Md Fazle Hasan Shiblee

Enhanced Cyber Resilient Load Frequency Control Scheme

School of Technology and Innovations

MSc in Technology

Major in Smart Grids

Master’s Programme in Smart Energy

Erasmus Mundus Joint Master’s Programme in Smart Cities and Communities

Vaasa 2026

Acknowledgements

I would like to express my sincere gratitude to my academic supervisor, Professor **Hannu Laaksonen**, for his continuous guidance, unwavering support, and valuable insights throughout the development of this thesis. His expertise and constructive feedback have been instrumental in shaping this work and deepening my understanding of the subject, and I am truly grateful for the time and dedication he invested in mentoring me throughout this journey.

I would also like to acknowledge the Erasmus Mundus Joint Master Programme in Smart Cities and Communities (SMACCs) and its partner universities for providing an enriching academic environment and the opportunity to pursue this research. The programme has been a truly rewarding experience, both academically and personally.

I extend my heartfelt thanks to my family and friends for their constant encouragement, patience, and unconditional support throughout my studies. Their motivation and belief in me have been invaluable in bringing this work to completion.

Use of Artificial Intelligence

During the preparation of this thesis, the author used artificial intelligence (AI) tools, including ChatGPT, Grammarly, and Claude, primarily to enhance the quality of academic writing. These tools were used for grammar correction, language refinement, sentence restructuring, readability improvement, paraphrasing suggestions, formatting assistance, and the review of writing style and clarity.

All AI-generated suggestions were carefully reviewed, verified, and modified where necessary by the author before inclusion in the thesis. The author takes full responsibility for the content of this thesis and confirms that all research activities, analyses, interpretations, results, discussions, and conclusions were independently developed and validated by the author. The use of AI tools was limited to writing support and did not replace the author's critical thinking, scientific judgment, or original contributions.

VAASAN YLIOPISTO
School of Technology and Innovations
Author: Md Fazle Hasan Shiblee
Thesis title: Enhanced Cyber Resilient Load Frequency Control Scheme
Degree: MSc in Technology
Supervisor: Hannu Laaksonen
Year of graduation: 2026 **Number of pages:** 118

ABSTRACT:
This study develops an integrated framework for improving load frequency control (LFC) performance and cyber resilience in modern interconnected power systems. A two-area multi-source power system is modelled in MATLAB/Simulink, where each area includes reheat thermal, hydro, and gas generation units with governor deadband and generation rate constraints. Renewable uncertainty is incorporated through a 50 MW photovoltaic plant in Area 1 and a 70 MW wind plant in Area 2. For controller tuning, a hybrid metaheuristic algorithm, Particle Swarm Optimization Grey Wolf Optimizer with Adaptive Artificial Bee Colony (PGWA), is proposed to optimize PID gains by minimizing the integral time absolute error (ITAE). PGWA combines the global search capability of PSO, the hierarchical exploitation mechanism of GWO, and the stagnation recovery ability of ABC. Its performance is validated using benchmark functions and five LFC scenarios involving step load perturbations, random load variations, asymmetric dual-area disturbances, renewable penetration, and communication delay. The results show that PGWA consistently achieves lower error indices, smaller frequency and tie-line deviations, and faster settling than PSO, GWO, ABC, and Modified Hybrid ABCPSO (MHABCPSO). To address cybersecurity, an unsupervised Disturbance-Aware Contrastive GRU Autoencoder (DA-CGAE) is developed for false data injection attack detection and mitigation. The DA-CGAE model learns the normal operating patterns of the LFC system and detects abnormal behaviour through attention-guided BiGRU encoding, disturbance-sensitive reconstruction, and contrastive feature learning. It achieves 97.61% accuracy, 99.99% recall, 97.47% F1 score, and 99.93% AUC, outperforming LSTM, BiLSTM, and CNN baselines. The findings confirm the effectiveness of the proposed control and detection framework under complex and uncertain grid conditions.

Keywords: Load Frequency Control, False Data Injection, Cyber-attack Detection, Unsupervised Anomaly Detection, Contrastive Learning, GRU Autoencoder, Hybrid Metaheuristic Optimisation, PID Controller Tuning, Area Control Error

Contents

List of Figures

List of Tables

Nomenclature

Acronyms and Abbreviations

Acronym	Description
ABC	Artificial Bee Colony
ACE	Area Control Error
AGC	Automatic Generation Control
AUC	Area Under the Curve
BiGRU	Bidirectional Gated Recurrent Unit
BiLSTM	Bidirectional Long Short-Term Memory
CNN	Convolutional Neural Network
CTD	Communication Time Delay
DA-CGAE	Disturbance-Aware Contrastive GRU Autoencoder
DL	Deep Learning
FDI	False Data Injection
GDB	Governor Deadband
GRC	Generation Rate Constraint
GRU	Gated Recurrent Unit
GWO	Grey Wolf Optimizer
IAE	Integral of Absolute Error
ITAE	Integral of Time-weighted Absolute Error
ITSE	Integral of Time-weighted Squared Error
LFC	Load Frequency Control
LSTM	Long Short-Term Memory
ML	Machine Learning
MHABCPSO	Modified Hybrid Artificial Bee Colony Particle Swarm Optimization
MSE	Mean Squared Error
PID	Proportional–Integral–Derivative

PGWA	Particle Swarm Optimization–Grey Wolf Optimizer with Adaptive Artificial Bee Colony
PSO	Particle Swarm Optimization
PV	Photovoltaic
RER	Renewable Energy Resource
RES	Renewable Energy Source
SCADA	Supervisory Control and Data Acquisition
SLP	Step Load Perturbation

1 Introduction

1.1 Background

In interconnected power systems, the key to the successful operation of load frequency control (LFC) lies in sustaining rapid equilibrium between generation and consumption during varying transient loads. As power systems evolve in complexity, LFC has become essential in system operation, while high operational costs and environmental concerns with traditional generation technologies have further elevated its importance in modern grids (Gouran-Orimi and Ghasemi-Marzbali (2023); Khan et al. (2023)).

The ever-increasing demand for electricity due to population growth and industrialization highlights the critical importance of matching power generation with fluctuating usage. Hybrid power networks coupling traditional plants with renewable energy resources (RERs) such as solar and wind, alongside energy storage technologies, help mitigate supply-demand imbalances and complement generation uncertainties, creating resilient and flexible systems capable of providing electricity reliably (J. Zheng et al. (2023)). Microgrids further extend this resilience as decentralized systems integrating renewable sources, traditional generators, and batteries, offering reduced fuel consumption, lower emissions, and improved reliability. However, the intermittent nature of renewables can cause power imbalances and frequency deviations, necessitating a robust LFC mechanism to regulate generation output and maintain grid stability (Rai and Das (2022)).

The growth of power infrastructure with the integration of RERs and new technologies such as smart grids and micro-networks has rendered the generation of energy more unpredictable. With the shift of the power grids to the deregulated and decentralized systems, based on the deregulation, LFC is important in the automatic generation control by reducing the fluctuations in the frequencies and controlling the tie-line power exchange, aiming to bring the control performance indicator to zero. The emergence of highly evolved frequency control systems has therefore become central in ensuring the

stability of systems in the interconnected domains (E. Ahmed et al. (2023); Khamies, Elkasem, Hassan, and Kamel (2023)). Coupled with these control issues, there is an increasing digitalization of LFC systems using advanced communication technologies that has presented severe cybersecurity risks, the most notable being false data injection (FDI) attacks, which present a severe risk to grid frequency stability and integrity of operation (Abbaspour, Sargolzaei, Forouzannezhad, Yen, and Sarwat (2020); Mokhtari and Yen (2024)).

1.2 Motivation

Modern power systems are rapidly changing because of the incorporation of RERs, decentralized control structures, and modern communication technologies. Although these advances have greatly increased the flexibility and efficiency of operations, they have also brought about new vulnerabilities to LFC structures. The growing use of digital communication networks to relay important control signals like frequency deviation, tie-line power flow, and ACE has turned LFC systems into prime targets by cyber adversaries (Abbaspour et al. (2020); Mokhtari and Yen (2024)). Another issue of multi-area load frequency control (LFC) systems is that area control error (ACE) signals are vulnerable to false data injection (FDI) attacks. The introduction of these attacks with different magnitudes and at different times in different control areas not only distorts local control responses but also propagates across interconnected areas through tie-line interactions. This results in the complex multi-area anomaly patterns, which can not be effectively captured using the traditional single-point detection techniques (Abbaspour et al. (2020); Mokhtari and Yen (2024)). Among other cyber threats to LFC systems, FDI attacks are the most critical issue to consider because they are covert and directly affect the stability of the frequency since they are specially tailored to stay within acceptable residual limits and manipulate the ACE signals silently, leading to erroneous control decisions that destabilize grid frequency and disrupt the inter-area power balance (Ranjan and Shankar (2024); e. a. Zheng (2025)).

Moreover, traditional LFC controllers are typically modeled on idealized assumptions, which fail to sufficiently reflect the nonlinearities, parameter uncertainties, and multi-source generation complexities of the contemporary power grids. The more unpredictable the system dynamics, the more constrained the classical control methods are, and the more intelligent and adaptive control methods are sought (Gouran-Orimi and Ghasemi-Marzbali (2023); Khan et al. (2023)). The holistic approach to controlling performance and cybersecurity aspects of LFC systems, thus, is a key and urgent research requirement, especially for the multi-area systems in which the ACE signal integrity is fundamental to the coordinated inter-area frequency regulation.

1.3 Research Challenges

The architecture of a powerful LFC controller and a practical FDI attack detection system of the present-day power systems are associated with a few interconnected technical issues. Conventional controllers like PI and PID are unable to achieve a satisfactory dynamic performance in the presence of nonlinearities and parameter uncertainties caused by RER integration and multi-area system interactions on the control side (E. Ahmed et al. (2023); Khamies et al. (2023)). Although metaheuristic optimization methods represent a good step towards better controller tuning, the choice and combination of suitable algorithms to provide consistent convergence and better dynamic response in a variety of operating conditions is not a trivial issue (Gouran-Orimi and Ghasemi-Marzbali (2023); Khan et al. (2023)). The individual algorithms like PSO, GWO, and ABC have unique drawbacks, premature convergence, slow multimodal search, and low-dimensional convergence rate, respectively, that cannot be addressed by two-algorithm hybrid methods alone (Gouran-Orimi and Ghasemi-Marzbali (2023); Iqbal et al. (2024); Khan et al. (2023)).

FDI attacks are specifically designed to stay within reasonable residual levels, enabling them to evade the conventional bad data detection (BDD) techniques and closely follow the pattern of normal load variations, which makes them naturally hard to detect (Kim

and Sasahara (2025)). In contrast to the typical attack scenario in the literature, where FDI is injected into tie-line power measurements, attacks on ACE signals in individual control areas are a more complicated detection problem. Different attack magnitudes and injection times on ACE1 and ACE2 result in asymmetric anomaly signals, and cross-area propagation of attack effects via tie-line dynamics causes the unattacked area to exhibit an anomalous behavior that does not directly correlate with an attack. Recent methods of attack have become more advanced, and the RL-based methods allow attackers to dynamically determine the vulnerabilities in the system and schedule their injections to create the greatest impact (e. a. Zheng (2025)).

Current model-based detection methods are based on an accurate mathematical modeling of the system and hence are not suitable for the complexity of contemporary cyber intrusions (Mokhtari and Yen (2024)). Though ML and DL-based approaches have proven to be effective in overcoming these drawbacks (Ahmad, Gulzar, Mustafa, et al. (2025); Ranjan and Shankar (2024)), trained models often fail to generalize across grid topologies and operating regimes, and supervised methods need labeled attack data, which is not readily available in real LFC operational conditions. The non-stationarity of power systems also implies that stationary pre-trained detectors may become degraded as the operating conditions change outside of the training distribution (Kim and Sasahara (2025)). Also, LFC control loops have very strict real-time latency requirements, which impose very strict computational requirements on any deployable detection solution (Mokhtari and Yen (2024); e. a. Zheng (2025)).

1.4 Research Objectives

The primary aim of this research is to enhance both the control performance and cyber resilience of LFC systems in modern interconnected power systems through two key contributions. To achieve this, the following specific objectives are defined:

1. To propose a novel hybrid metaheuristic algorithm, Particle Swarm Optimization–Grey

Wolf Optimizer with Adaptive Artificial Bee Colony (PGWA), for optimal tuning of PID controller gains in LFC systems, integrating the complementary strengths of PSO, GWO, and ABC within a unified sequential three-phase architecture.

2. To develop an unsupervised FDI attack detection framework, the Disturbance-Aware Contrastive GRU Autoencoder (DA-CGAE), capable of identifying FDI attacks in LFC systems without reliance on labeled attack data, by training offline on normal LFC operational data generated from MATLAB simulation and learning deviations from normal operational behavior through contrastive learning and disturbance-aware reconstruction.

3. To evaluate the dynamic performance of the PGWA-tuned PID controller against benchmark algorithms, including PSO, GWO, ABC, and ABCPSO, through standard benchmark functions and in terms of frequency deviation minimization, settling time, overshoot, and tie-line power regulation under various load disturbance scenarios.

4. To assess the FDI attack detection performance of DA-CGAE against established DL baselines, including LSTM, BiLSTM, and CNN, under a multi-point ACE injection scenario where FDI attacks of different amplitudes are injected into ACE1 and ACE2 at different time samples, evaluating detection accuracy, false alarm rate, and robustness against cross-area frequency propagation effects arising from asymmetric attack conditions targeting ACE signals rather than tie-line measurements.

5. To validate both the PGWA algorithm and the DA-CGAE framework through MATLAB-based simulation of a multi-area power system incorporating conventional and renewable generation sources.

1.5 Organization of the Thesis

This thesis is organized into eight chapters.

Chapter 1 introduces the research background, motivation, research challenges, and objectives of the study. It explains the importance of load frequency control in modern interconnected power systems and highlights the need for cyber-resilient control schemes under renewable energy uncertainty and false data injection attacks.

Chapter 2 presents the literature review. It discusses advanced controller architectures for load frequency control, metaheuristic optimization techniques for controller tuning, hybrid control strategies, and existing false data injection attack detection methods. The chapter also identifies the main research gaps addressed in this thesis.

Chapter 3 describes the system under study. It presents the mathematical model of the two-area multi-source interconnected power system, including thermal, hydro, and gas generation units. The chapter also explains the integration of photovoltaic and wind generation, system nonlinearities such as governor deadband and generation rate constraint, and the main system parameters.

Chapter 4 explains the nature-inspired optimization algorithms used for controller tuning. It reviews Artificial Bee Colony, Particle Swarm Optimization, and Grey Wolf Optimizer algorithms, then introduces the proposed PGWA algorithm for optimal PID parameter tuning in the load frequency control system.

Chapter 5 presents the proposed false data injection attack detection framework. It introduces the baseline deep learning models and describes the proposed Disturbance-Aware Contrastive GRU Autoencoder. The chapter explains the input representation, encoder structure, learning branches, training objective, threshold calibration, inference process, and attack mitigation strategy.

Chapter 6 describes the research methodology. It explains the complete simulation workflow, including MATLAB/Simulink modelling, controller optimization, disturbance scenarios, renewable energy integration, data generation, attack injection, model training, and evaluation procedures.

Chapter 7 presents and discusses the results. It evaluates the performance of the proposed PGWA algorithm using benchmark functions and different load frequency control scenarios. It also analyses the performance of the proposed DA-CGAE model for false data injection attack detection and mitigation, comparing it with selected baseline models.

Chapter 8 concludes the thesis. It summarizes the main findings, highlights the contributions of the proposed control and detection framework, discusses the limitations of the study, and recommends possible directions for future research.

2 Literature Review

2.1 Advanced Controller Architectures for LFC

Development of LFC controller design has moved towards classical PI and PID designs to more modern configurations of fractional-order and TID designs and multi-degree-of-freedom designs that provide finer control authority on the frequency dynamics. Although common in use, traditional PI and PID controllers are not always suitable for the needs of modern power systems because they cannot address nonlinearities, parameter uncertainties, and the growing complexity of RER integration (Khan et al. (2023), Gouran-Orimi and Ghasemi-Marzbali (2023)).

Tavakoli et al. (2024) implemented a TID intelligent controller optimized by an equilibrium optimizer for LFC in multi-source interconnected power systems, showing much greater frequency stability and grid resiliency than legacy regulators at high RER penetration (Tavakoli, Zamani, and Khajehoddin (2024)). Ahmed et al. (2022) suggested an adapted TID controller with the Archimedes Optimization Algorithm, establishing a direct connection between optimization methodology and closed-loop performance (M. Ahmed, Magdy, Khamies, and Kamel (2022b)), and further introduced a coordinated approach to frequency stability in hybrid power systems with communication delay resilience (M. Ahmed, Magdy, Khamies, and Kamel (2022a)). Ahmed et al. (2023) extended the fractional-order paradigm to a three-degree-of-freedom LFC system using a fractional-order PID with a TIDF controller optimized with a modified Manta-Ray Foraging Optimizer, allowing set-point tracking, disturbance rejection, and noise filtering to be tuned independently. Choudhary et al. (2022) added a cascade FOPI-FOPTID controller with energy storage devices, optimized with the global area algorithm and outperforming ant-colony-optimized PID controllers in transient response quality (Choudhary, Rai, and Arya (2022)). Rai and Das (2022) suggested a fuzzy TID controller using a sailfish optimizer for LFC in a microgrid with energy storage systems, enabling smooth gain adaptation to varying operating conditions (Rai and Das (2022)). Khamies et al. (2023) confirmed that advanced

LFC architectures coupled with storage control significantly improve frequency regulation under high renewable penetration (Khamies et al. (2023)). Gouran-Orimi and Ghasemi-Marzbali (2023) verified the significance of nonlinearity-aware controller design using an adapted Grasshopper Optimization Algorithm for LFC of a multi-area multi-source system (Gouran-Orimi and Ghasemi-Marzbali (2023)).

Although these more complex architectures exhibit obvious performance advantages over classical designs, their parameter optimization is carried out through single optimization algorithms prone to early convergence and limited flexibility to complex fitness landscapes, motivating the hybrid metaheuristic approaches considered in the next section.

2.2 Metaheuristic Optimization Algorithms for LFC Controller Tuning

One of the common findings in LFC literature is that controller architecture in itself is not enough to obtain high performance; parameter tuning quality is also a determinant (Khan et al. (2023), Gouran-Orimi and Ghasemi-Marzbali (2023)). PSO possesses good global search performance but can converge to local optima in high-dimensional spaces (Gouran-Orimi and Ghasemi-Marzbali (2023)). GWO strikes a balance between exploration and exploitation but may have sluggish convergence on multimodal problems (Khan et al. (2023)). ABC's exploitation-exploration balance weakens on high-dimensional problems such as fractional-order or cascaded LFC controller structures (Khamies et al. (2023), Iqbal et al. (2024)). These constraints drive hybrid solutions.

Khamies et al. (2023) suggested an improved Runge Kutta Optimizer to tune fractional-order PID controllers, achieving a maximum 66 percent improvement over traditional PI controllers and 44 percent improvement in grid stability under high RER penetration (Khamies et al. (2023)). Biswas et al. (2023) applied fuzzy logic-optimized PID controllers with a herd immunity optimizer to a 10-Machine New England Test System, robustly exploring the controller parameter space (Biswas, Bera, and Chakrabarty (2023)). Khan et al.

(2023) stated that hybrid optimization strategies are always superior to single-algorithm methods across a variety of power systems (Khan et al. (2023)).

Iqbal et al. (2024) created the Modified Hybrid ABCPSO algorithm, combining local exploration of ABC with the global search efficiency of PSO via an adaptive decision strategy with a dynamic limit parameter, demonstrating low settling times, zero steady-state error, and small frequency variations on thermal-hydro two-area power systems (Iqbal et al. (2024)). Nevertheless, ABCPSO combines only two constituent algorithms without a third complementary search mechanism, restricting its adaptive search ability, and lacks validation using standard benchmark functions (Iqbal et al. (2024)). The proposed PGWA algorithm addresses these limitations by incorporating PSO, GWO, and ABC in a single three-step sequential architecture with an adaptive mechanism, integrating the global search of PSO, hierarchical exploitation of GWO, and local search diversity of ABC. Validation is performed with both standard benchmark functions and LFC-specific controller tuning experiments.

2.3 Hybrid Control Frameworks and Multi-Area LFC

Taher et al. (2023) suggested an ideal model predictive control of energy storage devices for frequency stabilization, using real observational data to validate the practical applicability of their approach (Taher et al. (2023)). Wang et al. (2023) suggested intelligent LFC with real-time adaptive PI tuning for enhanced wind power penetration, continuously adjusting parameters based on wind speed measurements (Z. Wang et al. (2023)). Ansari et al. (2023) introduced a backstepping sliding mode controller with Lyapunov-based stability guarantees, demonstrating robustness in load disturbance rejection not offered by purely optimization-based methods (Ansari, Homayounzade, and Abbasi (2023)).

Although these frameworks reveal the importance of integrating complementary control strategies, two important limitations cut across the reviewed literature: the security implications of communication-dependent and adaptive LFC architectures have not been

studied, and controller optimization and cybersecurity are continually addressed as two distinct research areas without unified frameworks. These facts directly inspire the two-fold contribution of the present work: LFC controller optimization using PGWA and FDI detection using DA-CGAE within a single MATLAB simulation.

2.4 FDI Attack Detection in LFC Systems

The increasing digitalization of LFC systems and their growing dependence on open communication networks have made them vulnerable to cyber threats, with FDI attacks representing the most serious concern (Abbaspour et al. (2020), Mokhtari and Yen (2024)). Unlike physical faults, FDI attacks are deliberately designed to corrupt sensor measurements and control signals while remaining within acceptable residual thresholds, allowing them to bypass traditional BDD methods and cause sustained frequency instability (Abbaspour et al. (2020)). Interference with ACE signals, frequency deviation measurements, or tie-line power flow data can result in incorrect control responses that destabilize grid frequency and disrupt inter-area power balance (e. a. Zheng (2025), Ranjan and Shankar (2024)).

2.4.1 Model-Based Detection Approaches

Abbaspour et al. (2020) determined the inherent susceptibility of LFC systems to FDI attacks and suggested a robust control design as a mitigation strategy, showing that corrupted ACE and frequency deviation signals may lead to sustained frequency instability without detection (Abbaspour et al. (2020)). Their work emphasized that model-based techniques achieve real-time identification of anomalies with low computational complexity, but are limited by sensitivity to model uncertainties and growing nonlinearity from RER integration. Manias et al. (2024) offered a systematic vulnerability analysis framework for smart grid frequency control, identifying the weak links most prone to exploitation by FDI, although without an automated real-time detection mechanism for strict LFC latency constraints (Manias et al. (2024)). The inherent weakness of model-

based methods in maintaining accurate system models under increasing renewable complexity has motivated the research community to consider data-driven ML and DL alternatives (Mokhtari and Yen (2024)).

2.4.2 Machine Learning-Based Detection Approaches

Mokhtari and Yen (2024) suggested a detailed ML-based fault detection, isolation, and identification model for LFC systems using SCADA operational technology sensor data, demonstrating that data-driven techniques can detect FDI threats without accurate system models (Mokhtari and Yen (2024)). A Random Subspace Ensemble classifier relying on sample-to-sample signal characteristics achieved 100% detection of step, pulse, and random FDI attacks, though tested on a small scale of 300 cases with limited generalization to non-stationary operating conditions (Raghuvamsi et al. (2024)). Asiri et al. (2025) confirmed a Levenberg–Marquardt Fast Neural Network detection framework in SCADA-monitored multi-area LFC settings, achieving a regression coefficient of 0.99 between normal and compromised states, but requiring labeled attack samples during training, a practical constraint where attack data is scarce (Asiri et al. (2025)).

2.4.3 Deep Learning-Based Detection Approaches

DL architectures have enhanced FDI detection capability by enabling automatic feature extraction from raw time-series LFC signals without manually engineered features. Ranjan and Shankar (2024) suggested an LSTM-based cyber-attack detection system for smart-grid LFC with electric vehicles, showing that LSTM networks can successfully detect FDI attacks on LFC communication signals in multi-area systems with RERs (Ranjan and Shankar (2024)). Ahmad et al. (2025) applied AI-enabled frequency synchronization control with metaheuristic optimization and LSTM-based detection, achieving a regression coefficient of 0.99 in differentiating between normal and attack states (Ahmad et al. (2025)). However, these LSTM-based models rely on supervised learning with labeled attack data and predefined parameters unable to adapt to changing system conditions.

Kim and Sasahara (2025) suggested an adaptive FDI detection scheme with RNN retraining to keep LSTM and GRU models updated under unexpected operating conditions, though at the cost of computational burden and risk of catastrophic forgetting (Kim and Sasahara (2025)). Zheng et al. (e. a. Zheng (2025)) proposed a multi-model fusion framework combining supervised LSTM and unsupervised autoencoder-based anomaly detection with adaptive weight adjustment, achieving 99.4% accuracy across various LFC system states. The supervised LSTM component handles known attack patterns while the unsupervised autoencoder addresses unknown attack types, but labeled attack data is still needed for the supervised component (e. a. Zheng (2025)). Shrestha et al. (2025) addressed joint detection and localization of compound cyber threats using a hybrid CNN-Transformer-BiLSTM network for smart grid FDI under simultaneous DoS attacks, with spatial, global, and temporal correlations captured in parallel (Shrestha, Chamana, Adeyanju, Mohammadpourfard, and Bayne (2025)).

Although LSTM, BiLSTM, and CNN-based methods show high detection performance, none is tested in asymmetric multi-point ACE injection cases where attacks of varying magnitudes are imposed on ACE1 and ACE2 at varying time points. The current DL detection literature mainly addresses single injection-point tie-line measurements (e. a. Zheng (2025), Kim and Sasahara (2025), Ahmad et al. (2025), Ranjan and Shankar (2024)), and any supervised DL model needs labeled attack data, an inherent practical constraint when novel amplitude levels or injection timing patterns are absent from training data (Mokhtari and Yen (2024), Kim and Sasahara (2025)).

2.4.4 Unsupervised and Contrastive Learning Approaches

One of the most significant shortcomings of supervised and semi-supervised methods is their requirement for labeled attack data, which is generally hard to come by in real operational LFC scenarios where attack incidents are sparse and heterogeneous (Mokhtari and Yen (2024), e. a. Zheng (2025)). Autoencoder-based anomaly detection trains on normal operational data and identifies attacks as deviations from learned normal behavior.

However, standard autoencoders suffer from high false alarm rates in LFC settings because legitimate RER-induced frequency deviations also produce high reconstruction errors (Raghuvamsi et al. (2024), Manias et al. (2024)). This disturbance-false alarm tradeoff is a critical unresolved issue in unsupervised FDI detection. Contrastive learning is a new direction that trains models to learn discriminative representations by contrasting normal and augmented samples, though its use for LFC-specific FDI anomalies has not been studied in the literature (e. a. Zheng (2025), Kim and Sasahara (2025)). The proposed DA-CGAE model fills this gap by combining BiGRU-based temporal modeling with contrastive learning and a perturbation-sensitive reconstruction mechanism specifically designed to counteract false alarms due to legitimate RER-induced frequency deviations, enabling unsupervised FDI detection without labeled attack examples. The DA-CGAE is trained offline on normal LFC operational data from MATLAB simulation and critically evaluated on multi-point FDI attack scenarios where attacks of various magnitudes are injected into ACE1 and ACE2 at various time samples, addressing cross-area frequency propagation effects absent from the existing tie-line-focused literature.

2.5 Research Gaps and Summary

A synthesized reading of the reviewed literature across LFC controller design, metaheuristic optimization, and FDI attack detection reveals four critical gaps that collectively motivate the contributions of this work.

2.5.1 Gap 1: Limited Depth of Hybrid Optimization for LFC Tuning

Current methods, such as the equilibrium optimizer of Tavakoli et al. (2024) (Tavakoli et al. (2024)), the Archimedes Optimization Algorithm of Ahmed et al. (2022a) (M. Ahmed et al. (2022b)), and the coordinated optimization of Ahmed et al. (2022b) (M. Ahmed et al. (2022a)), utilize single-algorithm or two-component models vulnerable to premature convergence. The hybrid ABCPSO approach of Iqbal et al. (2024) (Iqbal et al. (2024)) combines only ABC and PSO without a third complementary mechanism, restricting adap-

tive search diversity. None of the reviewed hybrid algorithms integrates all three of PSO, GWO, and ABC into a unified adaptive framework, and none validate generalization ability with both standard benchmark functions and LFC-specific tuning objectives (Khan et al. (2023), Gouran-Orimi and Ghasemi-Marzbali (2023), Iqbal et al. (2024)).

