Defending against False Data Injection Attacks in Power Systems: Techniques for Securing State Estimation and Distance Protection

by

Mohammadmahdi Asghari

A thesis
presented to the Lakehead University
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Thunder Bay, Ontario, Canada, 2025

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Dr. Mohammadreza Arani Assistant Professor, Dept. of Electrical and Computer Engineering, Toronto Metropolitan University
Supervisor:	Dr. Amir Ameli Associate Professor , Dept. of Electrical and Computer Engineering, Lakehead University
Co-supervisor:	Dr. Mohammad Nassir Uddin Professor, Dept. of Electrical and Computer Engineering, Lakehead University
Internal Member:	Dr. Apparao Dekka Associate Professor, Dept. of Electrical and Computer Engineering, Lakehead University
Internal Member:	Dr. Qiang Wei Associate Professor, Dept. of Electrical and Computer Engineering, Lakehead University

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

The digitalization of power systems—enabled by technologies such as digital substations and Wide-Area Monitoring, Protection, and Control (WAMPAC) systems—has improved automation, visibility, and system control. However, this increased reliance on data and communication networks has also increased the system's vulnerability to cyber threats. Among them, False Data Injection Attacks (FDIAs) are particularly concerning due to their stealth and potential to disrupt core grid functions. Their far-reaching impact highlights the urgent need for comprehensive vulnerability assessments and robust defense strategies to protect digitalized power systems.

In response to these challenges, this thesis investigates two high-impact FDIA scenarios: (1) coordinated, stealthy attacks targeting Phasor Measurement Unit (PMU)-based state estimation, and (2) falsification of protection signals targeting distance relays. For each case, the thesis first conducts a detailed vulnerability analysis to assess attack feasibility and impact. Building on these insights, it then develops defense strategies to enhance the cyber-physical resilience of modern power systems.

The first part of this thesis evaluates the vulnerability of PMU-based state estimation to multi-step, stealthy FDIAs, in which adversaries coordinate sequential manipulations of PMU measurements not only to evade bad data detection but also to amplify the cumulative impact on system operation. To model this attack process, a vulnerability assessment framework is proposed based on a Markov Decision Process (MDP) integrated with bi-level optimization. The MDP, solved using Q-learning, models the attacker's sequential decision-making and yields a vulnerability index that enables operators to assess system impact and identify critical attack stages for targeted defense.

This analysis highlights a key insight: while stealthy FDIAs on state estimation typically require coordinated manipulation of multiple correlated PMUs—an operationally complex task—compromising a single Phasor Data Concentrator (PDC), which aggregates data from these PMUs, allows an attacker to simultaneously alter all associated measurements. This significantly increases the feasibility and potential impact of the attack. Yet, most defense strategies remain focused on individual PMUs, overlooking the critical role of PDCs as centralized aggregation points and high-value attack targets.

To address this overlooked threat, the second part of this thesis proposes a tri-level defender–attacker–operator optimization framework for redesigning PMU-to-Super PDC (SPDC) assignments as a defense mechanism against stealthy FDIAs targeting state estimation. The objective is to minimize vulnerability to such attacks while accounting for

communication constraints such as transmission delays. Leveraging Software-Defined Networking (SDN), the framework enables dynamic reassignment of PMUs to SPDCs without additional cost, providing system operators with a practical and scalable defense strategy.

To further strengthen data aggregation–based defense strategies, it is crucial to consider not only the assignment of PMUs to PDCs but also the cyber-layer structure—including communication paths—as both a source of system vulnerability and a target for defense strategies. Building on this, the thesis analyzes the often-overlooked role of the cyber layer in vulnerability to stealthy FDIAs and introduces a Cyber-Physical Risk Metric (CPRM) that combines both the likelihood and physical impact of attacks. The CPRM quantifies risk by combining the physical consequences of losing a transmission line with the probability that such a loss results from a stealthy FDIA. This probability is estimated by identifying minimal critical PMU sets whose compromise could stealthily overload transmission lines, using an algorithm that solves multiple bi-level optimization problems. Next, Bayesian Attack Graphs (BAGs) are developed for each substation and communication link to model potential access pathways and calculate the probability of compromising the identified critical PMU sets. The thesis then proposes an optimization-based data aggregation reconfiguration scheme that leverages SDN to dynamically reconfigure both PMU-to-PDC assignments and their communication paths, minimizing the risk quantified by the developed metric and serving as a defense mechanism against stealthy FDIAs.

Finally, this thesis addresses FDIAs targeting distance protection and demonstrates that falsified measurements can severely compromise fault detection and isolation, thereby threatening power system security and stability. To defend against such attacks, a cyber-resilient protection scheme is proposed, which activates during cyber threats and temporarily backs up distance relays to maintain system integrity. The proposed protection scheme mimics the zone-based fault detection of distance relays but leverages traveling waves (TWs)—which are the natural signatures of real faults—along with dedicated hard-wired current measurements and a Random Forest (RF) classifier to identify faults in each zone. The RF classifier is trained on the attenuation patterns of TW frequency components as they propagate from fault locations to the line terminal. Since attenuation patterns depend on both frequency and travel distance, the RF classifier can accurately determine the fault zone by extracting frequency-related features from the first TW using a wavelet transform and analyzing its attenuation characteristics.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to Dr. Amir Ameli for his invaluable supervision, guidance, and encouragement throughout the course of my doctoral studies. His expertise, insightful feedback, and mentorship have been instrumental in shaping my research and helping me develop as a scholar.

I would also like to extend my sincere thanks to Dr. Mohammad Nassir Uddin for his supervision, valuable advice, and insightful discussions throughout this research. His guidance and consistent support have been greatly appreciated.

In addition, I wish to acknowledge Dr. Mohsen Ghafouri, who, although not formally my supervisor, generously provided guidance, technical discussions, and support during the research process. His unofficial mentorship was of great value in helping me navigate challenges and explore innovative approaches.

Finally, I am grateful to my colleagues, friends, and family members for their continuous encouragement and understanding throughout this challenging journey.

Dedication

This is dedicated to the one I love.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AP Attack Path

BAG Bayesian Attack Graph

BDD Bad Data Detection

CADP Communication-Assisted Distance Protection

CPRM Cyber-Physical Risk Metric

CT Current Transformer

CVSS Common Vulnerability Scoring System

CVT Capacitor Voltage Transformer

DAO Defender–Attacker–Operator

DAR Data Aggregation Reconfiguration

DoS Denial of Service

DWT Discrete Wavelet Transform

EMS Energy Management System

EWS Engineering Workstation

FDIA False Data Injection Attack

FHR First-hop Router

GAMS General Algebraic Modeling System

GNSS Global Navigation Satellite System

GOOSE Generic Object-Oriented Substation Event

GPS Global Positioning System

HMI Human-Machine Interface

IDS Intrusion Detection System

IEC International Electrotechnical Commission

IED Intelligent Electronic Device

KKT Karush–Kuhn–Tucker

LAN Local Area Network

LCDR Line Current Differential Relay

LCI Line Capacity Increment

LHR Last-hop Router

LMP Locational Marginal Price

LR Load Redistribuation

MDP Markov Decision Process

MILP Mixed-Integer Linear Programming

MU Merging Unit

OCI Operation Cost Increase

OPF Optimal Power Flow

PDC Phasor Data Concentrator

PMU Phasor Measurement Unit

PUTT Permissive Under-reaching Transfer Trip

Q-learning Q-learning Reinforcement Algorithm

RF Random Forest

SCADA Supervisory Control and Data Acquisition

SDN Software-Defined Networking

SE State Estimation

SFDIA Stealthy False Data Injection Attack

SPDC Super Phasor Data Concentrator

SV Sampled Values

TSA Time Synchronization Attack

TW Traveling Wave

VT Voltage Transformer

WACS Wide-Area Control System

WAMPAC Wide-Area Monitoring, Protection, and Control

WAMS Wide-Area Monitoring System

WAN Wide-Area Network

WAPS Wide-Area Protection System

List of Symbols

A Finite set of available actions in the MDP

A_t Set of available actions at time t in the MDP

BG Bus-generator incidence matrix

$BG_{j,g}$ Entry of the bus-generator incidence matrix indicating connection between generator g and bus j

BL Bus-load incidence matrix

$BL_{j,d}$ Entry of the bus-load incidence matrix indicating whether load d is connected to bus j

C Distributed capacitance per unit length of the transmission line [F/m]

CA_r Maximum capacity of PDC r in terms of connected PMUs

DM A matrix with n rows and p columns, where each entry $DM_{n,p}$ represents the minimum end-to-end communication delay between PMU n and PDC p

$DM_{n,r}$ The minimum end-to-end delay between PMU n and PDC p, as specified in the delay matrix DM

E_{D_j} Absolute energy of the detail wavelet coefficients at decomposition level j

F Probability function for line tripping as a function of power flow ratio

$F(Z_A)$ Defender objective function to minimize the impact of false data injection attacks

G Distributed conductance per unit length of the transmission line [S/m]

H Linear measurement-to-state dependency matrix in DC SE

$I_a^{\mathbf{TW}}$ First arrival traveling wave current in phase a

$I_b^{\mathbf{TW}}$ First arrival traveling wave current in phase b

$I_c^{\mathbf{TW}}$ First arrival traveling wave current in phase c

L Distributed inductance per unit length of the transmission line [H/m]

$LP_{d,n}$ Element in row d and column n of the load-PMU incidence matrix, indicating the connection between load d and PMU n

M_g Ramp rate limit of generator g in MW per unit time

O_l^s Set of all possible combinations of compromised components (PMUs, PDCs, or communication links) that can be used to manipulate the data of critical set Ω_l^s

PD Vector of load demands

PD_t Vector of load demands at time t

PD_{t+1} Vector of load demand at time $t+1$

PG Vector of generator active power outputs

PG_t Vector of generator active power output at time t

PG_{t+1} Vector of generator active power outputs at time $t+1$

$PI(l)$ Physical impact associated with the loss of transmission line l

$PL(l)$ Active power flow on transmission line l

$PL_{t+1}(l)$ Active power flow on transmission line l at time $t+1$

PM A binary matrix with n rows and a columns, where $PM_{n,a} = 1$ if PMU n records measurement a, and 0 otherwise

P_d Active power demand at load bus d

P_d^h Active power demand of load d at hour h

P_g Active power dispatch of generator g (scalar)

P_g^0 Previous dispatch level of generator g

$P_g^{\max}$ Maximum active power output rating of generator g

$P_g^{\min}$ Minimum active power output rating of generator g

$P_l^{\max}$ Thermal capacity limit of transmission line l

R Distributed resistance per unit length of the transmission line [Ω/m]

$R(s_{t+1} \mid s_t, a_t)$ Reward function for transitioning from state s_t to s_{t+1} under action a_t

RE Residual vector, difference between actual and calculated measurements

S Finite set of system states in the MDP

SD_t Vector of load shedding amounts at time t

SD_{t+1} Vector of load shedding amounts at time $t+1$

SF_l Row l of the shift factor matrix, quantifying the sensitivity of power flow on line l to bus injections

S_d Amount of curtailed load demand at bus d

$T(s_{t+1} \mid s_t, a_t)$ Transition probability from state s_t to s_{t+1} given action a_t

T_h Look-ahead OPF time horizon

T_r Waiting time of PDC p after the first data packet arrives

$V(s_t)$ Value function representing the expected reward when starting from state s_t and following the optimal policy

Y Bus admittance matrix of the network

$Y_t^{l,r}$ Admittance matrix at time t after tripping line l and recovering line r

Y_t^l Admittance matrix at time t after tripping line l

Y_t^r Admittance matrix at time t after recovering line r

Y_t Bus admittance matrix of the power system at time t

$Y_{j,i}$ Element of the bus admittance matrix between buses j and i

Z Measurement vector

$Z^l_{A|D}$ Sub-vector of the attack vector injected into load measurements for overloading line l

$Z^l_{A|K}$ Sub-vector of the attack vector injected into line measurements for overloading line l

Z^l_A Attack vector injected into system measurements to overload line l

Z_A Overall false data injection attack vector applied to system measurements

Z_A False data injection attack vector

$Z_{A|D}$ Sub-vector of the attack vector injected into load measurements

$Z_{A|K}$ Sub-vector of the attack vector injected into line measurements

Z^A_{ag} Apparent impedance measured by the phase-A ground element under normal sampled values

Z^M_{ag} Apparent impedance measured by the phase-A ground element under manipulated sampled values

$\Delta P_{l,d}$ Change in the power flow of line l due to an attack targeting load d

$\Delta\hat{\theta}$ Change in the estimated voltage phase angles caused by the attack

$\Delta\hat{x}$ The deviation of the estimated states from their true values after injecting false data into measurements

Γ^i_l The i-th distinct combination of compromised targets within Γ_l

Γ_l Set containing all possible unique sets of compromised targets (PMUs, PDCs, or communication links) that could alter data of any critical set for line l

Ω^s_l The s-th critical PMU set for line l, defined as the set of PMUs selected for protecting line l during the s-th optimization iteration

α Attenuation constant, quantifies the exponential decay of wave amplitude along the line

α Learning rate for Q-learning updates

β Phase constant, represents the phase shift per unit length along the line

β_1 Weighting coefficient for the unserved load component in the reward function

β_2 Weighting coefficient for the available generation component in the reward function

β_3 Weighting coefficient for the operational margin component in the reward function

β_1 Weighting factor for unserved load

β_2 Weighting factor for available generation capacity

β_3 Weighting factor for operational security margin

δ_r Binary decision variable indicating whether PDC r is targeted by the attack

ϵ Congestion threshold factor defining when a line is considered congested

η Absolute maximum allowed perturbation on line measurements

γ Discount factor balancing immediate versus future rewards

$\hat{\theta}$ Estimated voltage phase angles at the system buses

$\hat{x}$ Estimated system states (voltage magnitudes and phase angles at buses)

λ Restoration rate parameter in the exponential distribution for line repair or reset times

$\mathbb{C}$ Set of conditions in the attack graph

$\mathbb{E}$ Set of exploits in the attack graph

$\mathbb{L}$ Privilege condition (user permissions or access levels) in the attack graph

$\mathbb{N}$ Connectivity condition (network reachability) in the attack graph

$\mathbb{S}$ Service existence condition (presence of a required vulnerable service) in the attack graph

$\mathbf{I}_{abc}$ Vector of actual phase currents in phases a, b, and c

$\mathbf{I}_{abc}^{M}$ Vector of manipulated phase currents in phases a, b, and c

$\mathbf{V}_{abc}$ Vector of actual phase-to-ground voltages in phases a, b, and c

$\mathbf{V}_{abc}^{M}$ Vector of manipulated phase-to-ground voltages in phases a, b, and c

$\mathcal{C}$ Set of congested transmission lines where the power flow exceeds the congestion threshold

$\mathcal{D}$ Set of all load buses in the system

$\mathcal{F}_r$ Set of all feasible communication paths between PDC_r and the control center

$\mathcal{G}$ Set of generators in the system

$\mathcal{L}$ Set of lines in the power system

$\mathcal{L}_t$ Set of in-service transmission lines at time t

$\mathcal{P}_R(t_{lost})$ Probability of restoring a previously tripped line during the out-of-service time t_{lost}

$\mathcal{P}_S$ Probability that action a_t^l causes tripping of line l due to overload

$\mathcal{Q}_{n,r}$ Set of all feasible communication paths between PMU_n and PDC_r

$\mathcal{R}$ Set of Phasor Data Concentrators (PDCs) to which PMUs can be assigned

μ^h Average daily load variation coefficient at hour h (identical across all loads)

ϕ Threshold parameter for determining critical PMUs based on their influence on congested lines

π^* Optimal policy mapping states to actions to maximize expected reward

σ Maximum proportion of change allowed relative to actual load demand

τ Detection threshold for the residual norm

θ^d Set of transmission lines connected to load d

θ_i Voltage phase angle at bus i

$\tilde{E}^a_{D_j}$ Relative energy at detail level D_j for phase a

$\tilde{E}^b_{D_j}$ Relative energy at detail level D_j for phase b

$\tilde{E}^c_{D_j}$ Relative energy at detail level D_j for phase c

$\tilde{E}_{D_j}$ Relative energy of the detail coefficients at decomposition level j as a percentage of the total energy across all levels

ϑ_d^h Random variation coefficient for load d at hour h, accounting for type-dependent differences

a_t Action taken at time t

c_g Unit generation cost for generator g in \$/MW

$c_{j,k}$ Approximation coefficient at decomposition level j and position k, capturing low-frequency components

ca_g Constant (fixed) cost coefficient of generator g, accounting for startup or maintenance costs independent of power output

cq_g Quadratic cost coefficient of generator g, representing the nonlinear cost component proportional to the square of the generated active power

cs_d Unit load shedding cost for load d in \$/MW

$d_{j,k}$ Detail coefficient at decomposition level j and position k, capturing high-frequency components

de Total end-to-end delay of a data packet

de_p Propagation delay component of the end-to-end delay

de_q Queuing delay component of the end-to-end delay

de_s Processing delay component of the end-to-end delay

de_t Transmission delay component of the end-to-end delay

$h(\hat{x})$ Nonlinear measurement function relating states to measurements

mc_1, mc_2, mc_3 Manipulation coefficients applied to the three-phase voltage samples

mc_4, mc_5, mc_6 Manipulation coefficients applied to the three-phase current samples

$p(A\_l)$ Probability of a successful cyberattack affecting transmission line l

$p(\Gamma_l^i)$ Probability of accessing the i-th combination of compromised components for line l

s_1 Initial state of the system at the start of each episode

s_t State of the system at time t

$t_{n,r,q}$ Processing and communication delay for path q between PMU n and PDC r

u_a Binary variable indicating whether measurement a is compromised ($u_a = 1$) or not ($u_a = 0$)

$u_{a|d}$ Component of u_a associated with load measurements

$u_{a|k}$ Component of u_a associated with line measurements

$v_{n,r,q}$ Binary variable indicating whether communication path q connects PMU n to PDC r

$w^l_{n,s}$ A binary variable indicating whether PMU n is selected for monitoring Line l during the s-th optimization iteration, or equivalently, whether critical set s contains PMU n

w^l_n A binary decision variable indicating whether the data of the Phasor Measurement Unit (PMU) at bus n (denoted by PMU_n) is manipulated in order to overload line l; 1 if attacked, 0 otherwise

w_n Binary variable indicating whether PMU n is compromised ($w_n = 1$) or not ($w_n = 0$)

$x^{h-1}_{n,r}$ Binary variable indicating whether PMU n was connected to PDC r at hour $h-1$

$x^h_{n,r}$ Binary variable indicating whether PMU n is connected to PDC r at hour h

$y_{r,f}$ Binary variable indicating whether path f connects PDC r to the control center

$z^l_{a|d}$ Element of $Z^l_{A|D}$ affecting load measurements

$z^l_{a|k}$ Element of $Z^l_{A|K}$ affecting line measurements

$z_{a|d}$ Element of $Z_{A|D}$ affecting load measurements

$z_{a|k}$ Element of $Z_{A|K}$ affecting line measurements

V Three-dimensional binary matrix representing available communication paths from PMUs to PDCs

X Binary PMU-to-PDC assignment matrix

Y Binary PDC-to-control-center connection matrix

$I(x,t)$ Instantaneous current at position x and time t

$V(x,t)$ Instantaneous voltage at position x and time t

$\mathcal{N}$ Set of PMUs available for assignment

$x_{n,r}$ Binary decision variable indicating whether PMU n is assigned to PDC r (1 if assigned, 0 otherwise)

Chapter 1

Introduction

The increasing complexity and dynamic behavior of modern electric power systems, driven by the integration of renewable energy resources, distributed generation, and evolving load patterns, have necessitated significant advancements in grid monitoring, protection, and control technologies [88]. To address this growing demand, Wide-Area Monitoring, Protection, and Control (WAMPAC) systems, together with digital substations, have emerged as critical enablers for enhancing grid resilience, situational awareness, and operational flexibility. WAMPAC systems leverage time-synchronized phasor measurements to provide operators with a system-wide, real-time view of grid dynamics, enabling early detection of disturbances, improved situational awareness, and coordinated wide-area protection [86]. Concurrently, digital substations replace conventional analog infrastructures with advanced communication networks and Intelligent Electronic Devices (IEDs), supporting flexible, automated, and efficient protection and control functions at the substation level [64]. Collectively, WAMPAC systems and digital substations constitute the two main elements of the modern smart grid, facilitating the seamless integration of renewable energy, improving operational visibility, and enabling rapid, informed control actions to maintain grid security and resilience [88, 86, 64].

However, the increasing reliance on digital communication technologies, standardized protocols, and information-centric architectures in both WAMPAC systems and digital substations has significantly expanded the cyber-physical attack surface. Although the interconnected nature of these systems provides substantial operational benefits, it simultaneously introduces novel vulnerabilities that may be exploited by sophisticated cyber adversaries. [88]. Ensuring the cybersecurity and reliability of these critical infrastructures is therefore paramount for safeguarding the stability, security, and resilience of modern power grids. Consequently, analyzing the vulnerability of these systems to cyber threats

and developing effective defense mechanisms is highly necessary. In the following sections, a concise background on WAMPAC systems and digital substations is provided, followed by a discussion of existing research, identified gaps, and the specific contributions of this thesis.

1.1 Wide Area Monitoring, Protection, and Control System

In general, WAMPAC systems are composed of three main subsystems: the Wide-Area Monitoring System (WAMS), the Wide-Area Protection System (WAPS), and the Wide-Area Control System (WACS) [11]. Figure 1.1 depicts the architecture of a wide-area measurement system within the power grid, which is essential for the operation of WAMPAC applications. As shown in Figure 1.1, PMUs provide the control center with measurements that are time-synchronized using the GPS signal. The measurements collected by PMUs are initially transmitted to PDCs via a communication network, where they are rearranged in chronological order. Subsequently, the sorted measurements are sent to the Super PDC of the control center to be utilized in WAMPAC applications.

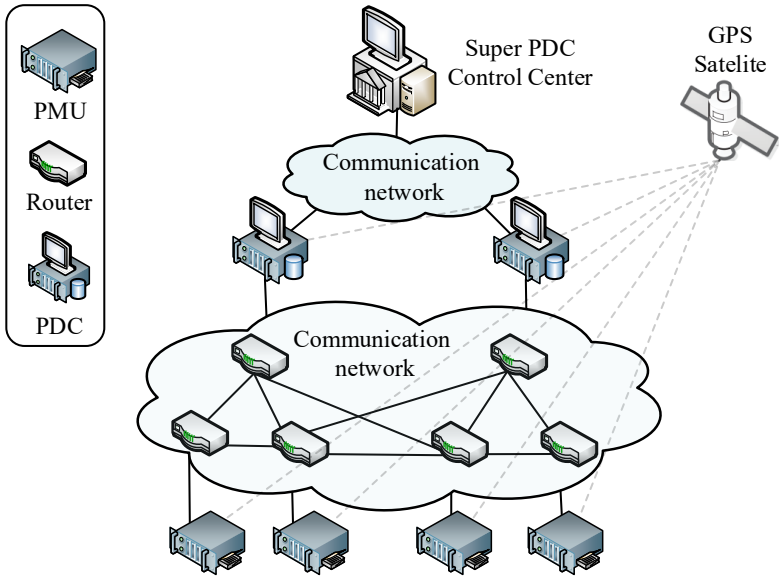


Figure 1.1: The architecture of wide area measurement system within the power systems.

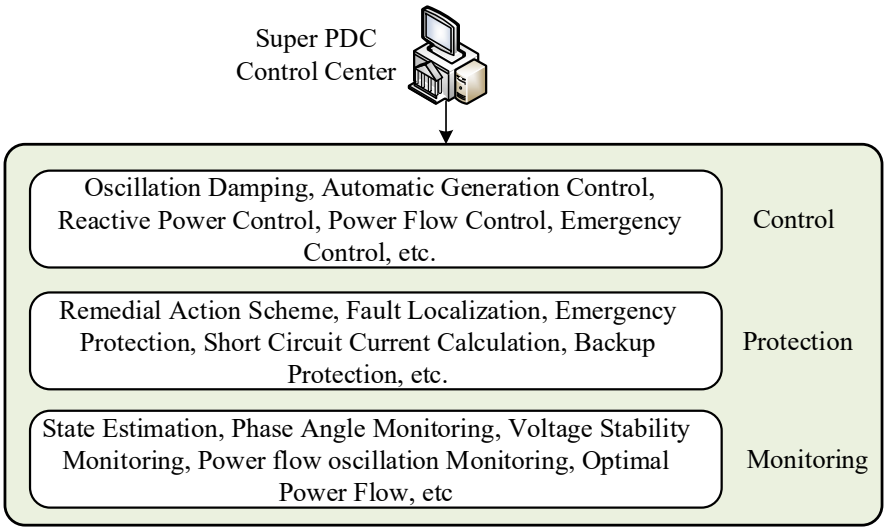


Figure 1.2: The application of WAMPAC system.

The applications operating within the WAMPAC system are depicted in Figure 1.2 and include numerous critical functions such as oscillation damping, emergency protection, voltage stability monitoring, and more. By utilizing synchronized data collected from PMUs, WAMPAC systems enable real-time monitoring and control of power grids, contributing to enhanced grid operational efficiency and reliability [88]. In addition to supporting WAMPAC functions, the data acquired from PMUs can also be leveraged by the Energy Management System (EMS). By providing high-resolution, time-synchronized measurements across the grid, PMU data enhances State Estimation (SE), improves the accuracy of network models, and supports advanced control and optimization functions within the EMS. This integration enables more reliable, secure, and efficient grid operation.

Nevertheless, the integration of WAMPAC systems introduces new operational and cybersecurity challenges due to their reliance on communication networks and digital infrastructures. As WAMPAC systems become an integral part of the smart grid, ensuring their security and resilience against cyber threats has become paramount.

1.1.1 Cybersecurity Challenges in WAMPAC System

The three main components of WAMPAC systems— PMUs, PDCs, and communication links—are essential for system operation but also present significant cybersecurity vulnera-

bilities [12, 68, 47, 88]. WAMPAC elements are susceptible to several types of cyberattacks, including data integrity attacks, Denial of Service (DoS) attacks, time-based attacks, replay attacks, and traffic analysis attacks. Among these threats, ensuring data integrity is particularly critical, as the reliability and accuracy of WAMPAC applications depend heavily on the trustworthiness of measurement and control data [88]. A compromise in data integrity can lead to erroneous decision-making processes that jeopardize system stability and security.

Within WAMPAC systems, data integrity attacks may manifest in various forms, including the alteration of PMU measurements [22, 94], manipulation of breaker statuses [57], injection of malicious control commands [6], and falsification of the Area Control Error (ACE) signal [76]. These attacks, whether executed individually or in combination, can escalate into sophisticated and highly damaging cyber incidents, underscoring the critical need to safeguard data integrity.

Among the various types of data integrity attacks, SFDIAs targeting SE have emerged as a significant concern for the security of the power system. A carefully designed SFDIA can bypass the Bad Data Detection (BDD) mechanisms embedded within the SE process—one of the most critical functions in WAMPAC and EMS—allowing falsified system states to be presented to operators without raising alarms [42]. When successful, such attacks compromise the system state, which not only misleads operators' situational awareness but also undermines the core functionalities of WAMPAC and EMS. These functionalities include real-time monitoring, wide-area protection schemes, and emergency control actions in WAMPAC, as well as contingency analysis and optimal power flow calculations in EMS—all of which depend on accurate and trustworthy system information [20]. When this information is corrupted, control decisions may be based on false data, potentially triggering inappropriate actions that jeopardize grid stability and increase the risk of widespread disturbances. Given their stealthy nature and the far-reaching consequences of a successful attack, SFDIAs pose a serious threat to grid resilience. This underscores the urgent need for comprehensive vulnerability assessments and the development of robust defense mechanisms to safeguard the operational integrity of modern power systems.

1.1.2 Vulnerability Analysis of WAMAPC Systems to SFDIAs: State-of-the-Art and Research Gaps

The vulnerability of WAMPAC systems to SFDIAs is often evaluated using a bi-level optimization framework [94, 44, 54, 28, 85, 29, 98]. In this framework, the upper level simulates the attacker's objectives and constraints, while the lower level models the system's

response to the compromised data. This method accurately identifies the worst-case attack scenarios by maximizing the potential impact (e.g., economic loss or physical damage) an attacker could inflict on the system. For instance, the authors of [94, 44] demonstrate that SFDIAs can cause substantial economic losses by deceitfully persuading operators to steer the power system away from its most cost-effective operating points. Additionally, as shown in [54, 28, 29, 98, 69, 85], SFDIAs can result in physical damage, which is particularly critical as it directly compromises the stability and reliability of the system. Such damage can occur if an attacker misleads the operators into making decisions that violate the operational constraints of the grid. For example, as detailed in [54], SFDIAs can deceive the operators into dispatching generators in a manner that causes one or more transmission lines to become significantly overloaded, triggering protective relays to trip the lines. Moreover, the authors of [28, 69] demonstrate that simultaneous overloading of several lines due to SFDIAs can lead to cascading failures.

Research Gaps in Vulnerability Analysis of WAMPAC System to SFDIAs

Despite the abundance of literature on the vulnerability analysis of WAMPA systems to SFDIAs, several critical aspects have not been adequately studied. Firstly, these vulnerability analyses generally assume that an attacker executes the SFDIA in a single step [44, 99, 94, 58, 60, 21, 95, 54, 28, 29, 56, 98, 69]. Based on this premise, SFDIAs are considered capable of causing significant physical impacts on the system only under specific conditions: when the power system operates near its operational constraints [28], or when FDIAs are coordinated with topology attacks [30, 93]. If these conditions are not met, the attack may not significantly affect the system's stability or performance. However, this assumption may not always hold, as attackers with access to a dataset can manipulate it over several steps. For instance, an attacker may strategically deploy SFDIAs across multiple time steps with the goal of amplifying their cumulative impact. Nevertheless, the vulnerability of power systems to such multi-step SFDIAs has not yet been thoroughly analyzed. This could lead to an underestimation of the system's vulnerability to SFDIAs.

The second gap in the existing literature is the neglect of the cyber layer in vulnerability analyses. While such analyses emphasize that executing SFDIAs requires access to and manipulation of data from numerous PMUs within the system, they rarely examine the feasibility of obtaining this access. In reality, such feasibility depends heavily on the specifications of the cyber layer and the structure of data aggregation. Most existing studies largely overlook the cyber layer and instead impose arbitrary limits on the number of measurements that can be manipulated [94, 44, 54, 28]. However, this approach oversimplifies the complex hierarchical data aggregation architecture, which involves multiple

PMUs, PDCs, and communication links. Such oversimplification can result in omitting critical vulnerabilities that significantly influence the results of vulnerability analysis and may ultimately lead to ineffective defense measures. For example, an attacker might gain access to data from several PMUs by compromising a single PDC or communication link. However, such a scenario is not considered in current vulnerability analysis, resulting in a focus on defense measures that primarily secure individual PMUs.

1.1.3 Defense Strategies Against SFDIAs: State-of-the-Art and Research Gaps

The defense mechanisms against SFDIAs can be broadly categorized into three main classes: proactive physical layer-based approaches, proactive cyber layer-based approaches, and reactive cyber layer-based approaches, which are described below.

- **Proactive Physical Layer-Based Approaches:** These methods focus on the physical infrastructure of the power system to enhance resilience against SFDIAs. For instance, the authors in [26, 32, 90] propose preventive generation dispatch strategies to mitigate the risks of line overloads and potential blackouts. These strategies ensure that even when false data is injected, transmission lines remain within safe operational limits. Similarly, [80] introduces a secure unit commitment approach to maintain grid operation under attack conditions.

- **Proactive Cyber Layer-Based Approaches:** These methods focus on strengthening the cyber layer by securing selected PMUs against cyberattacks. They can be further divided into two subcategories based on the scope of protection. The first subcategory, as represented by works such as [82, 59], aims to comprehensively protect PMUs to ensure that no stealthy attacks can be launched. For example, [59] formulates a bi-level optimization problem to identify the minimum number of measurements that must be secured to prevent an attacker from executing an SFDIA. The second subcategory, exemplified by studies such as [87, 36], focuses on safeguarding only the most critical PMUs to mitigate the risk of high-impact SFDIAs. These approaches often employ tri-level optimization frameworks to model the interactions between the attacker and the power system operator. For instance, [36] proposes a tri-level model to determine the optimal set of measurements to protect, thereby minimizing the adverse impact of FDIAs on operational costs.

- **Reactive Cyber Layer-Based Approaches:** Unlike proactive methods, reactive strategies mitigate cyberattacks after they have been detected. These methods typi-

cally focus on restoring system functionality and isolating compromised components. For example, [55] introduces a self-healing PMU network using Software-Defined Networking (SDN), which dynamically reconfigures the network to isolate compromised devices and restore observability. Similarly, [67] proposes disconnecting high-risk PMUs based on infection probability, while [49] reroutes communication paths to contain attack propagation.

Research Gaps in Defense Strategy against SFDIAs

Despite the range of defense mechanisms proposed in the literature, each major class of defense strategies exhibits critical limitations [26, 32, 90, 80, 82, 59, 67]. Proactive physical layer-based approaches, although effective at maintaining system stability, often lead to suboptimal economic performance and increased operational costs, making them less practical for routine operation. Proactive cyber-layer strategies, particularly those aiming to secure PMUs, typically require protecting a large number of measurement devices, which may not be feasible under realistic budget or infrastructure constraints [26, 32]. Even when prioritizing only the most critical PMUs, their effectiveness can vary significantly depending on system operating conditions, making complete protection difficult to achieve [36]. Moreover, most of these studies overlook the potential vulnerabilities introduced by the data aggregation architecture itself, such as the role of PDCs as aggregation points whose compromise could enable simultaneous manipulation of multiple PMUs. Finally, reactive cyber-layer defense strategies, while valuable for mitigating the consequences of an attack after it occurs, cannot proactively address vulnerabilities or prevent attacks before they are launched [67]. These observations highlight the urgent need for a more comprehensive defense strategy that does not impose excessive costs, does not depend on specific operating conditions, does not focus exclusively on PMUs, explicitly considers data aggregation vulnerabilities, and can be activated proactively before an attack occurs.

1.2 Digital Substation

The increasing complexity of modern power systems, combined with growing demands for enhanced reliability, efficiency, and operational flexibility, has accelerated the shift from conventional to digital substations [64]. Digital substations, based on the IEC 61850 standard, mark a major technological evolution by replacing traditional point-to-point analog wiring with Ethernet-based digital communication networks that interconnect intelligent

electronic devices (IEDs) [83]. At the core of this transformation are standardized communication services such as Generic Object-Oriented Substation Event (GOOSE) messaging, which enables fast, event-driven transmission of protection and control signals, and Sampled Values (SV) communication, which allows the real-time delivery of sampled current and voltage data from merging units to protection and monitoring IEDs.

The digital substation architecture, as shown in Fig. 1.3, is organized into four hierar-

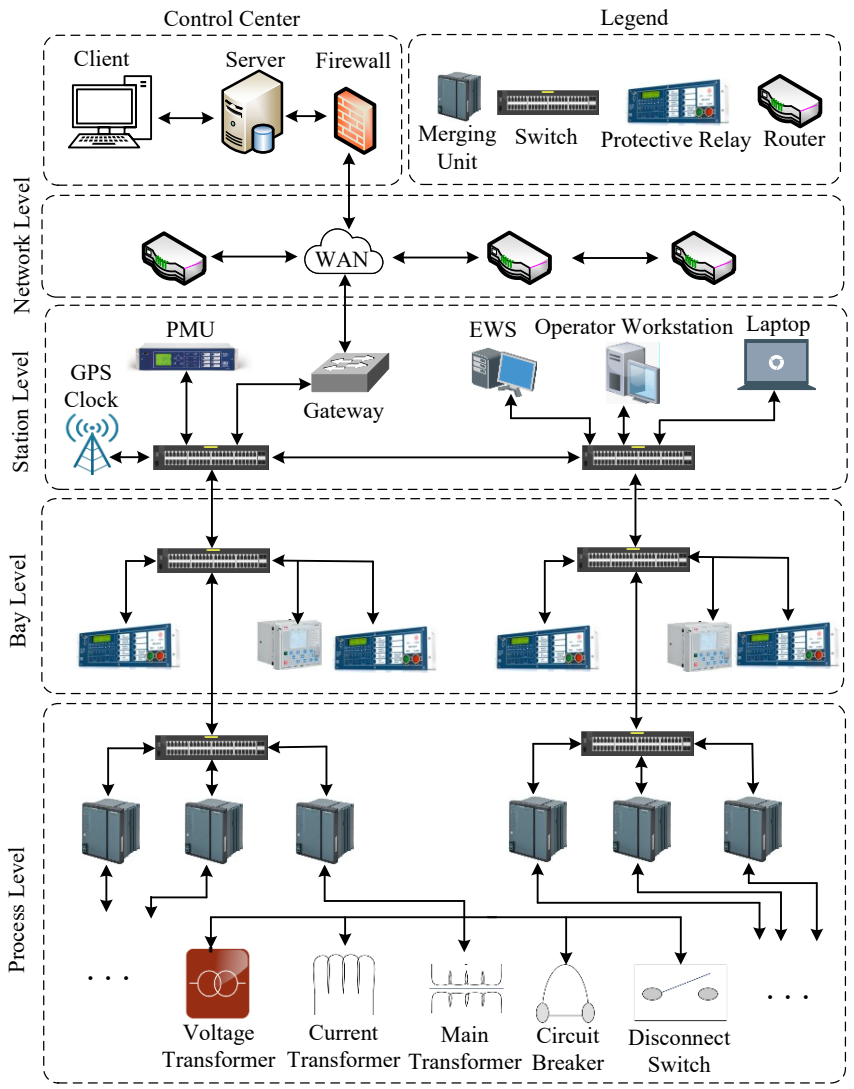


Figure 1.3: The structure of digital substations.

chical levels:

- **Process Level**: This level interfaces directly with primary equipment such as Current Transformers (CTs), Voltage Transformers (VTs), circuit breakers, and disconnect switches. Merging Units (MUs) located at the process level collect analog signals and convert them into digital SVs, transmitting these data streams over communication networks to higher levels.
- **Bay Level**: Bay controllers and protection IEDs reside at this level, receiving digital data from the process level. They perform local protection and control functions, making rapid decisions based on processed measurements and equipment status.
- **Station Level**: The station level hosts Human-Machine Interfaces (HMIs), engineering workstations, and Supervisory Control and Data Acquisitions (SCADAs) systems. It provides centralized monitoring, configuration, and control for the entire substation, and acts as the interface between the substation and the control center.
- **Network Level**: This level encompasses the communication infrastructure that interconnects devices across the substation and beyond. It includes switches, routers, and Wide-Area Networks (WANs) that facilitate inter-substation and control center communications.

This layered architecture, enabled by standardized communication protocols, facilitates interoperability, reduces wiring complexity, and enhances operational efficiency [64]. Nevertheless, this integration of digital communication networks introduces new cybersecurity vulnerabilities affecting critical components of digital substations, especially protection functions. Given their essential role in fault detection, isolation, and maintaining overall power system stability, these functions have become high-risk targets for cyberattacks capable of severely compromising system reliability and safety. Accordingly, the subsequent sections focus on protection functions within digital substations and the cybersecurity threats that endanger them.

1.2.1 Protection Functions in Digital Substations

Protection functions are fundamental to ensuring the stability and security of power systems. They detect abnormal operating conditions and initiate the timely isolation of faulty components to prevent system-wide disturbances and potential equipment damage [18]. In digital substations, these functions are implemented within IEDs, which operate based

on data exchanged over standardized communication networks. Specifically, protection functions rely on SV messages to receive time-synchronized measurements of current and voltage, and on GOOSE messages for the rapid exchange of control commands and status signals. This communication infrastructure enables fast, coordinated, and reliable protection responses across the substation [14].

There are several protection functions designed to secure transmission lines, including distance protection, directional ground fault, line differential, over/under voltage protection, etc. Among these, distance protection plays a particularly critical role in safeguarding high-voltage transmission networks. It enables rapid, zone-based fault detection by estimating the apparent impedance between the relay location and the fault point using real-time voltage and current measurements. This impedance-based approach allows distance protection to distinguish between in-zone and out-of-zone faults, ensuring fast and selective isolation of the affected line sections while minimizing unnecessary tripping [18].

Due to its speed, selectivity, and coordination capabilities, distance protection is widely employed as the primary protection scheme for transmission lines and often serves as a backup for other protection functions. In modern digital substations, it is further enhanced through communication-assisted schemes such as Permissive Underreach Transfer Trip (PUTT), Permissive Overreach Transfer Trip (POTT), and Direct Transfer Trip (DTT) [18]. These schemes rely on high-speed communication between relays at opposite ends of the line to coordinate trip decisions, thereby improving fault clearance times and enhancing system dependability in complex grid topologies [43].

The reliability and security of all protection functions—particularly conventional and communication-assisted distance protection schemes—highly depend on the integrity, authenticity, and availability of digital communication services. This dependence introduces new cybersecurity vulnerabilities, as the malicious manipulation, delay, or suppression of critical messages—such as SV and GOOSE—can result in false tripping, protection failure, or miscoordination between relays. Consequently, assessing the cyber vulnerabilities of protection systems and enhancing their resilience—especially for distance protection—have become critical tasks in securing modern power systems.

1.2.2 Cybersecurity Vulnerabilities of Protection Functions in Digital Substations: State-of-the-Art and Research Gaps

Research on the cybersecurity of protection systems within digital substations is still in its early stages but has begun to receive increasing attention. For instance, studies such

as [14, 15] have identified the susceptibility of various types of Line Current Differential Relay (LCDR)—including phasor-based, SV-based, and DC relays—to False Data Injection Attacks (FDIAs) and Time Synchronization Attacks (TSAs). These studies have also proposed detection mechanisms to mitigate such specific attack types. In parallel, researchers in [52, 74, 13, 75] have applied machine learning techniques to detect stealthy cyberattacks targeting LCDRs. However, most of these studies operate under the assumption that local substation data, such as current and voltage sample values, are inherently trustworthy, and only data transmitted over external communication links are susceptible to compromise. This assumption significantly limits their applicability, as FDIA scenarios involving compromised local data can render these methods ineffective for ensuring reliable fault protection.

Additionally, as discussed in Section 1.2.1, distance protection plays a vital role in securing transmission lines. However, most existing research has primarily focused on LCDRs, leaving distance relays relatively underexplored in the context of cybersecurity. To date, only a limited number of studies have specifically addressed the unique cyber threats and challenges associated with distance protection schemes. For instance, [39] proposes a defense strategy against cyberattacks targeting distance protection and circuit breaker control within a digital substation. This strategy employs a collaborative verification mechanism among IEDs, where devices cross-check configuration settings and validate measurement consistency using multi-source data comparison. This ensures resilience against FDIAs and prevents unauthorized modifications to protection settings. However, this approach overlooks pilot signal attacks and assumes that most relays in the substation remain healthy, which limits its applicability in adversarial scenarios. Similarly, [43] analyzes vulnerabilities in Communication-Assisted Distance Protection (CADP) schemes, demonstrating how attacks can trigger cascading outages. It also proposes physical mitigation strategies, such as communication channel redundancy and directional comparison blocking, to enhance resilience. While these solutions address pilot signal attacks and DoS threats, they rely on redundancy, which is neither efficient nor scalable. Furthermore, the study does not consider scenarios where attackers manipulate data within substations, focusing solely on pilot signal vulnerabilities. The limitations of these studies highlight the need for more comprehensive research into the cybersecurity of distance protection schemes, particularly in addressing pilot signal vulnerabilities and scenarios where measurements within a substation are manipulated.

1.3 Research Objectives

Driven by the above-mentioned motivations and identified research gaps, this thesis aims to address these challenges through the following main objectives:

1. Develop a framework to analyze the vulnerability of power systems to multi-step SFDIAs targeting state estimation, where each step is strategically planned to amplify the cumulative impact.
2. Develop a cyber-physical risk metric that not only considers the impact of SFDIAs targeting state estimation but also incorporates the cyber-layer architecture into the vulnerability analysis.
3. Develop a proactive, cyber-layer-based defense mechanism against SFDIAs targeting state estimation that does not impose additional costs on the power system.
4. Reveal the vulnerabilities of distance protection within digital substations and investigate the consequences of cyberattacks targeting these systems.
5. Develop a cyber-resilient distance protection scheme capable of providing zone-based protection for the power system under cyberattack conditions.

1.4 Dissertation Outline

This dissertation is divided into two main parts. The first part, presented in the next three chapters, concentrates on the vulnerability analysis of power systems to SFDIAs against SE, as well as defense mechanisms for securing these functions. The second part, presented in the subsequent chapter, focuses on the cybersecurity of distance protection within digital substations and proposes methods for cyber-resilient distance protection schemes. The individual chapters of this thesis are organized as follows:

Chapter 2 aims to develop a comprehensive framework for assessing the vulnerability of power systems to multi-step SFDIAs. To achieve this, it first provides essential background on the operating principles of SE and BDD, and highlights the conditions under which BDD can be bypassed, allowing false data to remain undetected while misleading the SE process. It then reviews bi-level optimization models typically used to assess the vulnerability of WAMPAC systems to SFDIAs, and introduces an integrated framework that combines bi-level optimization with a Markov Decision Process (MDP)

to evaluate the system's vulnerability to multi-step SFDIAs. The proposed MDP is solved using Q-learning to derive a vulnerability index, which supports operators in assessing the impact of multi-step SFDIAs and in identifying the attacker's most critical actions at each stage, thereby guiding the implementation of effective and targeted defense strategies.

