraints, i.e., (3.5)-(3.10) and (3.12)-(3.16), and the operator constraints, i.e., (3.18)-(3.22).

$$\min_{x_{luc}, \tau_c} \max_{\alpha_u, y_u} \sum_{u \in \Omega^u} \sum_{m \in \Omega^m} \sum_{c \in \Omega^c} \sum_{\omega \in \Omega^\omega} \pi_\omega (1 - v_{uc\omega}) G M O_u^m \quad (3.17)$$

s.t. Constraints (3.5)-(3.10) and (3.12)-(3.16)

$$\tau_{c\omega}^{trig} + \tau_c \leq \delta^{max} \quad (3.18)$$

$$\sum_{l' \in \Omega^l} A_{ll'} x_{l'uc} - x_{luc} \geq 0 \quad \forall l \in \Omega^\dagger, c \in \Omega^c \quad (3.19)$$

$$\sum_{l \in \Omega^l} A_{nl} x_{luc} \leq 1 \quad \forall n \in \Omega^\circ, c \in \Omega^c \quad (3.20)$$

$$\sum_{l' \in \Omega^l} A_{ll'} x_{l'uc} - 2x_{luc} \geq 0 \quad \forall l \in \{\Omega^l - \Omega^\dagger\}, c \in \Omega^c \quad (3.21)$$

$$\sum_{l \in \Omega^l} A_{nl} x_{luc} \leq 2 \quad \forall n \in \{\Omega^n - \Omega^\circ\}, c \in \Omega^c \quad (3.22)$$

The WADC latency requirement is satisfied by (3.18). Constraints (3.19)-(3.22) employ graph theory to construct a data forwarding tree between PMUs and PDCs in communication network graph G . Constraints (3.19)-(3.20) are applied on communication links $\Omega^\dagger$ and nodes Ω° that are directly connected to PMUs and PDCs. These two constraints present that if Link l is selected for transmitting data of PMU u to PDC c ($x_{luc} = 1$), at least one neighbor link must be selected and the degree of the connected node must be less than one, respectively. In contrast, Constraints (3.21)-(3.22) are considered for other communication links and nodes, where by selecting Link l , at least two neighbor links must be selected and degree of the connected node must be less than two.

Algorithm 1: Adopted C&CG approach

Initialization: set $x_{luc}^{(0)*}, \tau_c^{(0)*}, \mathbf{LB} = -\infty, \mathbf{UB} = \infty$, and $\text{it} = 1$

while $\mathbf{UB} - \mathbf{LB} \leq \varepsilon$ **do**

 Solve the following SP:

$$\mathbf{Q}(x_{luc}^{(\text{it}-1)*}, \tau_c^{(\text{it}-1)*}, \alpha_u^{(\text{it})}, \mathbf{z}_\omega^{(\text{it})}) = \max_{\alpha_u, \mathbf{z}_\omega} \sum_{\omega \in \Omega^\omega} \pi_\omega \mathbf{d}^T \mathbf{z}_\omega \quad (3.23)$$

$$\text{s.t.} \quad \mathbf{B} \mathbf{z}_\omega^{(\text{it})} = \mathbf{b}_2 \quad (3.24)$$

$$\mathbf{E} \alpha_u^{(\text{it})} + \mathbf{F} \mathbf{z}_\omega^{(\text{it})} \leq \mathbf{b}_3 - \mathbf{C} x_{luc}^{(\text{it}-1)*} - \mathbf{D} \tau_c^{(\text{it}-1)*} \quad \forall \omega \quad (3.25)$$

Update $\mathbf{UB} = \min\{\mathbf{UB}, \mathbf{Q}(x_{luc}^{(\text{it}-1)*}, \tau_c^{(\text{it}-1)*}, \alpha_u^{(\text{it})}, \mathbf{z}_\omega^{(\text{it})})\}$ Add following C&CG cuts to the MP:

$$\eta^{(\text{it})} \geq \sum_{\omega \in \Omega^\omega} \pi_\omega \mathbf{d}^T \mathbf{z}_\omega^{(\text{it})*} \quad (3.26)$$

$$\mathbf{C} x_{luc}^{(\text{it})} + \mathbf{D} \tau_c^{(\text{it})} \leq \mathbf{b}_3 - \mathbf{E} \alpha_u^{(\text{it})*} - \mathbf{F} \mathbf{z}_\omega^{(\text{it})*} \quad \forall \omega \quad (3.27)$$

 Solve the following MP:

$$\min_{x_{luc}^{(\text{it})}, \tau_c^{(\text{it})}, \eta^{(\text{it})}} \eta^{(\text{it})} \quad (3.28)$$

$$\text{s.t.} \quad \mathbf{A} x_{luc} \leq \mathbf{b}_1 \quad (3.29)$$

$$\eta^{(\text{it})} \geq \sum_{\omega \in \Omega^\omega} \pi_\omega \mathbf{d}^T \mathbf{z}_\omega^{(\text{it})*} \quad \forall \mathbf{k} \leq \text{it} \quad (3.30)$$

$$\mathbf{C} x_{luc}^{(\text{it})} + \mathbf{D} \tau_c^{(\text{it})} \leq \mathbf{b}_3 - \mathbf{E} \alpha_u^{(\text{it})*} - \mathbf{F} \mathbf{z}_\omega^{(\text{it})*} \quad \forall \omega, \mathbf{k} \leq \text{it} \quad (3.31)$$

 Obtain the optimal solution $(x_{luc}^{(\text{it})*}, \tau_c^{(\text{it})*}, \eta^{(\text{it})*})$,

 Update $\mathbf{LB} = \eta^{(\text{it})*}$, and $\text{it} = \text{it} + 1$

end

Terminate with the optimal $x_{luc}^{(\text{it})*}, \tau_c^{(\text{it})*}, \alpha_u^{(\text{it})*}$ and $\mathbf{z}_\omega^{(\text{it})*}$.

3.4.2 Methodology to solve Preventive Countermeasure Model

The proposed min-max robust optimization can be written in the following standard compact form:

$$\min_{x_{luc}, \tau_c} \overbrace{\max_{\alpha_u, \mathbf{z}_\omega} \sum_{\omega \in \Omega^\omega} \pi_\omega \mathbf{d}^T \mathbf{z}_\omega}^{\mathbf{Q}(x_{luc}, \tau_c, \alpha_u, \mathbf{z}_\omega)} \quad (3.32)$$

s.t.

$$\mathbf{A} x_{luc} \leq \mathbf{b}_1 \quad (3.33)$$

$$\mathbf{B} \mathbf{z}_\omega = \mathbf{b}_2 \quad (3.34)$$

$$\mathbf{C} x_{luc} + \mathbf{D} \tau_c + \mathbf{E} \alpha_u + \mathbf{F} \mathbf{z}_\omega \leq \mathbf{b}_3 \quad \forall \omega \quad (3.35)$$

in which $\mathbf{z}_\omega$ represent attacker-level decision variables and $\mathbf{Q}$ denotes attacker-level objective function in accordance with operator defense decision variables x_{luc} and τ_c . Additionally, $\mathbf{A}$ and $\mathbf{b}_1$ are

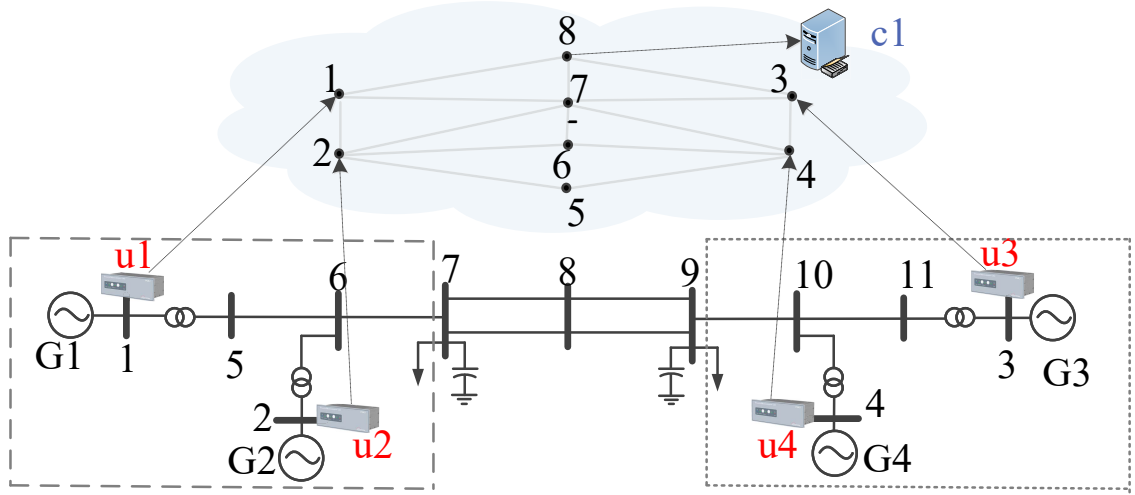


Figure 3.5: Two-Area Kundur test system.

coefficient matrix and constant vector associated with the operator-level constraints (3.18)-(3.22); and $\mathbf{B}$ and b_2 signify coefficient matrix and constant vector of the attacker-level constraints (3.5)-(3.9) and (3.13)-(3.16), respectively. Eventually, $\mathbf{C}$, $\mathbf{D}$, $\mathbf{E}$, and $\mathbf{F}$ are coefficient matrices and b_3 is constant vector corresponding to the constraints that combine decision variables of the operator-level and the attacker-level, including (3.10) and (3.12).

The proposed min-max robust model can be solved by developing KKT conditions and decomposition techniques, e.g., Benders and CC&G. However, extensive binary variables in the attacker-level violate the optimality of KKT conditions and duality condition required for Benders decomposition technique [99]. Therefore, this thesis employs CC&G technique since it (i) can deal with binary variables at the attacker-level and (ii) leads to superior convergence performance [99]. In this technique, the operator-level and attacker-level problems are respectively considered as master problem (MP) and sub-problem (SP), which are solved iteratively. As shown in Algorithm 1, in each iteration, the SP constructs TSA vector α_u based on the optimal operator defense decisions in the previous iteration. Then, the optimal TSA vector is utilized to create dynamic optimality cuts of equations (3.26) and (3.27). Afterward, the MP optimizes the operator defense decisions by adding the created cuts. This iterative procedure continues till the solutions of two problems converge to a specific value. The studies in [99] demonstrated that the CC&G technique can converge in a timely and effective manner.

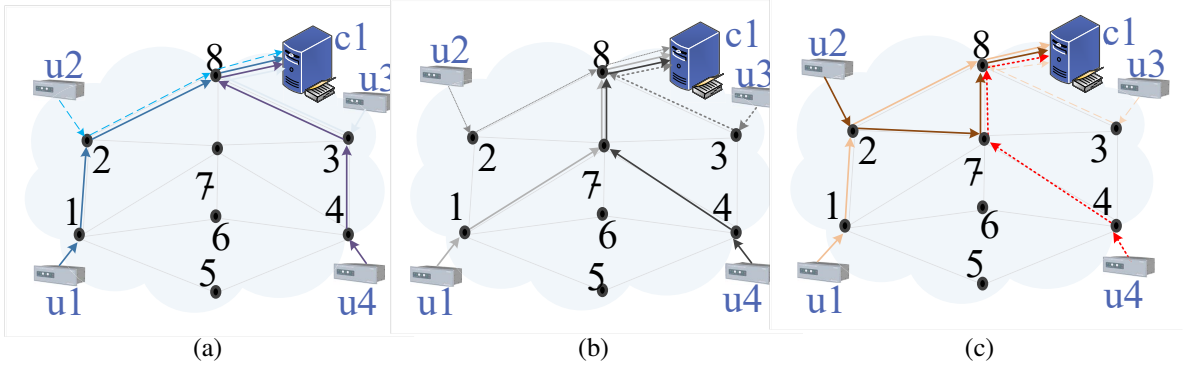


Figure 3.6: PMU-PDC data forwarding trees in Two-Area Kundur for Scenarios (a) S1, (b) S2, and (c) S3.

Table 3.1: Expected PMU-PDC Delay in Two-Area Kundur (ms).

PMUs	S1	S2	S3	PMUs	S1	S2	S3
u1	37	37	58	u3	52	52	52
u2	55	50	55	u4	66	52	52

3.5 Results and Discussion

This section investigates the impacts of the presented TSA model and evaluates the effectiveness of the proposed preventive countermeasure on Two-Area Kundur and New England 39-bus grids. It is assumed that each of these systems is equipped with a WADC comprising of state-feedback control integrated with a state observer, both designed optimally using Linear Quadratic Regulator (LQR) technique [96]. The performance of the WADC under the presented TSA model is discussed using the following three scenarios, for which the PMU-PDC data forwarding trees are designed based on

- **S1**- Shortest path technique [100], where minimum routers and communication links are used;
- **S2**- minimized overall delay for data transmission [101]; and
- **S3**- proposed preventive countermeasure.

In this thesis, inter-area oscillation modes are considered as DLO modes targeted by the adversary. Inter-area DLO modes are among slow and long-lasting oscillations that occur between synchronous generators in different interconnected areas following a power system contingency [90]. In such circumstances, mal-operation of WADCs regarding these modes can have severe implications for power system stability. Inter-area oscillations typically occur at the frequency range 0.1

Table 3.2: Optimal Attack Vector in Two-Area Kundur

Scenario	τ_c (ms)	Overall Delay (ms)	TSA vector (ms)	P_u^{drop}			
				u1	u2	u3	u4
S1 [100]	40	77	$\alpha_{u1}=24.99$	0	0.443	0.341	0.678
	50	87	$\alpha_{u4}=-24.99$	0	0	0	0.691
	60	97	$\alpha_{u4}=-24.99$	0	0	0	0.201
	70	107	$\alpha_{u1}=-8.33$	0	0	0	0
S2 [101]	40	77	$\alpha_{u1}=24.99$	0	0.366	0.475	0.511
	50	87	$\alpha_{u3}=-16.66$	0	0	0.125	0
	60	97	$\alpha_{u4}=-24.99$	0	0	0	0.083
	70	107	$\alpha_{u4}=-24.99$	0	0	0	0.027
S3	33	85	$\alpha_{u1}=33.32$	0	0.117	0	0
	40	92	$\alpha_{u3}=-24.99$	0	0	0	0

to 1 Hz with the damping ratio of less than 5% [90]. In the attack model discussed in Section 3.3, the adversary can prevent the WADC to effectively observe these DLO modes and make appropriate control decision if he/she succeeds to intentionally drop the identified critical measurements. Therefore, to mathematically evaluate if the manipulated PMU timestamps achieve the purpose of the attack, this thesis uses the dropout probability in critical measurement data caused by the crafted TSA vector, as follows:

$$P_u^{drop} = \frac{\sum_{c \in \Omega^c} \sum_{\omega \in \Omega^\omega} v_{uc\omega}^*}{N_\omega} \quad (3.36)$$

where $v_{uc\omega}^*$ refers to aggregation status of PMU u obtained in the attack model, and N_ω signifies number of delay scenarios. The TSA vector construction problem and the proposed model for the preventive countermeasure are solved by CPLEX solver of GAMS software with 0.001% optimality gap on a PC with Intel Core i7 and 16GB RAM. Additionally, to investigate the consequences of the crafted TSA on system stability, this thesis performs time-domain analyses.

3.5.1 Case-I: Two-Area Kundur Test System

Fig. 3.5 depicts the schematic of the under-study grid as well as PMU locations and the communication system. This system comprises four 900 MVA synchronous generators which are located in two areas interconnected with two 230 kV transmission lines. Each generator is equipped with a steam turbine and governor as well as an IEEE type-1 DC excitation system. The system data can be

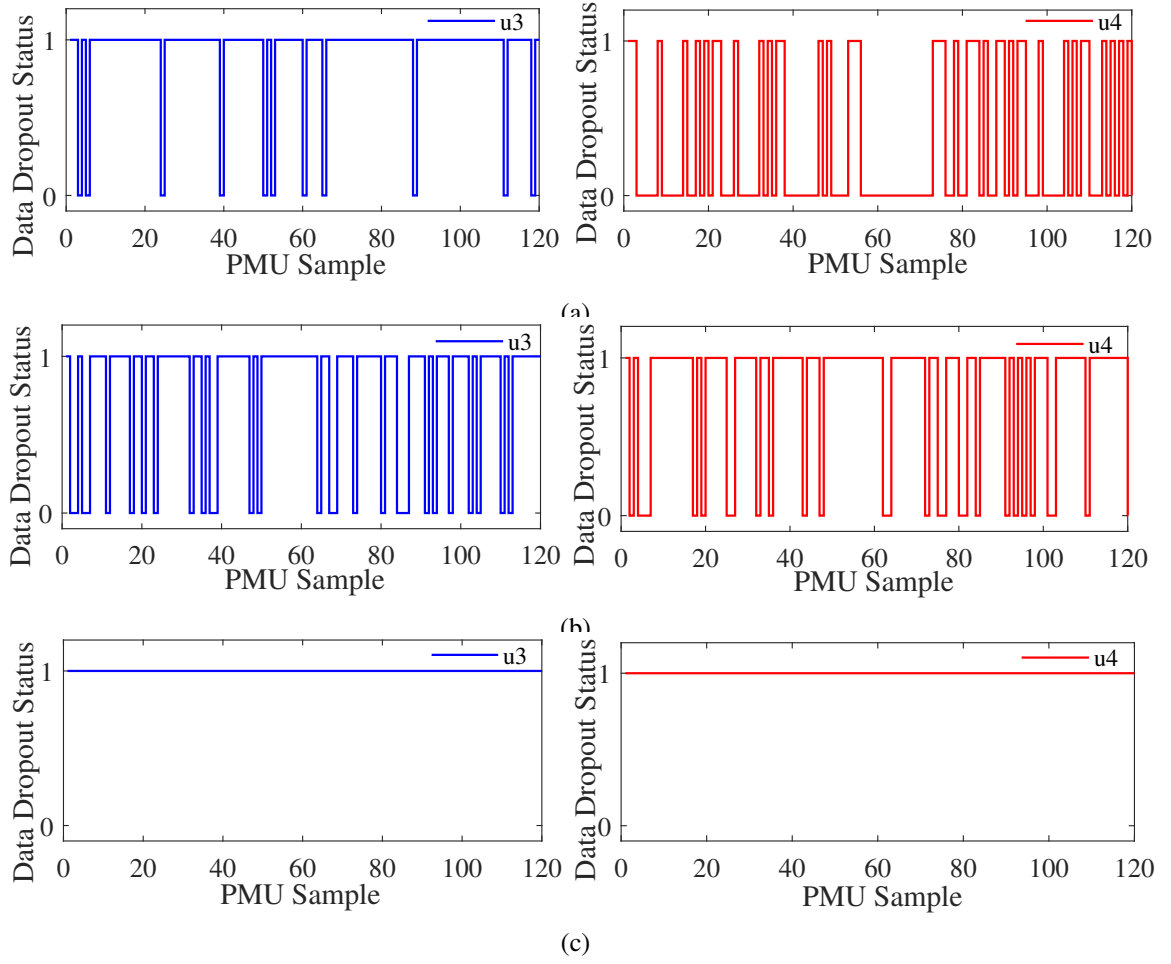


Figure 3.7: Post-attack dropout status of the critical PMUs u_3 and u_4 in Two-Area Kundur during Scenarios (a) S1: $\tau_c=40$ ms, (b) S2: $\tau_c=40$ ms, and (C) S3: $\tau_c=33$ ms or 40 ms

found in [102]. Using four PMUs, the speed deviations of the generators are provided to WADC as the input signals, and the control commands are sent back to the generators' excitation systems [96]. The disturbance studied in this case is a three-phase short circuit fault on a line between Buses 7 and 8, which is isolated from the grid after 20 ms. The adversary follows the implementation steps described in Fig. 3.3. They also obtain a pair of DLO modes, i.e., $o_1 = -0.105 \pm 4.024i$ for the system. Based on eigenvalue analysis, PMUs u_3 and u_4 have more contribution in observing the targeted DLO modes since they have relatively higher GMO equal to 1.0 and 0.996, respectively. Therefore, the adversary aims to maximize the dropout of these two PMU data by manipulating the timestamp of a single PMU data.

The PMU-PDC data forwarding trees and resultant expected transmitting delay in each routing

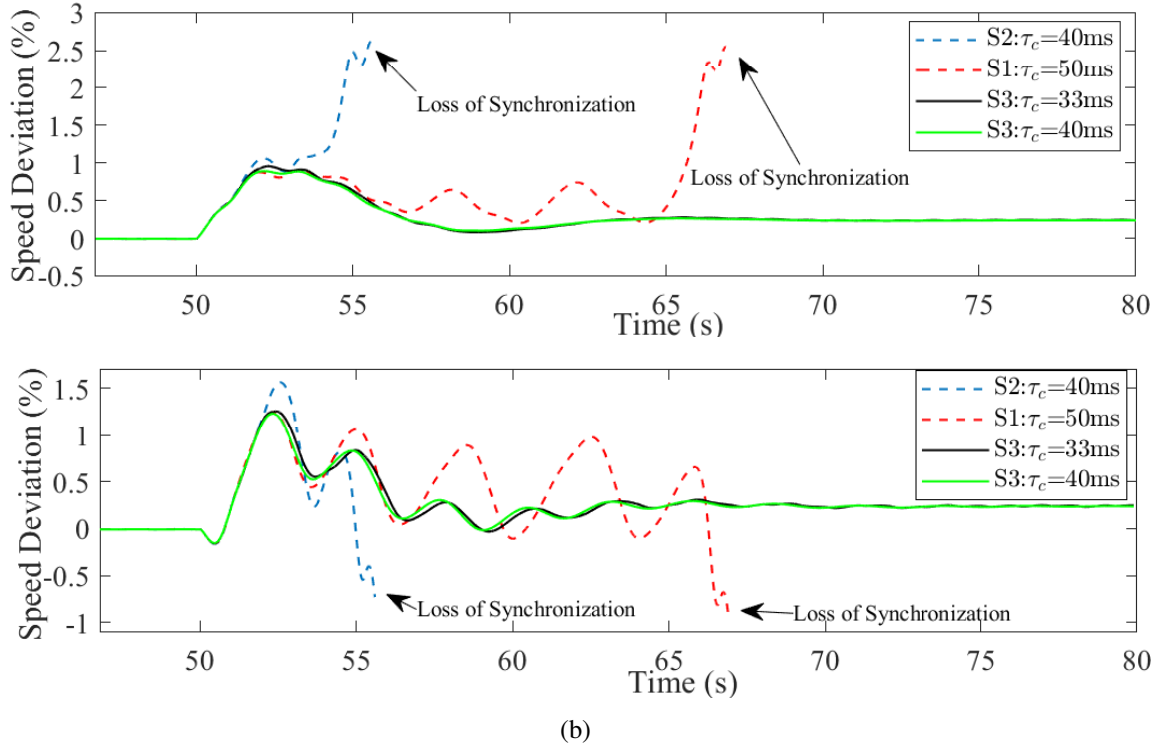


Figure 3.8: Post-attack Two-Area Kundur's WADC performance for generators (a) G1 and (b) G3.

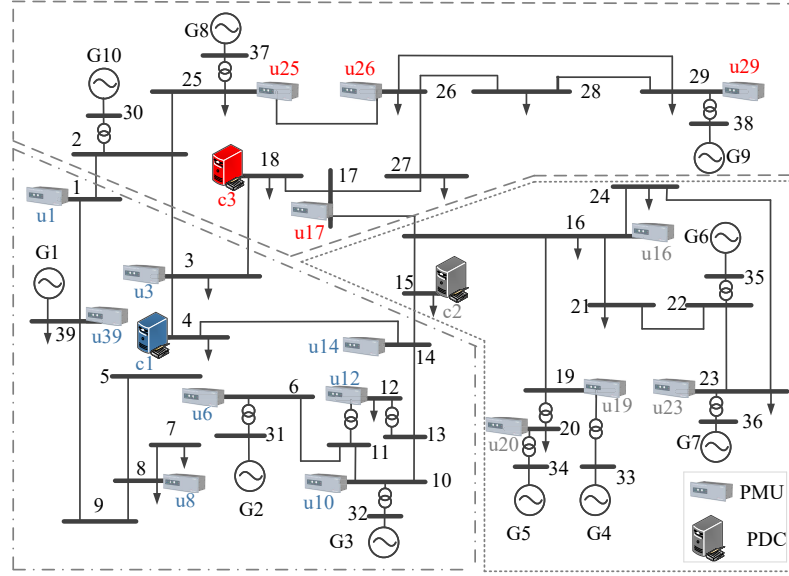


Figure 3.9: IEEE 39-Bus test system.

scenario are shown in Fig. 3.6 and Table 3.1, respectively. Table 4.2 also reports the targeted PMU and manipulated timestamps extracted from the attack model in the three scenarios and various PDC waiting times (τ_c). Additionally, Fig. 3.7 illustrates the post-attack dropout status of PMU data for

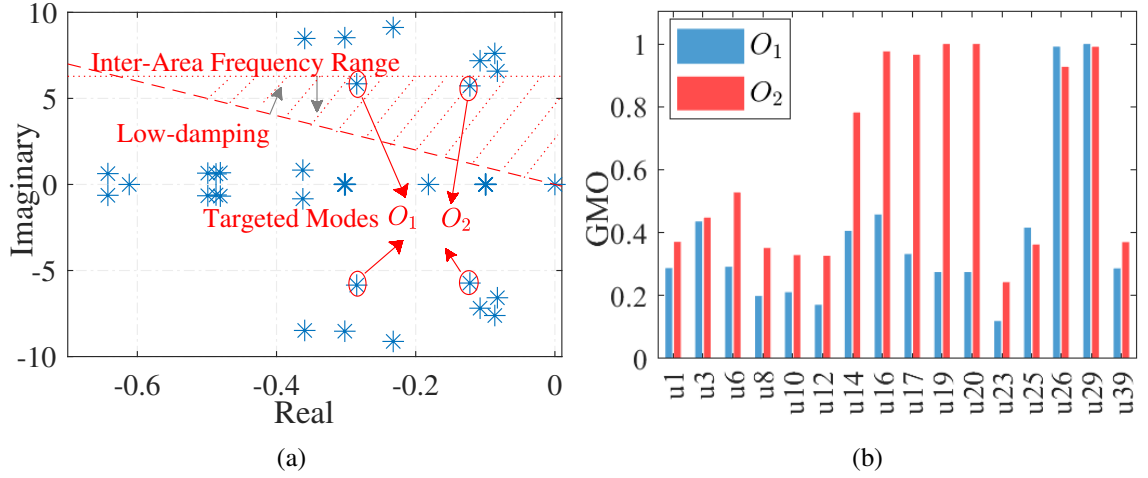


Figure 3.10: (a) Targeted modes and (b) GMO of PMU measurements in IEEE 39-Bus.

120 samples in Scenarios S1-S3. Based on Table 4.2 and Fig. 3.7, the proposed countermeasure in Scenario S3 effectively prevents the adversary from intentionally dropping the measurements of PMU u_3 and u_4 which are critical for the WADC modal observability. Fig. 3.8 shows the post-attack speed-deviation of Generators G1 and G3, which are located in different interconnected area, during Scenarios S1-S3. It can be observed that the proposed technique in Scenario S3 ensures the stability of the grid with a low PDC waiting time, i.e., 40 ms. However, in Scenarios S1 and S2, the system loses its synchronization for PDC waiting time of 50 ms and 40 ms, respectively. For a higher value of waiting time, Scenarios S1 and S2 can stabilize the grid, however, it comes at the cost of delay in control loops and low damping performance.

3.5.2 Case-II: IEEE 39-Bus Test System:

The single-line diagram of New England 39-bus system along with the PMU and PDC locations have been shown in Fig. 3.9. The entire system measurements are provided by 16 PMUs whose location is assumed based on optimal placement in [103]. Inspired from [104], since this system comprises three areas, this thesis also considers three local PDCs for aggregation of the regional PMU data. Without loss of generality, these three PDCs are located in Buses 4, 15, and 18. The deployed communication network has the same configuration as the power system, where there is a router and link corresponding to each bus and line [105]. Based on the method in [96], the WADC is designed considering three input active power measurements provided by PMUs u_{20} , u_{26} , and

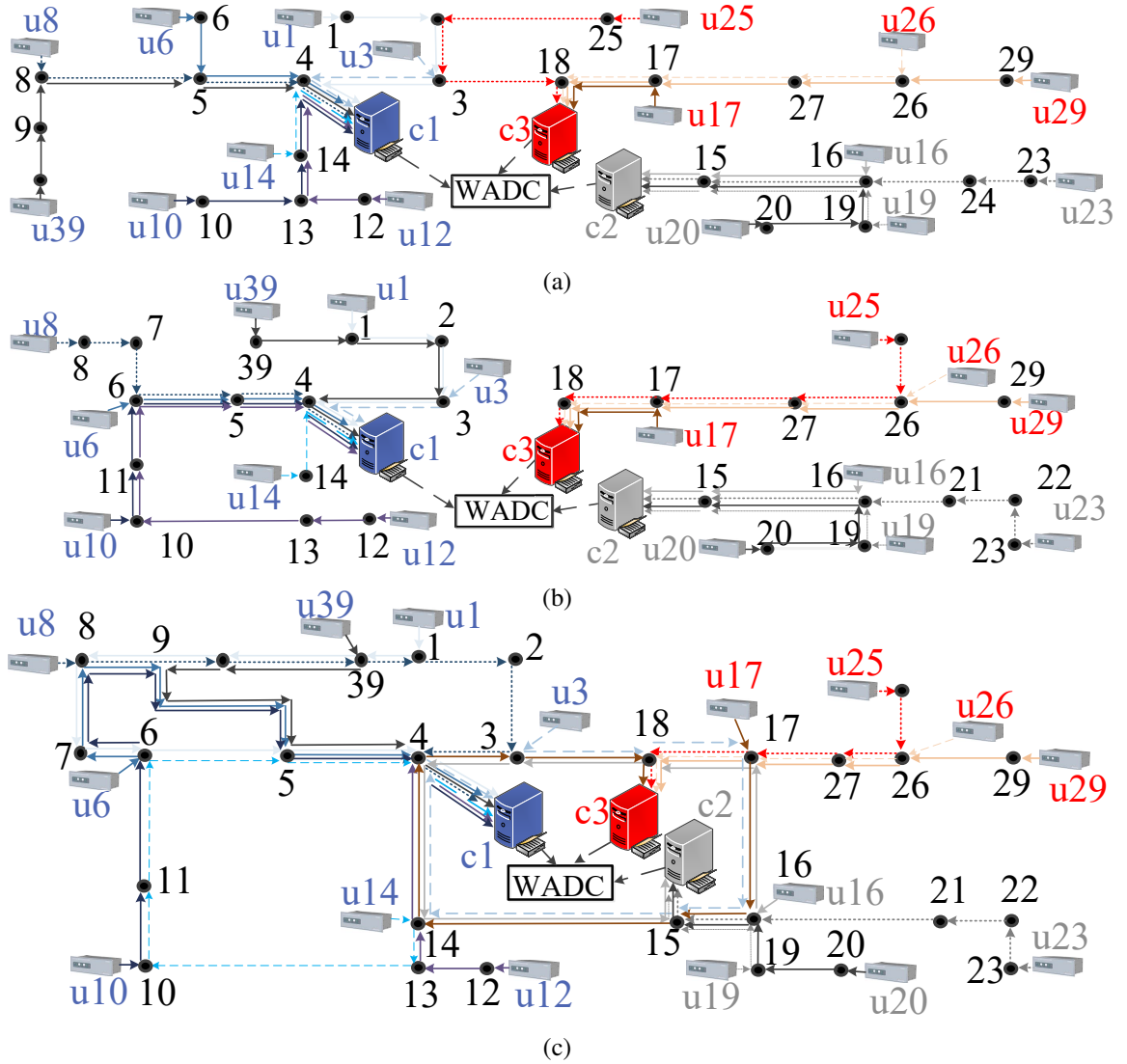


Figure 3.11: PMU-PDC data forwarding trees in IEEE 39-Bus for Scenarios (a) S1, (b) S2, and (c) S3.

u_{29} , and three output control signals modulating the voltage reference of generators G_2 , G_5 , and G_9 . The TSA model's impacts on the WADC are investigated following a three-phase short-circuit fault on Line 28-26 at $t = 50$ s cleared at $t = 50.05$ by isolating the line.

