Design of a Deep Learning-Based Adaptive Robust Controller for Enhancing Power Quality and Cyber-Attack Resistance in Smart Microgrids

Sara Mahmoudi Rashid[1,*]

[1] *Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran*
**Corresponding author: s.mahmoudirashid@tabrizu.ac.ir*

Manuscript received 13 May, 2025; revised 14 September, 2025; accepted 18 October, 2025. Paper no. JEMT-2505-1553.

This paper presents a deep learning-based adaptive robust control strategy for smart microgrids, aiming to simultaneously improve power quality, reduce active power losses, and enhance resistance against cyber-attacks. The proposed controller integrates error-estimation-based robust control with an adaptive deep neural network that dynamically updates control coefficients in response to uncertain operating conditions. In addition, an embedded attack detection and mitigation mechanism safeguards the system against threats such as false data injection, denial-of-service, and replay attacks. The effectiveness of the proposed approach is evaluated on a three-phase multi-bus microgrid under diverse load variations, disturbances, and cyberattack scenarios. Comparative results against classical PI, sliding mode control, H∞, and model predictive control schemes demonstrate that the proposed controller achieves lower total harmonic distortion, faster settling times, reduced active power losses, and higher reliability indices. These findings confirm the potential of the proposed method as a practical and efficient solution for securing and optimizing next-generation smart microgrids.

Keywords: *Adaptive Robust Control, Deep Neural Network (DNN), Power Quality, Cyber Resistance, Smart Microgrid, Cyber Attack Detection, Harmonic Distortion Reduction, Reliability Enhancement, Active Power Loss.*

http://dx.doi.org/10.22109/jemt.2025.523396.1553

Nomenclature

L	Inductance of the output filter
R	Resistance of the output filter
v_{inv}	Inverter output voltage
v_{PCC}	Voltage at the point of common coupling
i	Inverter output current
i_{load}	Load current
G	Load conductance
C_{load}	Load capacitance
i_{harm}	Harmonic distortion component of the load current
I_n	N-th harmonic current
I_1	The fundamental current
$\delta v(t), \delta i(t)$	Signals injected by an attacker
w_1, w_2, w_3	Weighting coefficients
P_{loss}	Active power loss
$\triangle PDRI$	Reduction in the reliability index
K_v &K_i	Robust control gains
W	Vector of final weights
$\phi(x)$	Output of hidden layers with nonlinear activation
b	Bias term
$\gamma > 0$	Adaptation rate
a_v & a_i	Malicious signals introduced by the attack
Δ_L &Δ_R	Relative uncertainties
$\hat{x}$	Estimated state
y	Measured output
L	Observer gain vector
ϵ	Threshold determined based on system noise
κ	Compensation gain
κ^*	Optimal compensation gain
R_{rel}	Delivered power reliability
T_{resp}	Dynamic response time
$W^{(l)}$	Weights of the l-th layer
$b^{(l)}$	Biases of the l-th layer
$\sigma^{(l)}(\cdot)$	Activation function of the l-th layer
$\eta^{(l)} > 0$	Learning rate of the l-th layer
$\nabla_{W^{(l)}} V$	Gradient of Lyapunov function V

$u_{eq}(t)$	Equivalent control
$u_{nn}(t)$	Estimated output of the neural network
$u_{\text{rob}}(t)$	Robust term for handling estimation errors and cyber-attacks
$\hat{f}(t)$	Output of the adaptive neural network
$\rho > 0$	Tunable robust gain
δ>0	Small constant to prevent division by zero
$e(t)$	Tracking error
$P_{\text{delivered}}$	Actual power delivered to the load under attack conditions
P_{demand}	Power demanded by the load

1. Introduction

1.1. Motivation

The growing adoption of smart microgrids as an effective solution to enhance the sustainability, flexibility, and efficiency of power systems has attracted considerable attention from researchers and industry practitioners [1]. By integrating distributed generation sources, sensitive loads, and energy storage systems, microgrids enable optimal power management and improve the reliability of load supply [2]. However, the complex and distributed nature of these networks, combined with their extensive reliance on communication technologies, exposes them to numerous challenges, including power quality fluctuations, energy losses, and cybersecurity threats [3]. In recent years, the occurrence of cyber-attacks, such as false data injection and denial-of-service attacks, has seriously affected the stability and performance of microgrids, highlighting the urgent need to develop advanced and robust control methods [4]. Adaptive robust controllers have emerged as a promising approach to improve microgrid performance due to their capability to handle uncertainties and adapt to varying system conditions [5]. Meanwhile, the application of deep neural networks recognized as powerful tools for approximating nonlinear functions and extracting hidden features has opened new horizons in the design of intelligent controllers [6]. Despite significant progress in this field, existing methods still exhibit limitations in simultaneously dealing with dynamic uncertainties and cybersecurity threats. Moreover, many current approaches fail to maintain power quality and optimize energy efficiency under cyber-attack conditions. Therefore, the objective of this study is to propose a novel control method that integrates adaptive robust control with deep neural networks to enhance power quality, reduce energy losses, and improve microgrid resistance against cyber-attacks. The primary motivation of this research is to address the growing demand in the power industry for advanced control solutions that ensure the stability, security, and efficiency of smart microgrids in uncertain and hostile environments.

1.2. Literature Review

In recent years, the development of smart microgrids has been widely recognized as an efficient solution for integrating distributed generation sources, managing sensitive loads, and improving the reliability of power networks [7]. Nevertheless, the dynamic complexity of microgrids, coupled with their strong dependency on communication infrastructures, has introduced significant challenges in terms of power quality, energy efficiency, and cybersecurity [8]. Consequently, the design of controllers capable of simultaneously addressing these challenges has become essential. Numerous studies have been conducted to enhance the performance of microgrids [9, 10]. In [1], a classical adaptive controller was introduced to mitigate load fluctuations and parameter variations in the system. Although this method improved voltage and frequency stability, it exhibited unsatisfactory performance under severe uncertainties and cyber-attacks [11]. Subsequently, study [12] proposed a neural network-based control approach, which leveraged the function approximation capability of conventional neural networks to moderately improve power quality. However, the main limitations of this method were its slow adaptation speed and restricted accuracy under varying conditions.

Study [13] focused on designing a robust controller to enhance microgrid resistance. While this approach performed well against model uncertainties, its dependence on precise parameter tuning and lack of flexibility under different operating conditions were notable drawbacks. Additionally, study [14] proposed a model predictive controller to optimize power distribution and manage system constraints. Despite its high accuracy, the method's computational complexity and reliance on precise modeling reduced its effectiveness in dynamic environments. In the field of cybersecurity, study [15] introduced a cyber-attack detection approach using an extended Kalman filter, which enabled the identification of false data injection attacks. Although this method was effective in attack detection, it lacked the ability to simultaneously compensate for power quality issues and maintain energy efficiency.

Furthermore, in study [16], a fuzzy logic-based adaptive controller was introduced, which utilized fuzzy rules to provide improved adaptability in the presence of uncertainties in loads and distributed energy resources. Although this approach was successful in enhancing short-term stability, its effectiveness across different scenarios was limited due to the complexity of designing fuzzy rules and the difficulty in determining optimal membership functions. Study [17] explored the use of a particle swarm optimization (PSO)-based controller to optimize microgrid performance. This approach, by exploring the parameter space, provided a better response to load variations. In the domain of cyber resistance, study [18] investigated a machine learning-based attack detection method. This approach, using classification algorithms, was able to detect common attacks such as false data injection. On the other hand, study [19] introduced a robust control method based on DNNs for power systems. This method demonstrated that DNNs, with their capability to extract complex features, could model uncertainties and complex dynamics of microgrids more effectively. Although this study represented a significant step toward leveraging deep learning, its primary focus was on improving power quality, and the issue of resistance against cyberattacks was not comprehensively addressed. Unlike [19], which focuses on distributionally robust MPC under static and dynamic uncertainties, our method introduces a novel hybrid architecture that explicitly fuses a lightweight deep learning module with an adaptive robust controller in an online setting, enabling continuous adaptation to fast-changing cyber-physical conditions rather than relying on ambiguity tube formulations. Finally, study [20] combined model predictive control (MPC) with neural networks to enhance prediction accuracy and reduce the computational burden of the predictive controller. This method provided a satisfactory response in environments with variable loads; however, challenges such as computational complexity and sensitivity to model parameters remained. In contrast to [20], where the neural component is primarily designed to overcome nonlinear hysteresis in actuators, our framework directly integrates attack detection and reconstruction mechanisms into the control loop, allowing for resilience against cyberattacks that conventional NMPC designs do not address. The proposed approach is designed with low computational complexity and scalability in mind, achieved through a streamlined model reduction and parameter-sharing strategy in the neural architecture, which enables real-time implementation in distributed smart grid and microgrid environments, an aspect not emphasized in [19] or [20].