Chapter 3 targets minimizing the power system's vulnerability to SFDIAs by optimizing the assignment of PMUs to PDCs. To motivate this goal, the chapter first demonstrates—through a case study—that the common practice of assigning PMUs to PDCs based on geographical proximity often results in spatially correlated PMUs being grouped under a single PDC, making them a critical entry point for stealthy cyberattacks. To address this risk, the chapter proposes a tri-level Defender–Attacker–Operator (DAO) optimization framework that redesigns the data aggregation scheme from PMUs to the Super Phasor Data Concentrator (SPDC) at the control center. This framework aims to minimize vulnerability to SFDIAs by optimizing the PMU-to-PDC assignment. It not only enhances grid resilience against cyber threats but also accounts for practical communication constraints, such as data transmission delays. Leveraging SDN, which enables reconfiguration of the network structure without additional infrastructure costs, the framework offers a viable defense strategy for power system operators against FDIAs.

Chapter 4 aims to minimize the power system's vulnerability to SFDIAs by optimizing both the assignment of PMUs to PDCs and the structure of the cyber layer, including communication paths. To achieve this, the chapter first proposes a novel Cyber-Physical Risk Metric (CPRM) that assesses the system's vulnerability to SFDIAs by integrating the physical consequences of transmission line loss—such as load shedding or generation loss—with the probability of such events being triggered by cyberattacks. The likelihood of losing a transmission line is quantified by identifying all critical PMUs sets, defined as sets whose measurements can be manipulated to stealthily overload a line. These sets are determined through an algorithm that solves multiple bi-level optimization problems. Subsequently, Bayesian Attack Graphs (BAGs) are developed for each substation and communication link to model potential access pathways and compute the probability of compromising these critical PMUs sets. Building on this vulnerability assessment, the chapter introduces a novel Data Aggregation Reconfiguration (DAR) scheme that dynamically reconfigures the cyber-layer structure using SDN to reduce the risk of successful SFDIAs.

Chapter 5 develops a cyber-resilient distance protection scheme that provides zone-based protection for power systems under cyberattack conditions. To highlight the need for such a solution, the chapter first presents a case study demonstrating that conventional

distance protection schemes are highly vulnerable to FDIAs targeting SV or pilot signal messages. In response, the proposed scheme replicates the zone-based fault detection functionality of traditional distance relays, but instead leverages Traveling Waves (TWs)—the natural signatures of real faults—combined with dedicated hard-wired current measurements and a Random Forest (RF) classifier for fault zone identification. The RF classifier is trained on the attenuation patterns of TW frequency components as they propagate from fault locations to line terminals. These patterns, which vary with both frequency and propagation distance, are extracted using wavelet transform techniques applied to the first arriving TWs, enabling accurate zone classification based on their attenuation characteristics.

Chapter 6 concludes the dissertation, highlights its contributions, and suggests topics for future research.

Chapter 2

Vulnerability Analysis of Power Systems to Multi-Step SFDIAs

SE is fundamental to modern power system operations, delivering accurate, real-time assessments of the system's operating state. Reliable SEs underpin critical steady-state functions—such as economic dispatch, contingency analysis, and Optimal Power Flow (OPF)—as well as dynamic functions including stability monitoring, oscillation damping, and wide-area protection coordination [88, 17]. Since these functions rely on timely and trustworthy system state information, the quality of SE has a direct and substantial impact on the security, reliability, and overall effectiveness of power system operations. Accurate SE enables operators to make informed decisions, coordinate protective and corrective actions, and maintain system stability under both normal and contingency conditions. Given this central role, the compromise of SE poses a profound threat to the security and stability of the entire power grid. SFDIAs, which are capable of bypassing traditional BDD algorithms within the state estimator, represent a particularly severe risk. By feeding operators falsified system states, these attacks can systematically mislead downstream applications, including OPF, contingency assessment, wide-area protection, and emergency control strategies. Such cascading impacts mean that decisions based on corrupted estimates could result in economically inefficient, insecure, or even hazardous system operation [54, 44, 28]. Therefore, conducting a thorough vulnerability analysis of power systems to SFDIAs targeting SE is critically important for safeguarding secure and resilient power system operations.

As discussed in Section 1.1.2, bi-level optimization is a common method for analyzing the vulnerability of power systems to SFDIAs [99, 94, 58, 44, 28, 54, 21]. This framework

determines the maximum potential damage an attacker can inflict on the system by manipulating measurement data. In this formulation, the upper level models the attacker's objectives and constraints in altering the data, while the lower level represents the operator's response to the manipulated measurements. However, these bi-level optimization models generally address only single-step SFDIAs, in which the attacker executes a single coordinated manipulation without considering sequential, interdependent actions. In reality, an attacker could adopt a more sophisticated strategy by executing the attack over multiple steps, gradually adapting to system responses and amplifying the cumulative impact. Despite this increased risk, the vulnerability of power systems to such multi-step SFDIAs has not been systematically explored.

Although multi-step strategies have been investigated in the context of topology attacks, these approaches cannot be directly applied to multi-step SFDIAs because of fundamental differences in their mechanisms and impacts. First, operators' decisions during topology attacks are based on genuine system measurements, while multi-step SFDIAs exploit manipulated data to influence those decisions. Second, topology attacks typically cause immediate line tripping, whereas multi-step SFDIAs progressively overload lines by leveraging delayed system responses, such as generator ramping constraints. Third, in multi-step SFDIAs, previously tripped lines might be restored in later stages, reflecting a fundamentally different and more dynamic attack progression. Although one study [63] has addressed multi-step SFDIAs, it does not explicitly aim to maximize the cumulative impact across multiple steps, instead treating each step as an independent single-step attack. Furthermore, it does not consider uncertainties, such as the possible restoration of previously tripped lines.

Based on the above review, there is a clear research gap in methods for assessing the vulnerability of power systems to forward-looking multi-step SFDIAs, in which attackers strategically plan sequential actions to maximize their cumulative impact. These attacks, despite requiring no additional access compared to single-step strategies, can present substantial challenges to traditional security assessments. To address these gaps, this chapter develops a vulnerability assessment framework that leverages a MDP to model the sequential decision-making of attackers and quantify the impacts of multi-step SFDIAs. In this framework, each MDP state encodes information about demand, generation, and the system admittance matrix, and reflects the effects of previous actions, including the restoration of tripped lines. At each stage, the attacker's action — that is, a one-step SFDIA maximizing the power flow on a targeted line — is obtained by solving a bi-level optimization problem. The reward function is defined based on the resulting system impact, including load shedding, unused generation capacity, and proximity to operational limits. The MDP is solved using a Q-learning algorithm to derive a vulnerability index that supports op-

erators in evaluating the multi-step SFDIA impact and in identifying the attacker's most critical actions at each step.

On this basis, the chapter is organized as follows. Section 2.1 reviews the fundamental operating principles of SE and BDD and explains how bad-data detection mechanisms can be bypassed to design SFDIAs that manipulate state estimation results. Section 2.2 examines bi-level optimization models commonly used to evaluate the vulnerability of power systems to SFDIAs. Section 2.3 provides a concise introduction to MDPs and the Q-learning algorithm, which serve as the theoretical foundation for the proposed methodology. Section 2.4 presents the MDP-based vulnerability assessment framework and explains how the Q-learning algorithm is employed to derive a vulnerability index to support operator decision-making. Section 2.5 presents a case study demonstrating the impact of multi-step SFDIAs on the power system and compares these effects with those of single-step SFDIAs. It then evaluates the performance of the proposed framework using simulation studies on the IEEE 39-bus and 57-bus test systems. Finally, Section 2.6 summarizes the key findings and concludes the chapter.

2.1 Stealthy FDIAs against SE

SE estimates the state of a system, i.e., the voltage magnitude and phase angle of each bus, based on measurements collected throughout the grid. This process is performed by solving the following least-squares problem:

$$\underset{\hat{x}}{\text{Minimize}} \ \|Z - h(\hat{x})\| \tag{2.1}$$

where $\hat{x}$ denotes the estimated states, Z represents the measurement vector, and $h(\hat{x})$ is a set of nonlinear functions that relate the states to the measurements. SE is often supported with a BDD module to detect faulty measurements. This module in current power systems operates based on a residual vector — i.e., the error between the actual measurements and calculated ones — defined as follows:

$$RE = Z - h(\hat{x}) \tag{2.2}$$

where RE is the residual vector. Bad data, e.g., attacked or erroneous measurements, are then detected if the norm of the residual vector exceeds a predefined threshold, i.e.,

$$\| \ Z - h(\hat{x}) \ \| \geq \tau \tag{2.3}$$

where τ is the detection threshold. To craft a stealthy FDIA, the attack vector Z_A should be designed such that the BDD module is bypassed, that is

$$\|Z + Z_A - h(\hat{x} + \Delta\hat{x})\| \leq \tau \tag{2.4}$$

where $\Delta\hat{x}$ denotes the deviation of the states from their actual values after injecting Z_A in the actual measurements. Thus, using (2.3) and (2.4), the FDIA remains stealthy if

$$Z_A = h(\hat{x} + \Delta\hat{x}) - h(\hat{x}) \tag{2.5}$$

As (2.5) shows, if an attacker wishes to alter a certain state variable by targeting SE, all the measurements dependent on the target state variable must be manipulated.

To eliminate the nonlinear relationships between measurements and state variables, i.e., a nonlinear $h(.)$ vector, SE is commonly linearized using DC power flow assumptions. These assume negligible line resistance, fix all bus voltage magnitudes at 1 p.u., and restrict voltage angle differences between connected buses to small values. Under these conditions, active power flows depend only on bus voltage phase angles and line reactances. Shunt capacitance is completely ignored because reactive power flows and voltage magnitude variations are not modeled. Series capacitance is not represented explicitly; instead, its effect is incorporated indirectly by reducing the net series reactance of the line. These simplifications reduce the state vector to bus voltage phase angles only and yield a constant-coefficient linear measurement model, allowing the state estimate to be obtained in a single weighted least squares step rather than through the iterative nonlinear solvers required in AC SE.

The DC form of SE is widely utilized by system operators due to its low computational complexity and acceptable accuracy [101]. Moreover, as shown in [54, 41], DC SE maintains sufficient accuracy for analyzing the vulnerabilities of power grids and defending against FDIAs. Using (2.5), the requirements for stealthy FDIAs (2.5) in DC SE can be expressed as:

$$Z_A = H(\hat{\theta} + \Delta\hat{\theta}) - H(\hat{\theta}) = H\left(\Delta\hat{\theta}\right) \tag{2.6}$$

where H is a linear matrix representing the dependencies between measurements and state variables in DC state estimation. Here, $\hat{\theta}$ denotes the estimated voltage phase angles, which, in the DC model, represent the complete system state since voltage magnitudes are assumed to be 1 p.u. at all buses. The term $\Delta\hat{\theta}$ denotes the change in these voltage angles caused by the attack.

An equivalent form of the stealthiness constraint in (2.6), which eliminates the explicit

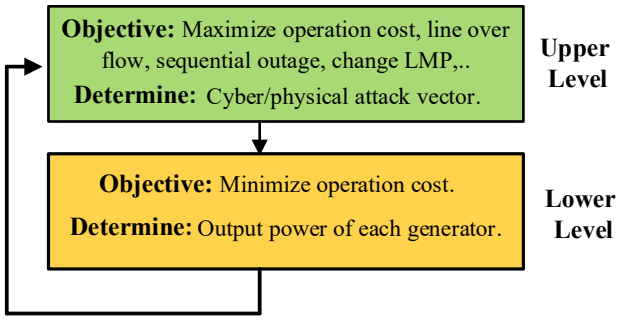


Figure 2.1: The bi-level optimization framework for modeling SFDIAs.

dependence on $\Delta\hat{\theta}$, can be derived as follows [62]. Let

$$\Upsilon = H(H^T H)^{-1} H^T. \tag{2.7}$$

It is straightforward to verify that $\Upsilon H = H$. By multiplying Υ on both sides of the relation $Z_A = H(\Delta\hat{\theta})$, a sequence of equivalent forms is obtained [62]:

$$\begin{aligned} & Z_A = H(\Delta\hat{\theta}) \\ & \Leftrightarrow \Upsilon Z_A = \Upsilon H(\Delta\hat{\theta}) \Leftrightarrow \Upsilon Z_A = H(\Delta\hat{\theta}) \Leftrightarrow \Upsilon Z_A = Z_A \\ & \Leftrightarrow \Upsilon Z_A - Z_A = 0 \Leftrightarrow (\Upsilon - I) Z_A = 0 \\ & \Leftrightarrow \left(H(H^T H)^{-1} H^T - I\right) Z_A = 0. \end{aligned} \tag{2.8}$$

This demonstrates that any vector Z_A satisfying $Z_A = H(\Delta\hat{\theta})$ must also satisfy the equivalent constraint

$$\left(H(H^T H)^{-1} H^T - I\right) Z_A = 0. \tag{2.9}$$

2.2 Bi-level Optimization

This section presents a general bi-level optimization model commonly used to evaluate power system vulnerabilities to SFDIAs, as illustrated in Fig. 2.1. This bi-level framework quantifies the maximum potential impact that FDIA can inflict on the system [99, 94, 58, 44, 28, 54, 21]. The upper level represents the attacker's objectives and constraints, while the lower level models the operator's response through an OPF formulation. The attacker's objective may involve economic damage, such as increasing operational costs

or manipulating Locational Marginal Prices (LMPs), as well as physical damage, such as overloading transmission lines. Given the critical importance of potential physical damage to the grid, this section focuses on the attacker's objective of maximizing power flow on a targeted transmission line. Accordingly, the objective of the upper-level optimization is formulated as

$$\underset{Z_A^l:\, Z_{A|K}^l, Z_{A|D}^l}{\text{Maximize}} \quad PL(l) = SF_l \cdot (BG \cdot PG - BL \cdot PD) \tag{2.10}$$

where $PL(l)$ denotes the power flow through line l, which the attacker aims to maximize in order to overload the line. Here, SF_l is the shift factor vector corresponding to line l, which quantifies how bus injections impact flows on that line; BG is the bus-generator incidence matrix describing generator-to-bus connections; PG is the vector of generator dispatch levels; BL is the bus-load incidence matrix; and PD is the vector of load demands. The decision variable Z_A^l represents the attack vector injected into the system measurements to maximize the power flow in line l. This vector is divided into two sub-vectors: $Z_{A|K}^l$ and $Z_{A|D}^l$, representing data injected into line measurements and load measurements for overloading line l, respectively. The elements of these sub-vectors are denoted by $z_{a|k}^l$ and $z_{a|d}^l$.

To preserve stealth, the attacker is subject to the following constraints.

First, the stealth constraint is formulated as

$$\left(H(H^T H)^{-1} H^T - I\right) Z_A^l = 0 \tag{2.11}$$

which ensures that the injected attack vector bypasses the BDD module of the state estimator, as demonstrated in Section 2.1.

Second, the load preservation constraint:

$$\sum_{d \in \mathcal{D}} z_{a|d}^l = 0 \tag{2.12}$$

guarantees that the total measured load across the system remains consistent, even if loads are redistributed, thereby maintaining stealth. This helps maintain stealth, since only load measurements are modified while generator measurements — which are more easily monitored and harder to falsify — remain untouched.

Third, a bound on load measurement manipulations:

$$-\sigma P_d \leq z_{a|d}^l \leq \sigma P_d \quad \forall d \in \mathcal{D} \tag{2.13}$$

which limits the magnitude of manipulation on load measurements. Here, σ denotes the maximum proportion of allowable change relative to the actual demand P_d.

Fourth, a bound on line measurement manipulations:

$$-\eta \leq z^l_{a|k} \leq \eta \quad \forall l \in \mathcal{L} \tag{2.14}$$

which limits the attack on line measurements, with η defining the absolute maximum permitted change.

Together, these upper-level constraints ensure the attacker's data modifications remain sufficiently small and consistent to evade BDD module while still achieving the objective of maximizing line flows.

On the other hand, the lower-level problem models the operator's corrective actions through an OPF to minimize costs. Its objective is given by

$$\underset{P_G, S_D}{\text{Minimize}} \quad \sum_{g \in \mathcal{G}} c_g P_g + \sum_{d \in \mathcal{D}} cs_d S_d \tag{2.15}$$

where c_g and P_g are associated with generator $g \in \mathcal{G}$, representing the unit generation cost (\$/MW) and its active power output, respectively; and cs_d and S_d are associated with load $d \in \mathcal{D}$, denoting the unit load-shedding cost and the curtailed demand at bus d, respectively. The first term models the total generation cost incurred to supply the active power demand, whereas the second term captures the cost associated with load shedding when curtailments are required.

The lower-level problem is subject to the following constraints.

First, the nodal power balance:

$$\sum_{g \in \mathcal{G}} BG_{j,g}\, P_g = \sum_{i \in \mathcal{B}} Y_{j,i}\, \theta_i + \sum_{d \in \mathcal{D}} BL_{j,d} \left(P_d - S_d + Z^l_{A|D}\right) \forall j \in \mathcal{B} \tag{2.16}$$

which ensures that total injections equal total withdrawals at each bus $j \in \mathcal{B}$. Here, $BG_{j,g}$ represents the element of the bus-generator incidence matrix BG, which indicates whether generator g is connected to bus j, and $BL_{j,d}$ denotes the element of the bus-load incidence matrix BL, indicating whether load d is connected to bus j. The term $Y_{j,i}$ is the admittance between buses j and i, drawn from the network admittance matrix Y, and θ_i is the voltage phase angle at bus i.

Second, transmission line flow limits:

$$-P_l^{\max} \leq SF_l \left(BG \cdot PG - BL \cdot (PD + Z^l_{A|D})\right) \leq P_l^{\max} \quad \forall l \in \mathcal{L} \tag{2.17}$$

which ensures that the power flow on each transmission line $l \in \mathcal{L}$ does not exceed its thermal capacity, denoted by $P_l^{\max}$.

Third, generator capacity limits are enforced as

$$P_g^{\min} \leq P_g \leq P_g^{\max} \quad \forall g \in \mathcal{G} \tag{2.18}$$

which ensure that each generator operates within its permissible active power range. Here, $P_g^{\min}$ and $P_g^{\max}$ denote the minimum and maximum active power ratings of generator g, respectively.

Fourth, load shedding is limited to the actual demand:

$$S_d \leq P_d \quad \forall d \in \mathcal{D} \tag{2.19}$$

Fifth, generator ramp rate constraints are enforced as

$$P_g \geq \max\left\{P_g^0 - M_g T_h, P_g^{\min}\right\} \quad \forall g \in \mathcal{G} \tag{2.20}$$

$$P_g \leq \min\left\{P_g^0 + M_g T_h, P_g^{\max}\right\} \quad \forall g \in \mathcal{G} \tag{2.21}$$

which ensure that generator outputs respect their ramping capabilities. Here, P_g^0 denotes the previous dispatch level of generator g, M_g is its ramp rate limit in MW per unit time, and T_h is the look-ahead OPF time horizon.

To solve this bi-level optimization problem, the lower-level problem is equivalently represented by its Karush–Kuhn–Tucker (KKT) optimality conditions, which are then incorporated into the upper-level problem. Using this approach, the attacker's and operator's decision processes are merged into a single-level problem with the same objective as the attacker. The only source of nonlinearity in the KKT conditions lies in the complementary slackness relations, which involve the product of a dual variable and its associated constraint function. These are linearized using the Fortuny-Amat and McCarl approach [35], which introduces binary variables and applies the Big-M technique to reformulate each complementarity condition as a set of linear inequalities. In this formulation, the Big-M constant serves as a sufficiently large upper bound that enforces logical consistency: when a constraint is inactive, the associated dual variable is forced to zero; when the constraint is active, the dual variable is permitted to take a positive value. As a result, the combined

attacker–operator bi-level problem is reformulated as a single-level Mixed-Integer Linear Programming (MILP) and can be efficiently solved using standard optimization solvers such as CPLEX.

2.3 Markov Decision Process

A discrete-time MDP is defined by a 5-tuple (S, A, T, R, γ) that frames the decision-making landscape. S represents a finite set of states where each state $s_t \in S$ encapsulates a possible scenario or condition of the system at time t. A is a finite set of actions, where $a_t \in A$ is a possible action that can be performed at state s_t. Transition probabilities $T(s_{t+1} \mid s_t, a_t)$ dictate the likelihood of moving from state s_t to a new state s_{t+1} following action a_t. The reward function $R(s_{t+1} \mid s_t, a_t)$ represents the reward for transitioning from state s_t to s_{t+1} with action a_t. This function quantifies the immediate benefit derived from taking a particular action in a particular state at time t. Lastly, the discount factor γ, which varies between 0 and 1, balances the priority between immediate and future rewards [25].

The objective of an MDP is to identify the optimal policy, π^*, which determines the best action at each state to maximize the expected reward. To solve the MDP, a model-free algorithm such as Q-learning can be utilized. Q-learning, which is a type of reinforcement learning, interacts directly with the environment and continuously updates its strategy based on the feedback received (Fig. 2.2). Q-learning does not require a predefined model of the environment, making it ideal for this problem, where the system is uncertain and dynamics are complex. By executing actions and observing the resulting rewards and state transitions, Q-learning incrementally refines its action-value function $Q(s_t, a_t)$, which predicts the expected utility of taking action a_t in state s_t, thereby improving the decision-making process over time. The Q-values are iteratively updated according to the following rule:

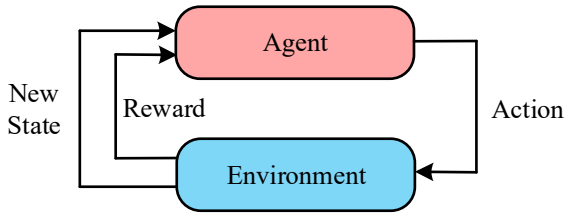


Figure 2.2: Schematic of the reinforcement learning process.

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \left[R(s_t, a_t, s_{t+1}) + \gamma \max_{a_{t+1}} Q(s_{t+1}, a_{t+1}) - Q(s_t, a_t) \right] \tag{2.22}$$

where α is the learning rate, and $\max_{a_{t+1}} Q(s_{t+1}, a_{t+1})$ represents the highest Q-value achievable from the new state s_{t+1}. This update is performed iteratively for each state-action pair experienced, converging to the optimal action-value function $Q^*(s_t, a_t)$ as more updates are applied. Upon convergence, the optimal policy can be derived simply by selecting the action that maximizes the Q-value in each state [25]:

$$\pi^*(s_t) = \arg\max_{a_t \in A} Q^*(s_t, a_t) \tag{2.23}$$

Once the optimal action-value functions are obtained for state s_t, the value function $V(s_t)$ for this state, which represents the maximum expected reward for being in state s_t and following the optimal policy, can be obtained using the following equation

$$V(s_t) = \max_{a_t \in A} Q^*(s_t, a_t), \tag{2.24}$$

indicating that $V(s_t)$ is the maximum Q-value over all actions a_t at state s_t.

2.4 Proposed Framework for Assessing the Impacts of Multi-step SFDIAs on Power Grids

This section delves into the structure of the proposed framework (Fig. 2.3) designed for analyzing the impacts of multi-step SFDIAs. The framework utilizes an MDP to provide a structured approach for analyzing sequential decision-making in the context of multi-step SFDIAs. Within this MDP, each decision or action is an attack vector that overloads a line in the power system, determined by solving a bi-level optimization problem. Since the impacts of SFDIAs depend entirely on the system's response to altered data—calculated through OPF—the decision intervals of the proposed MDP align with the intervals at which the operator computes the OPF solutions. Specifically, at each time interval, the attacker selects an action (i.e., an attack vector) by solving a bi-level optimization problem, which yields the corresponding generation dispatch and load shedding vectors. Moreover, using the obtained vectors and the probabilities of line restoration, the system topology is updated accordingly, and the admittance matrix is revised to reflect the new network

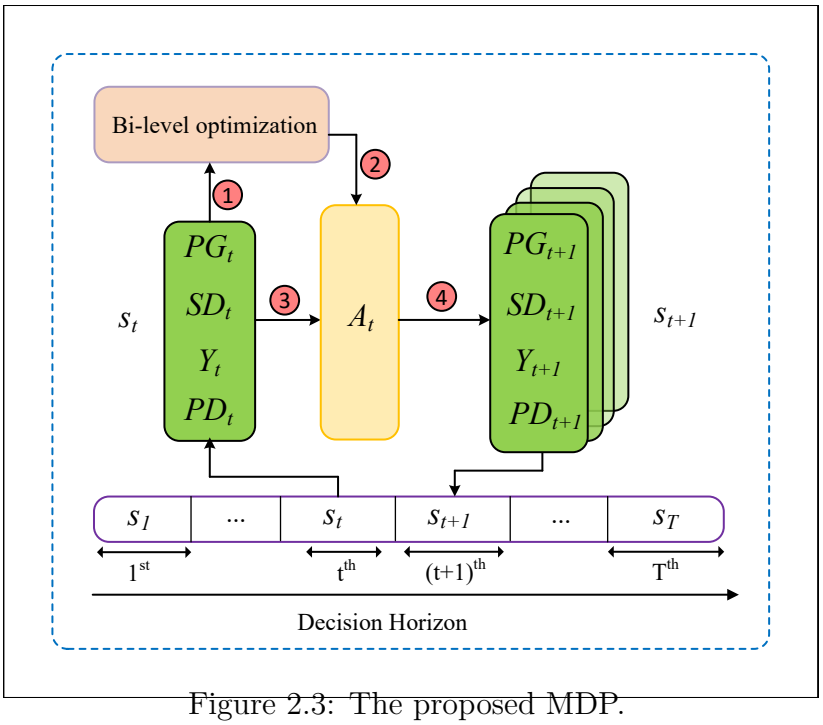


Figure 2.3: The proposed MDP.

configuration. Based on this process, the MDP structure, including its states, actions, and other essential elements, is detailed as follows:

2.4.1 States

In the MDP model, at any given time step $t = \{1, ..., T\}$, the state of a system is represented as follows:

$$s_t = \left[PG_t,\ SD_t,\ PD_t,\ Y_t\right] \tag{2.25}$$

where T is the decision horizon of the MDP, PG_t is the vector of power generation, SD_t is the vector of load shed, PD_t is the vector of load demand, and Y_t is the admittance matrix of the power system, all at time t. The admittance matrix Y_t is an important component of s_t, as it may change in response to line tripping caused by SFDIAs or the subsequent recovery from previous tripping.

It is noteworthy that the load demand vector PD_t is independent of the MDP's internal dynamics, as it is assigned based on actual demand at the initial step and forecasted values for subsequent steps.

2.4.2 Actions

The set of available actions A_t at time step t directly corresponds to the set of in-service transmission lines $\mathcal{L}_t$, as determined by the Y_t component of s_t. Each action $a_t^l \in A_t$ encompasses an attack vector, i.e., $Z_{A|D}^l$, which can overload line l at state s_t. The attack vectors can be calculated by solving a bi-level optimization problem, as explained in Section 2.2. The mathematical representation of actions is as follows:

$$A_t = \{a_t^l = Z_{A|D}^l \mid l \in \mathcal{L}_t\} \tag{2.26}$$

2.4.3 Transition Probabilities

In the developed MDP, the state transition from s_t to s_{t+1} following action a_t^l involves deterministic components, such as power generation and load shedding, as well as the network configuration, which is probabilistic. The load demand in the next time step PD_{t+1} is often known and available with good accuracy. Additionally, for a given state s_t and action a_t^l, the power generation PG_{t+1} and load shed SD_{t+1} can be calculated by solving the OPF problem, as detailed in (2.15)–(2.21). In this optimization, the initial power generation PG^0 is set to PG_t, and the attack vector $z_{a|d}^l$ is the action a_t^l.

The transition probability of the admittance matrix depends on the effectiveness of action a_t in overloading line l at s_{t+1} and the probability of restoring the previously tripped line r at s_{t+1}. The transition probability for the admittance matrix can be defined as follows:

$$T(Y_{t+1}|Y_t, a_t^l) = \begin{cases} \mathcal{P}_S \cdot \mathcal{P}_R(t_{lost}) & \text{if } Y_{t+1} = Y_t^{l,r} \\ \mathcal{P}_S \cdot (1 - \mathcal{P}_R(t_{lost})) & \text{if } Y_{t+1} = Y_t^{l} \\ (1 - \mathcal{P}_S) \cdot \mathcal{P}_R(t_{lost}) & \text{if } Y_{t+1} = Y_t^{r} \\ (1 - \mathcal{P}_S) \cdot (1 - \mathcal{P}_R(t_{lost})) & \text{if } Y_{t+1} = Y_t \end{cases} \tag{2.27}$$

where $Y_t^{l,r}$, Y_t^l, and Y_t^r are the admittance matrices of the system at time t under different conditions: $Y_t^{l,r}$ is the admittance matrix after tripping line l and recovering line r; Y_t^l is the admittance matrix after tripping line l; and Y_t^r is the admittance matrix after recovering line r, respectively. Additionally, $\mathcal{P}_R(t_{lost})$ represents the probability of restoring a previously tripped line during t_{lost}, which is the period during which the line is out of service. Moreover, $\mathcal{P}_S$ denotes the probability that action a_t increases the load on line l to the point of tripping this line. These probabilities are functions of the extent of the overload caused by action a_t, and are defined as follows:

$$\mathcal{P}_S = F\left(\frac{PL_{t+1}(l)}{P_l^{max}}\right) \tag{2.28}$$

where F is the probability function that gives the likelihood of line l tripping based on the ratio of its power flow, i.e., $PL_{t+1}(l)$, to its maximum capacity $P_l^{\max}$. The term $PL_{t+1}(l)$ can be calculated using:

$$PL_{t+1}(l) = SF_l \cdot (BG \cdot PG_{_{t+1}} - BL \cdot PD_{t+1}) \tag{2.29}$$

As discussed in Section 2.5.2, NERC Standard PRC-023-1 recommends setting the tripping threshold for protective devices of power lines and transformers at at least 150% of their maximum capacity [5]. Accordingly, this paper adopts 150% as the pickup threshold for relays [28, 27]. Consequently, function F can be defined as a step function, where it equals 1 when the ratio exceeds 1.5 and 0 when it is below 1.5.

2.4.4 Reward

The reward function of the MDP model is crucial for accurately quantifying the impacts of SFDIAs. Typically, the impact of losing a transmission line is measured by the amount of unserved load or required load shedding. Besides the impact on loads, losing a line can also lead to the loss of generators. Although this event might not directly affect the loads, it can result in significant economic losses, increased pressure on other generators, and a reduced safety margin due to the increased contribution from the remaining generators [8].

Based on the above-mentioned potential impacts, this paper defines the reward function as follows:

$$R(s_t, a_t, s_{t+1}) = RF(s_{t+1}) - RF(s_t) \tag{2.30}$$

where

$$RF(s_t) = \beta_1 \sum_{d\in\mathcal{D}} S_{d,t} - \beta_2 \sum_{g\in\mathcal{G}} C_{g,t} + \beta_3 \sum_{d\in\mathcal{D}} \sum_{k\in\theta^d} \max\left(0, 1 - \frac{\sum_{l\in\theta^d, l\neq k} P_l^{max}}{P_{d,t}}\right) \times P_{d,t} \tag{2.31}$$

where θ^d represents the set of transmission lines connected to load d. In this equation, the first term represents the total unserved load, the second term represents the available generation capacity, and the third term quantifies system operational margin [8]. The coefficients β_1, β_2, and β_3 determine the relative importance of each term in the reward.

Algorithm 1 Dynamic Q-learning for Solving the MDP

Initialize a dynamic structure for the Q-table and the system benchmark
for episode = 1 to M **do**
  Get initial state s_1.
  for time step $t = 1$ to T **do**
    Obtain the set of in-service lines $\mathcal{L}_t$ and solve the bi-level optimization problem (2.10) to derive the set A_t.
    If (s_t, a_t^l) is not in Q table, initialize $Q(s_t, a_t^l)$ for all $a_t^l \in A_t$ to a default value (e.g., 0).
    Select an action a_t^l from A_t
    Execute action a_t^l, which determines the deterministic elements of s_{t+1}.
    Determine the transition probabilities $\mathcal{P}_R(t_{lost})$ based on the t_{lost}, $\mathcal{P}_S$ based on (2.28).
    Assign Y_{t+1}, by selecting scenarios according to the transition probabilities $\mathcal{P}_S$, and $\mathcal{P}_R(t_{lost})$.
    Calculate the reward $R(s_t, a_t^l, s_{t+1})$ based on (2.31).
    Update Q-table dynamically:

$$Q(s_t, a_t^l) \leftarrow Q(s_t, a_t^l) + \alpha\Big[R(s_t, a_t^l, s_{t+1}) + \gamma \max_{a_{t+1}^l \in A_{t+1}} Q(s_{t+1}, a_{t+1}^l) - Q(s_t, a_t^l)\Big]$$

  end for
end for

2.4.5 Dynamic Q-Learning for Solving MDP

Dynamic Q-learning is employed to solve the developed MDP due to its capability to effectively handle the extensive and uncertain state space inherent in power system operation. This method dynamically adapts by creating Q-table entries only for state-action pairs as they are encountered, thus avoiding the computational impracticality of initializing a complete Q-table for the vast number of possible states. This makes the framework more scalable and memory-efficient.

Algorithm 1 details the dynamic Q-learning process for solving the proposed MDP. Following initialization, the algorithm iterates over M episodes. In each episode, the initial state s_1 of the power system is its current state. Within each episode, for every time step from 1 to T, the algorithm follows a structured sequence of operations. It begins by identifying in-service power lines and solving a bi-level optimization problem to

determine viable actions A_t. If the state-action pair (s_t, a_t^l) is not already in the Q-table, it is initialized. An action a_t^l is then selected from A_t using the ϵ-greedy policy [84], which balances exploration and exploitation based on the Q-values. This action is executed to determine the deterministic elements of the next state s_{t+1}. Then, the algorithm calculates the probabilities $\mathcal{P}_S$ and $\mathcal{P}_R(t_{lost})$. Afterwards, the algorithm chooses Y_{t+1} based on $\mathcal{P}_S$ and $\mathcal{P}_R(t_{lost})$ using (2.27). The reward for the transition from s_t to s_{t+1} using the selected action a_t^l is calculated by (2.31), and the Q-table is updated using (2.22).

When the optimal Q-value function $Q^*(s_t, a_t^l)$ is obtained using this algorithm, the operator can determine the next step of the most critical multi-step SFDIA by using (2.23). Moreover, the vulnerability index, which quantifies the potential impact of the SFDIA at the current state, is derived from (2.24). This is because the maximum Q-value at a given state s reflects the highest expected cumulative impact that can be inflicted starting from that state. As such, the maximum Q-value serves as a meaningful indicator of the system's vulnerability to multi-step SFDIAs.

2.5 Simulation Results

This section first introduces the test systems (i.e., the IEEE 39-bus and 57-bus test systems) used to illustrate the impact of multi-step SFDIAs and to demonstrate the effectiveness of the proposed framework. It then presents a case study on the IEEE 39-bus test system, demonstrating the impact of multi-step SFDIAs and comparing their effects with those of single-step SFDIAs. Finally, it illustrates the effectiveness of the proposed MDP framework in assessing the impact of multi-step SFDIAs on power grids through case studies conducted on both the IEEE 39-bus and 57-bus test systems.

2.5.1 Test Systems

IEEE 39-Bus Test System

Figure 2.4 depicts the IEEE 39-bus system, which includes 10 generators and 46 transmission lines. Generator specifications are provided in Table 2.1. Configuration data, such as the admittance matrix, are taken from the MATPOWER toolbox [102].

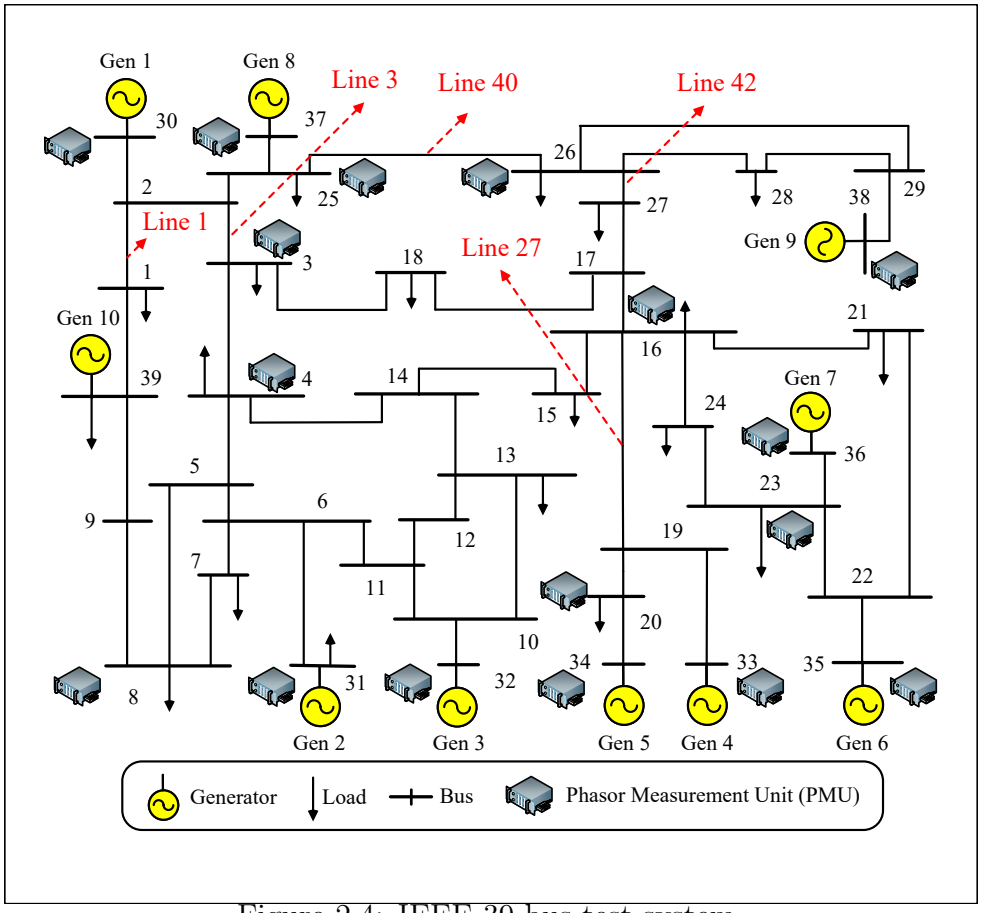


Figure 2.4: IEEE 39-bus test system.

IEEE 57-Bus Test System

Figure 2.5 shows the IEEE 57-bus system, composed of 7 generators and 80 transmission lines. Generator details are summarized in Table 2.2, with system parameters sourced from MATPOWER [102].

2.5.2 Impacts of Multi-step SFDIAs: A Simple Case Study

The IEEE 39-bus system shown in Fig. 2.4 is employed in this paper as the primary platform for assessing the impacts of SFDIAs on the system. Given that NERC Standard PRC-023-1 recommends setting the tripping threshold for protective devices of power lines and transformers at least at 150% of their maximum capacity [5], this paper chooses 150% as the pickup threshold for relays [28, 27]. In practice, however, this threshold might

Table 2.1: Generators specifications for IEEE 39-bus

Gen #	Gen 1	Gen 2	Gen 3	Gen 4	Gen 5
c_g (\$/MW)	10	12	14	16	18
$P_g^{max}(MW)$	900	1000	900	900	900
$P_g^{min}(MW)$	0	0	0	0	0
M_g (MW/Min)	10	10	10	15	20
Gen #	Gen 6	Gen 7	Gen 8	Gen 9	Gen 10
$c_g(\$/MW)$	20	17	15	13	11
$P_g^{max}(MW)$	900	1000	900	1000	1100
$P^{min}(MW)$	0	0	0	0	0
M_g (MW/Min)	30	25	10	10	10

Table 2.2: Generator specifications for the IEEE 57-bus test system

Gen #	Gen 1	Gen 2	Gen 3	Gen 4	Gen 5	Gen 6	Gen 7
c_g (\$/MW)	30	35	40	35	20	35	25
P_g^{max} (MW)	575	100	140	100	550	100	410
P_g^{min} (MW)	0	0	0	0	0	0	0
M_g (MW/min)	15	10	20	20	10	15	10

be lower. For instance, during the 2003 Northwest Blackout, the relays of a transformer tripped it 40 seconds after its power reached 130% of its capacity [2].

This section considers two scenarios as follows:

- **Scenario 1**: The adversary damages the system by injecting false data in multiple steps. In each step, the adversary aims to maximize the impact of the attack in that step without considering the next steps of the attack.
- **Scenario 2**: The adversary employs a forward-looking strategy, meticulously designing each step of the attack to progressively increase the cumulative impact on subsequent steps. In this scenario, the adversary aims to maximize the overall impact of the entire attack.

In both scenarios, the attacker intends to trip as many lines as possible to move the system towards a cascading failure. The attacks are executed stealthily, ensuring that (i) the attack vector is crafted to bypass the BDD module, (ii) manipulation of each measurement does not exceed 50% of its original value, and (iii) only load and line measurements are manipulated, as manipulating generator measurements is easily detectable. Additionally, for

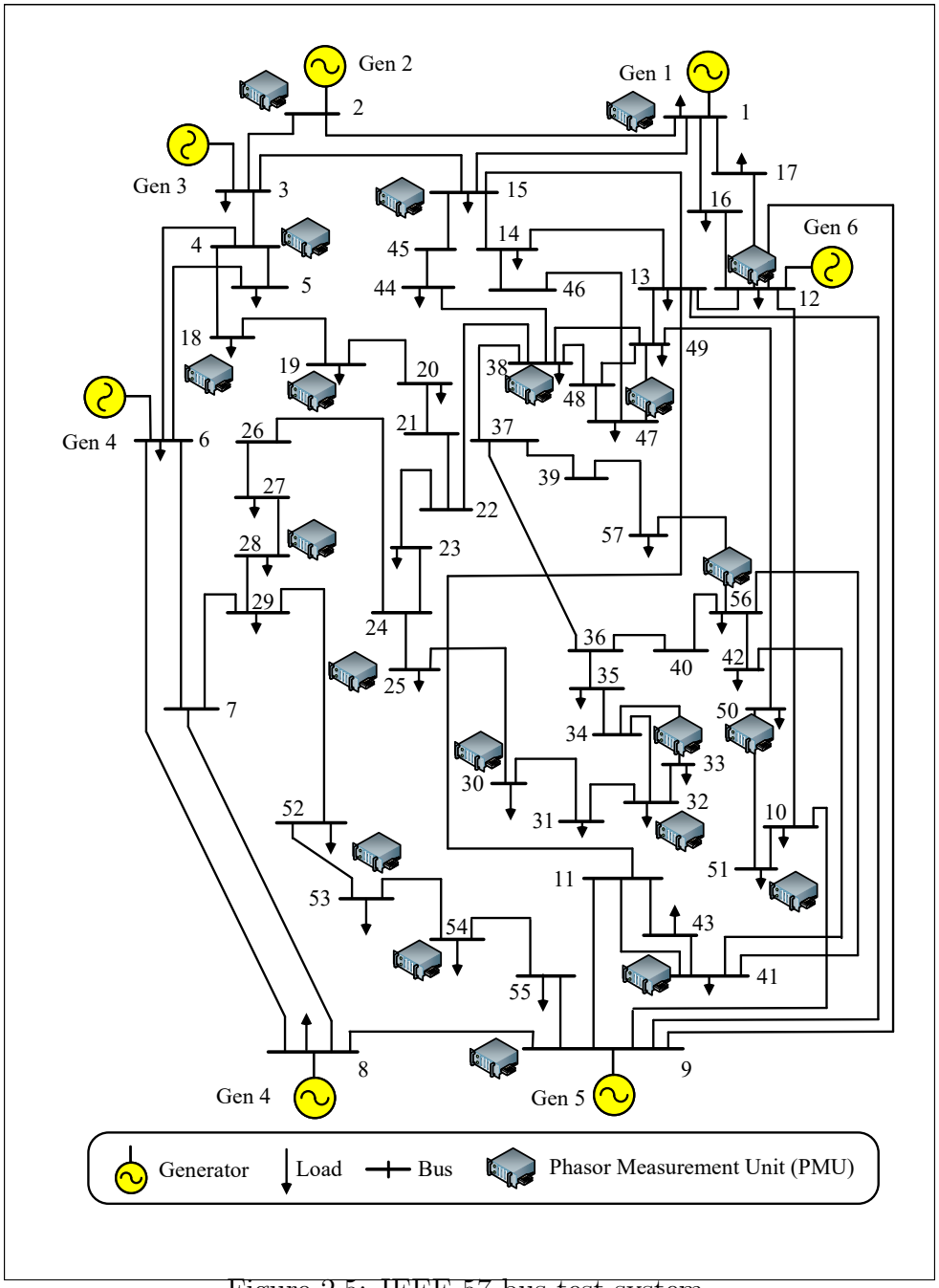


Figure 2.5: IEEE 57-bus test system.

clarity and simplicity in demonstrating the overall concept, these scenarios disregard generator ramp rates, allowing lines to become overloaded and trip before previously tripped

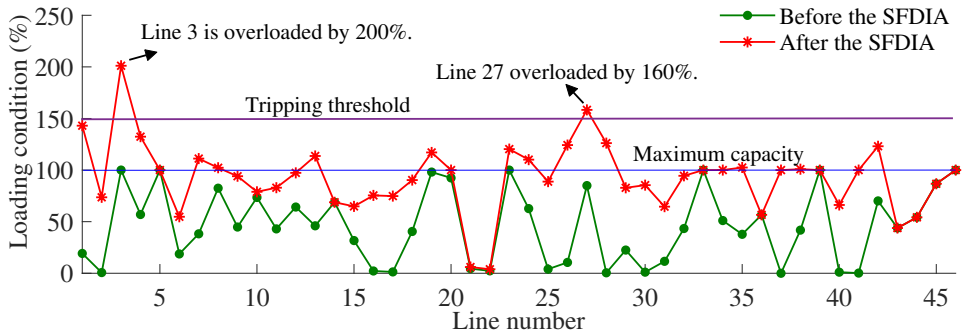


Figure 2.6: Loading condition of each line after injecting its associated attack vector at step 1 of Scenario 1.

lines are restored. This simplification is later relaxed in subsequent sections to enhance the practicality of the attack analysis.