Through retrieving the state-space of the system and performing eigenvalue analysis, the adversary determines two pairs of DLO modes, i.e., $o_1 = -0.28 \pm 5.84i$ and $o_2 = -0.12 \pm 5.72i$, as targeted modes shown in Fig. 3.10-(a). As Fig. 3.10-(a) illustrates, these two pairs of modes are located in the region visualizing the frequency and damping ratio range of inter-area DLO modes. Afterward, to compromise the WADC to observe these two pairs of oscillation modes, the adversary

Table 3.3: Expected PMU-PDC Delay in IEEE 39-Bus (ms)

PMUs	S1	S2	S3	PMUs	S1	S2	S3
u1	37	37	68	u16	30	30	51
u3	25	25	59	u19	41	41	41
u6	38	38	60	u20	50	50	50
u8	51	47	58	u23	54	52	52
u10	52	46	67	u17	28	28	50
u12	58	57	58	u25	67	53	53
u14	26	26	60	u26	39	39	39
u39	58	52	58	u29	50	50	50

Table 3.4: Optimal Attack Vector in IEEE 39-Bus for Single TSA Condition

Approach	τ_c (ms)	Overall Delay (ms)	TSA Vector (ms)	P_u^{drop}				
				u12	u20	u25	u29	u39
S1 [100]	40	70	$\alpha_{u17}=8.33$	0	0	0.608	0.359	0
	50	80	$\alpha_{u20}=-24.99$	0	0.514	0	0	0
	60	90	$\alpha_{u3}=8.33$	0.293	0	0	0	0.469
	70	100	$\alpha_{u17}=8.33$	0	0	0.081	0	0
S2 [101]	40	70	$\alpha_{u29}=-24.99$	0	0	0	0.674	0
	50	80	$\alpha_{u29}=-16.66$	0	0	0	0.443	0
	60	90	$\alpha_{u25}=-24.99$	0	0	0.392	0	0
	70	100	$\alpha_{u25}=-24.99$	0	0	0	0	0
S3	28	86	$\alpha_{u29}=-24.99$	0	0	0	0.050	0
	40	98	$\alpha_{u29}=-24.99$	0	0	0	0	0

aims to maximize data dropout in the measurements of seven PMUs, i.e., $u14$, $u16$, $u17$, $u19$, $u20$, $u26$, and $u29$, which have higher GMO (Fig. 3.10)-(b)).

PMU-PDC data forwarding trees and expected delay in the three scenarios are illustrated in Fig. 3.11 and Table 3.3, respectively. Table 4.4 and Table 3.5 also report the extracted targeted PMU and manipulated timestamps as well as the post-attack PMU data dropout probability in single and multiple attack conditions, respectively. As Fig. 3.3 reports, in Scenario S3, the difference between the first and last PMU arrival delay at PDCs is minimized. Meanwhile, the PMUs' data arrival time at the PDCs are rearranged such that the adversary is restricted to cause severe data dropout in the critical PMU data used in the WADC as reported in Table 4.4 and Table 3.5. It is worth noting that, in post-attack Condition I in Section 3.3.1, the dropout status of PMU data depends on their arrival time at the PDC. For instance, based on Table 4.4, in Scenario S1 when PDC waiting time is set to 40 ms, the adversary changes the timestamp of PMU $u17$ by 24.99 ms to drop data of PMUs $u25$

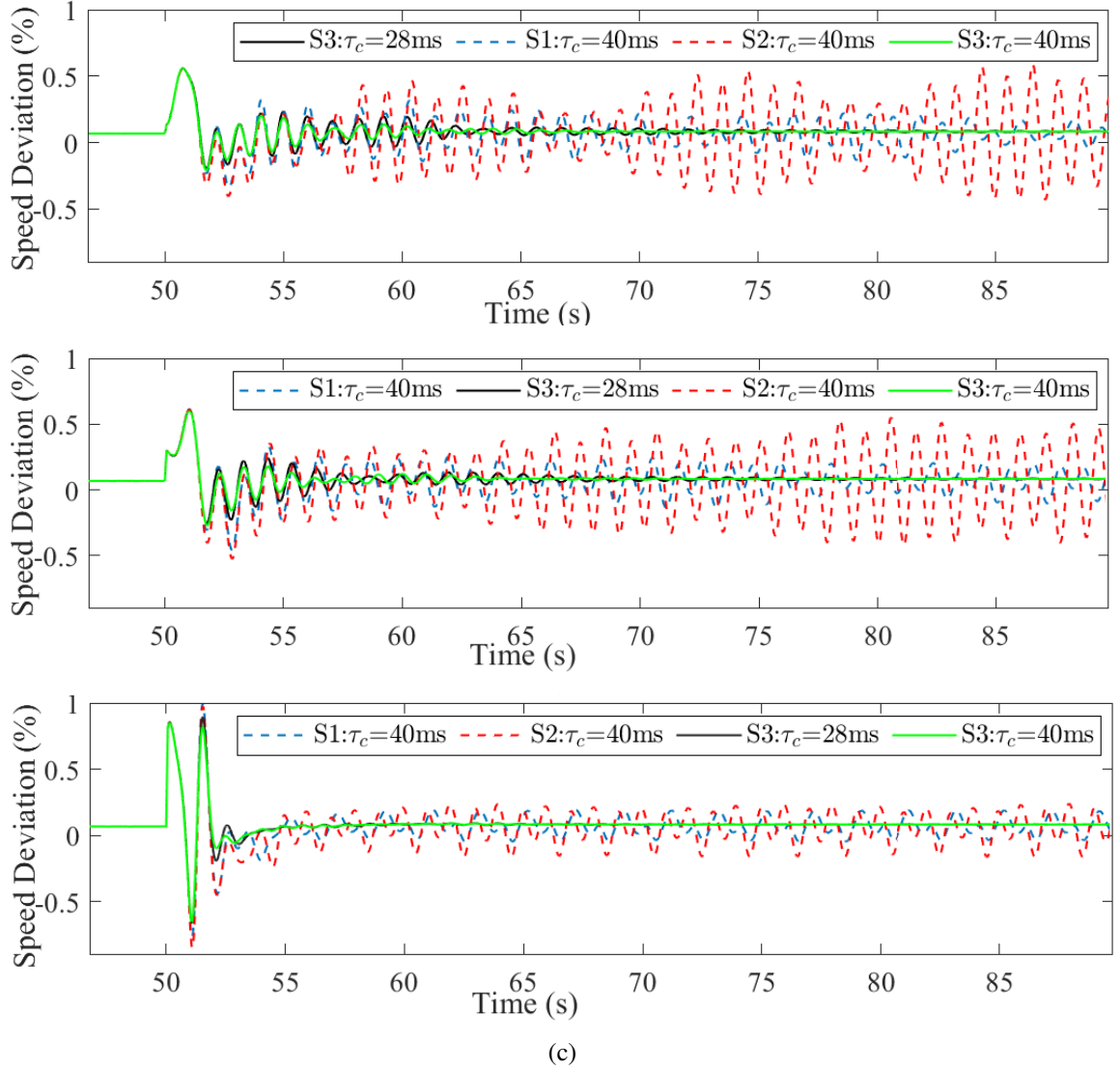


Figure 3.12: Post-attack 39-bus WADC performance for Generators (a) G2, (b) G5, and (c) G9 during single TSA.

and u_{29} at PDC c_3 . Refereed to Table 3.3, in this scenario, data of PMUs u_{25} and u_{29} experience higher communication delay of 67 ms and 50 ms compared to other PMUs connected to PDC c_3 , respectively. As a result, even though PMU u_{25} is not among the most critical PMUs, its data drops since it encounters relatively higher expected communication delays compared to other PMU data. The angular speed of the Generators G2, G5, and G9 located in three different areas under single and multiple attack conditions have been illustrated in Fig. 3.12 and Fig. 3.13, respectively. It can be observed that the proposed method keeps the system stable under both single and multiple TSAs

Table 3.5: Optimal Attack Vector in IEEE 39-Bus for Multiple TSA Condition

Approach	τ_c (ms)	TSA Vector (ms)	P_u^{drop}							
			u8	u10	u12	u19	u25	u26	u29	u39
S1 [100]	40	$\alpha_{u3}=16.6$ $\alpha_{u10}=-24.9$	0.37	0.63	0.36	0	0	0	0	0.61
	50	$\alpha_{u17}=8.3$ $\alpha_{u26}=-24.9$	0	0	0	0	0	0.76	0	0
	60	$\alpha_{u17}=8.3$ $\alpha_{u26}=-24.9$	0	0	0	0	0	0.35	0	0
	70	$\alpha_{u16}=8.3$ $\alpha_{u19}=-16.6$	0	0	0	0.43	0	0	0	0
S2 [101]	40	$\alpha_{u17}=8.3$ $\alpha_{u25}=-24.9$	0	0	0	0	0.86	0.19	0.51	0
	50	$\alpha_{u17}=8.3$ $\alpha_{u26}=-24.9$	0	0	0	0	0	0.74	0	0
	60	$\alpha_{u8}=-24.9$ $\alpha_{u39}=-24.9$	0.45	0	0	0	0	0	0	0.47
	70	$\alpha_{u16}=8.3$ $\alpha_{u19}=-24.9$	0	0	0	0.32	0	0	0	0
S3	28	$\alpha_{u19}=-24.9$ $\alpha_{u20}=16.6$	0	0	0	0.19	0	0	0	0
	40	$\alpha_{u26}=-24.9$ $\alpha_{u29}=-24.9$	0	0	0	0	0	0	0	0

even for a very small PDC waiting time, i.e., 28 ms. In the other scenarios, the local power system stabilizers (PSSs) start to interact against the WADC, causing undamped oscillation after the fault.

3.5.3 Sensitivity Analysis

This subsection investigates the effectiveness of the proposed preventive countermeasure respecting different optimal and blind TSA scenarios through a sensitivity analysis. To this aim, the set of optimal TSAs is constructed by executing the presented TSA construction model, i.e., (3.4)-(3.10) and (3.12)-(3.16), in Scenarios S1-S3 under different attacker's budget and PDC buffer waiting time ranging between $B^{max} \in [1, 2, 3]$ and $\tau_c \in [20 - 100 \text{ ms}]$, respectively. In contrast, the blind TSAs set includes 500 attacks where the targeted PMUs and associated attack vectors are randomly selected within $B^{max} \in [1, 2, 3]$ and $\alpha_u \in [-24.99, 24.99]$, respectively. Fig. 3.14 shows the post-attack PMU data dropout probability in IEEE 39-Bus test system during each PMU-PDC data forwarding scenario S1-S3 under the blind and optimal TSAs. Apparently, the resultant PMU data

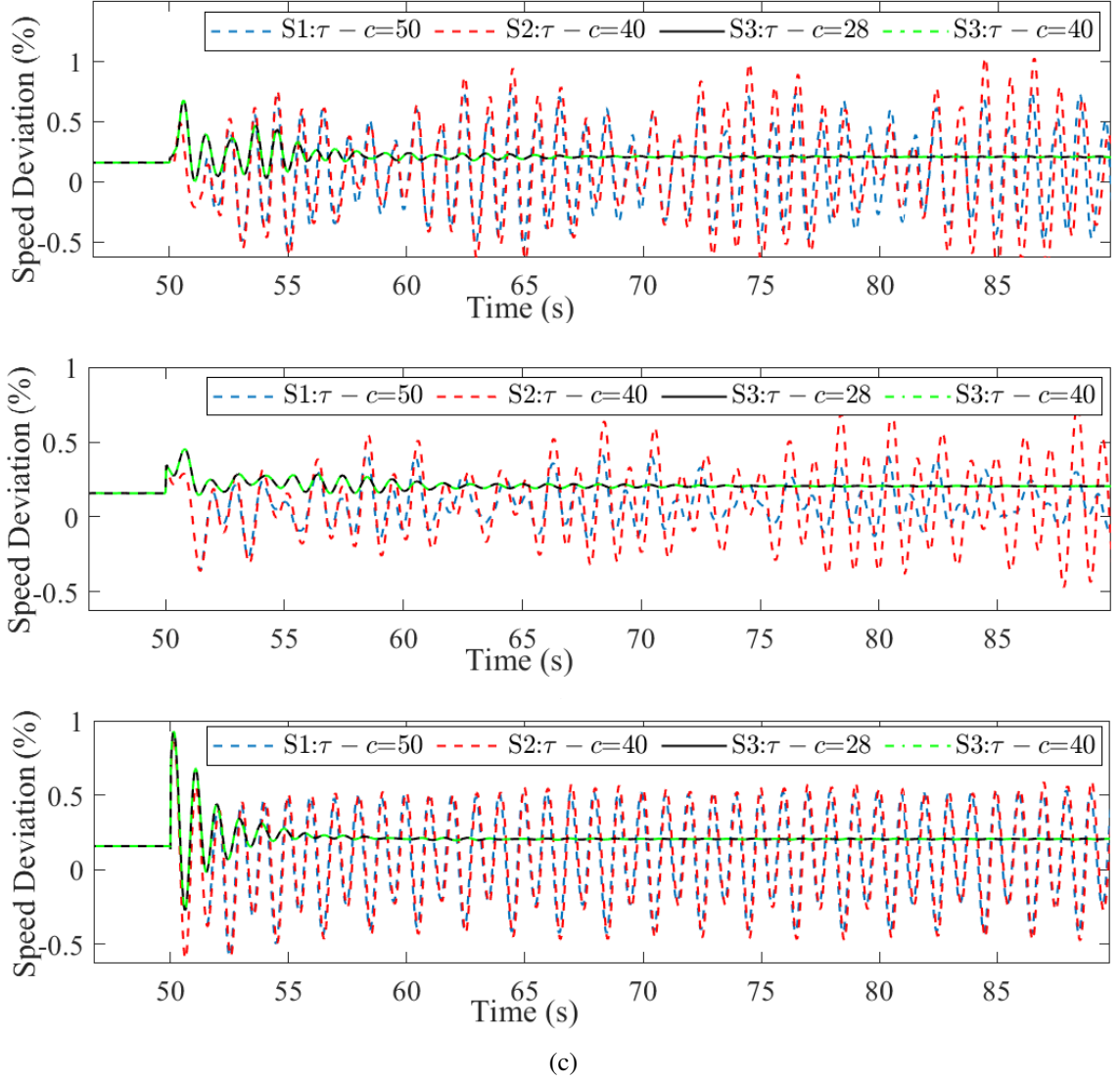


Figure 3.13: Post-attack 39-bus WADC performance for Generators (a) G2, (b) G5, and (c) G9 during multiple TSAs.

dropout during the optimal attacks (Fig. 3.14-(b)), is higher than the blind attacks (Fig. 3.14-(a)), particularly regarding PMUs with higher GMOs. The results of this sensitivity analysis, depicted in Fig. 3.14, demonstrate the superior capability of the proposed countermeasure to reduce the dropping of PMU data caused by both optimal and blind random TSAs.

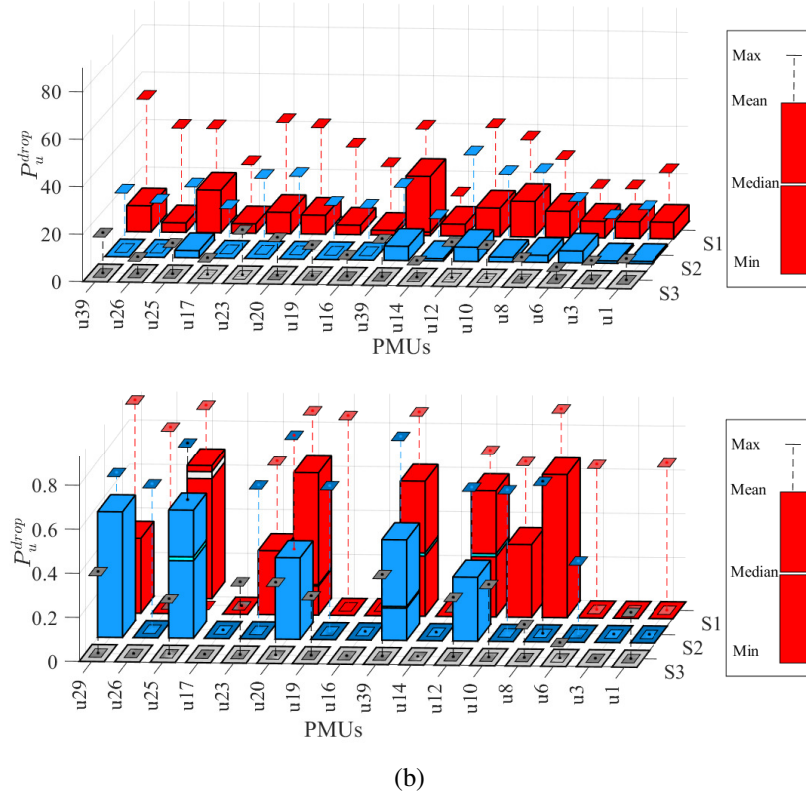


Figure 3.14: Sensitivity analysis of the presented TSA on IEEE 39-Bus: (a) blind attack, (b) optimal attack.

3.5.4 Impact of the Proposed Preventive Countermeasure on Other Wide Area Applications

Since the countermeasure proposed in this thesis focuses on PMU data aggregation in the communication layer, it is important to make sure this approach does not jeopardize the performance of other wide-area applications. Given that the majority of wide-area applications rely on state estimation [106], this thesis specifically analyzes the impact of the proposed countermeasure on this particular application. To this aim, this thesis utilizes the weighted least squares (WLS) approach to model PMU-based AC state estimation [106]. This approach solves the following problem to estimate the system states $\hat{x}$:

$$\min_{\hat{x}} [z - h(\hat{x})]^T R^{-1} [z - h(\hat{x})] \quad (3.37)$$

s.t.

Table 3.6: Performance of AC State Estimation In IEEE 39-Bus

Approach	Average $RMSE_k (\times 10^{-3})$		
	Attack Free	Blind Attack	Optimal Attack
S1 [100]	2.47	9.57	8.96
S2 [101]	2.47	8.61	8.34
S3	2.47	8.32	8.32

$$z = h(\hat{x}) + r \quad (3.38)$$

where z signifies the PMU measurement vector; $h(\cdot)$ denotes the measurement synthesizing functions; R presents the measurement error covariance matrix and r refers to the measurement noise. In the PMU-based AC state estimation method, the measurement vector z comprises phasors of bus voltage and line current at PMU locations while the system states include magnetite and phase of all bus voltages [106].

The PMU-PDC data forwarding trees and PDC waiting time driven from the proposed countermeasure under TSAs impact the data completeness of the PMU measurement vector z . To assess the performance of AC state estimation under TSAs when applying the proposed countermeasure, this thesis utilizes MCS. The employed MCS models the uncertain delay caused by the selected PMU-PDC data forwarding trees as well as the PDC data aggregation strategy to calculate post-TSA data dropout status of each PMU measurement within vector z . In each trial of MCS, the calculated PMU measurement vector z is utilized to obtain the system state $\hat{x}$ through the WLS problem (3.37). Eventually, the performance of AC state estimation in each MCS trial k is evaluated through root mean square error (RMSE) as follows:

$$RMSE_k = \sqrt{\frac{1}{N} \sum_{i=1}^N (\hat{x}_{ik} - x_{ik})^2} \quad (3.39)$$

where x_{ik} and $\hat{x}_{ik}$ denote the actual and estimated State i during trial k ; while N is the number of system states. This thesis executes this MCS on IEEE 39-Bus test system by 500 trials under different PMU-PDC data forwarding trees in Scenarios S1-S3 (Fig. 3.11) and attack conditions including attack-free, blind attack, and optimal attack. Additionally, the PDC waiting time is set to 40 ms. In each MCS trial, the blind and optimal attack vectors are uniformly selected among vectors

obtained in sensitivity analysis, i.e., Section 3.5.3. The WLS problem (3.37) is implemented using the AC state estimation module in MATLAB software. The measurement covariance error is also considered as 0.01 for all PMUs [106].

As Table 3.6 illustrates, due to the redundant measurement data, the post-attack performance of AC state estimation is not significantly degraded in all three scenarios. In the worst post-attack condition, the average RMSE only increases by 7×10^{-3} compared to the attack-free condition. Given this negligible amount, this analysis demonstrates that while the proposed countermeasure is optimized to ensure the data completeness of PMU measurements critical for WADCs, it also preserves the post-attack performance of state estimation. It should be noted that the proposed method (S3) provides less post-TSA error in state estimation compared to other scenarios (S1 and S2).

Chapter 4

Security Enhancement of WADCs- Part II

4.1 Problem Statement

Real-world incidents, e.g., [24], and experimental experiences, e.g., [12], have demonstrated that both technologies are susceptible to TSAs, which put the entire power grid at risk. TSAs on PMUs and PDCs can result in data dropout [91], phasor angle error [107], and delay [108], all of which can have a significant impact on the WADC's performance and power grid stability. In case of TSAs in power systems, the attack surface is time-synchronization schemes employed by PMUs and PDCs. In contrast to data transmission communication layer between PMUs and PDCs, the time-synchronization schemes employed in industry commonly lacks inherent authentication approaches and transport layer security (TLS) cryptographic protocol. While the latest PTP version 2.1 (IEEE 1588-2019) has introduced significant security updates including Type-Length-Value (TLV) authentication and the use of Media Access Control Security (MACsec) and IP Security (IPsec), these measures still leave PTP vulnerable to TSAs orchestrated by internal attackers with network or encryption keys access [109]. Additionally, these authentication measures are ineffective against delay attacks, especially those launching at the physical layer of PTP schemes [110]. Notably, the GPS-based time-synchronization systems commonly used in real-world power grids lack built-in

authentication security, making them vulnerable to TSAs. While there have been proposals for implementing cryptographic authentication methods to address this vulnerability, these methods often require significant changes to the existing GPS signal coding structure, which is unlikely to happen in the short term [111, 112]. More recent cryptographic techniques such as navigation message authentication (NMA) and signal authentication sequences (SAS) offer solutions that require minimal modifications to the current system and effectively combat signal spoofing, but they do not protect against unauthorized signal access and replay attacks [113]. Therefore, alongside device-level and communication-level data authentication, the implementation of a high-level detection and mitigation mechanism, as proposed in this research, becomes imperative to make the entire power grid resilient to potential TSAs.

4.2 Literature Review and Research Gaps

TSA detection and mitigation approaches have gained significant attention in recent literature. As illustrated in Table 4.1, the detection approaches can be grouped into two categories, i.e., device-level and system-level approaches. The device-level detection approaches use the features of time synchronization technology signals, e.g., code phase and carrier frequency, to realize malicious TSAs in local PMUs/PDCs. For instance, a model-based detection scheme was proposed in [114] using separate clock drift-matched filter methodology. More recently, two signal filters based on double exponential smoothing and signal quality monitor statistics were proposed in [115] and [116]. Additionally, the authors of [117] leveraged the coherency between the PMU clock's carrier frequency manipulations and the resulting phase angle change. In contrast, the system-level approaches leverage collected PMU data at control centers to recognize abnormal post-TSA phase angle errors based on power system equations. On this basis, two residual model-based GPS spoofing attack detection were proposed in [118] and [119] using Kalman filter and static state estimation, respectively. A TSA pattern recognition method was proposed in [120] based on post-attack phase angle deviation between the PMUs located at two sides of the transmission line. The authors in [85] proposed a robust PMU angle deviation detection and correction approach, which can be used to compensate for the manipulated phase angles after TSAs. The authors in [2] proposed a neural

Table 4.1: TSA Detection Approaches in The Literature

Category		Device-Level		System-Level	
Location		PMU/PDC		control center	
Approach		model based [114–116]	data driven [117]	model based [118–120]	data driven [2, 121]
Features	Utilized correlation between aggregated PMU data based on power system equations			✓	✓
	Utilized specific features of time synchronization technology signals	✓	✓		
Drawbacks	Failed to detect TSA on PDCs' time synchronization schemes			✓	✓
	Build based on NMSE and relied on residual threshold	✓		✓	
	Low computational efficiency			✓	✓
	Failed to take advantages of data quality information available at PDC level	✓	✓	✓	✓
	Lack of integrated mitigation approach	✓	✓	✓	✓

network-based detection model while introducing “phase coding” as the input features. The authors in [121] proposed the use of graph signal processing for modeling power grids which captures features suitable for learning-based TSA detection and localization approaches. These studies provide significant progress in securing wide-area applications, e.g., WADCs, against TSAs. However, as illustrated in Table 4.1, they suffer from at least one of the following drawbacks: (i) they fail to detect TSAs against time synchronization technologies of PDCs, (ii) they rely on normalized mean square error (NMSE) and residual threshold criteria, whose calculation may be system-dependent and challenging in real-world power grids, (iii) they are computationally inefficient in real-world power grids due to the analysis of large volumes of PMU data at the control center, and (iv) they ignore data quality information at the PDC level, which can improve detection performance. Furthermore, in the majority of works in the literature, the required mitigation measures after detecting TSAs have not been addressed.

TSAs can significantly jeopardize the power system stability by disrupting the PMU data which are critical for WADCs [12]. This situation is catastrophic as the malfunction of WADCs following a TSA can cause grid destabilization within tens of seconds [12, 25]. Therefore, a mitigation scheme incorporated into the detection system is crucial to ensure grid stability until the TSA is addressed, and the system becomes attack free. Despite the importance of the issue, limited efforts

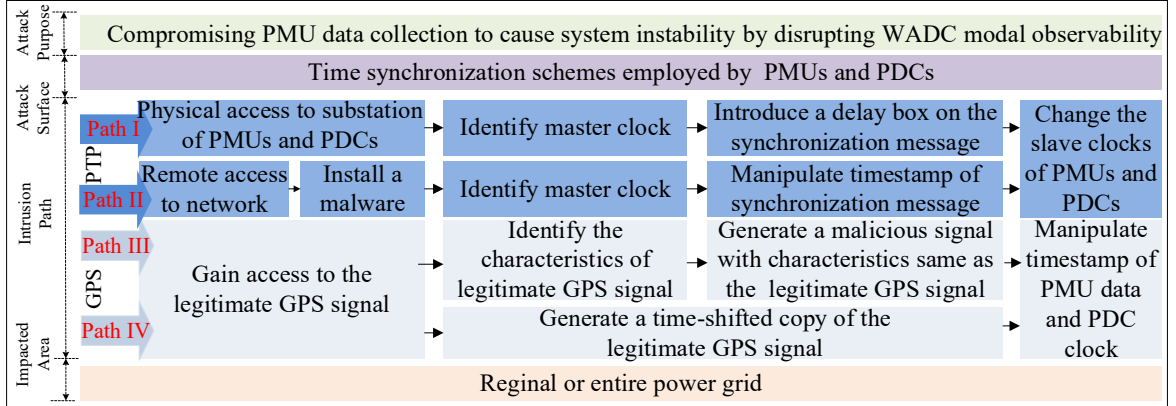


Figure 4.1: Threat model.

have been conducted to mitigate TSAs on WADCs. To deal with the abnormal delay caused by TSAs, the authors in [86] proposed a delay-aware variable loop gain WADC scheme. Moreover, a Luenberger observer-based controller was recently proposed in [108], which mitigates post-TSA delay and improves the damping performance of WADCs. Despite the provided advantages, none of these mitigation approaches is integrated to detection schemes. This integration enables mitigation schemes to adapt based on location of TSAs, resulting in improved post-attack performance of WADCs.

4.3 Attack Model

4.3.1 Attack Surface, Intrusion Path, and Vulnerability

In the threat model depicted in Fig. 4.1, the adversary's objective for launching the TSA is to intentionally cause dropout in critical PMU data, disrupt modal observability of WADCs, and jeopardize system stability. To this end, the attack surface encompasses the time synchronization schemes of PMUs and PDCs. It is worth noting that while PDCs are generally attributed a higher security level compared to PMUs, as shown in Fig. 4.2, both devices employ an identical time synchronization scheme in a power grid with an equivalent level of security. Consequently, both PMUs and PDCs exhibit similar vulnerabilities to TSAs that compromise this shared time synchronization scheme. Meanwhile, the device-level defense mechanisms can be employed to defend against TSAs on both PMUs and PDCs. These defense mechanisms include but not limited to (i) deployment of

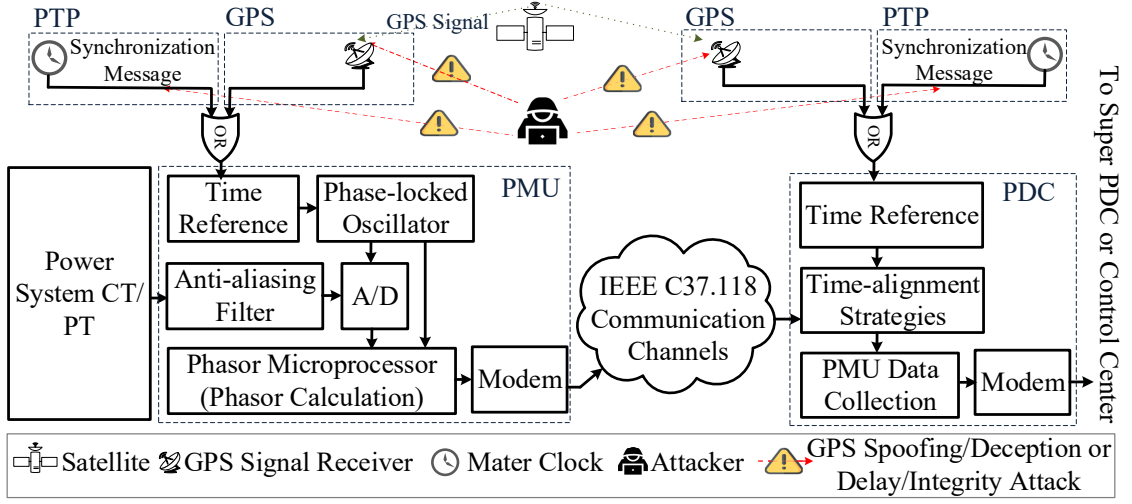


Figure 4.2: Attack surface.

device-level time anomaly detection modules [115], (ii) allocation redundant time sources within PMUs and PDCs or the host substation [84], (iii) employment of GPS signal robustness check approaches [25], (iv) installation of multi-frequency receivers, (v) deployment of multi-PNT services, e.g, GPS, GLONASS, GALILEO, and eLoran [12], and (vi) integration of advanced security measures such as key signal encryption [84] and clock synchronization status extension [88].