2.5.2 Gap 2: Reliance on Labeled Attack Data for FDI Detection

Partially and fully supervised DL models such as LSTM, BiLSTM, and CNN (e. a. Zheng (2025), Kim and Sasahara (2025), Ahmad et al. (2025), Ranjan and Shankar (2024)) essentially need labeled attack samples to train. In actual operational LFC scenarios such as those of Tavakoli et al. (Tavakoli et al. (2024)) and Ahmed et al. (M. Ahmed et al. (2022b), M. Ahmed et al. (2022a)), attack data is limited, highly heterogeneous, and challenging to gather, as FDI attacks are designed to be discrete. Models trained with supervised approaches are susceptible to attack patterns not reflected in the training data, restricting feasibility in real LFC deployments and driving the need for unsupervised detection models that train solely on normal operational behavior.

2.5.3 Gap 3: High False Alarm Rates under RER-induced Disturbances and ACE-targeted Multi-point Attacks

The multi-source systems of Tavakoli et al. (2024) (Tavakoli et al. (2024)) and Ahmed et al. (2022b) (M. Ahmed et al. (2022a)) incorporate high shares of renewable generation, creating environments where legitimate RER-induced frequency deviations are frequent and large in magnitude. Existing unsupervised detection approaches based on standard autoencoders do not explicitly model the distinction between legitimate disturbances and FDI-induced anomalies (Mokhtari and Yen (2024), e. a. Zheng (2025)). This is further compounded by the multi-point ACE injection scenario used in this work, where attacks of different amplitudes in ACE1 and ACE2 produce control-layer anomalies superimposed on normal transient responses, with cross-area propagation creating indirect attack signatures that overlap with legitimate disturbance responses (Abbaspour et al. (2020),

e. a. Zheng (2025)). No existing unsupervised approach addresses this combination of RER variability and asymmetric multi-point ACE attack propagation simultaneously.

2.5.4 Gap 4: Independent Treatment of LFC Control Optimization and FDI Detection

The reference system papers (Tavakoli et al. (2024), M. Ahmed et al. (2022b), M. Ahmed et al. (2022a)) represent state-of-the-art LFC controller design but do not address the cybersecurity dimension. Conversely, FDI detection frameworks reviewed in Sections 2.4.1–2.4.4 are designed independently of specific controller architectures, trained on generic data that may not reflect the closed-loop dynamics of advanced optimization-tuned controllers (Abbaspour et al. (2020), e. a. Zheng (2025)). This disconnect creates an important practical vulnerability: detection models may misclassify normal transient responses of the optimized controller as anomalies or fail to detect FDI attacks exploiting the specific dynamic characteristics of the optimized system (Asiri et al. (2025), Manias et al. (2024)). No existing work addresses both dimensions within a unified simulation framework, and the specific challenge of asymmetric multi-point FDI attacks on ACE signals across areas producing coupled anomaly signatures has not been addressed (Abbaspour et al. (2020), e. a. Zheng (2025), Asiri et al. (2025)).

This work addresses all four identified gaps through two complementary contributions within a unified MATLAB simulation framework (Tavakoli et al. (2024), M. Ahmed et al. (2022b), M. Ahmed et al. (2022a)). Gap 1 is addressed through the proposed PGWA algorithm, which integrates PSO, GWO, and ABC within a unified three-phase adaptive sequential architecture, validated through both standard benchmark functions and LFC-specific PID controller tuning experiments. Gaps 2 and 3 are simultaneously addressed through the proposed DA-CGAE framework, which performs offline unsupervised FDI detection by training exclusively on normal LFC operational data generated from MATLAB simulation as CSV files, eliminating the need for labeled attack samples. The disturbance-aware reconstruction mechanism and contrastive learning explicitly model the distinction between RER-induced disturbances and FDI-induced anomalies, and the framework is

evaluated on multi-point ACE injection scenarios with cross-area frequency propagation effects (Abbaspour et al. (2020), e. a. Zheng (2025), Ranjan and Shankar (2024)). Gap 4 is addressed by the integrated design of both contributions in a single simulation environment, where the PGWA-tuned PID controller defines the closed-loop LFC dynamics from which DA-CGAE training data is generated, ensuring the detection framework is precisely calibrated to the operational behavior of the optimized LFC system.

3 System Under Study

In this section, the dynamic model of the two-area multi-source interconnected power system that is discussed in this work will be presented. The system is analyzed in two scenarios: (i) a traditional multi-source power system that does not include RES, and (ii) an expanded hybrid system that includes photovoltaic (PV) solar and wind generation units in addition to conventional plants. The two configurations have an identical underlying area structure, which allows the actual performance comparison of the suggested control strategy at varying degrees of renewable penetration (Tavakoli et al. (2024), M. Ahmed et al. (2022b)).

In every control area, there are three of the traditional generation technologies: a reheat thermal plant, a hydraulic (hydro) plant, and a gas turbine plant. The two regions are connected via a tie-line, which allows the exchange of power and which has to be controlled to ensure the security of the systems. The basic necessity of any LFC scheme is to bring the system frequency back to its nominal level and drive the tie-line power deviation to zero after any load perturbation or generation imbalance (Tavakoli et al. (2024), M. Ahmed et al. (2022b), M. Ahmed et al. (2022a)).

3.1 Two-Area Multi-Source Power System Model

The dynamic model of the two-area multi-source power system is illustrated in Figure 1. Thermal, hydro, and gas generation units in each area are weighted by factors of participation, PF_{th}, PF_{hyd}, and PF_{g} to give their contribution to the overall area generation. Each region is characterized by a first-order transfer function with gain K_{ps} and time constant T_{ps} that represents the power system plant (Tavakoli et al. (2024), M. Ahmed et al. (2022b)).

The main control signal is the ACE of each area. It captures the local frequency deviation and scheduled tie-line power exchange deviation, hence reflecting the generation-load

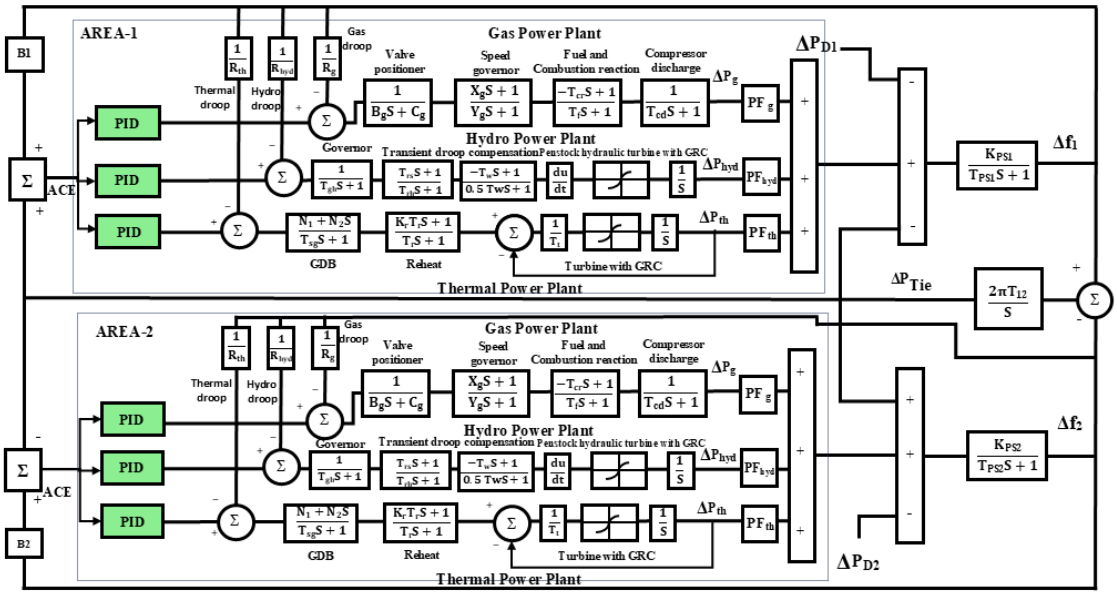


Figure 1. Schematic of the Two-Area Multi-Source Interconnected Power System (Without RES).

imbalance between and within areas. In the case of a two-area system, the ACE signals are characterized as follows:

$$\text{ACE}_1 = \Delta P_{tie12} + B_1 \Delta f_1 \tag{1}$$

$$\text{ACE}_2 = -\Delta P_{tie12} + B_2 \Delta f_2 \tag{2}$$

where B_1 and B_2 are the frequency bias coefficients of areas 1 and 2, respectively; Δf_1 and Δf_2 denote the respective frequency deviations; ΔP_{tie} is the tie-line power deviation; and α_{12} is the area size ratio. The objective of the LFC is to drive both ACE signals asymptotically to zero following any disturbance.

The tie-line power deviation between the two areas is governed by the synchronizing coefficient T_{12} as follows:

$$\Delta P_{tie}(s) = \frac{2\pi T_{12}}{s}(\Delta f_1 - \Delta f_2) \tag{3}$$

3.1.1 Reheat Thermal Unit

The reheat thermal unit is represented as having three cascaded subsystems: the governor with governor deadband (GDB) nonlinearity, the reheater, and the steam turbine with generation rate constraint (GRC). The GDB is a result of mechanical friction, backlash, and valve overlaps in hydraulic relays. It is characterized as the sum of constant speed variation within which the position of the turbine valve is kept constant. The GDB causes an incessant sinusoidal movement of about 0.5 Hz and decreases the stability of the entire power system. For a 0.5% backlash, it is linearized as (Tavakoli et al. (2024), M. Ahmed et al. (2022b)):

$$G_{GDB}(s) = \frac{N_1 + N_2 s}{T_{sg} s + 1} \tag{4}$$

where $N_1 = 0.8$ and $N_2 = -\frac{0.2}{\pi}$ are the Fourier linearization coefficients, and T_{sg} is the governor time constant. The reheater and non-reheat turbine transfer functions are, respectively:

$$G_R(s) = \frac{K_r T_r s + 1}{T_r s + 1} \tag{5}$$

$$G_T(s) = \frac{1}{T_t s + 1} \tag{6}$$

where K_r is the reheat steam constant, T_r the reheat time constant, and T_t the turbine time constant. A symmetric GRC of 10% p.u./min is enforced for both the rising and falling generation rates of the thermal unit.

3.1.2 Hydraulic Unit

The hydraulic unit model comprises the hydro governor, transient droop compensation, and the penstock hydraulic turbine, all subject to GRC. The governor and transient droop compensation transfer functions are given by (Tavakoli et al. (2024), M. Ahmed et al. (2022b)):

$$G_{hg}(s) = \frac{1}{T_{gh}s + 1} \tag{7}$$

$$G_{td}(s) = \frac{T_{rs}s + 1}{T_{rh}s + 1} \tag{8}$$

where T_{gh} is the hydro governor time constant, T_{rs} is the reset time, and T_{rh} is the transient droop time constant. The non-minimum phase penstock turbine transfer function, which reflects the characteristic initial inverse response of water flow, is modeled as:

$$G_{hyd}(s) = \frac{-T_w s + 1}{0.5T_w s + 1} \tag{9}$$

where T_w is the starting time of water in the penstock. Asymmetric GRC values of 270% p.u./min for rising generation and 360% p.u./min for falling generation are applied to capture the physical hydraulic constraints realistically (Tavakoli et al. (2024)).

3.1.3 Gas Turbine Unit

The gas turbine model consists of four subsystems in series: the valve positioner, the speed governor, the fuel system with combustion reaction delay, and the compressor discharge. Their respective transfer functions are (Tavakoli et al. (2024), M. Ahmed et al.

(2022b)):

$$G_{vp}(s) = \frac{C_g}{B_g s + C_g} \tag{10}$$

$$G_{sg}(s) = \frac{X_g s + 1}{Y_g s + 1} \tag{11}$$

$$G_{fc}(s) = \frac{-T_{cr} s + 1}{T_f s + 1} \tag{12}$$

$$G_{cd}(s) = \frac{1}{T_{cd} s + 1} \tag{13}$$

where B_g and C_g are the valve positioner parameters; X_g and Y_g are the lead and lag time constants of the speed governor; T_{cr} is the combustion reaction delay; T_f is the fuel time constant; and T_{cd} is the compressor discharge time constant. The gas turbine is not subject to GRC in this model.

In the former setup, the conventional generation sources, thermal, hydro, and gas, are the sole power providers in the two regions. The LFC problem can be investigated in this baseline scenario, with deterministic and well-characterized disturbances, including step and multi-step load perturbations. It also offers a point of reference on which the complexity added by the integration of renewable energy can be measured (Tavakoli et al. (2024), M. Ahmed et al. (2022b)).

Under this setup, the main causes of difficulty are load perturbations and the nonlinearities caused by the GDB and GRC constraints. The GDB makes governors less responsive and adds low-frequency oscillations, whereas the GRC constrains the rate at which gen-

eration can be varied, making the system slow to respond to sudden load changes. These physical constraints, combined, are realistic operating constraints of traditional power plants and should be explicitly considered in the controller design.

3.2 System Configuration With Renewable Energy Sources

The second setup builds on the first one by incorporating the renewable energy sources into the two regions, as shown in Figure 2. Area 1 is linked to a photovoltaic (PV) solar system of rated power of 50 MW, and Area 2 is linked to a wind power plant of rated power of 70 MW. Their production is added to the area power balances via factors of participation $P_{FPV} = 0.015$ and $P_{FWT} = 0.025$ (Tavakoli et al. (2024), M. Ahmed et al. (2022b), M. Ahmed et al. (2022a)). These sources are inherently stochastic and intermit-

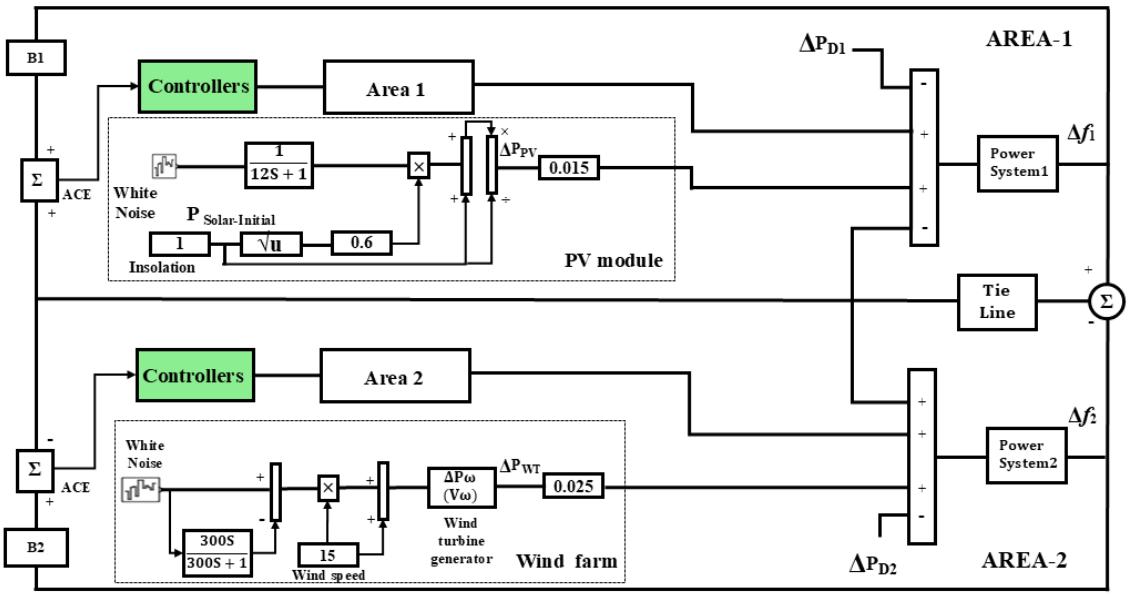


Figure 2. Schematic of the Two-Area Multi-Source Interconnected Power System (With RES).

tent, which adds further frequency perturbations on top of traditional load perturbations and makes the LFC problem a significantly more challenging problem. Since the effective

inertia of the system decreases due to RESs, especially when they replace synchronous generators, frequency deviations are magnified and accelerated by disturbances. The LFC system must thus be able to offer quick and sound corrective measures in these more volatile operating environments (M. Ahmed et al. (2022a), Z. Wang et al. (2023)).

3.2.1 Photovoltaic System Model

The photovoltaic system is linked to Area 1 with a capacity of 50 MW. Its power output is solely dependent on solar irradiance, which is constantly changing with weather conditions, cloud cover, and the angle at which the sun strikes the panel surface. Massive variations in irradiance generate uneven power injections that disrupt area frequency and impose extra load on the conventional units that are controlled by LFC (M. Ahmed et al. (2022b), M. Ahmed et al. (2022a)).

The dynamic model represents the stochastic change in solar irradiance by a white noise signal that drives the isolation input block. The real power deviation of the PV system, P_{Solar}, is determined by a square-root dependence on the instantaneous solar power P_{Solar}, due to the nonlinear dependence between irradiance and PV power (M. Ahmed et al. (2022b), M. Ahmed et al. (2022a)):

$$\Delta P_{Solar} = 0.6\sqrt{P_{Solar}} \tag{14}$$

The resultant perturbation in PV power is sent through a first-order low-pass filter with a time constant of 12 s, which captures the dynamic smoothing effect of the large PV array and power-electronic interface:

$$G_{PV}(s) = \frac{1}{12s + 1} \tag{15}$$

The filtered output ΔP_{PV} is injected into the power balance of Area 1 as an uncontrolled disturbance generation. Given that the PV system has no built-in inertia and does not engage in primary frequency regulation, any abrupt solar-power variation should be completely offset by the conventional units regulated by the LFC. This is a huge burden to the controller, especially in the case of a high-rate drop in irradiance due to clouds.

The inherent LFC problem with PV integration is that it is non-dispatchable: the PV cannot be ordered to produce more or less generation on command. Any deficit in generation due to low irradiance must be fully absorbed by the reserve capacity of the controllable units, and thus the LFC system must respond swiftly and precisely (M. Ahmed et al. (2022a)).

3.2.2 Wind Generation Unit Model

The wind generation unit is linked to Area 2, which has a rated capacity of 70 MW and $P_{FWT} = 0.025$. The power of wind depends on the speed of the wind, which is constantly changing and unpredictable. The classical wind power equation (Tavakoli et al. (2024), M. Ahmed et al. (2022b), M. Ahmed et al. (2022a)) describes the aerodynamic power that the turbine rotor extracts out of the wind:

$$P_W = \frac{1}{2}\rho A_T V_W^3 C_P(\lambda, \beta) \tag{16}$$

where ρ (kg/m³) is the air density, A_T (m²) is the rotor swept area, V_W (m/s) is the wind speed at hub height, and $C_P(\lambda, \beta)$ is the power coefficient, the aerodynamic efficiency of the rotor, which is a nonlinear function of the tip-speed ratio λ and the blade pitch angle β. The power coefficient is expressed as (Tavakoli et al. (2024), M. Ahmed et al. (2022b)):

$$C_P(\lambda, \beta) = C_1 \left[\frac{C_2}{\lambda_I} - C_3\beta - C_4\beta^2 - C_5\right] \exp\left(-\frac{C_6}{\lambda_I}\right) + C_7\lambda_T \tag{17}$$

where C_1 through C_7 are empirically derived turbine-specific constants. The nonlinear exponential term $\exp(-C_6/\lambda_I)$ causes C_P to peak sharply at the optimal operating condition and fall off rapidly on either side, making maximum power tracking essential for efficient operation.

The optimal tip-speed ratio λ_T, at which C_P is maximised, is determined by the ratio of the rotor tip speed to the free-stream wind velocity:

$$\lambda_T = \lambda_T^{OP} = \frac{\omega_T \times r_T}{V_W} \tag{18}$$

where ω_T is the rotor angular velocity and r_T is the rotor radius. Maintaining the rotor speed at the value corresponding to λ_T ensures maximum aerodynamic efficiency. The intermittent tip-speed ratio λ_I, which accounts for the effect of blade pitch angle on effective flow, is computed as:

$$\frac{1}{\lambda_I} = \frac{1}{\lambda_T + 0.08\beta} - \frac{0.035}{\beta^3 + 1} \tag{19}$$

This relationship shows that as the pitch angle β increases, λ_I decreases, reducing C_P and thereby limiting power extraction, a mechanism exploited for power curtailment at high wind speeds. The nominal coefficients of the wind generation unit are listed in Table 2.

In the simulation model, the wind speed input V_W is formed by multiplying a rated wind speed by a random perturbation generated from a white noise block, producing a realistic time-varying wind speed profile. The noise signal is shaped by a first-order filter that captures the slow variation of mean wind speed:

Table 2. The parameters of the wind generation unit.

Parameter / Setting	Value
PW	750 kW
VW	15 m/s
ρ	1.225 kg/m^3
AT	1684 m^2
rT	22.9 m
λT	22.5 rpm
C1	0.6175
C2	116
C3	0.4
C4	0
C5	5
C6	21
C7	0.1405

$$G_W(s) = \frac{300}{300s + 1} \tag{20}$$

The high time constant of 300 s indicates the relatively slow change in the mean wind speed, in contrast to short-term turbulence, which generates a low-frequency stochastic change in wind speed. This produces a resulting wind power output ΔP_{WT}, which is introduced as an uncontrolled perturbation of power to Area 2 power balance (Tavakoli et al. (2024), M. Ahmed et al. (2022b)).

The basic LFC dilemma of wind production is twofold. To begin with, wind production is completely dependent on the weather and cannot be called upon demand. Second, contemporary wind turbines are generally linked to the grid via power-electronic converters, which disconnect the rotor inertia from the grid frequency, in effect removing the inertial contribution of the turbine. High wind penetration and low system inertia lead to quicker and greater frequency swings following load or generation perturbations, and place more demanding conditions on the pace and flexibility of the LFC strategy (M. Ahmed et al. (2022a), Z. Wang et al. (2023)).

3.3 System Nonlinearities and Physical Constraints

In both system configurations, two physical constraints that are important to realistic LFC modelling are included: the governor deadband (GDB) and the generation rate constraint (GRC) (Tavakoli et al. (2024), M. Ahmed et al. (2022b)).

The GDB reduces governor responsiveness by ensuring that the speed error signal must surpass a dead-zone before any valve action is taken. This limit is due to the existence of friction and mechanical play due to hydraulic relay mechanisms. In the case of the thermal unit, the GDB generates a long-periodical oscillation at around 0.5 Hz, which adds to the settling time and worsens the overall stability. This gives its linearized 0.5% backlash model as Equation (4).

The GRC is an expression of the physical inertia of the boiler-turbine system or hydraulic machinery, which is the rate of change in the generated power. In the case of a reheat thermal unit, a symmetric GRC of 10% p.u./min is used. In the case of hydro units, the natural asymmetry between water acceleration and deceleration is represented by asymmetric GRC values: 270% p.u./min (rising generation) and 360% p.u./min (falling generation). These limits do not allow the controller to order instantaneous large corrective actions and have to be considered in the LFC design (Tavakoli et al. (2024)).

Besides these nonlinearities, there is a communication time delay (CTD) between the plant and the controller that is taken into account in one of the simulation scenarios. The controller output is delayed by 0.1 seconds to indicate the delay of digital communication channels in present-day energy management systems. These delays may destabilize traditional controllers and should be explicitly addressed by a strong LFC scheme.

3.4 System Parameters

Table 3 summarizes the entire set of nominal parameters of each system configuration. The traditional unit parameters of the two-area system are symmetric, and the factors of participation vary to indicate the extra units of RES in the hybrid arrangement. These values determine the operating point in all the controller design and simulation studies in the following sections (Tavakoli et al. (2024), M. Ahmed et al. (2022b), M. Ahmed et al. (2022a)).

Table 3. The parameters of the hybrid power system..

Parameter	Value	Description
Rhyd, Rg, RTh	2.4	Parameters regulating the speed control of governors in thermal, hydro, and gas power systems.
N1, N2	0.8, -0.2/π	Fourier coefficients utilized in the GDB transfer function model.
Trh	28.749	Constant that governs the transient droop of the system.
Tsg	0.06	Time constant associated with the steam turbine's governor.
Tt	0.3	Time constant of the steam turbine's operation.
Tw	1.1	Time required for water to start in the hydro turbine.
Kr	0.3	Constant that defines the steam turbine's reheating characteristics.
Tr	10.2	Time constant governing the reheating process of the steam turbine.
Tps1, Tps2	11.49	Time constants related to the overall power system.
Kps1, Kps2	68.9655	Gain parameters for the power system.
T12	0.0433	Coefficient used for synchronizing the system components.
PF$_{hyd}$, PF$_g$, PF$_{Th}$	0.2873, 0.138, 0.5747	Proportional contributions of the hydro, gas, and thermal units to the system's operation.
Xg	0.6	Time constant for the lead time of the gas turbine governor.
Yg	1.1	Time constant for the lag time of the gas turbine governor.
Bg	0.049	Time constant of the value positioner controlling the gas turbine.
Tgh	0.2	Time constant for the governor of the hydro turbine.
Tcd	0.2	Time constant related to the compressor discharge volume.
Cg	1	Constant governing the gas turbine's valve positioner.
Tf	0.239	Time constant for the gas turbine fuel system.
Tcr	0.01	Delay associated with the combustion reaction in the gas turbine.
Trs	4.9	Time required to reset the hydro turbine speed governor.
B1, B2	0.4312	Coefficients used for frequency bias in the system.
PF$_{PV}$, PF$_{WT}$	0.015, 0.025	Proportional contributions of the photovoltaic and wind generation systems to the overall operation.

3.5 False Data Injection Attack Scenario

To evaluate the cyber-resilience of the controller and detection framework developed in this thesis, false data injection (FDI) attacks are applied to the area control error signals of the adopted two-area load frequency control system. The considered power system model is taken from the literature and is used as a benchmark platform for analysing the effect of cyber-attacks on frequency regulation performance. Since the area control error is the main feedback signal used by the load frequency controller, manipulating this signal can lead to incorrect control actions and degraded system stability.

In this study, the FDI attack is modelled as a sinusoidal signal added directly to the ACE measurements. In Area 1, a sine-wave attack with an amplitude of 0.05 is injected into ACE_1 from $t = 40$ s to $t = 70$ s. The attack signal is generated using 100 samples per period with a sampling time of 0.01 s. In Area 2, a similar sine-wave attack with an amplitude of 0.05 is injected into ACE_2 from $t = 55$ s to $t = 85$ s, using 70 samples per period and the same sampling time of 0.01 s. The different attack intervals and sampling periods create an asymmetric multi-area attack condition, where the corrupted ACE signals affect local controller decisions and may also influence the neighbouring area through tie-line power dynamics.

The compromised ACE signals are expressed as

$$ACE_1^{att}(t) = ACE_1(t) + a_1(t), \tag{21}$$

$$ACE_2^{att}(t) = ACE_2(t) + a_2(t), \tag{22}$$

where $a_1(t)$ and $a_2(t)$ denote the sinusoidal FDI attack signals applied to Area 1 and

Area 2, respectively. These signals are defined in discrete form as

$$a_1[k] = \begin{cases} 0.05 \sin\left(\dfrac{2\pi k}{100}\right), & 40 \leq t \leq 70, \\ 0, & \text{otherwise}, \end{cases} \tag{23}$$

$$a_2[k] = \begin{cases} 0.05 \sin\left(\dfrac{2\pi k}{70}\right), & 55 \leq t \leq 85, \\ 0, & \text{otherwise}. \end{cases} \tag{24}$$

Here, k represents the discrete-time sample index. This attack configuration is used to examine whether the developed detection framework can distinguish malicious ACE manipulation from normal load disturbances and renewable-energy-induced variations.