In Scenario 1, the attacker performs a bi-level optimization for each line, as explained in Section 2.2, to find the attack vector that maximizes the power flow of that line through a single-step SFDIA. Fig. 2.6 illustrates the loading condition of each line with respect to its capacity when the attack vectors obtained from the optimizations are injected, and the operator responds accordingly. As this figure shows, the attacker can only increase the flow of Line 3 (between Buses 2 and 3) and Line 27 (between Buses 16 and 19) above the threshold. Given that Line 27 is a major one that connects Generators 4 and 5 to the rest of the system, disconnecting it results in a severe power imbalance in the system. More specifically, after disconnecting Line 27, the region that contains Generators 4 and 5 would experience a surplus of 760 MW, while the remaining system would encounter a corresponding deficit. If the system lacks sufficient capacity to manage this imbalance, load shedding might be required to stabilize the network. In contrast, the loss of Line 3, though impactful, does not result in such a drastic disconnection or severe imbalance. Therefore, in Scenario 1, as the attacker seeks to inflict maximum damage in each step of the attack, they opt to trip Line 27. In the next step of Scenario 1, the attacker runs bi-level optimizations again to find the attack vectors that maximize the power flow of each line after tripping of Line 27. As shown in Fig. 2.7, following the tripping of Line 27, the attacker is unable to trip any other line while maintaining all stealthiness conditions.

On the other hand, if the attacker aims to fulfill the objective outlined in Scenario 2, they should opt to trip Line 3 instead of Line 27. While this action may not cause maximum immediate damage to the system, it strategically sets the stage for more severe damage in subsequent steps. As depicted in Fig. 2.8, following the tripping of Line 3,

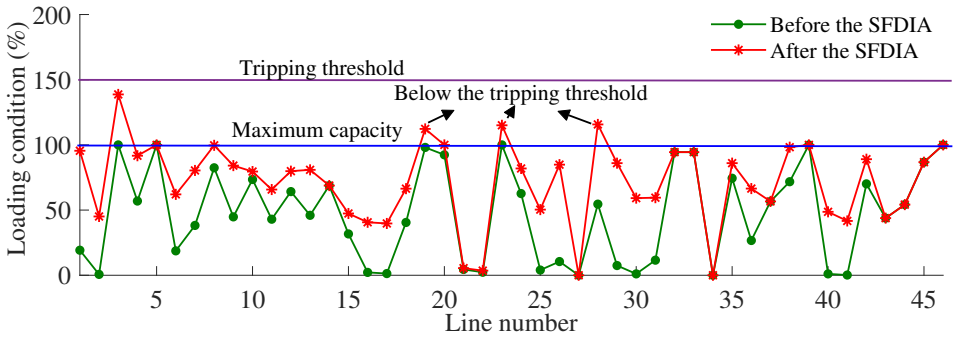


Figure 2.7: Loading condition of each line after injecting its associated attack vector at step 2 of Scenario 1.

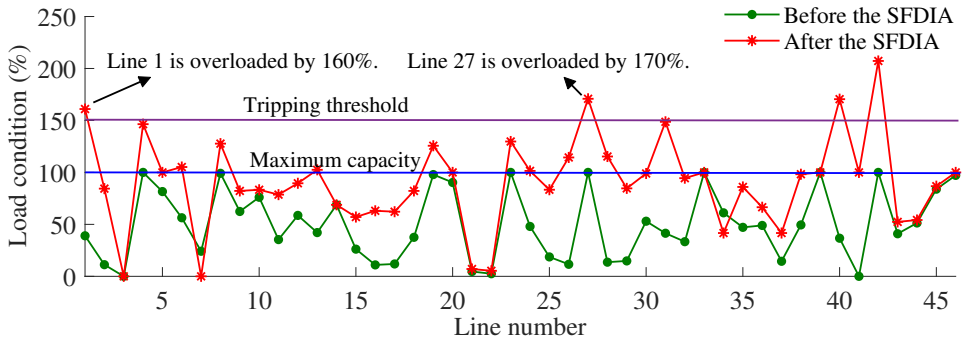


Figure 2.8: Loading condition of each line after injecting its associated attack vector at step 2 of Scenario 2.

Lines 1, 27, 40, and 42 emerge as potential targets for disconnection through an SFDIA in the second step. Notably, Line 27 appears among the potential lines for disconnection, indicating that Scenario 2 not only achieves the objective of Scenario 1 but also surpasses it. To maximize damage within two steps, the attacker may choose to disconnect Line 42 after the loss of Line 3 in the first step. This action would force the operator to shed at least 358 MW to ensure safe system operations.

This simplified case study clearly demonstrates that prioritizing defense mechanisms solely based on the most severe single-step SFDIAs, as suggested in existing literature, may not be adequate. Instead, the defense strategy must also account for multi-step SFDIAs, which have the potential to inflict more severe impacts.

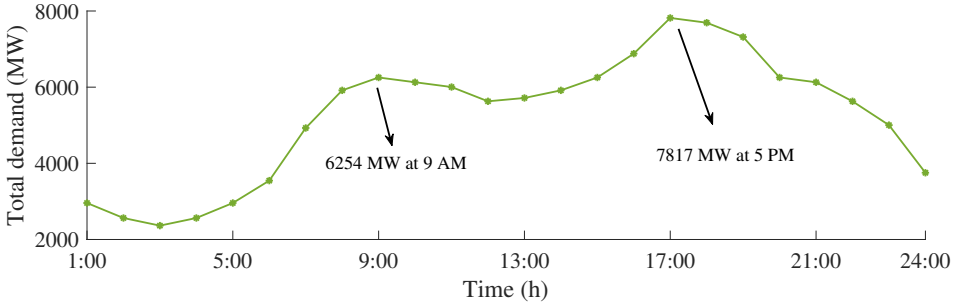


Figure 2.9: The load profile of the test system.

2.5.3 Evaluation of Proposed Framework on IEEE 39-Bus System

This section utilizes the IEEE 39-Bus test system, which was introduced in Section 2.5.1, to evaluate the proposed framework. Fig. 2.9 illustrates the loading profile of the test system. To supply the loads efficiently and reliably, OPF is run every 15 minutes, enabling the system to adapt to the dynamics within the same time frame.

In the next step, the probability of restoring tripped lines, $\mathcal{P}_R(t_{lost})$, should be defined. An exponential distribution is widely used to estimate restoration times of transmission lines affected by physical causes such as weather events, natural disasters, or vegetation interference [45]. In traditional reliability analysis, the restoration rate λ is typically derived from historical outage and repair data, capturing the combined influence of infrastructure conditions, logistics, and workforce availability. In contrast, this study addresses cyber-induced line trips, where coordinated attacks disrupt protective relays. Unlike physical damage, these events generally do not require extensive on-site repairs. Restoration may involve faster actions like software reconfiguration, remote relay resets, or operator interventions. While the exponential model remains applicable, the interpretation of λ shifts—reflecting factors such as system monitoring, automation, cyber-response protocols, and the maturity of detection and mitigation mechanisms. On this basis, the probability of restoring a previously tripped line in this test system is defined as follows:

$$\mathcal{P}_R(t_{\text{lost}}) = 1 - e^{-\lambda \times t_{\text{lost}}} \tag{2.32}$$

where λ is the restoration constant, which depends on the repair capability and the efficiency of the maintenance crew. In fact, the larger the λ, the faster a previously tripped line can be restored.

To develop the proposed framework, the bi-level optimization is solved using General Algebraic Modeling System (GAMS) software. Moreover, the MDP within this framework is modeled in MATLAB, and its decision interval is set equal to the OPF interval. The bi-level optimization not only provides the attack vector but also yields the corresponding generation dispatch and load shedding resulting from the selected attack vector. Thus, starting from the initial state s_1, which is the current operating point of the system, the next state's attack vector and its associated generation and load shedding are determined by the bi-level optimization. This is repeated for all possible states (i.e., all possible line overloads) in step one. Moreover, based on the probabilities of line tripping and restoration, and the initial structure of the power system, the structure of the power system in each new state is determined. Moreover, the loads in the next state are updated based on forecasted values. Consequently, all elements of the new state are determined, and the bi-level optimization can be re-solved to determine the generation dispatch and load shedding for the subsequent states. The developed MDP is solved in MATLAB using the dynamic Q-learning method, which was explained in Section 2.4.5. The most critical multi-step SFDIA for each step and the potential impact of this attack are found using (2.23) and (2.24), respectively, from the optimal Q-action value function $Q^*(s_t, a_t^l)$.

The proposed framework is evaluated using ten distinct scenarios, labeled as Sce1 through Sce10, as detailed in Table 2.3. These scenarios study the effects of various parameters—e.g., λ, γ, α, and weighting factors of the reward function, which are shown in columns 2-7—on the multi-step SFDIAs. The value of λ varies between 0.01 (slow maintenance) and 0.03 (fast maintenance). The value of γ varies between 0.5 (attacker's preference for immediate reward) and 0.9 (attacker's preference for future reward). The weighting factors also vary between 0 (no weight) to 1 (maximum weight). The second-to-last column of this table represents the value function $V(s_1)$, which in this context denotes the maximum expected cumulative reward obtainable by an attacker starting from the initial system state s_1, thereby quantifying the system's vulnerability to multi-step SFDIAs. The final column shows the sequence of actions in the most critical multi-step SFDIA, i.e., the optimal policy $\pi^*(s_t)$, for each scenario. All scenarios are applied to the test system at 9 AM and continue until two Lines are disconnected or the influence of the subsequent rewards falls bellow 5% of their original value due to the discount factor.

In Scenario 1, the maintenance speed is low, the attacker prioritizes the accumulated impact of the attack over its immediate effects, and the operator places the highest importance on minimizing unserved load, while giving low priority to both available generation capacity and stability margin. To evaluate this scenario, the MDP model is developed, with a concise representation illustrated in Fig. 2.10. The initial state of this model, denoted as s_1, comprises the admittance matrix Y_1, generation power vector PG_1, load

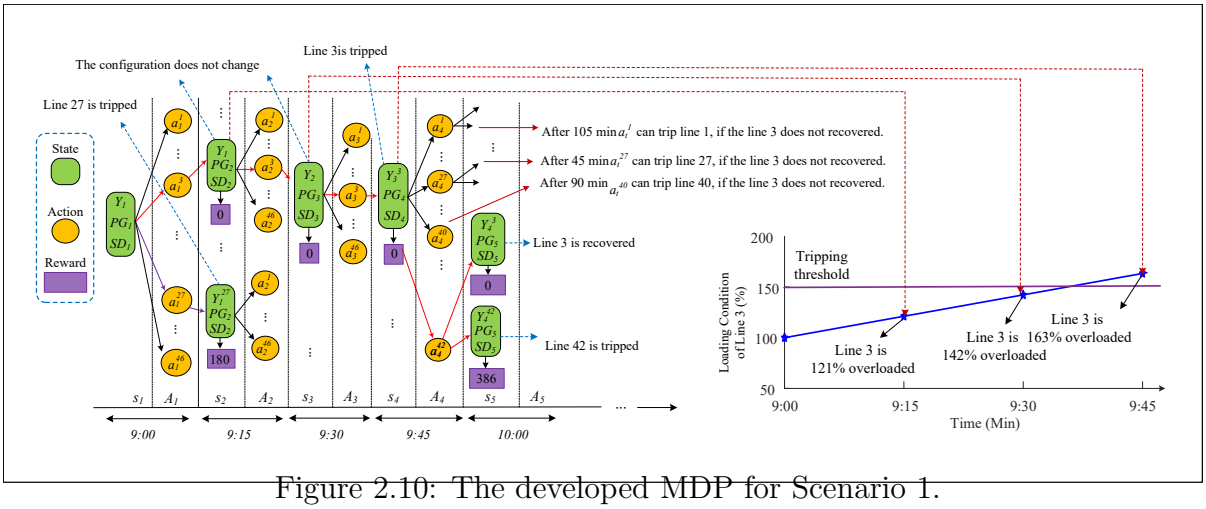


Figure 2.10: The developed MDP for Scenario 1.

shedding vector SD_1, and demand vector PD_1. Given that the demand is a state variable that is independent of the actions, it is not shown in Fig. 2.10. The operator solves the OPF at 9 AM based on this initial state. The set of available actions for the attacker at s_1, denoted as A_1, comprises 46 actions, corresponding to the number of lines in the system. Each $a_1^l \in A_1$ can be utilized by the attacker to influence the OPF solution and overload line l in the system. Considering the ramp rates of generators, only a_1^3 and a_1^{27} can trigger a line outage in the system. Specifically, action a_1^{27} can mislead the OPF into a dispatch that causes the flows on line 27 to reach 160% of its capacity. The reward of this action based on (2.31) is 180. Although a_1^{27} could trip line 27 immediately, no subsequent actions would have an immediate or future impact on the system following this event. On the other hand, action a_1^3 can increase the flow on Line 3 to 121% of its capacity in the next interval, as shown on the right side of Fig. 2.10. Although the immediate impact of this action in the first interval is negligible due to the ramp rate limitation of generators, its subsequent actions, i.e., a_2^3 and a_3^3, can increase the flow of Line 3 to 142% and 163% of its capacity, respectively. Therefore, after three intervals the attacker can overload and disconnect Line 3.

Although the loss of Line 3 does not have an immediate negative impact on the system, i.e., the reward remains zero, the new configuration of the system paves the way for subsequent actions to have more significant impacts. In the fourth interval, only actions a_4^1, a_4^{27}, a_4^{40}, and a_4^{42} can overload and eventually trip Lines 1, 27, 40, and 42 in the system. However, Lines 1, 27, and 40 can be tripped after at least 3 intervals if and only if Line 3 is not restored until then. The reward function for tripping these lines are 7.51, 180, and 28.7, respectively. However, if Line 3 is recovered in the mean time, the above-mentioned lines cannot be tripped anymore. Additionally, action a_4^{42} can increase the flow of Line 42

Table 2.3: Scenario used to evaluate the proposed framework for the IEEE 39-bus system.

Sce	β_1	β_2	β_3	γ	λ	α	$V(s_1)$	$\pi^*(s_t)$
1	1	0.1	0.1	0.9	0.01	0.1	295.7	a_1^3, a_2^3, a_3^3, a_4^{42}
2	1	0.1	0.1	0.9	0.03	0.1	219.1	a_1^3, a_2^3, a_3^3, a_4^{42}
3	1	0.1	0.1	0.5	0.01	0.1	181.7	a_1^{27}, a_2^3, ...
4	1	0.1	0.1	0.5	0.03	0.1	183.8	a_1^{27}, a_2^3, ...
5	0.5	0.1	0	0.9	0.01	0.1	192.1	a_1^{27}, a_2^3, ...
6	0.5	0.1	0	0.9	0.03	0.1	201.3	a_1^{27}, a_2^3, ...
7	1	0	0.2	0.5	0.01	0.1	89.1	a_1^3, a_2^3, a_3^3, a_4^{42}
8	1	0	0.2	0.5	0.03	0.1	65.9	a_1^3, a_2^3, a_3^3, a_4^{42}
9	1	0.1	0.1	0.9	0.01	0.15	295.7	a_1^3, a_2^3, a_3^3, a_4^{42}
10	1	0.1	0.1	0.9	0.01	0.3	Divergence	

beyond 150% 0f its capacity in the next interval if Line 3 remains disconnected, which is very likely since its restoration probability after 15 minutes is almost 14%. The reward function for tripping Line 42 while Line 3 is disconnected is 386. However, if Line 3 is restored, the reward function becomes zero. Therefore, the best course of actions in this scenario are a_1^3, a_2^3, a_3^3, and a_4^{42}, which result in $V(s_1) = 295.7$. This number can be used as a vulnerability index for the operator to quantify the potential impacts of multi-step SFDIAs at the current state of the system.

Scenario 2 maintains consistency with Scenario 1 across all parameters, except for the recovery rate, λ. In this scenario, λ is increased from 0.01 to 0.03 to explore the effect of this parameter on the vulnerability index for multi-step SFDIAs. As Table 2.3 shows, this modification reduces the vulnerability index (or potential impact of the attack) from 295.7 to 219.1 at 9:00 AM. This decrease in the vulnerability index highlights the critical importance of quickly restoring systems and components after malicious activities. To further investigate the impact of this parameter, the vulnerability index of the test system under Scenarios 1 and 2 has been calculated throughout the day, as depicted in Fig. 2.11. As this figure demonstrates, for both scenarios, the vulnerability index is zero from 1 to 7 AM, since the system loading is light and no line can be overloaded. Even if a line is overloaded and tripped, it does not impact the system. Conversely, during peak times, such as from 16:00 to 19:00, the system is highly vulnerable to multi-step SFDIAs, since overloading and tripping lines are easier during these hours, and the impact of losing a line is greater. This figure also reveals that the line recovery rate significantly affects the power system's vulnerability, particularly during peak hours. For instance, at 17:00, increasing

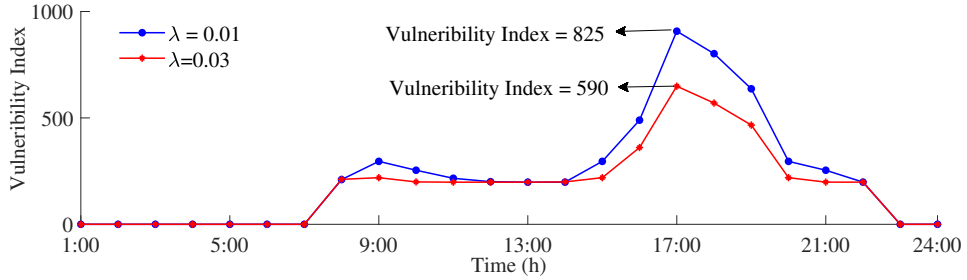


Figure 2.11: The daily vulnerability system to multi-step SFDIAs for the IEEE 39-bus system.

the line recovery rate can reduce the system's vulnerability index from 825 to 590.

In Scenarios 3 and 4, where the discount factor is lower than in Scenarios 1 and 2, the optimal action is to start with a_1^{27}, which has a more immediate impact and yields more immediate rewards compared to other actions. However, after tripping Line 27, no other line can be tripped unless the attacker waits for Line 27 to be restored. During this waiting period, the attacker can increase the flow on Line 3, enabling its immediate tripping once Line 27 is restored. Following this, tripping Line 42 becomes the most critical next action. In fact, these scenarios eventually converge to Scenarios 1 and 2, but with lower vulnerability indices due to the influence of the discount factor. Scenarios 5-8 are developed to study the influence of these coefficients. Comparing Scenario 1 with 5, 2 with 6, 3 with 7, and 4 with 8, as detailed in Table II, demonstrates that the coefficients assigned by the operator to the reward function can significantly alter both the vulnerability index and the steps of the most critical multi-step SFDIA. For example, comparing Scenario 1 with 5 demonstrates that if the operator reduces the coefficient of unserved load, β_1, the steps of the most critical multi-step SFDIA change from a_1^3, a_2^3, a_3^3, a_4^{42} to a_1^{27}, a_2^3.

Additionally, to evaluate the impact of α and assess the sensitivity of the proposed method to this parameter, Scenarios 9 and 10 are used. Comparing Scenario 1 with Scenario 9 shows that increasing α from 0.1 to 0.15 achieves the same results with faster convergence. However, this improvement comes with a higher risk of instability. Further increasing α to 0.3, as in Scenario 10, leads to divergence of the algorithm.

Table 2.4: Scenario used to evaluate the proposed framework for the IEEE 57-bus system.

Sce	β_1	β_2	β_3	γ	λ	α	$V(s_1)$	$\pi^*(s_t)$
1	1	0.1	0.1	0.9	0.01	0.1	80.2	a_1^3, a_2^3, a_3^8, a_4^8
2	1	0.1	0.1	0.9	0.03	0.1	50.8	a_1^3, a_2^3, a_3^8, a_4^8
3	1	0.1	0.1	0.5	0.01	0.1	47.3	a_1^3, a_2^3, a_3^8, a_4^8
4	1	0.1	0.1	0.5	0.03	0.1	46.8	a_1^3, a_2^3, a_3^8, a_4^8
5	0.5	0.1	0	0.9	0.01	0.1	9.3	a_1^{22}, a_2^{22}, a_3^3, ...
6	0.5	0.1	0	0.9	0.03	0.1	9.1	a_1^{22}, a_2^{22}, a_3^3, ...
7	1	0	0.2	0.5	0.01	0.1	150.4	a_1^3, a_2^3, a_3^8, a_4^8
8	1	0	0.2	0.5	0.03	0.1	110.3	a_1^3, a_2^3, a_3^8, a_4^8
9	1	0.1	0.1	0.9	0.01	0.15	80.2	a_1^3, a_2^3, a_3^8, a_4^8
10	1	0.1	0.1	0.9	0.01	0.3	Divergence	

2.5.4 Evaluation of the Proposed Framework on the IEEE 57-Bus System

This section utilizes the IEEE 57-Bus test system, which was introduced in Section 2.5.1, to evaluate the proposed framework. The load profile used for the IEEE 39-bus test system, as shown in Fig. 8, is also applied to this test system. Moreover, the probability of restoration defined in (2.32) is used for this test system as well.

Similar to the previous section, ten different scenarios are defined for this test system, as detailed in Table 2.5. The vulnerability index and best courses of action for these scenarios are also summarized in Table 2.5. For instance, for Scenario 3, the vulnerability index is 47.3, and the best course of action is a_1^3, a_2^3, a_3^8, a_4^8. Moreover, the vulnerability index of the test system under Scenarios 1 and 2, detailed in Table 2.5, has been calculated throughout the day, as depicted in Fig. 2.12. As this figure shows, the power system is highly vulnerable to multi-step SFDIAs, and quickly recovering the tripped lines can reduce the vulnerability of the power system.

2.6 Conclusion

This chapter first established that prioritizing defense mechanisms solely based on the most severe single-step SFDIAs, as suggested by existing literature, may be insufficient. Instead, the defense strategy must also consider multi-step SFDIAs, which can cause more severe impacts. Subsequently, a framework was developed employing MDP and bi-level

Table 2.5: Scenarios used to evaluate the proposed framework for the IEEE 57-bus system.

Sce	β_1	β_2	β_3	γ	λ	α	$V(s_1)$	$\pi^*(s_t)$
1	1	0.1	0.1	0.9	0.01	0.1	80.2	a_1^3, a_2^3, a_3^8, a_4^8
2	1	0.1	0.1	0.9	0.03	0.1	50.8	a_1^3, a_2^3, a_3^8, a_4^8
3	1	0.1	0.1	0.5	0.01	0.1	47.3	a_1^3, a_2^3, a_3^8, a_4^8
4	1	0.1	0.1	0.5	0.03	0.1	46.8	a_1^3, a_2^3, a_3^8, a_4^8
5	0.5	0.1	0	0.9	0.01	0.1	9.3	a_1^{22}, a_2^{22}, a_3^3, ...
6	0.5	0.1	0	0.9	0.03	0.1	9.1	a_1^{22}, a_2^{22}, a_3^3, ...
7	1	0	0.2	0.5	0.01	0.1	150.4	a_1^3, a_2^3, a_3^8, a_4^8
8	1	0	0.2	0.5	0.03	0.1	110.3	a_1^3, a_2^3, a_3^8, a_4^8
9	1	0.1	0.1	0.9	0.01	0.15	80.2	a_1^3, a_2^3, a_3^8, a_4^8
10	1	0.1	0.1	0.9	0.01	0.3	Divergence	

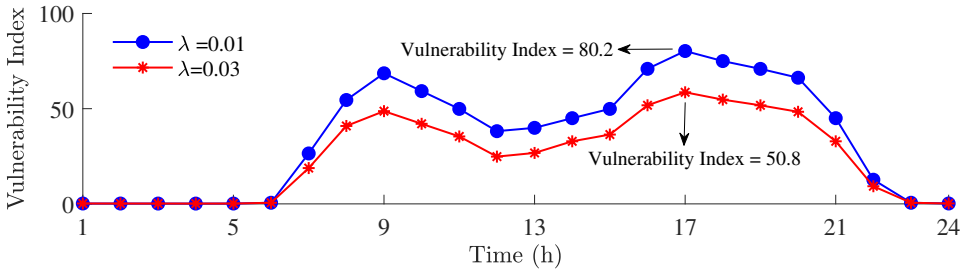


Figure 2.12: The daily vulnerability system to multi-step SFDIAs for the IEEE 57-bus system.

optimization to calculate an index quantifying the system's vulnerability to multi-step SFDIAs. The vulnerability index produced by the proposed framework can serve as a quantitative metric for utilities to weigh the cost of defense investments—such as securing PMUs, enhancing monitoring, or reconfiguring network topology—against the projected consequences of multi-step SFDIAs. Moreover, the proposed framework also identified the most critical action at each step of the attack, aiding the operator in defending against attacks more effectively. Simulation results on the IEEE 39-bus and 57-bus test systems (i) demonstrated the effectiveness of the proposed framework in pinpointing the most critical multi-step SFDIA and the attack vector associated with each step, (ii) underscored the importance of the vulnerability index across different scenarios, and (iii) highlighted the critical role of line recovery rates in mitigating the impacts of multi-step SFDIAs.

Chapter 3

Optimal Data Aggregation in Wide Area Measurement Systems

3.1 Introduction

As shown in Section 2.1, altering a certain state variable through the state estimator without being detected by BDD requires manipulating all measurements dependent on that state variable. Therefore, executing a successful SFDIA, particularly one with a significant impact on the system, often requires the simultaneous manipulation of multiple correlated PMUs, which is both technically complex and operationally challenging. However, if a PDC aggregating these PMUs is compromised, an attacker can manipulate all associated measurements at once, significantly increasing both the likelihood and the potential impact of an attack. This risk is further amplified by the common practice of assigning PMUs to PDCs based on geographical proximity, which frequently results in spatially correlated PMUs being grouped under a single PDC—making PDCs critical entry points for stealthy cyberattacks. As a result, this data aggregation scheme makes PDCs particularly attractive targets for stealthy FDIAs, since compromising a PDC at a local substation requires fewer resources than attacking multiple PMUs spread across a wide geographic area.

Despite this risk, most existing defense strategies focus on securing individual PMUs and often overlook vulnerabilities at PDCs, which serve as aggregation points for multiple correlated measurements. Motivated by this research gap, this chapter develops a tri-level DAO optimization model to determine the optimal data aggregation scheme that minimizes the impacts of SFDIAs when the PDCs are subject to attack. At the defender level, the allocation of PMUs to PDCs is determined through an optimization problem that

minimizes the impacts of SFDIAs while considering practical limitations such as communication delay. At the attacker level, the most critical PDC(s) is (are) selected for intrusion, and the optimal attack vector against the target PDC is determined to maximize the SFDIA impact while maintaining stealth by bypassing the bad-data detection mechanism. Finally, at the operator level, the OPF is used to model the system's response to the attack vector determined at the attacker level. Then, this chapter extends the proposed tri-level optimization—originally designed for a specific operating point—to operate over a time interval with varying operating conditions, employing either SDN or multicast IP technologies.

On this basis, the remainder of this chapter is organized as follows. Section 3.2 demonstrates, through a case study, the common practice of assigning PMUs to PDCs based on geographical proximity, which often results in spatially correlated PMUs being grouped under a single PDC, thereby making PDCs critical entry points for stealthy cyberattacks. Section 3.3 introduces a tri-level DAO optimization framework to redesign the data aggregation scheme from PMUs to the Super PDC (SPDC) at the control center, and develops a case reduction technique to address the computational complexity of the proposed method. Section 3.4 first discusses multicast communication architecture and SDN, which enable reconfiguring the network architecture without incurring additional costs for adapting the data-gathering structure. It then extends the proposed method over a time horizon with varying operating conditions and system configurations. Section 3.5 demonstrates the effectiveness of the proposed method through simulation studies, and Section 3.6 concludes the chapter.

3.2 Problem Statement

This section first introduces the test system employed to investigate the problem discussed here and to evaluate the proposed solutions presented in Section 3.5. It also elaborates on conventional allocation of PMUs to PDCs to aggregate data throughout the system. Afterward, through a case study, this section illustrates how the conventional allocation of PMUs can result in more-severe vulnerabilities to SFDIAs in power systems.

3.2.1 Test System

This thesis uses the IEEE 30-bus test system, which is shown in Fig. 3.1, for investigating the problem. The parameters of the generators within this system are presented in Table

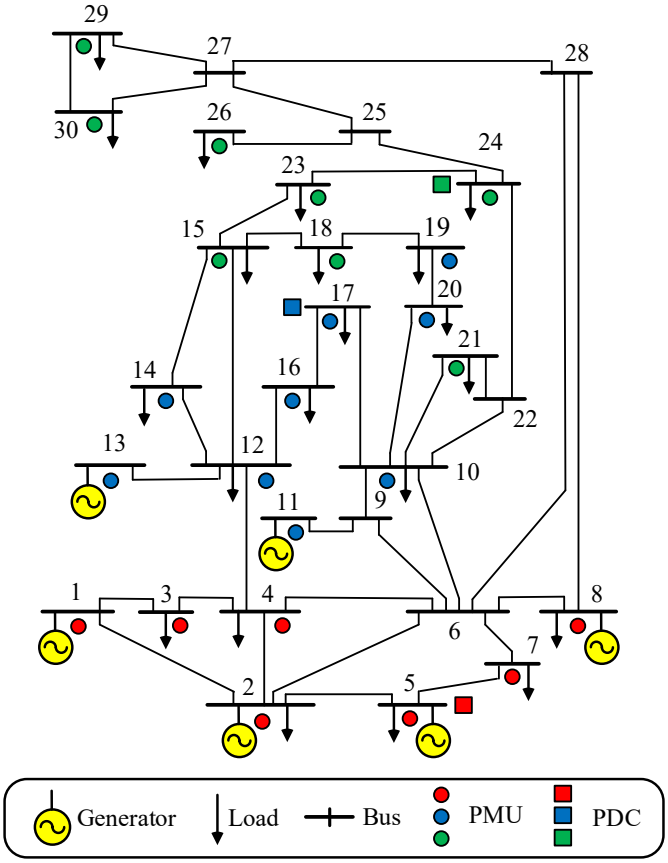


Figure 3.1: IEEE 30-bus test system.

3.1, and the power transfer limits for all transmission lines are detailed in Table 3.2. In this system, the cost of not-supplied demand is $cs = 500$ \$/MWh. More information about this test system, including parameters of the lines and other components, can be found in [72]. In this test system, all load and generation buses are equipped with a PMU to maximize the operator's situational awareness (Fig. 3.1) [96]. In the rest of this proposal, each PMU is specified by its bus number, e.g., PMU on Bus 15 is denoted by PMU 15. Three PDCs (i.e., PDC 5, PDC 17, and PDC 24) are installed in substations of Busses 5, 17, and 24 to aggregate the PMU data from throughout the grid. Additionally, routers are installed in every substation [48]. PMUs are allocated to PDCs based on their communication delay. Therefore, each PMU should be allocated to a PDC, such that the end-to-end delay between the two is minimized [53]. The end-to-end delay for a data packet from a PMU

Table 3.1: Specifications of generators in the IEEE 30-bus system.

Generator	1	2	5	8	11	13
P^{min} (MW)	0	0	0	0	0	0
P^{max} (MW)	200	150	100	100	100	100
cq_g (\$/MW^{2}h)	0.01	0.02	0.015	0.03	0.025	0.04
c_g (\$/MWh)	20	30	40	25	35	40
ca_g (\$/h)	0	0	0	0	0	0

to a PDC is calculated using the following equation

$$de = de_t + de_q + de_s + de_p \tag{3.1}$$

where de is the total end-to-end delay, composed of processing delay (de_s), propagation delay (de_p), transmission delay (de_t), and queuing delay (de_q) [48].

The processing delay can be ignored since routers only forward the data without further processing [46]. The propagation delay, which is the time needed by a data packet to reach from one end of a communication link to the other [48], depends on the length of the communication link between the PMU and its associated PDC. To appropriately model the propagation delay, in this study it is assumed that communication links are placed in parallel with the transmission lines [34]. The average propagation speed of the data through communication links is assumed to be 66% of the speed of light [53]. The transmission delay is defined as the size of the packet divided by the bandwidth of the communication link. To calculate this delay, the packet size and the communication link bandwidth are assumed to be 128 bytes and 2 Mbps, respectively [81]. The queuing delay is the time during which the packet waits in the router buffer, and is considered to be 2 ms. Allocation of PMUs to PDCs based on the minimum end-to-end delay is shown in Fig. 3.1 (a PMU with a certain color is connected to a PDC with the same color).

3.2.2 Case Study

This subsection shows how the conventional method of allocating PMUs to PDCs (i.e., based on communication delay) can endanger the integrity of the grid if a PDC is compromised. To this aim, this subsection uses Load Redistribuation (LR) attacks, which are a class of FDIAs that redistribute loads among buses without changing the total amount of the load [94, 61, 54, 44, 28]. LR attacks are more challenging to detect because (i) only the

Table 3.2: Power transfer limits of transmission lines in the IEEE 30-bus test system.

Line #	From -To	Cap (MW)	Line #	From -To	Cap (MW)	Line #	From -To	Cap (MW)
1	1-2	65	15	4-12	32	29	21-22	16
2	1-3	65	16	12-13	32	30	15-23	8
3	2-4	32	17	12-14	16	31	22-24	8
4	3-4	65	18	12-15	16	32	23-24	8
5	2-5	65	19	12-16	16	33	24-25	8
6	2-6	32	20	14-15	8	34	25-26	8
7	4-6	45	21	16-17	8	35	25-27	8
8	5-7	35	22	15-18	8	36	28-27	32
9	6-7	65	23	18-19	8	37	27-29	8
10	6-8	16	24	19-20	16	38	27-30	8
11	6-9	32	25	10-20	16	39	29-30	8
12	6-10	16	26	10-17	16	40	8-28	16
13	9-11	32	27	10-21	16	41	6-28	16
14	9-10	32	28	10-22	16			

power consumed by loads is altered without changing the power injected by generators, and (ii) the measurements are manipulated within a certain range (i.e., $\pm 50\%$ in this study) to prevent detection methods from easily identifying the attack.

Using the bi-level optimization model developed in [94], which is similar to the bi-level optimization framework discussed in Section 2.2 but with an attacker-oriented economic objective, and within the specified range of measurement manipulations, a stealthy LR attack targeting PMUs 15, 23, 24, 26, 29, and 30 can create a false indication of overload on Lines 27 and 38. As a result of this attack, the OPF is misled to assign an extra 20 MW of active power to high-cost generators on Buses 11 and 13. Additionally, 3.7 MW of the load on Bus 21 is shed. Therefore, this attack imposes 19% extra operation costs on the system. To perform such an attack, an option is to compromise all six PMUs simultaneously, which could be difficult to achieve. On the other hand, since all six PMUs are connected to PDC 24, the same goal can be achieved by only compromising PDC 24, making the PDC a critical entry point for intrusions. To hinder this attack, PMU 15 can be allocated to PDC 17. Thus, the same attack can be carried out by compromising two PDCs at the same time, which is more difficult to accomplish. However, allocation of the PMU 15 to PDC 17 facilitates a more-severe LR attack that can impose 29% extra operation costs on the system by only compromising PDC 17, and manipulating the measurements

received from PMUs 10, 12, 14, 15, 16, 17, 19 and 20. This extra operation cost is mainly due to misleading the operator into shedding 4.9 MW of the load on Bus 10 to protect the power system. To prevent both above-mentioned attacks, in addition to allocating PMU 15 to PDC 17, PMU 10 should be assigned to PDC 5 as well. As a result, the attacker cannot impose an extra cost greater than 1% by targeting PDCs 17 or 5.

The above case study clearly shows how appropriate allocation of PMUs to PDCs can restrain attackers from carrying out stealthy FDIAs with severe impacts when PDCs are compromised. In the next section, a tri-level optimization problem is developed to determine the optimal distribution of PMUs to PDCs such that the impacts of LR attacks are minimized.

3.3 Tri-Level DAO Optimization Framework for Resilient PMU–PDC Allocation

This section introduces a tri-level DAO optimization framework, depicted in Fig. 4.1, to determine the optimal allocation of PMUs to PDCs, thereby enhancing the system's resilience against LR attacks. A tri-level structure is adopted because three distinct decision-making entities—the defender, attacker, and operator—are involved in this scenario, each with conflicting objectives and interdependent decisions. This strategic interplay necessitates a hierarchical optimization framework to accurately capture their interactions. The Operator Level aims to minimize the system's operational cost by optimizing generation dispatch based on received measurement data, which essentially corresponds to solving a standard OPF problem. In contrast, the Attacker Level seeks to maximize this cost by compromising a selected PDC and injecting manipulated measurements into the operator's decision-making process. At the top of the framework, the Defender Level minimizes the maximum possible impact of such attacks by optimally configuring the PMU-to-PDC mapping. This allocation governs which measurements are accessible to the attacker and thus directly influences the effectiveness of potential stealthy intrusions.

3.3.1 Level 1: Defender

This level determines the allocation of PMUs to PDCs by minimizing the impact of LR attacks. The defender's optimization problem is formulated as follows:

$$\underset{x_{n,r}}{\text{Minimize}} \quad F(Z_A) \tag{3.2}$$

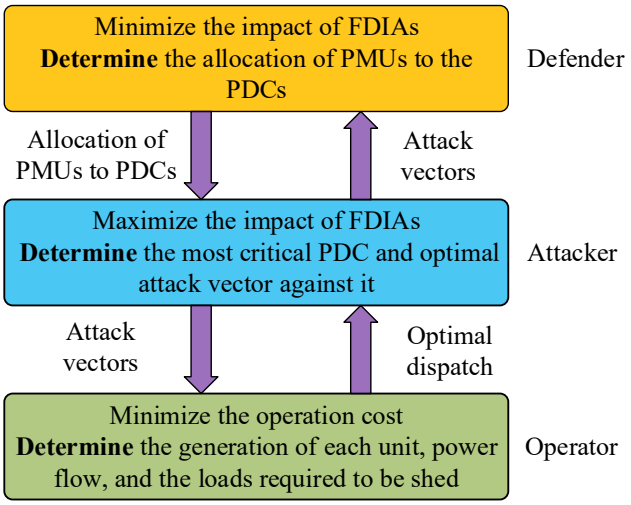


Figure 3.2: The proposed tri-level optimization model.

where $F(Z_A)$ is the defender objective function, which is defined to minimize the impact of FDIAs in general, and LR attacks in particular. The defender can formulate the objective function to defend against increasing operation costs, overloading lines, or manipulating LMPs, to name a few. For instance, the following objective function can be used if the defender's goal is to minimize the ability of attackers in increasing the operating costs of the grid:

$$F(Z_A) = \sum_{g \in \mathcal{G}} (cq_g \ P_g^2 + c_g \ P_g + ca_g) + \sum_{d \in \mathcal{D}} cs_d S_d \tag{3.3}$$

where cq_g, c_g, and ca_g denote, respectively, the quadratic, linear, and constant cost coefficients associated with generator g. The first and second terms respectively denote the active power generation and load shedding costs. The minimization problem of (3.2) should be solved subject to the following constraints:

$$\sum_{r \in \mathcal{R}} x_{n,r} = 1 \quad \forall n \in \mathcal{N} \tag{3.4}$$

$$x_{n,r} \cdot DM_{n,r} \leq de_p^{max}(x_{n,r}) \quad \forall n \in \mathcal{N}, \ \forall p \in \mathcal{P} \tag{3.5}$$

where the binary variable $x_{n,r}$ is the decision variable at this level, indicating whether PMU $n \in \mathcal{N}$ is assigned to PDC $r \in \mathcal{R}$. In fact, constraint (3.4) enforces that each PMU in the grid is connected to one PDC. Moreover, constraint (3.5) limits the minimum end-to-end delay between PMUs and their assigned PDCs. This constraint prevents packet dropouts

when PMUs send their data to their PDCs. In (3.5), $de_r^{max}(.)$ is the maximum possible delay for each PMU of PDC r to communicate its data with the PDC, and is defined as follows:

$$de_r^{max}(x_{n,r}) = T_r + \min\{x_{n,r} \cdot DM_{n,r}\} \quad \forall n \in \mathcal{N} \tag{3.6}$$

where $DM_{n,r}$ denotes the minimum end-to-end delay between PMU n and PDC r, as specified in the delay matrix DM. In addition, T_r represents the waiting time of PDC r for other data packets after the first one arrives, while the second term on the right-hand side of (3.6) captures the earliest arrival time of a data packet to PDC r. In fact, in this proposal the PDC uses the relative time alignment technique, in which a timer starts counting down after the first data packet with a certain time tag is received from PMUs. The PDC packs all the data packets that have the same time tag and are received before expiration of the timer to send them to the SPDC. In this process, late data packets are ignored.

3.3.2 Level 2: Attacker

Using the PMU-to-PDC allocation scheme obtained at the defender level, the attacker level identifies the most critical PDC and its associated attack vector to maximize the impact of LR attacks. The attacker level can be modeled as the following optimization problem

$$\underset{Z_A:=\{Z_{A|D},\ Z_{A|K}\},\ \delta_r}{\text{Maximize}} \quad F(Z_A) \tag{3.7}$$

where δ_r, which is one of the decision variables of this level, determines whether or not PDC r is attacked. The other decision variable in this level, i.e., Z_A, is the attack vector that should be injected into the actual measurements to maximize the impact of the attack. This attack vector is composed of $Z_{A|K}$ and $Z_{A|D}$, which respectively represent the injected values into the measurements of lines and loads. The elements of these sub-vectors are denoted by $z_{a|d}$ and $z_{a|k}$. This optimization problem should be solved subject to the following constraints:

$$\sum_{r \in \mathcal{R}} \delta_r \leq 1 \tag{3.8}$$

Constraint (3.8) indicates that the capabilities of the attacker are limited, and they cannot manipulate the measurements of more than one PDC. It should be noted that a

different limitation on the attacker, such as allowing the manipulation of more than one PDC, can be considered, as discussed in Section 3.5.4. However, in this section, the attacker is restricted to a single PDC.

$$\sum_{r \in \mathcal{R}} x_{n,r} \cdot \delta_r = w_n \quad \forall n \in \mathcal{N} \tag{3.9}$$

Based on the selected PDC for the attack, constraint (3.9) determines the PMUs whose measurements can be manipulated. In this constraint, w_n is a binary variable indicating whether PMU n is compromised (i.e., w_n=1) or not (i.e., w_n=0). In fact, this constraint connects the defender and attacker levels.

$$u_a \leq \sum_{n \in \mathcal{N}} w_n \cdot PM_{n,a} \quad \forall a \in \mathcal{A} \tag{3.10}$$

Constraint (3.10) determines the measurements (including load measurements and line power flow) that can be manipulated during the attack. These measurements depend on δ_r and ω_n. Here, u_a is a binary variable indicating whether measurement $a \in \mathcal{A}$ is compromised (i.e., $u_a = 1$) or not (i.e., $u_a = 0$). Similar to z_a, u_a consists of two components, namely $u_{a|k}$=0 and $u_{a|d}$=0, which are associated with the measurements of lines and loads, respectively.

$$\left(H(H^T H)^{-1} H^T - I\right) Z_A = 0 \tag{3.11}$$

Constraint (3.11) represents the necessary and sufficient condition for a stealthy LR attack [97].

$$\sum_{d \in \mathcal{D}} z_{a|d} = 0 \tag{3.12}$$

Constraint (3.12) ensures that the LR attack only redistributes loads, without changing their total amount. Given that the output of generators cannot be manipulated during an LR attack [94], this type of threat tries to achieve its malicious objectives by maintaining the balance between load and generation.

$$-u_{a|d}\, \sigma P_d \leq z_{a|d} \leq u_{a|d}\, \sigma P_d \quad \forall d \in \mathcal{D} \tag{3.13}$$

$$-u_{a|k}\,\eta \leq z_{a|k} \leq u_{a|k}\,\eta \quad \forall k \in \mathcal{K} \tag{3.14}$$

Constraints (3.13) and (3.14) restrict the extent of manipulation of load and line measurements, respectively, to keep the attack stealthy. Additionally, these constraints limit the attacked measurements to those determined by constraint (3.10).