To implement the TSA on PMUs and PDCs, the adversary can follow four intrusion paths of which Paths I-II and III-IV are applicable in PTP and GPS cases, respectively. In network-based time-synchronization schemes such as PTP, a synchronization message are distributed from master clock source to slave clocks (PMUs and PDCs) through communication channels [88]. These schemes are vulnerable to delay box insertion and synchronization message manipulation TSAs, i.e., Path I and II in Fig. 4.1, respectively. In Path I, unauthorized physical access to the substation houses PMUs and PDCs is required to identify the communication channels between the master and slave clocks and insert a delay box out of component in the middle. This TSA was experimentally performed in 2016 at Laboratory of Communications and Applications at Ecole Polytechnique Federale de Lausanne (EPFL), Switzerland [110]. In that attack, a delay-repeater box was placed along the fiber link connecting the master clock and a PMU. This device substituted the original bidirectional fiber with a shorter fiber in one direction and a lengthy fiber coil in the opposite direction, introducing an imbalanced delay [110]. In Path II, the attacker needs to gain unauthorized

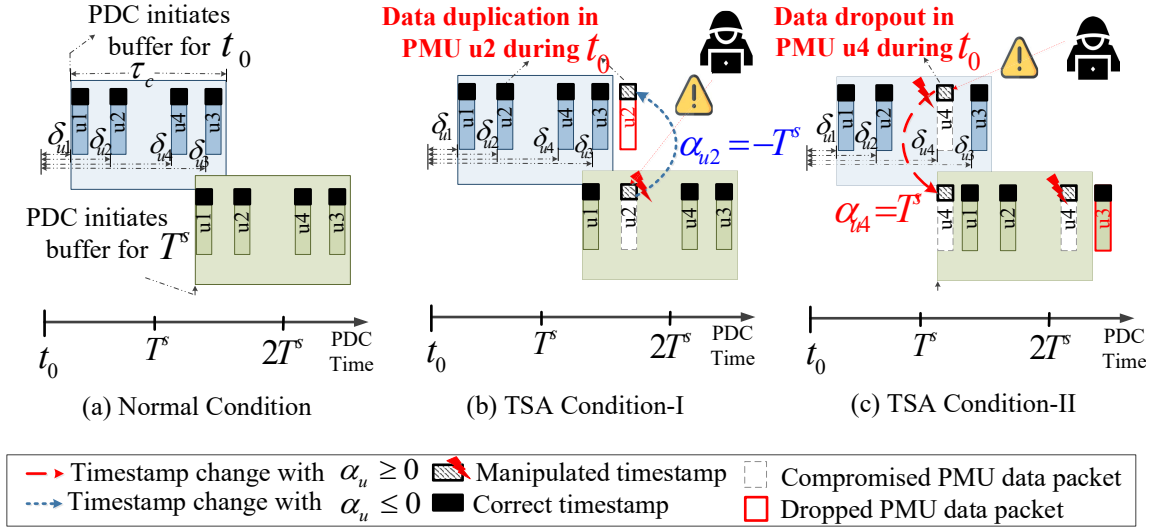


Figure 4.3: TSA impacts on PMU data collection in RTA.

remote access to the network or PTP infrastructure via VPN or fishing emails. By manipulating synchronization messages, an attacker could introduce false timing information, causing synchronization errors across the network [76]. In this intrusion path, the attacker can leverage various integrity attack methods across communication channels. For example, as practically implemented in [109], the adversary is able to compromise an intermediate node within communication channel, such as a router, switch, or transparent clock, and launch man-in-the-middle (MitM) attack to intercept specific PTP synchronization messages, manipulates their content, and forwards them to their destination.

In the space-based time-synchronization schemes such as GPS, the GPS receiver of PMUs and PDCs estimate their position and clock offset based on the signal received from GPS satellites [112]. These schemes, which are commonly used for PMUs and PDCs in power systems, are vulnerable to GPS spoofing and replay attacks illustrated in Paths III and IV in Fig. 4.1, respectively. In both Paths, the attacker needs to use a stand-alone commercial GPS receivers in nearby the targeted PMUs and PDCs to capture the legitimate GPS signal form satellites [112]. In Path III, the attacker retrieves the characteristics of the legitimate signal such as phase, code delay, and encoded data. Afterward, he/she uses a GPS simulator to generate a malicious signal identical to it but with a higher signal-to-noise ratio (SNR). Alternatively, in Path IV, the attacker can generate a higher

SNR time-shifted copy of the legitimate signal and transmit it to the targeted PMUs and PDCs' receivers [25]. In both paths, as the malicious signals have a higher SNR than the legitimate ones, the GPS receivers of the targeted PMUs and PDCs are deceived into tracking them, leading to errors in PMU data timestamp and PDCs clock [114–116]. While real-world occurrences of TSAs in power systems are yet to be reported, their feasibility has been proven through experimental simulations and actual incidents. For instance, a demonstration of this vulnerability occurred in 2008 when researchers at the University of Texas at Austin developed a portable civilian GPS spoofer [113]. This device, powered by a digital signal processor, successfully deceived a GPS receiver by transmitting falsified signals, showcasing the potential impact of such manipulation. Additionally, documented instances of GPS spoofing attacks have targeted operational navigation systems. Notably, in December 2011, a drone was reportedly hijacked through a GPS spoofing attack, misleading its navigation system to believe it was initiating a landing sequence at its intended base [24]. These incidents highlighted the need for improving knowledge about possible consequences of TSAs in power systems and developing effective countermeasures.

The manipulation of PMU data timestamps and PDC clocks can compromise the synchrophasor data collection, leading to significant dropout in PMU data. According to the IEEE std. C37.247-2019, PDCs collect PMU data into a unified data stream, employing either relative time-alignment (RTA) or absolute time-alignment (ATA) approaches [7]. In the RTA strategy depicted in Fig. 4.3-(a), the PDC creates a time-stamped buffer upon receiving the first complete PMU data packet. Assuming a variant communication latency, the PDC expects to receive all other PMU data labeled with the same timestamp within a set waiting time. Once the waiting time elapses, the PDC concludes the buffer and sends the aggregated data to the control center. On the other hand, in the ATA strategy illustrated in Fig. 4.4-(a), the PDC utilizes its own synchronized local clock to initiate time-stamped buffers and accumulate PMU data obtained before the waiting time expires [7]. In both methods, PMU data arriving after the PDC buffer waiting time will be dropped [7]. Thus, an adversary can maliciously exploit this vulnerability by tampering with the PMU data timestamp or PDC clock, compromising the time-alignment strategies, and forcing PDCs to drop crucial PMU data. This flaw creates a new avenue for an attacker to undermine the modal observability of WADCs.

As depicted in Fig. 4.2, a PMU uses time reference provided by the time synchronization

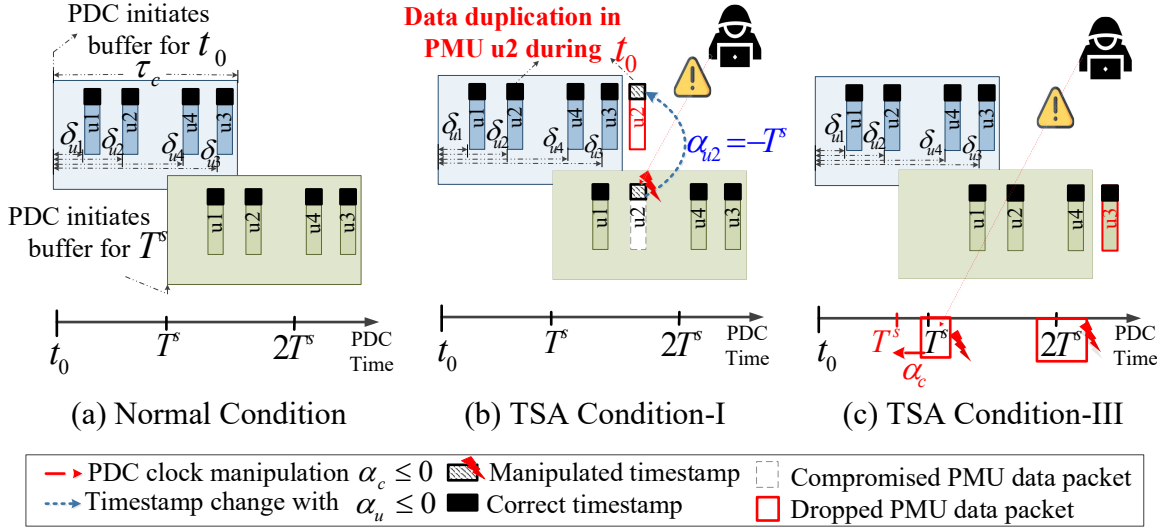


Figure 4.4: TSA impacts on PMU data collection in ATA.

schemes to (i) calculates the synchrophasor measurement data and (ii) do timestamp of IEEE C37.118 data packet. On the other hand, a PDC employs time synchronization schemes to collect and time-aligned a set of synchrophasor data received from multiple PMUs [97]. Therefore, in instances of TSAs targeting PMUs, the manipulation occurs within the timestamp of the synchrophasor data packet. On the contrary, when TSAs target PDCs, the manipulation alters the initiation time window of the buffer (only in ATA strategy). TSAs on PMUs and PDCs can result in the following conditions:

TSA Condition-I) Backward timestamp manipulation TSA on PMUs ($\alpha_u < 0$): In this case, the attacker maliciously alters the PMU data timestamp to a time whose corresponding buffer has expired when the PMU data arrives at the PDC. For instance, as shown in Figure 4.3-(b) and Figure 4.4-(b) for RTA and ATA strategies, respectively, data of PMU u_2 will be dropped by manipulating its timestamp from T^s to t_0 . This situation results in data duplication in the manipulated PMU during the time sampled before the TSA is launched. This attack can be executed on both RTA and ATA strategies.

TSA Condition-II) Forward timestamp manipulation TSA on PMUs ($\alpha_u > 0$): In this case, the PDC buffer is prematurely activated by the manipulated PMU data, causing other PMU data streams to arrive after the waiting time. For example, as depicted in Fig. 4.3-(c), PMU u_3 data drops after TSA since it arrives at the PDC when the premature buffer activated by the manipulated

data of PMU u_4 has expired. This TSA results in data loss in the manipulated PMU data at the exact moment of launching the attack. Note that this type of attack is only possible in the case of RTA strategy.

TSA Condition-III) Backward clock manipulation TSA on PDCs ($\alpha_c < 0$): In this case, in appose to other conditions, the adversary compromises the PDC clock such that the PDC buffer is initiated earlier than normal, causing dropout in the PMU data that arrive after waiting time expiration. As Fig. 4.4-(c) illustrates, this attack can be successful only in ATA strategy. It is worth noting that, since this TSA leaves PMU data unchanged, the system-level detection schemes, e.g., [2, 118–121], which are employed at the control center fail to detect it.

4.3.2 Attack Vector Optimization Model

To craft the optimal attack vector, this paper extends TSA model in Chapter 3 by formulating TSA on both RTA and ATA strategies at PDC while both PMUs and PDC clock can be targeted. Modeling TSAs on PDCs are crucial since the attack on a single PDC can impact data collection from a group of PMUs. The model in current paper enables (i) studying vulnerability of both RTA and ATA strategies at PDCs to simultaneous TSAs on PMUs and PDCs, (ii) enriching the dataset for training of the proposed CNN detection model by incorporating well-design TSA samples, and (iii) examining the performance of the proposed integrated detection and mitigation scheme against well-design severe TSA scenarios. This attack model aims to disrupt the WADC's observability performance by causing dropout in the critical PMU data. To this aim, the PMU data are prioritized based on their impact on the observability of dominant low-damping oscillation (DLO) modes, which can be quantified using the geometric measure of observability GMO_u^m . Further details regarding this index and implementation steps of the attack are elaborated in our previous work Chapter 3. On this basis, the adversary's objective can be stated as follows:

$$\max_{\alpha_u, \alpha_c, y_u, y_c} \sum_{u \in \Omega^u} \sum_{m \in \Omega^m} \sum_{c \in \Omega^c} \sum_{\omega \in \Omega^\omega} \pi_\omega (1 - v_{uc\omega}) GMO_u^m \quad (4.1)$$

In particular, this model obtains targeted PMUs y_u and PDCs y_c as well as the associated time manipulation α_u and α_c to maximize the dropout of the identified critical PMU data. The objective

function (4.1) is subject to a set of constraints including the attacker's budget constraint (4.2).

$$\sum_{u \in \Omega^u} y_u + \sum_{c \in \Omega^c} y_c = B^{max} \quad \forall \Xi = \{r, a\} \quad (4.2)$$

where $\Xi = \{r, a\}$ denotes the RTA and ATA strategies, respectively. To manipulate the timestamp of PMU u and clock of PDC c , the adversary must compromise their time-synchronization schemes, which are guaranteed in Constraints (4.3) and (4.4), respectively.

$$-M_1 y_u \leq \alpha_u \leq M_1 y_u \quad \forall \Xi = \{r, a\}, u \in \Omega^u \quad (4.3)$$

$$-M_1 y_c \leq \alpha_c \leq 0 \quad \forall \Xi = \{a\}, c \in \Omega^c \quad (4.4)$$

To keep the attack stealthy, the timestamp manipulation of PMUs must be a factor of sampling time, i.e., k_u , as represented in (4.5).

$$\alpha_u = k_u T^s \quad \forall \Xi = \{r, a\}, u \in \Omega^u \quad (4.5)$$

Meanwhile, Constraints (4.6) and (4.7) restrict the backward timestamp manipulation of PMU data ($\alpha_u < 0$) and PDC clock ($\alpha_c < 0$) in order to avoid abnormal data packet duplication and data packet dropout, respectively.

$$k_u \geq -D_u^{max} \quad \forall \Xi = \{r, a\}, u \in \Omega^u \quad (4.6)$$

$$\alpha_c \geq -D_c^{max} \quad \forall \Xi = \{a\}, c \in \Omega^c \quad (4.7)$$

If forward timestamp manipulation of PMU u exceeds its minimum arrival delay, the PDC will receive data tagged with a time that has not happened yet. As such, the TSA can be easily detected. Constraint (4.8) avoid this situation.

$$\begin{cases} \alpha_u \leq \delta_{uc\omega} & \forall \Xi = \{r\}, c \in \Omega^c, \omega \in \Omega^\omega \\ \alpha_u \leq \delta_{uc\omega} - \alpha_c & \forall \Xi = \{a\}, c \in \Omega^c, \omega \in \Omega^\omega \end{cases} \quad (4.8)$$

Considering the dedicated communication routing tree to transfer data of PMU u to PDC c , the

communication delay in each Scenario ω can be calculated using Constraint (4.9).

$$\delta_{uc\omega} = \sum_{l \in \Omega^l} x_{luc} \delta_{l\omega} \quad \forall \Xi = \{r, a\}, u \in \Omega^u, c \in \Omega^c, \omega \in \Omega^\omega \quad (4.9)$$

The PDC buffer triggering time and PDC buffer window in the RTA and ATA strategies are formulated as follows:

$$\tau_{c\omega}^{trig} = \begin{cases} \min(\delta_{uc\omega} - \alpha_u) & \forall \Xi = \{r\}, c \in \Omega^c, \omega \in \Omega^\omega \\ 0 & \forall \Xi = \{a\}, c \in \Omega^c, \omega \in \Omega^\omega \end{cases} \quad (4.10)$$

$$w_{uc\omega} = \begin{cases} \tau_{c\omega}^{trig} + \tau_c - \delta_{uc\omega} + \alpha_u & \forall \Xi = \{r\}, u \in \Omega^u, c \in \Omega^c, \omega \in \Omega^\omega \\ \tau_{c\omega}^{trig} + \tau_c - \delta_{uc\omega} + \alpha_u + \alpha_c & \forall \Xi = \{a\}, u \in \Omega^u, c \in \Omega^c, \omega \in \Omega^\omega \end{cases} \quad (4.11)$$

As mentioned before, PMU data received after the waiting time collapse will be dropped in both time-alignment strategies. This situation happens when the PDC buffer window $w_{uc\omega}$ for a PMU data u is negative. In contrast, the data of PMU u is aggregated in PDC c if the corresponding $w_{uc\omega}$ is positive. These conditions are formulated using Big-M method as follows:

$$-\frac{w_{uc\omega}}{M_2} + \varepsilon \leq v_{uc\omega} \leq 1 + \frac{w_{uc\omega}}{M_2} \quad (4.12)$$

$$\Xi = \{r, a\}, u \in \Omega^u, c \in \Omega^c, \omega \in \Omega^\omega$$

where ε denotes a small positive number. To recast the optimization model (4.1)-(4.12) into a stochastic MIL problem, Constraint (4.10) is linearized using an approach in Chapter 3. Therefore, the attack model can be solved using commercial mathematical-based solvers. It is worth noting that this model is a generic TSA vector optimization model which can be adopted to target other wide-area applications by changing the objective function (4.1).

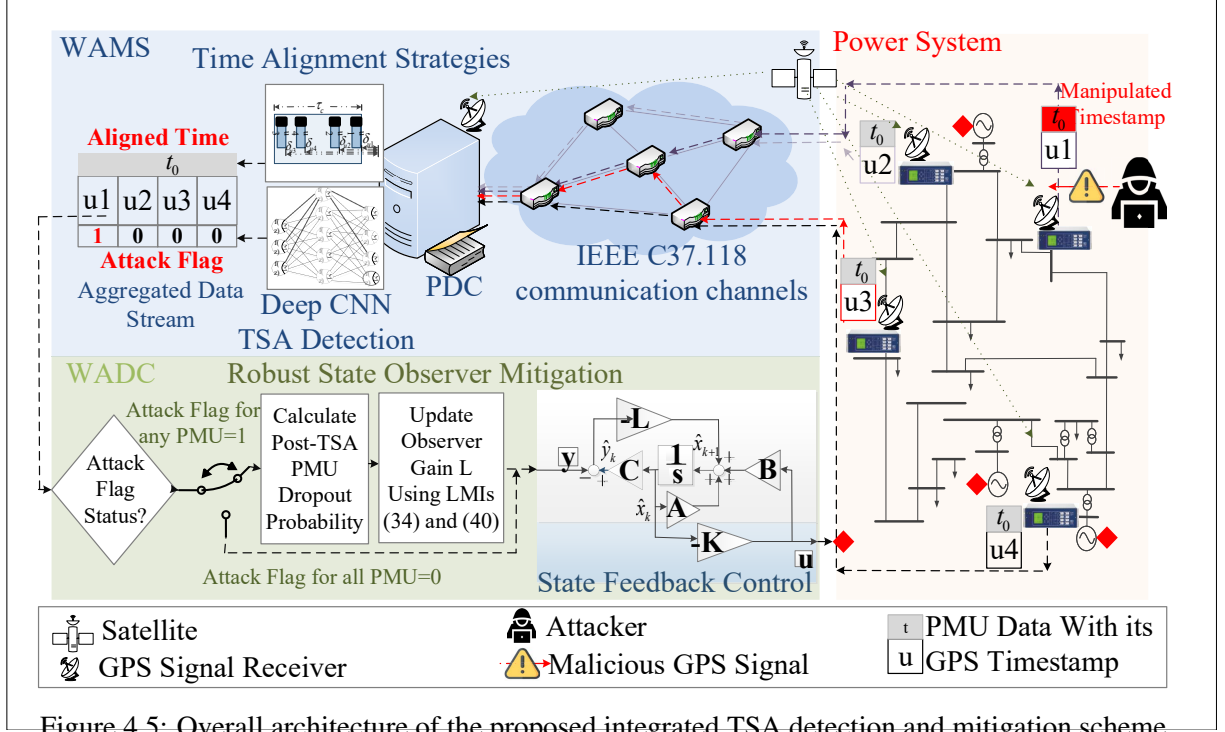


Figure 4.5: Overall architecture of the proposed integrated TSA detection and mitigation scheme.

4.4 Proposed Countermeasure

This section presents the proposed integrated deep CNN learning-based detection and robust state observer mitigation schemes depicted in Fig. 4.5. The proposed detection scheme is an auxiliary scheme implemented at regional PDCs that are connected to PMUs directly. This scheme leverages the available data quality information to identify manipulation in PMU data timestamps and PDC clock while distinguishing them from communication network incidents. This scheme generates a TSA flag extension corresponding to each PMU data in the aggregated output data stream of PDCs. Considering the 32-byte/256-bit structure of the IEEE C37.118 PMU data packet [122], it is feasible to allocate the 16th reserve byte to the TSA flag extension. The 16th reserve byte is typically set to zero and allows for flexibility in the protocol for future enhancements or modifications without requiring changes to the packet structure [122].

Upon receiving the aggregated data stream on the controller side, the WADC checks the TSA flag and switches to the TSA robust observer mitigation scheme if it is enabled for any PMU data. In such circumstances, the WADC calculates the PMU data dropout probability based on the location of the detected TSA, and then updates the observer gain L accordingly. The proposed mitigation

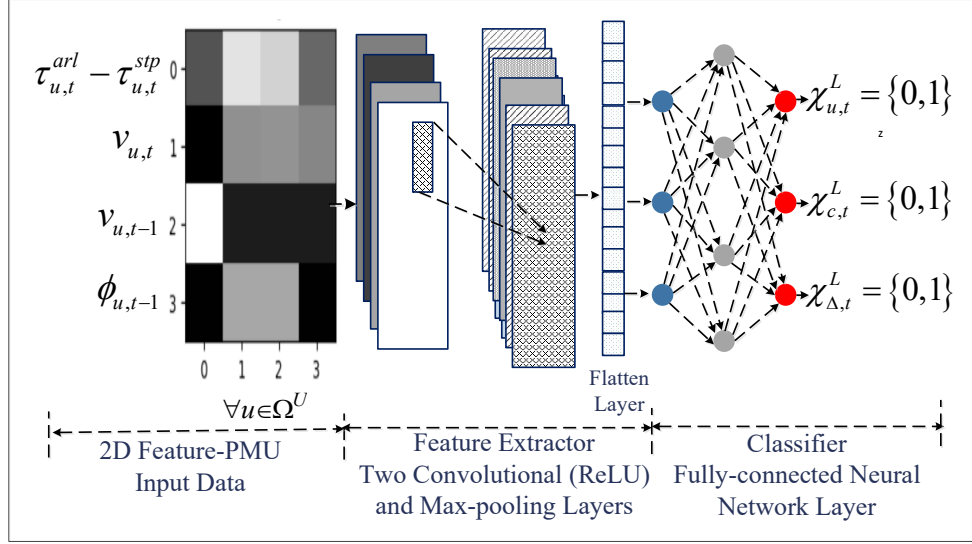


Figure 4.6: Architecture of the proposed deep CNN detection scheme.

scheme ensures that the power grid remains stable under TSAs until the grid becomes attack free. In the subsequent subsections, the structure of the detection and mitigation schemes are further elaborated.

4.4.1 Deep Learning Based Detection Scheme

To detect the TSA on PMUs and PDCs, this paper takes advantage of the temporal signature of TSAs appeared in the data quality information, i.e., calculated delay and dropout/duplication status of PMU data. These informative features not only exhibit distinct characteristics based on the type of attack initiated but also differentiate them from ordinary network incidents such as packet drop, communication link failure, and router congestion. As mentioned before, three types of TSAs can occur (TSA Conditions I-III in Section 4.3.1). TSA Condition-I results in an increase in the calculated delay and instances of data duplication within the affected PMUs at previously recorded timestamps. Conversely, TSA Condition-II causes a decrease in the calculated delay and instances of data dropout in the targeted PMUs at the time of the attack. TSA Condition-III leads to changes in the calculated delay across all PMU data, affecting them uniformly. However, routine network incidents exhibit distinct temporal patterns in the chosen data quality information features compared to attack scenarios. For example, normal occurrences like packet drops and communication link failures result in immediate data dropout in the affected PMUs without any duplication or alteration

in the calculated delay. Additionally, router congestion incidents may cause abnormal transmission delays in specific subsets of affected PMU data, unlike TSA Condition-III where the delay for all PMU data changes uniformly. Moreover, unlike TSAs, router congestion events do not cause any packet duplication in the data. These signatures of TSAs require a robust detection technique that can identify the temporal pattern in the data. As such, this paper utilizes a CNN deep learning model which has shown exceptional performance in recognizing temporal signatures in the data due to their ability to learn hierarchical representations of data and extract meaningful feature maps.

As this scheme directly imposes extra computational time and delay in PMU data aggregation at the PDC level, an effective structure of CNN fed by minimum input features is needed. As such, this paper employs a CNN consisting of three consecutive layers, i.e., feature-PMU input, feature extractor, and classifier for each regional PDC (Fig. 4.6). During each sampled time t , the input layer is fed by an 2D feature-PMU matrix (f, u) for the set of PMUs $\Omega_c^u = \{1, 2, \dots, U\}$ connected to the PDC c that houses the CNN scheme, as follows:

$$\chi^0 = \begin{bmatrix} \tau_{1,l}^{arl} - \tau_{1,l}^{stp} & v_{1,t} & v_{1,t-1} & \phi_{1,t-1} \\ \tau_{2,l}^{arl} - \tau_{2,l}^{stp} & v_{2,t} & v_{2,t-1} & \phi_{2,t-1} \\ \cdot & \cdot & \cdot & \cdot \\ \tau_{U,l}^{arl} - \tau_{U,l}^{stp} & v_{U,t} & v_{U,t} & \phi_{U,t-1} \end{bmatrix}_{U \times 4} \quad (4.13)$$

in which the first feature column denote the PMUs' data transmitting delay calculated by the PDC based on their data arrival time $\tau_{u,t}^{arl}$ and their tagged timestamp $\tau_{u,t}^{stp}$; the second and third feature columns $v_{u,t}$ and $v_{u,t-1}$ refer to data dropout status of PMUs during sampled time t and $t - 1$, respectively; and the forth feature column $\phi_{u,t-1}$ signifies the data duplication status of PMUs during sampled time $t - 1$. Consequently, the dimension of the input feature matrix for the CNN detection scheme at PDC c depends on the number of connected PMUs, taking the shape $U \times 4$. Since a PDC is typically connected to a limited number of PMUs, the performance of its TSA detection scheme remains uncompromised even as the system size increases. This represents a distinct advantage of the proposed scheme compared to TSA detection schemes used at control centers, which rely on data from all PMUs across the entire system. Based on the IEEE Std. C37.247-2019, all these input

features can be accessible at the PDC level.

As Fig. 4.6 shows, the input 2D feature-PMU data then passes through the feature extractor layer. In this layer, two consecutive convolutional layers followed by max pooling layers are utilized. The first convolutional layer applies a set of learnable filters to the input data. These filters are small in size and slide over the input data to detect local features. The output of this layer is a set of feature maps, each corresponding to a particular filter. The second convolutional layer applies another set of learnable filters to the feature maps obtained from the first layer. The max-pooling layer is applied after each convolutional layer. This layer downsamples the feature maps by selecting the maximum value in a small region of the feature map. This helps to reduce the number of parameters in the network and makes the network more computationally efficient. The classifier layer drives the binary classification outputs based on the flattened feature maps extracted in the previous layer. In the proposed CNN architecture, a three-layer dense fully-connected neural network is utilized. In each layer l , the output associated with the j th neuron is calculated as:

$$\chi_j^l = F\left(\sum_{i=1}^{N_{l-1}} w_{i,j}^l \chi_i^{l-1} + b_j^l\right) \quad (4.14)$$

where $F(\cdot)$ is the activation function, N_{l-1} is the number of neurons in the previous layer. For the first two layers, rectified linear unit (ReLU) activation functions are utilized, as follows:

$$f(\vartheta) = \max(0, \vartheta) \quad (4.15)$$

in which ϑ signifies the input argument. ReLU activation function sets negative input values to zero, which helps in (i) mitigating the vanishing gradient issue by providing a non-linear transformation without saturating and (ii) enabling faster training by allowing the network to learn more quickly [123]. Meanwhile, Sigmoid activation function (4.16) is used in the output layer.

$$f(\vartheta) = \frac{1}{1 + e^{-\vartheta}} \quad (4.16)$$

In apposed to other activation functions, Sigmoid is able to squash the network's output into a range between 0 and 1 [123]. This range is ideal for binary classification problems, such as TSA

detection in this paper, where each output neuron can be interpreted as a probability score between two classes. This function in the proposed CNN model yields probabilities that are thresholded (probability equal to 0.5) to classify instances into distinct normal and attack classes corresponding to each output neuron. As the proposed CNN aims to detect and localize TSAs, the output layer L is built by multiple neurons $\chi_{u,t}^L$ for each PMU u connected to the PDC, one neuron $\chi_{c,t}^L$ for the PDC class, and one neuron $\chi_{\Delta,t}^L$ for network incident class. The PDC then uses the output classification values $\chi_{u,t}^L$ and $\chi_{c,t}^L$ to generate the binary attack flag in the aggregated data stream.

The proposed deep CNN TSA detection scheme is trained offline using a comprehensive dataset including two legitimate and under-attack subsets. To enrich the dataset with a practical samples, four sets are incorporated as follows:

- **Normal samples Ω_N^n with correct PMU/PDC timing:** In this particular set of samples, the timing of both PMUs and PDCs remains unchanged, and no network incidents occur. Consequently, there is no dropout or duplication of PMU data in these samples. This set allows the TSA detection scheme to learn and recognize the normal delay between the PDC and the connected PMUs.
- **Network incident samples Ω_N^i including router congestion and link failure with correct PMU/PDC timing:** This set includes two common network incidents—router congestion and link failure—that impact the relevant features used in training and testing the proposed TSA detection scheme, particularly delay and PMU data dropout ratio. Router congestion occurs when the router’s buffer becomes overwhelmed by a high volume of data, resulting in abnormal delays [124]. In this study, it is assumed that router congestion incidents randomly increase the PMU-PDC delay of affected PMU data (based on data forwarding trees) according to a Gaussian distribution function with a mean value and standard deviation of 50% and 10% of the normal delay, respectively. On the other hand, link failure incidents manifest as data dropouts in the affected PMUs based on PMU-PDC data forwarding trees [98]. Since the temporal signatures of data dropout and delay differ between incidents and TSAs, these samples aid the TSA detection scheme in distinguishing between them.
- **Blind TSA samples Ω_{TSA}^b :** This set of samples comprises TSAs where the targeted PMUs/PDCs

and their associated time manipulations are chosen randomly. These samples are instrumental in training and testing the TSA detection scheme against random attacks.

- **Optimal TSA samples Ω_{TSA}^o :** In this set of samples, the targeted PMUs/PDC and their corresponding time manipulations are obtained by solving attack model (4.1)-(4.12) for various PDC waiting times and attacker budgets. These samples are crucial for training and testing the TSA detection scheme against carefully designed TSAs, where the adversary possesses sufficient information about the system to launch a severe TSA.

In each introduced sample, this paper uses Monte Carlo Simulation (MCS) to model the stochastic end-to-end communication latency between PMUs and the PDC as well as the behavior of PDC time-alignment strategies. On this basis, the end-to-end latency, dropout status, and duplication status of each PMU data are obtained to prepare the input 2D features χ^0 in (4.13) and the classification outputs $\chi_{u,t}^L$, $\chi_{c,t}^L$, and $\chi_{\Delta,t}^L$ in each sample.

4.4.2 Robust State Observer Mitigation Scheme

Observers are often employed in control systems where it is impractical or infeasible to directly measure all of the system's states. In power system applications, various configurations of WADCs, such as state-feedback controllers [1, 125] (as in the case of this paper), robust controllers [126, 127], and adaptive model predictive controllers (MPCs) [128], require integration with a state observer to estimate the system's states based on input measurement signals provided by PMUs. The state-space model of an observer integrated to a state-feedback controller can be presented as follows:

$$\hat{x}_{t+1} = (\mathbf{A} - \mathbf{BK})\hat{x}_t + L(y_t - \hat{y}_t) \quad (4.17)$$

$$\hat{y}_t = \mathbf{C}\hat{x}_t \quad (4.18)$$

where $\hat{x}$ denotes the vector of estimated system states, y_t and $\hat{y}_t$ respectively signify the vector of actual and estimated input measurements, $\mathbf{K}$ and L present the controller and observer gains, respectively, and $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ are matrices of state, input control, and output measurement, respectively. In this model, the post-TSA data dropout in the input measurements y_t provided by PMUs can lead

to errors in the estimated system states $\hat{x}_{t+1}$. Ultimately, the post-TSA estimation errors can result in incorrect control signals from the WADC to the system's actuators, thereby endangering the system stability. Therefore, it is crucial to mitigate the impacts of TSAs on WADC performance once they have been detected.