4 Nature-Inspired Metaheuristic Optimization Algorithms

Metaheuristic algorithms, which are nature-inspired, have become powerful tools in solving high-dimensional, complex optimization problems that are intractable using classical deterministic methods. They are based on biological, physical, or social phenomena seen in nature and use stochastic search processes to efficiently search large solution spaces. The Artificial Bee Colony (ABC) algorithm, Particle Swarm Optimization (PSO), and the Grey Wolf Optimizer (GWO) are among the most effective of these methods. All these processes are modeled after a particular natural process: group foraging behavior among honeybees, social movement behavior among bird flocks and fish schools, and the hierarchical group hunting behavior of grey wolves, respectively (Karaboga (2005), Mirjalili, Mirjalili, and Lewis (2014)).

4.1 Artificial Bee Colony (ABC) Algorithm

4.1.1 Background and Biological Inspiration

The Artificial Bee Colony (ABC) algorithm, developed by Karaboga (2005) (Karaboga (2005)) and discussed in Karaboga and Basturk (2007, 2008) (Karaboga and Basturk (2007), Karaboga and Basturk (2008)), is based on the foraging behavior in honeybee swarms where simple individual behaviors result in self-organised collective intelligence. The colony is made up of three functional groups: employed bees that exploit candidate sources of food and share quality information; onlooker bees that probabilistically choose sources according to this information; and scout bees that randomly search the search space when a source is depleted to a predetermined threshold (Karaboga and Basturk (2007)). The flowchart of ABC is demonstrated in Figure 3

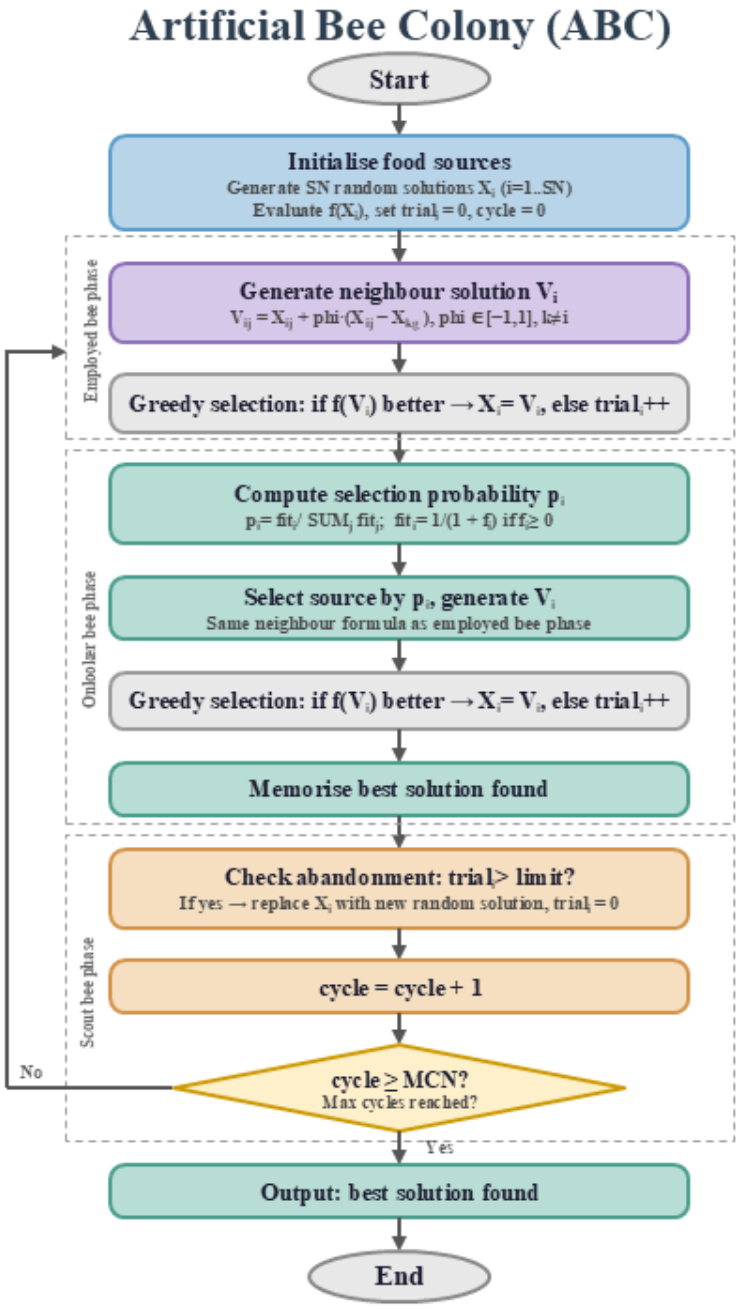


Figure 3. Flowchart ABC.

4.1.2 Benefits and Strengths

The ABC algorithm possesses several documented strengths as identified in the literature:

- Easy to implement, with limited control parameters (colony size, limit, maximum cycles), so that it can be used by practitioners that do not have much knowledge in parameter tuning (Karaboga and Basturk (2007)).
- Good trade-off between exploration (scout bees) and exploitation (employed and onlooker bees), a key to preventing premature convergence (Karaboga and Akay (2009)).
- Good performance on multi-modal, non-convex, non-differentiable benchmark functions, usually performing better on high-dimensional problems than genetic algorithms (GA) and particle swarm optimisation (PSO) (Karaboga and Basturk (2008)).
- Mechanisms of abandonment and scout ensure stagnation prevention mechanisms are built in, which assist the algorithm to avoid local optima without further adjustments (Garg (2016)).
- Can be used in a wide range of applications such as training neural networks, feature selection, clustering, power system optimisation, and parameter identification (Karaboga, Gorkemli, Ozturk, and Karaboga (2014)).

4.1.3 Drawbacks and Limitations

Despite its strengths, several limitations of the ABC algorithm have been reported:

- The neighbourhood search equation uses a single dimension at a time to perturb, and thus, may be slow to converge on separable or rotated benchmark functions and large-scale problems (Zhu and Kwong (2010)).

- The algorithm has a tendency to have a low convergence rate, especially on the later phases of optimisation since the algorithm is mostly random in terms of the neighbourhood search mechanism without any directional information (Garg (2016)).
- The limit parameter can influence performance in a bad way; a bad choice of the parameter may result in the premature rejection of otherwise potentially good solutions or a lack of exploration (Karaboga and Akay (2009)).
- In high-dimensional continuous optimisation, it can be much more expensive to get ABC to compete with newer algorithms like GWO or DE in terms of solution quality using few function evaluations (Mirjalili et al. (2014)).
- The fundamental ABC does not have a globally guided mechanism, which may minimize its exploitation power in comparison with PSO-based algorithms (Zhu and Kwong (2010)).

In response to these limitations, numerous modified variants have been proposed, including the best-guided ABC (GABC) by Zhu and Kwong (2010) (Zhu and Kwong (2010)), modified ABC (MABC) by Gao and Liu (2011) (Gao and Liu (2011)), and various hybrid approaches combining ABC with other metaheuristics.

4.2 Particle Swarm Optimization (PSO)

4.2.1 Background and Biological Inspiration

Particle Swarm Optimization (PSO) was first introduced by Kennedy and Eberhart (1995) (Kennedy and Eberhart (1995)) as a social behavior of flocking and schooling of birds, where they use their personal experience (pbest) and the global best position (gbest) that has been discovered by the swarm to update velocities and positions. The inertia weight to stabilize exploration and exploitation was pioneered by Shi and Eberhart (1998) (Shi and Eberhart (1998)) and became the standard PSO formulation, whereas Clerc and

Kennedy (2002) (Clerc and Kennedy (2002)) suggested the constriction factor as an alternative convergence mechanism. The flowchart of PSO is demonstrated in Figure 4

4.2.2 Benefits and Strengths

PSO has been extensively adopted in the literature due to the following well-documented strengths:

- Ease of use with few parameters to tune (swarm size, c_1, c_2, w), which makes it one of the simplest algorithms to use by researchers and practitioners alike among the population-based ones (Kennedy and Eberhart (1995)).
- The global best-guided social learning mechanism of the evolutionary algorithms, like Genetic Algorithms, especially on unimodal and low-dimensional problems, is a property of fast convergence speed of the algorithm (Shi and Eberhart (1998)).
- Effective behavior in a broad class of continuous optimisation problems, such as non-linear, non-convex, and multi-modal functions, which has been widely demonstrated in benchmark studies (Bratton and Kennedy (2007)).
- Memory-based mechanism (pbest and gbest) enables the swarm to store historically useful information during the optimisation procedure, which adds to an effective search (Eberhart and Kennedy (1995)).
- Easy hybridisation with other algorithms (e.g. PSO-DE, PSO-GA) and generalisation to multi-objective, discrete, and constrained optimisation spaces (Coello, Pulido, and Lechuga (2004)).
- PSO is computationally efficient in engineering applications because of its low computational overhead per iteration and scalability to moderate-dimensional problems (Poli, Kennedy, and Blackwell (2007)).

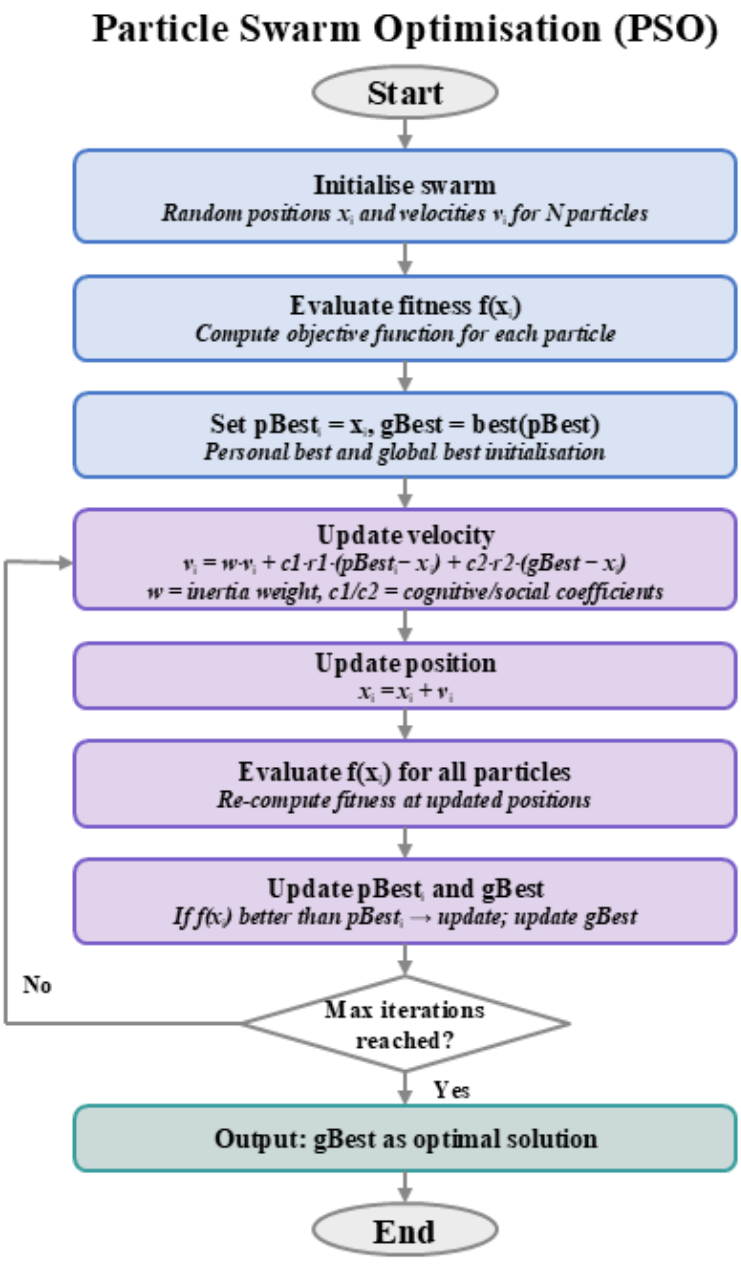


Figure 4. Flowchart PSO.

4.2.3 Drawbacks and Limitations

Despite widespread success, PSO exhibits several notable limitations as reported in the literature:

- Premature convergence: This is a well-known issue; when all the particles converge towards gbest at a very fast rate, diversity is lost, and the swarm becomes stuck in local solution sets, particularly on multi-modal problems (Van den Bergh and Engelbrecht (2006)).
- Performance is much lower on high-dimensional problems ($D > 100$) because the search space is exponentially growing and the default velocity-position update algorithm cannot ensure sufficient coverage (Bratton and Kennedy (2007)).
- PSO does not have an explicit stagnation recovery mechanism similar to that of the scout bees of ABC, i.e., a swarm converging too soon is not automatically reinitiated (Mirjalili et al. (2014)).
- Sensitivity to parameters: The inertia weight and acceleration coefficients are highly sensitive parameters that have a great effect on performance, and the best settings depend on the type of problem, often needing tuning on a problem-specific basis (Shi and Eberhart (1998)).
- It is not clear how the standard PSO can be adapted to discrete combinatorial optimisation unless it is changed, since the velocity and position updates are naturally defined in continuous space (Kennedy and Eberhart (1997)).
- Convergence guarantees at the theoretical level are conditional and require parameters to satisfy certain stability conditions, and thus rigorous convergence analysis is not trivial (Clerc and Kennedy (2002)).

Variants such as Fully Informed PSO (FIPS) by Mendes et al. (2004) (Mendes, Kennedy, and Neves (2004)), Comprehensive Learning PSO (CLPSO) by Liang et al. (2006) (Liang,

Qin, Suganthan, and Baskar (2006)), and Adaptive PSO (APSO) by Zhan et al. (2009) (Zhan, Zhang, Li, and Chung (2009)) have been developed to address these limitations.

4.3 Grey Wolf Optimizer (GWO)

4.3.1 Background and Biological Inspiration

The Grey Wolf Optimizer (GWO), proposed by Mirjalili, Mirjalili, and Lewis (2014) (Mirjalili et al. (2014)), is inspired by the social hierarchy and cooperative hunting behavior of grey wolves (*Canis lupus*), abstracting their pack structure into four leadership levels: alpha (α, best solution), beta (β, second-best), delta (δ, third-best), and omega (ω, remaining candidates), where the three elite wolves jointly guide the pack toward the optimal solution while maintaining population diversity (Mirjalili et al. (2014)). The flowchart of GWO is demonstrated in Figure 5.

4.3.2 Benefits and Strengths

GWO has gained significant attention in the literature due to the following strengths:

- Less control parameters than most competing algorithms, only population size and maximum iterations are needed as main settings, and no user-defined weights similar to PSO c_1, c_2 or ABC limit parameter (Mirjalili et al. (2014)).
- Good balance of exploration-exploitation obtained with the linearly declining parameter a and the adaptive coefficient A, which finds its own way out of global search to local refinement without being scheduled (Mirjalili et al. (2014)).
- Multi-guide mechanism with alpha, beta, and delta simultaneous position updates minimizes the threat of premature convergence as compared to single-guide algorithms like the standard PSO (Mirjalili et al. (2014), Faris, Aljarah, Al-Betar, and Mirjalili (2018)).

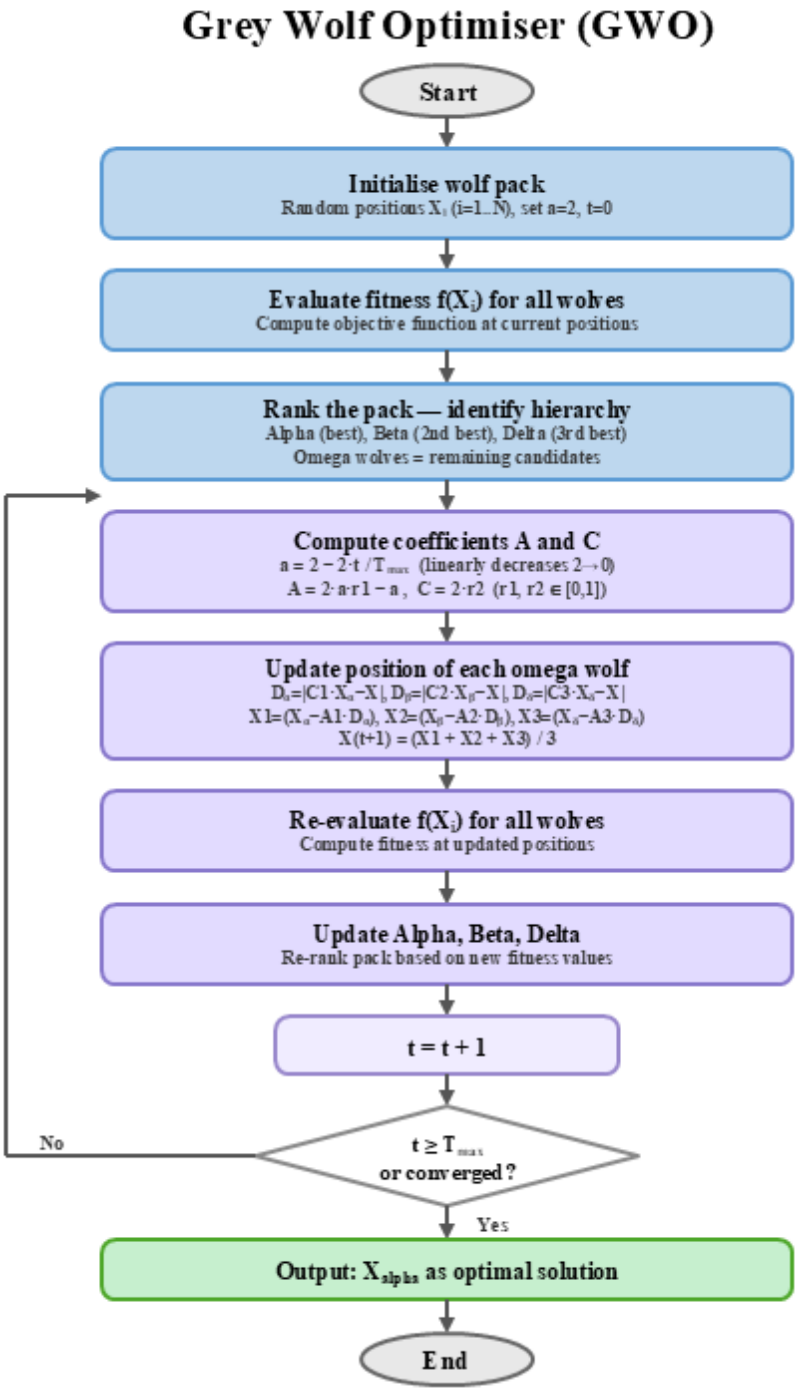


Figure 5. Flowchart GWO.

- Better or competitive performance on 29 benchmark functions (unimodal, multimodal, fixed-dimension multimodal) than PSO, GA, DE, EP, and ES reported by Mirjalili et al. (2014) (Mirjalili et al. (2014)) in the original article.
- Applied to a wide range of engineering problems such as optimal power flow, feature selection, medical image segmentation, PID controller tuning, and economic dispatch with great generalisation capability proven (Mirjalili (2015), Faris et al. (2018)).
- GWO is easy to implement, comprehend, and customize due to its simple conceptual model and clear mathematical formulation (Mirjalili et al. (2014)).

4.3.3 Drawbacks and Limitations

Several limitations of GWO have been identified in the subsequent literature:

- It has been reported to have a slow convergence rate and a lack of ability to exploit the solution at the later stages of optimisation due to the averaging position update equation that may overshoot the optimal solution in later iterations (Long, Jiao, Liang, and Tang (2018)).
- The linear reduction of a is inflexible and might not suit every type of problem; adaptive or non-linear update schemes have been suggested in variant forms to accommodate this (Kaveh and Zakian (2018)).
- The inefficiency of the basic position update in traversing correlated search dimensions can cause performance to degrade on high-dimensional, complex, and rotating benchmark functions (Kaveh and Zakian (2018)).
- Similar to most swarm algorithms, GWO can have early convergence when there is a rapid loss of population diversity, especially on problems with small global optima basins (Faris et al. (2018)).

- The algorithm lacks a stagnation recovery mechanism; once the three elite wolves have been drawn to a local optimum, the rest of the pack follows, making it unlikely that they can escape (Long et al. (2018)).
- A little theoretical study has been done on convergence properties of GWO relative to PSO, where more formal convergence properties are obtained (Mirjalili et al. (2014)).

In response to identified limitations, numerous improved GWO variants have been developed, including the Improved GWO (I-GWO) by Kaveh and Zakian (2018) (Kaveh and Zakian (2018)), the multi-strategy enhanced GWO by Long et al. (2018) (Long et al. (2018)), and hybrid GWO-PSO approaches that combine the complementary strengths of both algorithms.

4.4 Proposed PGWA Algorithm for PID Parameter Optimization

In this section, the Particle Swarm Optimization–Grey Wolf Optimizer with Adaptive Artificial Bee Colony (PGWA), a new hybrid metaheuristic suggested in this paper to tune the proportional-integral-derivative (PID) controller gains applied to the Load Frequency Control (LFC) problem is provided. The algorithm combines three swarm intelligence methods PSO, GWO, and ABC within a sequential three-phase architecture executed at every iteration. The set of PID gain parameters is directly encoded into each candidate solution in the population, and The objective function assesses the quality of the closed-loop LFC frequency response for each candidate. The subsections below describe the initialization, each algorithmic phase, and the adaptive mechanism that constitutes the primary contribution of PGWA. The flowchart of PGWA is demonstrated in Figure 6

4.4.1 Solution Encoding and Objective Function

The population of agents in PGWA corresponds to candidate PID parameter vectors for the LFC system. The search space is characterised by lower and upper bounds lb and ub on each dimension, and all positions are maintained within these bounds throughout optimization. The objective function $f(\cdot)$ evaluates the integral of the time-weighted absolute error (ITAE) of the frequency deviation signal resulting from the application of the candidate PID gains in the LFC closed-loop model. The optimization task is therefore to find the global minimum of f over the bounded search space.

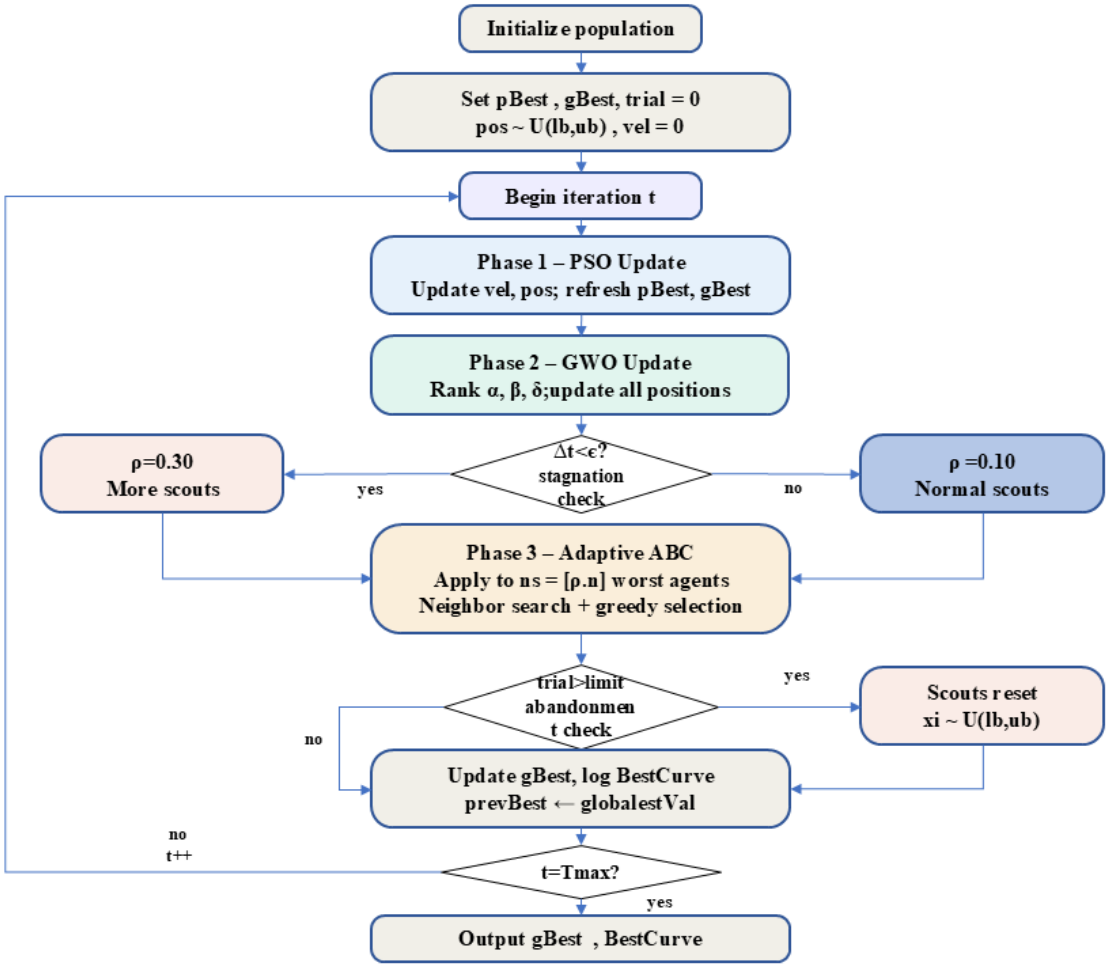


Figure 6. Flowchart PGWA.

4.4.2 Initialization

A population of n agents is initialized by uniform random sampling within the bounded search domain. The initial position of each agent i is given by:

$$\mathbf{x}_i^0 \sim \mathcal{U}(lb,\, ub), \qquad i = 1, 2, \ldots, n \tag{25}$$

Initial velocities are set to zero ($\mathbf{v}_i^0 = \mathbf{0}$). The fitness value of each agent is computed by evaluating the objective function, and personal best positions are set as $\mathbf{p}_i = \mathbf{x}_i^0$. The global best solution $\mathbf{g}^*$ is initialized as the agent with the minimum fitness value across the entire population. A trial counter $trial_i = 0$ is assigned to each agent for use in the adaptive ABC phase.

4.4.3 Phase 1: PSO Velocity and Position Update

In the first phase of each iteration t, all agents are updated using the PSO mechanism. The inertia weight w_t decreases linearly over the course of optimization to progressively shift the search behavior from exploration to exploitation:

$$w_t = w_{\max} - t \cdot \frac{w_{\max} - w_{\min}}{T_{\max}} \tag{26}$$

The velocity of each agent is updated by combining three influences: the agent's previous velocity scaled by the inertia weight, a cognitive term that attracts the agent toward its personal best position, and a social term that attracts it toward the population global best:

$$\mathbf{v}_i^{t+1} = w_t\, \mathbf{v}_i^t + c_1\, \mathbf{r}_1 \odot \left(\mathbf{p}_i - \mathbf{x}_i^t\right) + c_2\, \mathbf{r}_2 \odot \left(\mathbf{g}^* - \mathbf{x}_i^t\right) \tag{27}$$

where $\mathbf{r}_1, \mathbf{r}_2 \sim \mathcal{U}(0,1)^d$ are independently sampled random vectors at each iteration, $\odot$ denotes element-wise (Hadamard) multiplication, and c_1, c_2 are the cognitive and social acceleration coefficients, respectively. The velocity is clamped to $[v_{\min}, v_{\max}]$ to prevent

divergence. The agent position is then updated as:

$$\mathbf{x}_i^{t+1} = \mathbf{x}_i^t + \mathbf{v}_i^{t+1} \tag{28}$$

Positions that violate the domain bounds are projected back onto $[lb,\ ub]$. Personal and global best records are updated if the new fitness value is strictly lower than the previously recorded best.

4.4.4 Phase 2: GWO Hierarchical Position Update

Following the PSO phase, the GWO update is applied to the same population. Fitness values are recomputed, and the three fittest agents are designated as the alpha (α), beta (β), and delta (δ) wolves, representing the three best candidate PID solutions found in the current iteration. The GWO convergence parameter a_t decreases linearly from 2 to 0 over $T_{\max}$ iterations, controlling the balance between exploration and exploitation Mirjalili et al. (2014):

$$a_t = 2 - t \cdot \frac{2}{T_{\max}} \tag{29}$$

For each agent i and each dimension d, three position estimates are computed with reference to each leader wolf. The estimate guided by the alpha wolf is:

$$D_\alpha^d = \left| C_1 \cdot \alpha^d - x_i^d \right| \tag{30}$$

$$X_1^d = \alpha^d - A_1 \cdot D_\alpha^d \tag{31}$$

Analogous expressions X_2^d and X_3^d are computed for the beta and delta wolves, respectively, using independently drawn random coefficients:

$$A_k = 2\,a_t\,r_1 - a_t, \qquad C_k = 2\,r_2, \qquad r_1, r_2 \sim \mathcal{U}(0,1) \tag{32}$$

The updated position of agent i in dimension d is taken as the centroid of the three hunting estimates, ensuring that the new position is simultaneously attracted toward all three

leader wolves Mirjalili et al. (2014):

$$x_i^{t+1,\,d} = \frac{X_1^d + X_2^d + X_3^d}{3} \tag{33}$$

Boundary violations are corrected by projection. This multi-attractor update mechanism reduces the risk of premature convergence by maintaining multiple distinct reference points, which is particularly valuable for the multimodal PID gain landscape of the LFC system.