3.3.3 Level 3: Operator

This level models the response of the operator to the attack vector determined in the attacker level. The purpose of the operator level is to minimize the system operation cost by using OPF. The decision variables of this level are the active power of generators and the loads that are required to be shed. This level is comperhensivly discussed in 2.2, and so here only the required equation for reviwing expressed:

The operator level model can be formulated as follows:

$$\underset{PG,SD}{\text{Minimize}} \quad \sum_{g\in\mathcal{G}}(\alpha_g P_g^2 + \beta_g P_g + \gamma_g) + \sum_{d\in\mathcal{D}} cs_d S_d \tag{3.15}$$

This objective function aims to minimize the operation cost of system, which includes power generation and load shedding costs. The optimization problem of this level should be solved subjected to the following constraints:

$$\sum_{g\in\mathcal{G}} BG_{j,g}\cdot P_g = \sum_{i\in\mathcal{B}} Y_{j,i}\;\theta_i + \sum_{d\in\mathcal{D}} BL_{j,d}\cdot(P_d - S_d + Z_{A|D}) \quad \forall j \in \mathcal{B} \tag{3.16}$$

$$-P_l^{max} \leq SF_l \cdot \big(BG\cdot PG - BL\cdot(PD + Z_{A|D})\big) \leq P_l^{max} \quad \forall l \in \mathcal{L} \tag{3.17}$$

$$P_g^{\min} \leq P_g \leq P_g^{\max} \quad \forall g \in \mathcal{G} \tag{3.18}$$

$$S_d \leq P_d \quad \forall d \in \mathcal{D} \tag{3.19}$$

where (3.16) represents the power balance constraint for each bus; Constraints (3.17) limits the power flow of transmission lines; and Constraints (3.18)-(3.19) set the limits of generators and load shedding, respectively.

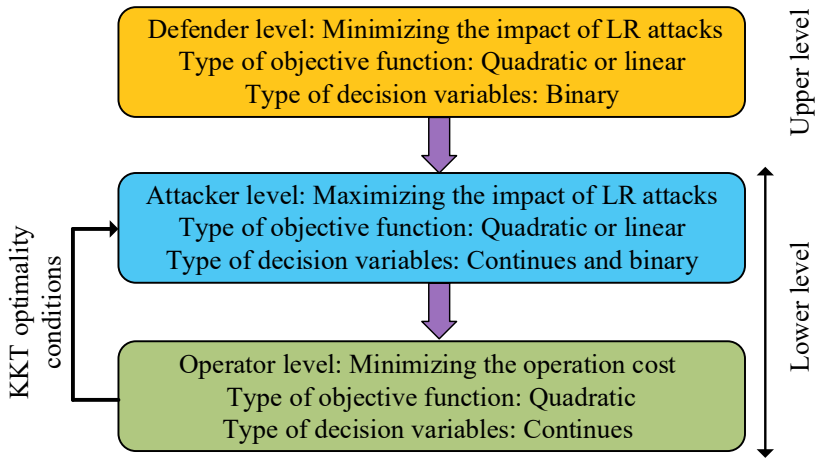


Figure 3.3: Methodology for solving the proposed DAO problem.

3.3.4 Methodology for solving the Proposed DAO Problem

The previous subsections formulated the proposed tri-level DAO problem to determine the optimal assignment of PMUs to PDCs, such that the impacts of LR attacks are minimized. This subsection elaborates on the proposed methodology to solve this optimization problem. This methodology consists of two steps: (i) the original tri-level DAO problem is converted to a bi-level problem, and (ii) an effective reduced enumeration method is employed to find the optimal solution.

Converting three levels to two

The operator level is a convex quadratic problem. Hence, this level can be equivalently replaced with its corresponding optimality Karush–Kuhn–Tucker (KKT) conditions, and added to the attacker level. Using this technique, the attacker and operator levels are merged into a single level (called the lower level), as shown in Fig. 3.3. Thus, the objective function of the lower level equals the objective function of the attacker level (i.e., $F(Z_A)$), which can be quadratic (e.g., operation cost) or linear (e.g., overloading transmission lines). In the case of a quadratic objective function, it should be linearized using the piece-wise linearization technique [97]. Hence, the lower level forms a mixed integer linear program. As Fig. 3.3 shows, the upper level is comprised of the defender level. It should be mentioned that due to the existence of binary decision variables in the lower-level, e.g., δ_r and w_n, the obtained bi-level problem cannot be transformed into a single-level one.

Proposed reduced enumeration technique

Potential techniques for solving the obtained bi-level optimization problem can be classified into three groups: (i) Bender decomposition-based approaches [91, 31, 92], (ii) heuristic approaches [24, 36], and (iii) enumeration-based approaches [10, 77]. Since binary variables (e.g., δ_r and $x_{n,r}$) and a non-convex feasible region (i.e., due to the multiplication of δ_r and $x_{n,r}$ in (3.9)) are present in upper and/or lower levels, decomposition-based approaches either are inapplicable or do not converge [91]. Additionally, Bender decomposition-based approaches may end up with sub-optimal solutions. Similarly, heuristic approaches suffer from two inherent drawbacks: they may result in a sub-optimal solution, or face convergence problems. On the other hand, enumeration method does not suffer from convergence problems and find the exact optimal solution. In this method, a constraint satisfaction problem is solved for the defender-level to determine all possible options for the allocation of PMUs to PDCs. However, this method should search among all feasible regions, and thus the computation time is highly impacted by the size of the problem [10]. On this basis, this proposal develops a reduced enumeration method to solve the above-mentioned optimization problem for large-scale power grids. In this method, a limited number of PMUs are determined as impactful and the defender only decides on allocation of Impactful PMUs. The non-impactful PMUs are thus allocated to the nearest PDCs based on the delay criterion explained in Section 3.2. Impactful PMUs are the ones that significantly impact the response of the OPF. If such PMUs are attacked, the economic operating point of the grid can be influenced the most, e.g., due to redispatching of generating units or shedding of loads. According to [60], impactful PMUs are those associated with lines whose power flows are close to their capacities. The reason is that the measurements of these PMUs have a great deal of influence over the economic operating point of the system [94, 60]. If an attacker portrays the lines whose power flow is close to their capacities more congested than what they actually are, to alleviate the fake congestion the OPF sheds some loads and/or commits high-cost generators to produce more power [94, 60]. As a result, the operation cost of the system increases. On the other hand, if the attacker portrays the lines whose power flow is close to their capacities less congested than what they actually are, the OPF commits low-cost generators to produce more power, thus congesting the lines more severely. Consequently, redispatching of generators might damage the system physically [94, 61].

Based on the above discussion, impactful PMUs are the ones that measure the loads with the highest impact on the power flow of congested lines. The set of congested lines can be defined as follows:

$$\mathcal{C} = \{l \mid \epsilon P_l^{max} \leq P_l\} \tag{3.20}$$

where ϵ is the congestion threshold, and P_l is the power flow of Line l. If during an LR attack an adversary alters Load d by $z_{a|d}$, the power flow of congested line $l \in \mathcal{C}$ changes according to the following equation:

$$\Delta PL_{l,d} = SF_l \cdot BL_d \cdot z_{a|d} \qquad \forall l \in C,\ \forall d \in \mathcal{D} \tag{3.21}$$

where $\Delta P_{l,d}$ is the change in the power flow of line l due to attack to load d [60]. By defining manipulation factor ρ_d for load d, $z_{a|d}$ can be written as

$$z_{a|d} = \rho_d P_d \qquad \forall d \in \mathcal{D} \tag{3.22}$$

where $-\sigma \leq \rho_d \leq \sigma$ denotes the extent to which the measurement of Load d is manipulated with respect to its actual value (P_d). By substituting $z_{a|d}$ from (3.13) into (3.21), $\Delta P_{l,d}$ can be obtained from the following equation:

$$\Delta P_{l,d} = \rho_d \underbrace{SF_l \cdot BL_d \cdot P_d}_{\zeta_{l,d}} \qquad \forall l \in \mathcal{C},\ \forall d \in \mathcal{D} \tag{3.23}$$

As (3.23) shows, the loads with larger $\zeta_{l,d}$ impact the flow of line l more significantly. Therefore, the impactful PMUs for congested Line $l \in \mathcal{C}$ are those that measure the loads with larger $\zeta_{l,d}$. These PMUs can be obtained by the following equation:

$$\mathcal{CP}_l = \{n \mid \zeta_{l,d} \cdot LP_{d,n} \geq \phi \cdot P_l^{max},\ \forall d \in \mathcal{D}\} \quad \forall l \in \mathcal{C} \tag{3.24}$$

where $LP_{d,n}$ is the element on row d and column n of the load-PMU incidence matrix, and ϕ is the threshold for determining impactful PMUs. To reduce the problem size, all the impactful PMUs of a congested line (i.e., all the PMUs in Γ_l) should not be allocated to one PDC, that is

$$\sum_{n \in \mathcal{CP}_l} x_{n,r} < |\mathcal{CP}_l| \qquad \forall l \in \mathcal{C},\ \forall r \in \mathcal{R} \tag{3.25}$$

where $|\mathcal{CP}_l|$ denotes the cardinality of set $\mathcal{CP}_l$. This constraint must be added to defender level. The remaining non-impactful PMUs can be allocated to the nearest PDCs based on the delay criterion, i.e.,

$$x_{n,r} \cdot DM_{n,r} = \min\{DM_{n,r}\ \forall r\} \qquad \forall n \in \Lambda \tag{3.26}$$

where Λ denotes the set of non-impactful PMUs, defined as follows

$$\Lambda = \{n \mid n \notin \mathcal{CP}_l, \quad \forall l \in \mathcal{C}\} \tag{3.27}$$

As a result, Constraint (3.26) should be also added to the defender level. As will be shown in Section 3.6, addition of these two constraints to the defender level reduce the size of problem and its computation time significantly.

3.4 Optimal Dynamic Data Aggregation in WAMSs

The method presented in Section 3.3 determines the optimal data aggregation scheme for a certain operating point. The operating point of the system, however, could alter after any change in loads, system configuration, and the cost of fuel, to name a few. Therefore, the proposed method in the previous section can be applied dynamically to minimize the vulnerabilities of the system to LR attacks during a time interval (e.g., 24 hours) in which the operating point of the system changes. This section first elaborates on the multicast communication architecture and SDN. Then, it explains how the optimal data aggregation scheme can be updated using these technologies when the operating point of the system changes.

3.4.1 Multicast Communication Architecture

Multicast refers to group communication, in which data transmission is simultaneously addressed to a number of destinations. In this architecture, PMUs are considered as multicast sources, which send their messages incessantly to their First-hop Router (FHR) (Fig. 3.4). The FHR is the first node in the multicast tree, which is a set of nodes that represents the route of data between a PMU to all its destinations. If a PDC wishes to receive messages from a specific PMU, it signals to the Last-hop Router (LHR) its willingness to receive messages from that PMU. Then a process is initiated to update the multicast tree [4]. The same process also happens if a PDC refrains from receiving data from a PMU [48]. Since updating the multicast tree can be done easily and quickly without imposing any extra costs, allocation of PMUs to PDCs can be updated when the operating point of the system changes.

3.4.2 Software Define Networking

SDN introduces a paradigm shift in communication network architecture by decoupling the control and data planes [70, 65]. In traditional communication networks, traffic flows are established using forwarding rules determined locally through distributed algorithms.

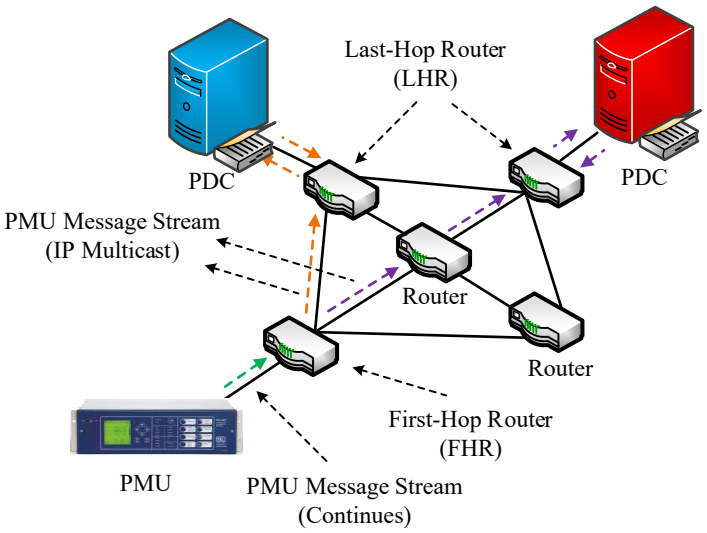


Figure 3.4: IP multicast tree and data transmission from a PMU to PDCs.

In contrast, SDN centralizes the control plane at a dedicated entity known as the SDN controller, which configures traffic flows across the entire network, as shown in Fig. 3.5. Data plane devices, therefore, act as simple forwarding elements, handling only the physical transmission of packets based on rules preinstalled by the controller. The communication between the controller and the forwarding devices is managed via the Southbound Interface (SBI), with OpenFlow being the most widely adopted industry-standard protocol for this purpose [65]. A significant advantage of SDN lies in the programmability of its controller, which—combined with a global view of the network state—enables real-time adaptation to changing network conditions. This centralization facilitates advanced traffic engineering capabilities, such as dynamic rerouting under congestion or failure scenarios, bandwidth guarantees, latency constraints, and rapid failover mechanisms. From a security perspective, SDN can be leveraged to transparently reroute flows through security appliances or to enforce unidirectional flows for sensitive applications. Economically, SDN holds the potential to simplify network deployment and reduce operational costs through standardization, centralized management, and enhanced simulation and verification capabilities. Overall, SDN empowers operators to control not only individual flows but also their complete end-to-end paths across the entire network, ultimately improving efficiency, flexibility, and security in power system communication infrastructures. Therefore, with SDN, the allocation of PMUs to PDCs can be easily and cost-effectively updated as system conditions change.

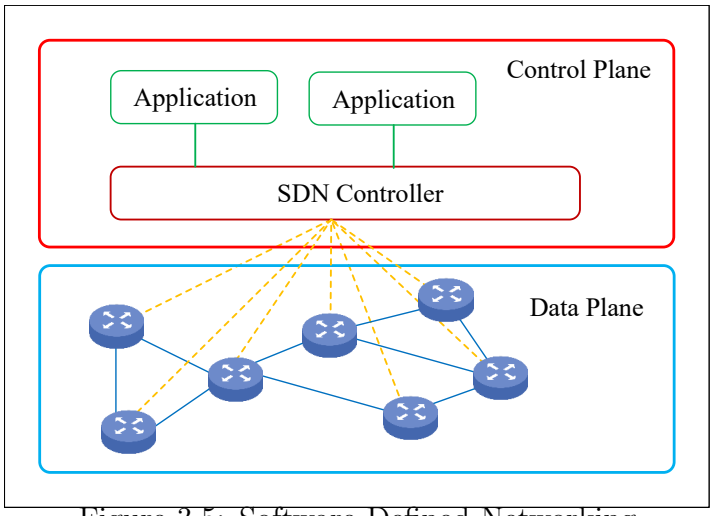


Figure 3.5: Software-Defined Networking.

3.4.3 Proposed Model for Dynamic Data Aggregation

As discussed in Section 3.3.4, congested lines and their associated impactful PMUs are determinant factors of the optimal data aggregation scheme. Therefore, any variation in the operating point that adds/removes lines to/from the list of congested lines (i.e., set $\mathcal{C}$) or their impactful PMUs (i.e., $n \in \mathcal{CP}_l,\ \forall l \in \mathcal{C}$) may necessitate updating the data aggregation scheme. By leveraging the multicast communication architecture or the capabilities of SDN, the allocation of PMUs to PDCs can be updated without incurring additional costs, Thus, in this subsection, the objective of the defender is to determine the optimal data aggregation scheme after any significant variation in the operating point while minimizing changes in the allocation of PMUs to PDCs. Hence, the defender's objective function in (3.2) can be substituted with the following one to determine the data aggregation scheme dynamically:

$$F_{dyn,h}(Z_a) = F(Z_a) + \zeta \sum_{r \in \mathcal{R}} \sum_{n \in \mathcal{N}} \left| x^h_{n,r} - x^{h-1}_{n,r} \right| \tag{3.28}$$

where $F_{dyn,h}(z_a)$ is the objective function of the proposed tri-level optimization problem at hour h; $x^h_{n,r}$ and $x^{h-1}_{n,r}$ represent the connection of PMU n to PDC r at hours h and $h-1$, respectively; and ζ is a weighting factor. In fact the second term is a penalty factor that is added to minimize changes in the updated data aggregation scheme against the previous one. Fig. 3.6 illustrates the flowchart of the proposed dynamic data aggregation scheme.

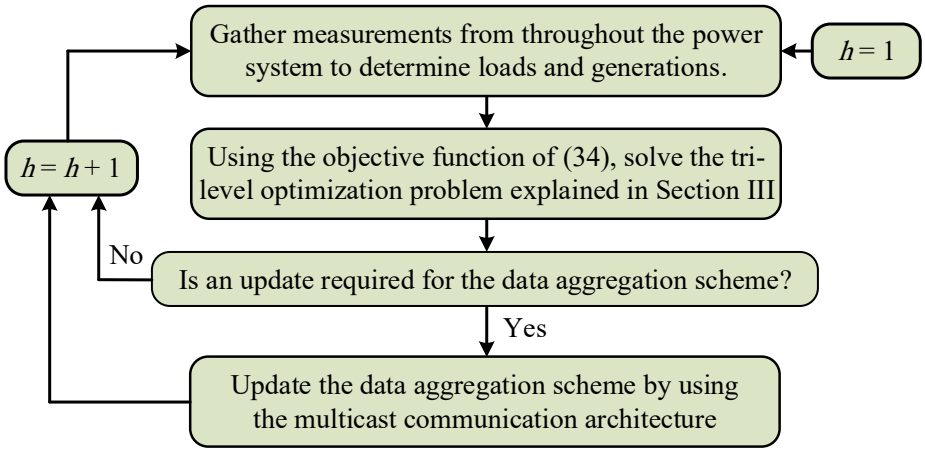


Figure 3.6: Flowchart of the proposed dynamic data aggregation scheme.

3.5 Performance Evaluation

This section evaluates the proposed optimal data aggregation scheme on the IEEE 30-bus test system, which was introduced in Section 3.2.1. It also compares the proposed scheme with the conventional one, which connects PMUs to PDCs based on minimum communication delay. In this study, the waiting time for all PDCs, i.e., T_r, is considered to be 10 ms [3]. Moreover, the congestion threshold of lines, i.e., ϵ, is set equal to 0.8. The weighting factor ζ, which determines the importance of the penalty factor in (3.28), is assumed to be 10. The proposed optimization problem is solved by using CPLEX solver of GAMS software and MATLAB on a PC with Intel Core i7 2.7 GHz CPU and 12GB of RAM.

To assess the effectiveness of the proposed method, the following two indices are used in the remaining of this section:

- Line Capacity Increment (LCI): As discussed in Section 3.3.4, congested lines and their associated impactful PMUs highly impact the consequences of LR attacks. Therefore, to evaluate the proposed method more effectively, the congestion level of transmission lines is changed during simulations using the LCI index (expressed in percent), which denotes the extent of increment in the capacity of lines. For instance, LCI= 20% signifies 20% increase in the capacity of lines for the same loading condition. In practice, such an increment for a line can be achieved using different techniques, such as series or parallel compensation of that line.

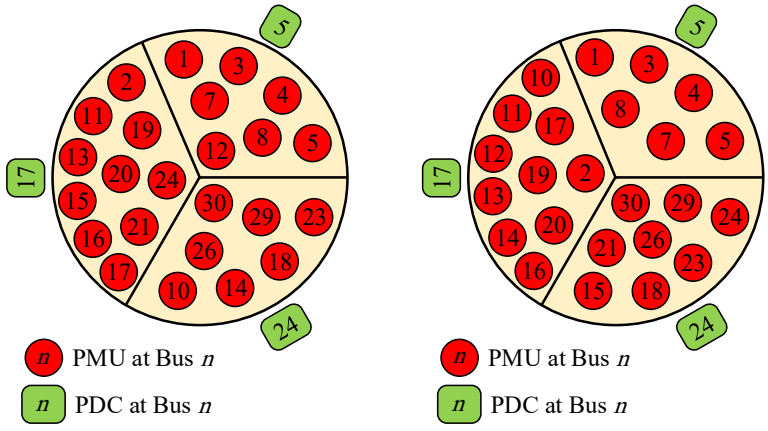
- Operation Cost Increase (OCI): This index is used to quantify the impacts of an LR attack on the operation cost of the grid, and is defined as follows:

$$OCI = \frac{F(Z_A) - F(Z_A = 0)}{F(Z_A = 0)} \times 100\% \tag{3.29}$$

  In fact, this index shows how much the cost is increased after a successful LR attack.

3.5.1 Minimizing Economic Vulnerabilities of Power Grids

This subsection determines the optimal data aggregation scheme for a certain operating point by minimizing the economic vulnerabilities of power grids against LR attacks. Thus, the operation cost of the system, i.e., (3.3), is selected as the objective function of defender and attacker levels. Figs. 3.7a and 3.7b illustrate the optimal data aggregation scheme obtained from the proposed tri-level optimization problem when LCI is 0% and 100%, respectively. To minimize the economic vulnerabilities of power grids when LCI= 0%, PMUs 10 and 14 must be reallocated from PDC 17 to 24, PMUs 15, 21, and 24 must be reallocated from PDC 24 to 17, and PMU 12 must be reallocated from PDC 17 to 5. However, when the system is lightly congested, i.e., LCI= 100%, fewer PMUs must be reallocated to meet the constraints of the three-level optimization problem and minimize its objective function. In this case, disconnecting PMU 2 from PDC 5 and connecting it



(a) (b)

Figure 3.7: The optimal data aggregation scheme when (a) LCI= 0% and (b) LCI= 100%.

to PDC 17 results in the minimum economic vulnerability compared to the conventional scheme. In fact, for LCI= 100%, only Lines 1 and 10 are congested. For Line 1, condition (3.25) is not met since all its impactful PMUs (i.e., PMUs 2, 5, and 8) are connected to one PDC. Thus, by reallocating PMU 2 from PDC 5 to 17 not only is condition (3.25) met, but the objective function is minimized as well. Therefore, as these two examples illustrate, the conventional scheme needs more modifications when the lines are more congested.

The OCI index can be used to compare the economic vulnerabilities of the conventional data aggregation scheme with the one obtained from the proposed method. Fig. 3.8 illustrates the OCI index versus the LCI index for both conventional and proposed data aggregation schemes. As explained in Section 3.3, the extra cost that an attacker can impose has two components: (i) extra cost due to utilizing more-expensive units instead of economic ones, which happens when the attacker portrays a fake congestion by manipulating measurements, and (ii) extra costs due to unnecessary load shedding, which happens by portraying fake congestions and misleading the operator. The second component is in fact more influential, since the cost of not-supplied demand is often much higher than the difference in the generation costs of various units. When the conventional scheme is used and the lines are not congested (i.e., LCI$\geq$ 40%), the attacker cannot increase the operation cost of the grid significantly, since (s)he can only impact the optimal dispatching of generators. When LCI$<$ 40%, however, the imposed extra cost to the power system can be increased significantly due to initiation of load shedding. For instance, the attackers can target PDC 24 to increase the operation cost of the power system by 19.2% when LCI= 0%. When the proposed data aggregation scheme is employed, however, the attacker cannot increase the operation cost by attacking one PDC. This happens since the proposed scheme connects the impactful PMUs that must be targeted simultaneously to keep the attack stealthy to more than one PDC.

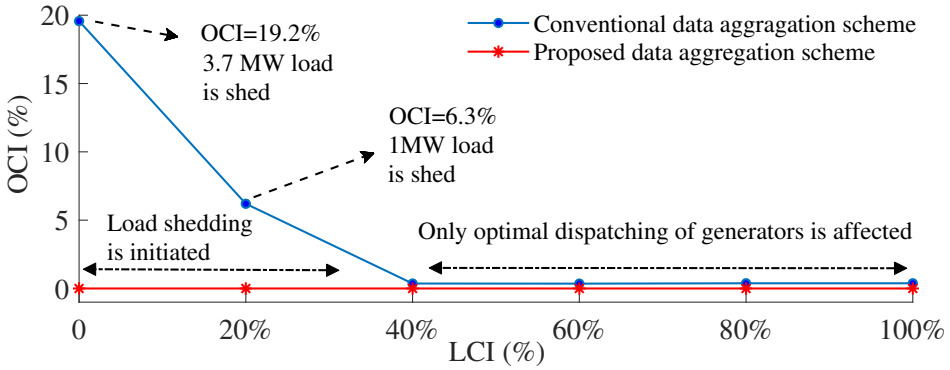


Figure 3.8: OCI index for various LCI values.

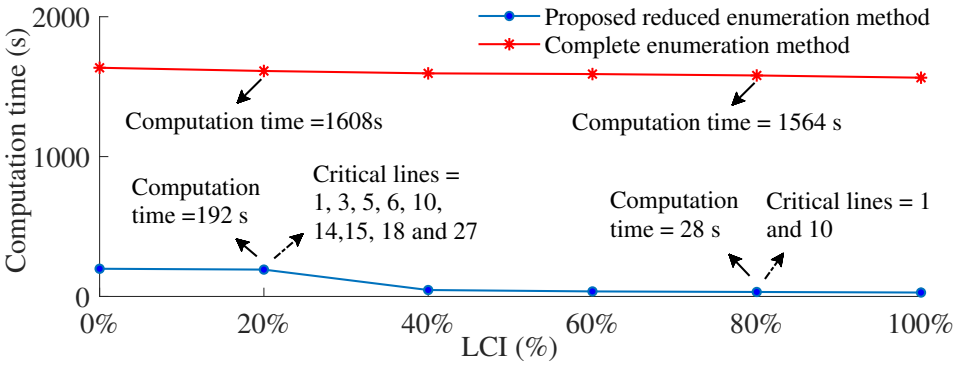


Figure 3.9: Computation time of the proposed tri-level optimization model

Finally, this subsection compares the performance of the proposed method when the reduced enumeration technique is employed with the case of using the complete enumeration method. As expected, both enumeration methods yield the same results for various LCI values. The computation time of the proposed reduced enumeration technique, however, is remarkably lower than that of the complete enumeration method (Fig. 3.9). For instance, in the case of LCI= 80%, the proposed method can solve the optimization problem in 28 seconds, while the same results are obtained by the complete enumeration method in 1564 seconds. Therefore, the proposed enumeration method is able to reach the optimal solution in a significantly lower time without sacrificing the accuracy considerably.

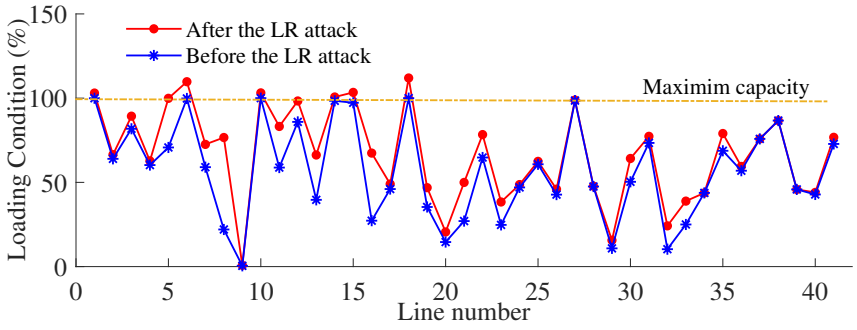


Figure 3.10: Loading condition of lines before and after LR attacks.

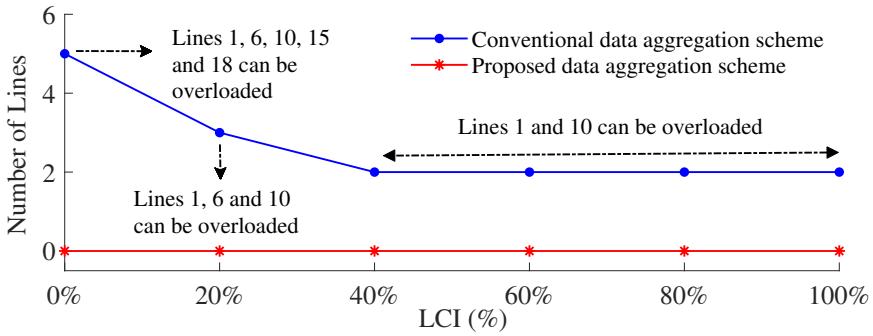


Figure 3.11: Number of lines that can be overloaded beyond their capacities for various values of the LCI index.

3.5.2 Minimizing Overloading Vulnerabilities of Power Grids

In this subsection, the optimal data aggregation scheme for a certain operating point is obtained by minimizing the ability of the attacker to overload the congested lines. Such risks can be imposed by LR attacks in which the measurements are manipulated such that the lines whose power flow is close to their capacities seem less congested than what they actually are. As a result of these attacks, the OPF commits low-cost generators to produce more power, thus overloading the congested lines. To minimize the ability of the attacker to overload the congested lines, the following objective function is used:

$$F(z_a) = \sum_{l \in \mathcal{L}} Heav\left(P_l^* - P_l^{max}\right) \tag{3.30}$$

in which, $Heav(.)$ is the Heaviside step function and P_l^* is the actual flow of line l after the attack, and is calculated using the following equation:

$$P_l^* = \left| SF_l \left(BG \cdot PG - BL \cdot PD\right) \right| \tag{3.31}$$

In fact, the objective function of (3.30) minimizes the number of lines whose flow can be pushed by LR attacks over their capacities. For instance, Fig. 3.10 shows the number of lines that are overloaded beyond their capacities when the conventional data aggregation scheme is utilized and the LCI = 0%: the attacker can overload Lines 1, 6, 10, 15, and 18 through LR attacks, i.e., $F(Z_A) = 5$. To evaluate the proposed method in minimizing the ability of the attacker to overload the lines, its performance is tested for various values of the LCI index. Fig. 3.11 compares the number of lines that can be overloaded when the

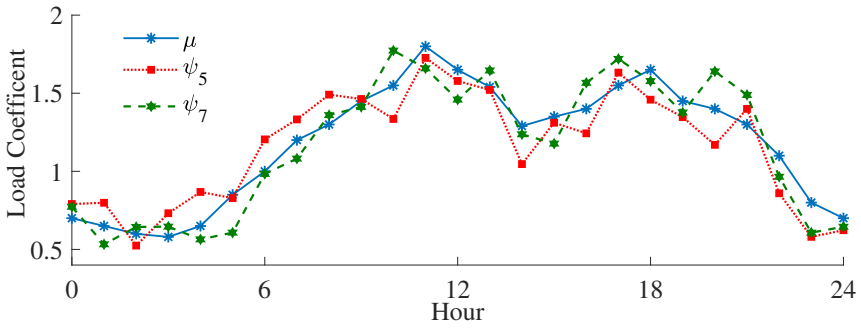


Figure 3.12: Daily Load Coefficient.

conventional and proposed data aggregation schemes are used. As this figure shows, the proposed method eliminates the risk of overloading by LR attacks for all lines for all values of the LCI index; however, in the conventional scheme, the smaller the LCI index, the higher the number of lines that can be overloaded. For instance, if the data is aggregated by utilizing the conventional scheme, the attacker can overload Lines 1, 6, and 10 when LCI= 20%. However, by utilizing the proposed data aggregation scheme, no line can be overloaded by the attacker for the same value of the LCI index.

3.5.3 Optimal Dynamic Data Aggregation

This subsection evaluates the proposed dynamic data aggregation scheme, which was explained in Section 3.4. To model variations in the operating point of the system, this proposal assumes that the load at each bus changes based on the following equation:

$$P_d^h = \underbrace{(\mu^h + \vartheta_d^h)}_{\psi_d^h} P_d \qquad \forall d \in N^d,\ h \in \{1, 2, \cdots, 24\} \tag{3.32}$$

where P_d^h represents the value of Load d in hour h. Coefficient μ^h (Fig. 3.12), which is the same for all loads at every hour, is used to model the average daily load change in the system. Since different load types—e.g., residential, commercial, and industrial—follow different patterns, coefficient ϑ_d^h is used to account for various load types incorporated in load d during hour h. This coefficient is selected randomly between 0.25 and -0.25 for each load in each hour. For example, the overall load coefficients for loads on Buses 5 and 7, i.e., ψ_5^h and ψ_7^h, respectively, are shown in Fig. 3.12. In this subsection, the operation cost of the system, i.e., (3.3), is selected as the objective function of the defender and attacker levels. Simulations are performed for LCI= 100%, i.e., the system is lightly congested.

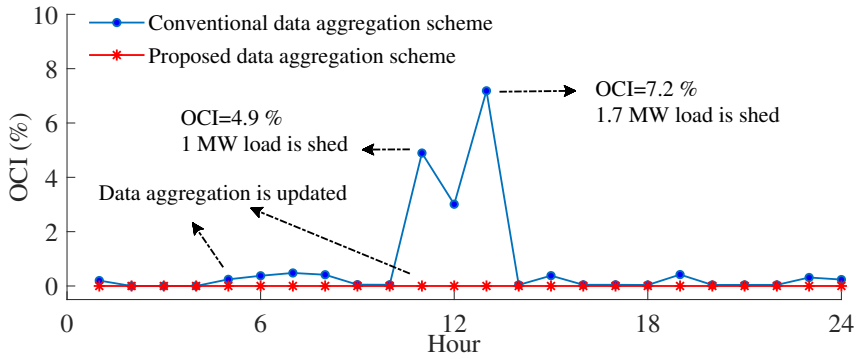


Figure 3.13: OCI index during 24 hours.

Fig. 3.13 shows the OCI index during the 24 hours of this study for both conventional and proposed data aggregation schemes. As this figure shows, when the conventional data aggregation scheme is used, the attacker can impose extra costs to the system by manipulating the measurements of a single PDC. The increase in the operation cost is significant at Hours 11, 12, and 13, when the attacker can portray a fake need to load shedding by manipulating the measurements of PMUs. For instance, the attacker can increase the operation cost by 7.2% during Hour 13 by initiating a load shedding for 1.7 MW. The proposed data aggregation scheme, however, makes the OCI index equal to zero for all hours by determining optimal data aggregation scheme one time at $h = 1$ and updating it two times afterwards, i.e., at $h = 5$ and $h = 11$.

3.5.4 Cyber Attacks Targeting Multiple PDCs Simultaneously

In practice, targeting multiple PDCs simultaneously is highly improbable, largely due to their robust security measures and geographical dispersion. However, to further corroborate the effectiveness of the proposed data aggregation technique, this subsection evaluates it when multiple PDCs are subject to a cyber attack. To this aim, constraint (3.8), which originally posits that attackers are constrained to manipulating measurements of only a single PDC, should be modified to determine the number of compromised PDCs. Given that the test system of this paper includes three PDCs, this constraint is modified to limit the attacker to two PDCs, as an assault on all three would grant the attacker control over the entire system and render the reallocation of PMUs inconsequential. Fig. 3.14 displays the OCI index against the LCI values for both the conventional and proposed data aggregation methods when two PDCs are subjected to cyberattacks. As this figure shows, when the lines are not overloaded (LCI $\geq 40\%$), an attacker's ability to significantly increase the grid's operating costs is limited for both proposed and conventional methods, primarily

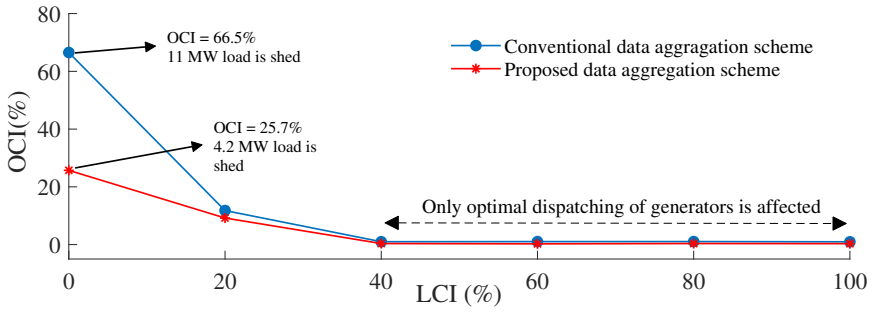


Figure 3.14: OCI index for various LCI values when two PDCs are subjected to cyberattacks for the IEEE 30 bus test system.

affecting only the optimal dispatch of generators. In cases where the LCI drops below 40% and the conventional method is used, the extra costs to the power system can rise markedly, triggered by the start of load shedding. For instance, attacking PDCs 24 and 17 can lead to a 66.5% increase in the operational costs of the grid when LCI= 0%. However, when the proposed data aggregation method is used, the attacker's capability to escalate the operational cost diminishes considerably. For instance, with the proposed approach, the OCI index is limited to a maximum of 25% when LCI= 0%.

It should be noted that the proposed method is specifically designed to secure the PMU-to-PDC aggregation structure and is not effective against attacks that target multiple PMUs independently, bypassing PDCs entirely. While such attacks are outside the scope of the current framework, they are considered significantly less probable and harder to execute in practice, as demonstrated through BAG analysis. Additionally, when both PMUs and PDCs are compromised simultaneously to reach a set of PMUs, the resulting impact is functionally equivalent to attacking multiple PDCs directly, reinforcing the focus and relevance of the proposed method.

3.6 Conclusion

This chapter showed that conventional data aggregation method in wide-area measurements systems could lead to economic and physical damages to the grid if LR attacks happen. To address this issue, this proposal presents a tri-level optimization model to determine the optimal data aggregation scheme for collecting the data of PMUs and sending them to the SPDC of the control center. The presented model takes into account

the resilience of the grid to cyberattacks, and considers its physical limitations, e.g., communication delays. The objective function of this study was to minimize the economic vulnerabilities of the grid or the risks of physical damages to it when LR attacks target the system. The objective function, however, can be changed to any other one that enhances the grid's resiliency against cyberattacks. Additionally, the proposed method can address alterations in the operating point and configuration of the system by updating the data aggregation scheme dynamically using the multicast IP protocol. The proposed method was tested on the IEEE 30-bus system and found to significantly increase power grid resilience to LR attacks. The proposal also introduced a case reduction technique to make the problem smaller and faster to solve, resulting in a significant decrease in computation time while maintaining high accuracy.

Chapter 4

A Cyber-Physical Risk Metric and Data Aggregation Reconfiguration Strategy for Mitigating SFDIAs

As demonstrated in Chapter 2, power systems are highly vulnerable to SFDIAs, particularly those capable of causing physical damage through line overloading. The feasibility of executing such attacks depends on compromising data from numerous PMUs across the system, which in turn is heavily influenced by the hierarchical data-gathering structure of the cyber layer. However, as discussed in Section 1, a significant gap in the existing vulnerability analysis literature is its neglect of the cyber-layer architecture, especially the manner in which measurement data are aggregated and transmitted. Prior studies have typically modeled attack feasibility by imposing arbitrary limits on the number of measurements that can be manipulated [94, 44, 54, 28]. This approach oversimplifies the complex hierarchical data aggregation framework, involving multiple PMUs, PDCs, and communication links. Such oversimplification risks overlooking critical vulnerabilities that could significantly influence vulnerability assessments and may ultimately result in ineffective defense measures.

Given the importance of the data-gathering structure, Chapter 3 of this thesis proposes a defense strategy that optimizes data aggregation by optimally allocating PMUs to PDCs. However, to further strengthen this strategy, it is essential to consider not only the assignment of PMUs to PDCs but also the broader cyber-layer architecture, including the communication paths between each source and destination, as both a contributor to system vulnerability and a target for optimization against SFDIAs. Building on this

perspective, this thesis first addresses the often-overlooked role of the cyber layer in vulnerability analyses of power systems facing SFDIAs. To incorporate this role, a CPRM is introduced, which jointly quantifies both the likelihood and the physical consequences of SFDIAs. The CPRM captures the impacts of transmission line losses—such as load shedding or generator outages—together with the probability that these losses result from an SFDIA. This probability is estimated by identifying critical PMUs sets, defined as minimal sets of measurements whose compromise could stealthily overload transmission lines. An efficient bi-level optimization algorithm is employed to determine these sets. Furthermore, to quantify access likelihoods, BAGs are constructed for each substation and communication link, modeling potential attack pathways and estimating their associated probabilities. Building on the CPRM, this chapter develops a proactive risk mitigation strategy to determine the optimal data aggregation structure within the power system's cyber-layer. This strategy is formulated as an optimization problem that minimizes the CPRM, effectively reducing the risk of SFDIAs. Following this, the chapter introduces a novel DAR scheme, which dynamically adjusts the cyber-layer structure using SDN to cope with changes in the operating point and/or configuration of the systems.

Building on the developed CPRM, this chapter proposes a proactive risk mitigation strategy to determine the optimal data aggregation structure within the power system's cyber layer. This strategy is formulated as an optimization problem aimed at minimizing the CPRM, thereby reducing the risk of SFDIAs. The proposed mitigation strategy not only optimizes the allocation of PMUs to PDCs, but also reconfigures the communication paths between them, thus enhancing system resilience against SFDIAs. Subsequently, the chapter introduces a novel DAR scheme that dynamically adjusts the cyber-layer structure using SDN to adapt to changes in the system's operating point and/or configuration.

The contributions of this chapter are summarized as follows:

- A comprehensive CPRM is proposed to quantify the risk posed by SFDIAs in power systems. This metric is established through a three-step procedure: (i) identifying critical PMUs sets for each transmission line by solving multiple bi-level optimization problems, (ii) estimating the attack probabilities on these critical sets using BAGs, and (iii) integrating these probabilities with the physical consequences of losing each line to compute the CPRM.

- A novel proactive risk mitigation strategy is developed to determine the optimal data aggregation structure within the power system's cyber layer. Formulated as an optimization problem, this strategy aims to reduce the risk of SFDIAs, improve system resilience, and strengthen the overall cyber-physical security posture.

- An SDN-enabled DAR scheme is presented to dynamically reconfigure the cyber-layer data aggregation architecture with the goal of minimizing the CPRM. The scheme operates in two phases: an offline phase, which generates and stores potential cyber-layer configurations using the proposed risk mitigation strategy, and an online phase, which selects and applies the optimal configuration in real time via SDN.

On this basis, the remainder of this chapter is organized as follows. Section 4.1 presents the bi-level optimization method for identifying critical PMUs sets for each transmission line. Section 4.2 introduces BAGs models to describe the attack paths used to access these critical PMUs sets and evaluates the probabilities of successful cyberattacks against them. Section 4.3 formulates the proposed CPRM and develops the corresponding proactive risk mitigation strategy. Subsequently, Section 4.4 evaluates the proposed CPRM and the mitigation strategy on the 39-bus test system. Finally, Section 4.5 concludes the chapter.

4.1 Identifying Critical PMU sets of a Line

This section first presents a bi-level optimization model to identify the minimal critical set of PMUs for a transmission line. This set includes the minimum number of PMUs that can be leveraged to overload a line stealthily through an SFDIA. Then, an algorithm is proposed to solve multiple bi-level optimization problems to systematically identify all critical PMUs sets associated with the line.