To address this issue, this paper proposes a robust state observer mitigation scheme designed to withstand PMU data dropout resulting from an attack detected by the CNN detection scheme. As explained before, in the proposed framework, the WADC accesses the output of the detection scheme through a binary attack flag in the aggregated data stream. During the attack condition, based on the location of TSA recorded in the attack flag of PMUs, the WADC calculates the PMU data dropout probability using the PDC data aggregation model (4.9)-(4.12), as:

$$\pi_u = \frac{\sum_{u \in \Omega^U} \sum_{c \in \Omega^C} (1 - v_{ucw})}{N_w} \quad (4.19)$$

where N_w denotes the number of communication latency scenarios. Since the data dropout probability in each individual PMU is independent, all combination of them are used to derive the dropout events $\{\mathbf{D}_k\}_{k \in 1:n}$, as follows:

$$\mathbf{D}_k = \text{diag} \begin{bmatrix} d_{u1}^m & d_{u2}^m & \dots & d_U^m \end{bmatrix} \quad \forall k \in \{1 : n\} \quad (4.20)$$

in which d_u^m represents the binary dropout status of Measurement m belonging to PMU u . On this basis, in each dropout event k , a set of collected and dropped measurements are built as $\Omega^\dagger$ and Ω° , respectively. Afterward, the occurrence probability of the dropout events $\{\pi_k\}_{k \in 1:n}$ are calculated using (4.21).

$$\pi_k = \prod_{u \in \Omega^\dagger} (1 - \pi_u) \times \prod_{u' \in \Omega^\circ} \pi_{u'} \quad \forall k \in \{1 : n\} \quad (4.21)$$

Referred to the block diagram shown in Fig. 4.5, the close-loop dynamic model of the state observer under calculated dropout events can be represented as follows:

$$\hat{x}_{t+1|\pi_k} = (\mathbf{A} - \mathbf{BK})\hat{x}_t + L(\mathbf{D}_k \mathbf{C}x_t - \mathbf{C}\hat{x}_t) \quad (4.22)$$

$$\forall k \in \{1 : n\}$$

On this basis, the observer error can be defined as:

$$e_{t+1|\pi_k} = x_{t+1|\pi_k} - \hat{x}_{t+1|\pi_k} \quad (4.23)$$

$$= (\mathbf{A} - L\mathbf{D}_k\mathbf{C}) e_t + (L\mathbf{C} - L\mathbf{D}_k\mathbf{C}) \hat{x}_t \quad \forall k \in \{1 : n\}$$

by substituting a new vector $\bar{e}_t = \begin{bmatrix} e_t & \hat{x}_t \end{bmatrix}^T$ into (4.22) and (4.23), the observer error can be rewritten as follows:

$$\bar{e}_{t+1|\pi_k} = A_k^e \bar{e}_t \quad \forall k \in \{1 : n\} \quad (4.24)$$

$$A_k^e = \begin{bmatrix} \mathbf{A} - L\mathbf{D}_k\mathbf{C} & L\mathbf{C} - L\mathbf{D}_k\mathbf{C} \\ L\mathbf{D}_k\mathbf{C} & \mathbf{A} - \mathbf{B}\mathbf{K} - L\mathbf{C} + L\mathbf{D}_k\mathbf{C} \end{bmatrix} \quad (4.25)$$

To ensure the stability of the observer in the presence of data dropout caused by TSAs, Theorems 1 and 2 are utilized for designing an appropriate gain L . The first theorem guarantees the stability of the observer under the possible post-attack dropout events, while the second theorem aims to enhance the convergence performance of the designed observer.

Theorem 1: Let $\{\mathbf{D}_k\}_{k \in 1:n}$ be the dropout events in the output measurement y_t at sampled time t and $\{\pi_k\}_{k \in 1:n}$ be occurrence probability corresponding to those events. The observer error is mean square stable if and only if there exists a symmetric positive definite matrix $P > 0$ and the observer gain L such that the following LMI is satisfied:

$$\begin{bmatrix} -\sum_{k=1}^n \pi_k P & \sqrt{\pi_k} A_1^e P & \dots & \sqrt{\pi_k} A_n^e P \\ * & -\sum_{k=1}^n \pi_k P & 0 & 0 \\ * & * & \dots & 0 \\ * & * & * & -\sum_{k=1}^n \pi_k P \end{bmatrix} \prec 0 \quad (4.26)$$

Proof: Let define the Lyapunov function as expected P -norm of the observer error as follows:

$$V(\bar{e}_t) = \mathbf{E} [\bar{e}_t^T P \bar{e}_t] \quad (4.27)$$

Accordingly, the observer error is bounded and decreases constantly as long as the following expression is satisfied: $V(\bar{e}_{t+1}) - V(\bar{e}_t) = \bar{e}_t^T \left[\sum_{k=1}^n \pi_k (A_k^{eT} P A_k^e - P) \right] \bar{e} \prec 0$ (4.28)

To this aim, the following internal argument must be negative definite.

$$\sum_{k=1}^n \pi_k (A_k^{eT} P A_k^e - P) \prec 0 \quad (4.29)$$

This argument can be rewritten as the expression (4.30).

$$\begin{aligned} & \begin{bmatrix} \sqrt{\pi_1} A_1^{eT} & \dots & \sqrt{\pi_n} A_n^{eT} \end{bmatrix} \begin{bmatrix} P & 0 \\ 0 & P \end{bmatrix}_{n \times n} \begin{bmatrix} \sqrt{\pi_1} A_1^e \\ \dots \\ \sqrt{\pi_n} A_n^e \end{bmatrix} \\ & - \sum_{k=1}^n \pi_k P \prec 0 \end{aligned} \quad (4.30)$$

Applying Schur Complement can transform the expression (4.30) into LMI (4.26).

Theorem 2: Let $\mathbb{D}$ be a region in complex S-plane as follows:

$$\mathbb{D} = \{x + jy | x < -\xi\} \quad (4.31)$$

where ξ is a scalar positive value. The observer is $\mathbb{D}$ -stable, meaning that all eigenvalues of the observer are located in the region $\mathbb{D}$, if only if there exists a symmetric positive definite matrix $P > 0$ and observer gain L to satisfy the following LMI:

$$\sum_{k=1}^n \pi_k A_k^{eT} P + \sum_{k=1}^n \pi_k P A_k^e + 2\xi P \prec 0 \quad (4.32)$$

Proof 1: Given the Lyapunov function (4.27), the observer is $\mathbb{D}$ -stable if the following condition holds:

$$\frac{d}{dt} (V(\bar{e}_t)) \leq -2\xi V(\bar{e}_t) \quad (4.33)$$

By substituting Equations (4.24) and (4.27) into (4.33), the LMI equation (4.32) can be easily achieved.

After substituting Equation (4.25), the extracted LMIs (4.26) and (4.32) become bilinear. However, defining an auxiliary variable $Y = PL$ recasts both LMIs into a linear form solvable using commercial convex optimization techniques.

4.5 Numerical Results and Discussions

This section evaluates the implications of the presented TSA model and the effectiveness of the proposed integrated TSA detection and mitigation schemes on three case systems, i.e., Two-Area Kundur [129], IEEE 39-bus [103], and the Simplified 14-Generator Model of the Southeastern Australian Power System [130]. The communication network configuration integrated to collect PMU data in each test case system is considered based on the shortest path routing strategy in [129]. The following scenarios are introduced considering the potential impacts of TSAs on data aggregation in WADC schemes.

- **S0**: Data collection strategy: RTA, $\tau_c=50\text{ms}$, and attack free;
- **S1**: Data collection strategy: RTA, $\tau_c=50\text{ms}$, and $B^{max}=1$;
- **S2**: Data collection strategy: RTA, $\tau_c=50\text{ms}$, and $B^{max}=2$;
- **S3**: Data collection strategy: ATA, $\tau_c=80\text{ms}$, and $B^{max}=1$;
- **S4**: Data collection strategy: ATA, $\tau_c=80\text{ms}$, and $B^{max}=2$.

The selected waiting times for the RTA and ATA strategies guarantee the completeness of the data of all PMU data based on the data transferring delay during normal conditions [129]. In each scenario, the optimal TSA vector is calculated using model (4.1)-(4.12) solved by the CPLEX solver in the GAMS software with an optimality gap of 0.001%. The impacts of the crafted TSA on system stability are evaluated based on the resultant data dropout probability in the critical PMUs as well as post-attack time-domain performance of the WADC.

For offline training of the proposed CNN detection scheme, by considering the dedicated communication network configuration in each system, the link failure and router congestion incidents are modeled by a uniform random delay between $[5, 20]\text{ms}$ and data dropout in the affected PMU data, respectively [98, 124]. On the other hand, the blind samples in the under-attack subset contain all combinations of TSAs on the PMUs and PDCs while the associated attack vectors are unified

Table 4.2: Optimal TSA Vectors in Case-I

Scenario	TSA Vector (ms)	Dropout Probability π_u			
		u1	u2	u3	u4
S1	$\alpha_{u4} = -24.99$	0	0	0	0.69
S2	$\alpha_{u1} = +24.99$ $\alpha_{u3} = -24.99$	0	0	0.88	0.67
S3	$\alpha_{u3} = -33.33$	0	0	0.28	0
S4	$\alpha_{u1} = -33.33$ $\alpha_{c1} = -30$	0	0.18	0.57	0.34

randomly selected as $\alpha_u \in [-83.3, 33.3]$ ms and $\alpha_c \in [-100, 0]$ ms, respectively. Moreover, the optimal TSA samples are built by attack model (4.1)-(4.12) for different data collection strategies, PDC buffer waiting time $\tau_c \in [20, 120]$ ms, and attack budget $B^{\max} \in [1, 3]$. It is worth noting that PMU data dropout in a specific PDC depends solely on its synchronized clock and connected PMU timestamps, operating independently of other PDCs and non-connected PMUs. In the under-studied test cases, despite varying system scales, the number of connected PMUs to each PDC, potential targets for attackers, remains largely similar. Therefore, the attacker budget within $B_{max} \in [1, 3]$ could include worst-case PMU data dropout scenarios in all test cases. To create a balanced database, 10,000 samples are generated for each category of normal and under-attack conditions. Eventually, 80% and 20% of the built dataset are selected for training and testing of the proposed CNN detection scheme, respectively.

This paper deploys the *TensorFlow.Keras* library in Python environment to build, train, and test the proposed CNN model. The detection performance of the proposed CNN model is quantified by the statistical metrics, i.e., accuracy (ACC), false negative rate (FNR), and false positive rate (FPR), which are calculated based on true positive (TP), true negative (TN), false positive (FP), and false negative (FN) [131]. Subsequently, this paper performs time-domain simulations to evaluate the impact of the crafted TSA vectors on WADC performance under the proposed robust observer compared to the linear quadratic regulator (LQR) observer in [96] and the stochastic data dropout robust (SDDR) observer in [1]. The derived LMIs (4.26) and (4.32) are solved using the LMI toolbox in MATLAB with ξ equal to 10. Additionally, the Hankel singular value (HSV) technique is employed to reduce the order of the open-loop control model of test systems, enhancing the computational efficiency of the LMI solver. All simulation studies are conducted on an Intel Core

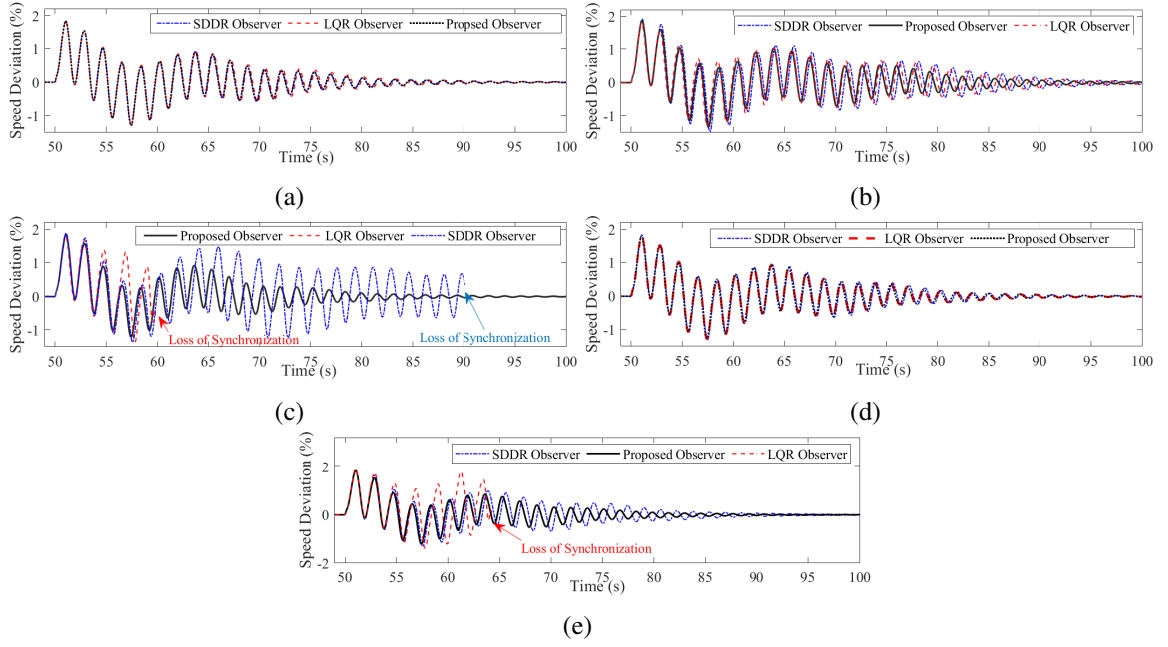


Figure 4.7: Post-attack speed deviation of G3 in Case-I during (a) attack free scenario S0 and TSA scenarios (b) S1, (c) S2, (d) S3, and (e) S4.

Table 4.3: TSA Detection Performance in Case-I

Learning Model	TSA Samples		Normal Samples		Network Incidents	
	TP (%)	FN (%)	TN (%)	FP (%)	TN (%)	FP (%)
ANN-LF	27.302	9.809	36.795	25.227	0.867	0.000
CNN-LF	49.397	7.850	38.614	3.270	0.869	0.000
ANN-FF	52.283	1.694	44.910	0.246	0.867	0.000
CNN-FF	52.523	0.120	46.484	0.006	0.867	0.000

ANN-LF	64.96	26.43	40.11
CNN-LF	88.91	13.71	7.6
ANN-FF	98.06	3.14	0.53
CNN-FF	99.87	0.23	0.01
	ACC	FNR	FPR

Figure 4.8: TSA detection performance indices in Case-I.

i7 PC with 16GB RAM.

4.5.1 Case-I: Two-Area Kundur Test System

The eigenvalue analysis performed on the open-loop state-space model of the two-area Kundur test system indicates that there is a pair of inter-area DLO modes as $-0.105 \pm 4.024i$ [132]. To damp the post-disturbance oscillations caused by those modes, a WADC modulates the excitation system of Generators $G1-G4$ based on the measurements provided by PMUs $u1-u4$. In this system, utilizing the threat model, the adversary can disrupt the WADC's ability to observe the inter-area DLO modes by maliciously dropping PMU measurements with higher GMOs. Given $GMO_{u1-u4}^m = [0.62, 0.34, 1, 0.97]$, PMUs $u3$ and $u4$ are identified as critical PMUs [129]. On this basis, the adversary obtains the optimal TSA vector, which is presented in Table 4.2. The worst post-attack data dropout conditions occur during Scenarios S2 and S4, where multiple PMUs and PDCs are manipulated simultaneously. Fig. 4.9 illustrates the post-attack performance of the WADC in Scenarios S0-S4 during a three-phase short circuit in Line 7-9 between 50 s to 50.05 s. As shown in Fig. 4.9-(c) and Fig. 4.9-(e), the LQR observer WADC fails to stabilize the system under post-attack dropout conditions in Scenario S2 and S4, respectively. The crafted TSA in these two attack Scenarios S2 and S4 also lead to system instability and performance reduction in case of the SDDR observer, respectively.

To counter TSAs in Case-I, the CNN detection scheme is trained using full features (FFs) of the proposed Vector 4.13 including latency and data quality features of the built dataset. In this case, one PDC collects data of four PMUs $u1$ to $u4$. Therefore, the dimension of the input feature matrix is 4×4 . Table 4.3 reports the performance of the proposed CNN detection scheme compared to the artificial neural network (ANN) and CNN models when they are trained using only latency features (LFs) and FFs of Vector (4.13). As shown in Fig. 4.8, compared to the ANN model, the CNN model achieves a superior detection performance due to its ability to identify temporal patterns in input features during TSAs, normal conditions, and network incidents. Meantime, the proposed data quality features in the CNN-FF and ANN-FF models contribute to significant improvement in detection performance, e.g., 10.96% and 33.1% in ACC, compared to the CNN-LF and ANN-LF models, respectively. The trained CNN-FF model successfully detects the designed optimal TSAs in Table 4.2. Following the detection of the TSAs, the proposed robust state observer mitigation

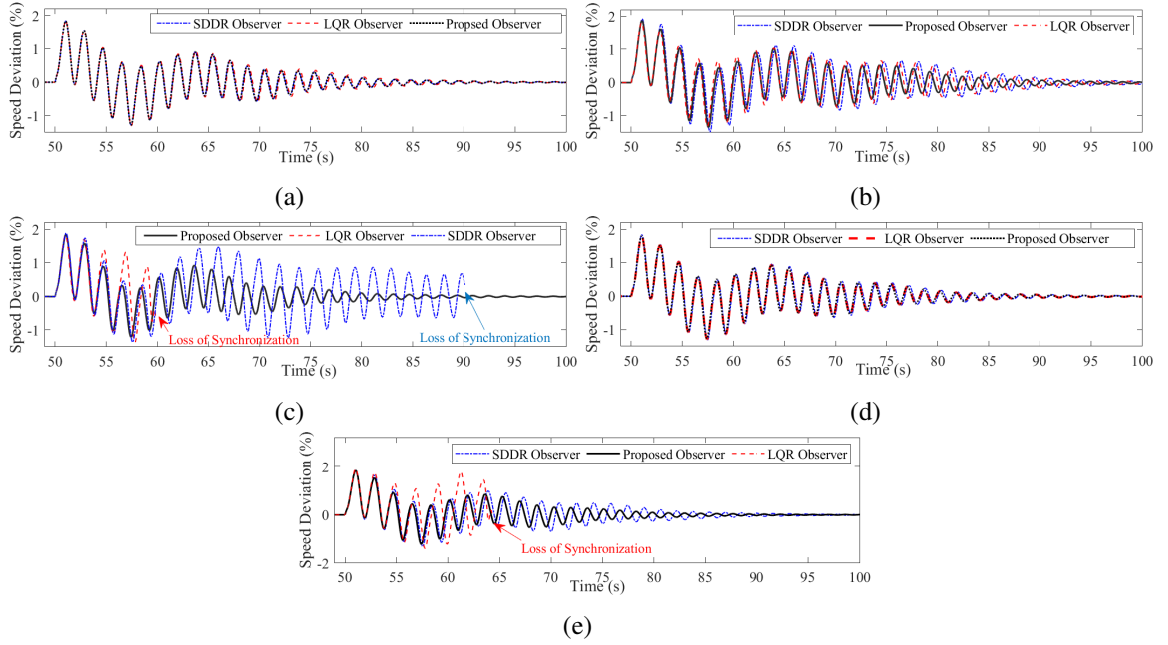


Figure 4.9: Post-attack speed deviation of G3 in Case-I during (a) attack free scenario S0 and TSA scenarios (b) S1, (c) S2, (d) S3, and (e) S4.

Table 4.4: Optimal TSA Vectors in Case-II

Scenario	TSA Vector (ms)	Dropout Probability π_u			
		u20	u25	u26	u29
S1	$\alpha_{u20} = -24.99$	0.51	0	0	0
S2	$\alpha_{u17} = +8.33$ $\alpha_{26} = -24.99$	0	0	0.76	0
S3	$\alpha_{c3} = -30$	0	0	0	0.46
S4	$\alpha_{u26} = -33.33$ $\alpha_{c3} = -30$	0	0.43	0.72	0.37

scheme takes place. As Fig. 4.9 depicts, the WADC with the proposed observer not only provides the same damping performance as the LQR and SDDR observers during the attack free condition (refer to Fig. 4.9-(a)), but also effectively stabilizes the system in all TSA Scenario S1-S4.

4.5.2 Case-II: IEEE 39-Bus Test System

The IEEE 39-Bus Test System is equipped with 16 PMUs and 3 local PDCs to collect measurement data for wide-area applications [103]. This system has two pairs of inter-area DLO modes, i.e., $-0.28 \pm 5.84i$ and $-0.12 \pm 5.72i$. To deal with these DLO, a WADC is integrated into the

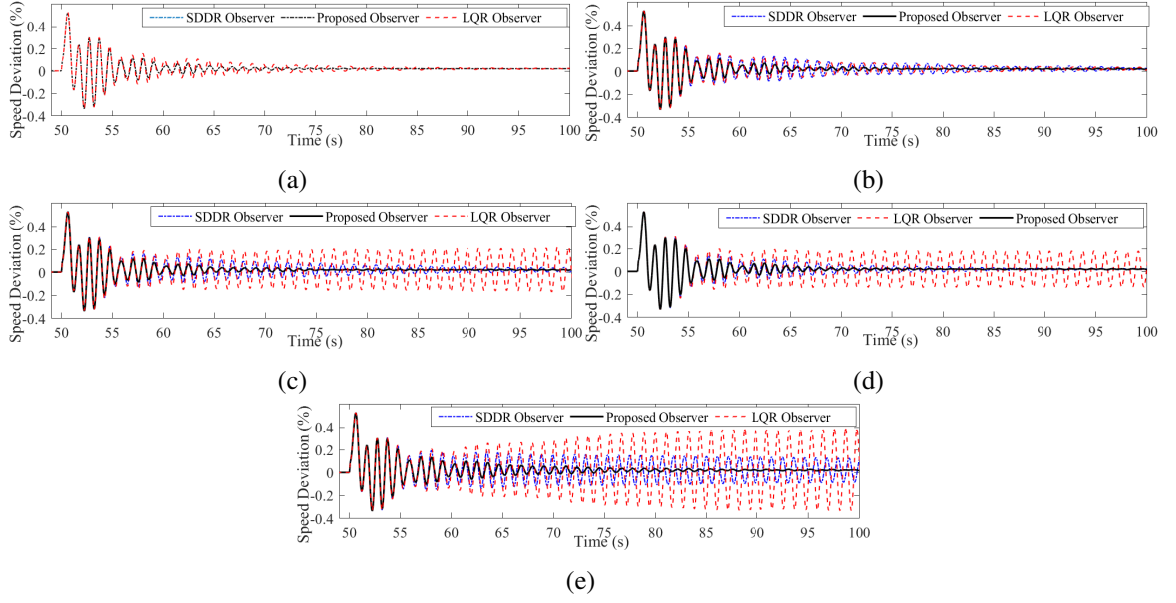


Figure 4.10: Post-attack speed deviation of G2 in Case-II during attack free scenario S0 and TSA scenarios (b) S1, (c) S2, (d) S3, and (e) S4.

system. This WADC uses the active power measurement of PMU u_{20} , u_{26} , and u_{29} to modulate the excitation systems of Generators G_2 , G_5 , and G_9 [129]. Since the adversary does not aware of the configuration of the WADC, he/she aims to design the TSA vector to maximize intentional data dropout in the PMUs with higher GMOs associated with two DLO modes. On this basis, PMUs u_{14} , u_{16} , u_{17} , u_{19} , u_{20} , u_{26} , and u_{29} which have relatively higher GMOs are identified as critical PMUs [129]. As reported in Table 4.4, the adversary is able to cause intentional dropout in the critical PMUs u_{20} , u_{25} , u_{26} , and u_{29} by launching TSAs on PMUs u_{17} , u_{20} , and u_{26} as well as PDC c_3 depending on the data collection strategy of PDCs and attacker budget. Fig. 4.10 shows the under-attack time-domain performance of the WADC during a three-phase short-circuit fault on Line 28-26 at $t = 50$ s to $t = 50.05$. This simulation illustrates that the crafted TSA in Scenarios S2-S4 causes interaction between the LQR observer WADC and local power system stabilizers (PSSs) which appears as an undamped oscillation. A similar situation happens during TSA Scenario S4 in the case of the SDDR observer.

To detect TSAs in Case-II, three CNN detection schemes are implemented in three local PDCs c_1 - c_3 . According to the number of linked PMUs to each regional PDC c_1 , c_2 , and c_3 , the dimensions of the input feature matrix for their associated detection schemes are 6×4 , 4×4 , and

Table 4.5: TSA Detection Performance in Case-II

Learning Model	TSA Samples		Normal Samples		Network Incidents	
	TP (%)	FN (%)	TN (%)	FP (%)	TN (%)	FP (%)
ANN-LF	33.653	7.745	34.935	22.992	0.656	0.019
CNN-LF	48.474	11.109	36.477	3.744	0.187	0.009
ANN-FF	52.854	1.362	44.908	0.526	0.345	0.005
CNN-FF	53.108	0.048	46.594	0.006	0.244	0.000

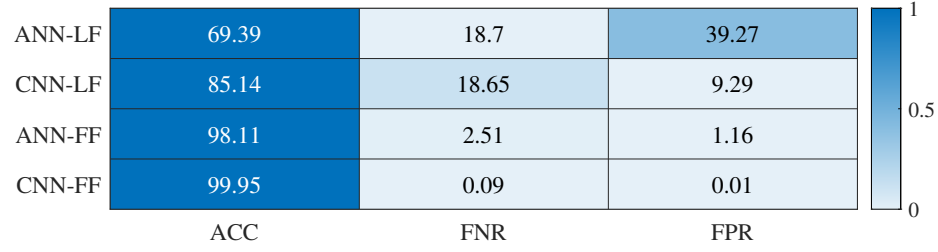


Figure 4.11: TSA detection performance indices in Case-II.

4×4 , respectively. Each CNN scheme is trained individually using the under-attack and legitimate datasets of the PMUs connected to them. The overall detection performance of these schemes in Case-II is reported in Table 4.5 and Fig. 4.11. The superior detection performance is achieved in the proposed CNN-FF model by ACC, FNR, and FPR equal to 99.95%, 0.09%, and 0.01%. This superior performance is due to the fact that the proposed CNN model (i) can more effectively recognize the temporal signature of TSAs and distinguish them from normal and network incident conditions, and (ii) deploys data quality information calculated by PDCs. The trained CNN-FF is able to detect all the optimal TSAs in Table 4.4. After the detection and localization of the TSAs, the integrated mitigation scheme calculates the data dropout probability of each PMU and updates the state observer gain. Time-domain simulation in Fig. 4.10 illustrates that the mitigation scheme can maintain the system stable in all TSA Scenarios S1-S4 while delivering the damping performance comparable to the LQR and SDDR observers in the normal condition S0.

4.5.3 Performance Comparison of the Detection Scheme

To showcase the superiority of the proposed detection scheme over existing system-level TSA detection models in the literature, its performance is compared with that of a recent model, an ANN-based detection scheme presented in [2]. To ensure a valid comparison, experiments are conducted

Table 4.6: Detection Performance comparison with ANN-based Model in [2]

Indices	Accuracy		Precision		Recall	
	PMU	PDC	PMU	PDC	PMU	PDC
ANN-based model in [2]	0.9978	-	1.0000	-	0.9786	-
Proposed Detection Scheme	0.9981	0.9919	1.0000	0.9969	0.9952	0.9869

under identical conditions, in terms of the test system and datasets generated for training and testing. From the various test systems used in [2], the IEEE 14 Bus test system is selected since: (i) the ANN-based model in [2] demonstrated superior accuracy on this test system among others, and (ii) the training and testing datasets in this system include scenarios involving simultaneous TSAs on multiple PMUs. Consistent with [2], the system topology and parameters are considered based on the Matpower toolbox. Furthermore, similar to [2], it is assumed that all load and generation buses are equipped with PMUs, and their data are collected by a single PDC located at non-load Bus 7. This single PDC is equipped with our proposed CNN-based detection scheme to identify TSAs on all PMUs and its own PDC clock. The communication network is considered aligned with the power grid configuration, while data forwarding trees between PMUs and PDCs are established using the shortest path algorithm. As per [2], the dataset is built comprising 126,858 normal samples and 84,438 TSA samples. In each TSA sample, one or two PMUs are randomly selected as the under-attack PMUs, and their timing is manipulated within the range of $[-8.33, +8.33]$ ms [2]. Additionally, the dataset includes 10,000 scenarios where the clock of the PDC is randomly manipulated within the range of $[-100, 0]$ ms. The feature inputs and labels for each sample are calculated using a similar algorithm to that used in other case studies in this paper. Similar to [2], 100,000 samples from the dataset are used for training, with the remainder used for testing.

As shown in Table 4.6, the proposed detection scheme in this paper results in a slight improvement compared to [2] in both Accuracy and Recall indices for TSAs on PMUs in the presented case study. Notably, both models achieve a Precision of 1.000, indicating that no false positives were detected. However, existing system-level detection schemes, such as one in [2], are unable to detect TSAs on PDCs. This limitation stems from the fact that these models rely on identifying mismatches in physical power flow equations caused by post-TSA phase errors in measurements from the under-attack PMUs. In contrast, TSAs on PDCs do not impact the phase of measurements;

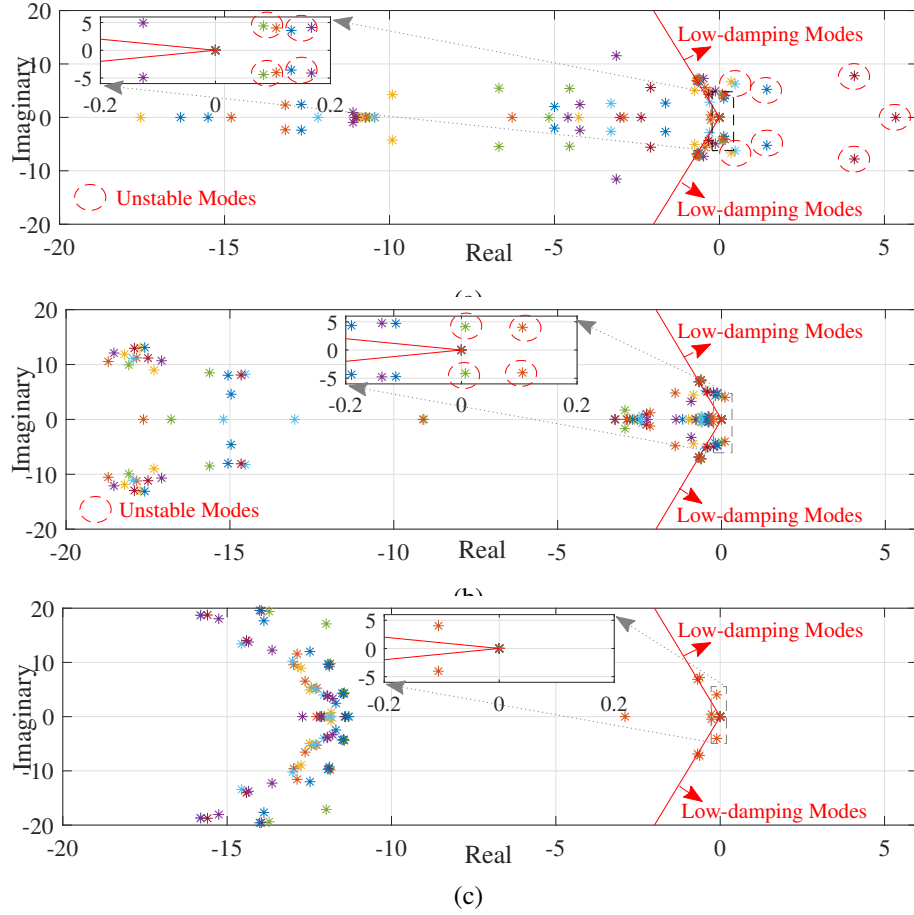


Figure 4.12: Eigenvalue analysis of observer error dynamic model in Case-II for various optimal TSAs (a) LQR, (b) SDDR [1], and (c) proposed observer.

instead, they lead to an increase in calculated delay for all PMUs and result in data dropout. Unlike existing models, the proposed detection scheme leverages these distinct data quality features to identify the temporal signature of TSAs on PDCs. This capability allows the proposed model to achieve an Accuracy of 0.9919 in detecting TSAs on PDCs in the presented case study.