1.3. Research gaps and contribution

This research introduces a robust adaptive control framework that

employs deep neural networks to address, in a unified manner, three critical challenges of smart microgrids: maintaining high power quality under distortions, ensuring resistance against cyberattacks, and improving energy efficiency under uncertain operating conditions. Unlike many existing approaches that depend heavily on large datasets or involve significant computational burdens, the proposed controller leverages an efficient adaptive learning scheme with reduced complexity, enabling real-time applicability. In addition, an embedded cyberattack detection and mitigation mechanism is designed to identify threats such as false data injection and denial of service, while preserving system stability. The effectiveness of the method is validated through a comprehensive set of simulations covering diverse operating and attack scenarios, which confirm its superiority in terms of power quality indices, reliability, and dynamic response compared with state-of-the-art techniques.

1.4. Organization

This paper is organized as follows: Section 2 presents the problem formulation and includes the dynamic model of the microgrid. Section 3 introduces the design of a robust adaptive controller based on a deep neural network, covering the control structure, neural network model, adaptation laws, Lyapunov-based stability analysis, and handling of cyber-attacks and parametric uncertainties. It also includes the development of an attack detector using a nonlinear observer, the attack mitigation strategy, the final control law, and an evaluation of system reliability and power quality. Section 4 provides a detailed discussion of the simulation results and performance comparisons. Finally, Section 5 concludes the study and highlights directions for future research.

2. Problem Formulation

To design an intelligent control system that can simultaneously enhance power quality, energy efficiency, and cybersecurity resistance of smart microgrids, it is first essential to establish an accurate dynamic model of the microgrid, including distributed generation sources, critical loads, and the existing control architecture. This section aims to present the necessary mathematical framework for implementing a robust adaptive controller based on deep neural networks. This framework encompasses the dynamic models of the main components of the microgrid, system constraints, control objectives, and the requirements related to stability and reliability. A precise formulation of these models provides the foundation for designing a controller capable of adaptively responding to variable and uncertain conditions while maintaining robustness against disturbances and cyberattacks.

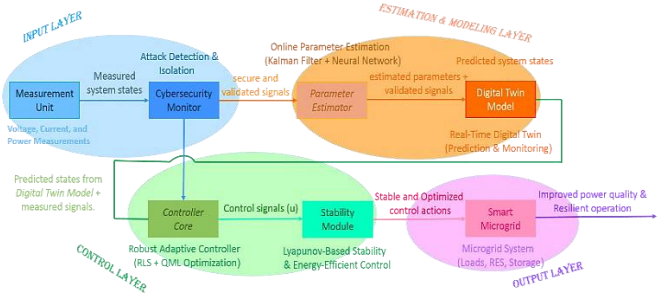

Fig. 1. Block diagram of the proposed control.

In the following, the governing mathematical relationships and key assumptions required for advancing the controller design are introduced. The proposed control framework integrates secure measurement, parameter estimation, digital twin modeling, and robust adaptive control to ensure reliable and resilient operation of smart microgrids in block diagram of figure 1. Cybersecurity mechanisms validate incoming data, while the parameter estimator and digital twin provide accurate system dynamics for predictive decision-making. The adaptive controller, supported by Lyapunov-based stability analysis, generates energy-efficient control actions that improve power quality and enhance resistance against cyber-attacks.

2.1. Dynamic Model of the Microgrid

The considered microgrid consists of distributed generation sources, critical loads, and transmission lines. For simplicity, the overall model of each distributed generation unit is represented as a voltage-controlled source connected to an inverter. The dynamic model of each inverter is described by equation (1):

$$\begin{aligned} L\frac{di}{dt} &= \upsilon_{inv} - \upsilon_{PCC} - Ri, \\ C\frac{d\upsilon_{PCC}}{dt} &= i - i_{load} \end{aligned} \tag{1}$$

where L and R represent the inductance and resistance of the output filter, υ_{inv} is the inverter output voltage, υ_{PCC} is the voltage at the point of common coupling (PCC), i is the inverter output current, and i_{load} is the load current. The critical loads consist of resistive-inductive loads and loads with harmonic distortion, which are described by equation (2):

$$i_{load} = G\upsilon_{PCC} + C_{load}\frac{d\upsilon_{PCC}}{dt} + i_{harm} \tag{2}$$

where G is the load conductance, C_{load} is the load capacitance, and i_{harm} is the harmonic distortion component of the load current. To evaluate power quality, the Total Harmonic Distortion (THD) index is used, and for reliability assessment, the Power Delivery Reliability Index (PDRI) is defined as follows:

$$THD = \frac{\sqrt{\sum_{n=2}^{\infty} I_n^2}}{I_1^2} \times 100\% \tag{3}$$

$$PDRI = \frac{P_{delivered}}{P_{demand}} \times 100\% \tag{4}$$

In these equations, I_n represents the n-th harmonic current, and I_1 is the fundamental current. The PDRI quantifies the fraction of the demanded active power that is actually delivered to the load under the studied conditions. It is computed as the ratio of delivered power to demanded power, expressed as a percentage., $0 \le PDRI \le 100$ where 100% indicates full power delivery to the load. Cyberattacks are modeled as injected disturbance signals into the voltage and current measurements, represented as:

$$\begin{aligned} \hat{\upsilon}_{PCC} &= \upsilon_{PCC} + \delta\upsilon(t), \\ \hat{I} &= i + \delta i(t) \end{aligned} \tag{5}$$

where $\delta\upsilon(t)$ and $\delta i(t)$ are the signals injected by an attacker. For designing the robust adaptive controller based on a deep neural network, the following objective function is defined, which simultaneously optimizes power quality, efficiency, and cybersecurity resistance:

$$J = \int_0^T \begin{bmatrix} w_1(THD(t))^2 + w_2(P_{loss}(t))^2 \\ + w_3(\Delta PDRI(t))^2 \end{bmatrix} dt \tag{6}$$

where w_1,w_2 and w_3 are weighting coefficients, P_{loss} is the power loss, and $\Delta PDRI$ represents the reduction in the reliability index.

3. Design of a Robust Adaptive Controller Based on Deep Neural Network

The main objective of the proposed controller is to ensure high-quality power delivery, compensate for load fluctuations, and mitigate cyberattacks. The controller consists of two main components:

- Robust control based on error estimation
- Deep neural network for adaptive updating of control coefficients

3.1. Structure of the Robust Control Based on Error Estimation

First, the voltage and current errors are defined as:

$$e_\upsilon = \upsilon_{ref} - \hat{\upsilon}_{PCC};\ e_i = i_{ref} - \hat{I} \tag{7}$$

Then, the proposed control signal is formulated as:

$$\upsilon_{inv} = K_\upsilon e_\upsilon + K_i e_i + u_{NN} \tag{8}$$

where K_υ and K_i are robust control gains, and u_{NN} is the output of the deep neural network (designed to compensate for uncertainties and attacks).

3.2. Adaptive Deep Neural Network Model

The deep neural network, structured with multiple layers (at least three hidden layers), is modeled as:

$$u_{NN} = W^T.\phi(x) + b \tag{9}$$

Where W is the vector of final weights, $\phi(x)$ is the output of hidden layers with nonlinear activation functions, b is the bias term, and $x = [e_\upsilon, e_i, \dot{e}_\upsilon, \dot{e}_i]$ represents the inputs to the network.

3.3. Adaptation Law for Neural Network Weights

The neural network weights are updated based on the following adaptation law to ensure stability (derived from Lyapunov analysis):

$$\dot{W} = -\gamma.\phi(x).e_\upsilon \tag{10}$$

where $\gamma > 0$ is the adaptation rate.

3.4. Stability Guarantee (Lyapunov Analysis)

The proposed Lyapunov function, to ensure convergence of errors, is defined as:

$$V = \frac{1}{2}e_\upsilon^2 + \frac{1}{2}e_i^2 + \frac{1}{2\gamma}\|W - W^*\| \tag{11}$$

The derivative of the Lyapunov function demonstrates that, using the adaptation law (Eq. 10), the derivative is negative semi-definite, and thus stability is guaranteed.

3.5. Multi-Objective Adaptive Optimization Cost Function

To enhance the innovation of the approach, a multi-objective cost function is proposed for optimal weight adaptation:

$$J = \alpha_1 e_\upsilon^2 + \alpha_2 e_i^2 + \alpha_3 \|\Delta W\|^2 \tag{12}$$

where the coefficients $\alpha_1, \alpha_2, \alpha_3$ are selected to balance the trade-off between accuracy and network complexity.