4.1.1 Determining the Minimal Critical PMU Set of a Line Using Bi-level Optimization

This section introduces a bi-level optimization problem (Fig. 4.1) to identify the minimal critical PMU set for a given line. In the upper-level model, the attacker aims to minimize the number of PMUs that are required to be manipulated in order to overload a target line. The lower-level model represents the operator's response to the manipulated data based on the OPF. The objective function of the upper-level for stealthily overloading line l is defined as follows

$$\underset{Z_A^l:\{Z_{A|K}^l, Z_{A|D}^l\}, w_n^l}{\text{Minimize}} \sum_{n \in \mathcal{N}} w_n^l \tag{4.1}$$

where w_n^l represents a binary variable that denotes whether the data of the PMU at bus n (denoted by PMU_n) is to be manipulated (1 if attacked, 0 otherwise) to overload line

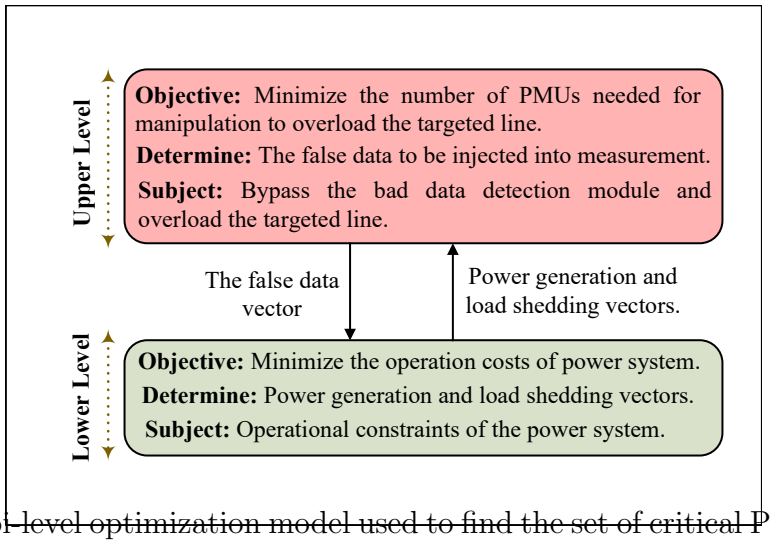


Figure 4.1: The bi-level optimization model used to find the set of critical PMUs to overload a target line.

l. Additionally, Z_A^l denotes the attack vector intended to be injected into the actual measurements to overload line l. The objective function of (4.1) should be minimized subject to several constraints. The first constraint limits the attacker to the measurements of PMUs whose associated w_n^l is one. This constraint can be defined as follows

$$u_a^l \leq \sum_{n \in \mathcal{N}} w_n^l \cdot PM_{n,a} \quad \forall a \in \mathcal{A} \tag{4.2}$$

where PM is a binary matrix that represents the measurement assignments of the PMUs in the system. Each element takes the value 1 if PMU n records measurement a, and 0 otherwise. The next constraint ensures that line l becomes overloaded, and is defined as follows

$$|P_l| > \zeta P_l^{\max} \tag{4.3}$$

where $\zeta > 1$ is the threshold at which the capacity exceedance is deemed an overload. Additionally, P_l is the actual power flow of line l, which can be calculated as follows

$$P_l = SF_l \cdot (BG \cdot PG - BL \cdot PD) \tag{4.4}$$

To address the non-linearity of the overload condition described in (4.3), the method outlined in [85] is employed, transforming the overload condition into a set of linear constraints. The non-linearity arises from the presence of the absolute value $|P_l|$ in the overload condition, which checks whether the magnitude of the power flow on line l exceeds a fraction ζ of its thermal limit $P_l^{\max}$. To linearize this, an auxiliary binary variable π_l is introduced

to indicate the direction of power flow in line l ($\pi_l = 1$ for positive flow, and $\pi_l = 0$ for negative flow).

Using the big-M technique, the absolute value constraint $|P_l| \geq \zeta P_l^{\max}$ is split into two mutually exclusive linear inequalities [85]:

$$P_l + \pi_l M \geq \zeta P_l^{\max} \tag{4.5}$$

$$-P_l + (1 - \pi_l) M \geq \zeta P_l^{\max} \tag{4.6}$$

Here, M is a large constant used to deactivate one of the two constraints depending on the value of π_l. When $\pi_l = 0$, the first constraint enforces $P_l \geq \zeta P_l^{\max}$ while the second becomes non-binding due to the large M term; when $\pi_l = 1$, the roles are reversed, and the second constraint enforces $-P_l \geq \zeta P_l^{\max}$. In the big-$M$ linearization method, M must be sufficiently large to ensure that the "inactive" constraint is automatically satisfied, yet not excessively large to avoid numerical instability in the solver. In practice, studies in power system optimization often set M to approximately 1.2–2 times the largest line flow limit in the network, which is large enough to relax the constraint when inactive but small enough to maintain numerical stability. Additionally, the following constraints must be met to keep the attack stealthy:

$$\left(H(H^T H)^{-1} H^T - I\right) Z_A^l = 0 \tag{4.7}$$

$$\sum_{d \in \mathcal{D}} z_{a|d}^l = 0 \tag{4.8}$$

$$-u_{a|d}^l \, \sigma P_d \leq z_{a|d}^l \leq u_{a|d}^l \, \sigma P_d \qquad \forall d \in \mathcal{D} \tag{4.9}$$

$$-u_{a|k}^l \, \eta \leq z_{a|k}^l \leq u_{a|k}^l \, \eta \qquad \forall k \in \mathcal{L} \tag{4.10}$$

Constraint (4.7) ensures that the injected data can bypass the BDD module of SE [97]. Constraint (4.8) maintains stealth by ensuring that the load is redistributed while its sum remains unchanged. In fact, without loss of generality, this constraint manipulates the measurements through a load redistribution attack, which is stealthy and does not require manipulation of PMUs connected to generators (which are often more secure and protected). Finally, Constraints (4.9) and (4.10) limit the extent of manipulation of load and line measurements, respectively. In fact, (4.9) and (4.10) limit the manipulated measurements to those defined by (4.2).

As shown in Fig. 4.1, the lower level of the model captures the operator's response to the attack vector defined at the upper-level. Excluding this layer would imply that the operator remains passive in response to the change in system states, which is inconsistent with real-

world operations. Incorporating the lower-level ensures a more realistic representation of the interactions between the operator and the attacker. The primary goal of the lower level is to minimize the operational costs via OPF. The formulation for the operator level is as follows

$$\underset{P_G, S_D}{\text{Minimize}} \quad \sum_{g \in \mathcal{G}} c_g P_g + \sum_{d \in \mathcal{D}} cs_d S_d \tag{4.11}$$

This optimization problem is subjected to the following constraints:

$$\sum_{g \in \mathcal{G}} BG_{j,g} \cdot P_g = \sum_{b \in \mathcal{B}} Y_{j,b}\ \theta_b + \sum_{d \in \mathcal{D}} BL_{j,d} \cdot (P_d - S_d + z^l_{a|d}) \quad \forall j \in \mathcal{B} \tag{4.12}$$

$$-P_k^{max} \leq SF_k \cdot \left(BG \cdot PG - BL \cdot (PD + Z^l_{A|D})\right) \leq P_k^{max} \quad \forall k \in \mathcal{L} \tag{4.13}$$

$$P_g^{min} \leq P_g \leq P_g^{max} \quad \forall g \in \mathcal{G} \tag{4.14}$$

$$S_d \leq P_d \quad \forall d \in \mathcal{D} \tag{4.15}$$

Where (4.12) denotes the power balance constraint for each bus, and (4.13)-(4.15) define the limits for power flow in transmission lines, generator output, and load shedding, respectively.

To address the complexities of this bi-level optimization problem, the lower level can be reformulated using the KKT optimality conditions, which are then integrated into the attacker level. This reformulation transforms the bi-level problem into a unified linear MILP model. The resulting MILP can be efficiently solved using conventional optimization solvers to determine all binary variables w_n^l that must be manipulated to overload line l. The critical set of PMUs for line l includes all the PMUs whose associated w_n^l are non-zero.

4.1.2 Determining All Critical PMU Sets of a Line

Since multiple critical PMUs sets may exist for a given line, the bi-level optimization needs to be run multiple times to identify all such sets. To ensure that previously identified solutions are not repeated, each time the optimization is executed, a constraint is added to the problem to exclude the critical sets already found. This is captured by the following constraint

$$\sum_{n \in \mathcal{N}} w^l_{n,s} < |\Omega^s_l| \tag{4.16}$$

where $|.|$ signifies the cardinality operator, and $w^l_{n,s}$ is the binary variable that denotes whether PMU_n has been selected for Line l in the s-th optimization, or equivalently if

Algorithm 2 Algorithm to Identify All Critical PMU Sets of Line l.

1: Initialization.
2: Set $s = 1$.
3: **while** the bi-level optimization problem is feasible **do**
4: Solve the bi-level optimization defined by (4.1)-(4.15).
5: Store the result in Ω_l^s.
6: Integrate a new constraint based on (4.16) into the bi-level optimization problem.
7: $s = s + 1$.
8: **end while**

critical set s includes PMU_n. Additionally, Ω_l^s represents the s-th critical PMU set for line l, and is defined as follows

$$\Omega_l^s = \left\{ n \mid w_{n,s}^l > 0, \forall n \in \mathcal{N} \right\} \tag{4.17}$$

In fact, constraint (4.16) ensures that the sum of all $w_{n,s}^l$ values from the s-th critical set of line l is less than the cardinality of the set Ω_l^s. This effectively prevents subsequent optimization problems from selecting all the PMUs of any previously identified critical set for line l. The process of solving bi-level optimizations and incorporating constraints related to each identified critical set continues until the optimization problem becomes infeasible. This approach guarantees that all potential sets of PMUs necessary for overloading a line are thoroughly identified. The proposed method is shown in Algorithm 2.

4.2 Bayesian Attack Graph for Modifying the Data of PMUs

When the critical PMUs sets of a line are identified, the probability of overloading a line depends on the likelihood of gaining access to all PMUs in a critical set. This access can be achieved through attacks on substations, communication links, or PDCs. BAGs are commonly used to model potential attack pathways by outlining exploitable vulnerabilities. On this basis, this section begins with an examination of the architecture of substations and data aggregation structure in power systems, highlighting potential attack entry points for data manipulation. Subsequently, it discusses the concept of BAGs and develops a BAG for modifying the data of PMUs through compromised substations and communication links. It is important to note that this paper assumes, for simplicity and without loss of generality, that the structure of all substations in the system is uniform and all communication links

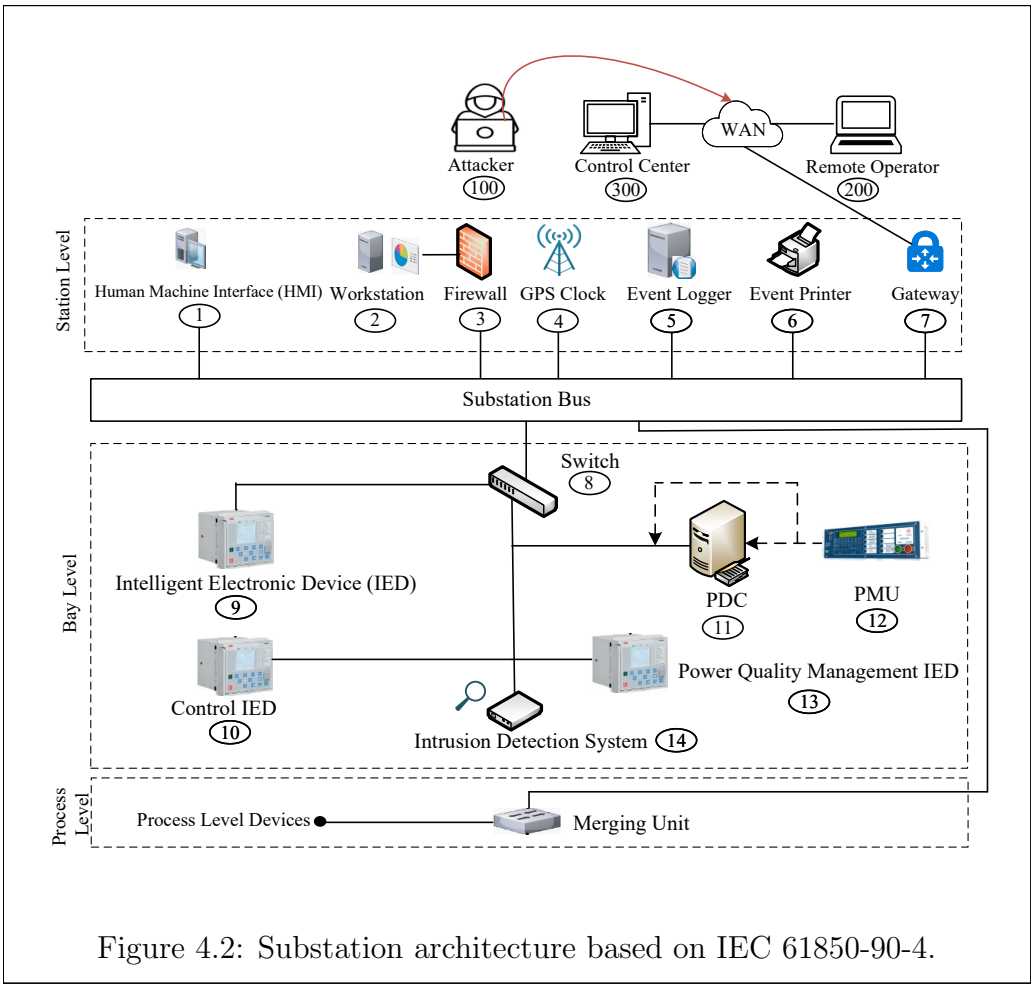


Figure 4.2: Substation architecture based on IEC 61850-90-4.

are identical. However, in practical scenarios where substations have different structures or communication links vary, separate BAGs should be constructed for those specific instances in the offline pre-processing phase. The probabilities derived from these BAGs can then be used as fixed parameters in subsequent calculations, ensuring the model remains adaptable to real-world power system diversity.

4.2.1 Substations Architecture and Data aggregation in Power Systems

The architecture of a substation, aligned with the International Electrotechnical Commission (IEC) 61850-90-4 standard, is shown in Fig. 4.2 [83]. This structure is designed to support data measurement and control within power networks and comprises intercon-

nected components that enhance the operation and monitoring of power grids. Central to the substation's measurement operations are PMUs (node 12), which are crucial for gathering real-time data. The units within the bay level, including PMUs and IEDs, are linked through a switch (node 8) to ensure continuous data flow within the substation. In some substations equipped with a PDC (node 11), the PDC collects PMU data from both local and neighboring substations. Communication with the control center (node 300) is conducted over a WAN, crucial for data transmission and remote control. The substation gateway (node 7) serves as the hub for gateway services. The HMI and workstations utilize SSH (Secure Shell) for remote maintenance and HTTP (HyperText Transfer Protocol) to deliver a user-friendly interface to substation operators. Additionally, the remote operator's machine supports both HTTP and SSH services [33].

The hierarchical structure of data aggregation in a power system is also depicted in Fig. 4.3: the data measured by PMUs in a substation is transmitted via a communication network to a substation equipped with PDCs, which then organize the data in chronological order. These organized measurements are subsequently forwarded to the Super PDC at the control center to be utilized for critical wide-area control and protection applications. As Fig. 4.3 shows, several pathways exist for manipulating the data coming from a set of PMUs. Attackers can (i) target the substations hosting the PMUs, (ii) exploit vulnerabilities in the communication network to alter PMUs data during transmission, or (iii) attack substations equipped with PDCs that aggregate data from multiple PMUs.

4.2.2 BAG for Compromising a Substation

Attack graphs depict the interdependencies among vulnerabilities and potential attack pathways. Fig. 4.4 displays the attack graph for compromising a substation and altering the data of its PMU. This graph consists of two types of nodes: exploits ($\mathbb{E}$) and conditions ($\mathbb{C}$). Exploits, represented by ovals, identify vulnerable hosts. For example, $<$V_SSH$, 100, 300>$ symbolizes the exploitation of an SSH vulnerability that enables an attacker to compromise the control center. An exploit can be executed only once all its requisite conditions are satisfied. Conditions, illustrated as borderless text, specify the prerequisites for exploiting vulnerabilities. These are generally categorized into three main types: connectivity ($\mathbb{N}$), privilege ($\mathbb{L}$), and service existence ($\mathbb{S}$), depicted in Fig. 4.4 in blue, red, and purple, respectively. The connectivity condition indicates the presence of a network path between two nodes in the graph, enabling an attacker to traverse the network. The privilege condition reflects the level of access or permissions an attacker needs to progress along a path, ensuring that the necessary privileges are acquired to advance further. The service existence condition involves the availability and operability of network

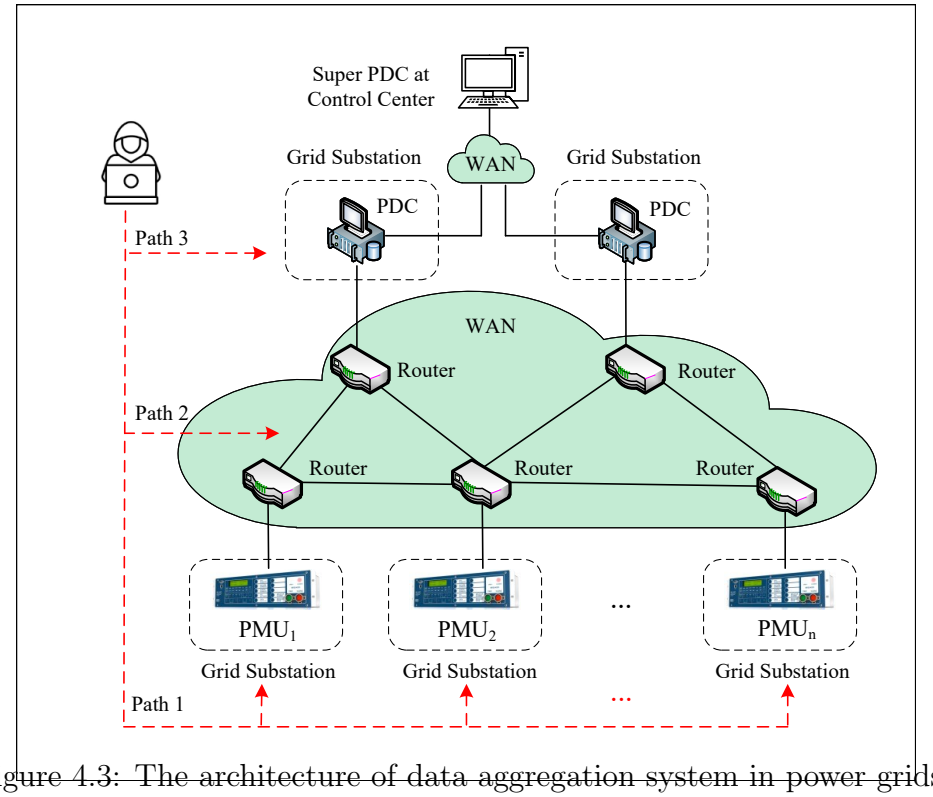


Figure 4.3: The architecture of data aggregation system in power grids.

services targeted by an attacker, ensuring that required services are active and accessible within the network [100]. A condition without a preceding exploit is termed an initial condition. Post-conditions are satisfied following the successful exploitation of a vulnerability. For instance, the privilege condition <root, 7> is fulfilled when an attacker takes advantage of any of the following exploits <V_Gateway, 300, 7> or <V_Gateway, 200, 7>.

Building on the foundational principles of attack graphs, BAGs utilize a probabilistic framework to assess the likelihood of intruders achieving their objectives. Estimating these probabilities involves two steps. Firstly, determining the likelihood of attackers independently executing each exploit node (i.e., $\mathbb{E}_i$), denoted as

$$p(\mathbb{E}_i \in \mathbb{E} | \mathbb{S}_i = T, \mathbb{N}_i = T, \mathbb{L}_i = T) \tag{4.18}$$

where $p(.)$ is the probability operator. Additionally, $\mathbb{S}_i = T$, $\mathbb{N}_i = T$, and $\mathbb{L}_i = T$ respectively denote that all connectivity, privilege, and service existence preconditions for exploit $\mathbb{E}_i$ are already met. In fact, (4.18) represents the probability of successfully executing an exploit when its preconditions are met. This thesis employs the CVSS [66] to

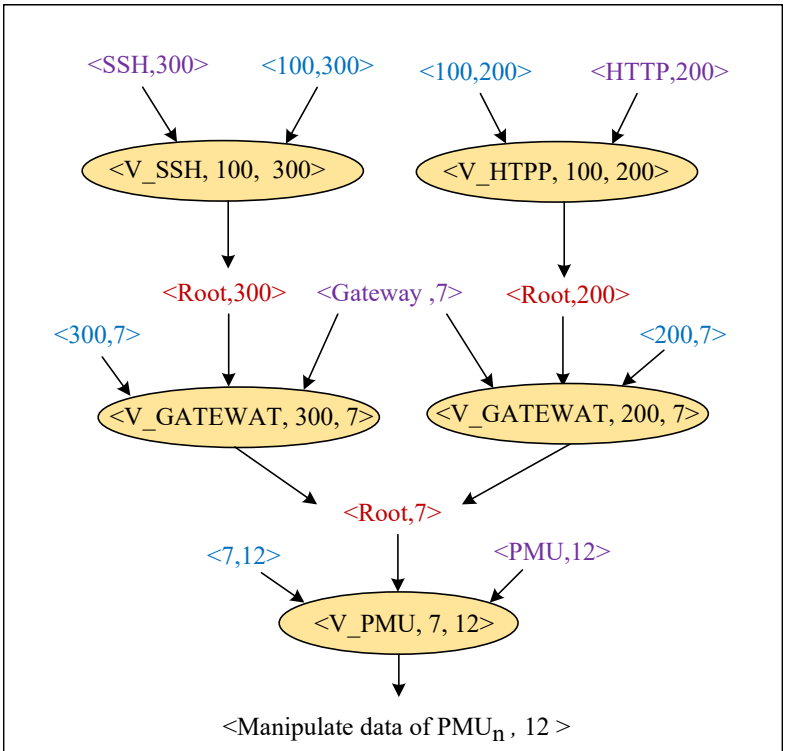


Figure 4.4: Attack graph For manipulating the data of PMU_n.

estimate exploit probabilities. For known vulnerabilities, the exploitation probability can be derived from the CVSS score calculator, which evaluates risk based on specific vulnerability characteristics [66]. In cases where no known vulnerabilities exist, CVSS incorporates zero-day vulnerabilities into its assessment. This ensures that CVSS not only considers vulnerabilities recognized by operators but also assigns a probability to unknown threats, strengthening the overall risk assessment framework.

In the subsequent step, conditional probabilities for each node—except initial conditions—are established to calculate overall probabilities and model the logical dependencies between the preconditions of an exploit and its successful execution. This framework imposes an "AND" logic for exploit nodes, requiring all preconditions to be met for the exploit to proceed. Conversely, privilege conditions are governed by an "OR" logic, indicating that the execution of any relevant exploit satisfies the precondition. Upon constructing the BAG for manipulating the data of PMU_n through compromising its substation, the probability of this data manipulation, denoted as $p(A\_PMU_n\_S_n)$, is derived via Bayesian inference. This methodology allows for the development of similar BAGs to estimate the probabilities

of manipulating data from other PMUs by targeting their respective substations. Additionally, a corresponding BAG can be created to assess the likelihood of altering the data of PMU_n by compromising its associated PDC (i.e., PDC_r), expressed as $p(A\_PMU_n\_PDC_r)$. A key distinction between the BAGs for PMUs and PDCs lies in the generally stricter security measures implemented at substations with PDCs, which tend to reduce the likelihood of successfully executing certain exploits.

4.2.3 BAG for Compromising a Communication Link

Fig. 4.5 presents the attack graph designed to compromise communication link m (i.e., CL_m), through which data from PMU_n is transmitted and potentially altered. To manipulate this data, an attacker must bypass security measures such as message encryption and network address locking that protect CL_m. These security vulnerabilities are represented by $\mathbb{E}_1$ to $\mathbb{E}_5$ in the graph, each aiming to acquire specific privileges ($\mathbb{L}_1$ to $\mathbb{L}_4$) within the network. The ultimate goal of the attack, depicted at the bottom of the graph, is to manipulate the data of PMU_n via CL_m. Achieving this objective requires that the attacker successfully obtains all listed privileges, and the probability of this comprehensive success is formulated as:

$$p(A\_PMU_n\_CL_m) = \prod_{i=1}^{4} p(\mathbb{L}_i = \text{T}) \tag{4.19}$$

The likelihood of successfully acquiring these privileges depends on the effectiveness of the security countermeasures in place, and can be calculated using:

$$p(\mathbb{L}_i = \text{T}) = \sum_{j \in N_{\mathbb{L}_i}} p(\mathbb{L}_i = \text{T} | \mathbb{E}_j) \cdot p(\mathbb{E}_j) \tag{4.20}$$

where $N_{\mathbb{L}_i}$ represents the set of countermeasures that must be bypassed to obtain privilege $\mathbb{L}_i$.

4.2.4 BAG for Compromising a Set of Critical PMUs

The previous subsections illustrated various strategies an attacker could employ to manipulate the data of a single PMU. To extend these tactics to a group of PMUs, an attacker might use one or several of these methods.

To thoroughly identify all feasible strategies for manipulating PMU data within a critical set, it is essential to examine every possible combination of compromised communication

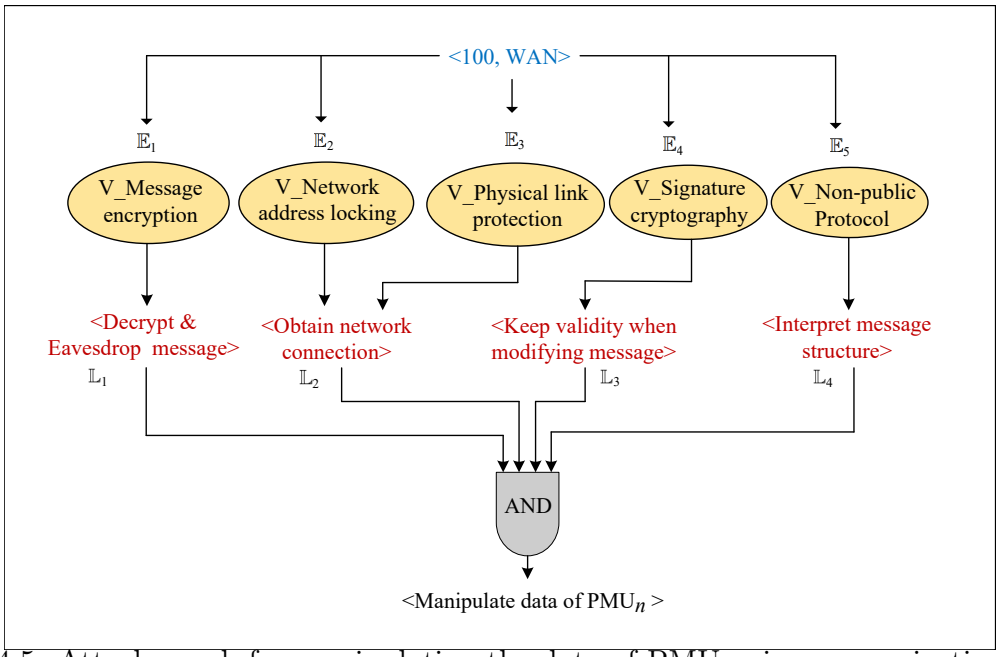


Figure 4.5: Attack graph for manipulating the data of PMU$_n$ via communication link m.

links, PMUs, and PDCs that could facilitate such manipulation. To this aim, the possible combination of compromised components for set Ω_l^s, where $s \in \mathcal{S}$, are stored in set O_l^s. Therefore, line l can be overloaded if any of the combinations in the following set are accessed

$$\Gamma_l = \bigcup_{s \in S} O_l^s \tag{4.21}$$

where $\Gamma_l = \{\Gamma_l^1, \Gamma_l^2, \ldots, \Gamma_l^I\}$ represents all possible unique sets of targets (i.e., PMUs, PDCs, and/or communication links) that can be compromised to alter the data of one of the critical sets of line l, and I represents the total number of these sets. Each Γ_l^i, where $1 \leq i \leq I$, specifies a distinct combination of compromised targets.

Therefore, the probability of overloading line l can be calculated using the following equation

$$p(A\_l) = \sum_{\Gamma_l^i \in \Gamma_l} p(\Gamma_l^i) \tag{4.22}$$

where $p(A\_l)$ is the probability of overloading and eventually tripping of line l. Additionally, $p(\Gamma_l^i)$ is the probability of accessing each combination, which can be calculated using the BAGs discussed in Sections 4.2.2 and 4.2.3, as follows

$$p(\Gamma_l^i) = \prod_{n \in \Gamma_l^i} p(A\_PMU_n\_S_n) \times \prod_{r \in \Gamma_l^i} p(A\_PMU_n\_PDC_r) \times \prod_{m \in \Gamma_l^i} p(A\_PMU_n\_CL_m) \quad (4.23)$$

where, n, r, and m in Γ_l^i represent the PMUs, PDCs, and communication links involved in each Γ_l^i, respectively. By substituting (4.23) into (4.22), the overall probability of overloading and eventually tripping of line l can be calculated.

4.3 Proposed Cyber-Physical Risk Metric and Proactive Mitigation Strategy

4.3.1 Cyber-Physical Risk Metric

This section introduces the proposed CPRM designed to evaluate the risk posed to the power system by SFDIAs. The CPRM systematically integrates two critical factors: the probability of cyberattack that can result in the loss of transmission lines, and the consequent physical impact of each loss on the stability and functionality of the grid. The proposed CPRM can be formulated as follows

$$CPRM = \sum_{l \in \mathcal{L}} PI(l) \times p(A\_l) \quad (4.24)$$

where $PI(l)$ represents the physical impact associated with the loss of transmission line l, and $p(A\_l)$ is calculated using (4.22). Typically, the impact of losing a transmission line is quantified by the amount of unserved load or the required load shedding. Beyond its impact on loads, the loss of a transmission line can also result in disconnection of a generator from the grid. Although such disconnections may not directly affect loads due to available reserve capacity, they can lead to significant economic losses, increased stress on other generators, and a diminished safety margin due to the higher demands placed on the remaining operational generators [8]. Therefore, the physical impact of losing line l is quantified as follows

$$PI(l) = \beta_1 \sum_{d \in \mathcal{D}} S_d - \beta_2 \sum_{g \in \mathcal{G}} C_g + \beta_3 \sum_{d \in \mathcal{D}} \sum_{k \in \theta^d} \max\left(0, 1 - \frac{\sum_{l \in \theta^d, l \neq k} P_l^{max}}{P_d}\right) \times P_d \quad (4.25)$$

where θ^d represents the set of transmission lines connected to load d. In this equation, the first term represents the total unserved load, the second term represents the available generation capacity, and the third term quantifies the system operational margin [8]. The coefficients β_1, β_2, and β_3 are weighting factors that represent the importance of each term.

4.3.2 Proactive Risk Mitigation strategy

The CPRM introduced in (4.24) offers a comprehensive assessment of the risk that SFDIAs pose to power systems. To mitigate the risk of SFDIAs, strategies can either reduce the probability or the physical impact of such attacks. Reducing the physical impact typically involves physical measures, such as altering the dispatch of generators, which incurs additional costs. Therefore, this paper primarily focuses on strategies that reduce the probability of SFDIAs that can result in losing a line, aiming for cost-effective cyber-security enhancements.

Based on (4.22) and (4.23), the probability $p(A\_l)$ is determined by the likelihood of compromising the components—PMUs, PDCs, and communication links—of each $\Gamma_l^i \in \Gamma_l$, which provide access to the data of the critical PMUs associated with line l. As these equations demonstrate, the overall probability of such an event highly depends on how the data is aggregated in the communication network. This is because the data aggregation structure determines the number of PDCs and communication links required for access to the set Γ_l^i. For example, if all critical PMUs of a line are connected to a single PDC, it is more likely for an attacker to gain access and overload the line compared to a scenario where they are connected to several PDCs. Thus, a power system's risk to SFDIAs can be minimized by reconfiguring the data aggregation structure. On this basis, this paper develops the following optimization problem to determine the optimal data aggregation structure for a given operating point

$$\underset{X,V,Y}{\text{Minimize}} \quad \text{CPRM} \tag{4.26}$$

The decision variables involved in this problem are defined as follows

- $X = [x_{n,r}]$, a matrix where each element $x_{n,r}$ for $n \in \mathcal{N}$ and $r \in \mathcal{R}$ is a binary variable indicating whether PMU_n is connected to PDC r (1 if connected, 0 otherwise).
- $V = [v_{n,r,q}]$, a three-dimensional binary matrix where each element $v_{n,r,q}$ for $n \in \mathcal{N}$, $r \in \mathcal{R}$, and $q \in \mathcal{Q}_{n,r}$ denotes whether communication path q (which comprises a sequence of routers and communication links) connects PMU_n to PDC_r (1 if connects,

0 otherwise). The set $\mathcal{Q}_{n,r}$ encompasses all feasible communication paths between PMU_n and PDC_r.

- $Y = [y_{r,f}]$, a binary matrix where each element $y_{r,f}$ for $r \in \mathcal{R}$ and $f \in \mathcal{F}_r$ denotes whether the communication path f (which comprises a sequence of routers and communication links) connects PDC_r to the control center (1 if connects, 0 otherwise). The set $\mathcal{F}_r$ encompasses all feasible communication paths between PDC_r and control center.

The objective function of (4.26) should be minimized subjected to the following constraints:

$$\sum_{r \in \mathcal{R}} x_{n,r} = 1 \quad \forall n \in \mathcal{N} \tag{4.27}$$

$$v_{n,r,q} \leq x_{n,r} \quad \forall n \in \mathcal{N},\ \forall r \in \mathcal{R},\ \forall q \in \mathcal{Q}_{n,r} \tag{4.28}$$

$$\sum_{q \in \mathcal{Q}_{n,r}} v_{n,r,q} = x_{n,r} \quad \forall n \in \mathcal{N},\ \forall r \in \mathcal{R} \tag{4.29}$$

$$\sum_{f \in \mathcal{F}_r} y_{r,f} = 1 \quad \forall r \in \mathcal{R} \tag{4.30}$$

$$\sum_{n \in \mathcal{N}} x_{n,r} \leq CA_r \quad \forall r \in \mathcal{R} \tag{4.31}$$

where CA_r represents the maximum number of PMUs that can be connected to PDC_r. Constraint (4.27) ensures that each PMU is connected to exactly one PDC. Meanwhile, constraint (4.28) ensures that $v_{n,r,q} = 1$ only if $x_{n,r} = 1$, meaning a path q exists between PMU_n and PDC_r only if PDC_r is assigned to PMU_n. Moreover, constraint (4.29) guarantees that exactly one path connects PMU_n to its designated PDC. Similarly, (4.30) ensures that there is a path between each PDC and the control center. Finally, (4.31) limits the number of PMUs connected to each PDC. In addition to the above constraints, the following one is defined to prevent data aggregation structures that could cause long communication delays, potentially resulting in undesirable packet dropouts:

$$v_{n,r,q} \cdot t_{n,r,q} \leq T_r + \min\{v_{n,r,q} \cdot t_{n,r,q}\} \quad \forall n \in \mathcal{N}, \forall r \in \mathcal{R}, \forall q \in \mathcal{Q}_{n,r} \tag{4.32}$$

where $t_{n,r,q}$ is the processing and communication delay for sending the measurements from PMU_n to PDC_r through the communication path q. Furthermore, T_r represents the waiting time of PDC_r for subsequent data packets after the first packet arrives. The term $\min\{v_{n,r,q} \cdot t_{n,r,q}\}$ denotes the arrival time of the first packet at PDC_r.

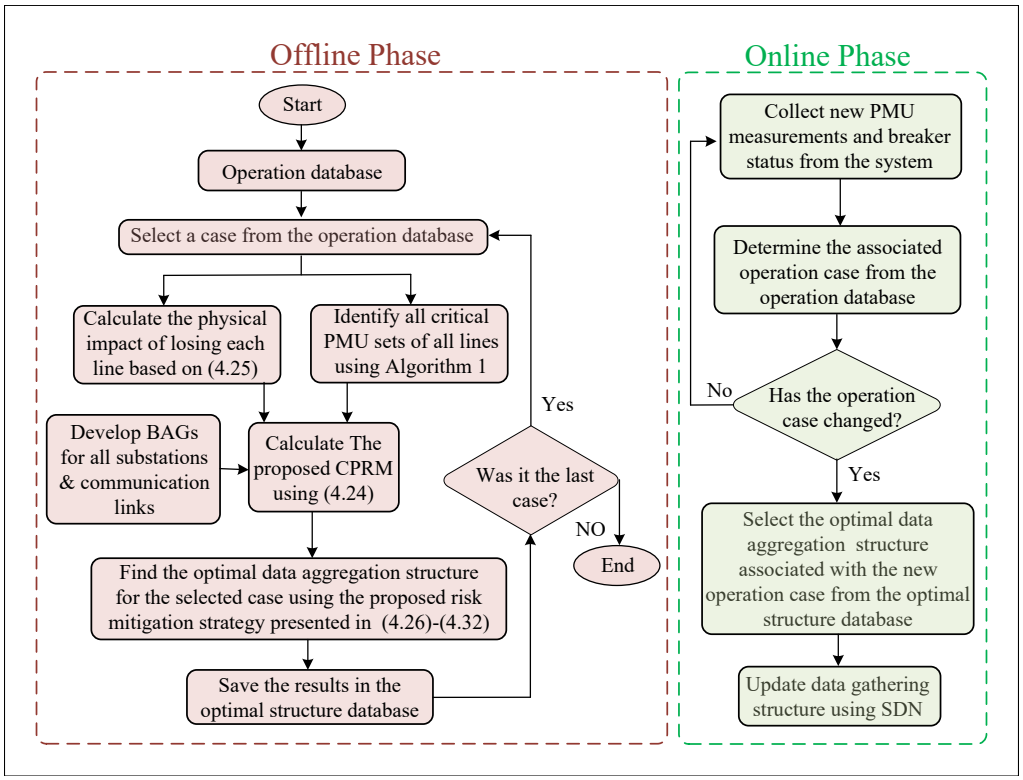


Figure 4.6: The proposed software defined networking-based data aggregation reconfiguration scheme

4.3.3 SDN-Based Implementation of the Proposed Risk Mitigation Strategy

All previous discussions have focused on a specific operating point of the power system. However, as system operating points change, it is crucial to continuously evaluate the CPRM for each new condition and update the data aggregation structure through the proposed risk mitigation strategy to minimize the risk of SFDIAs. In this context, this paper proposes an SDN-based data aggregation reconfiguration scheme, illustrated in Fig. 4.6, which dynamically adjusts the data aggregation structure in real-time.

The proposed scheme operates in two phases: offline and online. In the offline phase, all potential operating points—resulting from variations in load, generation, or system configuration—are predicted and stored in a database. Historical data plays a crucial role in this prediction, supplemented by advanced load forecasting methods that estimate demand for the upcoming hours or even the next day [23, 9, 7]. For each operating point, the

physical impact of losing each transmission line is assessed using equation (4.25), and all critical PMU sets for all lines are identified using Algorithm 2. Then, the CPRM for each case is calculated using equation (4.24), based on the identified physical impacts, critical PMU sets, and BAGs developed for substations and communication links. Subsequently, the optimal data aggregation structure for each case is determined using the proactive mitigation strategy outlined in equations (4.26) to (4.32). Finally, the optimal data aggregation structures are stored in the optimal structure database for future use. Therefore, all resource-intensive tasks are precomputed and stored in a database during the offline phase, eliminating the need for complex calculations in the online phase and thus avoiding latency in live operations.

On the other hand, in the online phase, the system continuously collects new PMU measurements and breaker statuses, and subsequently identifies the associated operational case from the database. The online phase relies solely on data already collected in power grid control centers, and therefore does not impose any additional data extraction demands on the system. If the operational case has changed, the system selects the appropriate data aggregation structure associated with the new operational case from the optimal structure database and sends this information to the SDN controller. The SDN controller is able to reconfigure the data aggregation system in under 10 milliseconds for small systems and under 50 milliseconds for large systems with over 500 switches [38, 51]. It is noteworthy to mention that if the operational case has not changed, the system maintains the current data aggregation structure until a change is detected. If an operational condition is not available in the database, its corresponding optimal data aggregation structure should be determined by executing the proposed risk mitigation strategy. The results should then be saved in the database and transmitted to the SDN controllers.

4.4 Performance Evaluation

This section begins by introducing the test systems—the IEEE 39-bus and 57-bus systems—followed by an evaluation of the effectiveness of the proposed CPRM and the corresponding mitigation strategy on these systems.

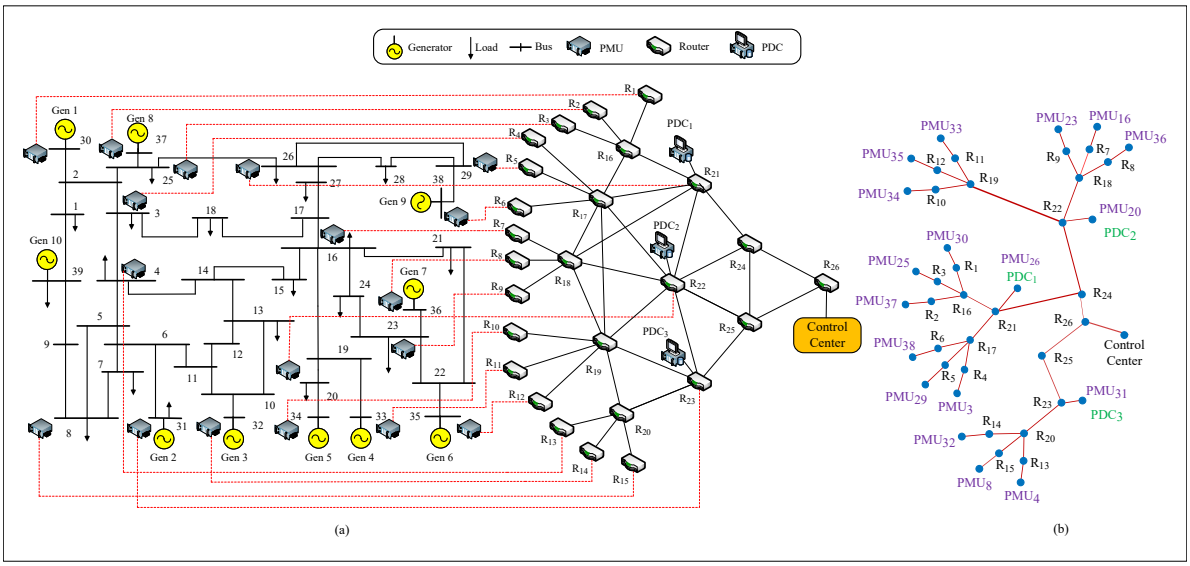


Figure 4.7: The IEEE 39 bus test system: (a) cyber and physical layers, (b) data aggregation structure

4.4.1 Test Systems

IEEE 39-Bus System

The physical-layer data of this test system (e.g., admittance matrix and generator specifications) are available in the MATPOWER toolbox [1]. The cyber-layer includes 15 PMUs, which are placed according to [50], and are shown in Fig. 4.7a. The PMUs are specified by their associated bus numbers, e.g., PMU on Bus 8 is denoted by PMU_8. Additionally, this system has three substations equipped with PDCs: PDC_1, PDC_2, and PDC_3, which are placed at Buses 26, 20, and 31, respectively. The communication network (Fig. 4.7a) contains 26 routers labeled R_1 to R_{26} and 34 communication links between the routers. A communication link between routers x and y is represented by $CL_{x,y}$. The data aggregation structure within this test system is shown Fig 4.7b. For instance, PMU_{25} uses R_3 to send its data to R_{16} and then R_{21} to reach PDC_1. This PDC, which collects data from PMUs installed at buses 3, 25, 26, 29, 30, 37, and 38, uses R_{21}, R_{24}, and R_{26} to send its data to the control center.

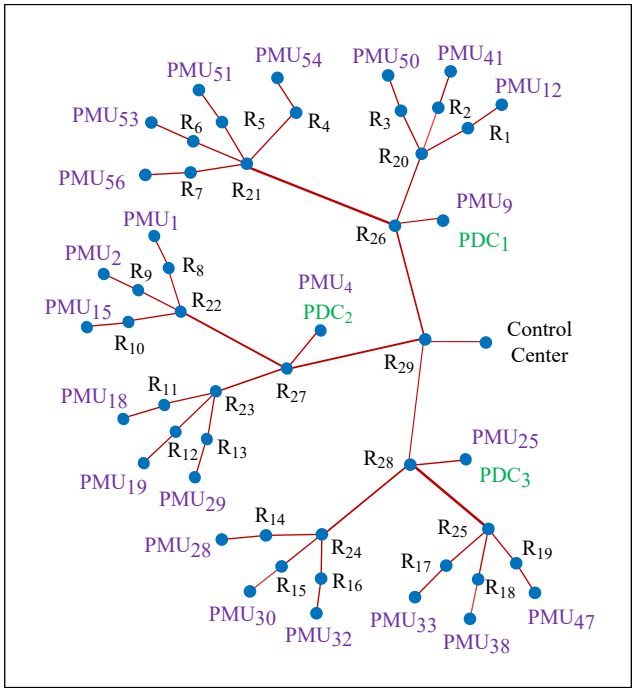


Figure 4.8: The original data aggregation structure for IEEE 57-bus test system.

IEEE 57-Bus System

Figure 2.5 in Section 2.5.1 illustrates the IEEE 57-bus test system, whose physical-layer data (e.g., the admittance matrix and generator specifications) are available in the MATPOWER toolbox [1]. The cyber-layer of the system includes 22 PMUs, which are placed according to [50]. Additionally, the system comprises three substations equipped with PDCs: PDC_1, PDC_2, and PDC_3, located at Buses 9, 4, and 25, respectively. The data aggregation structure within this test system is illustrated in Fig 4.8.