4.5.4 Performance Comparison of the Mitigation Scheme

This subsection evaluates the performance of the proposed robust state observer mitigation scheme compared to LQR and SDDR observers in both frequency and time domains. In frequency domain, the eigenvalues of the dynamic model of the observer error (4.24) are obtained for the various PMU data dropout events among the optimal TSA samples in the detection scheme's database. The presence of eigenvalues in the right half of the complex S-plane during each dropout event

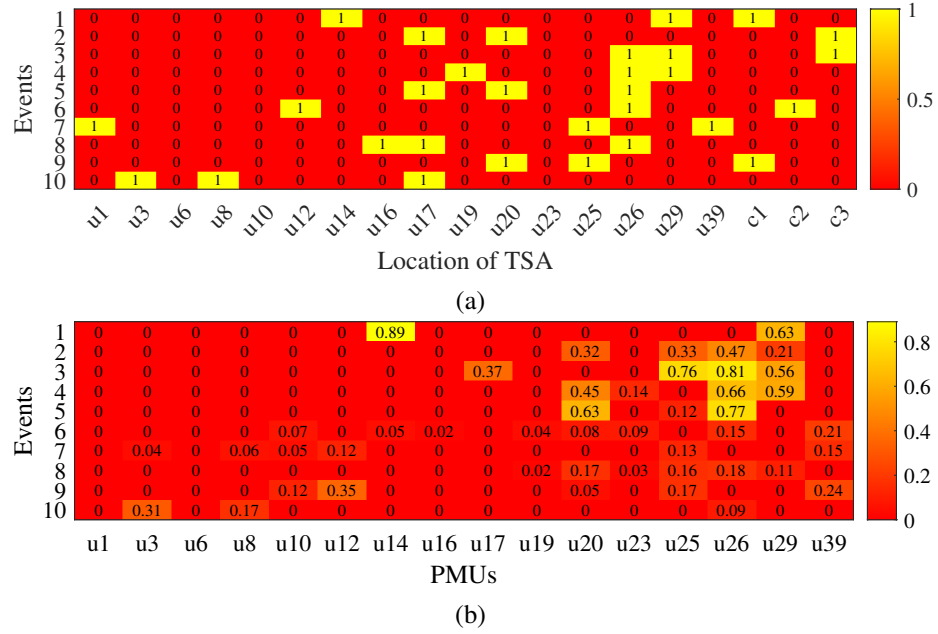


Figure 4.13: Sample optimal TSA Events 1-5 and blind TSA Events 6-10 in Case-II: (a) location of TSAs, and (b) PMUs' dropout probability.

indicates that the observer estimation error diverges in the time domain following a disturbance, resulting in the malfunction of the integrated WADC and system instability. Fig. 4.12 shows the results of this analysis on the IEEE 39-Bus test system. This analysis demonstrates that, unlike LQR and SDDR observers, the estimation error in the proposed observer converges in all optimal TSA samples.

In time domain, the adaptability of the proposed robust state observer mitigation scheme is assessed under various TSA events on different location in the IEEE 39 Bus test system. For each attack event, the performance of the proposed scheme is evaluated based on estimation error using the mean absolute error (MAE) [133], which is calculated as follows:

$$MAE = \frac{1}{N_s} \sum_{i=1:N_s} |x_t(i) - \hat{x}_t(i)| \quad (4.34)$$

where $x_t(i)$ and $\hat{x}_t(i)$ denote the actual and estimated system state i , respectively, and N_s signifies the number of system states. The attack events are randomly selected from the database built in the detection phase. These attacks are among severe samples, manipulating the timing of three PMUs/PDCs simultaneously, as illustrated in Fig.4.13-(a). Events 1 to 5 represent optimal TSA

Table 4.7: Stabilization Time (T_s [s]) During The Optimal and Blind TSA Events.

Event	LQR Observer	SDDR Observer	Proposed Observer
1	507.49	102.83	87.14
2	947.01	142.51	93.68
3	∞	∞	115.38
4	∞	∞	119.72
5	∞	351.49	107.46
6	106.97	82.03	81.40
7	91.55	77.08	76.85
8	242.27	92.81	85.13
9	91.55	77.08	76.85
10	91.55	77.08	76.85

samples, where the attack vectors are calculated by the attack model (Equations (4.1)-(4.12)), while Events 6 to 10 are blind. The resulting probability of PMU data dropout in each TSA event is depicted in Fig.4.13-(b). As expected, the PMU data dropout probability in the optimal TSA events is notably higher compared to the blind attack events, especially for PMUs u_{20} , u_{26} , and u_{29} , whose data are utilized in the WADC. The most significant data dropout occurs in these PMUs during Events 3, 4, and 5. During these events, illustrated in Fig. 4.14-(a) for Event 4 as an example, the estimation error does not converge in either the LQR or SDDR observer cases. However, in the case of the proposed observer, the estimation error diminishes to zero. This superiority of the proposed observer is further evident during Event 2, as depicted in Fig. 4.14-(b). Additionally, as shown in Fig. 4.14-(c), the proposed observer yields slightly lower estimation errors compared to LQR and SDDR observers during Events 7, 9, and 10, where PMUs connected to the WADC remain unaffected by TSA. Hence, the proposed observer not only demonstrates superior convergence performance in estimation error during both optimal and blind TSA events but also yields lower estimation errors during normal events where no data is dropped.

To quantify the system stability and damping performance of the WADC, this paper employs the stabilization time T_s , defined as follows:

$$T_s = \min \left\{ t > 0 : \left| \frac{x_{t'} - x_\infty}{x_\infty} \right| < \delta, \forall t' \geq t \right\}, \quad (4.35)$$

where δ is the predefined threshold, set here to 5%. As widely used in the literature, e.g., [134,

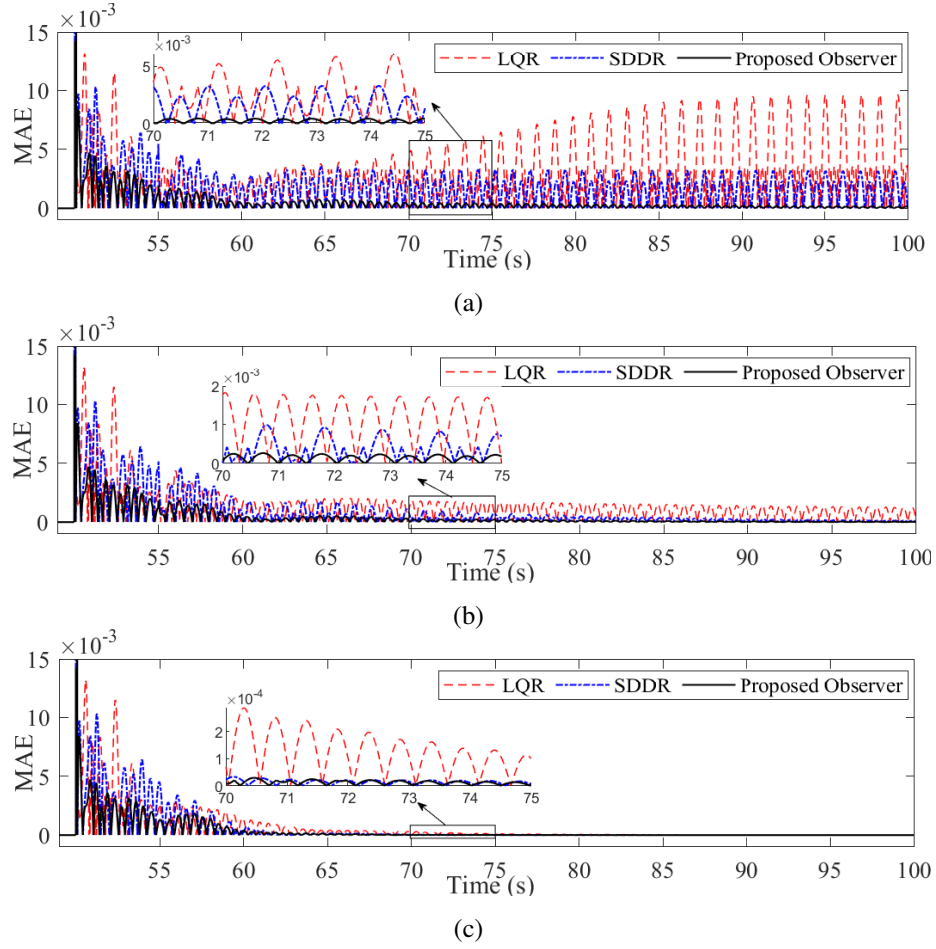


Figure 4.14: Estimation error of the observers in Case-II during (a) worst-case optimal TSA Event 4, (b) Optimal TSA Event 2, and (c) Blind TSA Events 7, 9, and 10.

135], T_s offers insights into damping performance by quantifying the time required for the system's response to stabilize within a specified tolerance band δ around its final steady-state value. Table 4.7 reports the stabilization time for the WADC integrated with the proposed observer mitigation, in comparison to the LQR and SDDR observers, across each TSA event. The results indicate that the WADC integrated with the proposed observer achieves faster stabilization times relative to the LQR and SDDR observers. This outcome can be attributed to the robust nature of the proposed observer, which is integrated with the detection scheme to mitigate the impact of PMU data dropouts resulting from detected TSAs. The proposed observer is adaptive based on the location of the TSA detected, contributing to its superior stability performance.

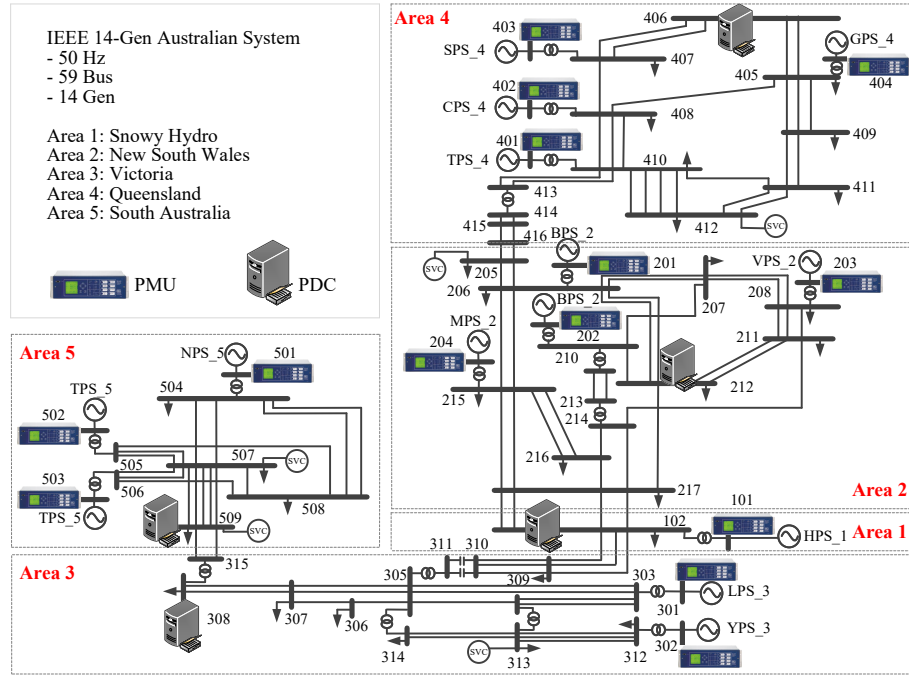


Figure 4.15: Test Case-III: Simplified 14-Generator Model of the Southeastern Australian Power System.

Table 4.8: Optimal TSA vectors in Case-III

Scenario	TSA Vector (ms)	Dropout Probability π_u			
		u301	u302	u501	u502
S2	$\alpha_{u301}=-24.99$ $\alpha_{u503}=+8.33$	0.37	0	0.41	0
S4	$\alpha_{c308}=-30$ $\alpha_{c509}=-30$	0.85	0.76	0.92	0.66

4.5.5 Solution Scalability

This subsection demonstrates the scalability of the proposed integrated detection and mitigation schemes on a large-scale system, i.e., the Simplified 14-Generator Model of the Southeastern Australian Power System [130, 136]. Illustrated in Fig. 4.15, this test system comprises 14 generators, five static VAR compensators (SVCs), 59 buses, and 104 lines, with voltage levels ranging from 15 kV to 500 kV. According to [136], all the generator buses are equipped with PMU (14 PMUs in total) whose data is collected by five regional PDCs. Without loss of generality, these PDCs are located in Buses 102, 212, 308, 406, and 509. Similar to test Case-II, the communication network is assumed to mirror the power grid configuration, with data forwarding trees between PMUs and

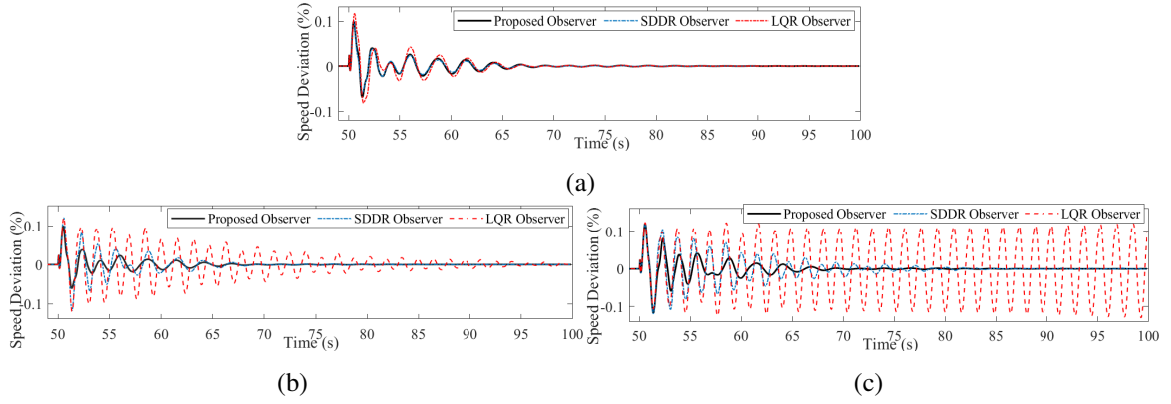


Figure 4.16: Post-attack speed deviation of Generator TPS-5 in Case-III during attack free scenario (a) S0 and TSA scenarios (b) S2 and (c) S4.

ANN-LF	82.6	14.38	20.09
CNN-LF	91.47	10.6	5.81
ANN-FF	98.39	2.26	0.85
CNN-FF	99.9	0.18	0.01
	ACC	FNR	FPR

Figure 4.17: TSA Detection Performance Indices in Case-III.

PDCs determined based on shortest path algorithm.

This system features multiple inter-area DLO modes with different range of frequency depending on loading conditions. During peak load condition, where the total load is 22,300 MW, five inter-area modes are exited with frequencies $\{0.57, 0.39, 0.33, 0.38, 0.22\}$ Hz [130]. As discussed in [136], to damp these inter-area DLO modes, a WADC can be integrated to modulate the excitation system of Generators HPS_1, BPS_2, YPS_3, TPS_4, and NPS_5 based on the measurements provided by PMUs $u101$, $u201$, $u302$, $u401$ and $u501$. According to Table 4.8, launching optimal TSAs in Scenarios S2 and S4 can disrupt the data collection of PDCs $c308$ and $c509$, resulting in the loss of data from PMUs $u301$, $u302$, $u501$, and $u502$. The impacts of the designed TSAs on the integrated WADC is evaluated following a three-phase short circuit on Line 305-307 between 50.00-50.05 s. As depicted in Fig. 4.16, the TSA in Scenario 2 notably deteriorates the system's damping performance when the WADC is integrated with LQR and SDDR observers. In Scenario S4, the significant data dropout during the optimal TSA results in undamped oscillations when using the LQR observer, as the WADC interacts with the local PSSs. This simulation serves as compelling

evidence that the TSA model holds validity in large-scale systems, highlighting how inadequately designed WADCs can potentially lead to undamped oscillations and system instability.

In Case III, the detection of TSAs necessitates the development of five CNN detection schemes, each tailored for a regional PDC. Leveraging similar assumptions and algorithms used in the previous case studies, a database has been constructed for training and testing these CNN detection schemes. As illustrated in Fig.4.17, akin to the outcomes in other cases, the proposed detection scheme exhibits notably higher accuracy compared to other learning-based models. Upon the detection of TSAs, the mitigation scheme is activated by updating the observer gain to be robust against post-TSA data dropout. As shown in Fig.4.16, the WADC integrated with the robust observer effectively dampens system oscillations in attack scenarios S2 and S4, a feat not achieved by the LQR and SDDR observer cases. Hence, the proposed integrated detection and mitigation schemes stand as effective countermeasures against TSAs in large-scale systems.

Chapter 5

Security Enhancement of Grid-Supporting Functions in Inverter-Based Resources

5.1 Problem Statement

Inverter-based resources (IBRs) have received a surge of attentions and interests from electricity producers and governmental initiatives worldwide to deal with climate change and energy security concerns [137]. Nevertheless, the dominant integration of IBRs has exposed power grids to voltage and frequency stability challenges, primarily due to their low-inertia nature and grid-following control structure [138–140]. To tackle these challenges and enhance hosting capacity, recent IEEE standards and grid codes mandate grid-connected IBRs to offer grid-supporting functions as specified in IEEE 2800, IEEE 1547-2018, and IEEE 1547.1-2020 [141]. To implement grid supporting functions, the IBRs should be able to communicate with the utility control center through communication protocols, e.g., SunSpec Modbus, IEEE 2030.5, IEEE 1815, and IEC 61850 [142]. However, deployment of communication protocols make IBRs prone to various threats originated from cyber-layer, including denial of service (DoS), data integrity and replay attacks [143, 144]. These threats compromise the functionality of closed-loop controllers of IBRs, thereby endangering inverter and

power grid stability. To deal with this problem, it is crucial to have a comprehensive understanding of the potential consequences of cyber-attacks on IBRs and enable system to detect them while distinguishing them from normal system operation contingencies.

5.2 Literature Review and Research Gaps

IBRs are commonly employed multiple-timescale feedback control system including phase-locked loop (PLL), direct dc-link voltage loop, and alternative voltage and current control loops [145]. These control system regulates the inverter's exchange of active and reactive power with the power grid. The interplay and cross-coupling of this control system with the electromagnetic dynamics of synchronous generators and the transient behavior of passive components in the power grid, can result in oscillations spanning a wide frequency range, from sub-synchronous frequencies to switching frequencies [145]. For instance, in 2013 and 2017, two oscillations with resonance frequency of several hundred Hz and 1270 Hz were reported in an islanded offshore grid in Germany and a HVDC transmission system in China, respectively [146]. These oscillations can appear with negative damping, leading to undesired harmonic voltage and current distortion and resonance, trigger protection functions, and endanger power grid stability. Numerous studies have been conducted to identify these oscillations and address the harmonic stability issues in IBRs. For instance, aiming at identifying and analyzing harmonic resonance of IBRs, the authors in [146] and [147] proposed two harmonic state-space and impedance-based models, respectively. To improve stability of IBRs connected to a weak grid, the authors in [148] proposed a impedance-phased compensation control approach that increases inverter's phase margin. Additionally, [147] proposed a strategy based on virtual harmonic resistance to mitigate resonances within the deadbeat current control bandwidth. However, these papers primarily focus on addressing the harmonic instability of IBRs from a power system and control perspective, largely overlooking the vulnerabilities in the cyber layer.

Real-world incidents have demonstrated an increase in both the frequency and sophistication of cyber-attacks targeting IBRs. For example, a DoS attack occurred in parts of California, Utah, and Wyoming, disrupting communication between about 500 MW wind and solar IBRs and the utility control center [143]. In 2022, a similar attack was reported in Germany, where a ransomware team

compromised the wide-area monitoring and operation of two wind turbines [143]. These vulnerabilities have prompted researchers to study the potential consequences of cyber-attacks on IBRs and to develop appropriate countermeasures. For example, the studies in [149] demonstrated that false data injection attack (FDIAs) on control schemes of modular multilevel converter (MMC) can lead to triggering protection relays. The impact of cyber-attacks on PLLs was investigated in [150], showcasing that manipulating PLL parameters can degrade voltage profiles and cause system-wide power-angle instability. Furthermore, studies in [151] demonstrated that manipulating the frequency measurement at the point of interconnection (POI) of a wind farm can compromise the functionality of the active power controller, leading to a wind farm trip. As an effective countermeasure, [152] leveraged the harmonic state space (HSS) models to develop a physics-data-based for detecting data integrity attacks on PV farms. A reinforcement learning-based model is also proposed in [153] to detect FDIAs on MMCs. Although these studies have made valuable contributions to enhancing the security of IBRs, the literature lacks exploration of the possibility of harmonic instability in IBRs induced by cyber attacks.

5.3 Attack Model

This section presents the resonance FDIA model on IBRs, detailing the attacker's objective, intrusion path, and the methodology for attack vector construction.

5.3.1 Attacker's Objective

The cyber-physical scheme of a LCL-type inverter is illustrated in Fig. 5.1. The communication protocols employed in this scheme are elaborated in [142]. In this attack, the adversary introduces sinusoidal disturbances with a certain resonance frequency into the measurement/control signal that communicates between sensors/grid-supporting functions and the IBR's controller, aiming at forcing the targeted IBR into resonance with the power grid, resulting in harmonic instability.

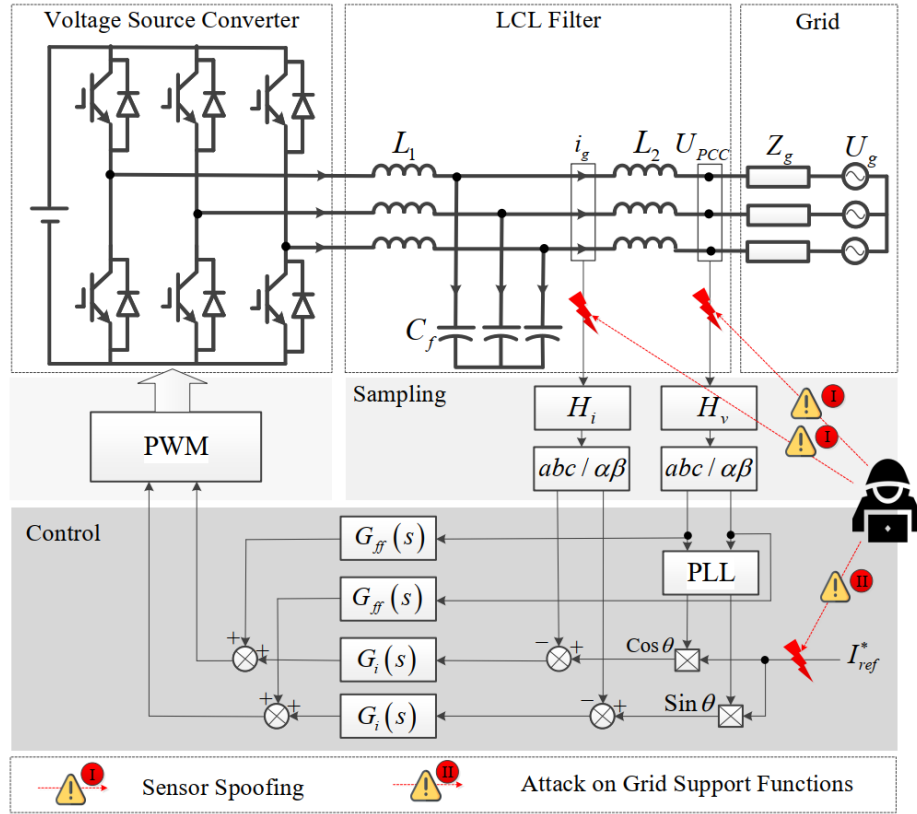


Figure 5.1: The overall scheme of LCL-type inverter and attack surface.

5.3.2 Intrusion Path

The adversary can follow two intrusion paths. In Path I, the adversary can execute a sensor spoofing attack through firmware modification, as illustrated in Fig. 5.1. Alternatively, the attacker can physically introduce external electromagnetic signals to disrupt the magnetic field intensity of the Hall sensors that measure current and voltage. This can be achieved by attaching or placing an electromagnet near the target inverter [143]. On the other hand, in Path II, to compromise the control signal between grid-supporting applications and the IBR controller, the adversary can execute a man-in-the-middle (MITM) attack on the IBR's site router or data aggregator. To achieve this, the adversary need to steal the transport layer security (TLS) certificate key of the inverter control center or session keys, and then set up a MITM attack. For instance, the authors in [154] implemented a practical MITM attack on a router between the Raspberry Pi gateway of a PV inverter and the control center communicating through the IEC61850 protocol. Further discussion on practical intrusion paths to target IBRs are available in [143].

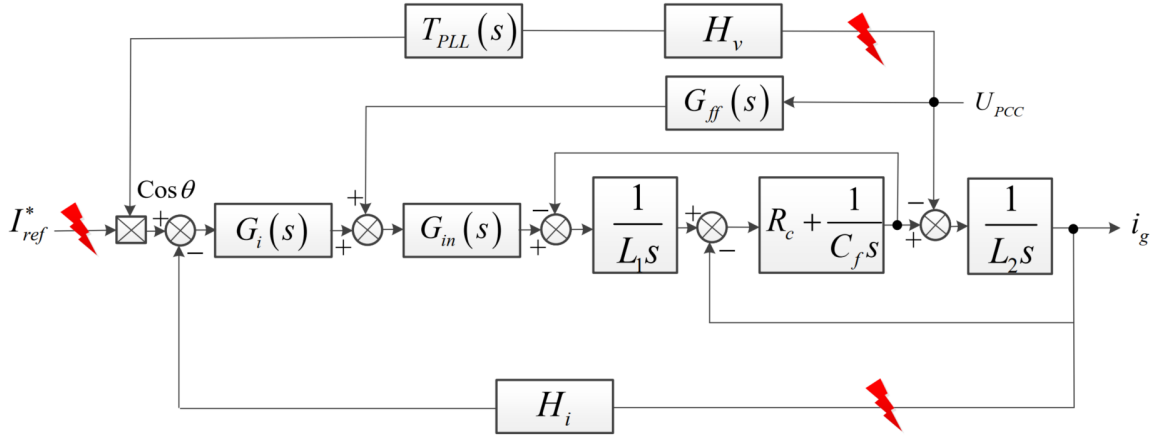


Figure 5.2: Diagram of LCL-type inverter under resonance FDIA.

5.3.3 Attack Vector Construction

Upon successful penetrating into the system, the attacker needs to inject the resonance attack vector into the communicated measurement or control signals of the inverter as follows:

$$S_a(t) = S_a^m \cos(\omega_r t) \quad (5.1)$$

where S_a^m and ω_r denote the magnitude and frequency of injected resonance attack vector. To capture the resonance frequency the attacker can follow two approaches. In former, the attacker takes advantage of frequency scanning techniques, which entail injecting voltage/current perturbation into the physical layer of inverter and eavesdropping voltage and current sensors. Therefore, the attacker must inject the perturbation signal with various frequency range and calculate the equivalent impedance observed from the inverter's PCC. More details regarding this approach is provided in [155].

Alternatively, the attacker can utilize impedance-based models of IBRs to determine the resonance frequency. To do so, the attacker should initially obtain the parameters of the inverter and the power grid using various methods, such as exploiting insiders [93], conducting reconnaissance activities [94], compromising the power grid's databases [95], or using publicly available data [95]. Afterward, the adversary can utilize the equivalent block diagram of IBRs, e.g., Fig. 5.2 for LCL-type inverter, to analyze frequency response of the under-attack inverter. It is worth noting that since

LCL-type inverters use the same control method for both the α -axis and β -axis without any inter-connection, this thesis focuses only on the α -axis to derive the impedance model of grid-connected inverters. As Fig. 5.2 illustrates, the PLL synchronizes the inverter current i_g injected to the grid based on the voltage at PCC (U_{PCC}). The transfer function of the synchronous rotating reference-frame Phase-Locked Loop (PLL), which is the most commonly used software-based PLL in inverters, can be expressed as follows [148]:

$$T_{pll}(s) = \frac{K_p^{pll}(s - j\omega_0) + K_i^{pll}}{2(s - j\omega_0)^2 + 2U_{PCC}^m (K_p^{pll}(s - j\omega_0) + K_i^{pll})} \quad (5.2)$$

where K_p^{pll} and K_i^{pll} present the PLL's controller gains, U_{PCC}^m denotes the peak PCC voltage, and ω_0 refers to perturbation angular frequency. Additionally, the proportional resonant (PR) controller modulates the inverter current, which is represented as follows:

$$G_i(s) = K_p^i + \frac{K_r^i \omega_c s}{s^2 + 2\omega_c s + \omega_0^2} \quad (5.3)$$

in which, K_p^i and K_r^i denote controller gains, while ω_c and ω_0 are the grid bandwidth and the fundamental frequency, respectively. The PMW can also be modeled by the inverter bridge gain K_{PWM} and delay of controller as follows:

$$G_{in}(s) = K_{PWM} e^{-1.5sT_s} \quad (5.4)$$

where T_s is sampling time. Disregarding the grid voltage feedforward $G_{ff}(s)$, the PLL and output admittances of the inverter can be calculated as transfer functions (5.5) and (5.6), respectively.

$$Y_{PLL}(s) = \frac{-(1 + C_f R_c s) H_v T_{pll}(s) G_i(s) G_{in}(s) I_{ref}^*}{H_o(s)} \quad (5.5)$$

$$Y_o(s) = \frac{1 + C_f L_1 s^2 + C_f R_c s}{H_o(s)} \quad (5.6)$$

In (5.5) and (5.6), L_1 and L_2 are the inverter-side and grid-side filter inductance, respectively; R_c and C_f are the resistance and capacitance of the parallel branch of the filter, respectively; and H_v

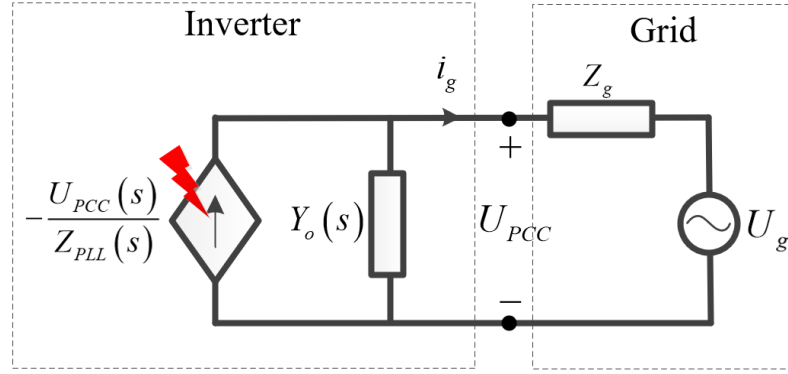


Figure 5.3: Equivalent circuit of grid-connected LCL-type inverter.

and H_i refer to the feedback coefficient of voltage and current of the inverter. Additionally, H_o can be calculated as follows:

$$H_o(s) = C_f L_1 L_2 s^3 + C_f (L_1 + L_2) R_c s^2 + (L_1 + L_2) s + G_i(s) G_{in}(s) H_i (1 + C_f R_c s) \quad (5.7)$$

Eventually, the equivalent admittance of the inverter can be calculated as (5.8).

$$Y_{in}(s) = Y_o(s) + Y_{PLL}(s) \quad (5.8)$$

Given the equivalent circuit in Fig. 5.3, the grid connected LCL-type inverter for harmonic stability analysis can be described as:

$$\overbrace{\begin{bmatrix} Y_{in1}^h + Y_1^h & -Y_1^h \\ -Y_1^h & Y_1^h + Y_g^h \end{bmatrix}}^{Y_{SYS}^h} \begin{bmatrix} U_{in1} \\ U_{PCC} \end{bmatrix} = \begin{bmatrix} -Y_{PLL1}^h U_{in1} \\ Y_g^h U_{PCC} \end{bmatrix} \quad (5.9)$$

where h presents the harmonic order. Therefore, the system impedance matrix can be calculated as follows:

$$Z_{SYS}^h = Y_{SYS}^h{}^{-1} \quad (5.10)$$

Z_{SYS}^h represents how a voltage variation spreads through the system after a harmonic current injection at a specific node. Therefore, injecting harmonic distortion in this circuit at the frequency

range where the Z_{SYS}^h for the inverter's PCC is maximized can result in significant voltage distortion and harmonic instability [156]. On this basis, the resonance attack vector frequency ω_r in (5.1) is designed within this frequency range. Furthermore, the magnitude S_a^m should be kept within the normal fluctuation range of legitimate signals to maintain the stealthiness of the attack.

5.4 Proposed Countermeasure

5.4.1 Wavelet-Enabled Resonance Attack Detection Scheme

Resonance attacks can have harmful effects on systems, necessitating the implementation of effective detection mechanisms. The methods employed for attack detection can be broadly classified into two main categories: model-based and data-driven approaches. Model-based detection methods depend on the assumption that the system remains accurate and experiences minimal changes. However, this assumption is often impractical as systems can undergo significant variations due to changes in operating conditions and the presence of variable parameters and components [157]. Consequently, model-based methods may not be suitable for systems with fluctuating characteristics. Conversely, data-driven detection methods offer greater flexibility and are more adept at handling changes in operating conditions and system uncertainties [157]. These methods rely on analyzing data to detect anomalies and potential attacks, making them more adaptable to dynamic environments [157]. A critical aspect of data-driven methods is the extraction of relevant features, which significantly influences the effectiveness of the detection process.