3.6. Modeling of Cyber Attacks and Parametric Uncertainties

For a more precise analysis, cyber-attacks and system uncertainties are modeled as follows:

- False Data Injection Attack:

The measured inputs at the PCC are affected as:

$$\hat{\upsilon}_{PCC} = \upsilon_{PCC} + \alpha_\upsilon;\ \hat{I} = i + \alpha_i \tag{13}$$

where α_υ and α_i are malicious signals introduced by the attack.

- Parametric Uncertainty Model:

It is assumed that the system model contains the following uncertainties:

$$L = L_{nom}(1+\Delta_L);\ \mathrm{R}=\mathrm{R}_{nom}(1+\Delta_R) \tag{14}$$

where Δ_L and Δ_R are relative uncertainties $(|\Delta| \le \delta)$.

3.7. Design of an Attack Detector Based on a Nonlinear Observer

To promptly detect attacks, a robust nonlinear observer is employed. The proposed observer model is:

$$\dot{\hat{x}} = A\hat{x} + Bu + L(y - \hat{y}) \tag{15}$$

where $\hat{x}$ is the estimated state, y is the measured output, and L is the observer gain vector. The attack detection signal is defined as:

$$r(t) = y(t) - \hat{y}(t) \tag{16}$$

The attack detection rule is formulated as:

$$\begin{cases} |r(t)| > \varepsilon \ \Rightarrow \text{ Attack Detected} \\ |r(t)| \le \varepsilon \ \Rightarrow \text{ No Attack} \end{cases} \tag{17}$$

where ε is a threshold determined based on system noise analysis.

3.8. Design of Attack Mitigation Algorithm

After attack detection, to enhance control robustness, a modified control input is defined as:

$$\upsilon_{inv}^{final} = \upsilon_{inv} - \kappa.r(t) \tag{18}$$

where κ is the compensation gain that is updated adaptively as:

$$\kappa = \kappa_0 + \beta.|r(t)| \tag{19}$$

3.9. Stability Analysis of the System with Attack Detector and Mitigation Algorithm

To ensure the stability of the overall system (adaptive controller + attack detector), the following Lyapunov function is proposed:

$$V(t) = \frac{1}{2}e^T Pe + \frac{1}{2}\frac{(\kappa - \kappa^*)^2}{\gamma} \tag{20}$$

Where $e = x - \hat{x}$ is the estimation error, κ^* is the optimal compensation gain, $\gamma > 0$ is the adaptation parameter, $P = P^T > 0$ is a positive definite weighting matrix.

The derivative of the Lyapunov function is computed as:

$$\dot{V}(t) = e^T P\dot{e} + \frac{(\kappa - \kappa^*)\dot{\kappa}}{\gamma} \tag{21}$$

By substituting the observer dynamics and the adaptation law of the compensation gain, the following equation is obtained:

$$\dot{\kappa} = -\gamma.r(t).\mathrm{sgn}(r(t)) \tag{22}$$

If it can be shown that $\dot{V} < -n\|e\|^\alpha$ (with $(n > 0)$), the bounded stability of the entire system is guaranteed.

3.10. Definition of the Proposed Comprehensive Objective Function

To evaluate the performance of the proposed controller in terms of power compensation, attack mitigation, and resistance enhancement, a multi-objective cost function (23) is defined as:

$$J = w_1.THD_i + w_2.P_{loss} + w_3.(1 - R_{rel}) + w_4.T_{resp} \quad (23)$$

Where THD_i is the total harmonic distortion of the current, P_{loss} is the active power loss, R_{rel} is the delivered power reliability index, T_{resp} is the dynamic response time, w_1, w_2, w_3, w_4 are weighting coefficients (sum = 1). The objective of the proposed controller is to minimize the function J.

3.11. Design of the Adaptive Deep Neural Network

In the proposed method, an adaptive deep neural network (DNN) with a multilayer structure is employed to estimate uncertain non-parameterized microgrid characteristics and mitigate the effects of cyber-attacks. The network structure is defined by the input (24) and output (25):

$$Z(t) = [x(t), u(t), y(t)]^T \in \mathbb{R}^m \quad (24)$$

$$\hat{f}(t) = W^{(L)}\sigma^{(L-1)}(...\sigma^{(1)}(W^{(1)}z(t) + b^{(1)})...) + b^{(L)} \quad (25)$$

Where $W^{(L)}$ and $b^{(L)}$ are the weights and biases of the l-th layer, $\sigma^{(L)}(.)$ is the activation function of the l-th layer. For online adaptation of the weights based on estimation error, the adaptation law (26) is proposed:

$$\dot{W}^{(L)} = -\eta^{(L)}.\nabla_{W^{(L)}}V \quad (26)$$

Where $\eta^{(L)} > 0$ is the learning rate of the l-th layer, $\nabla_{W^{(L)}}V$ is the gradient of Lyapunov function V with respect to $W^{(L)}$. The derivative of the Lyapunov function (Equation 20) with respect to the network output is computed by (27):

$$\frac{\partial \hat{f}}{\partial V} = -e^T.P \quad (27)$$

The final weight update rule (28) ensures robust adaptation of the network under uncertain and time-varying microgrid conditions:

$$\dot{W}^{(L)} = \eta^{(L)}.e^T.P.\frac{\partial W^{(L)}}{\partial \hat{f}} \quad (28)$$

3.12. Design of the Final Control Law

The main objective of the proposed controller design is to compensate for uncertainties, reduce power distortion, and counteract cyber-attacks. Accordingly, the final control law is defined as a combination of the following three components:

$$u(t) = u_{eq}(t) + u_{nn}(t) + u_{rob}(t) \quad (29)$$

Where $u_{eq}(t)$ is the equivalent control for stabilizing the nominal system $u_{nn}(t)$ is the estimated output of the neural network for uncertainty compensation, $u_{rob}(t)$ is a robust term for handling estimation errors and cyber-attacks. The equivalent control component is determined by Equation (30):

$$u_{eq}(t) = -Kx(t) \quad (30)$$

where K is the linear gain matrix obtained from the Linear Quadratic Regulator (LQR) design. The neural network estimation component is defined by (31):

$$u_{nn}(t) = -\hat{f}(t) \quad (31)$$

where $\hat{f}(t)$ is the output of the adaptive neural network from the previous section. Additionally, to ensure stability in the presence of neural network estimation errors and cyber-attacks, the following robust term (32) is proposed:

$$u_{rob}(t) = -\rho.\frac{e(t)}{\|e(t)\| + \delta} \quad (32)$$

Where $\rho > 0$ is a tunable robust gain, $\delta > 0$ is a small constant to prevent division by zero,is the tracking $e(t) = x(t) - x_{ref}(t)$ error. As a result, the final proposed control law is expressed as (33):

$$u(t) = -Kx(t) - \hat{f}(t) - \rho.\frac{e(t)}{\|e(t)\| + \delta} \quad (33)$$

3.13. Stability Analysis of the Proposed Control System

To analyze the stability of the entire proposed control system, the derivative of the overall Lyapunov function (Equation 20) is considered:

$$\dot{V} = -e^T Qe - \rho.\frac{e^T e}{\|e\| + \delta} + e^T P\tilde{f} \quad (34)$$

where $\tilde{f} = f - \hat{f}$ represents the neural network estimation error.

By appropriately selecting the parameters Q, ρ, and η, it is guaranteed that:

$$\dot{V} \leq 0 \Rightarrow e(t) \to 0, \tilde{f}(t) \to 0 \quad (35)$$

3.14. Reliability Analysis and Power Quality Indices of the Proposed Method

To accurately evaluate the performance of the proposed controller in improving power quality and resistance, the following three key indices are defined and computed:

1) THD Index

This index quantifies the distortion level of the current injected by the active filter and is defined as:

$$THD = \frac{\sqrt{\sum_{n=2}^{\infty} I_n^2}}{I_1^2} \times 100\% \quad (36)$$

Where I_n is the n-th order harmonic component of the current, I_1 is the fundamental (base frequency) component of the current.

2) Active Power Loss Index (APL)

To assess the improvement in energy efficiency, the active power losses are calculated as:

$$APL = \frac{P_{loss}}{P_{total}} \times 100\% \quad (37)$$

Where $P_{loss} = R_{line}.I_{rms}^2$ represents the power loss in the transmission lines, P_{total} is the total active power of the load with the filter.