4.4.2 Performance Evaluation on IEEE 39-Bus System

Calculating the CPRM

This section calculates the proposed CPRM for the IEEE 39-bus system introduced in Section 4.4.1, whose load profile is depicted in Fig. 4.9. To determine the critical PMU sets, ζ is set equal to 1.5 [28, 27]. The rational behind this threshold is that according to NERC Standard PRC-023-1 [5], protective devices on power lines and transformers should have a tripping threshold set at no less than 150% of their maximum capacity. However,

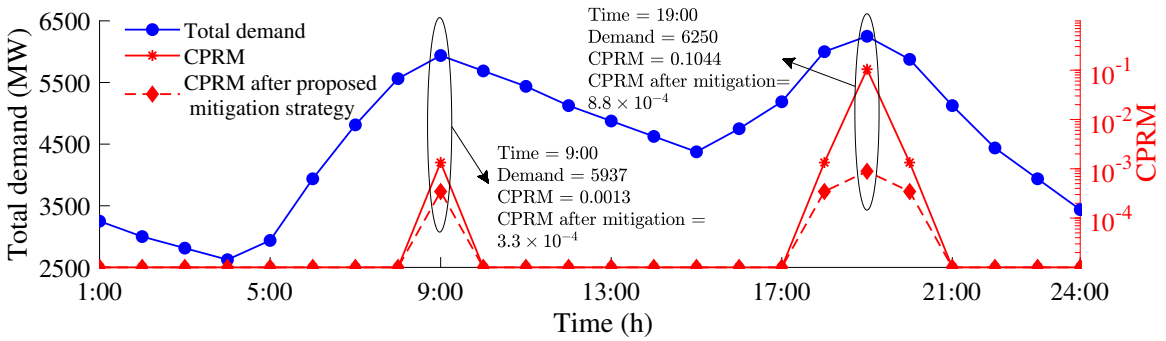


Figure 4.9: The daily total demand and CPRM of the IEEE 39 bus test system.

in practice, this threshold can be lower [28]. The bi-level optimization problems described in Algorithm 2 are solved for each line of the test system across all 24 hours, aiming to identify all critical sets of PMUs (denoted by Ω_l^s) at each time necessary to overload each line. However, due to space constraints, this paper elaborates deeply only on the results obtained for hour 19:00, i.e., when the load is at its peak. For the selected hour, it is observed that, except for lines 3 and 27, all other lines cannot be overloaded, even if all PMU data are available to the attacker for manipulation. Table 4.1 lists the critical PMU sets for lines 3 and 27. As seen in this table, lines 3 and 27 have 14 and 6 critical sets, respectively. For example, if the attacker gains access to the PMUs installed at buses 3, 4, 8, 16, and 25, they can manipulate the data to overload Line 3. Similarly, accessing PMUs at buses 4, 8, 16, 20, 26, and 29 enables the attacker to overload Line 27.

To calculate the probabilities of manipulating the data of PMUs in the critical sets shown in Table 4.1, BAGs for substations and communication links are developed as explained in Section 4.2. To determine the likelihood of executing each exploit, i.e, (4.18), the CVSS scores are normalized, as shown in Table 4.2. For certain services in the network, such as SSH, HTTP and gateway, when there are no known exploits, zero-day exploits—which are not publicly known—are considered. Given the nature of zero-day exploits, their CVSS score is generally assumed to be 0.8 [100]. Bayesian inference is conducted for the developed attack graphs, and the probabilities of attacking PMUs, PDCs, and communication links are determined as listed in Table 4.3.

In the next step, to calculate the probability of accessing the critical PMU sets of a specific line, set Γ_l is determined based on (4.21). Table 4.4 demonstrates all combinations of targets (denoted by $\Gamma_l \in \Gamma_l^i$) for $l = \{3, 27\}$. Then, the probability of accessing each Γ_l^i set is calculated using (4.23). The overall probabilities of overloading lines 3 and 27 are determined using (4.22), as shown in Table 4.4. For example, accessing PMU_4, PDC_1, and

Table 4.1: The critical PMUs of IEEE 39-bus test system for overloading lines 3 and 22 for hours 19:00.

Line	Ω_l^s
3	{3, 4, 8, 16, 25}, {3, 4, 8, 16, 20}, {3, 4, 8, 16, 26} {4, 8, 16, 20, 25, 26}, { 8, 16, 20, 25, 26, 29} {3, 8, 16, 20, 25, 26} ,{8, 16, 20, 23, 25, 26} {3, 8, 16, 20, 23, 25, 31}, {3, 8, 16, 23, 25, 26, 29} {3, 8, 16, 23, 25, 26, 31}, {3, 8, 16, 23, 25, 26, 29 } {3, 8, 16, 20, 23, 26, 29}, {3, 4, 16, 20, 25, 26, 29} {3, 8, 16, 20, 26, 29, 31}
27	{4, 8, 16, 20, 26, 29}, {3, 8, 16, 20, 26, 29} {8, 16, 20, 25, 26, 29}, {3, 16, 20, 25, 26, 29} {4, 16, 20, 25, 26, 29}, {3, 4, 16, 20, 23, 26, 29}

Table 4.2: CVSS Score.

Vulneribilty	CVSS/10	vulneribilty	CVSS/10
V_SSH	0.08	V_Message encryption	0.08
V_HTTP	0.08	V_Network address locking	0.08
V_Gateway	0.08	V_Physical link protection	0.08
V_PMU	0.9	V_Signature cryptography	0.08
V_PDC	0.3	V_Non-public Protocol	0.08

Table 4.3: Probability of attacking PMUs, PDCs, and communication links.

Attack point	$p(A\_PMU_n\_S_n)$	$p(A\_PMU_n\_PDC_k)$	$p(A\_PMU_n\_CL_m)$
Probability	0.0114	3.8×10^{-3}	7.6×10^{-5}

PDC_2 provides access to the data of PMUs 3, 4, 16, 20, 25, 26, and 29, which is necessary and enough for stealthily overloading Line 3, and the probability of this access is 1.6×10^{-7}. The overall probability of accessing the components using which an attacker can overload Line 27 is 9×10^{-5}. It should be noted that in Table 4.4, the Γ_l^i sets that result in $p(\Gamma_l^i)$ being two orders of magnitude smaller than the others are ignored. For example, if a Γ_l^i entails manipulating one communication link, one PDC, and one PMU, the probability of this combination is 3.3×10^{-9}, which is significantly lower compared to another that involves only one communication link, with a probability of 7.6×10^{-5}.

Table 4.4: Calculation of the proposed CPRM for hour 19:00.

Line	Γ_l^i	$p(\Gamma_l^i)$	$p(A\_l)$	$PI(l)$	$CPRM$
3	PMU_4, $CL_{24,26}$	8.6×10^{-7}	2.6×10^{-6}	0	0.1044
	PMU_8, $CL_{24,26}$	8.6×10^{-7}			
	PDC_3, $CL_{24,26}$	2.8×10^{-7}			
	PMU_3, PDC_2, PDC_3	1.6×10^{-7}			
	PMU_4, PDC_1, PDC_2	1.6×10^{-7}			
	PMU_8, PDC_1, PDC_2	1.6×10^{-7}			
	PMU_{16}, PDC_1, PDC_3	1.6×10^{-7}			
	...	Trivial			
27	$CL_{24,26}$	7.6×10^{-5}	9×10^{-5}	1160	
	PDC1 & 2	1.4×10^{-5}			
	...	Trivial			

To determine the CPRM for hour 19:00, the physical impact of losing each line, denoted by $PI(l)$, is calculated based on (4.25). The coefficients β_1, β_2, and β_3 in (4.25) are considered to be 1, 0.1, and 0.1, respectively, giving a higher weight to load shedding. The $PI(l)$ for each line is also presented in Table 4.4. Then, the CPRM is determined based on (4.24) and is also presented in Table 4.4. The CPRM value is 0.1044, representing the quantified risk of cyberattacks for this hour and data aggregation structure. A similar process can be applied to all other hours to find their CPRM values (Fig. 4.9). As shown in Fig. 4.9, the CPRM is non-zero only during the four peak-load hours, when the lines can become overloaded and their tripping has a significant impact. The obtained CPRM values will be utilized in the next subsection to optimize the data aggregation structure and minimize the risk of SFDIAs.

Proactive Risk Mitigation Strategy

As discussed in Section 4.3.2, the risk of SFDIAs can be reduced without imposing extra costs by changing the structure of the data aggregation system in power grids. This is because the data aggregation structure highly influences the probability of an attacker gaining access to the sets of PMUs required for overloading and eventually tripping a line. To determine the optimal data aggregation structure during hour 19:00, the proposed optimization problem, i.e., (4.26)-(4.32), is solved. Fig. 4.10 demonstrates the optimized data aggregation structure for this hour. Compared to the non-optimal data aggregation

Table 4.5: Calculation of the proposed CPRM at hour 19:00 for the IEEE 39-bus system.

Line	Γ_l^i	$p(\Gamma_l^i)$	$p(A\_l)$	$Pl(l)$	$CPRM$
3	$CL_{25,26}$	5.7×10^{-5}	7.1×10^{-5}	0	8.8×10^{-4}
	PDC_2, PDC_3	1.4×10^{-5}			
	PMU_8, PDC_1, PDC_2	1.6×10^{-7}			
	...	Trivial			
27	PDC_1, $CL_{25,26}$	2.8×10^{-7}	7.6×10^{-7}	1160	
	PMU_3, PDC_1, PDC_2	1.6×10^{-7}			
	PMU_4, PDC_1, PDC_2	1.6×10^{-7}			
	PMU_8, PDC_1, PDC_2	1.6×10^{-7}			
	...	Trivial			

structure shown in Fig. 4.7, in the new configuration, PMU_3 transmits its measurements to PDC_3 via communication links $CL_{17,19}$ and $CL_{19,23}$, whereas previously it sent data to PDC_1 through communication link $CL_{17,21}$. Moreover, PDC_2 uses R_{25} instead of R_{24} to reach the control center. These modifications in the data aggregation structure mainly increases the number of components that must be manipulated to overload and trip an impactful line, thereby significantly decreasing the probability of such an event. As shown in Table 4.5, after modifying the data aggregation structure, $p(A\_27)$ is reduced from 9×10^{-5} to 7.6×10^{-7}. This reduction leads to a decrease in the CPRM's value to 8.8×10^{-4}, reducing the CPRM to nearly 1% of its previous value.

Similarly, the optimal data aggregation structure and the corresponding CPRM for all other hours are illustrated in Fig. 4.9. As this figure demonstrates, the proposed strategy significantly mitigates the risk of cyberattacks. For instance, by adjusting the data aggregation structure at hour 9:00 from the configuration shown in Fig. 4.7-(b) to the one in Fig. 4.11, the CPRM decreases from 1.3×10^{-3} to 3.4×10^{-4}.

4.4.3 Performance Evaluation on IEEE 57-Bus System

Calculating the CPRM

This section calculates the proposed CPRM for the IEEE 57-bus system introduced in Section 4.4.1, whose load profile is depicted in Fig. 4.12. To this end, the bi-level optimization problems described in Algorithm 2 are solved for each line of the test system across all 24 hours, identifying the critical PMU sets required to overload each line at each time.

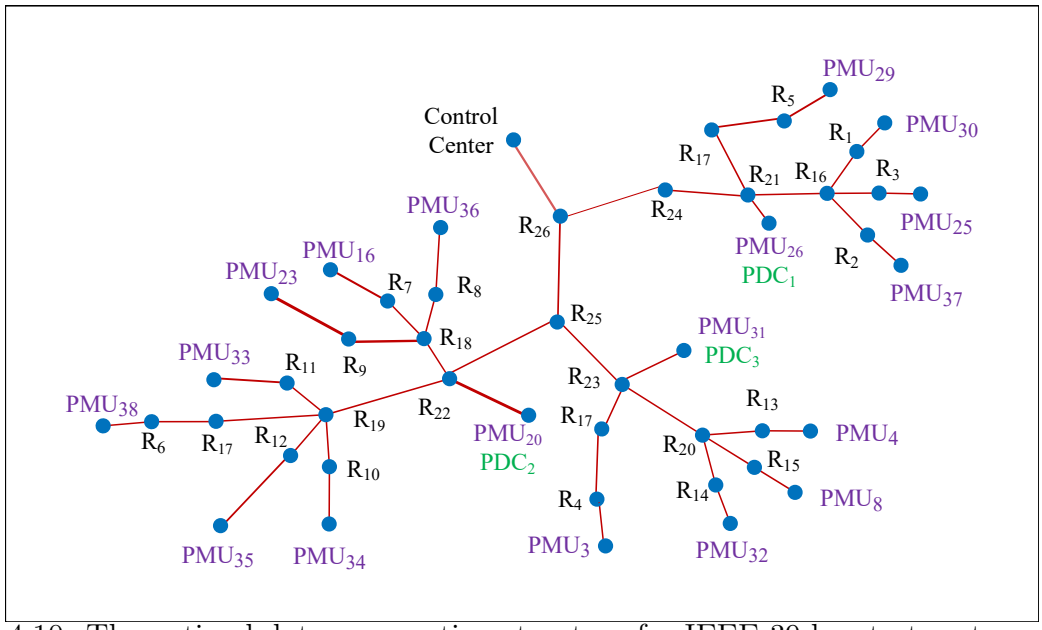


Figure 4.10: The optimal data aggregation structure for IEEE 39-bus test system at hour 19:00.

As an illustrative example, some of the sets corresponding to hour 19:00 (peak hour) are presented in Table 4.6. Subsequently, the probability of accessing to these critical PMU sets for each line, denoted as $p(A\_l)$, is calculated. These probabilities for hour 19:00 are provided in Table 4.7 as an example. Using these probabilities and the physical impact associated with the loss of transmission lines, i.e., $PI(l)$, the CPRM for each hour is computed. The CPRM values of IEEE 57-Bus system for the 24-hour period are shown in Fig. 4.12.

Proactive Risk Mitigation Strategy

To determine the optimal data aggregation structure, the proposed optimization problem, i.e., (4.26)-(4.32), is solved for the test system across the all 24 hours. The CPRM values after applying the proposed risk mitigation strategy are shown in Fig. 4.12 with the dashed red line. As seen in the figure, the proposed risk metric has been reduced significantly after hour 5:00. For instance, at hour 19:00, the CPRM has been reduced from 0.349 to 0.0102. The optimal data aggregation configuration for this hour is shown in Fig. 4.13.

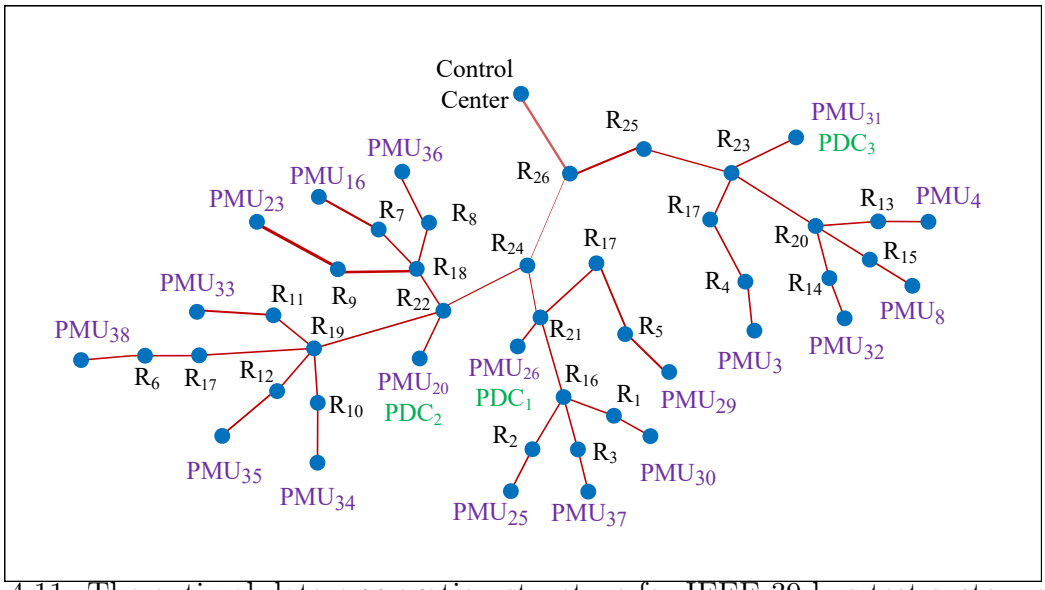


Figure 4.11: The optimal data aggregation structure for IEEE 39-bus test system at hour 9:00.

Table 4.6: The critical PMUs of IEEE 57-bus test system for overloading lines 3, 8 and 22 for hours 19:00.

Line	Ω_l^s
3	{1, 2, 4, 9, 12, 15, 18, 29, 30, 38, 41, 47, 51, 53, 54, 56}, {1, 2, 4, 9, 12, 15, 18, 29, 32, 38, 41, 47, 51, 53, 54, 56}, {1, 4, 9, 12, 15, 18, 28, 29, 32, 38, 41, 47, 50, 51, 53, 54, 56}, {1, 4, 9, 12, 15, 18, 29, 30, 32, 38, 41, 47, 50, 51, 53, 54, 56}, {1, 4, 9, 12, 15, 18, 25, 28, 29, 38, 41, 47, 50, 51, 53, 54, 56}, ...
8	{4, 9, 12, 29, 41}, {4, 9, 12, 28, 41}, {4, 9, 12, 41, 54}, {4, 9, 12, 30, 41}, {4, 9, 12, 41, 53}, {4, 9, 12, 38, 41}, {4, 9, 12, 15, 41}, {4, 9, 12, 30, 41}, {4, 9, 12, 41, 53}, {4, 9, 12, 38, 41}, {4, 9, 12, 15, 41}, {4, 9, 12, 15, 25, 56}, {1, 9, 12, 15, 41, 54}, {1, 9, 12, 15, 51, 56}, ...
22	{1, 9, 12, 15, 29, 41, 53, 54}, {1, 9, 12, 29, 41, 53, 54, 56}, {4, 9, 12, 29, 41, 53, 54, 56}, {9, 12, 29, 41, 51, 53, 54, 56}, {4, 9, 12, 18, 19, 29, 41, 53, 54}, {1, 9, 12, 15, 29, 47, 53, 54, 56}, {4, 9, 12, 15, 28, 29, 41, 53, 54}, {1, 9, 12, 28, 29, 41, 51, 53, 54}, {4, 9, 12, 15, 25, 29, 41, 53, 54}, {4, 9, 12, 29, 32, 41, 50, 53, 54}, ...

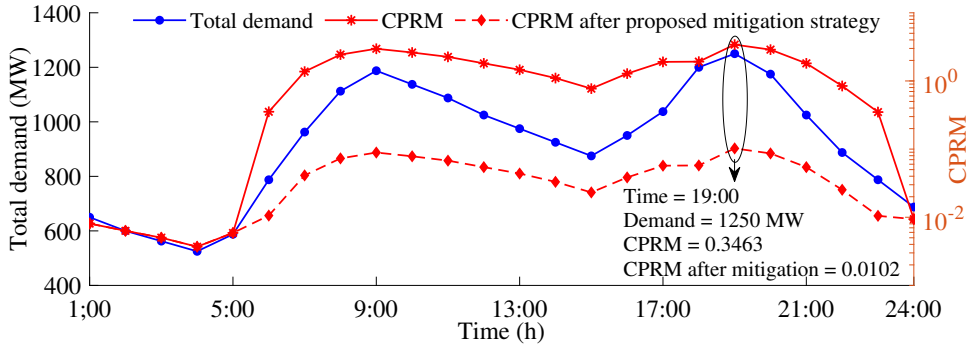


Figure 4.12: The daily total demand and CPRM of the IEEE 57-bus test system.

Table 4.7: Calculation of the proposed CPRM at hour 19:00 for the IEEE 57-bus system.

Line	Γ_l^i	$p(\Gamma_l^i)$	$p(A\_l)$	$PI(l)$	$CPRM$
3	PDC_1, PDC_2, PDC_3	5.4×10^{-8}	5.7×10^{-8}	0	0.346
	PDC_1, $CL_{27,29}$, $CL_{28,29}$	1.09×10^{-9}			
	PDC_2, $CL_{26,29}$, $CL_{28,29}$	1.09×10^{-9}			
	PDC_3, $CL_{26,29}$, $CL_{27,29}$	1.09×10^{-9}			
	...	Trivial			
8	PDC_1	3.8×10^{-3}	3.8×10^{-3}	89.8	
	$CL_{26,29}$	7.6×10^{-5}			
	PMU_9, PMU_{12} , PDC_2	4.9×10^{-9}			
	...	Trivial			
22	PMU_{29}, PDC_1	4.3×10^{-5}	5.7×10^{-5}	89.8	
	PDC_1, PDC_2	1.4×10^{-5}			
	...	Trivial			

4.5 Conclusion

A novel CPRM based optimal data aggregation scheme was proposed in this paper to assess and mitigate the risks of power systems to SFDIAs that can overload and trip transmission lines. The CPRM was developed through a three-step process: identifying all critical PMU sets by solving multiple bi-level optimization problems, constructing BAGs for each substation and communication link to determine the probability of compromising each critical PMU set, and integrating the obtained probabilities with the physical impact

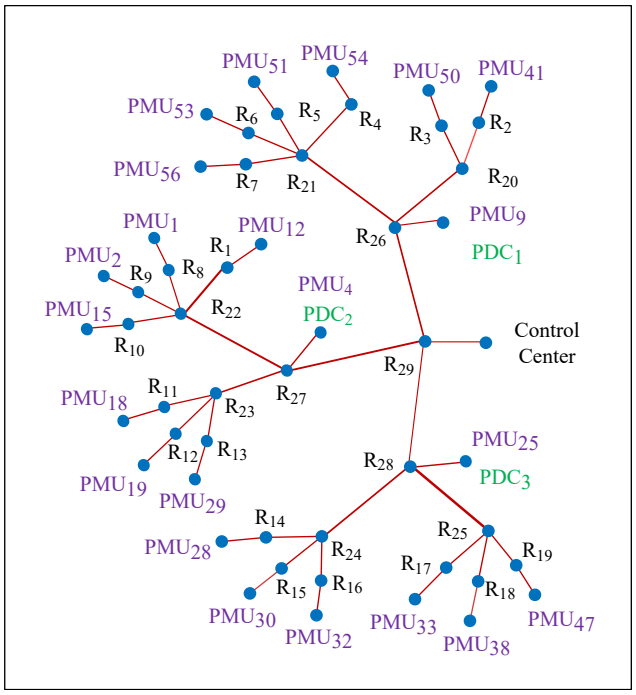


Figure 4.13: The optimal data aggregation structure for IEEE 57-bus test system at hour 19:00.

of line outages. Based on this metric, a proactive risk mitigation strategy was developed to establish the optimal data aggregation structure within the power system's cyber-layer, significantly reducing the risk of SFDIAs and boosting system resilience. Furthermore, a novel SDN-based DAR scheme was introduced to dynamically adjust the cyber-layer configuration in response to operational changes. These strategies together bolstered the cyber-physical security framework of power systems, providing a comprehensive approach to mitigate the risks associated with SFDIAs.

Chapter 5

Cyber-Resilient Distance Protection

Substations are currently undergoing a significant digital transformation aimed at enhancing operational efficiency and system reliability. This transformation is characterized by the integration of the IEC 61850 standard, which facilitates substation automation by standardizing communication protocols across IEDs. While the digitization of substations offers substantial benefits in terms of improved automation and the management of protection, control, and asset systems, it also introduces complex cybersecurity challenges that require careful consideration [89]. Among the devices in substations, protective relays for transmission lines are at particularly high risk of being targeted by cyberattacks. This is especially concerning because successful attacks on these relays have been shown to trigger major cascading failures, resulting in severe disruptions across the power grid [73]. Consequently, ensuring the robust security of these protective relays against cyber threats within substations is crucial.

As discussed in Section 1, although several studies have focused on the cybersecurity of protective relays — especially LCDR relays — in substations [14, 15, 52, 74, 13, 75], comprehensive research on the cybersecurity of distance protection schemes remains limited, particularly with respect to pilot signal vulnerabilities and scenarios in which measurements within a substation are manipulated.

To address this gap, this chapter first demonstrates the vulnerability of distance protection schemes to cyberattacks targeting pilot signals and substation measurements. It then proposes a cyber-resilient protection scheme that activates upon detecting an intrusion within a substation, temporarily replacing distance protection to maintain continuous and reliable transmission line protection, even when all substation-based measurements and communication links are compromised. The proposed scheme relies on a dedicated hard-

wired current measurement obtained directly from a separate protection core of the line's CT, bypassing vulnerable merging units and the internal substation network. Leveraging TWs as the natural signatures of real faults, the proposed method mimics the zone-based fault detection of distance relays to maintain coordination with upstream and downstream relays. To localize fault zones, a RF classifier is trained on the attenuation patterns of TWs frequency components as they propagate from fault locations to the line terminal. Since attenuation characteristics depend on both frequency and travel distance, the trained RF classifier accurately identifies the fault zone by extracting frequency-related features from the first TW using a wavelet transform and analyzing its attenuation patterns. Based on this RF classifier, the proposed protection scheme provides zone-based protection as a substitute for distance relays during cyber intrusions.

On this basis, this chapter is organized as follows. First, Section 5.1 illustrates, through a case study, that distance protection schemes within digital substations are highly vulnerable to false data injection attacks targeting SV or pilot signal messages. Section 5.2 presents the fundamental equations governing TW propagation and explains how each frequency component of a TW is attenuated depending on both its frequency and the distance traveled, with higher-frequency components experiencing more significant attenuation. To support a more effective analysis of these frequency-dependent characteristics, the wavelet transform is then introduced as a suitable tool for decomposing TWs into meaningful frequency bands for detailed examination. Section 5.3 first provides a brief background on the RF classifier and then proposes a cyber-resilient protection scheme designed to activate in response to detected cyber intrusions. Section 5.4 evaluates the proposed scheme for fault zone detection under TW attenuation patterns in the presence of cyberattacks. Finally, Section 5.5 concludes the chapter.

5.1 Problem Statement

This section begins with a detailed analysis of the architecture of digital substations, emphasizing potential attack paths that could be exploited to compromise the data integrity of distance relays. It then illustrates how this compromised data could lead to the maloperation of distance relays.

5.1.1 Digital Substation Structure and Potential Attack Paths

The architecture of a digital substation, designed in accordance with the IEC 61850-90-4 standard, is illustrated in Fig. 5.1. As depicted, substations are structured into four hier-

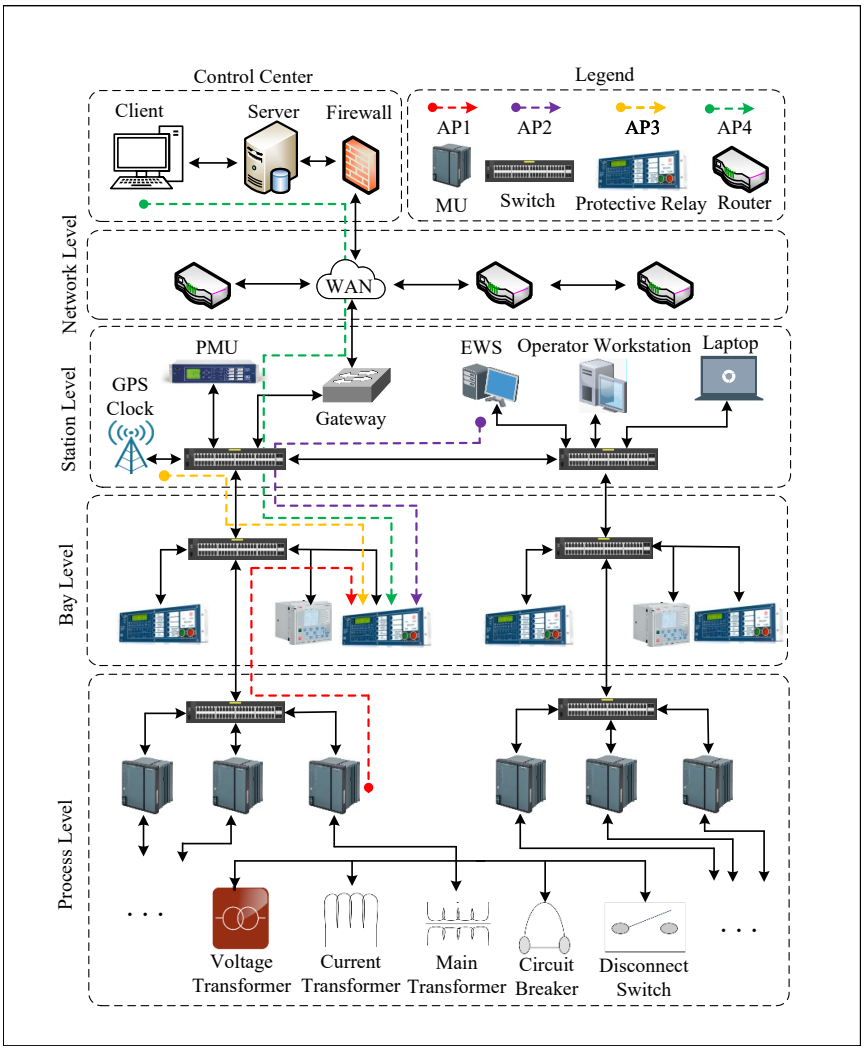


Figure 5.1: Structure of a digital substation and associated attack paths.

archical levels, each serving distinct functions to ensure efficient operation and control. At the process level, sensors and actuators interact directly with primary equipment, collecting raw data and executing real-time control commands. This level forms the foundation of the substation's operational framework. The bay level processes the data received from the process level, enabling critical local protection and control decisions. Above this, the station level integrates substation-wide operations through centralized systems such as SCADA, ensuring cohesive monitoring and management. Finally, the network level oversees all communication channels, facilitating secure and reliable data exchange between substations to maintain grid stability and responsiveness [83].

The protection system is a critical component of this architecture. At the process level, MUs collect analog data from CTs and VTs, converting it into digital signals. These digital signals are then transmitted to protective relays at the bay level via the IEC 61850 substation Local Area Network (LAN) using SV messages. For comprehensive protection, communication-assisted protection systems rely on the network level to exchange data with remote substations. This is achieved through the use of GOOSE and SV messages, enabling coordinated and timely responses across the grid. By leveraging the hierarchical structure and communication protocols of the digital substation, the protection system ensures rapid fault detection, isolation, and recovery, thereby safeguarding the stability and reliability of the power system.

Fig. 5.1 also illustrates various potential Attack Paths (APs) targeting the protection system within a digital substation. These paths originate from different components of the substation automation system or the telecommunication infrastructure, ultimately leading to the protective relays:

- **AP1**: Cyberattacks originating from MUs, which are critical for data collection and digitization.
- **AP2**: Attacks starting from the station-level Engineering Workstation (EWS) and passing through substation switches, exploiting the central role of the EWS in configuration and monitoring.
- **AP3**: Attack pathway beginning from the Global Positioning System (GPS)/Global Navigation Satellite System (GNSS) receiver or the grandmaster clock, targeting devices that rely on precise time stamps, such as PDCs, PMUs, MUs, and protective relays.
- **AP4**: Threats arising from the WAN, originating either from an adjacent substation or the grid control center.

It is crucial to recognize that while each AP represents a complete route, attackers can exploit individual segments within these paths. Furthermore, the vulnerability of an AP increases with the number of interconnected devices, as each device introduces its own set of potential security risks, emphasizing the need for robust cybersecurity measures across the substation architecture.

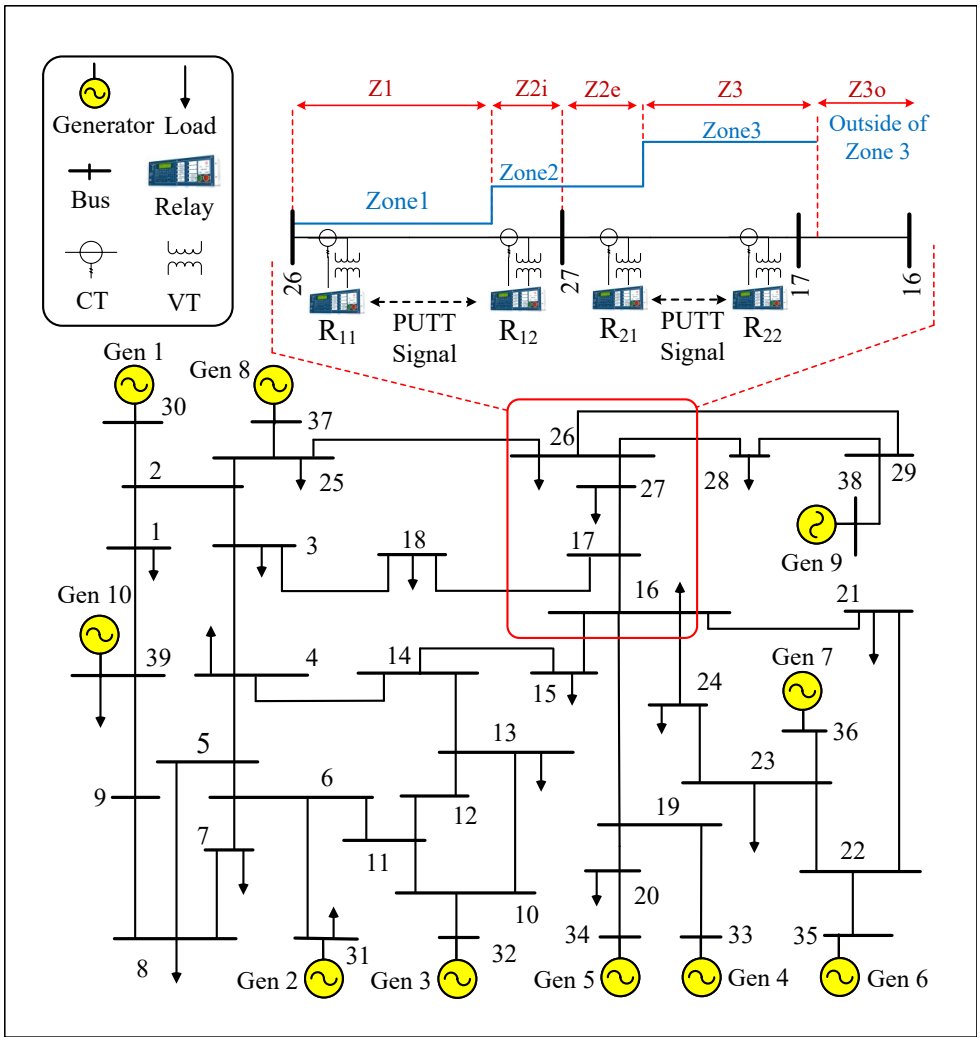


Figure 5.2: IEEE 39 Bus test system.

5.1.2 FDIAs Against Distance Relays

In this section, the IEEE 39-bus test system, depicted in Fig. 5.2, is employed for the analysis. Within this system, distance relays R_{11} and R_{12} are designated to protect line L_{26-27}, while R_{21} and R_{22} are assigned to protect line L_{27-17}. Each of these distance relays, operating with a mho characteristic, is configured with three protection zones. Zone 1 covers 80% of the line impedance and operates instantaneously. Zone 2 extends to 120% of the line impedance with a time delay of 300 ms. Zone 3 encompasses 150% of the combined impedance of the protected line and the longest subsequent line, operating with a delay

Table 5.1: Attack scenarios resulting in misrepresentation of fault location.

Scenario	Actual zone	Falsified zone	SV message	PUTT Signal	Impact
1	Z1	Z2i	✓	×	Nothing
2	Z1	Z2e	✓	×	Delayed trip
3	Z1	Z3	✓	×	Delayed trip
4	Z1	Z3o	✓	×	No trip
5	Z2i	Z1	✓	×	Nothing
6	Z2i	Z2e	×	✓	Delayed trip
7	Z2i	Z3	✓	×	Delayed trip
8	Z2i	Z3o	✓	×	No trip
9	Z2e	Z1	✓	×	False trip
10	Z2e	Z2i	×	✓	False trip
11	Z2e	Z3	✓	×	Back-up maloperation
12	Z2e	Z3o	✓	×	Back-up maloperation
13	Z3	Z1	✓	×	False trip
14	Z3	Z2i	✓	×	False trip
15	Z3	Z2e	✓	×	Back-up maloperation
16	Z3	Z3o	✓	×	Back-up maloperation
17	Z3o	Z1	✓	×	False trip
18	Z3o	Z2i	✓	×	False trip
19	Z3o	Z2e	✓	×	Back-up maloperation
20	Z3o	Z3	✓	×	Back-up maloperation

of 600 ms. Moreover, these relays are communication-assisted and transmit Permissive Under-reaching Transfer Trip (PUTT) signals to their counterparts at the opposite ends of the protected lines. Thus, if the relays detect impedance within the Zone 2 region while receiving a PUTT signal from the remote relay, they bypass the Zone 2 time delay and operate instantaneously.

The substation located at Bus 26, which hosts relay R_{11}, has been selected for the case study and has been targeted by a cyberattack. The reliable operation of R_{11} depends on receiving authentic and accurate current and voltage SV, as well as the PUTT signal. However, as discussed in Section 5.1.1, the SV messages can be manipulated at the process, bay, or station levels through AP1 and AP2, while the PUTT signal may be targeted via AP4. These manipulations result in misrepresenting the actual fault location to the relay and compromise its operation.

From the operational perspective of distance relay R_{11}, the fault location can manifest in five distinct zones: Zone 1 ($Z1$), which operates instantaneously; the internal section of Zone 2 ($Z2i$), which also operates instantaneously with the assistance of the PUTT signal; the external section of Zone 2 ($Z2e$), which incurs a 300 ms delay; Zone 3 ($Z3$), subject to a 600 ms delay; and the Zone 3 Overreach ($Z3o$), encompassing faults beyond the reach of Zone 3 and lying outside the relay's operational range. However, manipulating SV messages and PUTT signals can misrepresent the actual fault zone, causing the relay to perceive a falsified one. Table I details twenty distinct possible misrepresentation scenarios, labeled S1 to S20. This table systematically outlines the actual fault zone, the falsified fault zone perceived by the relay, the specific manipulation required (e.g., SV messages and/or PUTT signal) to induce this misrepresentation, and the potential consequences of the misrepresentation, which can be categorized into four distinct outcomes: *false trip*, *delayed trip*, *no-trip*, and *back-up maloperation*, as described below:

False Trip Attacks

These involve scenarios such as S9, S10, S13, S14, S17, and S18, where the SV of current and voltage and/or the PUTT signal are manipulated so that the impedance perceived by the relay is shifted from a time-delay zone ($Z2e$ or $Z3$) or the no-operation zone ($Z3o$) into an instantaneous zone ($Z1$ or $Z2i$). As a result, the local relay may trip for external faults, leading to a false trip. In what follows, the false trip attack scenarios S13 and S10 are explained in more detail.

- S13 occurs when the actual fault is located in $Z3$ of relay R_{11}, and the manipulated SV shifts the impedance to $Z1$, causing the relay to falsely trip the line. The SV of current and voltage received by relay R_{11} can be manipulated as follows:

$$\mathbf{V}_{abc}^{M} = \begin{bmatrix} mc_1 \\ mc_2 \\ mc_3 \end{bmatrix} \odot \mathbf{V}_{abc}, \quad \mathbf{I}_{abc}^{M} = \begin{bmatrix} mc_4 \\ mc_5 \\ mc_6 \end{bmatrix} \odot \mathbf{I}_{abc} \tag{5.1}$$

  where $\mathbf{V}_{abc}$ and $\mathbf{I}_{abc}$ represent the actual phase voltages and currents, $\mathbf{V}_{abc}^{M}$ and $\mathbf{I}_{abc}^{M}$ denote the manipulated samples, and $\odot$ denotes the element-wise multiplication operator. Additionally, the manipulation coefficients mc_1, mc_2, mc_3 for voltages and mc_4, mc_5, mc_6 for currents are attack parameters. To shift the fault from $Z3$ to $Z1$, the impedance observed by the relay must decrease; thus, the attacker should set the factors $mc_1, mc_2, mc_3 < 1$ (i.e., reducing the SV of voltage) and $mc_4, mc_5, mc_6 > 1$

(i.e., increasing the SV of current). To simulate this scenario, the test system is modeled in PSCAD/EMTDC, and a bolted phase-A-to-ground (AG) fault is simulated 60 km away from Bus 27 on line L_{27-17}. This fault lies within $Z3$ of relay R_{11}. Using the original SV, the apparent impedance of the phase-A ground element (i.e., Z_{ag}^{A}) lies within $Z3$, as illustrated in Fig. 5.3a, resulting in the relay operating with a 600 ms delay. However, manipulating the current and voltage SV as explained above, through AP1 or AP2, moves the apparent impedance Z_{ag}^{M} into $Z1$ (as shown in Fig. 5.3a), leading the relay to incorrectly trip for an external fault.

- S10 occurs when the actual fault is located within $Z2e$ of relay R_{11}, and the manipulated PUTT signal misrepresents the fault location as $Z2i$, causing the relay to falsely trip. To simulate this scenario, a bolted AG fault is initiated 10 km away from Bus 27 on line L_{27-17}. This fault lies within $Z2e$ of R_{11}. As illustrated in Fig. 5.4a, once the fault occurs, Zone 2 of relay R_{11} picks up (i.e., R_{11} $Z2$ becomes one). Since the fault is external, the PUTT signal (i.e., R_{12} $PUTT$) is not issued by R_{12}, and thus R_{11} should open the circuit breaker after a 300 ms delay if the upstream relay R_{21} does not clear the fault. However, in this scenario, the attacker initiates a false PUTT signal through AP4 as soon as Zone 2 picks up. This erroneous PUTT signal results in unintended instantaneous operation of R_{11} (i.e., R_{11} $Trip$ becomes one), causing both lines L_{26-27} and L_{27-17} to be tripped by their associated relays.

Delayed trip attacks

These involve scenarios such as S2, S3, S6, and S7, where the SV of current and voltage and/or the PUTT signal are manipulated in such a way that the apparent impedance of the relay is shifted from an instantaneous zone ($Z1$ or $Z2i$) to a time-delay zone ($Z2e$ or $Z3$). In what follows, the delayed trip attack scenarios S3 and S6 are explained in more detail.

- S3 occurs when the actual fault is located within $Z1$ of relay R_{11}, but the attacker manipulates voltage and current SV such that the apparent impedance of R_{11} appears in $Z3$, causing the relay to operate after a significant delay. To shift the apparent impedance from $Z1$ to $Z3$, the impedance observed by the relay must increase; thus, the attacker should set the coefficients $mc_1, mc_2, mc_3 > 1$ (i.e., increasing the SV of voltage) and $mc_4, mc_5, mc_6 < 1$ (i.e., reducing the SV of current). However, the SV must be manipulated through AP1 or AP2 in such a way that the apparent impedances of none of the phase or ground elements enter their associated $Z1$ or $Z2$. To simulate this scenario, a bolted AG fault is initiated 50 km away from Bus 26 on

line L_{26-27}, which lies within $Z1$ of R_{11}. In this scenario, Z_{ag}^{A} falls within Zone 1, as depicted in Fig. 5.3b, indicating that the relay should operate instantaneously. However, the manipulated SV of current and voltage mislead the relay into perceiving the fault as occurring in Zone 3 (Fig. 5.3b), resulting in operation of the backup relay after a time delay.

- S6 occurs when the actual fault is located within $Z2i$ of relay R_{11}, and the manipulated PUTT signal misrepresents the fault location as $Z2e$, causing the relay to experience a delayed trip. To simulate this scenario, a bolted AG fault is initiated 85 km away from Bus 26 on line L_{26-27}. This fault lies within $Z2i$ of R_{11}. As illustrated in Fig. 5.4b, once the fault occurs, Zone 2 of R_{11} picks up. Since the fault is internal, the PUTT signal (i.e., R_{12} $PUTT$) is issued by R_{12}. However, an attacker who has compromised the substation at Bus 26 could manipulate and block the PUTT signal through AP4. Consequently, R_{11}, which was supposed to operate immediately with the help of the PUTT signal, waits until the Zone 2 timer expires before initiating a trip. This unnecessary delay compromises the protection system's ability to isolate the fault promptly, increasing the risk of equipment damage and system instability.

No-trip Attacks

These occur in scenarios such as S4 and S8, where the SVs of current and voltage are manipulated to alter the apparent impedance seen by the relay, shifting it from an instantaneous tripping zone ($Z1$ or $Z2i$) to a no-operation zone ($Z3o$). For example, in S4, a fault originates within $Z1$; however, due to the manipulation of the SVs, the relay incorrectly perceives the fault as being in $Z3o$, thereby preventing it from tripping for an internal fault. To simulate this scenario, a fault is initiated in Zone 1, similar to S3, but is artificially displaced to $Z3o$, as illustrated in Fig. 5.5a. As shown in the figure, the relay fails to operate, effectively neutralizing the intended protection mechanism for internal faults.