4.4.5 Phase 3: Adaptive ABC Mechanism

Stagnation Detection. After the GWO update, the adaptive ABC phase is triggered. The algorithm first evaluates whether the population is making meaningful progress by computing the absolute improvement in the global best fitness value relative to the previous iteration:

$$\Delta_t = \left| f_{t-1}^* - f_t^* \right| \tag{34}$$

This improvement metric acts as a real-time convergence indicator. If Δ_t falls below the stagnation threshold ε, the population is deemed to have stagnatedthat is, the current swarm configuration is no longer producing useful improvement in LFC performance. The adaptive scout ratio is then set according to the following rule:

$$\rho_t = \begin{cases} 0.30 & \text{if } \Delta_t < \varepsilon \quad \text{(stagnation detected)} \\ 0.10 & \text{otherwise} \quad \text{(normal convergence)} \end{cases} \tag{35}$$

This binary switching rule is the central novelty of PGWA. During periods of active improvement, the scout ratio is kept at the baseline value of 0.10, conserving function evaluations for the PSO and GWO exploitation phases. When the global best stagnates, the ratio triples to 0.30, forcibly injecting new diversity into the population. The number of scouts applied at iteration t is:

$$n_s = \lfloor \rho_t \cdot n \rfloor \tag{36}$$

The ABC operator is applied exclusively to the n_s worst-performing agents, identified by sorting the population in descending order of fitness. This targeted approach concentrates the exploratory perturbation on agents that are least likely to contribute to progress through exploitation alone, preserving the quality of the elite solutions found by the PSO and GWO phases.

Neighbour Search and Greedy Selection. For each selected scout agent i, a distinct random neighbour $k \neq i$ is drawn uniformly from the population. A candidate PID parameter vector is generated using the ABC perturbation operator, which perturbs the current position along the direction toward the randomly selected neighbour Karaboga and Basturk (2007):

$$\mathbf{x}_i^{\text{new}} = \mathbf{x}_i + \boldsymbol{\phi} \odot (\mathbf{x}_i - \mathbf{x}_k)\,, \qquad \boldsymbol{\phi} \sim \mathcal{U}(-1, 1)^d \tag{37}$$

The candidate solution is projected onto the domain bounds and evaluated. A greedy selection rule determines whether the new solution replaces the current one:

$$\mathbf{x}_i \leftarrow \begin{cases} \mathbf{x}_i^{\text{new}} & \text{if } f(\mathbf{x}_i^{\text{new}}) < f(\mathbf{x}_i) \\ \mathbf{x}_i & \text{otherwise} \quad (trial_i \mathrel{+}= 1) \end{cases} \tag{38}$$

Scout Reinitialisation. If the trial counter of agent i exceeds the abandonment limit L, the agent is fully reinitialised by random sampling from the entire bounded domain, simulating the ABC scout bee abandonment behavior Karaboga and Basturk (2007). This provides a hard-reset escape mechanism that is independent of the current population topology:

$$\mathbf{x}_i \sim \mathcal{U}(lb,\, ub), \quad trial_i \leftarrow 0, \qquad \text{if } trial_i > L \tag{39}$$

This reinitialisation ensures that agents which have been persistently unsuccessful in improving their PID solutions are replaced with fresh candidates drawn from the entire gain space, preventing any single agent from indefinitely occupying an unproductive region of the search space.

4.4.6 Global Best Update and Convergence Logging

Following the completion of all three phases, the entire population is re-evaluated and the global best $\mathbf{g}^*$ is updated if any agent achieves a new minimum objective value. The best fitness at each iteration is recorded in the convergence curve $\mathrm{BestCurve}[t] = f_t^*$, which is used to assess convergence behavior. The stagnation reference is updated as $f_{t-1}^* \leftarrow f_t^*$ before proceeding to the next iteration.

4.4.7 Motivation for the Proposed PGWA Algorithm

Despite the demonstrated high performance of ABC, PSO, and GWO individually across a wide range of optimization problems, each algorithm carries inherent limitations that restrict its effectiveness when applied in isolation to complex, high-dimensional, and multimodal search landscapes such as the PID parameter tuning problem in Load Frequency Control (LFC) systems. A careful analysis of these limitations reveals complementary deficiencies that motivate the design of a unified hybrid framework capable of addressing them simultaneously.

The Particle Swarm Optimization (PSO) algorithm is well-regarded for its rapid early-stage convergence, driven by a global best-guided social learning mechanism that enables the swarm to identify promising regions of the search space with relatively few function evaluations Kennedy and Eberhart (1995); Shi and Eberhart (1998). However, this strength is also the source of its most critical weakness: premature convergence. As all particles are simultaneously attracted toward a single global best attractor, population diversity collapses rapidly, causing the swarm to stagnate in local optima before the global optimum is reached Van den Bergh and Engelbrecht (2006). PSO further lacks an explicit stagnation recovery mechanism, meaning that once convergence to a suboptimal region occurs, the algorithm has no inherent means of reinitialising or escaping Mirjalili et al. (2014). These drawbacks are particularly consequential in the nonlinear, multimodal ITAE surface of the LFC-PID tuning problem, where local optima are numerous and visually proximate to the

global minimum.

The Grey Wolf Optimizer (GWO) partially addresses the premature convergence problem of PSO by replacing the single-attractor update with a multi-guide mechanism that simultaneously incorporates the three fittest solutionsalpha, beta, and deltaas distinct reference points during position updates Mirjalili et al. (2014). This hierarchical structure reduces the risk of the entire population collapsing to a single suboptimal attractor and provides a more adaptive balance between exploration and exploitation through the linearly decreasing parameter a. Nevertheless, GWO exhibits its own documented limitations. The averaging position update equation can overshoot the global optimum in the final stages of optimization, resulting in insufficient fine-grained exploitation Long et al. (2018). Furthermore, GWO does not incorporate any stagnation detection or recovery mechanism; when all three elite wolves converge to a local optimum, the omega wolves follow unconditionally, and no reinitialisation is triggered Faris et al. (2018). The rigid linear decay of a also limits adaptability across different problem landscapes, as it does not respond to the actual convergence behavior of the population Kaveh and Zakian (2018).

The Artificial Bee Colony (ABC) algorithm offers a qualitative different search strategy that addresses the stagnation problem, absent in both PSO and GWO. The scout bee reinitialisation mechanism replaces exhausted food sources with entirely new, randomly sampled solutions, providing a population-level escape mechanism that operates independently of the current search topology Karaboga and Basturk (2007). This makes ABC inherently resistant to permanent entrapment in local optima and provides robust exploration across the full bounded search space. However, ABC suffers from slow convergence speed, particularly in the later stages of optimization, because its neighbourhood search is undirected and does not exploit gradient or swarm-level directional information Garg (2016). The one-dimensional-at-a-time perturbation in the employed bee phase further limits its exploitation efficiency on high-dimensional and correlated search spaces Zhu and Kwong (2010). Applied in isolation to the 18-dimensional PID gain space of the LFC problem, ABC would require substantially more function evaluations to achieve the convergence quality attainable by the velocity-driven mechanisms of PSO and GWO.

The deficiencies identified above exhibit a clear pattern of complementarity. PSO provides fast convergence but lacks diversity recovery; GWO provides a multi-attractor hierarchy that mitigates premature collapse but still lacks an active stagnation escape, and ABC provides reliable population-level reinitialisation but lacks the directional search efficiency necessary for competitive convergence speed. No single algorithm possesses all three properties simultaneously: fast early convergence, hierarchical multi-attractor exploitation, and adaptive stagnation recovery. This gap directly motivates the development of the Particle Swarm Optimization Grey Wolf Optimizer with Adaptive Artificial Bee Colony (PGWA) algorithm.

PGWA is specifically designed to unify these complementary strengths within a sequential three-phase architecture. In Phase 1, the PSO velocity position update is applied to achieve rapid identification of promising regions in the PID gain space through socially guided swarm movement. In Phase 2, the GWO hierarchical update refines the population by drawing each agent simultaneously toward three elite solution attractors, reducing the single-attractor collapse vulnerability of standalone PSO and enhancing the exploitation depth. In Phase 3, an adaptive ABC mechanism monitors the real-time convergence signal and deploys scout reinitialisation precisely when the global best fitness stagnates, ensuring that population diversity is restored at the moment it is most needed without sacrificing computational efficiency during productive exploitation phases. The adaptive scout ratio mechanism further extends beyond the capabilities of the standard ABC by dynamically scaling the exploration intensity in direct response to the observed convergence behavior, rather than applying reinitialisation at a fixed rate regardless of population progress. Together, these three phases form an integrated optimization strategy that preserves the individual advantages of ABC, PSO, and GWO while systematically eliminating their respective limitations.

4.4.8 Rationale for the Hybrid Architecture

The three-phase sequential architecture of PGWA is motivated by the complementary strengths of its constituent algorithms across distinct phases of the PID parameter search. PSO is effective in the early iterations for rapidly identifying promising regions of the gain space through velocity-driven swarm movement; however, it is susceptible to premature convergence as all particles are drawn toward a single global best attractor. GWO addresses this by maintaining three distinct leadership attractors (α, β, δ) that simultaneously guide the population toward multiple competitive solutions, reducing the risk that all agents converge to the same local minimum in the ITAE surface.

The adaptive ABC phase provides a qualitatively different form of diversity that neither PSO nor GWO can supply. The scout reinitialisation operator generates solutions drawn uniformly from fully bounded domain, completely independent of the current population configuration. This is critical for escaping deep local optima in the PID gain landscape, where both PSO and GWO may continue to refine solutions in an unproductive region because all reference points personal bests, global bests, and wolf leadershave collectively converged to that region.

The adaptive scout ratio mechanism further refines this behavior by ensuring that exploratory reinitialisation is deployed only when the observed convergence signal Δ_t indicates that the current population configuration is no longer capable of self-improvement. This prevents unnecessary expenditure of function evaluations on random reinitialisation during productive exploitation phases, maintaining computational efficiency while providing a reliable recovery mechanism when convergence stalls. The combined effect is an algorithm that exploits efficiently when progress is being made and explores aggressively when it is nota property that is particularly valuable for the nonlinear, multimodal PID tuning landscape of LFC systems.

4.4.9 Algorithm Parameters

The parameters of PGWA used in this work are summarised in Table 4. The PSO coefficients $c_1 = c_2 = 2$ and inertia weight range $[0.4,\ 0.9]$ follow established conventions Kennedy and Eberhart (1995). The ABC trial limit $L = 5$ is consistent with the original ABC formulation for moderate population sizes Karaboga and Basturk (2007). The stagnation threshold $\varepsilon = 10^{-6}$ is chosen to be responsive to genuine convergence stagnation while remaining insensitive to numerical noise in the objective function evaluations.

Table 4. PGWA algorithm parameter configuration..

Parameter	Symbol	Value	Role in PGWA
Population size	n	20	Number of search agents (PID candidates)
Problem dimension	d	18	PID parameter vector length
Maximum iterations	$T_{\max}$	20	Optimization stopping criterion
PSO cognitive coeff.	c_1	2.0	Attraction toward personal best
PSO social coeff.	c_2	2.0	Attraction toward global best
Inertia weight (max)	$w_{\max}$	0.9	Initial exploration emphasis
Inertia weight (min)	$w_{\min}$	0.4	Final exploitation emphasis
Velocity bounds	$[v_{\min},\ v_{\max}]$	± 0.2	Prevents unbounded acceleration
ABC trial limit	L	5	Abandonment threshold before scout reset
Base scout ratio	ρ_{base}	0.10	Normal ABC exploration proportion
Stagnation scout ratio	ρ_{stag}	0.30	Exploration proportion under stagnation
Stagnation threshold	ε	10^{-6}	Convergence sensitivity for detection

4.4.10 Algorithm Pseudocode

The complete PGWA procedure is summarised in Algorithm 1.

Algorithm 1 PGWA for PID Tuning in LFC

Require: $f(\cdot)$, lb, ub, n, $T_{\max}$, c_1, c_2, $w_{\max}$, $w_{\min}$, L, ε
Ensure: $\mathbf{g}^*$ (optimal PID gains), $\mathrm{BestCurve}$

Initialise $\mathbf{x}_i \sim \mathcal{U}(lb, ub)$, $\mathbf{v}_i = \mathbf{0}$, $trial_i = 0$ **for all** i
Evaluate $f(\mathbf{x}_i)$; set $\mathbf{p}_i = \mathbf{x}_i$, $\mathbf{g}^* = \arg\min_i f(\mathbf{x}_i)$
for $t = 1$ **to** $T_{\max}$ **do**
    Phase 1: PSO
    Compute w_t using Eq. (26)
    for each agent i **do**
        Update $\mathbf{v}_i$ using Eq. (27); clamp to $[v_{\min}, v_{\max}]$
        Update $\mathbf{x}_i$ using Eq. (28); project onto $[lb, ub]$
        Update $\mathbf{p}_i$ and $\mathbf{g}^*$ if $f(\mathbf{x}_i)$ improves
    end for
    Phase 2: GWO
    Evaluate $f(\mathbf{x}_i)$ for all i; rank population
    Assign α, β, δ as the three fittest agents
    Compute a_t using Eq. (29)
    for each agent i, each dimension d **do**
        Compute X_1^d, X_2^d, X_3^d using Eqs. (30)–(32)
        Update x_i^d using Eq. (33); project onto $[lb, ub]$
    end for
    Phase 3: Adaptive ABC
    Compute $\Delta_t = |f_{t-1}^* - f_t^*|$ using Eq. (34)
    Set ρ_t using Eq. (35); compute n_s using Eq. (36)
    Select n_s worst agents by descending fitness rank
    for each selected agent i **do**
        Select random neighbour $k \neq i$
        Generate $\mathbf{x}_i^{\mathrm{new}}$ using Eq. (37)
        Apply greedy selection using Eq. (38)
        if $trial_i > L$ **then**
            Reinitialise $\mathbf{x}_i$ using Eq. (39)
        end if
    end for
    Update & Log
    Update $\mathbf{g}^*$ across full population
    $\mathrm{BestCurve}[t] \leftarrow f_t^*$; $\quad f_{t-1}^* \leftarrow f_t^*$
end for
return $\mathbf{g}^*$, $\mathrm{BestCurve}$

4.5 Objective Functions in Load Frequency Control

In Load Frequency Control (LFC), a performance index also known as objective function is employed to measure the system error and drive optimization algorithms for optimal

controller gains. The error signal $e(t)$ is generally the frequency deviation (Δf) and/or tie-line power deviation (ΔP_{tie}), which is a combination of the Area Control Error (ACE). The Integral of Absolute Error (IAE), Integral of Time-weighted Absolute Error (ITAE), Integral of Squared Error (ISE), and Integral of Time-weighted Squared Error (ITSE) are the most commonly used criteria to design load frequency controllers. The controller gain values that make the minimum objective function optimal gives the optimum settings of the AGC system.

4.5.1 Integral of Absolute Error (IAE)

The IAE performance index is defined as:

$$J_{\text{IAE}} = \int_0^T |e(t)| \; dt \tag{40}$$

The IAE gives a clue to the overall error magnitude without focusing on the duration and the severity of the individual errors; the lower the IAE the greater the overall control performance in reducing deviations. Since all errors are equally weighted, independent of the time of their occurrence throughout the transient, IAE prefers controllers whose steady-state accuracy is good. IAE measures the cumulative error and is useful in assessing the overall control accuracy of LFC systems. It is extensively used together with other indices to give a holistic comparative assessment of the LFC controller performance Eltamaly, Sayed, Alotaibi, Abo-Khalil, and Ahmed (2026); Jagatheesan et al. (2023).

4.5.2 Integral of Time-weighted Absolute Error (ITAE)

The ITAE criterion is defined as:

$$J_{\text{ITAE}} = \int_0^T t \, |e(t)| \; dt \tag{41}$$

The time-weighting factor t gradually punishes the errors which remain longer in the transient, incentivizing optimization to the solutions that converge fast. The ITAE criterion is

considered the most useful, as it offers a trade-off between speed, smoothness, and stability; as it punishes long-term errors more than early deviations, the ITAE criterion is effective at reducing sustained oscillations, minimizing steady-state error, and increasing system damping. In LFC experiments, the ITAE objective function is found to be more effective in system performance than other functions, and also reduces the maximum overshoot. These are why ITAE is the most widely used objective function in LFC literature. A PSO-PID controller that uses an ITAE cost functional yields a more regulated frequency response than a controller tuned with traditional, GA, or DE algorithm techniques, providing faster settling with reduced deviations.

4.5.3 Integral of Time-weighted Squared Error (ITSE)

The ITSE criterion is defined as:

$$J_{\mathrm{ITSE}} = \int_0^T t\,[e(t)]^2\,dt \tag{42}$$

ITSE is a combination of the time-weighting of ITAE and the squared penalty of ISE. The ITSE measure squares the error multiplied by time to integration, thereby assigning greater weight to those errors that happen later in the simulation, thereby assessing the performance of the controller in stabilizing the system over time. ITSE emphasizes errors that remain constant in the long term, and therefore it is effective in controllers that are intended to remove long-term oscillations. The ITSE objective function however, provides a large controller output when there is a sudden change in input, which might not be preferable in some LFC configurations. In spite of this drawback, ITSE-optimal controllers have been shown to exhibit competitive dynamic performance in multi-source and microgrid LFC investigations Manoharan, Dash, and Rajesh (2017); Paliwal, Srivastava, and Pandit (2020).

5 Proposed System for Attack Detection

To rigorously evaluate the proposed DA-CGAE framework, three well-established deep learning architectures Long Short-Term Memory (LSTM), Bidirectional LSTM (BiLSTM), and Convolutional Neural Network (CNN) are implemented as baseline comparators. Each model is trained under identical experimental conditions on the same labelled dataset, using the same input window of $T = 200$ time steps and $F = 3$ features (Δf, ΔP_{tie}, and ACE). All baselines employ Binary Cross-Entropy (BCE) loss with the Adam optimiser and dropout regularisation ($p = 0.3$) to ensure a fair comparison.

5.1 Long Short-Term Memory (LSTM)

Introduced by Hochreiter and Schmidhuber Hochreiter and Schmidhuber (1997), LSTM builds on regular RNNs by adding forget, input, and output gating to address the vanishing-gradient problem and capture long-range temporal correlations. These features render LSTM suitable for sequential signal analysis in LFC cyber-attack detection. Both Zografopoulos et al. Zografopoulos, Ospina, Liu, and Konstantinou (2021) and He et al. He, Mendis, and Wei (2017) have shown that LSTM can identify false data injection (FDI) attacks in multi-area LFC systems with high precision under different attack scenarios.

The LSTM baseline in this work consists of two stacked LSTM layers with 128 hidden units, a fully connected binary classification head, and dropout regularisation between layers to mitigate overfitting.

5.2 Bidirectional LSTM (BiLSTM)

BiLSTM, introduced by Schuster and Paliwal Schuster and Paliwal (1997), extends the standard LSTM by processing input sequences in both temporal directions, allowing the network to use future context at any given time step. This has proven beneficial for cyber-

attack detection in power systems. Both Takiddin et al. Takiddin, Ismail, Zafar, and Serpedin (2021) and Habibi et al. Habibi, Khairuddin, Norouzi, and Islam (2022) found that bidirectional temporal modelling is more effective than unidirectional LSTM for detecting low-magnitude stealthy FDI attacks in LFC systems. The BiLSTM baseline comprises two stacked bidirectional layers with 128 hidden units in each direction (256 effective output dimensions per time step), and a fully connected sigmoid layer for binary classification. Training follows the same BCE loss and Adam optimiser setup as the LSTM baseline.

5.3 Convolutional Neural Network (CNN)

CNNs, originally developed for image recognition by LeCun et al. LeCun, Bengio, and Hinton (2015), were subsequently applied to time-series classification, where temporal signals are treated as one-dimensional spatial structures from which hierarchical features are extracted automatically. Wang et al. D. Wang, Wang, Zhang, and Jin (2019) and Pinceti et al. Pinceti, Sankar, and Kosut (2021) demonstrated their effectiveness in detecting FDI attacks in LFC systems, showing that CNNs outperform classical machine-learning algorithms in identifying local temporal patterns indicative of coordinated attacks. The CNN baseline consists of three consecutive 1-D convolutional blocks, each containing a `Conv1D` layer, Batch Normalisation, ReLU activation, and Max-Pooling with filter sizes 64, 128, and 256 and a kernel size of 3. The output of the final block is global-average-pooled into a fixed-size feature vector, which is passed through a fully connected sigmoid layer for binary classification. Dropout ($p = 0.3$) is applied before the output layer, and input windows are transposed to shape (3×200) to match the channel-first convention of PyTorch.

5.4 Proposed Methodology: DA-CGAE

This section introduces the architecture, mathematical formulation, and operational workflow of the proposed *Disturbance-Aware Contrastive GRU Autoencoder* (DA-CGAE). DA-

CGAE is an unsupervised anomaly detector that identifies FDI cyber-attacks in LFC systems without requiring labeled training data; it detects attacks by estimating deviations between learned normal behaviour and live operational data. The framework comprises four consecutive phases: Training (Phase A), Threshold Calibration (Phase B), Inference and Attack Detection (Phase C), and FDI Attack Mitigation (Phase D), illustrated in Figures 7, 8, and 9.

5.4.1 Input Representation and Preprocessing

The model takes three LFC signals as input: frequency deviation (Δf), tie-line power deviation (ΔP_{tie}), and Area Control Error (ACE), sampled at 100 Hz. The raw signal is segmented into windows of $T = 200$ samples (5 seconds each), and each window $\mathbf{x} \in \mathbb{R}^{T \times F}$ is independently z-score normalised per feature channel before being fed into the model.

Each input channel is standardised as:

$$\mathbf{x}_{\text{norm}} = \frac{\mathbf{x} - \mu}{\sigma} \tag{43}$$

where μ and σ are the mean and standard deviation computed on the training set for each feature. This ensures that all input signals have zero mean and unit variance, enhancing optimisation stability.

To promote scale-invariant and noise-robust representations, each training window is augmented twice to produce a positive pair $(\mathbf{x}_1, \mathbf{x}_2)$:

$$\mathbf{x}_i = \mathbf{x} \cdot s_i + \boldsymbol{\epsilon}_i, \qquad i = 1, 2 \tag{44}$$

where $s_i \sim \mathcal{U}[0.992,\ 1.008]$ is a uniform random scaling factor introducing minor amplitude perturbations, and $\boldsymbol{\epsilon}_i \sim \mathcal{N}(0,\ 0.004)$ is Gaussian noise simulating sensor measurement uncertainty. The two augmented views constitute a positive pair in the contrastive

objective and are passed independently through the shared encoder.

5.4.2 Shared Encoder Backbone

Both augmented views are processed by the same shared encoder, which comprises three sequential blocks: Feature Attention, Bidirectional GRU, and Temporal Attention. Each input window is encoded into a compact 64-dimensional latent vector $\mathbf{z}$ that captures the essential temporal structure of normal LFC behaviour.

A channel-wise attention mechanism adaptively weights the contribution of each input signal. Given the input window $\mathbf{x} \in \mathbb{R}^{B\times 200\times 3}$, the attention vector is computed as:

$$\boldsymbol{\alpha} = \sigma(\mathbf{W}_2\,\mathrm{ReLU}(\mathbf{W}_1\,\mathbf{x})) \tag{45}$$

where $\mathbf{W}_1, \mathbf{W}_2 \in \mathbb{R}^{3\times 3}$ are learnable weight matrices. The attended input is:

$$\hat{\mathbf{x}} = \mathbf{x} \odot \boldsymbol{\alpha} \tag{46}$$

where $\odot$ denotes element-wise (Hadamard) multiplication. This mechanism enables the model to suppress less informative channels and focus on signals that carry more discriminative information about normal system dynamics.

The attended input $\hat{\mathbf{x}}$ is processed by a 2-layer Bidirectional GRU with hidden size $h = 128$ per direction, capturing temporal dependencies in both the forward and backward directions:

$$\mathbf{h}_t^{(\text{fwd})} = \mathrm{GRU}_{\text{fwd}}\left(\hat{\mathbf{x}}_t,\, \mathbf{h}_{t-1}^{(\text{fwd})}\right) \tag{47}$$

$$\mathbf{h}_t^{(\text{bwd})} = \mathrm{GRU}_{\text{bwd}}\left(\hat{\mathbf{x}}_t,\, \mathbf{h}_{t+1}^{(\text{bwd})}\right) \tag{48}$$

$$\mathbf{H}_t = \left[\mathbf{h}_t^{(\text{fwd})} \parallel \mathbf{h}_t^{(\text{bwd})}\right], \qquad \mathbf{H} \in \mathbb{R}^{B\times 200\times 256} \tag{49}$$

where $\parallel$ denotes vector concatenation. The full hidden state matrix $\mathbf{H} \in \mathbb{R}^{B\times 200\times 256}$ encodes both past and future context at every time step, which is essential for detecting

subtle temporal distortions introduced by FDI attacks.

Since time steps are not equally informative, a temporal attention mechanism aggregates the BiGRU hidden states into a single fixed-length context vector $\mathbf{c}$ using learned scalar weights:

$$e_t = \mathbf{V}^\top \tanh(\mathbf{W}_a \mathbf{H}_t + \mathbf{b}_a) \tag{50}$$

$$\alpha_t = \frac{\exp(e_t)}{\sum_{t'} \exp(e_{t'})} \tag{51}$$

$$\mathbf{c} = \sum_t \alpha_t \mathbf{H}_t, \qquad \mathbf{c} \in \mathbb{R}^{B\times 256} \tag{52}$$

where $\mathbf{W}_a$, $\mathbf{b}_a$, and $\mathbf{V}$ are learnable parameters. The context vector $\mathbf{c}$ is a weighted summary that places greater emphasis on time steps most characteristic of normal or anomalous behaviour.

The context vector $\mathbf{c}$ is projected to a 64-dimensional latent space through two fully connected layers with ReLU activation and Dropout regularisation ($p = 0.3$):

$$\mathbf{z} = \mathrm{Linear}(128, 64)(\mathrm{ReLU}(\mathrm{Linear}(256, 128)(\mathbf{c}))), \qquad \mathbf{z} \in \mathbb{R}^{B\times 64} \tag{53}$$

Dropout is applied between the two linear layers during training to prevent overfitting. The latent vector $\mathbf{z}$ is the compact representation of the input window shared by the two learning branches described below.

5.4.3 Dual Learning Branches

The latent vector $\mathbf{z}$ is fed in parallel into two branches: a Contrastive Projection Head and a GRU Decoder. These streams interact to define the learned representation via complementary objectives.

The contrastive branch maps $\mathbf{z}$ to a 32-dimensional embedding via a two-layer projection

head:

$$\mathbf{p} = \mathrm{Linear}(64, 32)(\mathrm{ReLU}(\mathrm{Linear}(64, 64)(\mathbf{z}))) \tag{54}$$

The output is ℓ_2-normalised before the loss is computed:

$$\hat{\mathbf{p}} = \frac{\mathbf{p}}{\|\mathbf{p}\|_2} \tag{55}$$

Training employs the Normalised Temperature-scaled Cross-Entropy (NT-Xent) loss. For a batch of N windows, each yielding two augmented views, the loss for sample i is:

$$\mathcal{L}_c = -\frac{1}{N}\sum_{i=1}^{N} \log \frac{\exp\big(\mathrm{sim}(\mathbf{z}_i,\, \mathbf{z}_i^{+})/\tau_c\big)}{\sum_{k \neq i} \exp(\mathrm{sim}(\mathbf{z}_i,\, \mathbf{z}_k)/\tau_c)} \tag{56}$$

where $\mathrm{sim}(\mathbf{u}, \mathbf{v}) = \mathbf{u}^{\top}\mathbf{v} \,/\, (\|\mathbf{u}\|\,\|\mathbf{v}\|)$ is cosine similarity, $\tau_c = 0.07$ is the temperature hyperparameter, and $\mathbf{z}_i^{+}$ denotes the embedding of the second augmented view of the same window (the positive pair of $\mathbf{z}_i$). This loss encourages the encoder to produce representations that are invariant to augmentation perturbations, capturing the underlying structure of normal LFC behaviour rather than superficial amplitude patterns.