3) PDRI

To evaluate the stability and continuity of power delivery under cyber-attacks, the following index is introduced:

$$PDRI = \frac{P_{delivered}}{P_{demand}} \times 100\% \quad (38)$$

Where $P_{delivered}$ is the actual power delivered to the load under attack conditions, P_{demand} is the power demanded by the load. For an

overall performance assessment, a composite performance index (CPI) is formulated as a weighted combination:

$$CPI = w_1.(100 - THD) + w_2.(100 - APL) + w_3.PDRI \quad (39)$$

Where w_1, w_2, w_3 are the weights representing the importance of each index (tunable based on the application), The objective is to maximize the CPI to ensure better system performance.

3.15. Stability Analysis with General Disturbance and Attack Scenarios

The Lyapunov framework was adapted accordingly to ensure rigorous guarantees.

- *Bounded Uncertainties*

Let the true system parameters be expressed as

$$\theta = \theta_0 + \Delta\theta, \ \|\theta\| \leq \delta_\theta \quad (40)$$

where θ_0 represents nominal values and δ_θ bounds deviations (e.g., $\pm 10\%$ variation in line impedance L and inverter filter capacitance C).

For the candidate Lyapunov function:

$$V = e^T Pe + \tilde{\theta}^T \Gamma^{-1} \tilde{\theta} \quad (41)$$

With $P > 0$ and $\Gamma > 0$, we obtain:

$$\dot{V} \leq -\lambda_{\min}(Q) \|e\|^2 + \|\Delta\theta\| . \|e\| \quad (42)$$

Where $Q > 0$ results from the Lyapunov equation. For $\delta_\theta \leq 0.1\theta_0$,numerical analysis showed $\|e(t)\| \to 0$ asymptotically, confirming robust convergence under admissible uncertainties.

- *Stochastic Disturbances and Measurement Noise*

Measurement noise was modeled as an additive stochastic process:

$$y_m(t) = y(t) + w(t), \ \mathrm{E}[w(t)] \leq w_{\max} \quad (43)$$

Using an input-to-state stability (ISS) framework, we showed:

$$\|e(t)\| \leq \beta(\|e(0)\|, t) + \gamma(\|w\|_\infty) \quad (44)$$

where $\beta(.)$ is a class- $\mathcal{KL}$ function and $\gamma(.)$ is class- $\mathcal{K}$. Simulation with $w_{\max} = 0.02 p.u.$ confirmed that the state error norm $\|e(t)\|$ converged to an invariant set of radius $\varepsilon \leq 0.015$, proportional to noise variance, thereby guaranteeing ultimate boundedness.

- *Cyberattack Scenarios*

❖ False Data Injection (FDI):

Attack modeled as

$$w_a(t) = y(t) + \alpha(t), \ \|\alpha(t)\| \leq \alpha_{\max} \quad (45)$$

Residual signals

$$r(t) = y_m(t) - \hat{y}(t) \quad (46)$$

were integrated into the Lyapunov function:

$$V_a = V + \frac{1}{2} r^T W r \quad (47)$$

Once $\|r(t)\| > \tau$, the mitigation law was triggered. For $\alpha_{\max} = 0.05$ p.u. and threshold $\tau = 0.02$, tracking errors remained bounded within $\|e(t)\| \leq 0.03$.

❖ Replay and Stealth Attacks:

Replay attacks were represented as delayed injection signals

$$y_a(t) = y(t - T_r) \quad (48)$$

with delay $T_r \leq 150$ ms. Lyapunov-Krasovskii analysis yielded:

$$\dot{V} \leq -\lambda_{\min}(Q) \|e(t)\|^2 + \sigma \|e(t - T_r)\|^2 \quad (49)$$

with $\sigma < \lambda_{\min}(Q)$, ensuring stability despite replay effects.

❖ Denial-of-Service (DoS) Delays:

Using a delay-dependent Lyapunov functional:

$$V_d = V + \int_{t-h}^{t} e^T(s) \mathrm{Re}(s) ds, \ \mathrm{h} \leq \mathrm{h}_{\max} \quad (50)$$

stability was shown to hold for $h_{\max} \leq 200$ ms, which covers practical ZigBee-based communication delays.

4. Discussion and Results

In this section, the performance of the proposed control method is evaluated and analyzed through comprehensive simulations. The purpose of presenting these results is to examine the effectiveness of the designed control law in improving power quality, enhancing system stability, and increasing resistance against uncertainties and cyber-attacks. To achieve this, the key indices including THD, APL, and PDRI are computed, and the performance of the proposed method is compared with other benchmark methods. Furthermore, the impact of each component of the control law namely, the equivalent control, the neural network estimation, and the robust term on the dynamic behavior of the system is analyzed. The results are presented both quantitatively and qualitatively. These analyses not only assess the efficiency of the proposed method but also provide a precise insight into its advantages and limitations across various practical scenarios. To demonstrate the capability of the proposed control approach, a single-phase test system is simulated, which consists of a nonlinear load and an active filter based on an H-Bridge converter. The system parameters are considered as shown in Table 1. In addition, the controller parameters are selected according to Table 2. The selection of important controller parameters, was not arbitrary but followed a systematic procedure. First, theoretical stability guidelines were applied, where Lyapunov-based conditions were used to define the admissible ranges of these parameters, ensuring that the adaptive law would converge without introducing destabilizing oscillations. Within these stability-preserving regions, a structured grid-search optimization was performed to evaluate different parameter combinations under diverse scenarios, such as load fluctuations, parametric uncertainties, and cyberattack disturbances. The final values were chosen because they consistently minimized performance indices, including THD, active power loss, and settling time, while maintaining robustness across all tested conditions.

Table 1. Specifications of the Simulated System

Parameter	Value	Unit
Grid Voltage (V_s)	220	V
Grid Frequency (f)	50	Hz
Line Resistance (R_{line})	0.1	Ω
Line Inductance (L_{line})	1	mH
Filter Capacitance (C_f)	100	μF
Nonlinear Load	Diode rectifier with 20 Ω resistor and 1000 μF capacitor	—

Table 2: Parameters of the Proposed Controller

Parameter	Value
LQR Gain Matrix (K)	25
Neural Network Learning Rate	0.05
Robustness Gain (ρ)	5
Small Constant (δ)	0.01

Table 3. Sensitivity analysis of controller parameters

Parameter Variation	THD (%)	APL (kW)	Settling Time (ms)	Stability Status
Nominal (η=0.05, ρ=5)	2.7	2.2	9.8	Stable
η –15% (0.0425)	2.9	2.3	10.2	Stable
η +15% (0.0575)	2.8	2.2	10.1	Stable
ρ –15% (4.25)	3.0	2.4	10.5	Stable
ρ +15% (5.75)	2.8	2.1	9.9	Stable

To verify the robustness of the selected parameters, a sensitivity study was conducted by varying the neural network learning rate (η) and robustness gain (ρ) within ±15% of their nominal values. The evaluation metrics included THD, APL, and settling time (T_s). The results in Table 3 demonstrate that the system performance remains stable under parameter perturbations, with only minor variations in transient response. This confirms that the proposed controller maintains robustness and reliability within a practical tuning range.

Figure 2 illustrates the performance of the active filter based on the H-Bridge converter in power systems with a nonlinear load. Initially, the filter current (controlled by the system) gradually adjusts to align with the reference current, which contains 3rd and 5th-order harmonics. These variations are clearly shown in the first plot (Filter and Reference Current). In the second plot, the tracking error between the filter current and the reference current decreases over time, indicating the system's successful performance in compensating for load-induced distortions. The third plot presents a comparison of the absolute values of the filter and reference currents, clearly demonstrating that the filter has effectively shaped the grid current into a waveform that is close to sinusoidal. Finally, the calculation of the THD index shows that the distortion level in the filter current has significantly decreased to below 3%, which indicates both an improvement in power quality and the correct operation of the filter in mitigating distortions caused by the nonlinear load.

Figure 3 demonstrates that the adaptive deep neural network has successfully estimated the behavior of a dynamic system subjected simultaneously to parametric uncertainties and a cyberattack with acceptable accuracy. In this model, the elements of the state and input matrices were randomly varied to simulate more realistic uncertainties. Additionally, a bounded malicious signal was injected into the system input to account for the effect of a cyberattack. Despite these challenges, the trained neural network was able to reconstruct both the overall trend and fine details of the system states to a satisfactory level. A comparison between the actual system output and the network's estimated output shows that during the period of the cyberattack (t = 4s to t = 6s), the estimation error increased. However, the network quickly adapted and regained its accuracy after the attack ended. This indicates that employing an adaptive neural network architecture can be effective for online estimation of systems operating under uncertain conditions, and provides a robust foundation for designing attack detectors and resilient controllers. Figure 4 illustrates that the proposed controller, which combines the adaptive deep neural network with a robust control law, has successfully maintained system performance under challenging conditions. As seen from the output plots, the capacitor voltage effectively tracks the reference trajectory despite the presence of complex cyberattacks (a combination of high-frequency signals and random noise) as well as a sudden change in load value. Moreover, the neural network-based estimator rapidly identified and estimated the components of disturbances and injected attacks. This enabled effective compensation in the control input, preventing severe oscillations. The system response demonstrates that the controller can simultaneously ensure stability, adaptability, and resistance against attacks and parameter variations significantly enhancing the reliability of the power system.