Back-up Maloperation Attack

encompasses scenarios such as S11, S12, S15, S16, S19, and S20, where the manipulation of current and voltage SVs disrupts the relay's backup protection function. For instance, in S11, a fault that is actually within $Z2e$ of R_{11} is deliberately shifted by the attacker to $Z3$, causing the relay's backup protection—-which is supposed to operate after 300 ms delay—to operate after 600 ms. To simulate this scenario, a fault is introduced in $Z2e$,

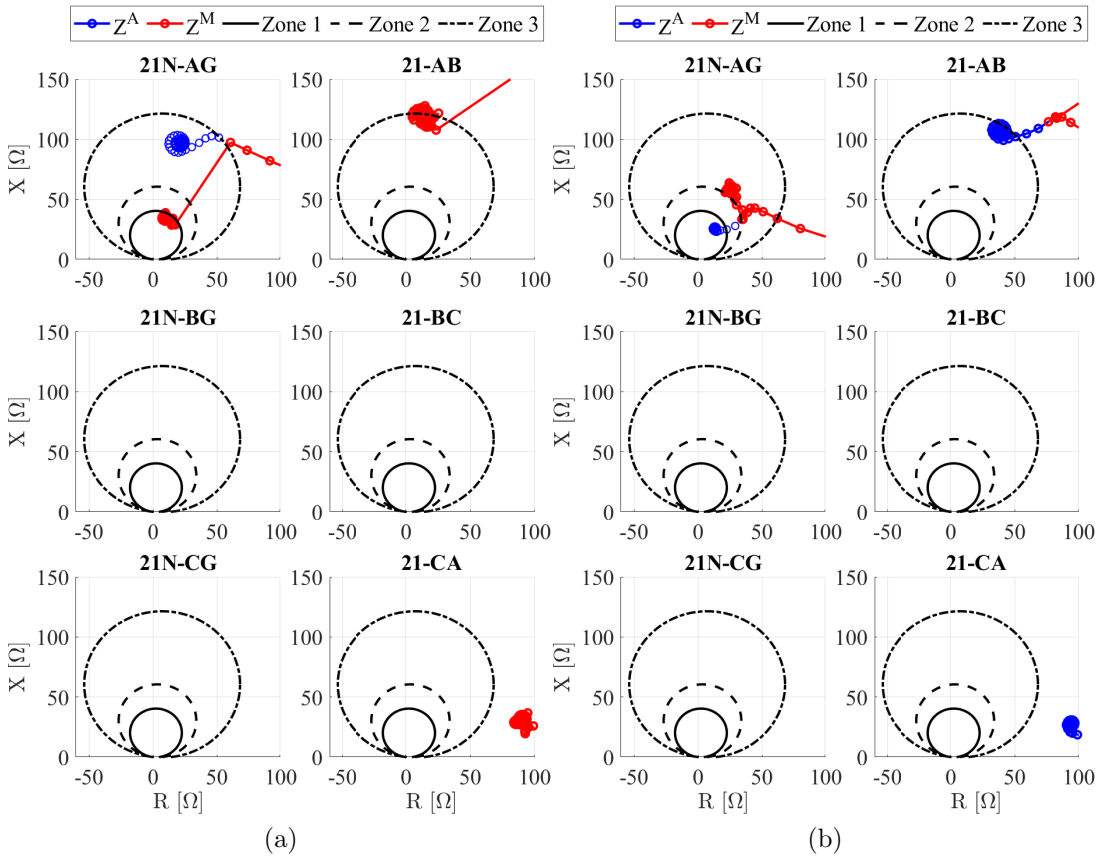


Figure 5.3: Actual and manipulated apparent impedance trajectories of R_{11}: (a) false trip attack of scenario S13 (b) delayed trip attack of scenario S3.

as in S10; however, due to SV manipulation, it is misclassified into $Z3$, as illustrated in Fig. 5.5b. As the figure demonstrates, the relay incorrectly delays its operation by 600 ms for a Zone 2 fault, highlighting the failure of the backup protection mechanism.

5.2 Traveling Wave Modeling and Analysis

This section presents the fundamental equations governing TW propagation, and explains how each frequency component of a TW is attenuated based on both its frequency and the distance traveled by the wave, with higher-frequency components experiencing more

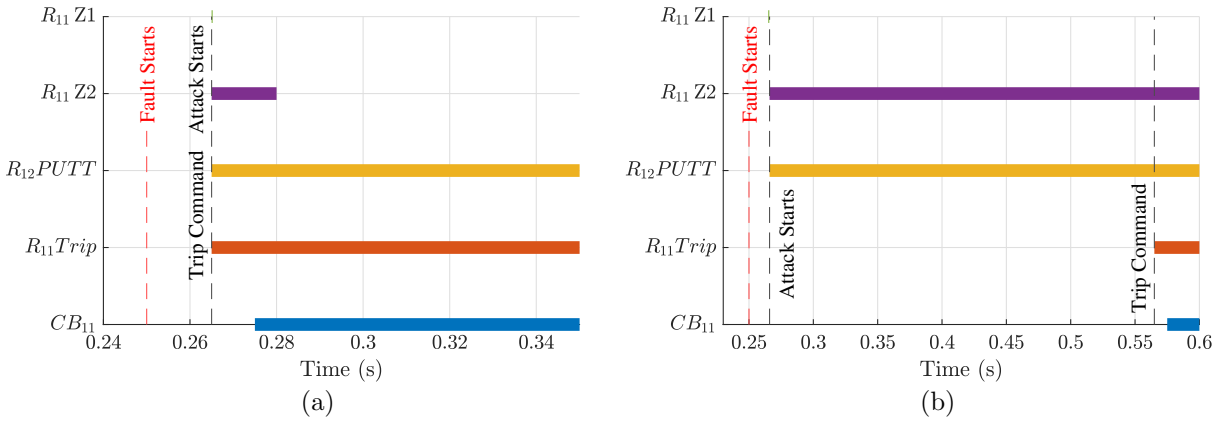


Figure 5.4: Protection signals (a) false trip attack of scenario S10, and (b) delayed trip attack of scenario S6.

significant attenuation. To enable more effective analysis of these frequency-dependent characteristics, the wavelet transform is then introduced as a suitable tool for decomposing TWs into meaningful frequency bands, enabling detailed analysis.

5.2.1 Mathematical Modeling of TW Propagation on Transmission Lines

TWs are high-frequency transient disturbances in voltage or current that propagate along transmission lines in response to abrupt system changes, such as faults, lightning strikes, or switching operations. These waves contain valuable information regarding the location and characteristics of the initiating event and are therefore central to high-speed protection and fault location methodologies.

The propagation of TWs on a single-conductor homogeneous line can be modeled using a lumped-parameter approach, where the line is characterized by distributed resistance R, inductance L, conductance G, and capacitance C per unit length. Applying Kirchhoff's voltage and current laws to an infinitesimal segment of the line yields the well-known Telegrapher's equations in the time domain:

$$\frac{\partial V(x,t)}{\partial x} = -RI(x,t) - L\frac{\partial I(x,t)}{\partial t} \tag{5.2}$$

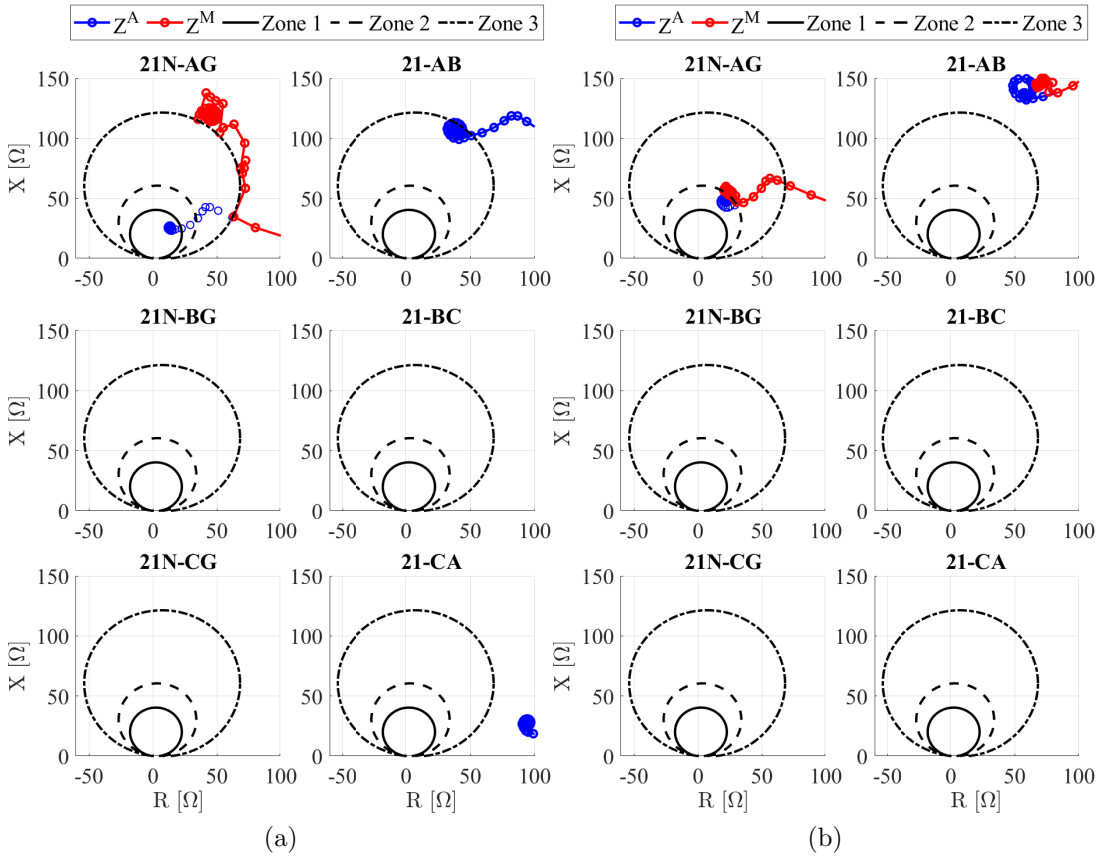


Figure 5.5: Actual and manipulated apparent impedance trajectories of R_{11}: (a) No-trip attack of scenario S4 (b) back-up maloperation attack of scenario S10.

$$\frac{\partial I(x,t)}{\partial x} = -GV(x,t) - C\frac{\partial V(x,t)}{\partial t} \tag{5.3}$$

where $V(x,t)$ and $I(x,t)$ denote the instantaneous voltage and current at position x and time t, respectively.

To derive the general solution for the current, the system of Telegrapher's equations is decoupled by differentiating (5.3) with respect to x and substituting the result into (5.2). By assuming a time-harmonic solution, where voltage and current vary sinusoidally with time—i.e., $I(x,t) = I(x)e^{j\omega t}$—the governing equations can be simplified using phasor analysis. Substituting this expression into the resulting second-order differential equation

yields:

$$I(x,t) = I^{+}e^{-\gamma x}e^{j\omega t} + I^{-}e^{\gamma x}e^{j\omega t} \tag{5.4}$$

where I^{+} and I^{-} are the phasor amplitudes of the forward- and backward-propagating waves, respectively, and γ is the complex propagation constant, defined as:

$$\gamma = \alpha + j\beta = \sqrt{(R + j\omega L)(G + j\omega C)} \tag{5.5}$$

where α is the attenuation constant, which quantifies the exponential decay of wave amplitude as it propagates along the line. Higher values of α at certain frequencies lead to faster attenuation of those frequency components. Additionally, β in (5.5) is the phase constant, which determines the rate of phase change per unit distance and directly influences the wave's propagation speed and wavelength. Together, α and β characterize how transmission lines affect TWs during propagation. High-frequency components experience greater attenuation due to increased resistive and dielectric losses, causing them to decay more rapidly than low-frequency components. This frequency-dependent attenuation behavior is described as:

$$H(\omega, x) = e^{-\gamma(\omega)x} = e^{-\sqrt{(R+j\omega L)(G+j\omega C)}x} \tag{5.6}$$

which explains how each frequency component of a TW is attenuated and phase-shifted as it propagates a distance x along the line. As x increases, higher-frequency components tend to attenuate more rapidly due to series resistance and shunt conductance.

Although the analysis up to this point has been based on a single-phase line model, it can be readily extended to real-world three-phase transmission lines, where both C and L are 3×3 matrices, and $I(x,t)$ and $V(x,t)$ are 3×1 vectors. These quantities can then be substituted into the Telegrapher's equations for multi-conductor systems, leading to a similar outcome in terms of the TW frequency attenuation pattern [37].

5.2.2 Time-Frequency Analysis of TWs with Wavelet Transform

The wavelet transform is a mathematical tool that enables the simultaneous analysis of a signal's time and frequency characteristics. This property makes it particularly well-suited for analyzing TWs, which are inherently transient and exhibit frequency-dependent attenuation as they propagate through transmission lines.

To leverage this capability in practical settings, the Discrete Wavelet Transform (DWT) is applied to sampled TW current or voltage signals—i.e., $I_{\mathrm{TW}}[n]$ and $V_{\mathrm{TW}}[n]$—acquired at N discrete time points. The DWT decomposes these signals into time-localized frequency components, allowing for a detailed analysis of their transient behavior. Specifically, the

DWT performs multi-resolution analysis by successively applying a pair of digital filters—known as quadrature mirror filters—to separate the signal into low-frequency (approximation) and high-frequency (detail) components across multiple scales.

At each decomposition level j, the approximation coefficients $c_{j,k}$ and detail coefficients $d_{j,k}$ are computed as:

$$\begin{aligned} c_{j,k} &= \sum_n I_{\mathrm{TW}}[n] \cdot l[2k-n], \\ d_{j,k} &= \sum_n I_{\mathrm{TW}}[n] \cdot h[2k-n], \end{aligned} \tag{5.7}$$

where $l[n]$ and $h[n]$ denote the low-pass and high-pass filters, respectively. These filters isolate complementary frequency bands, and each is followed by a downsampling operation by a factor of two (represented by $2k$) to reduce redundancy and adapt the sampling rate to the narrower bandwidth of the filtered signal. This process ensures that each decomposition level accurately captures its designated frequency range with the appropriate time resolution.

As illustrated in Fig. 5.6, the decomposition in (5.7) is applied recursively to the approximation coefficients $c_{j,k}$, enabling a hierarchical, multiscale representation of the signal. For a J-level decomposition, the final approximation A_J captures the coarse (low-frequency) content of the signal, while the set $\{D_1, \ldots, D_J\}$ reveals progressively finer (higher-frequency) transient details. Specifically, for a signal with an original sampling frequency F, the frequency content captured by each detail level corresponds to specific bands: D_1 captures components between $F/4$ and $F/2$; D_2 captures components between $F/8$ and $F/4$; D_3 captures components between $F/16$ and $F/8$; and so on. At each level, the approximation A_j retains the remaining low-frequency content below the lower bound of D_j. This structured decomposition enables effective isolation of frequency-specific features for TW analysis.

To demonstrate the performance of the DWT by example, a bolted AG fault is initiated at distances of 10 km and 80 km from Bus 26 on line L_{26-27}, and the first current TWs are captured at the location of relay R_{11} with a 10 MHz sampling rate, as shown in Fig. 5.7. Current TWs are preferred over voltage TWs due to the superior frequency response and broader bandwidth of CTs compared to Capacitor Voltage Transformers (CVTs), making them more effective for capturing the high-frequency components of TWs. These current TW signals are analyzed using a five-level DWT, with high-pass and low-pass filters derived from the Haar wavelet. The corresponding detail coefficients at each decomposition level are illustrated in Fig. 5.7. A comparison of the detail coefficients from the two fault

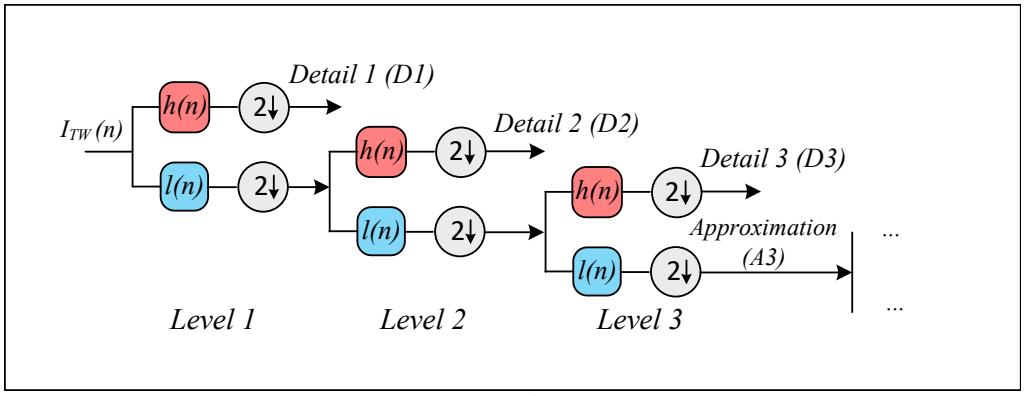


Figure 5.6: Wavelet multi-resolution analysis.

locations shows that the higher frequency bands (e.g., levels 1 and 2) have larger coefficients for the 10 km fault, whereas the lower frequency bands (e.g., level 5) are more prominent for the 80 km case. This observation confirms that high-frequency components attenuate more rapidly with increasing propagation distance.

To quantitatively analyze the attenuation of high-frequency components in TW signals, the energy associated with each detail level is computed using the squared sum of the wavelet coefficients. The energy at level j is defined as

$$E_{D_j} = \sum_{k=1}^{N/2^j} d_{j,k}^2, \quad j = 1, 2, \ldots, J \tag{5.8}$$

where E_{D_j} denotes the absolute energy of the detail signal at level j. While absolute energy provides a sense of signal strength at each level, it is sensitive to the overall signal amplitude. To more effectively capture the frequency-dependent attenuation pattern independently of signal magnitude, the relative energy can be computed as

$$\tilde{E}_{D_j} = \frac{E_{D_j}}{\sum_{j=1}^{J} E_{D_j}} \times 100\% \tag{5.9}$$

where the relative energy $\tilde{E}_{D_j}$ expresses the proportion of total energy concentrated at level j with respect to the energy across all levels, enabling consistent comparison of the energy distribution across different frequency bands for various propagation distances. To demonstrate the effectiveness of relative energy in capturing the frequency-dependent attenuation pattern of TWs, a bolted AG fault is initiated at distances ranging from 10 km to 90 km, and the relative energy across five levels of wavelet decomposition is computed, as shown in Fig. 5.8. This figure shows that as the fault distance increases, the relative

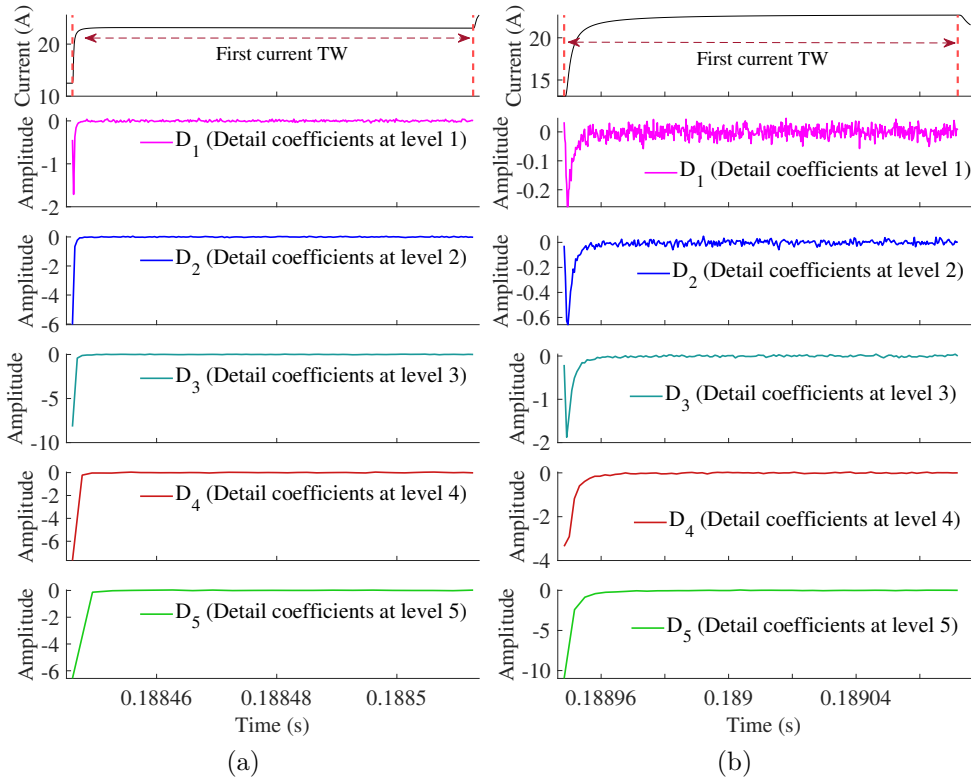


Figure 5.7: The first TW for fault (a) at 10 km (b) at 80 km.

energy in the high-frequency components (i.e., levels 1 and 2) decreases, while that in the lower-frequency components (i.e., levels 4 and 5) becomes more prominent. These frequency-dependent energy features can be exploited to estimate the fault location or to identify the faulty zone.

5.3 The Proposed Substitude for Distance Relays Under Attacks

This section first explains how a RF classifier—trained using the relative energy extracted from different levels of TW decomposition via the DWT—can be used to detect the faulted zone in a power system. Then, the performance of an incremental-quantity overcurrent

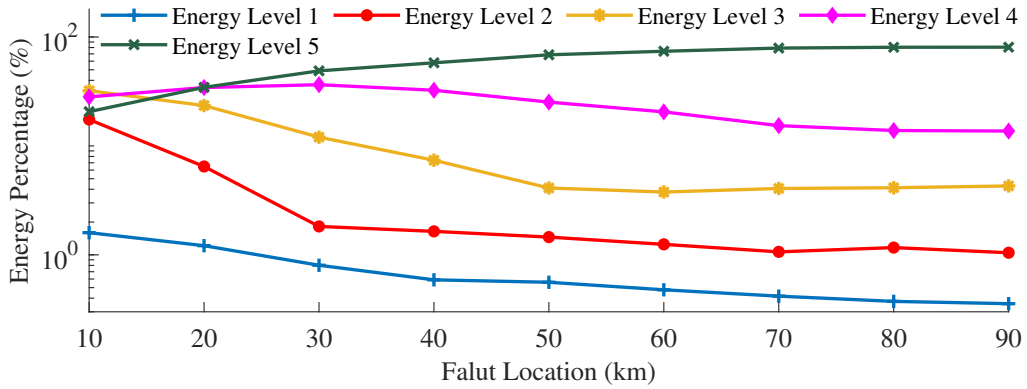


Figure 5.8: The relative energy at different decomposition levels of TWs.

relay, which is an essential element in TW-based protection schemes, is examined. Finally, the proposed substitute for distance relays during cyberattacks is introduced.

5.3.1 Detecting the Fault Zone using Random Forest Classifier

RF is an ensemble learning method that builds multiple decision trees using bootstrap aggregating (bagging) and feature randomness to improve classification accuracy. Each tree is trained on a bootstrapped sample of the dataset (drawn with replacement), and node splits are based on a random subset of features, which reduces overfitting and decorrelates the trees. As illustrated in Fig. 5.9, final predictions are made through majority voting across the ensemble, stabilizing results and enhancing generalization. RF's computational scalability and robustness to noise make it well-suited for complex classification tasks. In this work, RF is selected due to its superior accuracy compared to neural networks, its robust performance with limited data relative to deep learning models, its faster training time and better performance compared to support vector machines, and its inherent ability to mitigate the overfitting commonly observed in single decision tree classifiers [71].

The overall process of the proposed RF-based fault zoning method is illustrated in Fig. 5.10. Initially, the first current TWs for each of the three phases, i.e., I_a^{TW}, I_b^{TW}, and I_c^{TW}, are extracted and analyzed using the DWT to obtain frequency-related features. As discussed in Section 5.2.2, the relative energy at different detail levels of the TW, obtained via the DWT, can serve as an effective feature for detecting the fault location or identifying the fault zone. Therefore, the DWT is applied to the three initial current TWs, and their corresponding relative energy values are computed. These values form the input feature

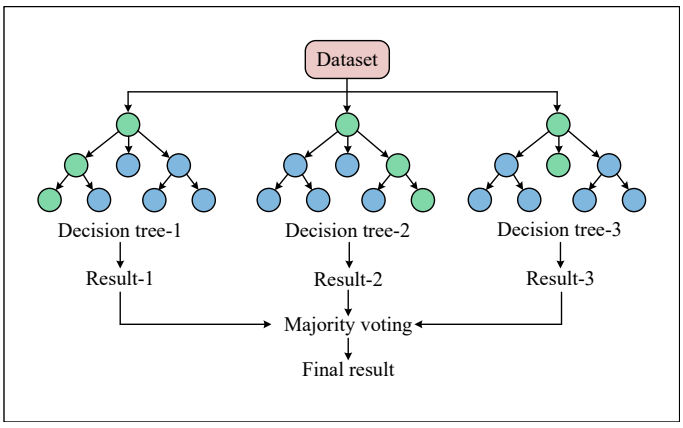


Figure 5.9: The general structure of the RF classifier.

vector for the RF classifier, defined as

$$\mathbf{x} = \left[\tilde{E}^a_{D_1}, \ldots, \tilde{E}^a_{D_J}, \tilde{E}^b_{D_1}, \ldots, \tilde{E}^b_{D_J}, \tilde{E}^c_{D_1}, \ldots, \tilde{E}^c_{D_J}\right] \tag{5.10}$$

where $\tilde{E}^a_{D_j}$, $\tilde{E}^b_{D_j}$, and $\tilde{E}^c_{D_j}$ represent the relative energy at detail level D_j for the TW signals of phases a, b, and c, respectively.

The output label is the fault zone, which can be one of the following: Zone 1 ($Z1$), internal Zone 2 ($Z2i$), external Zone 2 ($Z2e$), or Zone 3 and overreach combined ($Z3\_Z3o$), representing faults located beyond the Zone 2 boundary and within or beyond the Zone 3 range.

The training phase of the RF classifier, which involves generating a comprehensive dataset and extracting relevant features, is crucial for the accuracy of the proposed method. As demonstrated in [37, 16], parameters such as fault inception angle, fault resistance, and the system operating point affect the amplitude of TWs but do not influence their frequency content. The only significant parameter affecting the frequency components is the fault location. Therefore, to construct a representative training dataset for the RF classifier, faults are simulated within the different protection zones of the relay, and the corresponding current TWs captured by the relay are used for feature extraction via the DWT. To achieve this, faults are simulated at 1 km intervals along the protected line. Based on the true fault zones, the dataset is labeled for training of the RF classifier.

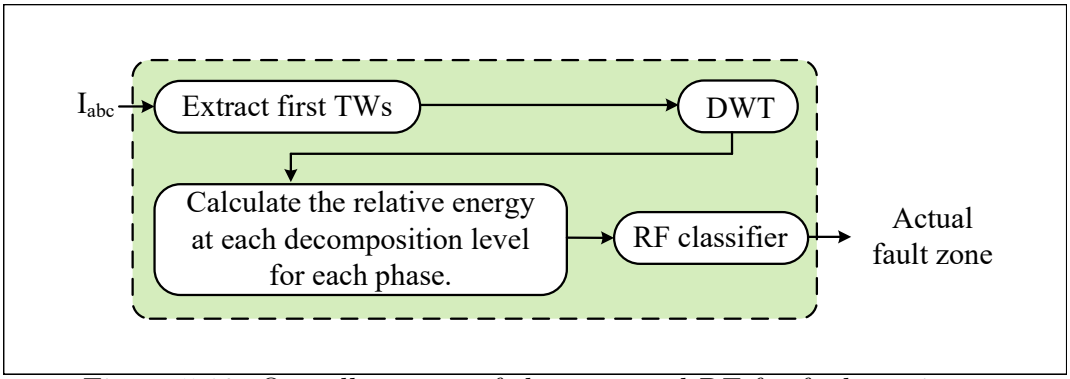


Figure 5.10: Overall process of the proposed RF for fault zoning

5.3.2 Incremental-quantity Overcurrent Relay

The TW-based protection scheme generally uses overcurrent supervision, a technique commonly employed in commercial protective relays, to ensure security for switching events that may generate high-frequency transients and TWs [79]. Incremental overcurrent elements are employed to verify the presence of sufficient energy in the power frequency band, ensuring that events detected by the TW protection logic are valid faults and not transient disturbances.

The incremental-quantity-based protection elements operate by responding to the fault-induced components of the loop voltages and replica currents. These fault-induced components, known as incremental quantities, are calculated as the difference between the present signal values and their corresponding values one cycle earlier. Figure 5.11 illustrates the process of deriving incremental quantities, where the delay is precisely one power cycle. To maintain accuracy under dynamic power system conditions, the protective relay continuously monitors the system frequency and adjusts the delay accordingly.

The logic of the incremental overcurrent element involves integrating the incremental replica current and comparing it against a straight line representing the element's pickup threshold, as shown in Fig. 5.12. When the current magnitude exceeds the pickup threshold—i.e., the integral surpasses the straight line—it indicates a pickup condition. Conversely, if the current magnitude remains below the threshold, the integral stays beneath the line, indicating no pickup. The procedure for determining this pickup threshold is fully discussed in [79]. First, the minimum fault current for the system is calculated, defined as the lowest fault current level under the worst-case scenario, typically assuming a fault at the end of the line (remote bus), the weakest local system, the strongest remote system, and a specified fault resistance for single-line-to-ground faults. Based on this minimum fault current, the pickup threshold is selected with an appropriate security margin

to ensure sensitivity to faults while maintaining stability against non-fault conditions.

5.3.3 Proposed Protection Scheme

Fig. 5.13 presents the proposed protection scheme designed to ensure the reliable operation of the distance relay under cyberattack conditions. As shown in the figure, as long as the Intrusion Detection System (IDS) does not detect a cyber intrusion (i.e., IDS-T = 0), the distance relay remains in service, and the proposed scheme is bypassed, exerting no influence on the relay's operation. However, once the IDS detects a cyber intrusion (i.e., IDS-T = 1), the distance relay is bypassed by forcing a logic zero into its AND gate, and the proposed TW-based protection scheme is activated to serve as a substitute for the distance relay. The trained RF classifier within the proposed scheme captures the first current TWs of all phases (if present) from a dedicated hard-wired current measurement and detects the location of the fault, which can be within Zone 1, internal Zone 2 ($Z2i$), external Zone 2 ($Z2e$), or beyond these regions. It should be noted that, since the proposed method must determine the fault location both within and beyond the protected line without relying on the communication system, the conventional single-ended TW-based methods that depend on the arrival time of TWs cannot be used.

When a fault occurs within Zone 1 or Zone 2 and the distance relay is bypassed due to the IDS, the RF classifier identifies the actual fault zone and initiates the trip command. Before this trip signal is sent to the relay, it is further validated through an AND gate in conjunction with the pickup signal from the incremental-quantity overcurrent relay. This ensures that the detected TW is associated with a genuine fault rather than a switching event.

5.4 Performance Evaluation

This section utilizes the test system described in Section 5.1 to evaluate the performance of the proposed protection scheme. Within this system, it is assumed that the substation at Bus 26, where relay R_{11} is located, is under attacks. Once the attack is detected by the IDS, the SVs of current and voltage, as well as the PUTT signal, are identified as unreliable. Therefore, the distance relay R_{11} is substituted by the proposed scheme, and the RF classifier, supervised by the incremental overcurrent relay, is assumed to provide protection for the system. The following subsections evaluate the performance of the RF classifier in detecting zone of faults and providing accurate protection.

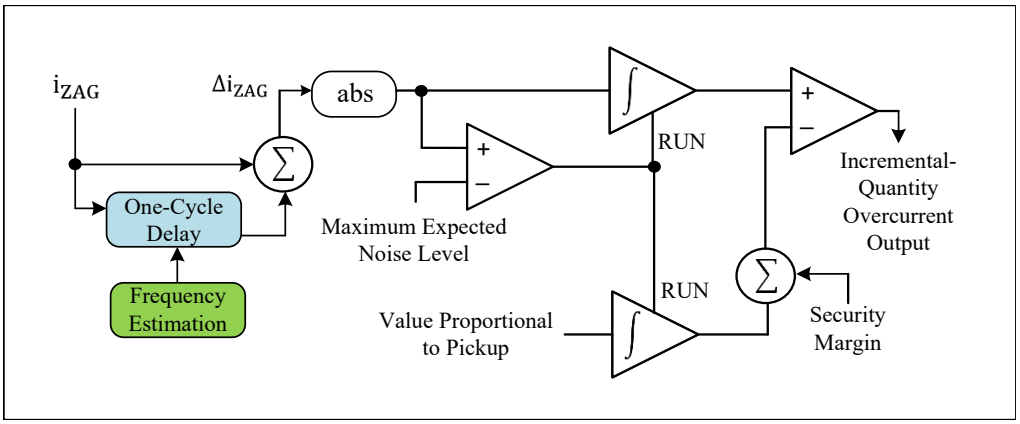


Figure 5.11: Incremental-Quantity Overcurrent Element Simplified Logic Diagram (AG Loop) [79].

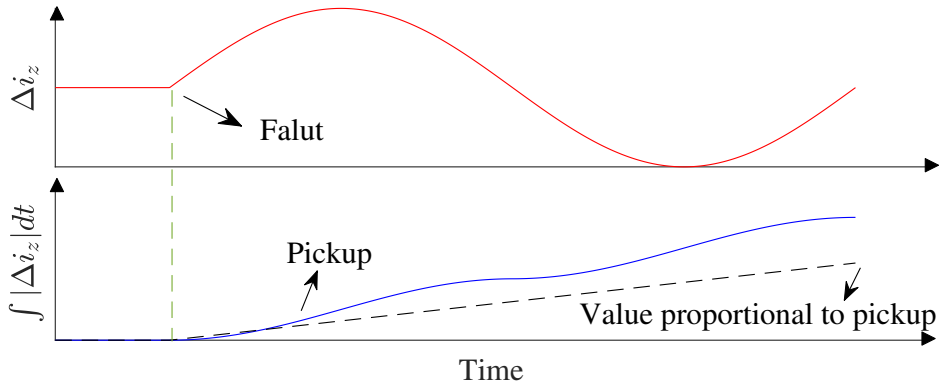


Figure 5.12: Incremental Replica Current and Its Integral Over Time.

5.4.1 Performance of RF classifer During Training and Testing Phases

To train the RF classifier, a comprehensive dataset is first constructed. Without loss of generality, this study focuses on Phase A faults, including AG, AB, AC, ABG, ACG, and ABCG types. Equivalent datasets for Phases B and C can be generated using the same procedure, replicating the fault types, locations, and parameters used for Phase A while substituting the corresponding phase conductors. The six Phase A fault types are simulated in PSCAD/EMTDC at 1 km intervals along lines $L_{26\text{–}27}$ and $L_{27\text{–}17}$, with a fault resistance of 0 Ω and a Phase A fault inception angle of $\theta = 45°$. This results in 1278 fault cases. The current TWs at Bus 26 are captured using phase-specific CTs, with specifications detailed in [19]. Although higher sampling frequencies f_s can improve TW capture accuracy, a

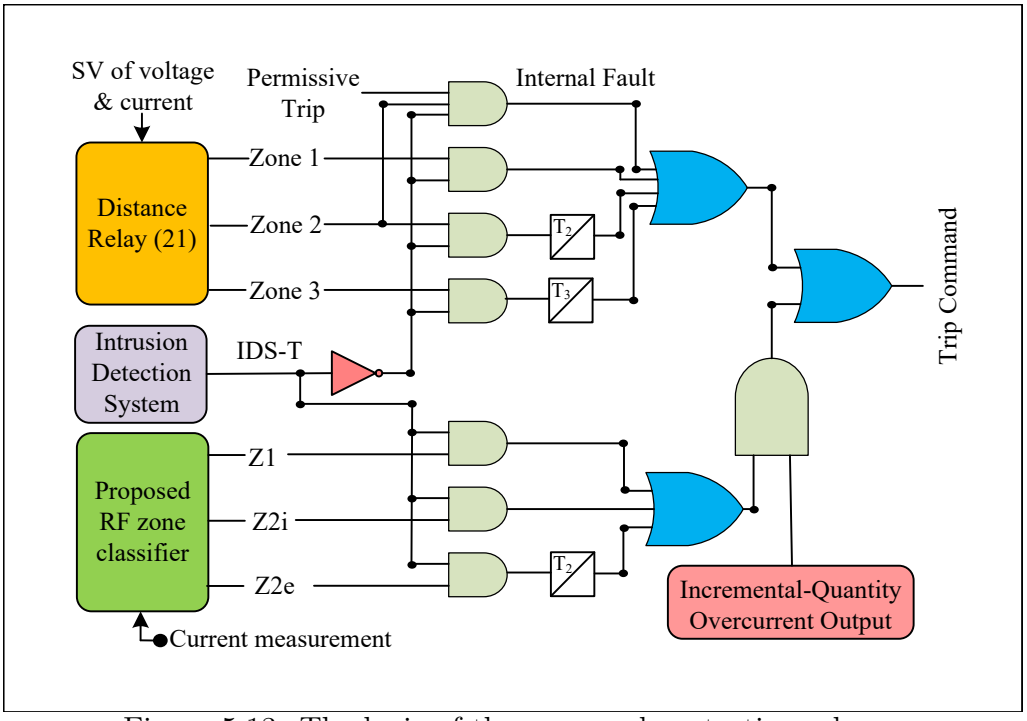


Figure 5.13: The logic of the proposed protection scheme.

practical rate of 1.5625 MHz—typical of modern protective relays [78]—is adopted in this study.

Additionally, to model the noise present in practical applications, the CT measurements are contaminated with zero-mean, white, and uncorrelated noise, with a signal-to-noise ratio (SNR) of 35 dB [40]. To account for the impact of measurement noise on the classifier's training and testing accuracies, each simulation case is repeated twenty-five times. As a result, a total of 31,950 fault cases are generated for the transmission lines.

To extract features from the TW, the DWT, as described in Section 5.2.2, is applied with a five-level decomposition. The Haar wavelet is used to construct both low-pass and high-pass filters. This wavelet is selected for its simple structure and computational efficiency, which make it suitable for real-time and resource-constrained applications, as demonstrated in Section 5.4.3. Moreover, its sensitivity to abrupt signal changes makes it particularly effective for capturing the sharp transients characteristic of TWs. The multi-level decomposition enables detailed frequency-band analysis, enhancing the identification of key transient features. The energy at each level is computed using (5.8), and the feature vector for the RF classifier is subsequently formed as defined in (5.10).

Once the dataset is prepared, 70% is used for training the RF classifier, and the re-

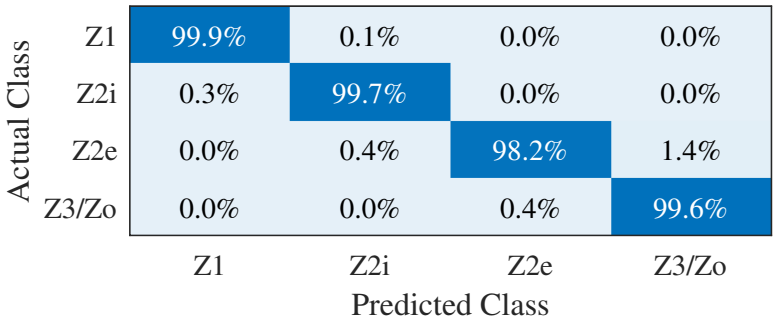


Figure 5.14: Confusion matrix of the proposed method for test cases.

maining 30% is reserved for testing. The RF classifier in this study is implemented using MATLAB's built-in `fitcensemble` function with the bagging method. The ensemble consists of 30 decision trees, each trained on a bootstrap sample of the training data. At each decision split, a random subset of features is selected to promote decorrelation among trees. The final classification output is determined through majority voting across all trees in the ensemble.

The trained RF classifier achieves an overall accuracy of 99.56%, demonstrating reliable fault zone identification across various fault types and locations. However, in protection applications, not all classification errors have the same operational impact. Some errors can cause critical issues, such as false or delayed tripping, while others may only affect backup protection or have minimal consequences. Thus, overall accuracy alone does not fully capture practical performance. To address this, the study also quantifies critical misoperations: only 0.01% of test cases result in false tripping, 0.04% in delayed tripping, and 0.0% in no-trip events (i.e., failure to trip when required). The remaining misclassifications have no impact on primary protection or only affect backup operation. A detailed breakdown of the classification results is provided by the confusion matrix shown in Fig. 5.14. Each row of the matrix corresponds to the actual fault zone, while each column represents the predicted zone. As seen in the matrix, the classifier demonstrates strong performance across all classes, with the majority of samples correctly classified.

5.4.2 Evaluation Based on New Cases

To further corroborate the effectiveness of the proposed method, this section tests its performance under various operating conditions, as well as for different fault parameters. In fact, this section evaluates the RF model's generalization capability and robustness, as none of these cases were included in the training phase.

Table 5.2: Accuracy of the proposed method for various fault impedance.

Fault Impedance	Accuracy	False Trip	No Trip	Delay Trip	Backup maloperation
0 Ω	99.5%	0.01%	0%	0.04%	0.3%
0.1 Ω	99.5%	0.01%	0%	0.03%	0.4%
1 Ω	99.4%	0.01%	0%	0%	0.5%
10 Ω	99.4%	0.01%	0%	0.03%	0.5%
20 Ω	99.4%	0.02%	0%	0.03%	0.4%
40 Ω	99.4%	0.02%	0%	0.02%	0.5%
60 Ω	99.3%	0.01%	0%	0.03%	0.6%
80 Ω	99.3%	0.01%	0%	0%	0.7%
100 Ω	99.2%	0.02%	0%	0%	0.7%

Table 5.3: Accuracy of proposed method for various fault inception angle.

Inception Angle	Accuracy	False Trip	No Trip	Delay Trip	Backup maloperation
10°	91.7%	0.3%	0%	4%	2.9%
45°	99.5%	0.01%	0%	0.04%	0.32%
90°	96.1%	0.28%	0%	0.02%	2.8%
135°	95%	0.6%	0%	0.26%	3.5%
170°	95.6%	0.68%	0%	0.02%	3.04%

fault Impedance

To evaluate the influence of fault resistance on the accuracy of the proposed RF classifier, ABCG faults with resistance values $R_f \in \{0, 0.1, 1, 10, 20, 40, 60, 80, 100\}$ Ω are simulated at 1 km intervals, with a fixed fault inception angle of $\theta = 45°$. Fig. 5.15 shows the confusion matrix of the proposed RF model for the case with $R_f = 100$ Ω, and Table 5.3 summarizes the classification accuracy across all resistance values. As shown in the table, the classification error remains below 1% across all resistance values, indicating that R_f has minimal impact on the model's performance. Furthermore, the proportion of cases resulting in false tripping and delayed tripping is less than 0.03% and 0.04%, respectively, demonstrating that the proposed scheme maintains reliable performance even under high-resistance faults.

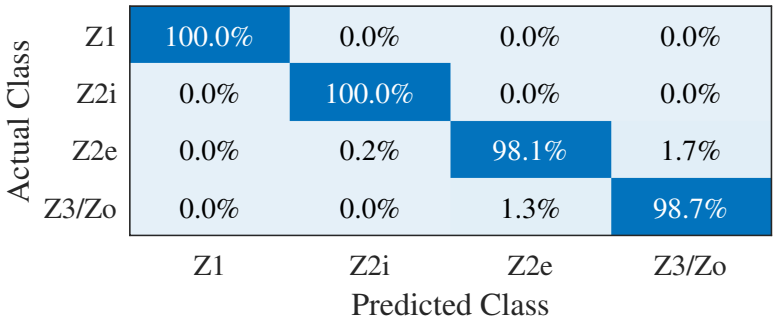


Figure 5.15: Confusion matrix for the simulation with $R_f = 100$.

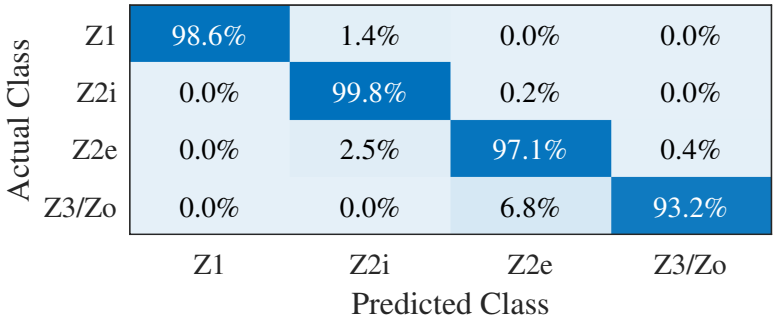


Figure 5.16: Confusion matrix for the simulation with $\theta = 90$.