The reconstruction branch decodes $\mathbf{z}$ back to the original signal space using a GRU-based decoder. The initial hidden state is conditioned on the latent vector:

$$\mathbf{h}_0 = \tanh(\mathbf{W}_{\text{dec}}\,\mathbf{z} + \mathbf{b}_{\text{dec}}) \tag{57}$$

The decoder unrolls over $T = 200$ steps to produce the reconstructed sequence:

$$\hat{\mathbf{x}}_{\text{recon}} = \mathrm{GRU}_{\text{decoder}}(\mathbf{z},\, \mathbf{h}_0)\,, \qquad \hat{\mathbf{x}}_{\text{recon}} \in \mathbb{R}^{B\times 200\times 3} \tag{58}$$

The reconstruction loss applies disturbance-aware time-step weighting to avoid penalising the model during legitimate high-variability events:

$$\mathcal{L}_r = \frac{1}{T}\sum_{t=1}^{T} w_t \;\|\mathbf{x}_t - \hat{\mathbf{x}}_{\text{recon},t}\|_2^2 \tag{59}$$

where the weight at each time step is:

$$w_t = 1 + \lambda \operatorname{Var}(\mathbf{x}_{t-\delta\,:\,t+\delta}) \tag{60}$$

Here λ scales the sensitivity to local variance and δ is the half-window size for local variance computation. This formulation assigns greater weight to transient disturbances, ensuring the decoder faithfully reconstructs high-energy events typical of normal system operation.

5.4.4 Joint Training Objective

The model is trained end-to-end by minimising the weighted sum of both branch losses:

$$\mathcal{L} = \alpha_r \mathcal{L}_r + \alpha_c \mathcal{L}_c \tag{61}$$

with $\alpha_r = 1.0$ and $\alpha_c = 0.08$ as the loss weighting coefficients. The dominant weight on $\mathcal{L}_r$ ensures faithful signal reconstruction, while $\mathcal{L}_c$ acts as a regulariser that promotes discriminative and robust latent representations. The AdamW optimiser is employed with early stopping (patience $= 20$ epochs) based on validation loss.

5.4.5 Threshold Calibration (Phase B)

After training, a detection threshold τ is calibrated on a held-out healthy validation set to define the boundary between normal and anomalous windows.

For each validation window, a hybrid anomaly score S is computed by combining two standardised components:

$$S = z_{\text{recon}} + z_{\text{latent}} \tag{62}$$

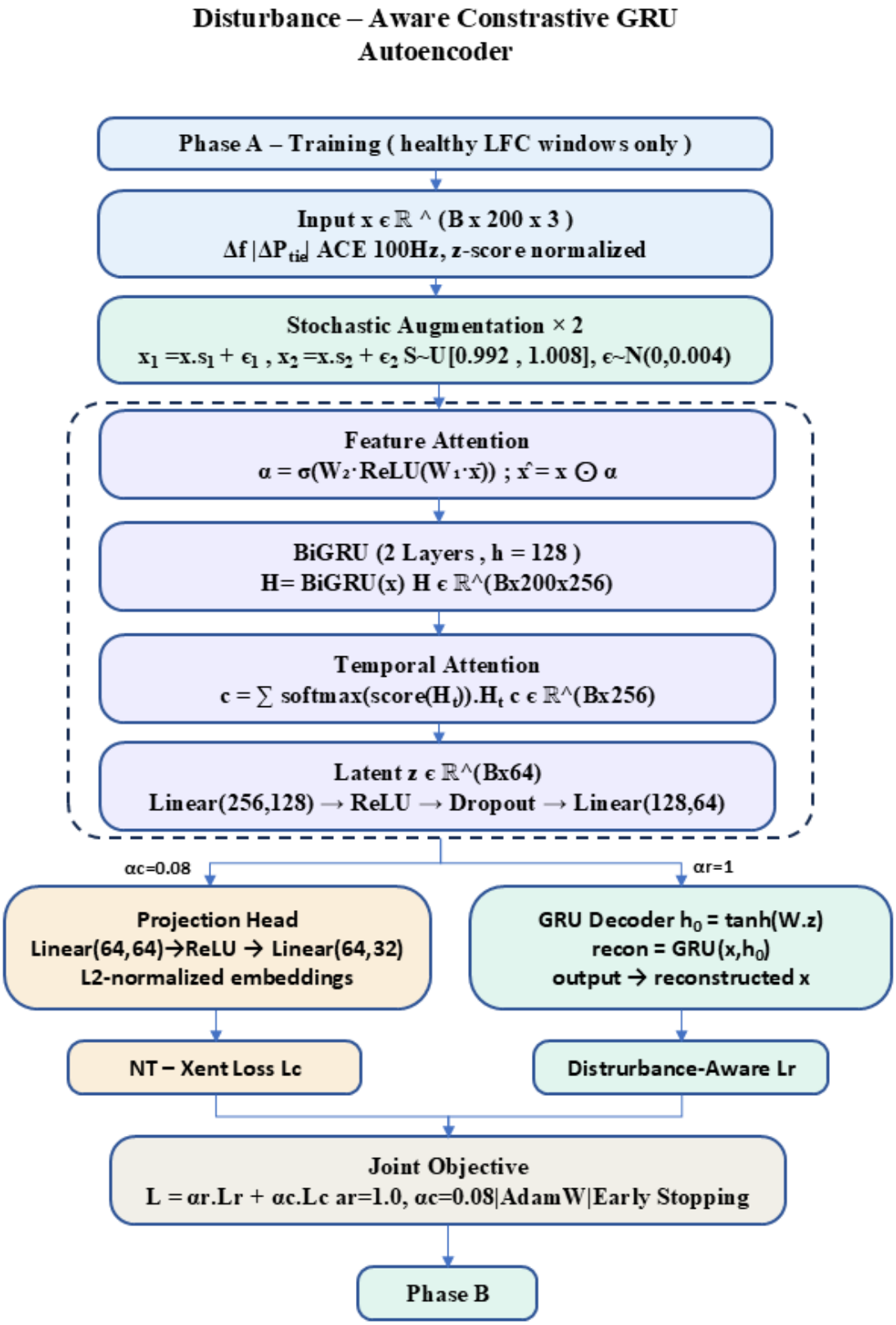


Figure 7. Flowchart of the DA-CGAE framework covering Phase A (Training).

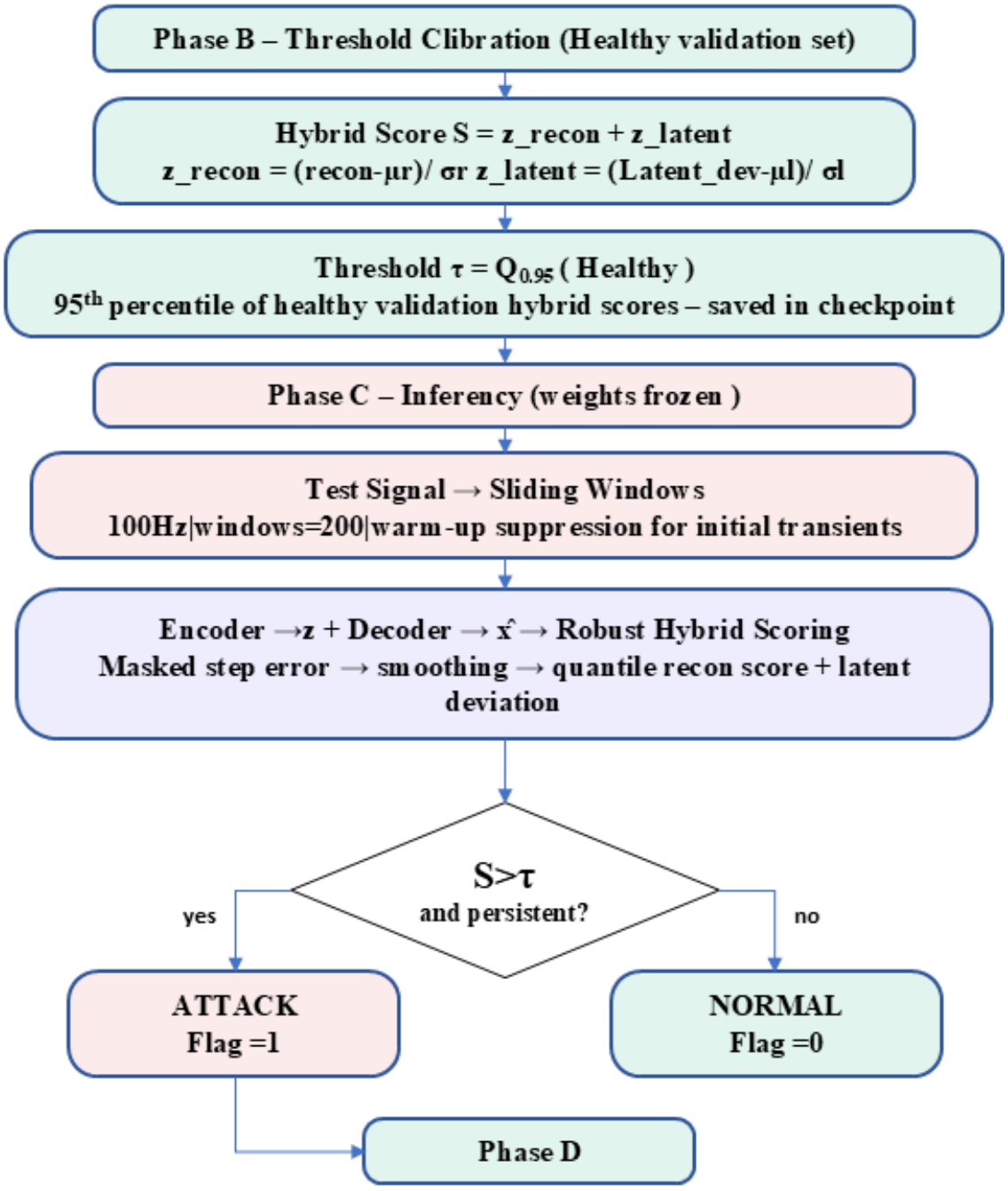


Figure 8. Flowchart of the DA-CGAE framework covering Phase B (Threshold Calibration), and Phase C (Inference and Attack Detection)..

where the individual components are:

$$z_{\text{recon}} = \frac{\text{recon\_score} - \mu_r}{\sigma_r} \tag{63}$$

$$z_{\text{latent}} = \frac{\text{latent\_dev} - \mu_l}{\sigma_l} \tag{64}$$

Here μ_r, σ_r, μ_l, and σ_l are the mean and standard deviation of the corresponding scores computed on the training set. The reconstruction error is the average squared error between $\mathbf{x}$ and $\hat{\mathbf{x}}_{\text{recon}}$, and the latent deviation is the Euclidean distance between $\mathbf{z}$ and the centroid of healthy latent representations.

The detection threshold is set at the 95th percentile of hybrid scores over the healthy validation set:

$$\tau = Q_{0.95}(S_{\text{healthy}}) \tag{65}$$

This percentile choice balances the false-alarm rate against detection sensitivity. The calibrated threshold is saved in the model checkpoint and remains fixed during inference.

5.4.6 Inference and Attack Detection (Phase C)

During inference, model weights are frozen and the calibrated threshold τ is applied. The test signal is processed using a sliding window at 100 Hz with window length $T = 200$. Each test signal includes a warm-up suppression period to eliminate false positives caused by system-initialisation transients. The robust hybrid score for each successive window is computed as follows:

1. Compute the per-step reconstruction error using a disturbance mask to suppress known high-variability steps.
2. Apply a moving-average filter to smooth the step-wise error sequence.
3. Compute the quantile reconstruction score as a robust measure of overall recon-

struction quality.

4. Compute the latent deviation as the Euclidean distance between $\mathbf{z}$ and the training mean.

5. Aggregate into the hybrid score S according to Equations (62)–(64).

A window is classified as an attack if two conditions are simultaneously satisfied:

$$S > \tau \quad \text{AND} \quad \text{persistent\_abnormality} = \mathrm{True} \tag{66}$$

The persistence condition requires S to exceed τ for at least K consecutive windows, reducing sensitivity to transient noise. The binary output flag is defined as:

$$\text{flag} = \begin{cases} 1\ (\text{ATTACK}) & \text{if } S > \tau \text{ and persistent} \\ 0\ (\text{NORMAL}) & \text{otherwise} \end{cases} \tag{67}$$

5.4.7 FDI Attack Mitigation (Phase D)

The DA-CGAE framework extends beyond detection to provide an active mitigation capability that reconstructs clean LFC signals corrupted by FDI attacks. Once an attack window is identified during Phase C, the decoder output serves as a surrogate for the clean signal, replacing the corrupted samples in the original time series. Because the encoder is trained exclusively on normal LFC operational data, the latent representation $\mathbf{z}$ encodes only the manifold of healthy system dynamics. When an attacked window is passed through the encoder, the resulting $\mathbf{z}$ is projected onto this healthy manifold, and the decoder reconstructs a signal that approximates what the LFC signals would have been in the absence of the FDI injection. This property makes the decoder output a principled estimate of the clean signal under attack conditions, without requiring any prior knowledge of the attack type, magnitude, or injection timing.

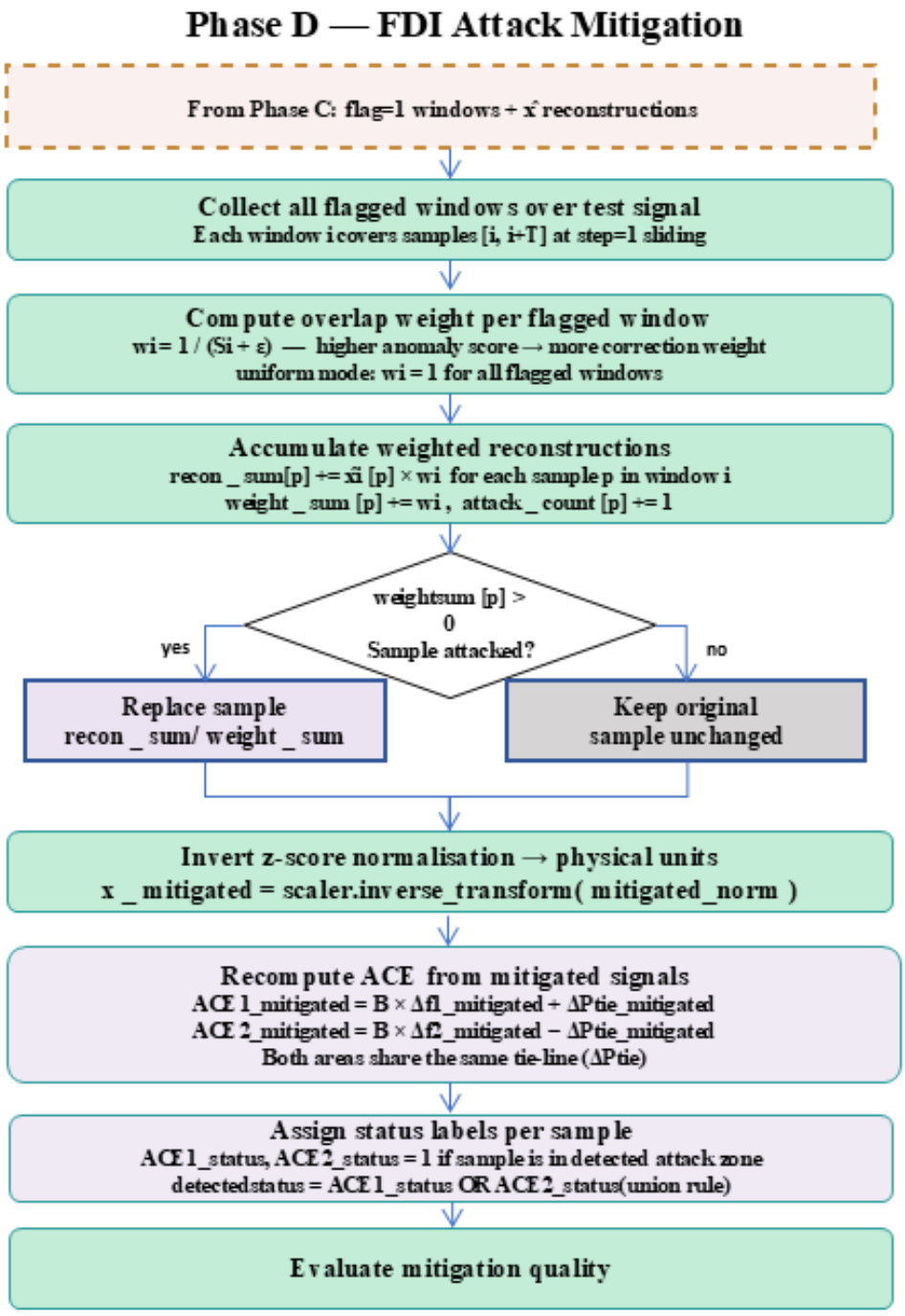


Figure 9. Flowchart of the DA-CGAE FDI Attack Mitigation pipeline (Phase D): sliding-window reconstruction, confidence-weighted overlap aggregation, inverse normalisation, and ACE signal recomputation..

Sliding-Window Reconstruction: The mitigation procedure operates on the full test signal using a sliding window with step size $s = 1$ sample, consistent with the inference procedure in Phase C. Let $\mathbf{X} \in \mathbb{R}^{N \times F}$ denote the normalised test signal, where N is the total number of samples and $F = 3$ is the number of input features (Δf_1, Δf_2, ΔP_{tie}). For window index i, the input window is:

$$\mathbf{x}_i = \mathbf{X}[i \,:\, i+T] \in \mathbb{R}^{T \times F}, \qquad i = 0, 1, \ldots, N_w - 1 \tag{68}$$

where $T = 200$ is the window length and $N_w = N - T + 1$ is the total number of windows. Each window is processed by the encoder to produce latent vector $\mathbf{z}_i$, and the decoder reconstructs the estimated clean signal:

$$\hat{\mathbf{x}}_i = \text{Decoder}(\mathbf{z}_i,\, \mathbf{h}_0) \in \mathbb{R}^{T \times F} \tag{69}$$

where $\mathbf{h}_0 = \tanh(\mathbf{W}_{\text{dec}}\, \mathbf{z}_i + \mathbf{b}_{\text{dec}})$ is the initial hidden state of the GRU decoder, as defined in Equation (57). This reconstruction is computed in the same forward pass used for anomaly scoring, adding no additional computational overhead.

Confidence-Weighted Overlap Aggregation: Since the sliding window operates with step size $s = 1$, consecutive windows overlap significantly. Within an attacked region, up to T windows may cover any given sample. To aggregate reconstruction contributions from all overlapping attack windows, a confidence-weighted averaging scheme is employed.

For each flagged attack window i (i.e., $\text{flag}_i = 1$), a confidence weight is assigned as the inverse of its hybrid anomaly score:

$$w_i = \frac{1}{S_i + \varepsilon} \tag{70}$$

where S_i is the hybrid score defined in Equation (62) and $\varepsilon = 10^{-6}$ prevents division by zero. Windows with higher anomaly scores receive lower reconstruction weight, reflect-

ing greater uncertainty in the decoder's output under severe corruption. The aggregated reconstruction at sample position n is:

$$\hat{x}_n^{\text{agg}} = \frac{\sum_{i \in \mathcal{A}(n)} w_i \cdot \hat{\mathbf{x}}_i[n-i]}{\sum_{i \in \mathcal{A}(n)} w_i} \tag{71}$$

where $\mathcal{A}(n) = \{i : \text{flag}_i = 1,\ i \leq n < i + T\}$ is the set of flagged windows whose coverage includes sample n. The mitigated signal is then constructed as:

$$\tilde{x}_n = \begin{cases} \hat{x}_n^{\text{agg}} & \text{if } \sum_{i \in \mathcal{A}(n)} w_i > 0 \\ x_n & \text{otherwise} \end{cases} \tag{72}$$

Only samples covered by at least one flagged attack window are replaced; all remaining samples retain their original values.

Signal Reconstruction in Physical Units: The mitigation procedure operates in the normalised feature space defined by the z-score transformation applied during preprocessing (Equation (43)). After aggregation, the mitigated signal $\tilde{\mathbf{X}} \in \mathbb{R}^{N_s \times F}$ is inverted back to physical units using the fitted StandardScaler:

$$\tilde{\mathbf{X}}_{\text{phys}} = \tilde{\mathbf{X}} \cdot \boldsymbol{\sigma} + \boldsymbol{\mu} \tag{73}$$

where $\boldsymbol{\mu} \in \mathbb{R}^F$ and $\boldsymbol{\sigma} \in \mathbb{R}^F$ are the per-feature mean and standard deviation vectors estimated on the clean training set.

ACE Signal Recomputation: Following physical-unit reconstruction of Δf_1, Δf_2, and ΔP_{tie}, the Area Control Error signals are recomputed analytically from the mitigated feature signals. The ACE formulas for the two-area LFC system, consistent with Equations (1)–

(2) of Section 3.1, are:

$$\widetilde{\mathrm{ACE}}_1 = B \cdot \widetilde{\Delta f}_1 + \widetilde{\Delta P}_{\text{tie}} \tag{74}$$

$$\widetilde{\mathrm{ACE}}_2 = B \cdot \widetilde{\Delta f}_2 - \widetilde{\Delta P}_{\text{tie}} \tag{75}$$

where $B = 0.432$ p.u./Hz is the frequency bias coefficient of the system (equal to $B_1 = B_2$ in Table 2), $\widetilde{\Delta f}_1$ and $\widetilde{\Delta f}_2$ are the mitigated frequency deviations in Areas 1 and 2 respectively, and $\widetilde{\Delta P}_{\text{tie}}$ is the mitigated tie-line power deviation shared by both areas. The sign convention for $\widetilde{\mathrm{ACE}}_2$ reflects the standard two-area formulation in which the tie-line contribution is subtracted in Area 2, consistent with the area size ratio α_{12} under symmetric area configuration.

Mitigation Quality Metrics: The quality of the mitigation is assessed over the detected attack region using two complementary metrics. Let $\Omega_{\text{atk}} = \{n : \tilde{x}_n \neq x_n\}$ denote the set of sample indices where reconstruction was applied.

The Root Mean Square Error (RMSE) between the mitigated and original signals within the attack zone quantifies the magnitude of the correction applied:

$$\mathrm{RMSE} = \sqrt{\frac{1}{|\Omega_{\text{atk}}|} \sum_{n \in \Omega_{\text{atk}}} \left(\tilde{x}_n^{\text{phys}} - x_n^{\text{phys}}\right)^2} \tag{76}$$

The Pearson correlation coefficient between the mitigated signal in the attack zone and the pre-attack healthy baseline assesses how closely the decoder restores the expected normal operational profile:

$$r_{\text{healthy}} = \frac{\sum_{k=1}^{K} \left(\tilde{x}_k^{\text{phys}} - \bar{\tilde{x}}\right)\left(x_k^{\text{healthy}} - \bar{x}^{\text{healthy}}\right)}{\sqrt{\sum_{k=1}^{K} \left(\tilde{x}_k^{\text{phys}} - \bar{\tilde{x}}\right)^2 \cdot \sum_{k=1}^{K} \left(x_k^{\text{healthy}} - \bar{x}^{\text{healthy}}\right)^2}} \tag{77}$$

where x_k^{healthy} is drawn from the pre-attack healthy segment and $K = \min(|\Omega_{\text{atk}}|,\ |\Omega_{\text{healthy}}|)$. A high r_{healthy} indicates that the reconstructed signal is behaviourally consistent with the

expected normal LFC dynamics. Both metrics are computed separately for Δf_1, Δf_2, ΔP_{tie}, $\widetilde{\text{ACE}}_1$, and $\widetilde{\text{ACE}}_2$.

Integrated Detection and Mitigation Workflow: The mitigation module is tightly coupled with the detection and inference pipeline described in Sections 5.4.5 and 5.4.6. The combined DA-CGAE detection and mitigation workflow proceeds as follows:

1. The test signal is segmented into overlapping windows of length $T = 200$ at step $s = 1$.
2. Each window is passed through the encoder to obtain $\mathbf{z}_i$ and the decoder to obtain $\hat{\mathbf{x}}_i$ simultaneously in a single forward pass.
3. The hybrid anomaly score S_i is computed using Equations (62)–(64).
4. The persistence filter (Section 5.4.6) suppresses transient false alarms.
5. Flagged windows (flag$_i = 1$) trigger the mitigation pipeline: decoder outputs $\hat{\mathbf{x}}_i$ are accumulated with confidence weights w_i at all overlapping sample positions via Equation (71).
6. The aggregated mitigated signal is inverted to physical units via Equation (73), and ACE signals are recomputed from Equations (74)–(75).

This integrated design ensures that detection and mitigation share a single forward pass through the model, adding no additional computational overhead beyond the inference stage. The mitigation therefore satisfies the strict real-time latency requirements of LFC control loops identified in Section 1.3.

5.4.8 Hyperparameter Summary

Table 5 presents a consolidated summary of all key hyperparameters and architectural settings of the DA-CGAE model, including the mitigation-specific parameters introduced in Phase D.

Table 5. DA-CGAE Architectural, Training, and Mitigation Hyperparameters.

Hyperparameter / Setting	**Value**
Architecture	
Input window length	200 samples (5 s at 100 Hz)
Input features (F)	3: Δf_1, Δf_2, ΔP_{tie}
BiGRU hidden size	128 per direction (256 concatenated)
Number of BiGRU layers	2
Latent vector dimension	64
Projection head output	32 (ℓ_2-normalised)
Dropout rate	0.3
Training	
Reconstruction loss weight (α_r)	1.0
Contrastive loss weight (α_c)	0.08
NT-Xent temperature (τ_c)	0.07
Augmentation scaling s	$\mathcal{U}[0.992,\ 1.008]$
Augmentation noise $\boldsymbol{\epsilon}$	$\mathcal{N}(0,\ 0.004)$
Optimiser	AdamW
Batch size	20
Early stopping patience	20 epochs
Detection	
Detection threshold τ	$Q_{0.95}$ of healthy validation scores
Persistence window K	5 consecutive windows
Startup suppression t_{ignore}	15 s
Mitigation	
Overlap weighting mode	Score-based ($w_i = 1\ /\ (S_i + \varepsilon)$)
ACE frequency bias B	0.432 p.u./Hz

6 Methodology

In this study, two related issues in contemporary power systems are addressed to: Optimal tuning of the LFC controller and unsupervised detection of FDI attacks. The overall methodological flow diagram is shown in Figure 10. The methodology is split into two parallel directions: (1) metaheuristic optimization and (2) deep learning-based anomaly detection, running in a shared MATLAB simulation platform.

A two-area multi-source interconnected power system is modeled in MATLAB/Simulink, and each area consists of a reheat thermal unit, a hydraulic unit, and a gas turbine which is subject to governor deadband and generation rate constraint nonlinearities. A hybrid configuration is also built on a 50 MW PV plant (Area 1) and a 70 MW wind generation plant (Area 2), which adds stochastic renewable disturbances. Five signal streams are generated during the simulation, once every 100 seconds and at a 100 Hz sampling rate: frequency deviation in Area 1 (ΔF_1), frequency deviation in Area 2 (ΔF_2), tie-line power deviation (ΔP_{tie}), area control error in Area 1 (ACE_1), and area control error in Area 2 (ACE_2).