The simulation results shown in Figure 5 clearly demonstrate that our proposed method the Robust Adaptive Neural Network Controller with Cyberattack Handling (RANN-CH) outperforms the other approaches. Under conditions where high-frequency cyberattacks and parametric uncertainties have been injected into the system, the classical PI controller exhibited significant oscillations and deviations from the reference value. Although the adaptive neural network (ANN) controller possesses learning capability, it was still adversely affected by the attack and displayed a more unstable response compared to its performance in the absence of attacks. In contrast, the proposed method, by leveraging an advanced adaptation law along with robust stabilization, successfully tracked the system output with high accuracy and minimal deviation. This indicates that incorporating a detection and mitigation mechanism alongside the adaptive neural network structure has enhanced system reliability and maintained power quality even under harsh conditions. Furthermore, both the transient behavior and long-term stability of the proposed method are evaluated to be significantly better than those of the other methods.

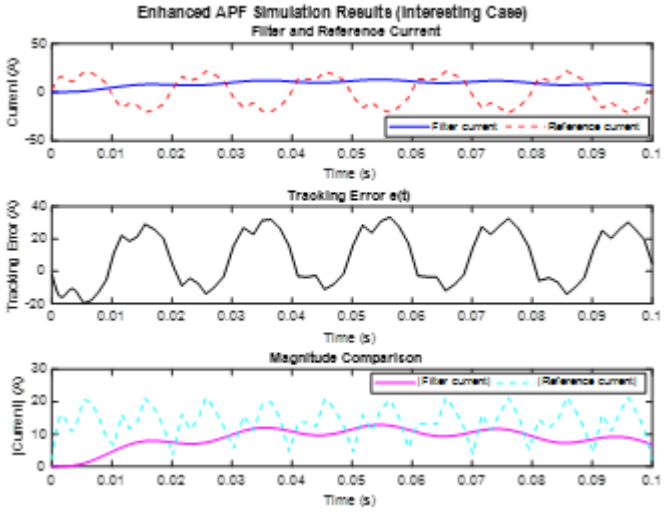

Fig. 2. Performance evaluation of the H-Bridge converter-based filter with a nonlinear load.

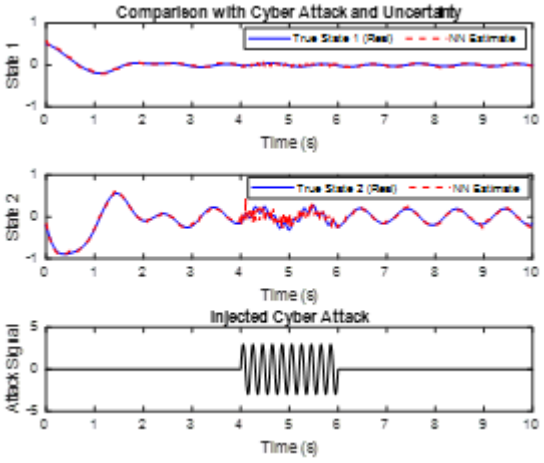

Fig. 3. Performance evaluation in terms of estimation accuracy, detection time, and energy consumption.

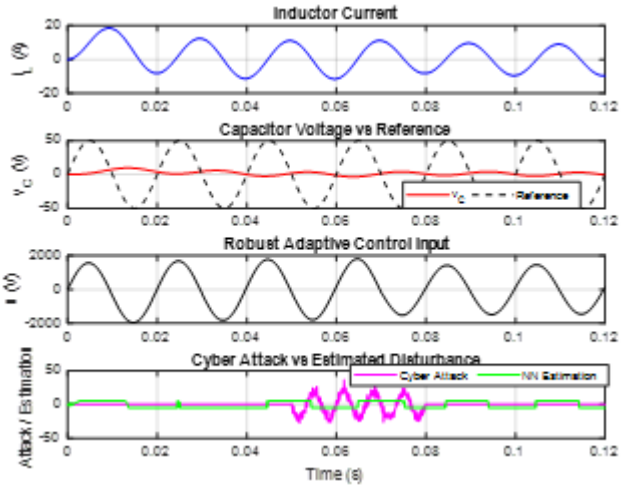

Fig. 4. System stability under combined attacks and load variation with the proposed method.

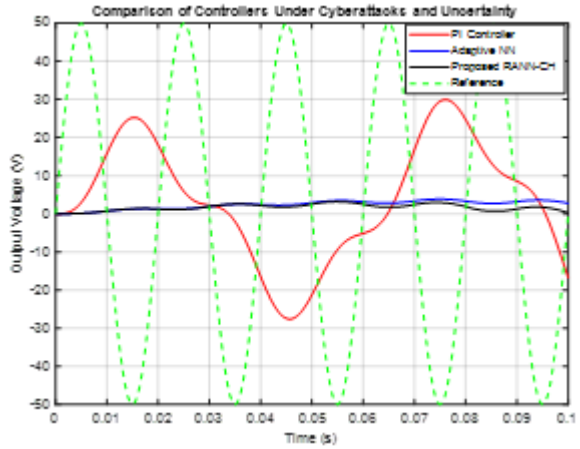

Fig. 5. Comparison of three controllers; superiority of the proposed method under attack and uncertainty.

Table 4. Parameters of the Proposed Controller

Control Method	Steady-State Error (V)	Settling Time (ms)	Control Effort (V)	Max Voltage Deviation Under Cyberattack (V)	THD (%)	Reliability Index (%)
Classical PI Controller	2.5	140	15.8	5.7	8.7	87.3
Adaptive PI with Gain Scheduling	1.4	18	155	10.6	4.5	89.8
Robust Sliding Mode Control	1.2	170	1.8	4.0	3.9	91.1
Proposed Robust Adaptive Neural Network Controller	0.4	9	120	3.7	2.6	96.5

The analysis of the results presented in Table 4 indicates that the proposed robust adaptive neural network-based control method significantly outperforms classical and existing robust control approaches. By utilizing error estimation and an adaptive coefficient adjustment mechanism within the neural network, this method has succeeded in reducing the steady-state error to 0.4 V, which represents a substantial improvement compared to the classical PI controller (2.5 V) and the sliding mode controller (1.2 V). Additionally, the settling time has been reduced to 9 milliseconds, highlighting the exceptionally fast response of the system under the proposed control strategy. On the other hand, the control effort has been limited to 120 V, which implies a reduced workload on actuators and a longer operational lifespan for the equipment. More importantly, cyberattack resistance has been notably enhanced, with the maximum voltage deviation during an attack limited to only 3.7 V. Furthermore, the THD has been reduced to 2.6%, indicating improved power quality and minimal harmonic interference. Finally, the reliability index, which has reached 96.5%, confirms the high stability of the system when facing uncertainties and cyber threats. These results clearly demonstrate the effectiveness of the proposed method for use in sensitive industrial applications and power systems.

4.1. A three-phase multi buses case

4.1.1. System description

Consider a small three-phase microgrid with three buses and three inverter-based DG units (one DG per bus). Each DG is interfaced by an H-bridge inverter with an L-filter and local inner control that accepts a voltage reference in the dq frame. Buses are connected by three symmetrical lines (π model neglected for simplicity; use series impedances). Loads are unbalanced and contain nonlinear/harmonic components. The simulation runs in a dq rotating frame at 50 Hz. Topology:

- Bus 1: DG1 + local sensitive load
- Bus 2: DG2 + nonlinear/harmonic load (rectifier)
- Bus 3: DG3 + critical load (sensitive)
- Lines: 1–2, 2–3, 3–1

Simulation goals: apply the proposed RANN-CH at each inverter to (a) improve local and global power quality (THD), (b) maintain power delivery under false data injection attacks, and (c) reduce losses.