The selection of appropriate features depends on understanding the nature of the attack's impact. Given the characteristics of resonance attacks, frequency-domain analysis emerges as a suitable approach for feature extraction. This feature selection approach allows for the identification of resonant frequencies indicative of an attack, thereby enhancing detection accuracy. To achieve this, this thesis employs the discrete wavelet transform (DWT) to extract frequency features. The details of this process are described in the following.

Table 5.1: The poor performance of well-known machine learning models when used time-domain features.

Methods	Accuracy		TPR-Normal		TPR-Attack		FPR-Normal		FPR-Attack	
	TV	TE	TV	TE	TV	TE	TV	TE	TV	TE
Fine Tree	66.5%	69.2%	72.9%	92.2%	60.3%	45.3%	27.1%	7.8%	39.7%	54.7%
Medium Tree	67.9%	66.6%	92.6%	92.9%	48.4%	39.2%	7.4%	7.1%	56.6%	60.8%
Linear SVM	55.7%	52.8%	55%	49%	56.4%	56.7%	45%	51%	43.6%	43.3%
Quadratic SVM	64.8%	64	82%	80%	47.8%	47.3%	18%	20%	52.2%	52.7%
Fine KNN	64.7%	67%	64.8%	71.4%	64.6%	62.4%	35.2%	28.6%	35.4%	37.6%
Medium KNN	68.1%	68.8%	83.9%	85.1%	52.6%	51.8%	16.1%	14.9%	47.4%	48.2%
Medium NN	69.9%	71.4%	83.8%	84.7%	56.3%	57.6%	16.2%	15.3%	43.7%	42.4%
Wide NN	66.7%	69.8%	73.3%	77.6%	60.1%	61.6%	26.7%	22.4%	39.9%	38.4%

5.4.2 Frequency Features Extracted by DWT

The DWT is a powerful technique for frequency domain analysis, making it highly suitable for our research objectives. Unlike traditional time-domain methods, the DWT offers superior time-frequency localization capabilities. This characteristic allows DWT to effectively capture both the frequency components and their temporal evolution within a signal [158]. Such dual-domain analysis is particularly vital for detecting resonance attacks, as it enables the identification of changes in frequency content over time, which are indicative of an ongoing attack. The ability to monitor and analyze these dynamic variations makes DWT an invaluable tool in the feature extraction of resonance-based intrusions. Table 1 demonstrate the poor performance of data-driven methods that are used in time-domain features extractions techniques. These well-known ML methods are trained and tested with statistical features, including mean, max, standard deviation, etc, that are extracted from time-domain suignal . Table 5.1 illustrates the suboptimal performance of data-driven approaches used input data provided by time-domain features extraction tourniquets [158]. These established ML techniques are both trained and evaluated using a variety of statistical features derived from time-domain signals. Specifically, features such as the mean, maximum, minimum, standard deviation, etc. This evaluation aims to highlight the insufficiency of time-domain features extraction techniques in effectively capturing the complexities of attack patterns within the data.

Another significant advantage of the DWT rather that time-domain feature extraction methods is its adaptability in analyzing signals across multiple scales. This merit enhances its versatility, enabling it to effectively address various types of resonance attacks that manifest across different frequency ranges and amplitudes [159]. By decomposing signals into components that reveal

both temporal and frequency information, DWT allows for precise detection and characterization of anomalies, thereby providing robust defense mechanisms against resonance-based interferences.

The DWT offers several advantages over other frequency-based analysis methods, as outlined below:

- **Localization and Multi-Resolution Capability:** In contrast to the Short-Time Fourier Transform (STFT), which uses a fixed window size, DWT employs variable-sized windows. This flexibility allows for a more nuanced analysis of signals containing both high and low-frequency components, ensuring that subtle variations are not overlooked. Additionally, DWT tends to be more computationally efficient than the Continuous Wavelet Transform (CWT) and even some implementations of STFT, particularly when handling large datasets or real-time detection scenarios. This computational efficiency is crucial for practical deployment in security systems [160].
- **Extraction from Non-Uniform Signals:** Resonance attacks may induce non-uniform signal variations. The ability of DWT to decompose signals into different frequency bands makes it more effective at capturing these non-uniformities compared to methods like Power Spectral Density (PSD) analysis [160].
- **Handling Non-Stationary Signals:** Many resonance attacks involve non-stationary signals, where the frequency content changes over time. DWT is particularly adept at analyzing such signals because it does not assume signal stationarity, unlike traditional spectral methods. This makes DWT a powerful tool for the analysis and detection of non-stationary signal components typically associated with such attacks. The following subsection provides a comprehensive description of DWT implementation for feature extraction [160].

The DWT is a powerful tool for signal processing, capable of analyzing both stationary and non-stationary signals. Its efficacy lies in its ability to decompose a signal into various frequency components while retaining temporal information, which is particularly useful for extracting relevant features in diverse applications such as image processing, audio analysis, and biomedical signal processing.

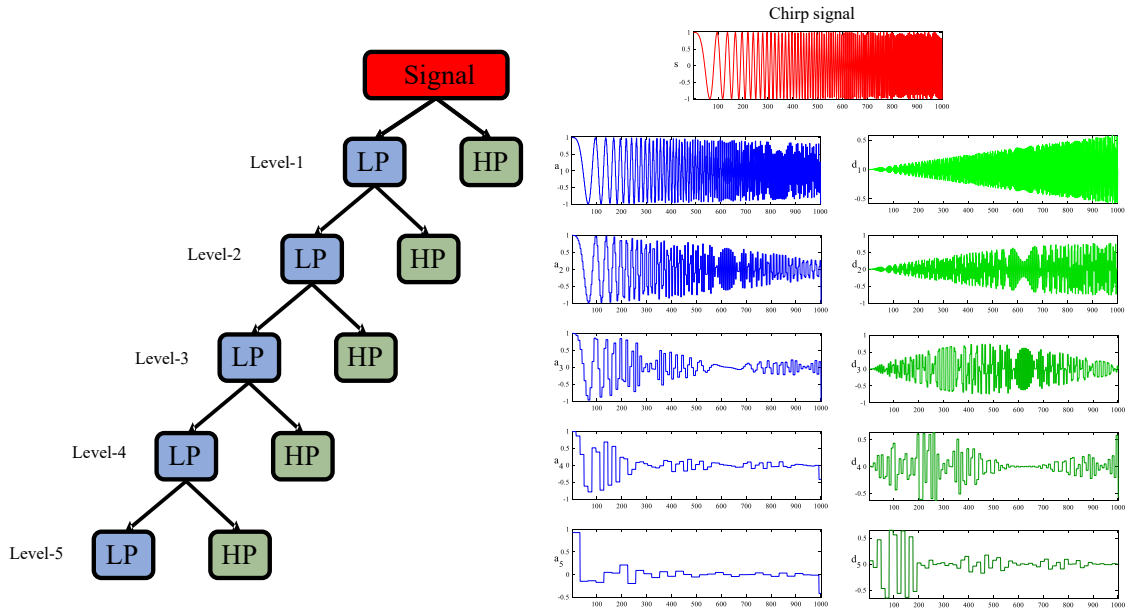


Figure 5.4: Overview of applying a DWT on a chirp signal, its approximation and details levels.

The implementation of DWT encompasses a sequence of critical steps that facilitate signal analysis and compression. The process begins with the signal being subjected to a cascade of high-pass and low-pass filters. These filters decompose the signal into various levels, each yielding an approximation and detail components. The approximation represents the low-frequency components of the signal, while the detail coefficients capture the high-frequency elements. This decomposition can be recursively applied, generating a multi-level, hierarchical representation of the signal. This hierarchical decomposition allows for efficient analysis and processing, making DWT a powerful tool in various applications such as feature extraction. The extraction of features can be conducted through details and approximations at various levels, tailored to the specific characteristics of the given problem. Fig. 5.4 shows an overview of applying a DWT on a chirp signal, its approximation and details levels.

In mathematical terms, the DWT can be formally expressed as follows: consider $x[n]$ as the input signal, $g[n]$ the high-pass filter, and $h[n]$ the low-pass filter. The convolution operation of $x[n]$ with these filters, subsequently followed by down sampling, yields the detail coefficients $d[n]$ and the approximation coefficients $a[n]$, respectively [161]:

$$d[n] = \sum_k x[k].g[2n - k] \quad (5.11)$$

$$a[n] = \sum_k x[k].h[2n - k] \quad (5.12)$$

The coefficients derived from the initial decomposition undergo subsequent decompositions across multiple levels, facilitating the extraction of intricate details across various scales. In the realm of feature extraction, the detail coefficients obtained from diverse decomposition levels hold significant importance. These coefficients capture transient features and edge information inherent within the signal, characteristics often pivotal in discerning patterns within recognition tasks. Through suitable selection of decomposition levels and relevant coefficients, a compact and informative set of features can be obtained [161].

5.4.3 Statistical Features

As previously discussed, the integration of mathematical and statistical features, including mean, maximum, minimum, and L2-norm, extracted from the initial two levels of DWT details, has yielded significant enhancements in the efficacy of data-driven methodologies. However, there remains a necessity for the inclusion of further features to optimize performance. Among these features, derivative characteristics emerge as particularly relevant, especially for scenarios characterized by evolving dynamics.

Derivative features entail the computation of a signal's rate of change concerning an independent variable, commonly time. This computation employs diverse mathematical methodologies, including differentiation, to determine metrics such as first-order derivatives (slope) and second-order derivatives. These features provide insights into the temporal or spatial evolution of the input data, exhibiting sensitivity to rapid alterations or fluctuations therein, thereby facilitating the identification of anomalies or noteworthy occurrences. Moreover, by capturing the rate of change, derivative features can improve the discriminative power of machine learning models. They capture additional information that may not be fully extracted by raw data, leading to enhanced detection and classification performance. Within the context of this investigation, we incorporate the squared values of

the first and second-order derivatives of each temporal window's signals, along with their respective DWT-derived d1 and d2 levels, as supplementary features.

5.4.4 Optimized Wide Neural Network Classifier

This thesis employs wide neural network empowered by Bayesian optimization to effectively detect resonance attack while distinguishing them from normal operation conditions. Wide neural networks offer a multitude of advantages and flexibilities in contrast to alternative data-driven methods such as SVM, Fine-KNN, and Fine-tree for the purpose of resonance attack detection and classification in this system [162]. Foremost, their capacity to manage intricate non-linear relationships within the data is invaluable, especially in contexts where feature interrelations are non-linear. Additionally, wide neural networks excel in autonomously discerning relevant features from the data, diminishing the necessity for manual feature engineering. Their scalability facilitates the efficient handling of substantial datasets and high-dimensional feature spaces prevalent in attack detection scenarios [162]. Furthermore, their architectural flexibility empowers researchers to explore diverse network structures to enhance performance, complemented by techniques such as transfer learning which further augment their efficacy. Wide neural networks also possess the capability to adapt to shifts in data distribution over time, rendering them suitable for dynamic environments. While interpretability may necessitate additional methodologies, approaches like feature importance analysis can provide insights into the factors influencing the network's decision-making process, thereby augmenting overall comprehension [162].

To achieve the best performance in detecting attack and classifying all classes the wide neural network is retuned by replacing Stochastic Gradient Descent with Momentum (SGDM) to a new optimizer that is Bayesian optimization. SGDM is a variant of the standard Stochastic Gradient Descent (SGD) optimization algorithm commonly used in training neural networks. In SGDM, along with the gradient of the current iteration, a momentum term is also considered, which is a fraction of the update vector from the previous iteration. This momentum term helps accelerate the optimization process by continuing in the direction of previous updates and smoothing out oscillations in the gradient descent trajectory, leading to faster convergence and potentially escaping local minima more effectively [162]. Despite these advantages, replacing SGDM with a Bayesian

Table 5.2: The Parameters of The Test Case Grid-Connected LCL-Type Inverter

Parameters	Value	Parameters	Value
L_1/ L_2	0.5 mH/ 0.15 mH	R_c/ C_f	0 Ohm/ 20 μF
R_g/ L_g	0.2 Ohm/ 0.5 mH	ω_c/ ω_0	5/ 100 π
k_p^i/ k_r^i	10/ 500	k_p^{pll}/ k_i^{pll}	10/ 500

optimizer for attack detection and classification yield better results due to its ability to efficiently explore the hyperparameter space and adaptively select hyperparameters that maximize the performance metric, such as accuracy or FNR. Unlike SGDM, which relies on manual tuning of hyperparameters and might overlook optimal configurations, the Bayesian optimizer dynamically adjusts its exploration-exploitation trade-off based on the observed performance, effectively navigating the high-dimensional space to discover configurations that lead to improved detection and classification accuracy [162]. Additionally, the Bayesian optimizer's ability to model the uncertainty in the objective function allows it to make informed decisions, potentially leading to better generalization and robustness of the attack detection and classification models across different datasets and scenarios.

5.5 Numerical Results and Discussion

This section investigates the consequences of the defined attack model and the performance of the proposed wavelet-enabled resonance attack detection scheme on a test case LCL-type inverter in Fig. 5.1. The information of the test case is provided in Table 5.2.

5.5.1 Impact of Resonance Attack

To investigate the impact of attack by performing time-domain simulation, this thesis implemented the test case under resonance FDIAs in MATLAB Simulink 2022b environment. This thesis assumes that the attacker has knowledge of the system's parameters and uses the impedance-based model described in Section 5.3.3 to determine the inverter's resonance frequency with the grid. Given that, the magnitude and phase of the inverter impedance can be calculated, as shown in Fig.5.5 where Z_s , Z_{sg} , and Z_{gg} denote the equivalent impedances at the inverter PCC, between the inverter and the grid, and grid bus, respectively. As depicted in Fig.5.5-(a), the resonance frequency

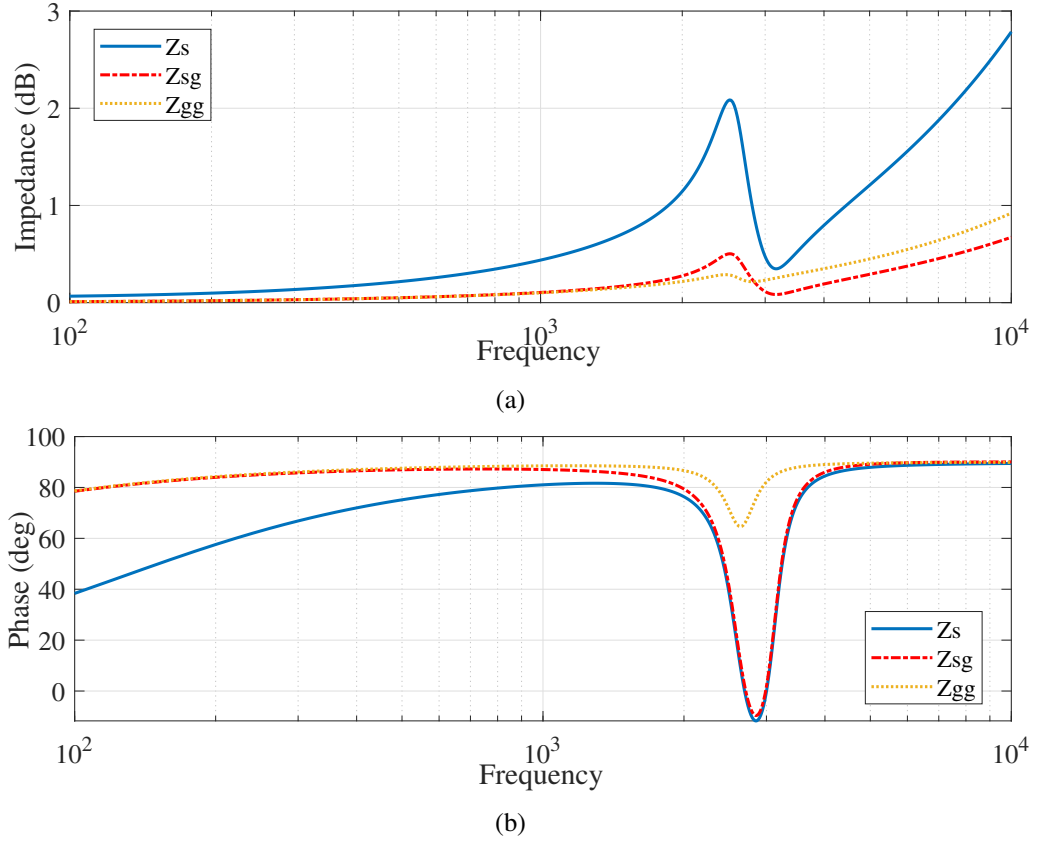


Figure 5.5: Bode plots of output impedance of the inverter.

falls between 2500Hz and 2700Hz, corresponding to the 50th-54th harmonic orders. Figure 5.5-(b) illustrates that the inverter's phase margin indicating its stability margin is also minimized. Therefore, any harmonic distortion generated at the cyber-layers of the inverter in this frequency range can manifest as amplified voltage distortion at the inverter's PCC and lead to inverter harmonic instability.

To analyze the time-domain behavior of the test case inverter under various resonance FDIA scenarios, this thesis injects the attack vector (5.1) into the signal I_{ref}^* provided by the grid-supporting functions. The attack magnitude S_a^m is assumed to be 5% of the magnitude of the manipulated signal, while the frequency ω_r varies from 1500Hz to 3500Hz. In this simulation, the resonance FDIA is initiated at 25ms, followed by a 10% step change in reference reactive current ($I_{q,ref}^*$) at 50ms. As Figure 5.6 illustrates, during the FDIA resonance at a frequency of 1500Hz, the attack induces a slight distortion in the current and voltage waves at the inverter's PCC. Similarly, in the

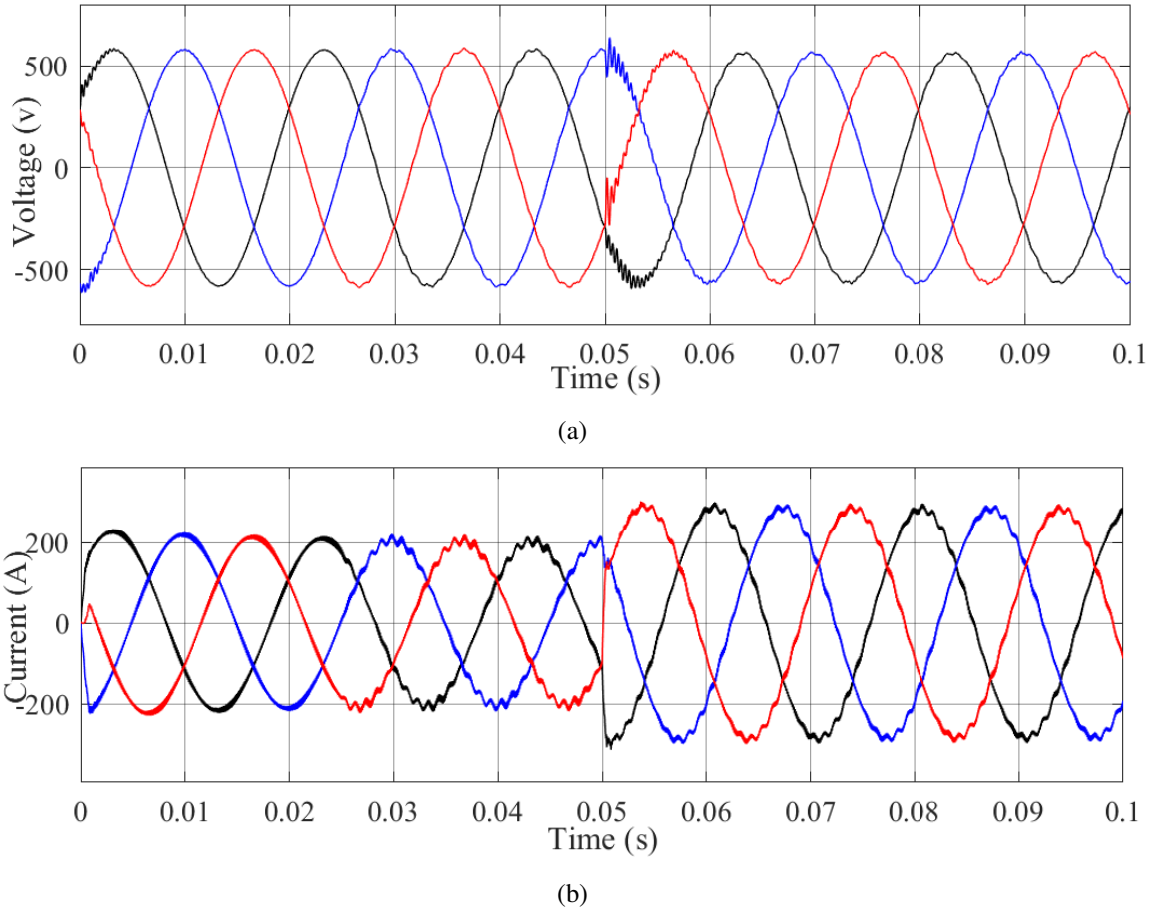


Figure 5.6: Resonance FDIA with frequency of 1500 Hz (a) Voltage at PCC and (b) inverter current.

case of FDIA resonance at 3500Hz, no significant oscillation or resonance occurs. In contrast, for the FDIA resonance at 2500Hz, which falls within the calculated inverter resonance frequency range, extensive harmonic distortion in both current and voltage is observed, as shown in Figure 5.8. This experiment highlights the threat posed by carefully designed resonance FDIAs when launched within the harmonic resonance range of the inverter. The resulting post-attack harmonic distortion can not only damage system equipment but also trigger protection devices, leading to the tripping of the inverter.

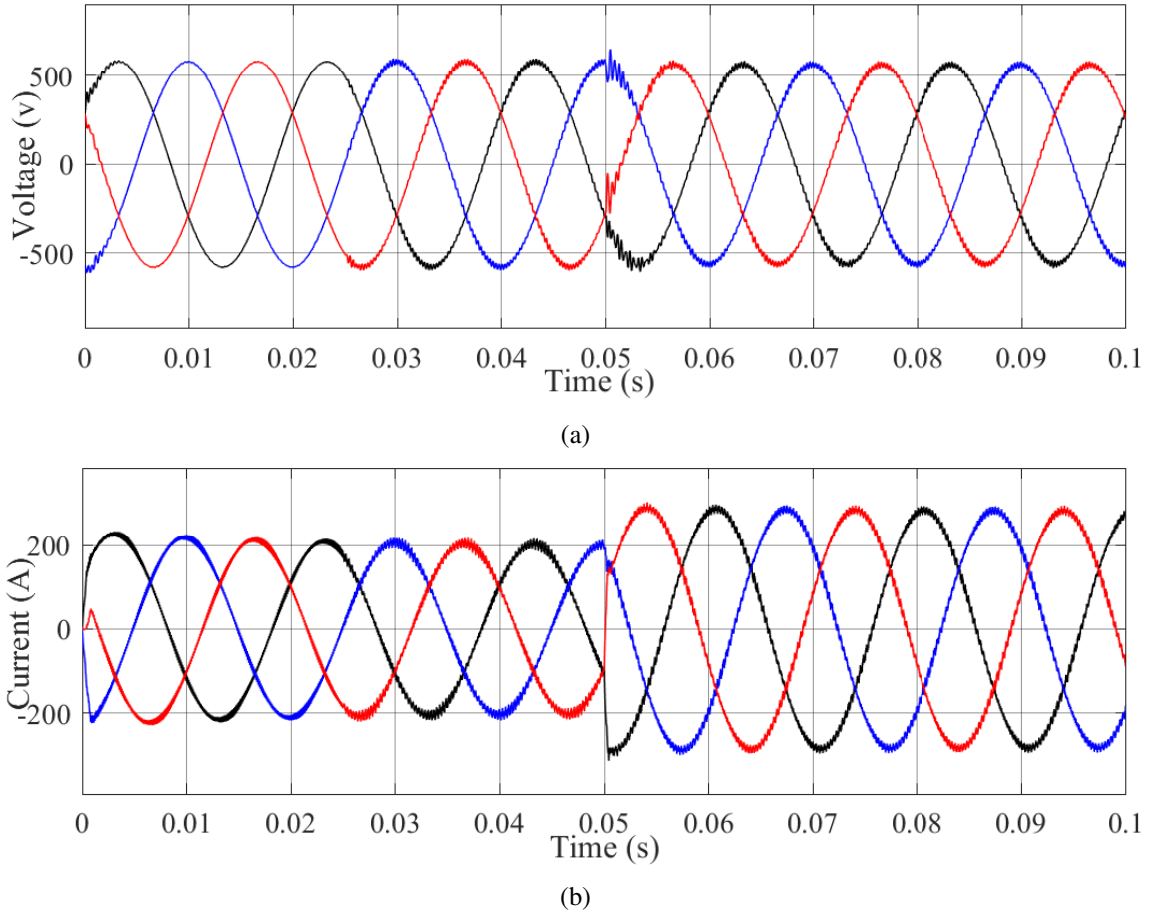


Figure 5.7: Resonance FDIA with frequency of 3500 Hz (a) Voltage at PCC and (b) inverter current.

5.5.2 Performance of the Proposed Resonance Attack Detection Scheme

In this study, the detection of attacks is based on signals obtained from the voltage and current measurements at the PCC. These signals are analyzed within discrete time-windows, each comprising 500 samples, extracted at a sampling rate of 256 samples per cycle. Attack instances are characterized by a 5-10% gain, following a normal distribution with a mean frequency of 2500 Hz and a variance of 500 Hz. Both normal operation and attack cases encompass a range of operating points. Fig. 5.9 illustrates the various levels of detail for both normal operation signals and attack signals within a given time-window. As depicted, the differences in the first two levels of detail between normal and attack signals are highly discernible. Conversely, distinguishing differences in the primary signals proves to be more challenging. This marked contrast at the initial levels of detail justifies their selection as input features for the attack detection system. It is worth noting that the

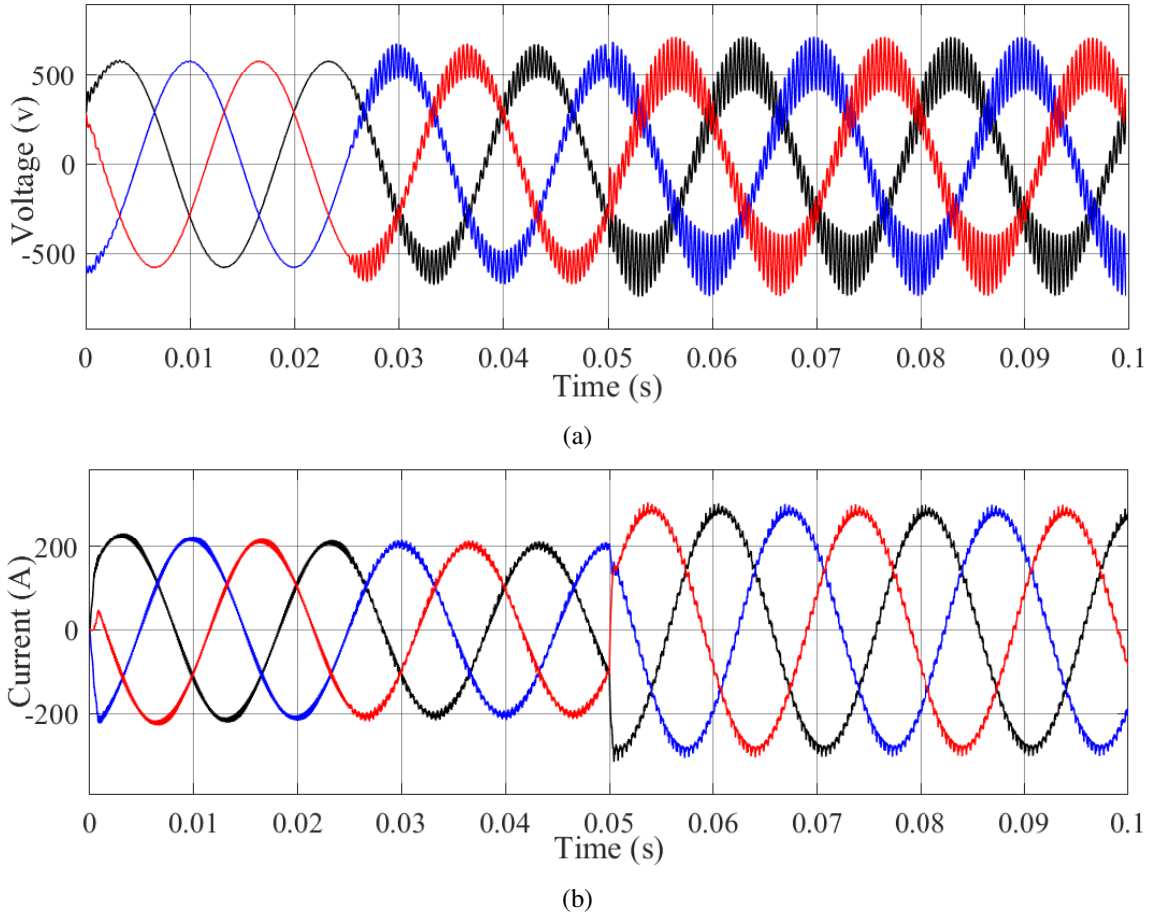


Figure 5.8: Resonance FDIA with frequency of 2500 Hz (a) Voltage at PCC and (b) inverter current.

choice of these levels can be tailored based on the specific nature and resonance frequency of each system.

In the operation of a system, various conditions beyond typical and attack scenarios occur, such as fluctuations in controllable parameters and occurrences of short circuit faults. These events are able to actuate resonance frequency of system and manifest across two levels, denoted as d1 and d2 in DWT, exhibiting characteristics related to both normal and attack states. Despite DWT's capability to discern between normal and attack signals, additional discriminative features are imperative to accurately distinguish among normal operation, attacks, and other natural anomalies like step changes in currents value.

Fig. 5.10 illustrates that step changes, such as a 10% deviation in the reference values of I_d and

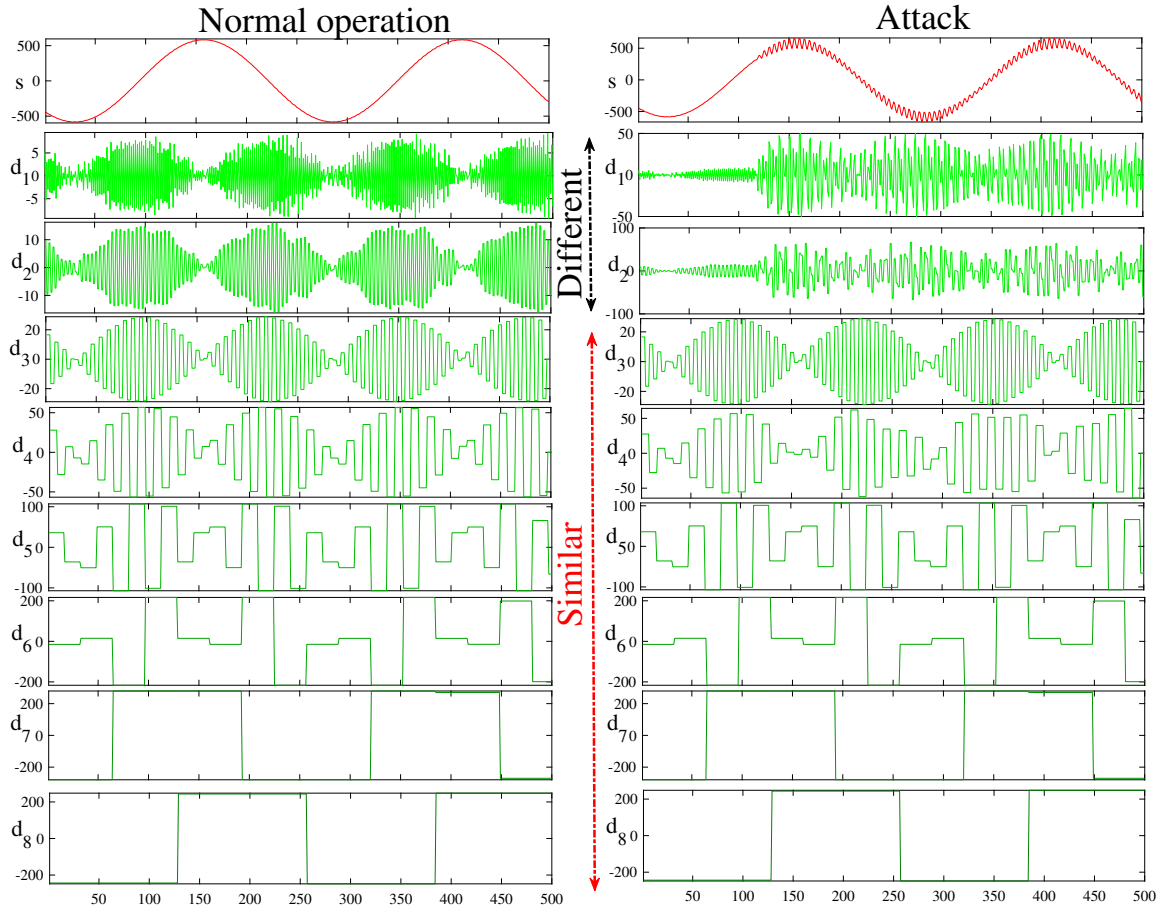


Figure 5.9: Overview of applying a DWT on PCC's voltage signal during normal and attack conditions.