The four algorithms used as comparators are PSO, GWO, ABC, and Modified hybrid ABCPSO (MHABCPSO). The proposed algorithm PGWA combines all three algorithms (PSO, GWO, and ABC) in a sequential three-phase per-iteration architecture. For every iteration, Phase 1 implements the velocity-position updates of PSO to search globally, Phase 2 implements the GWO hierarchical update guided by the three best agents (alpha, beta, delta) to exploit the search space in a structured way, and Phase 3 implements an adaptive ABC mechanism that detects convergence stagnation and resets any scout agents if improvement is below a threshold. The ITAE of the closed loop frequency deviation is minimized for all of the five algorithms to optimize the PID controller gains. The performance is first validated on nine classical benchmark functions that cover unimodal and multimodal landscapes, and then tested for five LFC simulation cases with increasing complexity, such as step load perturbations, random multi-step disturbances, asymmetric dual-area load-

ing, renewable energy integration, and communication time delay. The results are also compared with the TID-IC and ID-T controllers reported in the literature. Normal LFC op-

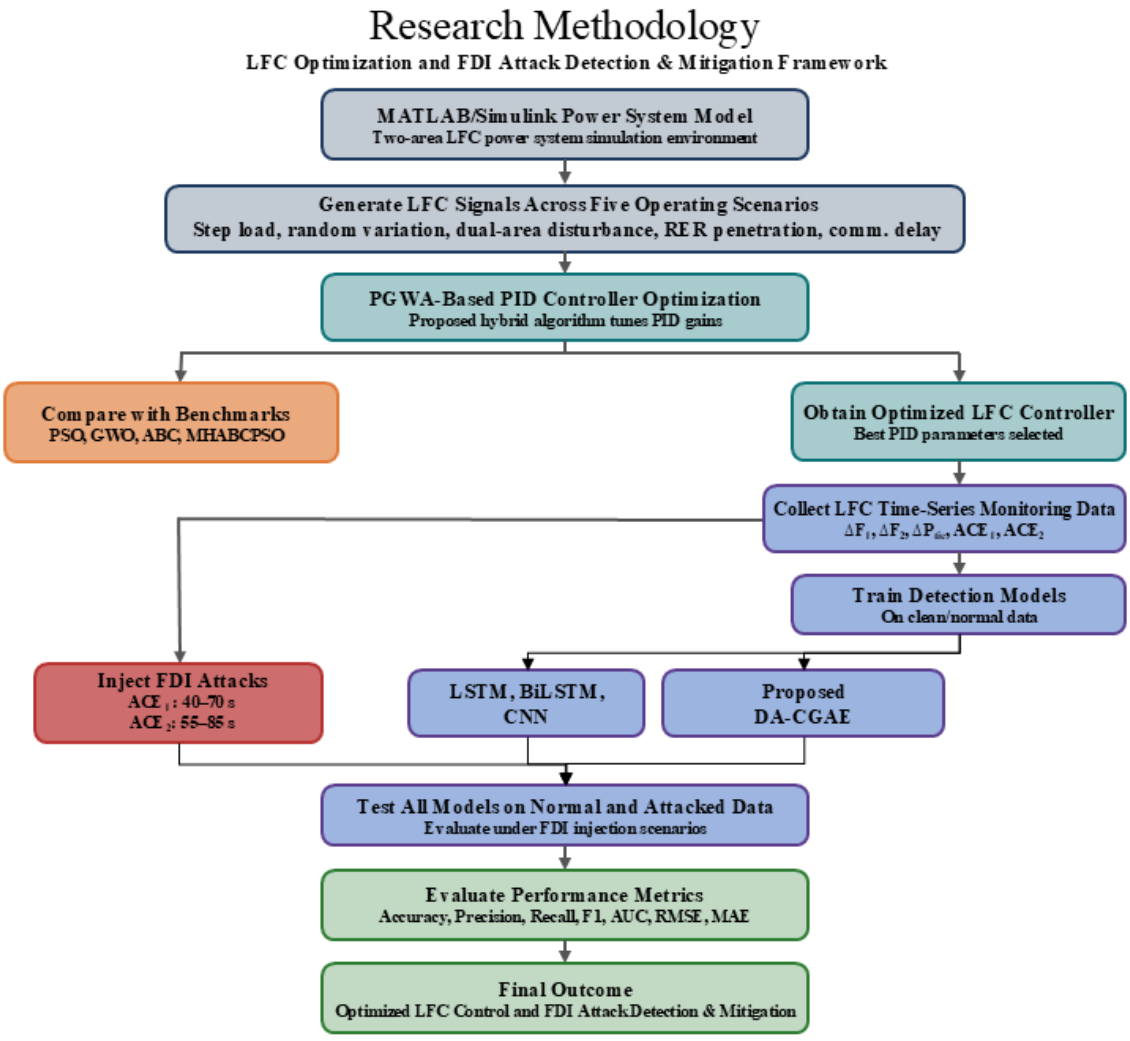


Figure 10. Methodological flow diagram for PGWA-based LFC controller optimization and DA–CGAE-based FDI attack detection..

erational data collected from the MATLAB simulation under the PGWA-tuned controller with no attacks present is used to train three supervised baseline deep learning models (LSTM, BiLSTM, CNN) and the proposed unsupervised DA-CGAE framework. The test data set is then created by injecting FDI attacks into the simulation: an asymmetric multi-point injection with overlapping attack windows and frequency propagation in different areas between the two attacks occurs starting from $t = 40$ s until $t = 70$ s for ACE_1 and from $t = 55$ s until $t = 85$ s for ACE_2. The DA-CGAE is only trained on normal data, with a BiGRU encoder that employs feature and temporal attention, a disturbance-aware GRU

decoder, and a contrastive projection head with an NT-Xent loss. Detection is performed with a hybrid anomaly score based on the reconstruction error and latent deviation, and the threshold is set to the 95th percentile of healthy validation scores. All four models are tested on the same attacked test set and assessed based on accuracy, precision, recall, F1 score, AUC, and per-signal RMSE and MAE.

7 Results and Discussion

7.1 Benchmark Function Analysis

For the purpose of proving the capability of optimization of the proposed PGWA algorithm, the following classical benchmark functions were used. These functions were chosen to span various optimization challenges such as unimodal, multimodal, separable, non-separable, low-dimensional, and high-dimensional search spaces. Thus, they can serve as a benchmark to assess the convergence stability, exploitation accuracy, and exploration capability of the compared metaheuristic algorithms. The values of the benchmark functions and preliminary result values in this section are those obtained on the benchmark-function result sheet prepared for this study.

All metaheuristic algorithms compared in this study were evaluated under identical experimental conditions to ensure a fair comparison. Each algorithm was executed with a population size of 100 particles and a maximum of 10,000 iterations. These parameter settings were applied uniformly across all nine benchmark functions and all five compared algorithms, so that the performance differences observed in Table 7 reflect solely the algorithmic behaviour of each method rather than any disparity in computational budget.

The results of the benchmark-function in Table 7 demonstrate that the proposed PGWA algorithm gives the best overall optimized results when compared to the other algorithms. PGWA has achieved the global optimum value of 0 for all nine test functions on both low-dimensional and high-dimensional benchmark landscapes, showing strong convergence accuracy. The result verifies that the hybrid structure of PGWA is effective not only for simple unimodal functions like Sphere and Schwefel 2.22, but also more difficult multimodal and non-separable functions like Ackley, Levy, Rastrigin and Rosenbrock.

It is because PGWA has a three-stage hybrid search mechanism, which makes it superior

Table 6. Classical Benchmark Test Functions.

Function	Name	Equation	Range	Dim	Opt.
F1	Ackley	$f(\mathbf{x}) = -20\exp\left(-0.2\sqrt{\frac{1}{d}\sum_{i=1}^{d} x_i^2}\right) - \exp\left(\frac{1}{d}\sum_{i=1}^{d}\cos(2\pi x_i)\right) + 20 + e$	$[-32,\ 32]$	30	0
F2	Alpine	$f(\mathbf{x}) = \sum_{i=1}^{d} \lvert x_i \sin(x_i) + 0.1x_i \rvert$	$[-10,\ 10]$	30	0
F5	Bohachevsky 1	$f(\mathbf{x}) = x_1^2 + 2x_2^2 - 0.3\cos(3\pi x_1) - 0.4\cos(4\pi x_2) + 0.7$	$[-100,\ 100]$	2	0
F19	Leon	$f(\mathbf{x}) = 100(x_2 - x_1^3)^2 + (1 - x_1)^2$	$[-1.2,\ 1.2]$	2	0
F20	Levy	$f(\mathbf{x}) = \sin^2(\pi w_1) + \sum_{i=1}^{d-1}(w_i - 1)^2\left[1 + 10\sin^2(\pi w_{i+1})\right] + (w_d - 1)^2\left[1 + \sin^2(2\pi w_d)\right], \quad w_i = 1 + \frac{x_i - 1}{4}$	$[-10,\ 10]$	20	0
F24	Rastrigin	$f(\mathbf{x}) = 10d + \sum_{i=1}^{d}\left[x_i^2 - 10\cos(2\pi x_i)\right]$	$[-5.12,\ 5.12]$	30	0
F25	Rosenbrock	$f(\mathbf{x}) = \sum_{i=1}^{d-1}\left[100\left(x_{i+1} - x_i^2\right)^2 + (1 - x_i)^2\right]$	$[-30,\ 30]$	30	0
F27	Schwefel 2.22	$f(\mathbf{x}) = \sum_{i=1}^{d} \lvert x_i \rvert + \prod_{i=1}^{d} \lvert x_i \rvert$	$[-10,\ 10]$	30	0
F30	Sphere	$f(\mathbf{x}) = \sum_{i=1}^{d} x_i^2$	$[-100,\ 100]$	30	0

Table 7. Performance of Metaheuristic Algorithms on Classical Benchmark Functions.

Function	PGWA	MHABCPSO	ABC	PSO	GWO
F1	**0**	1.4983×10^{-16}	1.0250×10^{-4}	7.9936×10^{-15}	4.4409×10^{-15}
F2	**0**	2.667×10^{-16}	2.2970×10^{-3}	2.5535×10^{-15}	8.8818×10^{-15}
F5	**0**	1.0294×10^{-16}	1.1658×10^{-4}	3.5527×10^{-15}	5.3291×10^{-15}
F19	**0**	9.385×10^{-16}	2.6510×10^{-5}	0	5.4658×10^{-10}
F20	**0**	1.001×10^{-32}	4.0554×10^{-5}	1.3498×10^{-31}	9.4335×10^{-11}
F24	**0**	5.147×10^{-15}	1.3694	20.8941	0
F25	**0**	7.614×10^{-4}	2.1995	10.4636	25.3030
F27	**0**	2.331×10^{-62}	2.4100×10^{-4}	6.0742×10^{-61}	8.8818×10^{-16}
F30	**0**	4.069×10^{-117}	6.6890×10^{-8}	2.4611×10^{-116}	0

in performance. In the first phase, the PSO part gets the learner closer to the best areas of the search space, using personal-best and global-best learning. This enables PGWA to speed up the convergence process in the initial search efforts. However, one disadvantage of standalone PSO is the potential for early convergence to one global best solution, which can be a local optimum in high-dimensional functions. It is observed that this weakness is present in the results obtained by PSO for the functions F24 and F25, particularly on the Rastrigin and Rosenbrock functions.

The second phase of PGWA is the GWO hierarchical update, in which the population is led by the three best solutions: alpha, beta, and delta. In this multi-leader mechanism, the search agents are not only guided by one solution as in standard PSO, so that the improvement in exploitation is achieved. However, stand-alone GWO has its drawbacks. The probability of finding the alpha, beta, and delta wolves near the true global optimum decreases with the number of dimensions. The rest of the population follows these leaders, and the algorithm may become less diverse once these leaders gather around a local area. This is why GWO, despite reaching the global optimum on simpler functions such as Rastrigin and Sphere, struggles significantly on the Rosenbrock function, recording the largest error among all compared methods.

The adaptive ABC mechanism is the third and most crucial step in PGWA. The ABC scout mechanism is only used when the convergence improvement is no longer adequate, unlike standard ABC, which is mostly based on random neighbourhood search. If stagnation is found, the ratio of scouts is raised, and the poorest agents are reinitialized or perturbed to re-diversify the population. This ensures that the algorithm will not burn up computational time during productive convergence and will not get stuck in local optima when the search stagnates. PGWA design is thus a combination of PSO fast convergence, GWO multi-leader exploitation, and ABC stagnation-recovery capability in a single sequential framework.

The results also demonstrate that MHABCPSO is the second-best algorithm in the comparison. This is expected since MHABCPSO is a fusion of the exploration capability of ABC

and the quick social learning mechanism of PSO. Consequently, it is superior to the single ABC, PSO and GWO algorithms on most test functions. However, MHABCPSO still does not have a hierarchical exploitation mechanism like GWO. Thus, while it may be able to get very close to the global optimum, it is not always able to find the actual optimum, unlike PGWA.

As the dimensionality of the benchmark functions grows, the drawbacks of the single algorithms become more apparent. The size of the search space grows exponentially in 30-dimensional functions, which makes it more difficult to maintain a good balance between exploration and exploitation in a single search strategy. ABC is penalised since the neighbourhood search is not very directional and has a high percentage of random search. PSO suffers because particle diversity can deteriorate rapidly around the global best solution found so far. GWO addresses this problem with three leaders, but does not have an active recovery mechanism when the population is stagnant. Such restrictions are particularly relevant for multimodal functions, which can have many local minima to confuse the search process.

In general, the performance of PGWA is the most reliable and accurate across all benchmark functions, as it does not rely on a single optimization behaviour. Rather, it relies on PSO for rapid global movement, GWO for structured leader-based refinement, and adaptive ABC for diversity restoration in stagnation. This balance mechanism is the reason PGWA shows the best results across all benchmark functions and outperforms MHABCPSO, ABC, PSO, and GWO. The benchmark results thus justify the use of PGWA as a powerful optimization tool prior to its application in the more challenging PID parameter tuning problem in load frequency control.

7.2 Performance Evaluation of Metaheuristic Algorithms in Load Frequency Control

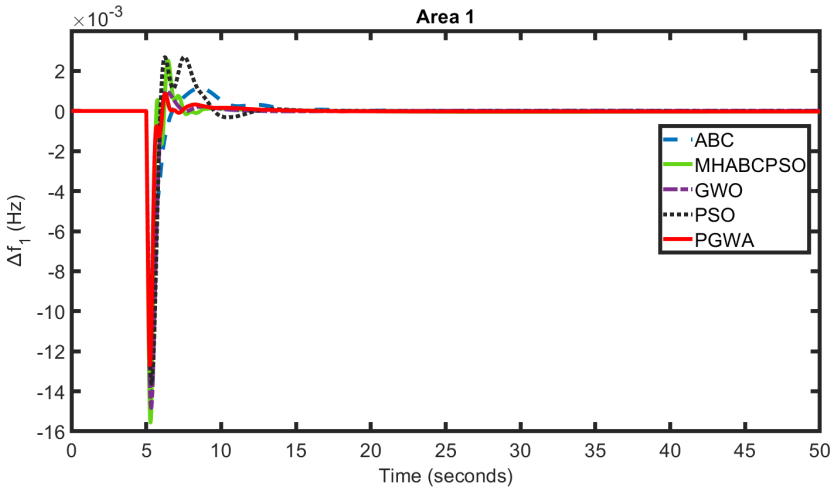
In this subsection, a detailed comparative assessment of five metaheuristic optimization algorithms, PGWA, Modified Hybrid ABCPSO (MHABCPSO), ABC, PSO, and GWO, is conducted. These algorithms are used to tune the parameters of LFC applied to a two-area interconnected power system. The results are further benchmarked against two controllers reported in the extant literature: the Tilted Integral Derivative Intelligent Controller (TID-IC) proposed in Tavakoli et al. (2024), and the Integral Derivative-Tilted (ID-T) controller proposed in M. Ahmed et al. (2022b). Performance is measured in terms of the integral error criteria ITAE, ITSE, and IAE, maximum frequency and power deviations, and settling times of both areas and the inter-area tie-line.

7.2.1 Case 1: 1% Step Load Perturbation (SLP) in Area 1

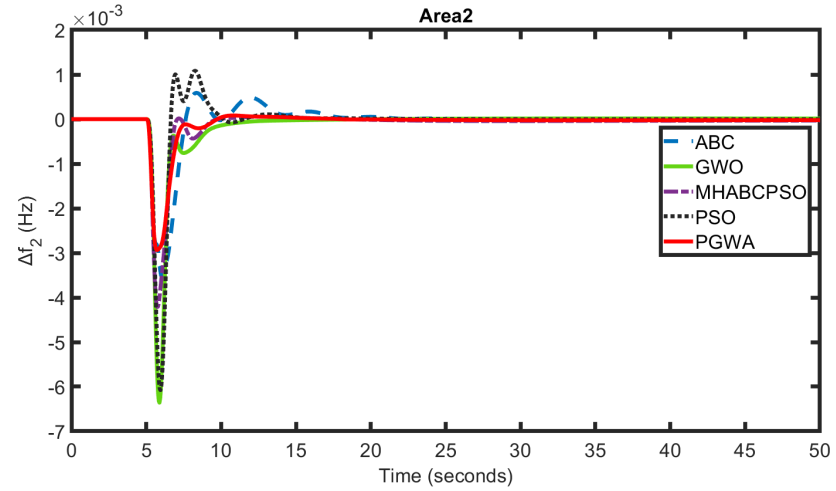
In order to provide a baseline, a 1% step load perturbation was introduced to Area 1 but not Area 2, a common benchmark in LFC literature to assess the initial controller responsiveness and oscillation damping.

The controller optimized by PGWA achieved the lowest ITAE (0.2019) and ITSE (0.00016), as shown in Table 8 and Figure 11. The peak frequency deviation in Area 1 ($\Delta f_1 = 0.0127$ Hz) was the smallest recorded, followed by $\Delta f_2 = 0.0029$ Hz and $\Delta P_{\text{tie}} = 0.0010$ pu MW. The settling times of Δf_1, Δf_2, and ΔP_{tie} were 8.6841 s, 9.1474 s and 10.3090 s, respectively always the fastest of all the algorithms. These values also considerably undermine the reported settling times of the TID-IC controller Tavakoli et al. (2024) and the ID-T controller M. Ahmed et al. (2022b), which were reported to have settling times of 10–12 s and frequency deviations greater than 0.020 Hz.

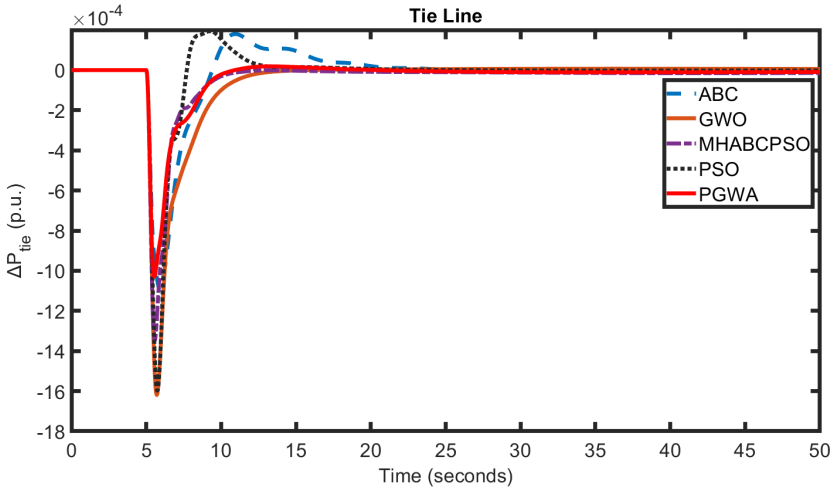
MHABCPSO was second with ITAE $= 0.2574$ and ITSE $= 0.0002$, significantly better than all standalone methods. Its settling times (9.7592 s, 11.2133 s, 11.0223 s) and peak de-



(a) Area 1.



(b) Area 2.



(c) Tie-line.

Figure 11. Frequency deviation with 1% SLP in (a) Area 1, (b) Area 2, and (c) Tie-line..

viations ($\Delta f_1 = 0.0156$ Hz, $\Delta f_2 = 0.0042$ Hz) were clearly superior to those of ABC, PSO, and GWO, confirming the benefit of its hybrid search architecture. GWO, PSO, and ABC returned higher ITAE values of 0.3111, 0.3431, and 0.3872 respectively. The performance of all proposed algorithms was significantly higher than that of TID-IC Tavakoli et al. (2024) and ID-T M. Ahmed et al. (2022b), proving the efficiency of the metaheuristic tuning method.

Table 8. Comparative analysis of ITAE, peak response, and settling time for 1% SLP in Area 1..

Metric		PGWA	MHABCPSO	ABC	PSO	GWO	TID-IC Tavakoli et al. (2024)	ID-T M. Ahmed et al. (2022b)
ITAE		**0.2019**	0.2574	0.3872	0.3431	0.3111	—	—
ITSE		**0.00016**	0.0002	0.0003	0.0004	0.0006	0.0010	0.001
IAE		0.1198	0.1528	0.2298	0.2035	0.1847	—	—
Settling Time (s)	Δf_1	**8.6841**	9.7592	13.4138	9.9759	9.0815	10	11
	Δf_2	**9.1474**	11.2133	17.3727	12.2233	12.1906	11	12
	ΔP_{tie}	**10.3090**	11.0223	19.8192	12.1254	11.6245	12	11
Max. freq. deviation (Hz)	Δf_1	**0.0127**	0.0156	0.0132	0.0136	0.0148	0.029	0.028
	Δf_2	**0.0029**	0.0042	0.0035	0.0061	0.0064	0.020	0.024
Max. power deviation (pu MW)	ΔP_{tie}	**0.0010**	0.0013	0.0011	0.0016	0.0016	0.004	0.004

7.2.2 Case 2: Multiple/Random Step Load Perturbations in Area 1

The performance of the controllers under sustained and unpredictable demand variation, more akin to real power system operation, was evaluated by applying a sequence of random step load perturbations to Area 1 during a 300-second simulation.

As Table 9 and Figure 13 demonstrate, PGWA achieved the best values across all metrics: ITAE $= 13.87$, ITSE $= 0.0844$, and IAE $= 0.1338$. The earliest settling times were recorded at each segment Δf_1, Δf_2 and ΔP_{tie} settled at 8.9492 s, 7.7965 s and 14.7584 s respectively in the first interval, and this pattern of rapid stabilization was consistently repeated in all subsequent intervals up to 300 s, confirming the strength of PGWA to withstand time-varying loading without loss of performance. The step load pattern applied in this case is illustrated in Figure 12.

MHABCPSO followed as the second-best, with ITAE $= 17.58$, ITSE $= 0.169$, and IAE $= 0.1826$. Its interval settling behaviour was more stable than ABC, GWO, and PSO, indicating the ability of the hybrid optimizer to navigate multi-modal search spaces effectively. The frequency response plots confirm that, at each perturbation event, the PGWA con-

troller returns the system frequency closest to the zero-deviation baseline.

Table 9. Comparative analysis of ITAE, peak response, and settling time for random SLP in Area 1..

Algorithm	ITAE	ITSE	IAE	Signal	0–50 s	50–100 s	100–150 s	150–200 s	200–250 s	250–300 s
				Δf_1	**8.9492**	**53.9703**	**103.8908**	**152.4278**	**201.4061**	**251.4069**
PGWA	**13.87**	**0.0844**	**0.1338**	Δf_2	**7.7965**	**52.7915**	**102.7749**	**151.3391**	**201.4711**	**252.5446**
				ΔP_{tie}	**14.7584**	**60.3201**	**110.0721**	**155.2515**	**203.3105**	**253.3343**
				Δf_1	10.1408	55.1517	105.1519	153.2302	203.2245	253.2217
MHABCPSO	17.58	0.169	0.1826	Δf_2	13.3128	58.3777	108.3600	152.2724	202.2773	252.2809
				ΔP_{tie}	16.8826	61.9545	111.9369	153.4771	203.4830	253.4852
				Δf_1	9.3231	54.3693	104.5432	152.9619	202.9496	252.9474
ABC	17.55	0.111	0.1818	Δf_2	8.1820	53.1890	103.9144	152.6154	202.5809	253.5731
				ΔP_{tie}	16.1583	61.5128	111.7811	157.8871	207.2327	254.0668
				Δf_1	9.2552	54.2833	104.2655	152.6667	202.6692	252.6663
PSO	15.4	0.1254	0.1593	Δf_2	8.1401	53.1635	104.1459	152.7323	202.7462	253.7480
				ΔP_{tie}	15.7394	61.0450	110.8792	156.6658	206.7325	253.7586
				Δf_1	9.6245	54.7148	104.6746	152.6389	202.6351	252.6373
GWO	16.3	0.1616	0.1688	Δf_2	12.9839	58.2719	108.1684	152.1938	202.2286	253.2315
				ΔP_{tie}	13.7320	61.8192	111.1319	156.4920	206.5745	253.6585

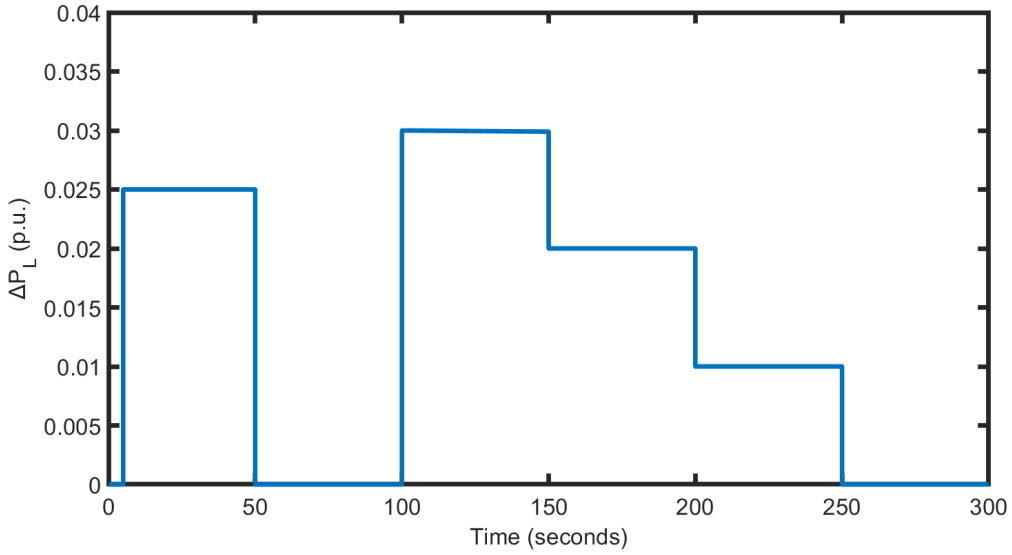
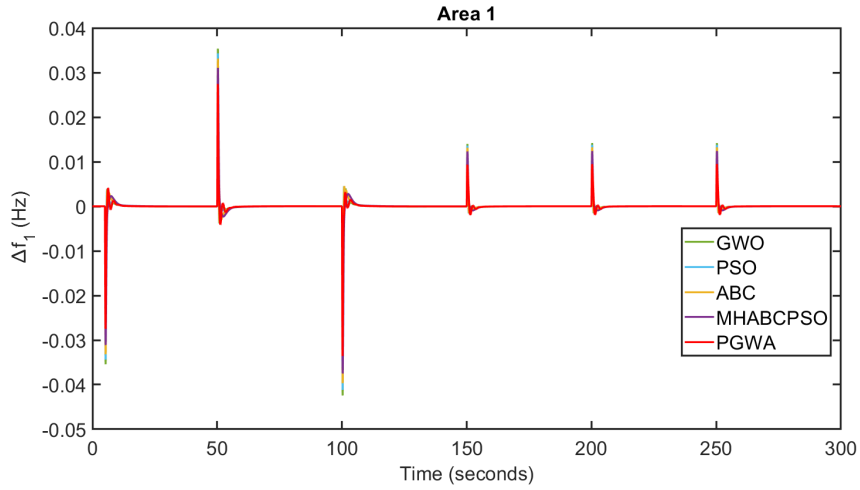
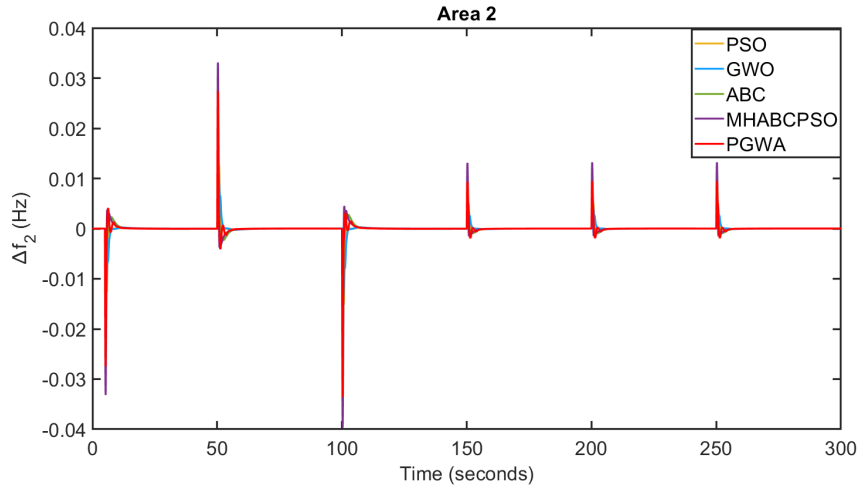


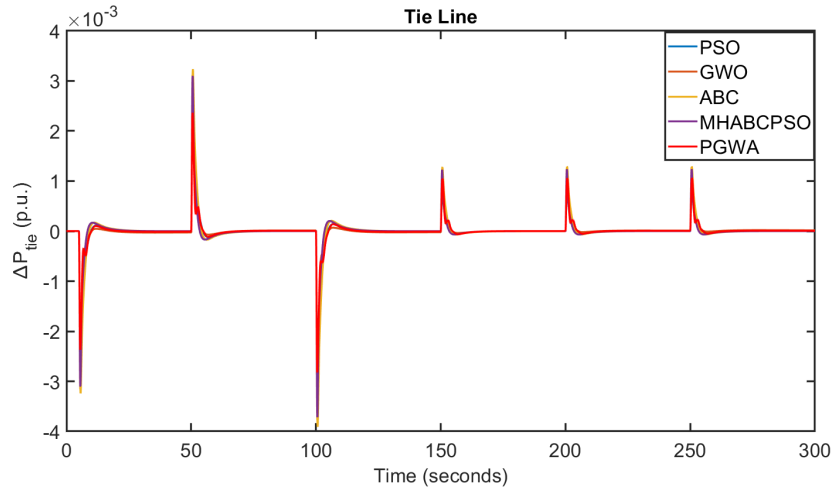
Figure 12. Step load pattern for Case 2..