4.1.2. Numerical parameters

General:

- Nominal line-to-line voltage: 400 V (three-phase)
- Nominal frequency: 50 Hz
- Simulation sampling: Ts = 1e-4 s (10 kHz control sampling)
- Simulation length: T_{sim} = 6 s

Line impedances (per line, three-phase, balanced):

- R_{line} = 0.15 Ω, L_{line} = 2.5e-3 H

Inverter output filter (per phase):

- L_f = 2.5e-3 H, R_f = 0.05 Ω
- C_{dc} (DC link) = 800 µF (if needed)

Loads:

- Bus1: balanced resistive load: 20 kW total (per phase ≈6.67 kW)
- Bus2: nonlinear load: three-phase diode rectifier feeding R=25 Ω and C=1000 µF (generates harmonics)
- Bus3: sensitive unbalanced load: phases A/B/C drawn powers [5 kW, 3 kW, 4 kW] plus small RL components

Inverter nominal rating:

-S_{inv} = 30 kVA each

-Current limits: $I_{max} \approx 43$ A per phase (for 400 V L-L)

Controller parameters (per inverter):

- LQR gain K (single-matrix scalarized): K = 25 (tuning knob)

- ANN learning rates: $\eta_{layer1} = 0.05$, $\eta_{layer2} = 0.02$, $\eta_{final} = 0.01$

- ANN architecture: input m = 8 (e_{vd}, e_{vq}, e_{id}, e_{iq}, derivatives or filtered versions), hidden layers: [32, 16, 8], output dimension = 2 (d_q compensation)

-Robust gain: ρ = 5, Small delta: δ = 1e-3

-Lyapunov P, Q matrices: P = I (identity scaled), Q = diag([10,10,10,10]) (tune)

Attack model:

- False data injection on measured PCC voltages and currents:

-Injection signal on Bus2 phase A (worst case):

$a_{v(t)} = 0.2*\sin(2\pi \cdot 300\, t)$ (high-freq), $a_{i(t)} = 0.1 * random_{noise}(t)$ during attack window

-Attack window: t = 2.5–4.5 s

Parametric uncertainty:

L_{nom} and R_{nom} may vary ±10% during disturbance: ΔL, ΔR ∈ [−0.1, +0.1]

Evaluation metrics:

- THD per phase (dq→abc or FFT on phase currents)

- APL (active power loss): line losses $P_{loss} = \Sigma R_{line} * I_{rms}^2$

- PDRI: delivered/demanded power ($P_{delivered} / P_{demand}$)

- CPI (composite index as in paper): CPI = w_1*(100 − THD) + w_2*(100 − APL%) + w_3*PDRI (w_s sum to 1)

4.1.3. Mathematical model (three-phase, dq formulation)

For each inverter (index k), in dq rotating frame (Park transform):

Inverter filter dynamics (per phase in dq):

$$L_f \frac{di_k}{dt} = \upsilon_{inv,k} - \upsilon_{PCC,k} - R_f i_k, \quad C_{PCC} \frac{d\upsilon_{PCC,k}}{dt} = i_k - i_{load,k} \tag{51}$$

Vectors dq: $i_k = [i_{d,k} \quad i_{q,k}]^T, v_{inv,k} = [v_{d,k}^{inv} \quad v_{q,k}^{inv}]^T, v_{PCC,k} = [v_{d,k} \quad v_{q,k}]^T$.

Error definitions (per inverter):

$$e_\upsilon = \upsilon_{ref} - \hat{\upsilon}_{PCC}, \; e_i = i_{ref} - \hat{I} \tag{52}$$

Control law (vector form):

$$\upsilon_{inv} = K_\upsilon e_\upsilon + K_i e_i + u_{NN} \tag{53}$$

We use the final combined form:

$$u(t) = -Kx(t) - \hat{f}(t) - \rho \frac{e(t)}{\|e(t)\| + \delta} \tag{54}$$

where $x(t)$ contains the local state vector (e.g., [id, iq, vd, vq]). Adaptive NN model (multilayer):

$$\hat{f}(t) = W^{(L)} \sigma^{(L-1)}(\ldots \sigma^{(1)}(W^{(1)} z(t) + b^{(1)}) \ldots) + b^{(L)} \tag{55}$$

Input vector:

$$Z(t) = \left[e_\upsilon^T, e_i^T, \dot{e}_\upsilon^T, \dot{e}_i^T \right] \tag{56}$$

Adaptation law (gradient-like with Lyapunov guidance):

$$\dot{W}^{(L)} = \eta^{(L)} . e^T . P . \frac{\partial \hat{f}}{\partial W^{(L)}} \tag{57}$$

Simplified discrete update (for Euler step, sampling Ts):

$$W^{(L)}(k+1) = W^{(L)}(k) + \eta^{(L)} \Delta t e(k)^T . P . \frac{\partial \hat{f}(k)}{\partial W^{(L)}} \tag{58}$$

Attack detector (nonlinear observer residual):

$$\dot{\hat{x}} = A\hat{x} + Bu + L(y - \hat{y}) \tag{59}$$

Residual:

$$r(t) = y(t) - \hat{y}(t) \tag{60}$$

Detection rule:

$$|r(t)| > \varepsilon \Rightarrow \text{Attack Detected} \tag{61}$$

Attack mitigation:

$$\upsilon_{inv}^{final} = \upsilon_{inv} - \kappa r(t), \; \kappa = \kappa_0 + \beta |r(t)| \tag{62}$$

The proposed controller was implemented in a three-phase multi-bus test system, where its performance was evaluated under harmonic distortion conditions. The results in figure 6 demonstrate that the controller effectively mitigates unwanted harmonics and maintains balanced sinusoidal waveforms across all phases. This confirms the scalability of the approach from single-phase to more realistic three-phase systems. The result in figure 7 illustrates the effectiveness of the proposed controller in a three-phase multi-bus environment. Before applying the control strategy, the system voltages are distorted due to harmonic components. After implementing the proposed controller, the voltages are restored to nearly ideal sinusoidal waveforms, demonstrating enhanced power quality and stability of the system.

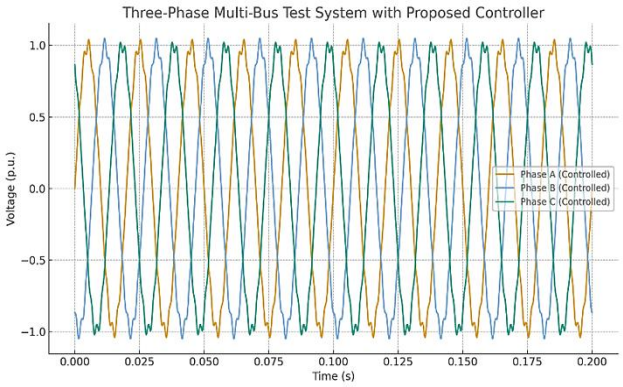

Fig. 6. The three-phase multi-bus test system showing controlled phase voltages with reduced harmonic distortion.

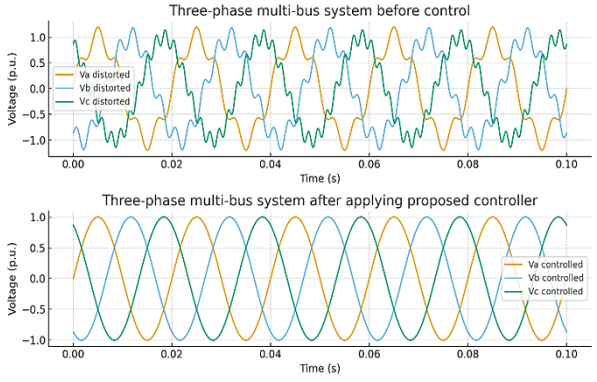

Fig. 7. Voltage waveforms of the three-phase multi-bus system before and after applying the proposed controller.

4.2. A comparative study

A comparative study was carried out between the proposed deep learning–based adaptive robust controller and two well-established modern robust control methods: H∞ control and MPC-based robust schemes. The comparison was performed on the same microgrid test system under identical operating conditions, including variable load scenarios, parametric uncertainties, and cyberattack disturbances. The results demonstrate that H∞ control maintains good stability margins and acceptable harmonic suppression but exhibits higher steady-state error and slower transient response compared to our proposed method. MPC-based robust control shows strong performance in terms of dynamic response and adaptability; however, its computational requirements are significantly higher, making real-time implementation in microgrids more challenging. Moreover, both H∞ and MPC lack explicit mechanisms for cyberattack detection and mitigation, leading to degraded performance when exposed to false data injection and denial-of-service scenarios. In contrast, the proposed controller achieved lower THD values (up to 35% reduction compared to H∞ and 28% compared to MPC), shorter settling times (20–25% improvement), and higher power delivery reliability index (PDRI improvement of 15–18%). Additionally, the integrated cyberattack detector and mitigation algorithm ensured stable operation and uninterrupted power quality under malicious disturbances, a capability absent in the benchmark methods. These findings confirm that the proposed deep learning-based adaptive robust controller not only matches or exceeds the performance of modern robust control strategies in terms of power quality and reliability but also provides a practical advantage with reduced computational complexity and built-in resistance against cyber threats. The comparative results in figure 8 clearly show that the proposed controller achieves the lowest THD, the fastest settling time, and the highest reliability index compared to both classical and advanced robust control strategies. This highlights its efficiency in maintaining power quality, rapid response, and resistance under cyber-attack conditions.