I_q , exhibit distinct characteristics between those of normal and attack signals. Consequently, data-driven methodologies may encounter challenges in effectively detecting diverse system conditions. To indicate this necessity for more refined features, three distinct data-driven approaches—namely, fine tree, SVM, and medium neural network—are tuned and evaluated using features extracted from the d1 and d2 levels of DWT. Fig. 5.11 displays the outcomes achieved from the classification of various states, encompassing normal operation, attacks, step changes, and short-circuits. While the obtained results appear promising, the false negative rate (FNR) proves to be inadequate for evaluating the efficacy of this system. The FNR stands as a pivotal metric for this particular system due to its significance in discerning instances where potentially hazardous events might go undetected. This parameter assumes paramount importance in ensuring the system's reliability and effectiveness in real-world applications. Therefore, the outcomes underscore the requirement for enhanced

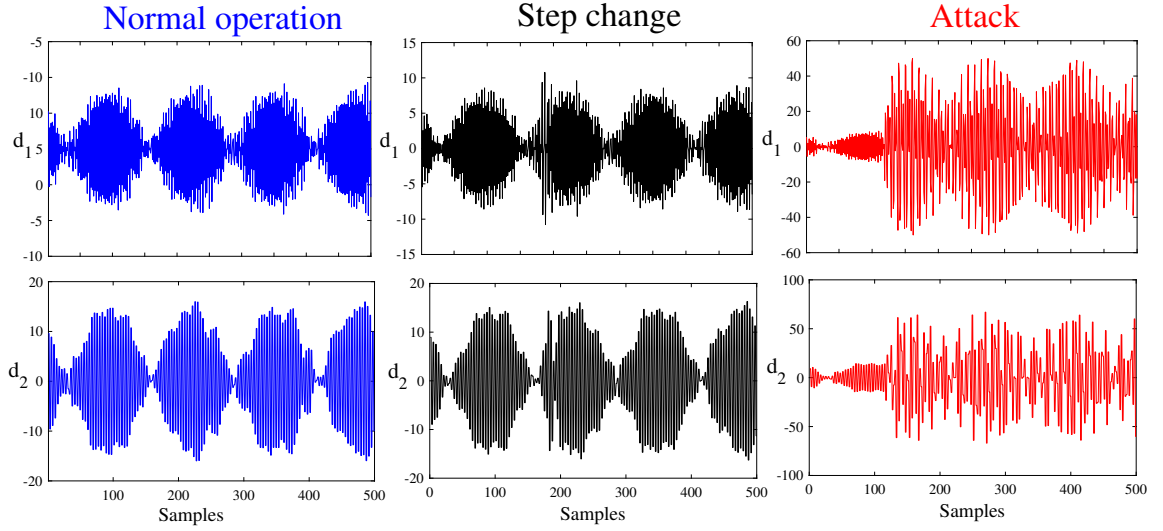


Figure 5.10: Two first levels of DWT of normal operation, step change, and attack.

feature extraction methods to discern the nuances among the system's natural events effectively.

5.5.3 Impact of Integration Statistical Features

Fig. 5.12 depicts the outcomes derived from employing data-driven methodologies for detection and classification, integrating the aforementioned features. A comparative examination with Fig. 5.11 reveals notable enhancements in the performance of these data-driven approaches, alongside an acceptable FNR. Following a thorough examination of feature extraction techniques, it becomes evident that further advancements in detection and classification can be attained by refining the structure and efficacy of data-driven techniques. Among these methodologies, wide neural networks emerge as particularly adaptable to refinement.

5.5.4 Performance of the Optimized Wide Neural Network model

To train the proposed optimized neural network model, this thesis utilized a dataset consisting of 4000 time-windows. Each time-window is composed of 500 samples, which were extracted at a sampling rate of 256 samples per cycle. This data set comprises four distinct labels that are as follows: i) Normal operation: this label encompasses normal operation of system across various normal system's operating points, ii) Attacks: these events are marked by a 5-10% gain, following

a normal distribution with a mean frequency of 2500 Hz and a variance of 500 Hz. Such characteristics are indicative of anomalous activities or potential cybersecurity threats within the system.

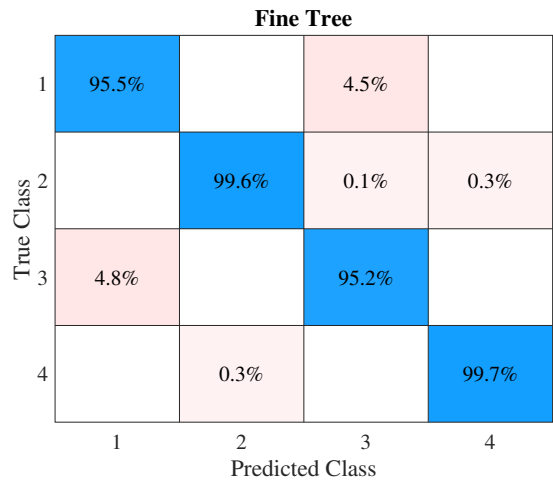
iii) Step Changes in Reference Values: this category includes sudden alterations in the reference values of I_d and I_q ; and iv) Short Circuit Events: These are defined by specific parameters (detail the parameters here) and represent critical faults within the system. Upon completion of the training phase, the model's performance was evaluated using a set of 1500 time window samples. The outcomes of this evaluation are illustrated in Fig. 5.13-(a) indicated that the wide neural network that is used Bayesian optimizer has improved the performance of detection system in our problem. Fig. 5.13-(b) also area under the curve (AUC) of receiver operating characteristic (ROC) are commonly used as evaluation metrics in the performance of data-driven detection methods. Since a perfect classifier would have an AUC of 1, indicating it achieves perfect separation between classes, this figure indicates the prefect performance of the proposed method.

In the process of training the optimized neural network, the iteration of hyperparameters plays a critical role. Fig. 5.14 presents a visual representation of the classification and hyperparameter errors across various iterations, delineating the minimum error achieved as well as the optimal point in hyperparameter space. As discerned from the figure, the 20th iteration emerges as the most favorable for hyperparameter adjustment, signifying a convergence towards optimal model performance. The error trends depicted in the graph underscore the efficacy of the proposed methodology, showcasing the precious performance of the proposed methodology throughout the training procedure.

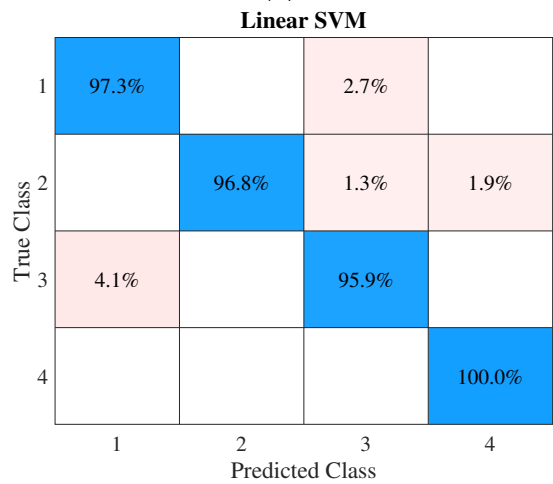
5.5.5 Detection Model's Robustness to Imbalanced Real-World Data

In the realm of data-driven methods, the robustness and reliability of a classification model are paramount, particularly when dealing with real-world data that may exhibit varying class distributions. This investigation focuses on assessing the performance of a machine learning, trained on a balanced dataset, across varying balanced ratio (B-ratio) among classes data set. To evaluate the model's adaptability and generalizability, it is subsequently tested on datasets with balanced but varied class distributions, ranging from 0.15 to 0.35 per class. This approach ensures a comprehensive understanding of the model's capability to maintain high performance across different scenarios, reflecting real-world conditions where class imbalance is often inevitable. Fig. 5.15 indicated the

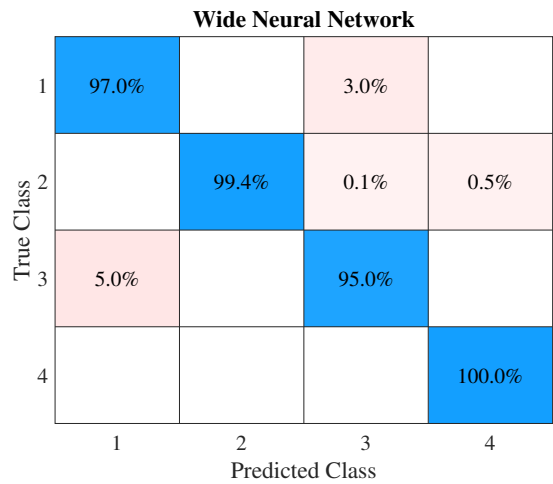
outstanding performance of the proposed method across various balanced ratios. Firstly, such a performance exhibits high generalizability, ensuring that the model remains effective even when the class distribution deviates from the ideal training conditions. This adaptability is crucial for real-world applications where the distribution of data can be unpredictable and dynamic. Secondly, a model that performs well across different balance rates reduces the risk of bias towards any particular class, thereby enhancing the fairness and reliability of the classification outcomes. Lastly, the ability to maintain consistent performance regardless of class balance underscores the robustness of the training methodology, instilling confidence that the model can handle diverse and imbalanced datasets effectively. This robustness is particularly valuable in critical applications such as attack detection systems.



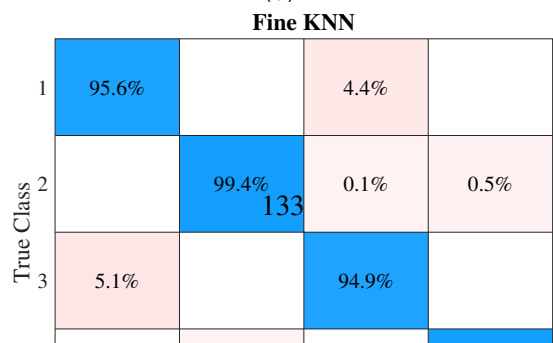
(a)

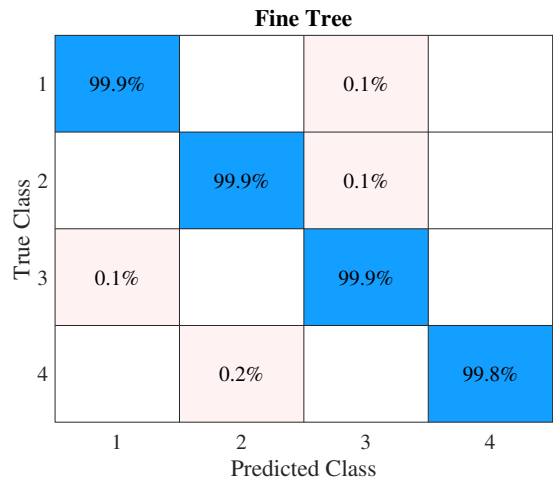


(b)

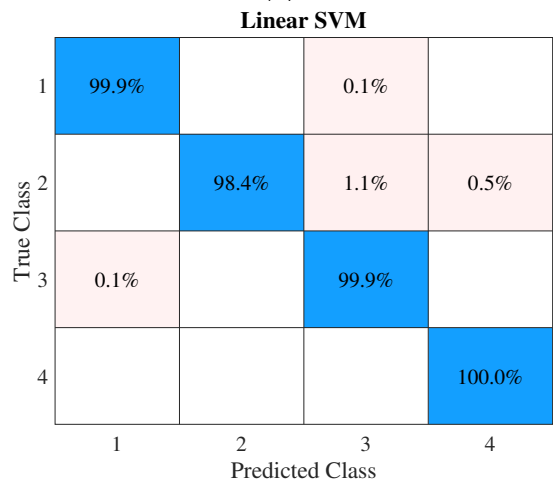


(c)

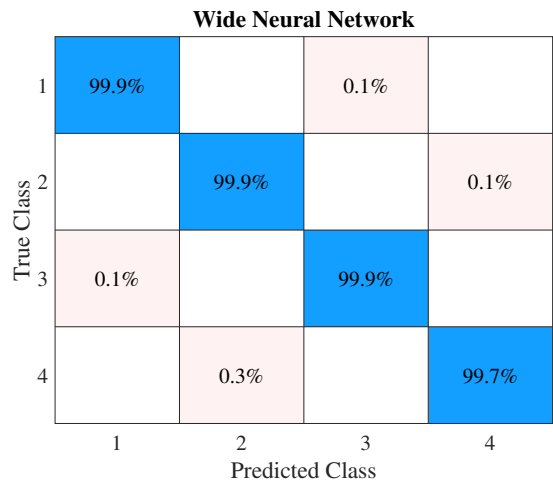




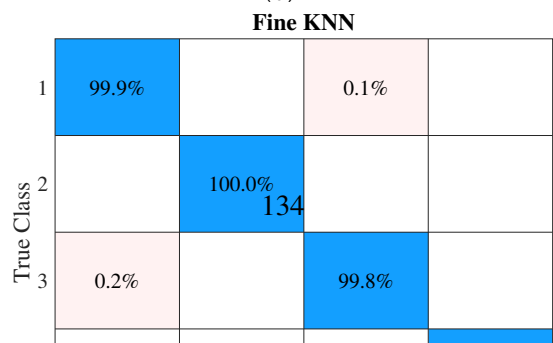
(a)

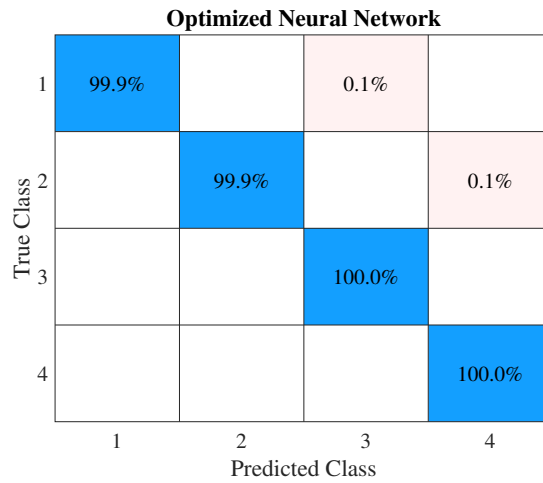


(b)

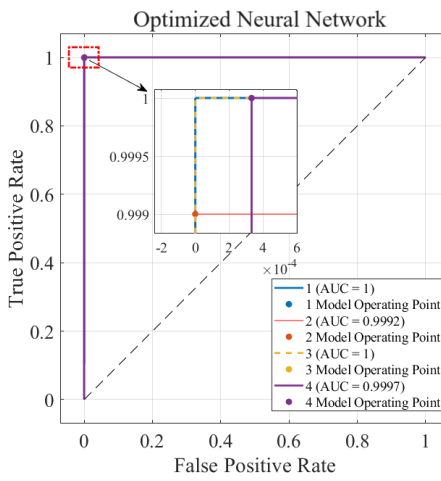


(c)





(a)



(b)

Figure 5.13: The performance of the wide neural networks optimized Bayesian optimizer.

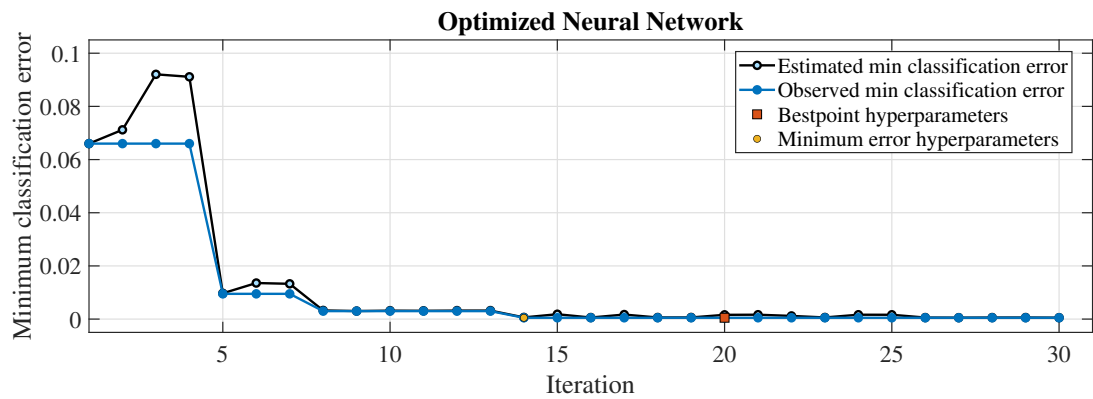
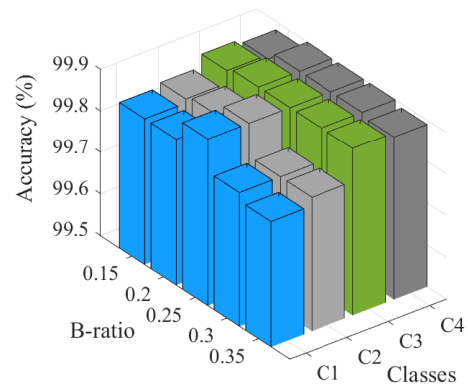
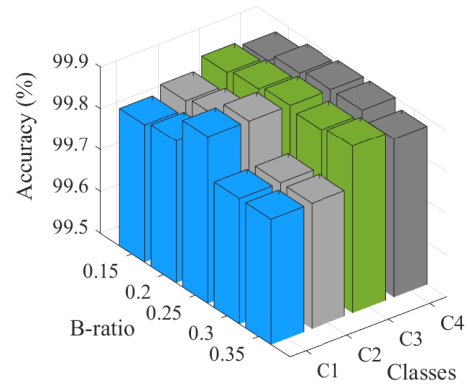


Figure 5.14: Classification and hypermeters error, as well as best point of hypermeter for the proposed detection method.



(a)



(b)

Figure 5.15: Robust performance of proposed detection method across varying B-ratios.

Chapter 6

Conclusion and Future Work

This Ph.D. thesis mainly aims to: (i) assess the cyber vulnerability of two essential wide-area control applications, namely EMS and WADC; (ii) analyze the potential consequences of cyber attacks on these applications; and (iii) develop robust countermeasures for prevention, detection, and mitigation to enhance the resilience of these applications against cyber threats. In pursuit of these aims, this Ph.D. thesis takes two significant steps.

In the first step, within content of EMS, this thesis emphasizes the vulnerability of IPGSs by developing a coordinated stealthy FDIA, which aims to disconnect GFPPs. The attack vector is constructed through a two-stage model. In the first stage, the EMS is targeted to maximize the system reliance on the targeted GFPPs. In the second stage, the pipeline monitoring system is misled into detecting fake leakage on the pipelines whose disconnection causes fuel interruption in the target GFPPs. Numerical results on IEEE 24-Bus 20-Node and IEEE 118-Bus 135-Node IPGSs demonstrate that a precise coordinated FDIA on a small group of the power and gas measurements can lead to outage of the targeted GFPPs. The developed FDIA can not be detected by the currently-deployed monitoring systems since the operational constraints of both power and gas systems are satisfied while constructing the attack vector. Meanwhile, since the pipeline network is generally buried underground, recognizing the attack may take several hours. Therefore, the presented FDIA on pipeline monitoring system could be hidden for several hours and cause severe consequences to the IPGSs. To defend against the developed FDIA, two countermeasures, i.e., preventive defense

strategy and online learning-based detection scheme, are proposed. In former, a systematic algorithm is proposed, which identifies high-risk measurements and improve the security of subset of those measurements to reduce the adversary's ability for constructing an effective attack vector. In latter, a MLP neural network model to distinguish normal and under-attack condition using trusted data source. Numerical analysis on IEEE 24-Bus 20-Node IPGS indicates the effectiveness of the deployed defense strategy, where protecting just six out of 115 measurements in the sample IPGS can reduce the attacker's capability rate about 40%, and also improve the performance of the online detection scheme. Additionally, the results on the large-scale IEEE 118-Bus 135-Node prove that (i) the developed coordinated FDIA and the proposed countermeasures can be scaled to the real-world IPGSs, and (ii) since the developed attack is originated from the GN and then propagated to the power system, protecting the critical gas measurements plays a significant role in improving the accuracy of online detection scheme. The outcomes of this step has been published as a conference paper in 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON) [163] and a journal paper in IEEE Transactions on Power Systems [131].

In the second step, this thesis emphasizes on the vulnerability of data aggregation standards and protocols in PMU-enabled WADCs against TSAs. In the presented attack model, the adversary launches an optimal TSA against PMUs to maximize data dropout in critical PMU measurements, aiming at hindering the WADC to observe DLO modes. A stochastic MIL model is utilized from the adversary's perspective to craft the TSA vector, which includes targeted PMUs and manipulated timestamps. The time-domain dynamic studies on two case studies, i.e., Two-Area Kundur and New England 39-bus grids, demonstrate that this TSA can compromise WADC's modal observability, causing system instability or undamped oscillation. To encounter this family of TSAs, a new preventive countermeasure is initially proposed by co-optimizing PMU-PDC data forwarding trees and PDC buffer waiting time. It has been demonstrated that not only the proposed countermeasure reduces the post-attack PMU data dropout, but also it improves overall data aggregation delay compared to other scenarios, by all of which the performance of the WADC improves. The proposed countermeasure can be utilized along with the device-level defense methods in the literature to make WADCs more resilient to TSAs. This step of the work also is published in form of a conference paper in 2022 IEEE Electrical Power and Energy Conference (EPEC) [97] and a journal paper in

IEEE Transactions on Instrumentation and Measurement [164].

Following the prevention stage, the next step of this thesis proposed an integrated CNN detection and robust state observer mitigation scheme to safeguard WADCs against TSAs. To this aim, this thesis first formulates an optimal TSA model on PMUs and PDCs that targets modal observability of WADCs. This model enables training of the CNN detection scheme against optimal TSAs and investigating the effectiveness of the proposed mitigation scheme during worst-TSAs. The proposed CNN detection leverages data quality information at the PDC level, i.e., PMU-PDC data transferring latency and dropout/duplication status of PMU data, to detect and localize TSAs on PMUs and PDCs. The output of the CNN detection is integrated as an extension into IEEE C37.118 data stream to inform the WADC in control center about the status of TSAs. Once this extension is enabled for any PMU data, the mitigation scheme calculates dropout probability for each PMU data and accordingly designs a state observer robust against the detected TSA. The numerical studies on Two-Area Kundur, IEEE 39-Bus, and the Simplified 14-Generator Model of the Southeastern Australian Power System demonstrated that (i) the crafted optimal TSA model can jeopardize WADC performance and lead to system stability issues, especially when multiple PMUs and PDCs are compromised, (ii) the proposed data quality information, which is only available at PDC level, contributes to significant improvement in TSA detection, and (iii) the proposed mitigation scheme can maintain the system stable even under worst-TSA conditions. This step of the work is published in form of a conference paper in 2nd IEEE Industrial Electronics Society Annual Online Conference (ONCON) [165] and a journal paper in IEEE Transactions on Smart Grid [144].

Eventually, this thesis emphasized the vulnerability of grid-connected IBRs to a new family of resonance FDIAs launched on cyber layers, aiming at inducing the inverter harmonic instability. In this attack, the adversary initially identifies the system's resonance frequency using impedance-based models or frequency scanning approaches. Then, by compromising sensors or grid-supporting functions, the adversary injects a sinusoidal attack vector into the system to excite the inverter's resonance modes with grid, causing harmonic instability. The simulation results on a test case LCL-type inverter demonstrated that a carefully constructed resonance FDIAs can lead to severe harmonic distortion at voltage and current at the inverter's PCC point, which can potentially lead to outage of the inverter. To enhance grid-connected IBR security against this type of resonance FDIA,

this thesis proposed a new detection scheme leveraging wavelet-based approaches. In this stage, the attack model is published in form of a conference paper in 24 IEEE International Conference on Environment and Electrical Engineering [166]. The extended version of the conference paper is also invited for publication in IEEE Transaction of Industrial Application by integrating the detection model.

For future work, this thesis underscores the need for research focused on enhancing the security of WAMPAC applications, particularly in the context of large-scale integration of IBRs. IBRs are the most significant driver of transformation in modern power grids to deal with climate change and energy security concerns. Nevertheless, the dominant integration of IBRs is exposed power grids to voltage and frequency stability challenges, primarily due to their low-inertia nature and grid-following control structure [166]. IBRs are commonly employed multiple-timescale feedback control system including PLL, direct dc-link voltage loop, and alternative voltage and current control loops, to regulate the inverter's exchange of active and reactive power with the power grid. The interplay and cross-coupling of this control system with the electromagnetic dynamics of synchronous generators and the transient behavior of passive components in the power grid, can result in oscillations spanning a wide frequency range, from sub-synchronous frequencies to switching frequencies. For instance, in 2013 and 2017, two oscillations with resonance frequency of several hundred Hz and 1270 Hz were reported in an islanded offshore grid in Germany and a HVDC transmission system in China, respectively [166]. These oscillations can appear with negative damping, leading to undesired harmonic voltage and current distortion and resonance, trigger protection functions, and endanger power grid stability. Aiming at detecting and mitigating the stability issues of IBRs, it is crucial to observe the high frequency oscillations in a system-wide and time-aligned manner with high-resolution waveform levels. To cope with this important need, waveform measurement units (WMU) technology has recently emerged as a promising solution, which take the advantageous of ICTs, e.g., IoT, digital merging units (MUs), and GPS, to measure system-wide and time-synchronized data with accuracy of 1 microseconds. In this technology, MUs located at substations digitize measurements of current and potential transformer in form of standard protocol data packets, e.g., IEEE C37.118 and IEC 61850. The data packets are tagged with the precision time stamps provided by GPS and transmitted through substation communication links to the control

center to be used for various monitoring, protection, and control applications. Despite the promising capabilities of WMU technology in enhancing the situational awareness of modern power grid operators, it remains in the preliminary research stage and has yet to be implemented in real-world power grids. Therefore, substantial adoptions are required for empowering modern power grids under penetration of IBRs to detect and mitigate recent stability issues using WMU technology. Motivated by this need, four research directions are introduced:

- **WMU-enabled dynamic state estimation (DSE):** In this research direction, drawing inspiration from the models proposed in [5] and [6], a WMU-enabled DSE model will be proposed to provide the wide-area control and protection systems with the optimum estimation of the power grid's states given the redundancy and noise in the sensory layer. Not only does the proposed DSE reduce the complexity of control and protection systems by eliminating the need for coordination measures, but it also identifies the root causes of faults and hidden failures through hypothesis testing. Additionally, the proposed DSE will improve overall system security by identifying anomalies and bad data in a set of measurements, substituting them with the estimated value, and alarming the system operator.
- **WMU-enabled Damping Controller for Harmonic Stability of IBRs:** WMUs enable the capturing of system-wide high-frequency oscillations that occur due to the resonance instability of IBRs with grids and with each other. In this research direction, the WMUs' data are used to identify the possible IBR-to-grid and IBR-to-IBR resonance frequency, distinguish the source of harmonic distortion in real-time, and mitigate the resonance instability issue by adaptive tuning of damping controllers integrated within close-loop current control loops of IBRs.
- **WMU-enabled event identification and localization:** WMUs facilitate tracking the behavior of system states during various large-scale disturbances and events. Since each event in the power grid is accompanied by a distinctive change in system states, this research direction focuses on applying data analytics techniques to WMU data for real-time event detection, classification, and localization. These techniques can be further utilized to enhance the performance of control and protection applications.

- Time-synchronization anomalies detection and mitigation in WMUs: The accuracy and authenticity of time-synchronization technologies, e.g., GPS, integrated with WMUs can be manipulated by satellite/receiver clock errors, radio frequency interaction, and GPS spoofing attacks [97]. This vulnerability leads to wrong WMU data timestamp, compromising the functionality of monitoring, control, and protection applications and endangering overall system stability and security. In this research direction, a time anomaly detection and mitigation scheme will be proposed to tackle vulnerability of WMU-enabled system against GPS malfunctions.

Bibliography

- [1] A. Yogarathinam and N. R. Chaudhuri, “Wide-area damping control using multiple DFIG-based wind farms under stochastic data packet dropouts,” *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3383–3393, 2018.
- [2] R. Huang and Y. Li, “False phasor data detection under time synchronization attacks: A neural network approach,” *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4828–4836, 2022.
- [3] force NASPI Time Synchronization Task, “Time synchronization in the electric power system,” *NASPI, Richland, WA, USA, Rep. NASPI-2017-TR-001*, 2017.
- [4] D. Trudnowski, B. Pierre, F. Wilches-Bernal, D. Schoenwald, R. Elliott, J. Neely, R. Byrne, and D. Kosterev, “Initial closed-loop testing results for the pacific DC intertie WADC,” *IEEE PESGM*, 2017.
- [5] K. E. Martin, G. Benmouyal, M. Adamiak, M. Begovic, R. Burnett, K. Carr, A. Cobb, J. Kusters, S. Horowitz, G. Jensen *et al.*, “IEEE standard for synchrophasors for power systems,” *IEEE Transactions on Power Delivery*, vol. 13, no. 1, pp. 73–77, 1998.
- [6] NAPS, “NASPI 2014 survey of synchrophasor system networks - results and findings,” 2015. [Online]. Available: <https://www.naspi.org/node/359>
- [7] P. S. R. Committee *et al.*, “IEEE standard for phasor data concentrators for power systems,” *IEEE Std C37.247-2019*, pp. 1–44, 2019.

- [8] S. Vahidi, M. Ghafouri, M. Au, M. Kassouf, A. Mohammadi, and M. Debbabi, "Security of wide-area monitoring, protection, and control (WAMPAC) systems of the smart grid: A survey on challenges and opportunities," *IEEE Communications Surveys & Tutorials*, 2023.
- [9] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," vol. 3, no. 3, pp. 1362–1370, 2012.
- [10] E. W. S. Ângelos, A. Abur, E. N. Asada, and O. R. Saavedra, "External topology tracking based on state estimation," vol. 36, no. 3, pp. 2623–2631, 2020.
- [11] S. Nabavi, J. Zhang, and A. Chakraborty, "Distributed optimization algorithms for wide-area oscillation monitoring in power systems using interregional PMU-PDC architectures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2529–2538, 2015.
- [12] M. S. Almas, L. Vanfretti, R. S. Singh, and G. M. Jonsdottir, "Vulnerability of synchrophasor-based WAMPAC applications' to time synchronization spoofing," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4601–4612, 2017.
- [13] M. Ghafouri, M. Au, M. Kassouf, M. Debbabi, C. Assi, and J. Yan, "Detection and mitigation of cyber attacks on voltage stability monitoring of smart grids," vol. 11, no. 6, pp. 5227–5238, 2020.
- [14] M. K. Neyestanaki and A. M. Ranjbar, "An adaptive PMU-based wide area backup protection scheme for power transmission lines," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1550–1559, 2015.
- [15] M. K. Jena, S. Samantaray, and B. K. Panigrahi, "A new adaptive dependability-security approach to enhance wide area back-up protection of transmission system," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6378–6386, 2017.
- [16] A. S. Dobakhshari and A. M. Ranjbar, "A wide-area scheme for power system fault location incorporating bad data detection," *IEEE Transactions on Power Delivery*, vol. 30, no. 2, pp. 800–808, 2015.