(a) Area 1.



(b) Area 2.



(c) Tie-line.

Figure 13. Frequency deviation with random (multiple) SLP in (a) Area 1, (b) Area 2, and (c) Tie-line..

7.2.3 Case 3: Asymmetric Dual-Area Disturbance 1% SLP in Area 1 and 5% SLP in Area 2

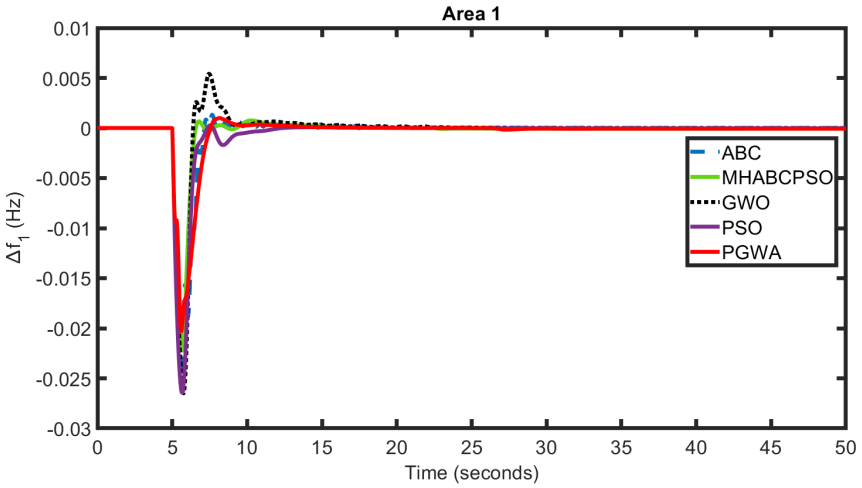
To investigate the ability of each controller to coordinate inter-area responses in the presence of asymmetric loading conditions, this case introduces simultaneous yet unequal disturbances 1% in Area 1 and a significantly larger 5% in Area 2 to examine each controller's inter-area coordination capability.

Table 10 and Figure 14 confirm the further superiority of PGWA, providing ITAE $= 0.5663$, ITSE $= 0.00907$, and IAE $= 0.0851$ are the lowest possible values. Although Area 2 had a larger disturbance, the maximum deviations of Δf_2 and Δf_1 were 0.0601 Hz and 0.0214 Hz respectively, the smallest observed. Settling times of 9.7056 s (Δf_1), 9.4850 s (Δf_2) and 11.8374 s (ΔP_{tie}), together with a tie-line power deviation of only 0.0041 pu MW, further underline the superior inter-area regulation performance of PGWA.

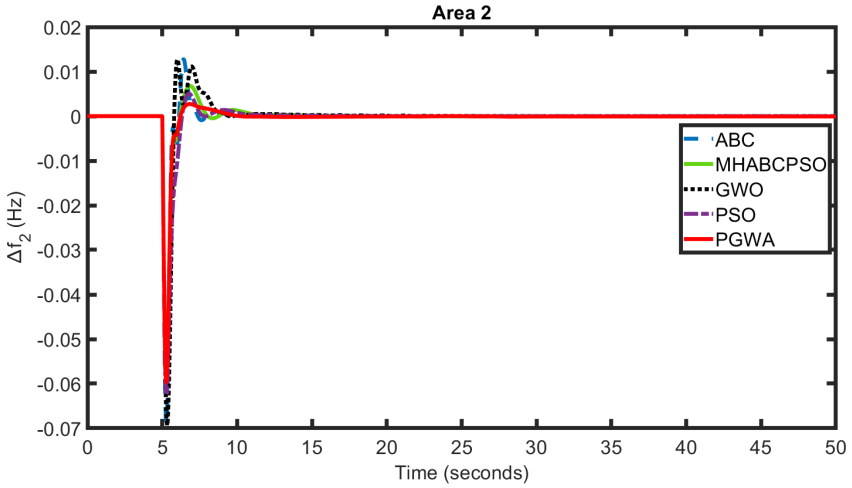
MHABCPSO ranked second with ITAE $= 0.6425$ and ITSE $= 0.01294$. The relatively high ITSE indicates high instantaneous error at the transient stage, and the ΔP_{tie} settling time of 14.4882 s indicates slower tie-line recovery under the asymmetric condition. GWO was worst off in this case with ITAE $= 1.433$ almost 2.5 times that of PGWA, confirming that it is not well suited to strongly coupled, one-sided control problems.

Table 10. Comparative analysis of 1% SLP in Area 1 and 5% SLP in Area 2..

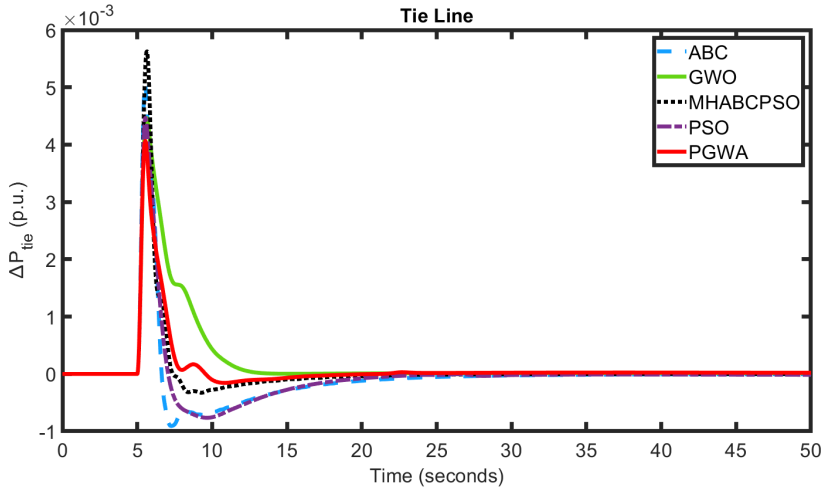
Metric		PGWA	MHABCPSO	ABC	PSO	GWO
ITAE		**0.5663**	0.6425	0.6587	0.6887	1.433
ITSE		**0.00907**	0.01294	0.00984	0.0098	0.007
IAE		**0.0851**	0.09369	0.0962	0.1014	0.2115
Settling Time (s)	Δf_1	**9.7056**	12.4676	10.1166	11.8132	11.3929
	Δf_2	**9.4850**	9.5458	9.5794	10.1990	10.1102
	ΔP_{tie}	**11.8374**	14.4882	19.4786	20.8934	14.4579
Max. freq. deviation (Hz)	Δf_1	**0.0214**	0.0235	0.0265	0.0264	0.0265
	Δf_2	**0.0601**	0.0673	0.0694	0.0626	0.0694
Max. power deviation (pu MW)	ΔP_{tie}	**0.0041**	0.0056	0.005	0.0045	0.0046



(a) Area 1.



(b) Area 2.



(c) Tie-line.

Figure 14. Frequency deviation with dual SLP in (a) Area 1, (b) Area 2, and (c) Tie-line..

7.2.4 Case 4: Multi-Step Load Disturbances with Wind and Solar Energy Penetration

Scenario four couples recurring multi-step load disturbances with the integration of a 50 MW photovoltaic (PV) system (connected after 250 s) and a 70 MW wind farm (connected after 100 s), reflecting the growing challenge of frequency regulation in grids with high and intermittent renewable penetration.

As shown in Table 11 and Figure 16, PGWA recorded the best performance across all indices: ITAE $= 24.72$, ITSE $= 0.0958$, and IAE $= 0.1364$. The step load pattern for this case is presented in Figure 15. Its settling times of 105.0696 s (Δf_1), 106.2414 s (Δf_2), and 108.4226 s (ΔP_{tie}) were competitive with and in several metrics superior to the TID-IC controller Tavakoli et al. (2024) (107 s, 108 s, 109 s) and better than the ID-T controller M. Ahmed et al. (2022b) (110 s for all three). More notably, PGWA's maximum frequency deviations (0.0389 Hz and 0.0162 Hz for Δf_1 and Δf_2) were dramatically lower than TID-IC's reported value of 0.051 Hz, and its tie-line deviation of 0.004 pu MW represented a more than five-fold reduction compared to TID-IC's 0.023 pu MW is a remarkable improvement given the added complexity of renewable intermittency.

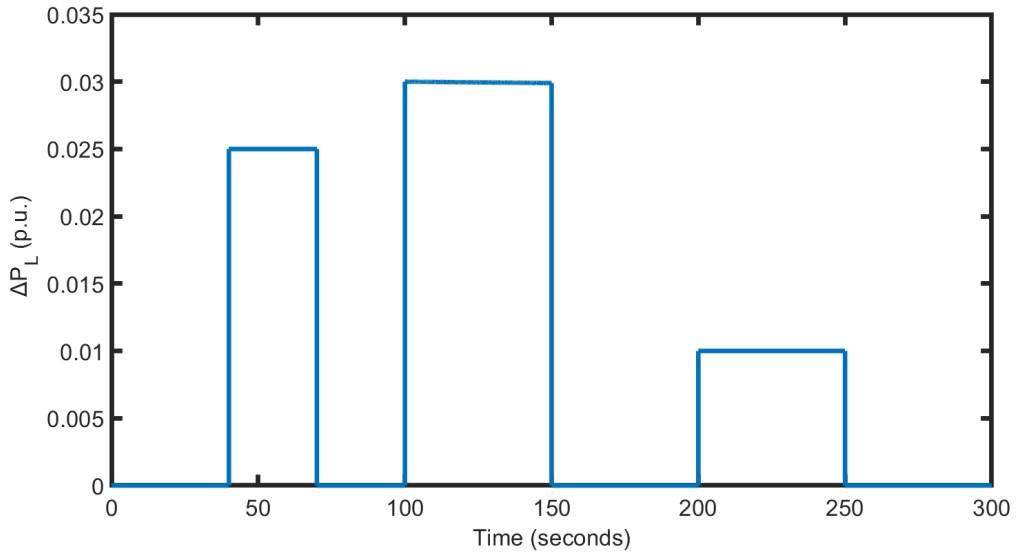
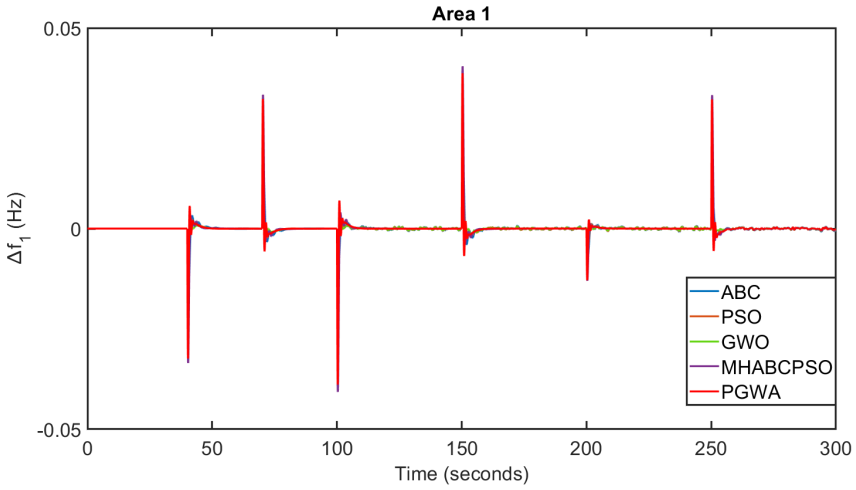
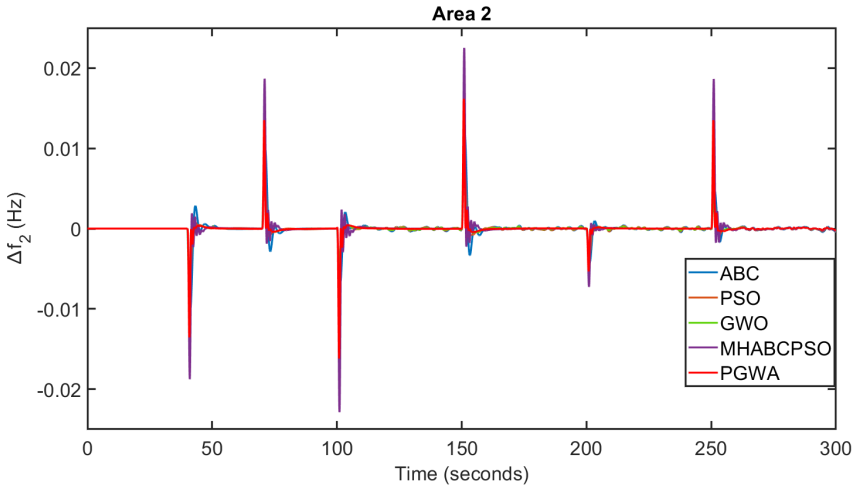


Figure 15. Step load pattern for Case 4..

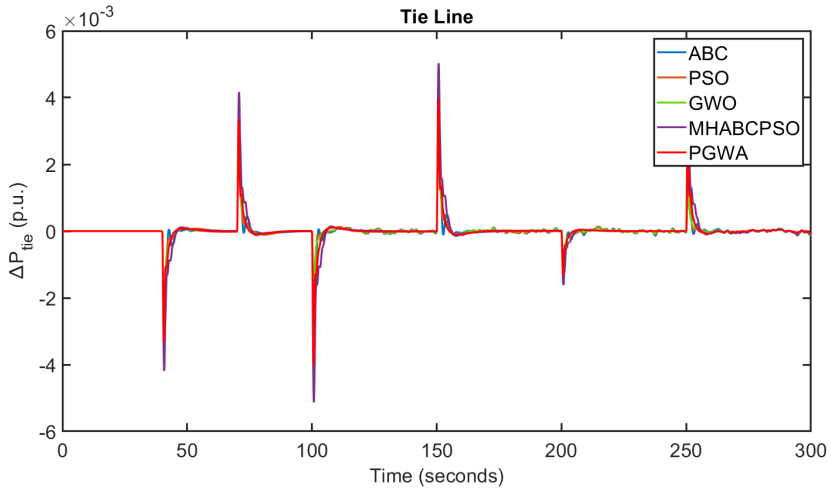
MHABCPSO again placed second, with ITAE $= 32.98$, ITSE $= 0.1687$, and IAE $= 0.2221$. Its



(a) Area 1.



(b) Area 2.



(c) Tie-line.

Figure 16. Frequency deviation with multi-step SLP and renewable integration in (a) Area 1, (b) Area 2, and (c) Tie-line..

settling times (105.1345 s, 106.409 s, 109.5541 s) were remarkably close to PGWA, confirming the hybrid optimizer's resilience in stochastic renewable environments. ABC, GWO, and PSO settled between 124 and 149 s with substantially larger ITAE values, highlighting that single-population methods are ill-suited to the compounded dynamics of renewable-integrated power systems.

Table 11. Comparative analysis of ITAE, peak response, and settling time for multi-step load disturbances with renewable energy penetration..

Metric		PGWA	MHABCPSO	ABC	GWO	PSO	TID-IC Tavakoli et al. (2024)	ID-T M. Ahmed et al. (2022b)
ITAE		**24.72**	32.98	34.75	40.74	41.46	—	—
ITSE		**0.0958**	0.1687	0.212	0.2103	0.2377	—	—
IAE		**0.1364**	0.2221	0.2792	0.3016	0.2858	—	—
Settling Time (s)	Δf_1	**105.0696**	105.1345	124.8721	149.0781	142.6251	107	110
	Δf_2	**106.2414**	106.409	143.0136	148.8574	148.734	108	110
	ΔP_{tie}	**108.4226**	109.5541	141.9703	148.4149	148.3372	109	110
Max. freq. deviation (Hz)	Δf_1	**0.0389**	0.0407	0.0372	0.0375	0.0369	0.051	0.05
	Δf_2	**0.0162**	0.0229	0.015	0.0152	0.0159	0.051	0.05
Max. power deviation (pu MW)	ΔP_{tie}	**0.004**	0.0051	0.0039	0.0038	0.0038	0.023	0.02

7.2.5 Case 5: Communication Time Delay with Renewable Integration and Sequential Multi-Area Disturbances

The most demanding scenario simultaneously incorporates a 0.1 s communication time delay (CTD) in the controller feedback path, PV integration after 80 s, wind turbine connection after 220 s, and independently timed step load disturbances (0.01 pu in Area 1 at 10 s; 0.05 pu in Area 2 at 150 s). This compound test evaluates delay robustness and overall controller resilience under near-practical deployment conditions.

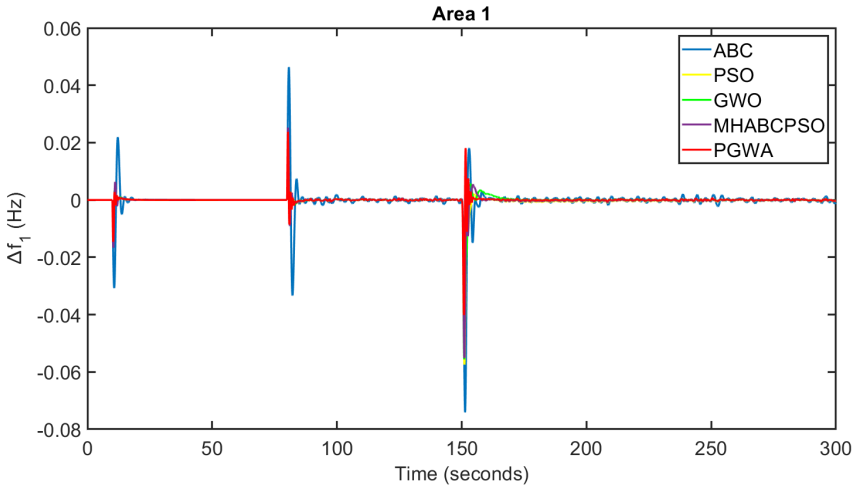
Table 12 and Figure 17 confirm that PGWA delivered the most resilient performance. Its ITAE $(= 31.47)$, ITSE $(= 0.7915)$, and IAE $(= 0.2259)$ were the lowest among all algorithms by a considerable margin. Peak frequency deviations of 0.0402 Hz (Δf_1) and 0.0937 Hz (Δf_2) were substantially below the values reported for TID-IC Tavakoli et al. (2024) (0.14 Hz and 0.13 Hz) and ID-T M. Ahmed et al. (2022b) (0.13 Hz and 0.12 Hz). The tie-line deviation of 0.0101 pu MW was approximately 40% lower than TID-IC's 0.017 pu MW and 50% lower than ID-T's 0.02 pu MW. Settling times of 154.6206 s (Δf_1), 153.3069 s (Δf_2), and 158.4557 s (ΔP_{tie}) were the fastest recorded and closely aligned with TID-IC benchmarks while outperforming ID-T across the board.

MHABCPSO was the strongest runner-up, posting ITAE $= 52.4$, ITSE $= 1.247$, and IAE $= 0.3618$ far better than GWO (53.55), PSO (61.17), and especially ABC (102.3), whose ITAE exceeded PGWA's by more than a factor of three. MHABCPSO's settling times (157.0471 s, 155.622 s, 158.5568 s) were the second-fastest, and its Area 1 deviation of 0.0552 Hz, though above PGWA, remained well within acceptable bounds relative to both TID-IC and ID-T benchmarks.

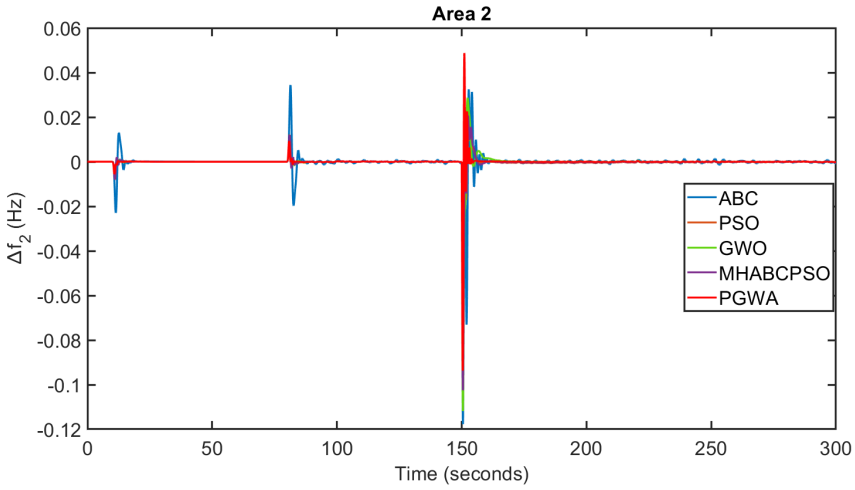
Table 12. Comparative analysis of ITAE, peak response, and settling time under CTD $= 0.1$ s, renewable integration, and sequential multi-area disturbances..

Metric		PGWA	MHABCPSO	GWO	ABC	PSO	TID-IC Tavakoli et al. (2024)	ID-T M. Ahmed et al. (2022b)
ITAE		**31.47**	52.4	53.55	102.3	61.17	—	—
ITSE		**0.7915**	1.247	1.545	2.672	1.445	—	—
IAE		**0.2259**	0.3618	0.3703	0.7961	0.4041	—	—
Settling Time (s)	Δf_1	**154.6206**	157.0471	163.0029	199.0709	155.7308	158	160
	Δf_2	**153.3069**	155.622	158.3597	158.9348	155.7644	158	160
	ΔP_{tie}	**158.4557**	158.5568	166.2196	160.5839	160.406	159	160
Max. freq. deviation (Hz)	Δf_1	**0.0402**	0.0552	0.0556	0.0741	0.0574	0.14	0.13
	Δf_2	**0.0937**	0.1025	0.1118	0.1177	0.1063	0.13	0.12
Max. power deviation (pu MW)	ΔP_{tie}	**0.0101**	0.0134	0.0145	0.0158	0.0144	0.017	0.02

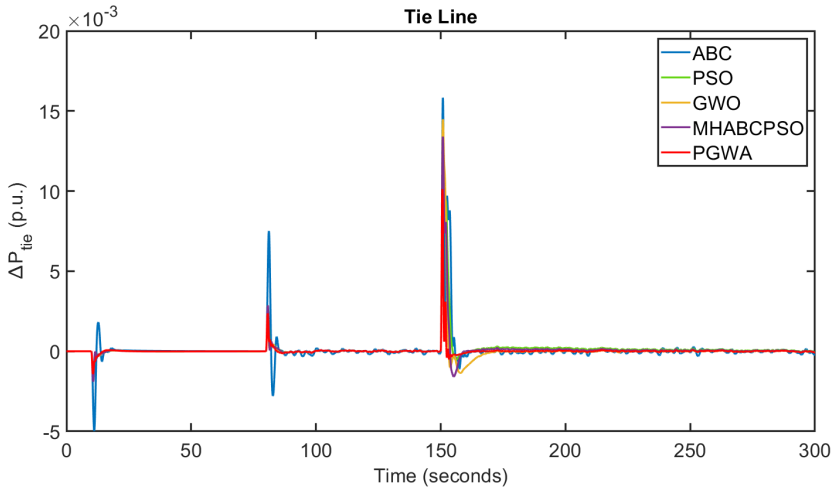
In all five test cases, the best LFC performance was consistently delivered by PGWA, which achieved the lowest integral error indices, the smallest frequency and power deviations, and the shortest settling times. MHABCPSO was a reliable second-best in all cases, and its hybrid search strategy allowed it to perform significantly better than the standalone ABC, PSO, and GWO algorithms, a performance gap that increased markedly as scenario complexity grew under conditions of renewable penetration and communication time delay. The TID-IC Tavakoli et al. (2024) and ID-T M. Ahmed et al. (2022b) controllers are advanced fractional-order control structures which have demonstrated competitive performance in the existing LFC literature. However, when compared to the metaheuristic-optimized controllers in the current study, both were consistently outperformed, especially in Cases 4 and 5, which model the current conditions of grids with renewable sources and realistic communication constraints. In all conditions, the combination of an excellent optimization algorithm with a well-organized controller is essential to robust LFC in the contemporary power system with renewable energy integration.



(a) Area 1.



(b) Area 2.



(c) Tie-line.

Figure 17. Frequency deviation with CTD $= 0.1$ s, renewable energy integration, and sequential multi-area step load disturbances in (a) Area 1, (b) Area 2, and (c) Tie-line..

7.3 FDI Attack Detection and Mitigation in Load Frequency Control

The proposed DA-CGAE model was tested on the dataset generated by a two-area Load Frequency Control (LFC) simulation model with False Data Injection (FDI) attacks. There are 58,859 samples collected during a 100-second simulation period, with the FDI attack injected from $t = 40$ s to $t = 85$ s. The proposed model's performance is evaluated in two aspects: attack detection and signal mitigation.

7.3.1 FDI Attack Detection Performance

Table 13 presents a comparative evaluation of the proposed DA-CGAE model against three baseline deep learning models, LSTM, BiLSTM, and CNN, across five standard classification metrics: Accuracy, Precision, Recall, F1 Score, and AUC.

Table 13. FDI Attack Detection Performance Comparison..

Model	Accuracy	Precision	Recall	F1 Score	AUC
Proposed (DA-CGAE)	**0.9761**	**0.9506**	**0.9999**	**0.9747**	**0.9993**
LSTM	0.9363	0.9333	0.9799	0.9510	0.9716
BiLSTM	0.9418	0.9331	0.9799	0.9587	0.9805
CNN	0.9411	0.9367	0.9798	0.9578	0.9862

The proposed DA-CGAE outperforms all models across every metric. Most notably, it achieves a Recall of 0.9999, near perfect, meaning it detects almost all attack windows, a critical requirement in power system security where missed detections can result in severe grid instability. The AUC value of 0.9993 demonstrates that the model's anomaly score separates healthy from attacked operating conditions with almost perfect accuracy across all thresholds. The F1 Score of 0.9747 and Accuracy of 0.9761 both reflect a strong balance between precision and recall, well above all baselines.