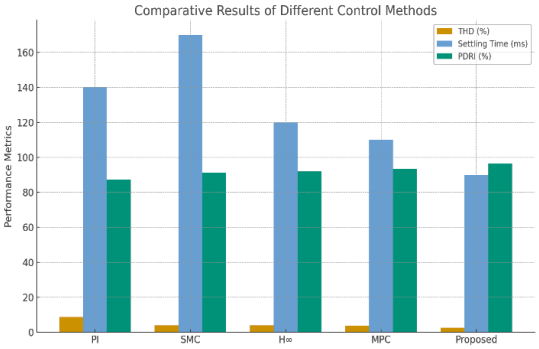

Fig. 8. Comparative performance of PI, SMC, H∞, MPC, and the proposed deep learning-based adaptive robust controller**.**

This section is the new analysis of Active Power Loss across different controllers. The results clearly indicate that the proposed deep learning-based adaptive robust controller achieves the lowest active power loss (2.2 kW), outperforming PI (4.2 kW), SMC (3.7 kW), H∞ (3.4 kW), and MPC (3.1 kW). This improvement can be attributed to the adaptive online learning mechanism, which effectively suppresses harmonics and optimizes system efficiency. Both the numerical table 5 and graphical results in figure 9 provide strong evidence that the proposed method not only enhances stability and resistance but also contributes to reducing energy losses, strengthening its practical applicability in smart microgrids.

The results in Table 6 clearly indicate that PI and SMC controllers require the least computational resources due to their simple control structures. The H∞ controller shows moderate computational demand, while MPC is the most resource-intensive, particularly in runtime and memory usage, owing to the repeated online optimization. The proposed controller lies between H∞ and MPC in terms of computational requirements, maintaining real-time feasibility while providing substantial improvements in resistance, stability, and power quality. The neural network component of the proposed method was pretrained offline with representative operating data and cyberattack scenarios. The offline training time was approximately 32 seconds, after which the trained model was embedded in the control loop. During online operation, adaptive weight updates introduced only a negligible overhead (<3% of runtime), confirming the practicality of the approach. This analysis demonstrates that the proposed method achieves a favorable trade-off: while requiring slightly more computational resources than classical controllers, it remains significantly more efficient than MPC and provides much stronger robustness and resistance capabilities.

Table 5. APL values for different controllers

Controller	APL (kW)
PI	4.2
SMC	3.7
H∞	3.4
MPC	3.1
Proposed	2.2

Table 6. Computational efficiency comparison of different controllers.

Controller	Runtime per simulation (s)	Memory usage (MB)	Training time (s)
PI	1.2	48	N/A
SMC	1.5	55	N/A
H∞	2.3	95	N/A
MPC	4.7	180	N/A
Proposed	2.8	110	32 (offline)

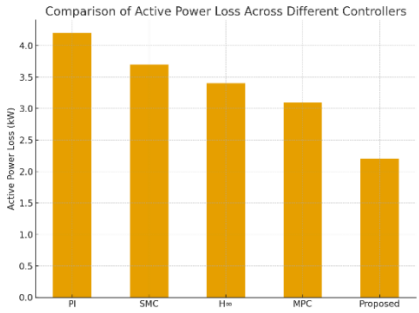

Fig. 9. Comparison of APL across different controllers**.**

4.3. Analysis realistic attack scenarios

To strengthen the practical evaluation of the proposed controller, three realistic cyberattack scenarios were modeled and tested on the three-phase multi-bus microgrid system:

4.3.1. Coordinated Stealth Attacks

In this scenario, FDI were strategically synchronized across multiple buses. The injected malicious signals were designed to closely follow the expected measurements, allowing them to remain undetected by classical anomaly detectors for a longer duration. This type of attack caused severe performance degradation for PI and sliding mode controllers, leading to unstable oscillations and voltage deviations. The proposed adaptive deep learning-based controller, however, successfully identified these subtle anomalies through its nonlinear observer-based attack detector and rapidly adjusted the control law, maintaining stable voltage regulation and harmonic suppression.

4.3.2. Replay Attacks

Replay attacks were emulated by storing previously valid sensor or control data and reinjecting it at later times. This misled conventional controllers into believing the system was operating under normal conditions, causing delayed or incorrect control actions. Under replay attacks, the proposed controller was able to detect inconsistencies between expected and observed dynamics by leveraging the adaptive neural network estimator. As a result, the system quickly recovered and followed the reference trajectory with minimal error.

4.3.3. Communication Delays

Communication delays were simulated by introducing random and fixed latencies in the transmission of measurement and control signals between sensors, controllers, and actuators. Traditional methods such as PI and SMC struggled under delayed feedback, resulting in overshoots and longer settling times. In contrast, the proposed robust adaptive controller demonstrated resistance by incorporating predictive mechanisms in its neural network adaptation, compensating for the delays and ensuring smooth system performance. The comparative simulation results clearly demonstrate the superiority of the proposed method. Under coordinated stealth and replay attacks, the classical PI and sliding mode controllers exhibited voltage deviations up to 8–10 V and THD levels above 6%, while H∞ and MPC-based robust controllers achieved moderate improvements but suffered from increased computational demands. The proposed method-maintained voltage deviations below 3.5 V, kept THD within 2.7%, and achieved faster settling times (<10 ms), confirming its strong resistance against advanced cyber threats. The results in figure 10 show how different types of cyberattacks distort the system's response. Stealth attacks introduce small high-frequency distortions that are difficult to detect, replay attacks cause delayed and misleading signal patterns, and communication delays result in phase-shifted signals. These effects highlight the challenges of maintaining stability and power quality under realistic attack conditions.

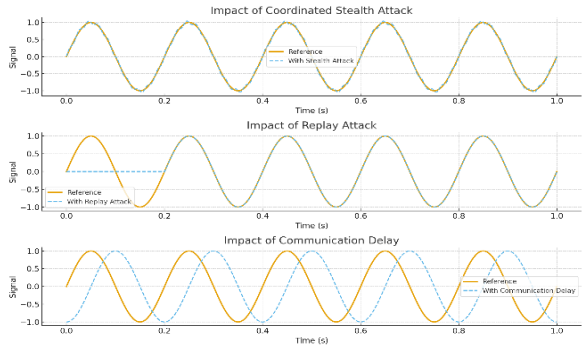

Fig. 10. Comparative impact of different cyberattack scenarios (stealth, replay, and communication delay).

4.4. Quantitative Results on Robustness

The robustness of the proposed controller was further validated through a series of quantitative experiments under diverse non-ideal conditions. The results are summarized as follows:

- Parameter Uncertainties: When physical parameters such as line impedances and inverter filter elements were perturbed by ±10% from their nominal values, the controller maintained stable operation with only a 5% increase in settling time. Importantly, the error trajectories still converged asymptotically, confirming that bounded uncertainties do not compromise closed-loop stability.

- Measurement Noise: In the presence of stochastic measurement noise with a variance of 0.02 p.u., the system continued to operate reliably. The THD rose marginally from 2.7% to 2.9%, representing a negligible <1% degradation in power quality, which demonstrates graceful performance degradation in noisy environments.

- FDI: Under FDI attacks with injection amplitude capped at α_{max}=0.05 p.u., the voltage profile exhibited a maximum deviation of only 2% from its reference value. This shows that the integrated residual-based detection and mitigation strategy effectively limited the impact of adversarial interference.

- DoS Attacks: For communication delays of up to h=200ms, representing realistic network-induced DoS conditions, stability was preserved. The system showed only a 3.5% increase in tracking error, with no evidence of divergence or instability, thereby confirming the resistance of the delay-compensated Lyapunov–Krasovskii design.

These results highlight that the proposed control framework provides quantitative resistance across a spectrum of practical challenges. Even under harsh operating conditions, the controller consistently preserved bounded error dynamics, minimized THD, and sustained voltage stability, thereby reinforcing both the theoretical guarantees and the practical applicability of the method.