- [17] P. Gopakumar, M. J. B. Reddy, and D. K. Mohanta, “Adaptive fault identification and classification methodology for smart power grids using synchronous phasor angle measurements,” *IET generation, transmission & distribution*, vol. 9, no. 2, pp. 133–145, 2015.
- [18] Q. Zhang and F. Li, “Cyber-vulnerability analysis for real-time power market operation,” vol. 12, no. 4, pp. 3527–3537, 2021.
- [19] M. E. C. Bento, “A hybrid particle swarm optimization algorithm for the wide-area damping control design,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 592–599, 2022.
- [20] T. Bi, J. Guo, K. Xu, L. Zhang, and Q. Yang, “The impact of time synchronization deviation on the performance of synchrophasor measurements and wide area damping control,” *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1545–1552, 2016.
- [21] A. Ameli, A. Hooshyar, A. H. Yazdavar, E. F. El-Saadany, and A. Youssef, “Attack detection for load frequency control systems using stochastic unknown input estimators,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2575–2590, 2018.
- [22] M. Ghafouri, M. Au, M. Kassouf, M. Debbabi, C. Assi, and J. Yan, “Detection and mitigation of cyber attacks on voltage stability monitoring of smart grids,” *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5227–5238, 2020.
- [23] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 ukraine blackout: Implications for false data injection attacks,” vol. 32, no. 4, pp. 3317–3318, 2016.
- [24] D. Goodin, “Us spy drone hijacked with GPS spoof hack,” *spy drone GPS spoofing*, 2011.
- [25] J. Allnutt, D. Anand, D. Arnold, A. Goldstein, Y.-S. Li-Baboud, A. Martin, C. Nguyen, R. Noseworthy, R. Subramaniam, and M. Weiss, “Timing challenges in the smart grid,” *NIST Special Publication*, vol. 1500, p. 08, 2017.
- [26] A. Lee, “Electric sector failure scenarios and impact analyses-version 3.0,” *National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group: Palo Alto, CA, USA*, 2015.

- [27] A. Sundararajan, T. Khan, A. Moghadasi, and A. m. Sarwat, "Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 3, pp. 449–467, 2019.
- [28] M. Shahidehpour, Y. Fu, and T. Wiedman, "Impact of natural gas infrastructure on electric power systems," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 1042–1056, 2005.
- [29] S. Clegg and P. Mancarella, "Integrated modeling and assessment of the operational impact of power-to-gas (P2G) on electrical and gas transmission networks," vol. 6, no. 4, pp. 1234–1244, 2015.
- [30] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2831–2848, 2019.
- [31] E. Guelpa, A. Bischì, V. Verda, M. Chertkov, and H. Lund, "Towards future infrastructures for sustainable multi-energy systems: A review," *Energy*, vol. 184, pp. 2–21, 2019.
- [32] M. Saad, S. B. A. Bukhari, and C. H. Kim, "A review of various modern strategies for mitigation of cyber attacks in smart grids," in *2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific)*. IEEE, 2019, pp. 1–7.
- [33] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2020.
- [34] N. S. Malik, R. Collins, and M. Vamburkar, "Cyberattack pings data systems of at least four gas networks," *Bloomberg*, 2018. [Online]. Available: <https://www.bloomberg.com/news/articles/2018-04-03/day-after-cyber-attack-a-third-gas-pipeline-data-system-shuts?leadSource=uverify%20wall>
- [35] Q. Zhang, F. Li, Q. Shi, K. Tomsovic, J. Sun, and L. Ren, "Profit-oriented false data injection on energy market: Reviews, analyses and insights," 2020.

- [36] X. Liu and Z. Li, “False data attacks against AC state estimation with incomplete network information,” vol. 8, no. 5, pp. 2239–2248, 2016.
- [37] C. Liu, H. Liang, and T. Chen, “Network parameter coordinated false data injection attacks against power system AC state estimation,” vol. 12, no. 2, pp. 1626–1639, 2021.
- [38] M. Du, G. Pierrou, X. Wang, and M. Kassouf, “Targeted false data injection attacks against AC state estimation without network parameters,” vol. 12, no. 6, pp. 5349–5361, 2021.
- [39] X. Liu and Z. Li, “Local topology attacks in smart grids,” vol. 8, no. 6, pp. 2617–2626, 2017.
- [40] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, Y. Zhang, and C.-K. Wen, “Local cyber-physical attack for masking line outage and topology attack in smart grid,” vol. 10, no. 4, pp. 4577–4588, 2019.
- [41] Z. Wang, H. He, Z. Wan, and Y. Sun, “Coordinated topology attacks in smart grid using deep reinforcement learning,” vol. 17, no. 2, pp. 1407–1415, 2021.
- [42] M. Jorjani, H. Seifi, and A. Yazdian-Varjani, “A graph theory-based approach to detect false data injection attacks in power system AC state estimation,” 2020.
- [43] T. Nguyen, B.-H. Liu, N. Nguyen, B. Dumba, and J.-T. Chou, “Smart grid vulnerability and defense analysis under cascading failure attacks,” vol. 36, pp. 2264–2273, 2021.
- [44] T. Wu, W. Xue, H. Wang, C. Chung, G. Wang, J. Peng, and Q. Yang, “Extreme learning machine-based state reconstruction for automatic attack filtering in cyber physical power system,” vol. 17, no. 3, pp. 1892–1904, 2020.
- [45] G. Zhang, J. Li, O. Bamisile, D. Cai, W. Hu, and Q. Huang, “Spatio-temporal correlation-based false data injection attack detection using deep convolutional neural network,” vol. 13, no. 1, pp. 750–761, 2021.
- [46] S. V. S. Chauhan and G. X. Gao, “Spoofing resilient state estimation for the power grid using an extended kalman filter,” vol. 12, no. 4, pp. 3404–3414, 2021.

- [47] G. Cheng, Y. Lin, J. Zhao, and J. Yan, “A highly discriminative detector against false data injection attacks in AC state estimation,” 2022.
- [48] J. Shang, M. Chen, and T. Chen, “Optimal linear encryption against stealthy attacks on remote state estimation,” *IEEE Transactions on Automatic Control*, vol. 66, no. 8, pp. 3592–3607, 2020.
- [49] B. Donmez and A. Abur, “Static state estimation without topology processor,” vol. 36, no. 5, pp. 4712–4722, 2021.
- [50] Y. Xu, J. Valinejad, M. Korkali, L. Mili, Y. Wang, X. Chen, and Z. Zheng, “An adaptive-importance-sampling-enhanced bayesian approach for topology estimation in an unbalanced power distribution system,” vol. 37, no. 3, pp. 2220–2232, 2021.
- [51] P. Cramton, “Lessons from the 2021 texas electricity crisis,” *Utility Dive*, vol. 23, 2021. [Online]. Available: <https://www.utilitydive.com/news/lessons-from-the-2021-texas-electricity-crisis/596998/>
- [52] P. Zhao, C. Gu, and D. Huo, “Coordinated risk mitigation strategy for integrated energy systems under cyber-attacks,” vol. 35, no. 5, pp. 4014–4025, 2020.
- [53] P. Zhao, Z. Cao, D. D. Zeng, C. Gu, Z. Wang, Y. Xiang, M. Qadrdan, X. Chen, X. Yan, and S. Li, “Cyber-resilient multi-energy management for complex systems,” vol. 18, no. 3, pp. 2144–2159, 2021.
- [54] A. M. Sawas, H. Khani, and H. E. Farag, “On the resiliency of power and gas integration resources against cyber attacks,” vol. 17, no. 5, pp. 3099–3110, 2020.
- [55] H. Lu, T. Iseley, S. Behbahani, and L. Fu, “Leakage detection techniques for oil and gas pipelines: State-of-the-art,” *Tunnelling and Underground Space Technology*, vol. 98, p. 103249, 2020.
- [56] P. Radoglou-Grammatikis, P. Sarigiannidis, T. Liatifis, T. Apostolakis, and S. Oikonomou, “An overview of the firewall systems in the smart grid paradigm,” in *2018 Global information infrastructure and networking symposium (GIIS)*. IEEE, 2018, pp. 1–4.

- [57] O. N. Nyasore, P. Zavorsky, B. Swar, R. Naiyeju, and S. Dabra, “Deep packet inspection in industrial automation control system to mitigate attacks exploiting modbus/tcp vulnerabilities,” in *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity)*. IEEE, 2020, pp. 241–245.
- [58] T. M. Hoang, N. M. Nguyen, and T. Q. Duong, “Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and k-means clustering,” *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 139–142, 2019.
- [59] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, “MARINE: Man-in-the-middle attack resistant trust model in connected vehicles,” *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3310–3322, 2020.
- [60] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.
- [61] C. Liu, W. He, R. Deng, Y.-C. Tian, and W. Du, “False data injection enabled network parameter modifications in power systems: Attack and detection,” Early Access, 2022.
- [62] L. Che, X. Liu, Z. Li, and Y. Wen, “False data injection attacks induced sequential outages in power systems,” vol. 34, no. 2, pp. 1513–1523, 2018.
- [63] S. Mhanna and P. Mancarella, “An exact sequential linear programming algorithm for the optimal power flow problem,” vol. 37, no. 1, pp. 666–679, 2021.
- [64] C. M. Correa-Posada and P. Sanchez-Martin, “Integrated power and natural gas model for energy adequacy in short-term operation,” vol. 30, no. 6, pp. 3347–3355, 2014.
- [65] S. Espinoza, A. Poulos, H. Rudnick, J. C. de la Llera, M. Panteli, and P. Mancarella, “Risk and resilience assessment with component criticality ranking of electric power systems subject to earthquakes,” *IEEE Systems Journal*, vol. 14, no. 2, pp. 2837–2848, 2020.

- [66] M. Zadsar, S. S. Sebtahmadi, M. Kazemi, S. Larimi, and M. Haghifam, "Two stage risk based decision making for operation of smart grid by optimal dynamic multi-microgrid," *International Journal of Electrical Power & Energy Systems*, vol. 118, p. 105791, 2020.
- [67] G. Cybenko, "Approximation by superpositions of a sigmoidal function," *Mathematics of control, signals and systems*, vol. 2, no. 4, pp. 303–314, 1989.
- [68] S. Sharma, S. Sharma, and A. Athaiya, "Activation functions in neural networks," *towards data science*, vol. 6, no. 12, pp. 310–316, 2017.
- [69] M. Ansari, M. Zadsar, H. Zareipour, and M. Kazemi, "Resilient operation planning of integrated electrical and natural gas systems in the presence of natural gas storages," *International Journal of Electrical Power & Energy Systems*, vol. 130, p. 106936, 2021.
- [70] A. Ameli, A. Ayad, E. El-Saadany, M. Salama, and A. Youssef, "A learning-based framework for detecting cyber-attacks against line current differential relays," 2020.
- [71] W. Jia, T. Ding, C. Huang, Z. Wang, Q. Zhou, and M. Shahidehpour, "Convex optimization of integrated power-gas energy flow model with applications to probabilistic energy flow," vol. 36, no. 2, pp. 1432–1441, 2020.
- [72] C. Lu, X. Wu, J. Wu, P. Li, Y. Han, and L. Li, "Implementations and experiences of wide-area HVDC damping control in china southern power grid," in *2012 IEEE Power and Energy Society General Meeting*. IEEE, 2012, pp. 1–7.
- [73] Y. Wang and J. P. Hespanha, "Distributed estimation of power system oscillation modes under attacks on GPS clocks," *IEEE Transactions on Instrumentation and Measurement*, vol. 67, no. 7, pp. 1626–1637, 2018.
- [74] Y.-h. Tang, G. N. Stenbakken, and A. Goldstein, "Calibration of phasor measurement unit at NIST," *IEEE Transactions on Instrumentation and Measurement*, vol. 62, no. 6, pp. 1417–1422, 2013.

- [75] A. Carta, N. Locci, C. Muscas, and S. Sulis, “A flexible GPS-based system for synchronized phasor measurement in electric distribution networks,” *IEEE transactions on instrumentation and measurement*, vol. 57, no. 11, pp. 2450–2456, 2008.
- [76] M. Lixia, A. Benigni, A. Flammini, C. Muscas, F. Ponci, and A. Monti, “A software-only PTP synchronization for power system state estimation with pmus,” *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 5, pp. 1476–1485, 2012.
- [77] S. Barreto, A. Suresh, and J.-Y. Le Boudec, “Cyber-attack on packet-based time synchronization protocols: The undetectable delay box,” in *2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings*. Ieee, 2016, pp. 1–6.
- [78] B. Chen, S.-i. Yim, H. Kim, A. Kondabathini, and R. Nuqui, “Cybersecurity of wide area monitoring, protection, and control systems for HVDC applications,” *IEEE Transactions on Power Systems*, vol. 36, no. 1, pp. 592–602, 2020.
- [79] A. Chawla, A. Singh, P. Agrawal, B. K. Panigrahi, B. R. Bhalja, and K. Paul, “Denial-of-service attacks pre-emptive and detection framework for synchrophasor based wide area protection applications,” *IEEE Systems Journal*, vol. 16, no. 1, pp. 1570–1581, 2021.
- [80] G. Barchi, D. Fontanelli, D. Macii, and D. Petri, “On the accuracy of phasor angle measurements in power networks,” *IEEE Transactions on Instrumentation and Measurement*, vol. 64, no. 5, pp. 1129–1139, 2014.
- [81] E. Shereen, M. Delcourt, S. Barreto, G. Dán, J.-Y. Le Boudec, and M. Paolone, “Feasibility of time-synchronization attacks against PMU-based state estimation,” *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 6, pp. 3412–3427, 2019.
- [82] S. Siamak, M. Dehghani, and M. Mohammadi, “Dynamic GPS spoofing attack detection, localization, and measurement correction exploiting PMU and SCADA,” *IEEE Systems Journal*, vol. 15, no. 2, pp. 2531–2540, 2020.

- [83] E. Shereen and G. Dán, “Model-based and data-driven detectors for time synchronization attacks against PMUs,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 1, pp. 169–179, 2019.
- [84] W. Gao, H. Li, M. Zhong, and M. Lu, “The separate clock drift matched filter to detect time synchronization attacks towards global navigation satellite systems,” *IEEE Transactions on Industrial Electronics*, 2022.
- [85] A. Xue, L. Gu, H. Hong, J. Zhao, H. Kong, F. Xu, N. Chang, Z. Jiang, J. Ma, and M. Lu, “PMU angle deviation detection and correction using line reactive power measurements,” *IEEE Transactions on Power Systems*, 2022.
- [86] D. Roberson and J. F. O’Brien, “Variable loop gain using excessive regeneration detection for a delayed wide-area control system,” *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6623–6632, 2017.
- [87] M. L. Psiaki and T. E. Humphreys, “GNSS spoofing and detection,” *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.
- [88] B. Moussa, M. Kassouf, R. Hadjidj, M. Debbabi, and C. Assi, “An extension to the precision time protocol (PTP) to enable the detection of cyber attacks,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 18–27, 2019.
- [89] P. Bhattacharya, M. Ghafouri, A. Soeanu, M. Kassouf, and M. Debbabi, “Security enhancement of time synchronization and fault identification in WAMS using a two-layer blockchain framework,” *Applied Energy*, vol. 315, p. 118955, 2022.
- [90] Y. Zhao, W. Yao, C.-K. Zhang, X.-C. Shangguan, L. Jiang, and J. Wen, “Quantifying resilience of wide-area damping control against cyber attack based on switching system theory,” *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2331–2343, 2022.
- [91] B. Moussa, A. Al-Barakati, M. Kassouf, M. Debbabi, and C. Assi, “Exploiting the vulnerability of relative data alignment in phasor data concentrators to time synchronization attacks,” *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2541–2551, 2019.

- [92] P. W. Sauer, M. A. Pai, and J. H. Chow, *Power system dynamics and stability: with synchrophasor measurement and power system toolbox*. John Wiley & Sons, 2017.
- [93] B. Li, R. Lu, G. Xiao, H. Bao, and A. A. Ghorbani, "Towards insider threats detection in smart grid communication systems," *IET Communications*, vol. 13, no. 12, pp. 1728–1736, 2019.
- [94] S. Roy, N. Sharmin, J. C. Acosta, C. Kiekintveld, and A. Laszka, "Survey and taxonomy of adversarial reconnaissance techniques," *ACM Computing Surveys*, vol. 55, no. 6, pp. 1–38, 2022.
- [95] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles+ grid data: Is a new cyberattack vector viable?" *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5099–5113, 2020.
- [96] T. Surinkaew and I. Ngamroo, "Hierarchical co-ordinated wide area and local controls of DFIG wind turbine and PSS for robust power oscillation damping," *IEEE Transactions on Sustainable Energy*, vol. 7, no. 3, pp. 943–955, 2016.
- [97] M. Zadsar, M. Ghafouri, A. Ameli, and B. Moussa, "Time-synchronization attack on data aggregation in wide-area damping controllers," in *2022 IEEE Electrical Power and Energy Conference (EPEC)*. IEEE, 2022, pp. 368–373.
- [98] Y. Yao, Y. Xu, and M. Chow, "Distributed optimal dynamic communication paths planning for PMUs in the WAMS communication network," *IEEE Transactions on Industrial Informatics*, 2022.
- [99] B. Zeng and L. Zhao, "Solving two-stage robust optimization problems using a column-and-constraint generation method," *Operations Research Letters*, vol. 41, no. 5, pp. 457–461, 2013.
- [100] M. B. Mohammadi, R.-A. Hooshmand, and F. H. Fesharaki, "A new approach for optimal placement of pmus and their required communication infrastructure in order to minimize the cost of the wams," *IEEE Transactions on smart grid*, vol. 7, no. 1, pp. 84–93, 2015.

- [101] X. Li, Y.-C. Tian, G. Ledwich, Y. Mishra, and C. Zhou, “Minimizing multicast routing delay in multiple multicast trees with shared links for smart grid,” *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5427–5435, 2018.
- [102] P. S. Kundur, N. J. Balu, and M. G. Lauby, “Power system dynamics and stability,” *Power system stability and control*, vol. 3, 2017.
- [103] S. Chakrabarti and E. Kyriakides, “Optimal placement of phasor measurement units for power system observability,” *IEEE Transactions on power systems*, vol. 23, no. 3, pp. 1433–1440, 2008.
- [104] T. R. B. Kushal, M. S. Illindala, and J. Wang, “Dynamic multicast routing management for robust wide area power grid communication,” *IEEE Transactions on Industry Applications*, vol. 57, no. 6, pp. 5658–5666, 2021.
- [105] B. Appasani and D. K. Mohanta, “Co-optimal placement of PMUs and their communication infrastructure for minimization of propagation delay in the WAMS,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 2120–2132, 2018.
- [106] M. Göl and A. Abur, “LAV based robust state estimation for systems measured by PMUs,” *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1808–1814, 2014.
- [107] P. Risbud, N. Gatsis, and A. Taha, “Vulnerability analysis of smart grids to GPS spoofing,” *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3535–3548, 2018.
- [108] S. Vahidi, A. Amini, M. Ghafouri, M. Au, A. Mohammadi, and M. Debbabi, “Resilient periodic observer-based control for wide area oscillation damping against time synchronization attacks,” in *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2022, pp. 1–5.
- [109] W. Alghamdi and M. Schukat, “Cyber attacks on precision time protocol networks—a case study,” *Electronics*, vol. 9, no. 9, p. 1398, 2020.

- [110] S. Barreto, A. Suresh, and J.-Y. Le Boudec, “Cyber-attack on packet-based time synchronization protocols: The undetectable delay box,” in *2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings*. Ieee, 2016, pp. 1–6.
- [111] M. Yuan, X. Tang, and G. Ou, “Autenticating GNSS civilian signals: A survey,” *Satellite Navigation*, vol. 4, no. 1, pp. 1–18, 2023.
- [112] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, A. D. Domi *et al.*, “Spoofing GPS receiver clock offset of phasor measurement units,” *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3253–3262, 2013.
- [113] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O’Hanlon, P. M. Kintner *et al.*, “Assessing the spoofing threat: Development of a portable GPS civilian spoofer,” in *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008)*, 2008, pp. 2314–2325.
- [114] W. Gao, H. Li, M. Zhong, and M. Lu, “The separate clock drift matched filter to detect time synchronization attacks towards global navigation satellite systems,” *IEEE Transactions on Industrial Electronics*, 2022.
- [115] V. Formichella and P. Tavella, “A recursive clock anomalies detector with double exponential smoothing,” in *2018 European Frequency and Time Forum (EFTF)*. IEEE, 2018, pp. 245–248.
- [116] W. Gao, H. Li, M. Zhong, and M. Lu, “An underestimated cybersecurity problem: Quick-impact time synchronization attacks and a fast-triggered detection method,” *IEEE Transactions on Smart Grid*, 2023.
- [117] E. Shereen and G. Dán, “Model-based and data-driven detectors for time synchronization attacks against PMUs,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 1, pp. 169–179, 2019.

- [118] S. Siamak, M. Dehghani, and M. Mohammadi, “Dynamic GPS spoofing attack detection, localization, and measurement correction exploiting PMU and SCADA,” *IEEE Systems Journal*, vol. 15, no. 2, pp. 2531–2540, 2020.
- [119] S. V. S. Chauhan and G. X. Gao, “Synchrophasor data under GPS spoofing: Attack detection and mitigation using residuals,” *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3415–3424, 2021.
- [120] A. Xue, F. Xu, J. Xu, J. H. Chow, S. Leng, and T. Bi, “Online pattern recognition and data correction of pmu data under gps spoofing attack,” *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 6, pp. 1240–1249, 2020.
- [121] E. Shereen, R. Ramakrishna, and G. Dán, “Detection and localization of PMU time synchronization attacks via graph signal processing,” *IEEE Transactions on Smart Grid*, vol. 13, no. 4, pp. 3241–3254, 2022.
- [122] S. S. Hussain, S. M. Farooq, and T. S. Ustun, “A security mechanism for IEEE C37.118.2 PMU communication,” *IEEE Transactions on Industrial Electronics*, vol. 69, no. 1, pp. 1053–1061, 2021.
- [123] T. Szandała, “Review and comparison of commonly used activation functions for deep neural networks,” *Bio-inspired neurocomputing*, pp. 203–224, 2021.
- [124] R. Kateb, P. Akaber, M. H. Tushar, A. Albarakati, M. Debbabi, and C. Assi, “Enhancing WAMS communication network against delay attacks,” *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2738–2751, 2018.
- [125] M. Ghafouri, U. Karaagac, H. Karimi, S. Jensen, J. Mahseredjian, and S. O. Faried, “An LQR controller for damping of subsynchronous interaction in DFIG-based wind farms,” *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4934–4942, 2017.
- [126] M. Nadeem, M. Bahavarnia, and A. F. Taha, “On wide-area control of solar-integrated DAE models of power grids,” in *2023 American Control Conference (ACC)*. IEEE, 2023, pp. 4495–4500.

- [127] A. Amini, M. Ghafouri, A. Mohammadi, M. Hou, A. Asif, and K. Plataniotis, "Secure sampled-data observer-based control for wind turbine oscillation under cyber attacks," *IEEE Transactions on Smart Grid*, vol. 13, no. 4, pp. 3188–3202, 2022.
- [128] S. P. Azad, R. Iravani, and J. E. Tate, "Damping inter-area oscillations based on a model predictive control (MPC) HVDC supplementary controller," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3174–3183, 2013.
- [129] M. Zadsar, M. Ghafouri, A. Ameli, and b. Moussa, "Preventing time-synchronization attacks on synchrophasor measurements of wide-area damping controllers," *IEEE Transactions on Instrumentation and Measurement*, 2023.
- [130] M. Ghafouri, E. Kabir, B. Moussa, and C. Assi, "Coordinated charging and discharging of electric vehicles: A new class of switching attacks," *ACM Transactions on Cyber-Physical Systems (TCPS)*, vol. 6, no. 3, pp. 1–26, 2022.
- [131] M. Zadsar, A. Abazari, A. Ameli, J. Yan, and M. Ghafouri, "Prevention and detection of coordinated false data injection attacks on integrated power and gas systems," *IEEE Transactions on Power Systems*, 2022.
- [132] P. S. Kundur and O. P. Malik, *Power system stability and control*. McGraw-Hill Education, 2022.
- [133] H. H. Alhelou, M. E. H. Golshan, and N. D. Hatziargyriou, "Deterministic dynamic state estimation-based optimal lfc for interconnected power systems using unnon input observer," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1582–1592, 2019.
- [134] D. Roberson and J. F. O'Brien, "Loop shaping of a wide-area damping controller using HVDC," *IEEE Transactions on Power Systems*, vol. 32, no. 3, pp. 2354–2361, 2016.
- [135] E. Rebello, L. Vanfretti, and M. S. Almas, "Experimental testing of a real-time implementation of a PMU-based wide-area damping control system," *IEEE Access*, vol. 8, pp. 25 800–25 810, 2020.

- [136] M. E. Bento, D. Dotta, R. Kuiava, and R. A. Ramos, "A procedure to design fault-tolerant wide-area damping controllers," *IEEE access*, vol. 6, pp. 23 383–23 405, 2018.
- [137] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—the new and improved power grid: A survey," *IEEE communications surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2011.
- [138] A. Abazari, M. M. Soleymani, M. Zadsar, M. Ghafouri, C. Assi, and M. Shafie-Khah, "Online recursive detection and adaptive fuzzy mitigation of cyber-physical attacks targeting topology of img: An LFC case study," *IEEE Transactions on Smart Grid*, 2023.
- [139] A. Abazari, M. Zadsar, M. Ghafouri, and C. Assi, "Detection of cyber-physical attacks using optimal recursive least square in an islanded microgrid," in *2022 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2022, pp. 1–5.
- [140] A. Abazari, M. Zadsar, M. Ghafouri, R. Atallah, and C. Assi, "A data mining/ANFIS and adaptive control for detection and mitigation of attacks on DC MGs," *IEEE Transactions on Smart Grid*, vol. 14, no. 3, pp. 2406–2422, 2022.
- [141] D. G. Photovoltaics and E. Storage, "IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," *IEEE std*, vol. 1547, pp. 1547–2018, 2018.
- [142] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, vol. 38, no. 2, pp. 2364–2383, 2022.
- [143] B. Ahn, T. Kim, S. Ahmad, S. K. Mazumder, J. Johnson, H. A. Mantooth, and C. Farnell, "An overview of cyber-resilient smart inverters based on practical attack models," *IEEE Transactions on Power Electronics*, 2023.
- [144] M. Zadsar, M. Ghafouri, A. Ameli, and B. Moussa, "Integrated deep learning-based detection and robust state observer mitigation of time-synchronization attacks: A WADC case study," *IEEE Transactions on Smart Grid*, pp. 1–1, 2024.

- [145] X. Wang and F. Blaabjerg, "Harmonic stability in power electronic-based power systems: Concept, modeling, and analysis," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2858–2870, 2018.
- [146] X. Wang, Y. He, D. Pan, H. Zhang, Y. Ma, and X. Ruan, "Harmonic instability of LCL-type grid-connected inverter caused by the pole-zero cancellation: A case study," *IEEE Transactions on Industrial Electronics*, vol. 69, no. 11, pp. 11 580–11 589, 2021.
- [147] J. He, Y. W. Li, D. Bosnjak, and B. Harris, "Investigation and active damping of multiple resonances in a parallel-inverter-based microgrid," *IEEE Transactions on Power Electronics*, vol. 28, no. 1, pp. 234–246, 2012.
- [148] X. Chen, Y. Zhang, S. Wang, J. Chen, and C. Gong, "Impedance-phased dynamic control method for grid-connected inverters in a weak grid," *IEEE Transactions on Power Electronics*, vol. 32, no. 1, pp. 274–283, 2016.
- [149] C. Burgos-Mellado, F. Donoso, T. Dragičević, R. Cardenas-Dobson, P. Wheeler, J. Clare, and A. Watson, "Cyber-attacks in modular multilevel converters," *IEEE Transactions on Power Electronics*, vol. 37, no. 7, pp. 8488–8501, 2022.
- [150] A. Bamigbade, Y. Dvorkin, and R. Karri, "Cyberattack on phase-locked loops in inverter-based energy resources," *IEEE Transactions on Smart Grid*, 2023.
- [151] 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)*. IEEE, 2022, pp. 79–84.
- [152] J. Zhang, L. Guo, and J. Ye, "Cyber-attack detection for photovoltaic farms based on power-electronics-enabled harmonic state space modeling," *IEEE transactions on smart grid*, vol. 13, no. 5, pp. 3929–3942, 2021.

- [153] C. Burgos-Mellado, C. Zuñiga-Bauerle, D. Muñoz-Carpintero, Y. Arias-Esquivel, R. Càrdenas-Dobson, T. Dragičević, F. Donoso, and A. Watson, “Reinforcement learning-based method to exploit vulnerabilities of false data injection attack detectors in modular multilevel converters,” *IEEE Transactions on Power Electronics*, 2023.
- [154] B. Kang, P. Maynard, K. McLaughlin, S. Sezer, F. Andrén, C. Seitzl, F. Kupzog, and T. Strasser, “Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations,” in *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*. IEEE, 2015, pp. 1–8.
- [155] M. Shirinzad, “Frequency scan based stability analysis of power electronic systems,” 2021.
- [156] Z. Li, H. Hu, L. Tang, Y. Wang, T. Zang, and Z. He, “Quantitative severity assessment and sensitivity analysis under uncertainty for harmonic resonance amplification in power systems,” *IEEE Transactions on Power Delivery*, vol. 35, no. 2, pp. 809–818, 2019.
- [157] M. Kumar, S. Prasad, M. R. Ansari, and B. Mohapatra, “Resonance attacks detection and mitigation control scheme on frequency regulation in multi-area smart grid,” *International Journal of Control*, vol. 96, no. 9, pp. 2212–2229, 2023.
- [158] A. Paul, A. Kundu, N. Chaki, D. Dutta, and C. Jha, “Wavelet enabled convolutional autoencoder based deep neural network for hyperspectral image denoising,” *Multimedia tools and applications*, pp. 1–27, 2022.
- [159] J. Zhang, G. G. Walter, Y. Miao, and W. N. W. Lee, “Wavelet neural networks for function learning,” *IEEE transactions on Signal Processing*, vol. 43, no. 6, pp. 1485–1497, 1995.
- [160] A. K. Alexandridis and A. D. Zapanis, “Wavelet neural networks: A practical guide,” *Neural Networks*, vol. 42, pp. 1–27, 2013.
- [161] H.-L. Wei, S. A. Billings, Y. Zhao, and L. Guo, “An adaptive wavelet neural network for spatio-temporal system identification,” *Neural Networks*, vol. 23, no. 10, pp. 1286–1299, 2010.

- [162] D. Li and H. Zhang, “Improved regularization and robustness for fine-tuning in neural networks,” *Advances in Neural Information Processing Systems*, vol. 34, pp. 27 249–27 262, 2021.
- [163] M. Zadsar, A. Abazari, M. Ansari, M. Ghafouri, S. Muyeen, and F. Blaabjerg, “Central situational awareness system for resiliency enhancement of integrated energy systems,” in *2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON)*. IEEE, 2021, pp. 1–6.
- [164] M. Zadsar, M. Ghafouri, A. Ameli, and B. Moussa, “Preventing time-synchronization attacks on synchrophasor measurements of wide-area damping controllers,” *IEEE Transactions on Instrumentation and Measurement*, 2023.
- [165] M. Zadsar, M. Ghafouri, and A. Ameli, “Cyber attack-aware security hardening of time synchronization technologies in WAMPAC systems,” in *2023 IEEE 2nd Industrial Electronics Society Annual On-Line Conference (ONCON)*. IEEE, 2023, pp. 1–5.
- [166] M. Zadsar, M. Babaei, M. Ghafouri, and A. Ameli, “Cyber induced harmonic instability of inverter-based renewable generators,” in *24 IEEEIC International Conference on Environment and Electrical Engineering*. IEEE, 2024, pp. 1–5.