CNN achieves the second-best AUC (0.9862) among the baselines, and BiLSTM achieves the best baseline F1 Score (0.9587). Both, however, fall significantly below DA-CGAE in Recall and AUC, suggesting that their anomaly boundaries are less reliable for real-time detection. LSTM gives the lowest Accuracy (0.9363) and AUC (0.9716) overall.

The qualitative detection behaviour is illustrated in Figure 18, which shows the system status output (Attack / Healthy) over time for all four models compared to the ground truth. The DA-CGAE detection output closely follows the onset of the attack window ($t = 40$–85 s) with minimal delay and negligible false positives in healthy regions. The baseline models exhibit noticeably more erratic detection patterns, particularly near the attack boundaries where false positives cluster in the pre-attack region ($t = 0$–20 s) and detection is delayed or fragmented around $t = 85$ s.

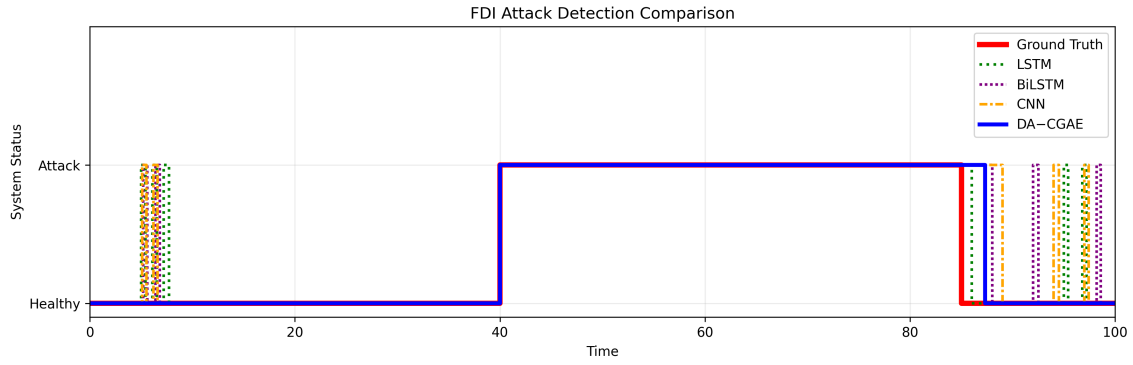


Figure 18. FDI attack detection comparison: ground truth vs. LSTM, BiLSTM, CNN, and DA-CGAE..

7.3.2 FDI Attack Mitigation Performance

Beyond detection, the DA-CGAE is designed to reconstruct the corrupted LFC signals during the attack window and restore them to their expected clean values. Table 14 presents the per-signal reconstruction error metrics Root Mean Squared Error (RMSE) and Mean Absolute Error (MAE) computed exclusively over the attacked region ($t = 40$–85 s).

Table 14. Signal reconstruction error metrics by DA-CGAE (attacked region only)..

Metric	Δf_1	Δf_2	ΔP_{tie}	ACE_1	ACE_2
RMSE	0.002395	0.001513	0.000567	0.001483	0.000201
MAE	0.001481	0.001073	0.000440	0.000957	0.000156

The reconstruction errors are small across all five LFC signals, indicating that the DA-CGAE decoder successfully reconstructs clean signal trajectories from corrupted inputs. The reconstruction quality of ACE_2 is near-optimal with RMSE $= 0.000201$ and MAE $= 0.000156$ pu, meaning the Area 2 error signal is essentially restored following tie-line correction. ΔP_{tie} follows closely with RMSE $= 0.000567$ and MAE $= 0.000440$ pu. The errors

of the frequency deviation signals Δf_1 and Δf_2 are slightly higher (RMSE $= 0.002395$ and 0.001513 respectively) due to the high oscillation amplitude of the two signals during the attack, but remain within acceptable bounds for LFC operation.

The time-domain mitigation results for all five signals are shown in Figures 19–23, each displaying the original corrupted signal (blue), the DA-CGAE mitigated signal (green), and the clean reference signal from the no-attack simulation (orange dashed). The pre-attack segment ($t < 20$ s) is synchronised across all three traces providing a consistent baseline, while the attack zone ($t = 40$–85 s) is shaded in red.

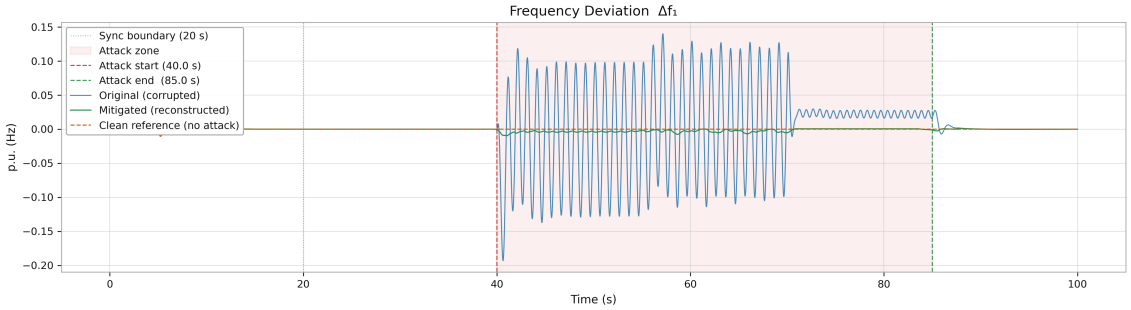


Figure 19. DA-CGAE mitigation results frequency deviation Δf_1 ($t = 40$–85 s attack zone)..

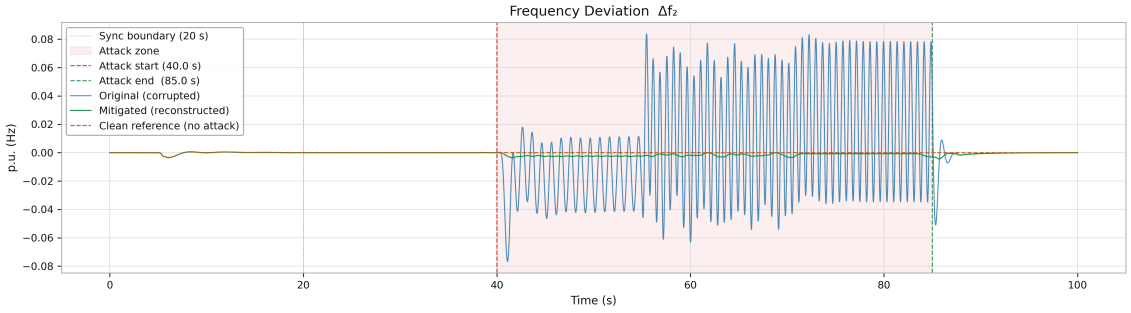


Figure 20. DA-CGAE mitigation results frequency deviation Δf_2 ($t = 40$–85 s attack zone)..

Figures 19 and 20 indicate that the frequency deviations of the original signals reach amplitudes of up to ± 0.20 pu and ± 0.08 pu respectively during the attack, which would destabilise the grid if they were interpreted as normal LFC operating conditions. The DA-CGAE mitigated signal closely follows the clean reference over the entire attack window, with only a minor residual deviation in the first few seconds after attack onset. Figure 21 shows that the tie-line power deviation is effectively suppressed during the attack period,

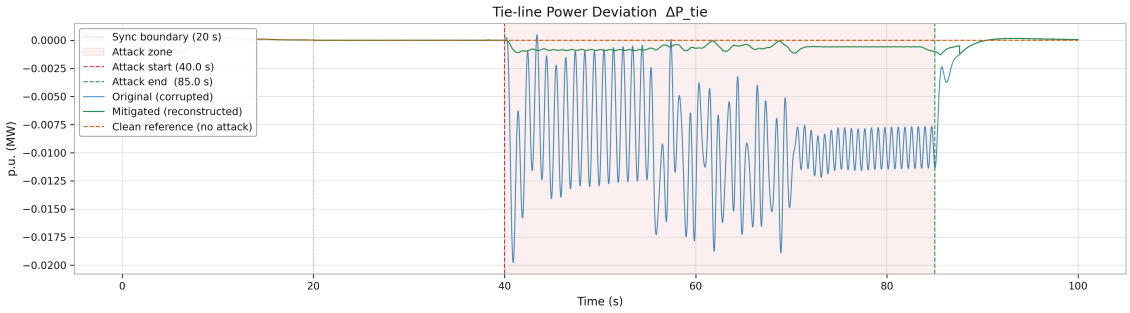


Figure 21. DA-CGAE mitigation results tie-line power deviation ΔP_{tie} ($t = 40$–85 s attack zone)..

with the reconstructed signal maintained close to the clean reference level. A small transient is visible at $t = 85$ s, reflecting the model's response to the sudden discontinuity at attack removal.

Figures 22 and 23 show that the area control errors are also well restored. ACE_2 (Figure 23) exhibits the smallest RMSE over the full simulation horizon and the best agreement between the mitigated and clean reference signals.

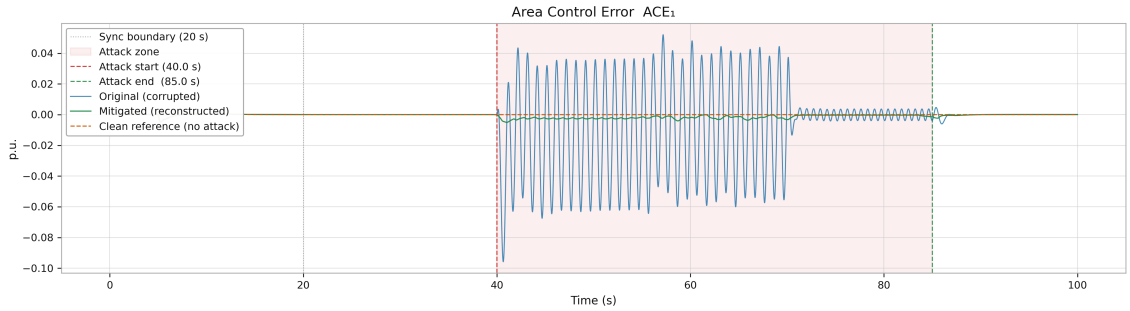


Figure 22. DA-CGAE mitigation results area control error ACE_1 ($t = 40$–85 s attack zone)..

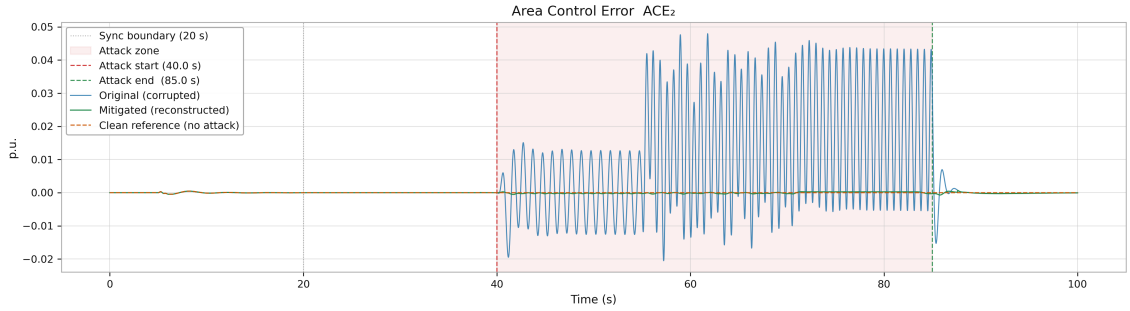


Figure 23. DA-CGAE mitigation results area control error ACE_2 ($t = 40$–85 s attack zone)..

Overall, the results demonstrate that the DA-CGAE is able to detect FDI attacks with near-perfect AUC and Recall, and to reconstruct LFC signals with high fidelity, recovering them

to within sub-milliunit accuracy of the clean reference. The practical benefit of this dual capability is that simultaneous detection and mitigation can be implemented, allowing the LFC controller to operate with confidence on estimated clean signals even while an attack is present.

8 Conclusion and Future Work

This thesis presented an integrated approach for improving both the control performance and cyber-resilience of LFC systems in modern interconnected power networks. The study focused on two major challenges: the optimal tuning of PID controller parameters for a two-area multi-source power system and the detection of FDI attacks affecting LFC signals. A MATLAB/Simulink-based two-area power system was developed by considering thermal, hydro, and gas generation units, along with practical nonlinearities such as governor deadband and generation rate constraints. The system was further extended by incorporating photovoltaic generation in Area 1 and wind generation in Area 2 to reflect the uncertainty and variability introduced by renewable energy sources.

For optimal controller tuning, this work proposed a hybrid metaheuristic algorithm named PGWA, which combines the search capabilities of Particle Swarm Optimization, Grey Wolf Optimizer, and Artificial Bee Colony. The proposed algorithm was designed to improve the balance between exploration and exploitation during the optimization process. By minimizing the ITAE objective function, PGWA was used to tune the PID controller parameters for the LFC system. Its performance was compared with PSO, GWO, ABC, and MHABCPSO under several operating conditions, including step load perturbations, random load variations, asymmetric dual-area disturbances, renewable energy integration, and communication time delay. The simulation results showed that the PGWA-tuned controller provided improved dynamic responses, reduced frequency deviations, lower tie-line power deviations, and shorter settling times compared with the other optimization techniques.

In addition to controller optimization, this thesis developed an unsupervised deep learning framework, DA-CGAE, for detecting FDI attacks in LFC systems. The model learns normal LFC operating behaviour and identifies abnormal deviations using attention-guided temporal feature extraction, disturbance-aware reconstruction, and contrastive representation learning. Unlike supervised detection methods, the proposed DA-CGAE frame-

work does not require labeled attack data during training, making it more suitable for practical power system environments where real attack samples are limited or unavailable. The detection model was evaluated using attack test data generated by injecting asymmetric FDI attacks into ACE signals. Its performance was compared with LSTM, BiLSTM, and CNN models using accuracy, precision, recall, F1 score, AUC, RMSE, and MAE. The results confirmed that DA-CGAE can effectively distinguish between normal disturbances and cyber-induced anomalies, even under renewable energy variability and multi-point attack conditions.

Overall, the findings demonstrate that combining optimized LFC control with intelligent cyber-attack detection can substantially enhance the stability, reliability, and security of modern power systems. The proposed PGWA algorithm improves the dynamic performance of the LFC controller, achieving the lowest ITAE values across all five test scenarios, for example, ITAE $= 0.2019$ under step load perturbation and ITAE $= 31.47$ under the most demanding combined scenario (communication time delay, renewable integration, and sequential multi-area disturbances), along with peak frequency deviations as low as $\Delta f_1 = 0.0127$ Hz and tie-line power deviations of only 0.0010 pu MW, representing reductions of up to 40–50% in tie-line deviation compared to benchmark controllers such as TID-IC and ID-T. The DA-CGAE framework strengthens the system against FDI attacks, achieving 97.61% accuracy, near-perfect recall of 99.99%, an F1 score of 97.47%, and an AUC of 99.93%, while reconstructing corrupted LFC signals to within sub-milliunit accuracy of clean references (e.g., ACE_2 RMSE $= 0.000201$ pu), outperforming LSTM, BiLSTM, and CNN baselines across all detection and mitigation metrics. Therefore, the proposed methodology provides a unified and effective framework for addressing both control and cybersecurity challenges in renewable-integrated interconnected power systems.

Future work can extend this research in several directions. First, different advanced controller structures, such as fractional-order PID, tilt-integral-derivative controllers, model predictive controllers, sliding mode controllers, and fuzzy or adaptive controllers, can be investigated with the proposed PGWA optimization framework. This would allow a broader evaluation of the algorithm under more complex control architectures. Second,

hardware implementation can be carried out using real-time digital simulators, hardware-in-the-loop platforms, or embedded control boards to verify the practical feasibility of the proposed control and detection methods under real operating constraints. Third, the cybersecurity analysis can be expanded by considering different types of cyber attacks, including denial-of-service attacks, replay attacks, data integrity attacks, coordinated multipoint attacks, and stealthy adaptive attacks. Fourth, future studies may examine larger multi-area power systems with higher renewable penetration, energy storage systems, electric vehicle integration, and demand response programs. Finally, online and adaptive versions of the DA-CGAE model can be developed so that the detection framework can continuously update itself under changing grid conditions without requiring full retraining.

Bibliography

Abbaspour, A., Sargolzaei, A., Forouzannezhad, P., Yen, K., & Sarwat, A. (2020). Resilient control design for load frequency control system under false data injection attacks. *IEEE Transactions on Industrial Electronics*, *67*(9), 7951–7962.

Ahmad, H., Gulzar, M., Mustafa, G., et al. (2025). Ai-enabled frequency synchronization control considering fdi attack using metaheuristic algorithm. *Neural Computing and Applications*, *37*, 17541–17570.

Ahmed, E., Mohamed, E., Selim, A., Aly, M., Alsadi, A., Alhosaini, W., … Ramadan, H. (2023). Improving load frequency control performance in interconnected power systems with a new optimal high degree of freedom cascaded fotpid-tidf controller. *Ain Shams Engineering Journal*, *14*, 102207.

Ahmed, M., Magdy, G., Khamies, M., & Kamel, S. (2022a). An efficient coordinated strategy for frequency stability in hybrid power systems with renewables considering interline power flow controller and redox flow battery. *Journal of Energy Storage*, *52*, 104835.

Ahmed, M., Magdy, G., Khamies, M., & Kamel, S. (2022b). Modified tid controller for load frequency control of a two-area interconnected diverse-unit power system. *International Journal of Electrical Power and Energy Systems*, *135*, 107528.

Ansari, J., Homayounzade, M., & Abbasi, A. (2023). Load frequency control in power systems by a robust backstepping sliding mode controller design. *Energy Reports*, *10*, 1287–1298.

Asiri, M., et al. (2025). Ai-based approach for detecting fdi attacks in load frequency control for centralized multi-area power systems. *Computers & Electrical Engineering*.

Biswas, J., Bera, P., & Chakrabarty, K. (2023). Determination of control area and design of fuzzy rule-tuned pid controller for lfc of multimachine power system. *Electric Power Systems Research*, *221*, 109411.

Bratton, D., & Kennedy, J. (2007). Defining a standard for particle swarm optimization. In *Proceedings of the 2007 ieee swarm intelligence symposium (sis 2007)* (pp. 120–127). IEEE.

Choudhary, R., Rai, J., & Arya, Y. (2022). Cascade fopi-foptid controller with energy storage devices for agc performance advancement of electric power systems. *Sustainable Energy Technologies and Assessments*, *53*, 102671.

Clerc, M., & Kennedy, J. (2002). The particle swarm explosion, stability, and convergence in a multidimensional complex space. *IEEE Transactions on Evolutionary Computation*, *6*(1), 58–73.

Coello, C., Pulido, G., & Lechuga, M. (2004). Handling multiple objectives with particle swarm optimization. *IEEE Transactions on Evolutionary Computation*, *8*(3), 256–279.

Eberhart, R., & Kennedy, J. (1995). A new optimizer using particle swarm theory. In *Proceedings of the sixth international symposium on micro machine and human science* (pp. 39–43). IEEE.

Eltamaly, A., Sayed, K., Alotaibi, M., Abo-Khalil, A., & Ahmed, M. (2026). A hybrid fuzzy-PIDD^2 control strategy for coordinated LFC and AVR in renewable-integrated multi-area power systems. *Scientific Reports*, *16*.

Faris, H., Aljarah, I., Al-Betar, M., & Mirjalili, S. (2018). Grey wolf optimizer: A review of recent variants and applications. *Neural Computing and Applications*, *30*(2), 413–435.

Gao, W., & Liu, S. (2011). Improved artificial bee colony algorithm for global optimization. *Information Processing Letters*, *111*(17), 871–882.

Garg, H. (2016). A hybrid pso-ga algorithm for constrained optimization problems. *Applied Mathematics and Computation*, *274*, 292–305.

Gouran-Orimi, S., & Ghasemi-Marzbali, A. (2023). Load frequency control of multi-area multi-source system with nonlinear structures using modified grasshopper optimization algorithm. *Applied Soft Computing*, *137*, 110135.

Habibi, M., Khairuddin, M., Norouzi, A., & Islam, M. (2022). Anomaly detection in load frequency control using bidirectional LSTM. In *Proceedings of the ieee international conference on power system technology (powercon)*. IEEE.

He, Y., Mendis, G., & Wei, J. (2017). Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Transactions on Smart Grid*, *8*(5), 2505–2516.

Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, *9*(8), 1735–1780.

Iqbal, M., Limon, M., Kabir, M., Rabby, M., Soeb, M., & Jubayer, M. (2024). A hybrid optimization algorithm for improving load frequency control in interconnected power systems. *Expert Systems with Applications*, *249*, 123702.

Jagatheesan, K., Anand, B., Dhanasekaran, S., Samanta, S., Ghosh, A., & Tavares, J. (2023). Load frequency control assessment of a PSO-PID controller for a standalone multi-source power system. *Technologies*, *11*(1), 22.

Karaboga, D. (2005). *An idea based on honey bee swarm for numerical optimization* (Tech. Rep. No. TR06). Kayseri, Turkey: Erciyes University, Engineering Faculty, Computer Engineering Department.

Karaboga, D., & Akay, B. (2009). A comparative study of artificial bee colony algorithm. *Applied Mathematics and Computation*, *214*(1), 108–132.

Karaboga, D., & Basturk, B. (2007). A powerful and efficient algorithm for numerical function optimization: Artificial bee colony (ABC) algorithm. *Journal of Global Optimization*, *39*(3), 459–471.

Karaboga, D., & Basturk, B. (2008). On the performance of artificial bee colony (ABC) algorithm. *Applied Soft Computing*, *8*(1), 687–697.

Karaboga, D., Gorkemli, B., Ozturk, C., & Karaboga, N. (2014). A comprehensive survey: Artificial bee colony (ABC) algorithm and applications. *Artificial Intelligence Review*, *42*(1), 21–57.

Kaveh, A., & Zakian, P. (2018). Improved GWO algorithm for optimal design of truss structures. *Engineering with Computers*, *34*(4), 685–707.

Kennedy, J., & Eberhart, R. (1995). Particle swarm optimization. In *Proceedings of the ieee international conference on neural networks* (Vol. 4, pp. 1942–1948). IEEE.

Kennedy, J., & Eberhart, R. (1997). A discrete binary version of the particle swarm algorithm. In *Proceedings of the 1997 ieee international conference on systems, man, and cybernetics* (Vol. 5, pp. 4104–4108). IEEE.

Khamies, M., Elkasem, A., Hassan, M., & Kamel, S. (2023). Enhancing frequency stability in diverse power systems with conventional and renewable energy sources based on an innovative lfc and controlled energy storage integration. *Journal of Energy*

Storage, *73*, 108960.

Khan, I., Mokhlis, H., Mansor, N., Illias, H., Jamilatul Awalin, L., & Wang, L. (2023). New trends and future directions in load frequency control and flexible power system: A comprehensive review. *Alexandria Engineering Journal*, *71*, 263–308.

Kim, K., & Sasahara, H. (2025). Adaptive false data injection attack detection in load frequency control using recurrent neural networks. *SICE Journal of Control, Measurement, and System Integration*.

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*, 436–444.

Liang, J., Qin, A., Suganthan, P., & Baskar, S. (2006). Comprehensive learning particle swarm optimizer for global optimization of multimodal functions. *IEEE Transactions on Evolutionary Computation*, *10*(3), 281–295.

Long, W., Jiao, J., Liang, X., & Tang, M. (2018). An exploration-enhanced grey wolf optimizer to solve high-dimensional numerical optimization. *Engineering Applications of Artificial Intelligence*, *68*, 63–80.

Manias, D., et al. (2024). Cyber security of smart-grid frequency control: A review and vulnerability assessment framework. *ACM Transactions on Cyber-Physical Systems*.

Manoharan, N., Dash, S., & Rajesh, K. (2017). Load frequency control of nonlinear power system employing firefly algorithm. *Indian Journal of Science and Technology*, *10*(13), 1–6.

Mendes, R., Kennedy, J., & Neves, J. (2004). The fully informed particle swarm: Simpler, maybe better. *IEEE Transactions on Evolutionary Computation*, *8*(3), 204–210.

Mirjalili, S. (2015). How effective is the grey wolf optimizer in training multi-layer perceptrons. *Applied Intelligence*, *43*(1), 150–161.

Mirjalili, S., Mirjalili, S., & Lewis, A. (2014). Grey wolf optimizer. *Advances in Engineering Software*, *69*, 46–61.

Mokhtari, S., & Yen, K. (2024). False data injection attack detection, isolation, and identification in industrial control systems based on machine learning: Application in load frequency control. *Electronics*, *13*(16), 3239.

Paliwal, N., Srivastava, L., & Pandit, M. (2020). PSO-based PID controller designing for LFC of single area electrical power network. In *Nature inspired optimization for electrical power system*. Singapore: Springer.

Pinceti, A., Sankar, L., & Kosut, O. (2021). Data-driven false data injection attack detection in smart grids with temporal convolutional features. In *Proceedings of the ieee power & energy society general meeting*. IEEE.

Poli, R., Kennedy, J., & Blackwell, T. (2007). Particle swarm optimization: An overview. *Swarm Intelligence*, *1*(1), 33–57.

Raghuvamsi, Y., et al. (2024). Random subspace ensemble-based detection of false data injection attacks in automatic generation control systems. *Heliyon*.

Rai, A., & Das, D. (2022). The development of a fuzzy tilt integral derivative controller based on the sailfish optimizer to solve load frequency control in a microgrid, incorporating energy storage systems. *Journal of Energy Storage*, *48*, 103887.

Ranjan, M., & Shankar, R. (2024). Cyber-attack and defense method for load frequency control in smart grid systems with electric vehicles. *Optimal Control Applications and Methods*.

Schuster, M., & Paliwal, K. (1997). Bidirectional recurrent neural networks. *IEEE Transactions on Signal Processing*, *45*(11), 2673–2681.

Shi, Y., & Eberhart, R. (1998). A modified particle swarm optimizer. In *Proceedings of the ieee world congress on computational intelligence evolutionary computation* (pp. 69–73). IEEE.

Shrestha, R., Chamana, M., Adeyanju, O., Mohammadpourfard, M., & Bayne, S. (2025). Detection and localization of the fdi attacks in the presence of dos attacks in smart grid. *Smart Cities*, *8*(5), 144.

Taher, A., Hasanien, H., Abdel Aleem, S., Tostado-Véliz, M., Ćalasan, M., Turky, R., & Jurado, F. (2023). Optimal model predictive control of energy storage devices for frequency stability of modern power systems. *Journal of Energy Storage*, *57*, 106310.

Takiddin, A., Ismail, M., Zafar, U., & Serpedin, E. (2021). Robust electricity theft detection against data poisoning attacks in smart grids. *IEEE Transactions on Smart Grid*, *12*(3), 2675–2684.

Tavakoli, S., Zamani, A.-A., & Khajehoddin, A. (2024). Efficient load frequency control in multi-source interconnected power systems using an innovative intelligent control framework. *Energy Reports*, *11*, 2805–2817.

Van den Bergh, F., & Engelbrecht, A. (2006). A study of particle swarm optimization

particle trajectories. *Information Sciences*, *176*(8), 937–971.

Wang, D., Wang, X., Zhang, Y., & Jin, L. (2019). Detection of power grid disturbances and cyber-attacks based on machine learning. *Journal of Information Security and Applications*, *46*, 42–52.

Wang, Z., Li, D., Lyu, X., Gao, S., Fu, C., Zhu, S., & Wang, B. (2023). Intelligent load frequency control for improving wind power penetration in power systems. *Energy Reports*, *9*, 1225–1234.

Zhan, Z., Zhang, J., Li, Y., & Chung, H. (2009). Adaptive particle swarm optimization. *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, *39*(6), 1362–1381.

Zheng, e. a. (2025). Research on load frequency control system attack detection method based on multi-model fusion. *Energy Informatics*, *8*, 72.

Zheng, J., Du, J., Wang, B., Klemeš, J., Liao, Q., & Liang, Y. (2023). A hybrid framework for forecasting power generation of multiple renewable energy sources. *Renewable and Sustainable Energy Reviews*, *172*, 113046.

Zhu, G., & Kwong, S. (2010). Gbest-guided artificial bee colony algorithm for numerical function optimization. *Applied Mathematics and Computation*, *217*(7), 3166–3173.

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access*, *9*, 29775–29818.