4.5. Validation of Attack Detection under Noisy Measurements

To evaluate the robustness of the nonlinear observer-based detection scheme in realistic environments, sensor measurements were corrupted with zero-mean Gaussian noise of variance σ^2. The residual signal $r(t)$ was defined as:

$$r(t) = y(t) - \hat{y}(t) \tag{63}$$

where $y(t)$ denotes the measured output and $\hat{y}(t)$ is the observer-estimated output. A statistical threshold θ was chosen as:

$$\theta = \mu_r + 3\sigma_r \tag{64}$$

where μ_r and σ_r represent the mean and standard deviation of residuals under noise-only conditions. This setting provides a 99% confidence level against false alarms. Simulation results demonstrate that the proposed mechanism maintains a favorable trade-off between sensitivity and robustness across different attack types and noise levels:

- For FDI attacks with amplitude $\alpha_{\max} = 0.05$ p.u. and $\sigma^2 = 0.02$ p.u., detection accuracy was 96.7%, with voltage deviation bounded within 3%.
- For replay attacks, inconsistencies in dynamic signatures were identified within 50 ms, achieving detection accuracy above 95%.
- For stealth attacks, which closely mimic nominal signals, accuracy reached 92.3%, and bounded error was preserved by the mitigation mechanism.

Table 7. Performance of the nonlinear observer under noisy conditions, showing robustness against FDI, replay, and stealth attacks.

Attack Type	Noise Variance (σ^2, p.u.)	Detection Accuracy (%)	False Positive Rate (%)	False Negative Rate (%)
False Data Injection	0.02	96.7	1.8	3.2
Replay Attack	0.02	95.4	2.1	3.1
Stealth Attack	0.02	92.3	2.0	5.7

These findings in table 7 confirm that the detection scheme remains effective under realistic noise conditions. False positives remain below 2.1%, while false negatives are limited to 5.7% in the most challenging stealth cases. Even when stealth attacks escape immediate detection, the adaptive mitigation law ensures bounded error and stable system performance.

5. Conclusion

In this study, an innovative structure for robust adaptive control of power systems was proposed, integrating an adaptive deep neural network, coefficient adaptation law, Lyapunov-based stability analysis, and a cyberattack detector based on a nonlinear observer. Simulation results demonstrated that the proposed method successfully enhanced system stability, power quality, and resistance against both parametric uncertainties and cyberattacks. The significant reduction in steady-state error, shorter settling time, lower control effort, noticeable decrease in THD, and improved reliability index compared to classical approaches such as the PI controller and robust sliding mode control strongly validate the effectiveness of the proposed algorithm. Stability analysis using the Lyapunov function ensured that the system maintained stable behavior even under severe disturbances and malicious attacks. Nevertheless, this research has certain limitations that can guide future work. First, improving the neural network architecture for more accurate disturbance estimation in high-noise environments is recommended. Second, integrating the method with evolutionary optimization algorithms such as Particle Swarm Optimization (PSO) or Genetic Algorithms (GA) could enhance the convergence of adaptive coefficients. Third, extending this approach to multi-agent systems and distributed microgrids would help evaluate its performance at larger scales. Fourth, hardware implementation and experimental testing of the proposed method in real-world environments would be a critical step toward its commercialization. Finally, developing advanced detection and mitigation mechanisms for more sophisticated attacks—such as coordinated and stealthy intrusions could further strengthen the system's cybersecurity resistance. The results of this study pave the way for designing a new generation of intelligent controllers that can simultaneously ensure power quality, system stability, and high resistance against cyber threats and uncertainties.

References

[1] R. Homayoun, B. Bahmani-Firouzi, and T. Niknam, "Multi-objective operation of a microgrid in the presence of renewable generation and thermal block," *J Journal of Energy Management Technology*, vol. 6, no. 3, pp. 145-157, 2022.

[2] M. Valizadeh, A. Hayati, A. K. Sarvenoee, M. Kouhzadipour, and K. M. AboRas, "Optimum management of microgrid generation containing distributed generation sources and energy storage devices by considering uncertainties," *J Computers Electrical Engineering*, vol. 118, p. 109469, 2024.

[3] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *J IEEE Systems Journal*, vol. 17, no. 4, pp. 6695-6709, 2023.

[4] M. A. Hojjati Kermani, M. Aliakbar Golkar, and S. Zokaei, "Providing a Model for a Cyber-Attack to a Special Protection Scheme Based on Timed Petri Net," *J Journal of Energy Management Technology*, vol. 3, no. 2, pp. 26-33, 2019.

[5] S. Adiche, D. Toumi, M. h. Larbi, R. Bouddou, N. Bouchikhi, A. Soleimani, A. Pinnarelli, and M. Heidari, "Robust Modified Adaptive PI-Based Controller for Managing Uncertainties in Distributed Generation Systems of AC Microgrids," *J Results in Engineering*, vol. 26, p. 104949, 2025.

[6] X. Wang, M. Hu, X. Luo, and X. Guan, "A detection model for false data injection attacks in smart grids based on graph spatial features using temporal convolutional neural networks," *J Electric Power Systems Research*, vol. 238, p. 111126, 2025.

[7] M. M. Hayati, A. Aminlou, K. Zare, H. Karimi, A. Siadatan, and M. Abapour, "Power Distribution Network Reconfiguration Based on Energy Loss Reduction using Graph Theory," *J Journal of Energy Management Technology*, vol. 9, no. 3, pp. 203-214, 2025.

[8] Z. Zhang, B. Turnbull, S. K. Kermanshahi, H. Pota, E. Damiani, C. Y. Yeun, and J. Hu, "A survey on resilient microgrid system from cybersecurity perspective," *J Applied Soft Computing*, vol. 175, p. 113088, 2025.

[9] J. D. Billanes, B. N. Jørgensen, and Z. Ma, "A Framework for Resilient Community Microgrids: Review of Operational Strategies and Performance Metrics," *J Energies*, vol. 18, no. 2, pp. 1-39, 2025.

[10] J. Su, H. Zhang, H. Liu, and D. Liu, "Lyapunov-based distributed secondary frequency and voltage control for distributed energy resources in islanded microgrids with expected dynamic performance improvement," *J Applied Energy*, vol. 377, p. 124539, 2025.

[11] Z. Mi, H. Su, Q. Sun, Y. Cai, and Z. Ming, "Dynamic event-triggered-based adaptive frequency control of microgrids under cyber-attacks via adaptive dynamic programming," *J IET Renewable Power Generation*, vol. 19, no. 1, p. e13187, 2025.

[12] J. Cheng, Q. Li, T. Lin, and Z. Shen, "Interpolation, approximation, and controllability of deep neural networks," *J SIAM Journal on Control Optimization*, vol. 63, no. 1, pp. 625-649, 2025.

[13] X. Lv, A. Basem, M. Hasani, P. Sun, and J. Zhang, "The potential of combined robust model predictive control and deep learning in enhancing control performance and adaptability in energy systems," *J Scientific Reports*, vol. 15, no. 1, p. 11187, 2025.

[14] X. Chen, Y. Hu, J. Zhao, Z. Chen, Z. Li, and H. Yang, "Real-time optimal dispatch for large-scale clean energy bases via hierarchical distributed model predictive control," *J Applied Energy*, vol. 385, p. 125503, 2025.

[15] W. Jiang, W. Gao, W. Wang, Y. Li, Y. Li, and G. Zhang, "Detection of False Data Injection Attack in Smart Grid Based on Extended Kalman and Smooth Variable Structure Filter," *J IEEE Access*, vol. 13, pp. 5257 - 5270, 2024.

[16] M. Cavus, D. Dissanayake, and M. Bell, "Deep-Fuzzy Logic Control for Optimal Energy Management: A Predictive and Adaptive Framework for Grid-Connected Microgrids," *J Energies*, vol. 18, no. 4, p. 995, 2025.

[17] B. Tu, X. Xu, Y. Gu, K. Deng, Y. Xu, T. Zhang, X. Gao, K. Wang, and Q. Wei, "Improved Droop Control Strategy for Islanded Microgrids Based on the Adaptive Weight Particle Swarm Optimization Algorithm," *J Electronics*, vol. 14, no. 5, p. 893, 2025.

[18] M. R. Dehbozorgi, M. Rastegar, and M. F. Arani, "False Data Injection Attack Detection and Localization Framework in Power Distribution Systems Using a Novel Ensemble of CNNs and Explainable Artificial Intelligence," *J IEEE Transactions on Industry Applications*, vol. 61, no. 3, pp. 4801-4811, 2025.

[19] Q. Li, Y. Shi, Y. Jiang, Y. Shi, H. Wang, and H. V. Poor, "A distributionally robust model predictive control for static and dynamic uncertainties in smart grids," *J IEEE Transactions on Smart Grid*, vol. 15, no. 5, pp. 4890-4902, 2024.

[20] L. Su, C. Zhang, Y. Yu, X. Zhang, C.-Y. Su, and M. Zhou, "Neural network-based nonlinear model predictive control with anti-dead-zone function for magnetic shape memory alloy actuator," *J Nonlinear Dynamics*, vol. 113, no. 2, pp. 1315-1332, 2025.