Fault inception angle

To assess the impact of fault inception angle on the proposed method, bolted AG faults are simulated every 1 km for five inception angles: 10°, 45°, 90°, 135°, and 170°, resulting in 213 faults per angle to cover a range of conditions within a sinewave cycle. It should be noted that for inception angles of $\theta = 0°$ and $\theta = 180°$, no current TW is generated; therefore, the proposed method cannot detect such faults. However, the probability of faults occurring at exactly these angles is mathematically negligible, and thus they are not considered in this analysis. Figure 5.16 shows the confusion matrix for faults with an inception angle of 90°, and Table 5.3 summarizes the classification accuracy of the proposed RF model across all tested angles. As shown in the table, the inception angle has a minimal overall impact, with the highest accuracy observed at 90°, and slightly lower performance at low-angle cases such as 10°. Nevertheless, even at 10°, the false trip rate remains below 0.3%, indicating that the proposed method maintains reliable protection performance under all evaluated conditions. Notably, the no-trip rate is 0%, confirming that the method consistently avoids failure to trip when required.

5.4.3 Computational Complexity and Inference Time Estimation

The computation time of the proposed protection scheme is a critical factor in assessing its suitability for real-time applications. To evaluate its feasibility for deployment in embedded digital relays, the number of floating-point operations (FLOPs) required by each processing stage is analytically estimated. These estimates are subsequently used to calculate the total inference time based on typical processor characteristics.

In a multilevel one-dimensional DWT, the signal is recursively filtered and downsampled. For each output sample, the filtering operation involves a convolution with a wavelet filter of length F, requiring F multiplications and $F-1$ additions. This results in a total of $2F-1$ floating-point operations per output. As the signal length is halved at each level, the number of operations at level j is $\frac{N}{2^j}(2F-1)$, where N is the original signal length. Summing across all J levels, the total required Flops can be calculated as:

$$\text{FLOPs}_{\text{DWT}} = 2N(2F-1)\left(1-\frac{1}{2^J}\right). \tag{5.11}$$

Following decomposition, the energy of the wavelet coefficients is computed at each level to extract time-frequency features relevant to classification. This computation requires one multiplication and one addition per coefficient, yielding approximately $2n-1$ FLOPs per level. Accounting for the progressive downsampling across levels, the total number of FLOPs required for energy computation is given by:

$$\text{FLOPs}_{\text{Energy}} = 2N\left(1-\frac{1}{2^J}\right) - J. \tag{5.12}$$

Additionally, during the inference of the RF classifer, each input sample follows a path from the root to a leaf node in every decision tree. Each node traversal involves a single comparison, which is approximated as one FLOP. Therefore, for a forest consisting of T trees with an average depth D, the total FLOPs required for classification can be expressed as:

$$\text{FLOPs}_{\text{RF}} = T \times D. \tag{5.13}$$

Therefore, using (5.11)-(5.13), the total required Flops can be calculated as follows:

$$\text{FLOPs}_{\text{total}} = \text{FLOPs}_{\text{Energy}} + \text{FLOPs}_{\text{DWT}} + \text{FLOPs}_{\text{RF}} \tag{5.14}$$

In the proposed protection scheme, the DWT is configured with $J = 5$ levels, and the

Haar wavelet is employed, corresponding to a filter length of $F = 2$. The longest initial TW segment contains $N = 513$ samples. Thus, based on (5.11) and (5.12), the required number of FLOPs for DWT and energy computation are approximately 2,983 and 990, respectively.

The RF classifiers with different numbers of trees were tested, and the corresponding accuracies and required FLOPs are presented in Fig. 5.17. As shown, the RF with thirty trees ($T = 30$) achieves high and reliable accuracy, with an average tree depth of $D = 18$ and a computational cost of approximately 540 FLOPs. Therefore, the total number of FLOPs required to process the proposed method is approximately 4,513, as derived from (5.14).

Assuming a processor operating at $f_{\text{CPU}} = 100\,\text{MHz}$ and an average of $C_{\text{op}} = 4$ (where C_{op} denotes the average number of CPU clock cycles required to perform a single floating-point operation) the total number of CPU cycles can be calculated as:

$$C_{\text{Total}} = \text{FLOPs}_{\text{Total}} \times C_{\text{op}} = 4513 \times 4 = 18{,}052. \tag{5.15}$$

The corresponding inference time is then computed as:

$$t_{\text{inference}} = \frac{C_{\text{Total}}}{f_{\text{CPU}}} = \frac{18{,}052}{100 \times 10^6} = 0.18\,\text{ms}. \tag{5.16}$$

This estimate does not include the memory access time and also assumes that the processor is fully dedicated to this task. When this process is implemented in MATLAB on a computer with an Intel Core i5 processor (1.3 GHz) and 16 GB of RAM, where the CPU is not solely dedicated to this process, it takes about 1.1 milliseconds. This result demonstrates that the proposed scheme satisfies the strict timing constraints of real-time digital protection systems, making it suitable for high-speed embedded applications.

5.4.4 Feature Importance Analysis

To quantify how much each wavelet-based feature influences fault-zone classification, the mean decrease in Gini impurity is calculated for each feature in the trained RF. These features, i.e., the relative energy at each decomposition level for all three phases, were grouped by level, and the corresponding importance scores were summed within each group. The resulting normalized contributions are depicted in Fig. 5.18, where each bar represents the total importance of detail coefficients D_1–D_5. The fifth and third decomposition levels,

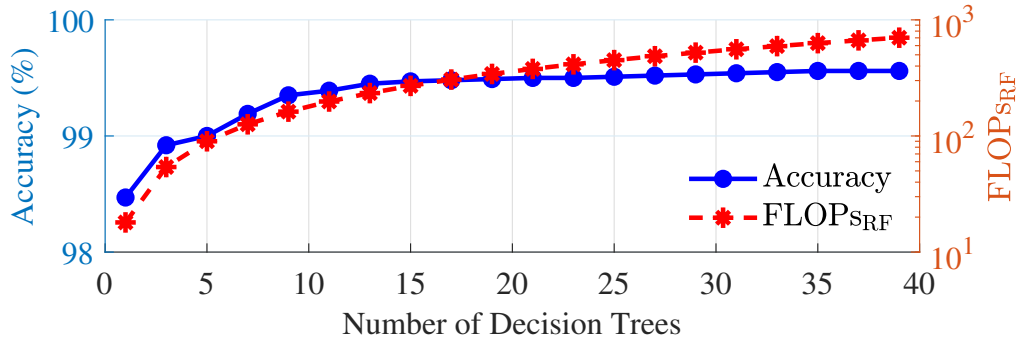


Figure 5.17: Accuracy and required FLOPs of the proposed RF classifier for varying numbers of decision trees.

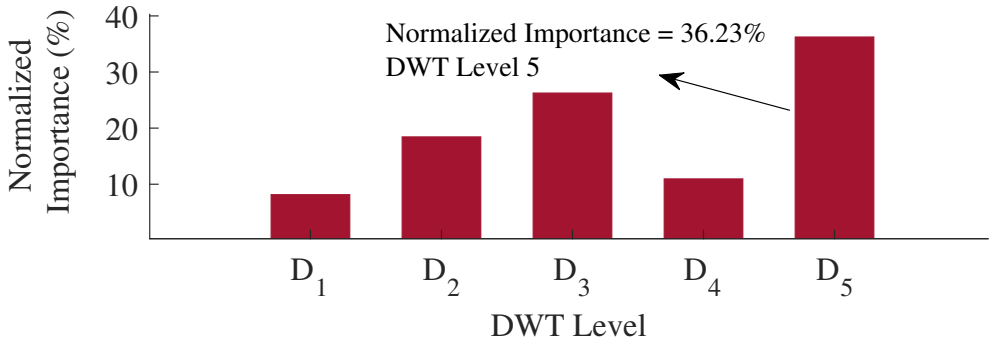


Figure 5.18: Normalized importance of wavelet detail levels in fault zone classification.

D_5 and D_3, dominate the decision process, contributing approximately 36% and 26% of the total importance, respectively.

5.4.5 Impact of Wavelet Type on Classifier Performance

To evaluate the influence of wavelet type on the performance of the proposed protection method, the RF classifier was trained using features extracted from several commonly used wavelets, including Haar, Daubechies-2 (db2), Daubechies-4 (db4), and Daubechies-6 (db6). All experiments were conducted using the same training dataset, classifier configuration, and fault simulation parameters described in Section 5.4.1. Table 5.4 summarizes the classification accuracy and computational cost for each wavelet. The results show that while some alternatives achieve slightly higher accuracy, the Haar wavelet offers a better trade-off between accuracy and computational efficiency, making it the most practical

Table 5.4: Performance Comparison for Different Wavelets.

Wavelet Type	**Accuracy (%)**	**False Trip (%)**	**No Trip (%)**	**Backup Mal.** (%)	**Inference Time (ms)**
Haar	99.56	0.01	0.00	0.32	0.18
Daubechies-2	99.90	0.04	0.00	0.06	0.339
Daubechies-4	99.95	0.01	0.0	0.03	0.658
Daubechies-6	99.96	0.01	0.00	0.0	0.976

Table 5.5: Performance Comparison for Different ML Models.

Model	**Accuracy (%)**	**False Trip (%)**	**No Trip (%)**	**Backup Mal. (%)**	**Inference Time (ms)**
DT	98.8	0.17	0.08	0.64	0.158
RF	99.56	0.01	0.00	0.32	0.180
SVM	92.75	2.97	0.01	2.62	0.495
k-NN	98.8	0.17	0.01	0.67	0.819
CNN	97.2	0.57	0.49	1.14	7.7

option for the proposed method.

5.4.6 Comparative Analysis

To justify the choice of RF for the proposed fault zone classification scheme, a comparative evaluation was conducted against representative models from various machine learning methods, including a single decision tree (DT), a support vector machine (SVM) with an RBF kernel, a k-NN classifier, and a CNN. All models were trained using the same dataset described in Section 5.4.1, with input features extracted from the DWT-based relative energy values of the traveling wave signals. Table 5.5 summarizes their classification performance and inference time. As shown in the table, the RF achieves the highest classification accuracy while maintaining the second-lowest inference time, offering a favorable balance between accuracy and computational efficiency. This makes RF the most effective and practical choice for the proposed method.

5.5 Conclusion

This chapter presented a cyber-resilient protection scheme designed to operate as a backup to conventional distance relays during cyberattacks in digital substations. By leveraging the physical signatures of TWs and machine learning–based classification, the proposed method ensures reliable fault zone identification when the substation is compromised and the SVs are no longer reliable. The scheme utilizes a DWT and an RF classifier trained on frequency-dependent attenuation patterns extracted from the first TW of phase currents. The hard-wired connection to the CT ensures immunity to communication-layer vulnerabilities, enabling secure and robust current measurement during cyber events. Simulation studies conducted on the IEEE 39-bus system confirm that the method achieves high fault classification accuracy across various fault types, locations, and conditions. Furthermore, the proposed approach exhibits low computational complexity and fast response times, making it suitable for practical applications. These results highlight the potential of the method to enhance power system resilience by maintaining protective functionality under cyber-compromised scenarios.

Chapter 6

Conclusion

6.1 Summary

The digital transformation of power systems, driven by the need for enhanced reliability, real-time control, and situational awareness, introduced a growing reliance on WAMPAC systems and digital substations. While these technologies offered significant operational benefits, they also exposed the power grid to a broader and more sophisticated range of cyber threats. Among cyber threats to digitalized power systems, FDIAs were particularly concerning due to their stealth and disruptive potential. In response to emerging threats, this dissertation examined critical vulnerabilities of power systems to two high-impact FDIAs: (i) attacks targeting state estimation in WAMPAC systems, and (ii) attacks compromising distance protection relays in digital substations. Following this analysis, the dissertation proposed targeted defense strategies to mitigate these threats.

This thesis began by analyzing the vulnerability of power systems to multi-step SFDIAs—an often-overlooked yet highly impactful threat targeting state estimation. To evaluate this vulnerability, a framework was proposed based on a MDP combined with bi-level optimization. The MDP, solved using Q-learning Reinforcement Algorithm (Q-learning), modeled the attacker's sequential decision-making process and produced a vulnerability index that enabled system operators to assess attack severity and identify critical stages for targeted defense.

Although a PDC gathers several correlated PMUs—access to which is required for launching SFDIAs—most defense strategies focused solely on securing individual PMUs, overlooking critical vulnerabilities at the PDC level. To address this gap, this thesis proposed a tri-level DAO optimization framework to redesign PMU-to-SPDC assignments,

aiming to minimize vulnerability to SFDIAs. By leveraging SDN, the framework enabled reconfiguration of the network structure without incurring additional costs, providing power system operators with a practical and effective defense strategy against SFDIAs.

Strengthening data aggregation–based defenses required considering both PMU-to-PDC assignments and cyber-layer structures, including communication paths, as targets for SFDIAs mitigation. Building on this insight, the thesis analyzed the often-overlooked role of the cyber layer in vulnerability to SFDIAs and introduced a CPRM that combined both the likelihood and physical impact of such attacks. The CPRM evaluated the consequences of losing transmission lines alongside the probability that these losses could result from an SFDIA. This probability was estimated by identifying minimal critical PMU sets whose compromise could stealthily overload transmission lines, using a bi-level optimization algorithm. Additionally, BAGs were employed to model potential attack pathways and estimate access probabilities for substations and communication links. To mitigate these risks, the thesis proposed a DAR scheme that leveraged SDN to dynamically reconfigure both PMU-to-PDC assignments and their communication paths, thereby enhancing system resilience against SFDIAs.

Finally, this thesis investigated FDIAs targeting protection measurements, with a focus on the vulnerability of distance relays in digital substations. The analysis demonstrated that falsified measurements could severely compromise the fault detection and isolation capabilities of these relays, thereby threatening system stability. To counter this threat, a cyber-resilient protection scheme was proposed that activated during cyber incidents, temporarily backing up distance relays to maintain system security and stability. The proposed strategy replicated the zone-based fault detection functionality of conventional distance relays but instead relied on TWs—the natural signatures of real faults—along with dedicated hard-wired current measurements and a RF classifier for fault zone identification. The RF classifier was trained on the attenuation patterns of TW frequency components as they propagated from fault locations to line terminals. Since these attenuation patterns depended on both frequency and propagation distance, the classifier accurately identified the fault zone by extracting frequency-domain features from the first arriving TWs using wavelet transform techniques and analyzing their attenuation characteristics.

The contents of each chapter can be summarized as follows:

- **Chapter 2** established that relying solely on defenses against the most severe single-step SFDIAs, as commonly found in the literature, is insufficient for ensuring system resilience. It then developed a framework based on Markov Decision Processes and bi-level optimization to calculate a vulnerability index for multi-step SFDIAs. This index enables utilities to balance the costs of securing PMUs, improving monitoring,

or reconfiguring network topology against the potential consequences of such attacks. The proposed framework also identified the most critical actions at each stage of a multi-step SFDIA, supporting operators in implementing more effective defense strategies. Finally, simulation results on the IEEE 39-bus system demonstrated the framework's effectiveness in pinpointing critical attack vectors, confirmed the value of the vulnerability index across scenarios, and highlighted the role of line recovery rates in mitigating multi-step attack impacts.

- **Chapter 3** demonstrated that conventional data aggregation methods in WAMSs can expose power grids to economic and physical risks under LR attacks. To mitigate these vulnerabilities, a tri-level optimization framework was proposed to determine the optimal PMU-to-SPDC data aggregation scheme, taking into account both grid resilience against cyberattacks and practical constraints such as communication delays. The chapter showed how the objective function can be tuned to prioritize minimizing economic or physical vulnerabilities, depending on the system's needs. Furthermore, it discussed how the proposed method can dynamically adapt to changes in the grid's operating point through SDN. Finally, by applying the framework to the IEEE 30-bus system, it was shown that the proposed approach significantly improves grid resilience while a case reduction technique was introduced to achieve high accuracy with much faster computation.

- **Chapter 4** proposes a new CPRM to assess the system's vulnerability to SFDIAs. The CPRM combines the physical impact of losing a transmission line—such as load shedding or generation loss—with the probability of such a loss resulting from an SFDIA. The likelihood of losing a transmission line is estimated by identifying all critical PMUs sets, defined as sets whose measurements can be manipulated to stealthily overload the line. These critical PMUs sets are determined using an algorithm that solves multiple bi-level optimization problems. Next, BAGs are developed for each substation and communication link to model potential access pathways and calculate the probability of compromising the identified critical PMUs sets. Building on this analysis, the chapter introduces a novel DAR scheme that dynamically modifies the cyber-layer structure using SDN to minimize the risk of SFDIAs.

- **Chapter 5** presented a cyber-resilient backup protection scheme for distance relays in digital substations, designed to maintain protection functions during cyberattacks. The proposed method leverages traveling wave physical signatures and a Random Forest classifier trained on features from the first traveling wave, extracted through discrete wavelet transform, to reliably identify fault zones even when sampled values are compromised. By using hard-wired connections to current transformers,

the scheme avoids communication-layer vulnerabilities and ensures secure current measurements. Simulation studies on the IEEE 39-bus system confirmed high fault classification accuracy, low computational complexity, and fast response times across different fault scenarios. These results demonstrate that the proposed approach can significantly enhance power system resilience under cyber-compromised conditions.

6.2 Contributions

The research presented in this dissertation made the following key contributions:

- Developed a vulnerability assessment framework based on a MDP combined with bi-level optimization to quantify the risk of multi-step SFDIAs. This framework introduces a vulnerability index that helps operators weigh defense costs and prioritize protection strategies, with demonstrated effectiveness on the IEEE 39-bus system.
- Proposed a tri-level defender–attacker–operator optimization framework to redesign PMU-to-SPDC data aggregation in wide-area monitoring systems. By incorporating SDN, the scheme dynamically adapts to changing grid conditions and optimizes the trade-off between communication constraints and resilience, as validated through IEEE 30-bus system simulations with improved computational efficiency.
- Introduced a CPRM that integrates the probability and physical consequences of line losses caused by SFDIAs. Using Bayesian attack graphs to estimate compromise probabilities of critical PMU sets, the approach supports proactive risk mitigation. A data aggregation reconfiguration scheme based on SDN was also developed to dynamically reduce these vulnerabilities.
- Designed a cyber-resilient backup protection scheme for distance relays in digital substations, using traveling wave features and a Random Forest classifier to identify fault zones even under cyberattacks compromising sampled values. By employing hard-wired measurements, the scheme ensures secure, low-latency, and reliable fault detection, as demonstrated on the IEEE 39-bus system.

6.3 Directions for Future Work

Although this dissertation has made significant advances in defending power system state estimation and protection schemes against stealthy false data injection attacks, there are

several promising directions for future research:

- **Limited-data stealthy FDIAs:** Much of the existing literature on stealthy false data injection attacks assumes that attackers have complete knowledge of the power system, even though operators generally protect system data and frequently modify configurations. Motivated by recent research on blind or data-driven FDIAs, future work could examine how attackers with limited or partial knowledge might still design high-impact attacks. One promising direction would involve building predictive models of the system's response using infiltrated measurements and publicly available data, and then applying reinforcement learning to strategically optimize multi-step stealthy FDIAs without full system knowledge. Such investigations would expand understanding of emerging threat scenarios and support the development of more robust and adaptive defense strategies.

- **Machine learning for scalable data aggregation:** As power systems become larger and more complex, optimizing the structure of data gathering and aggregation presents significant computational challenges. Future research could explore the use of machine learning techniques to enhance the scalability, speed, and adaptability of data aggregation frameworks, enabling more efficient and responsive data flows for monitoring, protection, and control across large-scale power systems. Such approaches could help operators better manage cyber-physical risks while maintaining high situational awareness with minimal computational overhead.

- **Other substation protection schemes:** While this work focused on distance protection, many other substation protection schemes — such as differential protection, directional overcurrent relays, and busbar protection — also rely heavily on digital measurements and communications, making them potentially vulnerable to cyberattacks. Future research could investigate the specific vulnerabilities of these schemes under false data injection and other cyberattack scenarios, and develop dedicated defense mechanisms to ensure secure, coordinated, and resilient protection across the entire substation infrastructure.

References

[1] MATPOWER: A MATLAB power system simulation package. Online, http://www.pserc.cornell.edu/matpower/.

[2] Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations. https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf, 2003. [Online; accessed 2023-05-23].

[3] Ieee standard communication delivery time performance requirements for electric power substation automation. *IEEE Std 1646-2004*, pages 1–36, 2005.

[4] PMU networking with IP multicast. Technical report, CISCO, 2012.

[5] Standard prc-023-1 — transmission relay loadability, 2024. Accessed: 2024-05-23.

[6] Uttam Adhikari, Thomas Morris, and Shengyi Pan. Wams cyber-physical test bed for power system, cybersecurity study, and data mining. *IEEE Transactions on Smart Grid*, 8(6):2744–2753, 2016.

[7] Naqash Ahmad, Yazeed Ghadi, Muhammad Adnan, and Mansoor Ali. Load forecasting techniques for power system: Research challenges and survey. *IEEE Access*, 10:71054–71090, 2022.

[8] Parisa Akaber, Bassam Moussa, Mohsen Ghafouri, Ribal Atallah, Basile L Agba, Chadi Assi, and Mourad Debbabi. Cases: concurrent contingency analysis-based security metric deployment for the smart grid. *IEEE Transactions on Smart Grid*, 11(3):2676–2687, 2019.

[9] Abdullah Al Mamun, Md Sohel, Naeem Mohammad, Md Samiul Haque Sunny, Debopriya Roy Dipta, and Eklas Hossain. A comprehensive review of the load forecasting techniques using single and hybrid predictive models. *IEEE access*, 8:134911–134939, 2020.

[10] Natalia Alguacil, Andrés Delgadillo, and José M Arroyo. A trilevel programming approach for electric grid defense planning. *Computers & Operations Research*, 41:282–290, 2014.

[11] Hassan Haes Alhelou, Almoataz Y Abdelaziz, and Pierluigi Siano. *Wide area power systems stability, protection, and security*. Springer, 2020.

[12] Muhammad Shoaib Almas, Luigi Vanfretti, Ravi S Singh, and Gudrun M Jonsdottir. Vulnerability of synchrophasor-based wampac applications' to time synchronization spoofing. *IEEE Transactions on Smart Grid*, 9(5):4601–4612, 2017.

[13] Amir Ameli, Abdelrahman Ayad, Ehab F El-Saadany, Magdy MA Salama, and Amr Youssef. A learning-based framework for detecting cyber-attacks against line current differential relays. *IEEE Transactions on Power Delivery*, 36(4):2274–2286, 2020.

[14] Amir Ameli, Ali Hooshyar, and Ehab F El-Saadany. Development of a cyber-resilient line current differential relay. *IEEE Transactions on Industrial Informatics*, 15(1):305–318, 2018.

[15] Amir Ameli, Ali Hooshyar, Ehab F El-Saadany, and Amr M Youssef. An intrusion detection method for line current differential relays. *IEEE Transactions on Information Forensics and Security*, 15:329–344, 2019.

[16] Amir Ameli, Khaled A Saleh, Ehab F El-Saadany, Magdy MA Salama, and Hatem H Zeineldin. Wide-band current transformers for traveling-waves-based protection applications. *IEEE Transactions on Smart Grid*, 12(1):845–858, 2020.

[17] Ameli Amir and Sarjan Hamed. False data injection attacks in power systems. *Wiley Encyclopedia of Electrical and Electronics Engineering*, pages 1–15, 1999.

[18] Paul M Anderson, Charles F Henville, Rasheek Rifaat, Brian Johnson, and Sakis Meliopoulos. *Power system protection*. John Wiley & Sons, 2021.

[19] UD Annakkage, PG McLaren, E Dirks, RP Jayasinghe, and AD Parker. A current transformer model based on the jiles-atherton theory of ferromagnetic hysteresis. *IEEE transactions on power delivery*, 15(1):57–61, 2000.

[20] Souhila Aoufi, Abdelouahid Derhab, and Mohamed Guerroumi. Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. *Journal of Information Security and Applications*, 54:102518, 2020.

[21] Mohammadmahdi Asghari, Amir Ameli, Mohsen Ghafouri, and Mohammad N. Uddin. On the economic vulnerability analysis of power grids to false data injection attacks against wide area measurement systems. In *2022 IEEE 1st Industrial Electronics Society Annual On-Line Conference (ONCON)*, pages 1–6, 2022.

[22] Aditya Ashok, Manimaran Govindarasu, and Venkataramana Ajjarapu. Online detection of stealthy false data injection attacks in power system state estimation. *IEEE Transactions on Smart Grid*, 9(3):1636–1646, 2016.

[23] Abdul Azeem, Idris Ismail, Syed Muslim Jameel, and Vivekananda Rajah Harindran. Electrical load forecasting models for different generation modalities: a review. *IEEE Access*, 9:142239–142263, 2021.

[24] Vicki M Bier, Eli R Gratz, Naraphorn J Haphuriwat, Wairimu Magua, and Kevin R Wierzbicki. Methodology for identifying near-optimal interdiction strategies for a power transmission system. *Reliability Engineering & System Safety*, 92(9):1155–1161, 2007.

[25] Di Cao, Weihao Hu, Junbo Zhao, Guozhou Zhang, Bin Zhang, Zhou Liu, Zhe Chen, and Frede Blaabjerg. Reinforcement learning and its applications in modern power and energy systems: A review. *Journal of modern power systems and clean energy*, 8(6):1029–1042, 2020.

[26] Liang Che, Xuan Liu, and Zuyi Li. Mitigating false data attacks induced overloads using a corrective dispatch scheme. *IEEE Transactions on Smart Grid*, 10(3):3081–3091, 2018.

[27] Liang Che, Xuan Liu, and Zuyi Li. Fast screening of high-risk lines under false data injection attacks. *IEEE Transactions on Smart Grid*, 10(4):4003–4014, 2019.

[28] Liang Che, Xuan Liu, Zuyi Li, and Yunfeng Wen. False data injection attacks induced sequential outages in power systems. *IEEE Transactions on Power Systems*, 34(2):1513–1523, 2018.

[29] Zhigang Chu, Jiazi Zhang, Oliver Kosut, and Lalitha Sankar. $n-1$ reliability makes it difficult for false data injection attacks to cause physical consequences. *IEEE Transactions on Power Systems*, 36(5):3897–3906, 2021.

[30] Hwei-Ming Chung, Wen-Tai Li, Chau Yuen, Wei-Ho Chung, Yan Zhang, and Chao-Kai Wen. Local cyber-physical attack for masking line outage and topology attack in smart grid. *IEEE Transactions on Smart Grid*, 10(4):4577–4588, 2018.

[31] Hamzeh Davarikia and Masoud Barati. A tri-level programming model for attack-resilient control of power grids. *Journal of Modern Power Systems and Clean Energy*, 6(5):918–929, 2018.

[32] Min Du, Xuan Liu, Zuyi Li, and Hai Lin. Robust mitigation strategy against dummy data attacks in power systems. *IEEE Transactions on Smart Grid*, 2023.

[33] Onur Duman, Mengyuan Zhang, Lingyu Wang, Mourad Debbabi, Ribal F Atallah, and Bernard Lebel. Factor of security (fos): quantifying the security effectiveness of redundant smart grid subsystems. *IEEE Transactions on Dependable and Secure Computing*, 19(2):1018–1035, 2020.

[34] Fariborz Haghighatdar Fesharaki, Rahmat-Allah Hooshmand, and Amin Khodabakhshian. Simultaneous optimal design of measurement and communication infrastructures in hierarchical structured wams. *IEEE Transactions on Smart Grid*, 5(1):312–319, 2013.

[35] José Fortuny-Amat and Bruce McCarl. A representation and economic interpretation of a two-level programming problem. *Journal of the operational Research Society*, 32(9):783–792, 1981.

[36] Jian Fu, Weixin Zhang, Bo Hu, Kaigui Xie, Leibao Wang, Gang Wang, and Lu Zhong. A tri-level defense model against load redistribution attacks. In *2019 IEEE Sustainable Power and Energy Conference (iSPEC)*, pages 1606–1611. IEEE, 2019.

[37] Shayan Mohajer Hamidi, Amir Ameli, Mohsen Ghafouri, and Felipe V Lopes. A learning-based framework for locating faults on power grid lines based on distortion of traveling waves. *IEEE Transactions on Instrumentation and Measurement*, 71:1–15, 2022.

[38] Keqiang He, Junaid Khalid, Sourav Das, Aaron Gember-Jacobson, Chaithan Prakash, Aditya Akella, Li Erran Li, and Marina Thottan. Latency in software defined networks: Measurements and mitigation techniques. In *Proceedings of the 2015 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, pages 435–436, 2015.

[39] Junho Hong, Reynaldo F Nuqui, Anil Kondabathini, Dmitry Ishchenko, and Aaron Martin. Cyber attack resilient distance protection and circuit breaker control for digital substations. *IEEE Transactions on Industrial Informatics*, 15(7):4332–4341, 2018.

[40] Ali Hooshyar, Majid Sanaye-Pasand, Saeed Afsharnia, Mahdi Davarpanah, and Bashir Mahdi Ebrahimi. Time-domain analysis of differential power signal to detect magnetizing inrush in power transformers. *IEEE Transactions on power delivery*, 27(3):1394–1404, 2012.

[41] Yudi Huang, Ting He, Nilanjan Ray Chaudhuri, and Thomas F La Porta. Preventing outages under coordinated cyber–physical attack with secured pmus. *IEEE Transactions on Smart Grid*, 13(4):3160–3173, 2022.

[42] Gabriela Hug and Joseph Andrew Giampapa. Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks. *IEEE Transactions on smart grid*, 3(3):1362–1370, 2012.

[43] Amir Abiri Jahromi, Anthony Kemmeugne, Deepa Kundur, and Aboutaleb Haddadi. Cyber-physical attacks targeting communication-assisted protection schemes. *IEEE Transactions on Power Systems*, 35(1):440–450, 2020.

[44] Liyan Jia, Jinsub Kim, Robert J Thomas, and Lang Tong. Impact of data quality on real-time locational marginal price. *IEEE Transactions on Power Systems*, 29(2):627–636, 2013.

[45] Sameera Kancherla and Ian Dobson. Heavy-tailed transmission line restoration times observed in utility data. *IEEE Transactions on Power Systems*, 33(1):1145–1147, 2018.

[46] Prashant Kansal and Anjan Bose. Bandwidth and latency requirements for smart transmission grid applications. *IEEE Transactions on Smart Grid*, 3(3):1344–1352, 2012.

[47] Reem Kateb, Parisa Akaber, Mosaddek HK Tushar, Abdullah Albarakati, Mourad Debbabi, and Chadi Assi. Enhancing wams communication network against delay attacks. *IEEE Transactions on Smart Grid*, 10(3):2738–2751, 2018.

[48] Reem Kateb, Mosaddek Hossain Kamal Tushar, Chadi Assi, and Mourad Debbabi. Optimal tree construction model for cyber-attacks to wide area measurement systems. *IEEE Transactions on Smart Grid*, 9(1):25–34, 2016.

[49] Reem Kateb, Mosaddek Hossain Kamal Tushar, Chadi Assi, and Mourad Debbabi. Optimal tree construction model for cyber-attacks to wide area measurement systems. *IEEE Transactions on Smart Grid*, 9(1):25–34, 2018.

[50] Kiarash Gharani Khajeh, Erfan Bashar, Ali Mahboub Rad, and Gevork B Gharehpetian. Integrated model considering effects of zero injection buses and conventional measurements on optimal pmu placement. *IEEE Transactions on Smart Grid*, 8(2):1006–1013, 2015.

[51] Ramin Khalili, Zoran Despotovic, and Artur Hecker. Flow setup latency in sdn networks. *IEEE Journal on Selected Areas in Communications*, 36(12):2631–2639, 2018.

[52] Yew Meng Khaw, Amir Abiri Jahromi, Mohammadreza FM Arani, Scott Sanner, Deepa Kundur, and Marthe Kassouf. A deep learning-based cyberattack detection system for transmission protective relays. *IEEE Transactions on Smart Grid*, 12(3):2554–2565, 2020.

[53] Xiaohui Li, Yu-Chu Tian, Gerard Ledwich, Yateendra Mishra, Xiaoqing Han, and Chunjie Zhou. Constrained optimization of multicast routing for wide area control of smart grid. *IEEE Transactions on Smart Grid*, 10(4):3801–3808, 2018.

[54] Jingwen Liang, Lalitha Sankar, and Oliver Kosut. Vulnerability analysis and consequences of false data injection attack on power system state estimation. *IEEE Transactions on Power Systems*, 31(5):3864–3872, 2015.

[55] Hui Lin, Chen Chen, Jianhui Wang, Junjian Qi, Dong Jin, Zbigniew T. Kalbarczyk, and Ravishankar K. Iyer. Self-healing attack-resilient pmu network for power system operation. *IEEE Transactions on Smart Grid*, 9(3):1551–1565, 2018.

[56] Chensheng Liu, Wangli He, Ruilong Deng, Yu-Chu Tian, and Wenli Du. False-data-injection-enabled network parameter modifications in power systems: Attack and detection. *IEEE Transactions on Industrial Informatics*, 19(1):177–188, 2023.

[57] Ren Liu, Ceeman Vellaithurai, Saugata S Biswas, Thoshitha T Gamage, and Anurag K Srivastava. Analyzing the cyber-physical impact of cyber events on the power grid. *IEEE Transactions on Smart Grid*, 6(5):2444–2453, 2015.

[58] Rong-Peng Liu, Xiaozhe Wang, Bo Zeng, and Rawad Zgheib. Modeling load redistribution attacks in integrated electricity-gas systems. *IEEE Transactions on Smart Grid*, 15(4):4115–4127, 2024.

[59] Xuan Liu, Zhiyi Li, and Zuyi Li. Optimal protection strategy against false data injection attacks in power systems. *IEEE Transactions on Smart Grid*, 8(4):1802–1810, 2016.

[60] Xuan Liu, Zuyi Li, Zhikang Shuai, and Yunfeng Wen. Cyber attacks against the economic operation of power systems: A fast solution. *IEEE Transactions on Smart Grid*, 8(2):1023–1025, 2016.

[61] Xuan Liu, Zuyi Li, Zhikang Shuai, and Yunfeng Wen. Cyber attacks against the economic operation of power systems: A fast solution. *IEEE Transactions on Smart Grid*, 8(2):1023–1025, 2016.

[62] Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):1–33, 2011.

[63] Yigu Liu, Shibin Gao, Jian Shi, Xiaoguang Wei, and Zhu Han. Sequential-mining-based vulnerable branches identification for the transmission network under continuous load redistribution attacks. *IEEE Transactions on Smart Grid*, 11(6):5151–5160, 2020.

[64] Juan C. Lozano, Keerthi Koneru, Neil Ortiz, and Alvaro A. Cardenas. Digital substations and iec 61850: A primer. *IEEE Communications Magazine*, 61(6):28–34, 2023.

[65] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. Openflow: enabling innovation in campus networks. *ACM SIGCOMM computer communication review*, 38(2):69–74, 2008.

[66] Peter Mell, Karen Scarfone, and Sasha Romanosky. Common vulnerability scoring system. *IEEE Security & Privacy*, 4(6):85–89, 2006.

[67] Seyedamirabbas Mousavian, Jorge Valenzuela, and Jianhui Wang. A probabilistic risk mitigation model for cyber-attacks to pmu networks. *IEEE Transactions on Power Systems*, 30(1):156–165, 2015.

[68] Bassam Moussa, Abdullah Al-Barakati, Marthe Kassouf, Mourad Debbabi, and Chadi Assi. Exploiting the vulnerability of relative data alignment in phasor data concentrators to time synchronization attacks. *IEEE Transactions on Smart Grid*, 11(3):2541–2551, 2019.

[69] Da-Tian Peng, Jianmin Dong, and Qinke Peng. Overloaded branch chains induced by false data injection attack in smart grid. *IEEE Signal Processing Letters*, 27:426–430, 2020.

[70] Thomas Pfeiffenberger and Jia Lei Du. Evaluation of software-defined networking for power systems. In *2014 IEEE International Conference on Intelligent Energy and Power Systems (IEPS)*, pages 181–185. IEEE, 2014.

[71] Saad Pola, Marko Jovanovic, Maher A Azzouz, and Mitra Mirhassani. Cyber resiliency enhancement of overcurrent relays in distribution systems. *IEEE Transactions on Smart Grid*, 15(4):4063–4076, 2023.

[72] HB Püttgen. Computational cycle time evaluation for steady state power flow calculations. *Thomson-CSF, Division Simulateurs, La Défense, France*, 1985.

[73] Vetrivel Subramaniam Rajkumar, Alexandru Ştefanov, Alfan Presekal, Peter Palensky, and José Luis Rueda Torres. Cyber attacks on power grids: Causes and propagation of cascading failures. *IEEE Access*, 11:103154–103176, 2023.

[74] Ahmad Mohammad Saber, Amr Youssef, Davor Svetinovic, Hatem H Zeineldin, and Ehab F El-Saadany. Anomaly-based detection of cyberattacks on line current differential relays. *IEEE Transactions on Smart Grid*, 13(6):4787–4800, 2022.

[75] Ahmad Mohammad Saber, Amr Youssef, Davor Svetinovic, Hatem H Zeineldin, and Ehab F El-Saadany. Cyber-immune line current differential relays. *IEEE Transactions on Industrial Informatics*, 20(3):3597–3608, 2023.

[76] Srikrishna Sarangan, Vivek Kumar Singh, and Manimaran Govindarasu. Cyber attack-defense analysis for automatic generation control with renewable energy sources. In *2018 North American Power Symposium (NAPS)*, pages 1–6. IEEE, 2018.

[77] Maria P Scaparra and Richard L Church. A bilevel mixed-integer program for critical infrastructure protection planning. *Computers & Operations Research*, 35(6):1905–1923, 2008.

[78] Schweitzer Engineering Laboratories. *SEL-411L Instruction Manual: Advanced Line Differential Protection, Automation, and Control System.* Schweitzer Engineering Laboratories, December 2024. [Online].

[79] Schweitzer Engineering Laboratories, Inc. *SEL-T401L Ultra-High-Speed Line Relay Instruction Manual.* Schweitzer Engineering Laboratories, Pullman, WA, USA, 2024. Document No. 20240524.

[80] H. Shayan and T. Amraee. Network constrained unit commitment under cyber attacks driven overloads. *IEEE Transactions on Smart Grid*, 10(6):6449–6460, 2019.

[81] V.K. Sood, D. Fischer, J.M. Eklund, and T. Brown. Developing a communication infrastructure for the smart grid. In *2009 IEEE Electrical Power & Energy Conference (EPEC)*, pages 1–7, 2009.

[82] Kin Cheong Sou. Protection placement for power system state estimation measurement data integrity. *IEEE Transactions on Control of Network Systems*, 7(2):638–647, 2019.

[83] IEC Standard. Network engineering guideline for communication networks and systems in substations. *tech. rep., IEC 61850-90-4*, 2013.

[84] Richard S Sutton and Andrew G Barto. *Reinforcement learning: An introduction*. MIT press, 2018.

[85] Yi Tan, Yong Li, Yijia Cao, and Mohammad Shahidehpour. Cyber-attack on overloading multiple lines: A bilevel mixed-integer linear programming model. *IEEE Transactions on Smart Grid*, 9(2):1534–1536, 2017.

[86] Vladimir Terzija. Wide area monitoring protection and control-wampac. In *IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007)*, pages 1119–1126. IET, 2007.

[87] Meng Tian, Mingjian Cui, Zhengcheng Dong, Xianpei Wang, Shengfei Yin, and Le Zhao. Multilevel programming-based coordinated cyber physical attacks and countermeasures in smart grid. *IEEE Access*, 7:9836–9847, 2019.

[88] Saghar Vahidi, Mohsen Ghafouri, Minh Au, Marthe Kassouf, Arash Mohammadi, and Mourad 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*, pages 1–1, 2023.

[89] Saghar Vahidi, Mohsen Ghafouri, Minh Au, Marthe Kassouf, Arash Mohammadi, and Mourad 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*, 25(2):1294–1335, 2023.

[90] Kehe Wu, Jiawei Li, Bo Zhang, Zongchao Yu, and Xuan Liu. Preventive dispatch strategy against fdia induced overloads in power systems with high wind penetration. *IEEE Access*, 8:210452–210461, 2020.

[91] Xuan Wu and Antonio J Conejo. An efficient tri-level optimization model for electric grid defense planning. *IEEE Transactions on Power Systems*, 32(4):2984–2994, 2016.

[92] Yingmeng Xiang and Lingfeng Wang. An improved defender–attacker–defender model for transmission line defense considering offensive resource uncertainties. *IEEE Transactions on Smart Grid*, 10(3):2534–2546, 2018.

[93] Yingmeng Xiang, Lingfeng Wang, and Nian Liu. Coordinated attacks on electric power systems in a cyber-physical environment. *Electric Power Systems Research*, 149:156–168, 2017.

[94] Yanling Yuan, Zuyi Li, and Kui Ren. Modeling load redistribution attacks in power systems. *IEEE Transactions on Smart Grid*, 2(2):382–390, 2011.

[95] Yanling Yuan, Zuyi Li, and Kui Ren. Quantitative analysis of load redistribution attacks in power systems. *IEEE Transactions on Parallel and Distributed Systems*, 23(9):1731–1738, 2012.

[96] Ye Yuan, Steven H Low, Omid Ardakanian, and Claire J Tomlin. Inverse power flow problem. *IEEE Transactions on Control of Network Systems*, 2022.

[97] 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.

[98] Jiazi Zhang, Zhigang Chu, Lalitha Sankar, and Oliver Kosut. Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems? *IEEE Transactions on Power Systems*, 33(5):4775–4786, 2018.

[99] Qiwei Zhang and Fangxing Li. Cyber-vulnerability analysis for real-time power market operation. *IEEE Transactions on Smart Grid*, 12(4):3527–3537, 2021.

[100] Yichi Zhang, Lingfeng Wang, Yingmeng Xiang, and Chee-Wooi Ten. Power system reliability evaluation with scada cybersecurity considerations. *IEEE Transactions on Smart Grid*, 6(4):1707–1721, 2015.

[101] Zhenyong Zhang, Ruilong Deng, David KY Yau, Peng Cheng, and Jiming Chen. Analysis of moving target defense against false data injection attacks on power grid. *IEEE Transactions on Information Forensics and Security*, 15:2320–2335, 2019.

[102] Ray D Zimmerman, Carlos E Murillo-Sánchez, and Deqiang Gan. Matpower: A matlab power system simulation package. *Manual, Power Systems Engineering Research Center, Ithaca NY*, 1:10–7, 1997.

APPENDICES

Appendix A

List of Publications

The following is a list of publications by the author during doctoral studies.

A.1 Peer-Reviewed Journal Article

1. **M. Asghari**, A. Ameli, M. Ghafouri, and M. N. Uddin, "Optimal Data Aggregation Reconfiguration Scheme to Mitigate Stealthy False Data Injection Attacks in Energy Management Systems," *IEEE Transactions on Smart Grid*, vol. 16, no. 4, pp. 3269–3281, July 2025.

2. **M. Asghari**, A. Ameli, M. Ghafouri, and M. N. Uddin, "Development and Impact Assessment of Multi-Step Stealthy False Data Injection Attacks Against Power Systems," *IEEE Journal of Modern Power Systems and Clean Energy*, accepted for publication, July 2025.

A.2 Under-Review Journal Articles

1. **M. Asghari**, A. Ameli, J. Southgate, A. Doostmohammadi, M. Ghafouri, and M. N. Uddin, "Cyber-Resilient Fault Diagnosis in Transmission Lines: A Substitute for Distance Relays Under Cyber-Attacks," *IEEE Transactions on Instrumentation and Measurement*, revision submitted.

2. **M. Asghari**, M. Zadsar, A. Ameli, M. Ghafouri, and M. N. Uddin "Optimal Data Aggregation in Wide Area Measurement Systems: A Cyber-Security Approach," *IEEE Transactions on Industry Applications*, revision submitted.

A.3 Book Chapter

1. **M. Asghari**, A. Ameli, M. Ghafouri, and M. N. Uddin, "Application of State Observers and Filters in Protection and Cyber-Security of Power Grids," in *Smart Cyber-Physical Power Systems: Fundamental Concepts, Challenges, and Solutions*, vol. 1, pp. 451–503, 2025.

A.4 Conference Proceedings

1. **M. Asghari**, A. Ameli, M. Ghafouri, and M. N. Uddin, "On the Economic Vulnerability Analysis of Power Grids to False Data Injection Attacks Against Wide Area Measurement Systems," *Proceedings of the 2022 IEEE 1st Industrial Electronics Society Annual On-Line Conference (ONCON)*, Kharagpur, India, 2022, pp. 1–6.

2. **M. Asghari**, A. Ameli, M. Ghafouri, and M. N. Uddin, "Unveiling a New Vulnerability in Modern Power Systems: Leveraging Publicly-Available LMPs for Crafting Cyber-Attacks," *Proceedings of the 2023 IEEE 2nd Industrial Electronics Society Annual On-Line Conference (ONCON)*, South Carolina, USA, 2023, pp. 1–6.

3. **M. Asghari**, A. Ameli, M. Ghafouri, and M. N. Uddin, "Assessing the Vulnerability of Power Systems to False Data Injection Attacks: A Bayesian Attack Graph-Based Approach," *Proceedings of the 2024 IEEE International Conference on Environment and Electrical Engineering (EEEIC) / Industrial and Commercial Power Systems Europe (I&CPS Europe)*, Rome, Italy, 2024, pp. 1–6.