Energy Systems Planning and Optimization

Journal home page: https://espo.kut.ac.ir

Research paper

Adaptive Neuro-Fuzzy Control for Enhancing DC-Link Voltage Stability and Security in Renewable-Integrated Distribution Networks under Advanced False Data Injection Attacks

Omar Mohammad, Mehdi Ahmadi Jirdehi*

Department of Electrical Engineering, Faculty of Electrical Engineering, Kermanshah University of Technology, Kermanshah, Iran

Article Info

Received
2 Jan 2026

Revised
29 Jan 2026

Accepted
16 March 2026

Published online
04 April 2026

Keywords

Grid-connected microgrid;
DC-link voltage stability;
False Data Injection Attack (FDIA);
Adaptive Neuro-Fuzzy Inference System (ANFIS) controller

Abstract

As distributed generation units and renewable energy sources become increasingly integrated into modern power systems, ensuring the stability of the DC-link voltage—especially in the presence of potential cyber threats-poses a significant challenge. Traditional control methods, such as proportional-integral (PI) controllers, and even many contemporary intelligent algorithms, often struggle to maintain performance under unexpected cyberattacks or falsified data due to their reliance on accurate system models or extensive retraining. This study proposes an Adaptive Neuro-Fuzzy Inference System (ANFIS)-based control strategy that merges the adaptive learning ability of neural networks with the robustness of fuzzy logic, enabling real-time adjustment of control parameters. The primary contribution of this approach is its capacity to autonomously detect and mitigate sophisticated cyber threats including False Data Injection Attacks (FDIA), Denial-of-Service (DoS) attacks, and cyber-induced load fluctuations without the need for predefined system models or extensive retraining. Simulation results on the IEEE 13-bus network with integrated solar and wind generation, implemented in MATLAB/Simulink, show that the proposed controller significantly improves DC-link voltage stability, shortens recovery time, and enhances overall network resilience compared to conventional PI and other intelligent controllers. These findings highlight that the ANFIS-based controller effectively addresses the limitations of traditional methods, offering a practical and robust solution for modern smart and resilient power grids.

*Mehdi Ahmadi Jirdehi: m.ahmadi@kut.ac.ir

 https://doi.org/10.22034/espo.2026.2082853.1003

1. Introduction

The rapid expansion of renewable energy resources and distributed generation within power systems has underscored the need to reconsider existing control strategies. The DC-link voltage, as a critical component of power converters, plays a pivotal role in maintaining stable and reliable energy exchange. Any fluctuation or instability in this section can disrupt the entire network, degrade power quality, and even trigger large-scale outages. Meanwhile, the growing use of digital technology and interconnection of power systems through communication networks have rendered contemporary grids more vulnerable to sophisticated cyber–physical attacks. Such threats can manipulate measurement data and control signals, thereby compromising the performance of converters and microgrids and ultimately endangering energy security. Under these circumstances, the development of innovative control solutions capable of simultaneously addressing uncertainties stemming from renewable energy sources and cyber threats has become more crucial than ever. Conventional controllers, such as PI regulators, along with numerous current intelligent methods, often demonstrate limited effectiveness against complex attacks due to their dependence on accurate modeling or the need for frequent retraining.

To address these challenges, the present study introduces an adaptive framework based on an Adaptive Neuro-Fuzzy Inference System (ANFIS). This approach integrates the learning ability of neural networks with the robustness of fuzzy logic, enabling real-time tuning of control parameters and improving network resilience against various cyber threats. Consequently, the findings of this research not only contribute to improving the stability and security of microgrids but also provide a practical foundation for the development of resilient, future-oriented smart grids. A review of recent studies further indicates that extensive efforts have been made in recent years to enhance DC-link voltage stability in grid-connected microgrids, underscoring the continued importance of this research domain. In [1], a comprehensive review of the challenges associated with energy management and power sharing in hybrid AC/DC microgrids was presented. The study highlighted the critical role of interlinking converter dynamics while addressing issues such as voltage fluctuations and the complexity of control in hybrid environments. However, it lacked a real-time adaptive mechanism to ensure DC-link stability under cyber threats. Subsequently, research in [2] proposed a control strategy for boost converters using a CFLC compensator, resulting in a system efficiency exceeding 92%. Although this method improved transient response and enhanced stability, it was still vulnerable to cyberattacks since it relied on an accurate model and attack-free operating conditions. In recent years, passivity-based approaches have also gained considerable attention. For example, [3] utilized an energy-storage-based control scheme to guarantee output voltage stability in a fuel cell/boost converter system. While this approach proved highly effective in maintaining dynamic stability, it failed to incorporate data-driven attack scenarios that could destabilize the DC-link voltage. Similarly, study [4] proposed a two-stage control strategy for grid-connected PV converters, resulting in high precision in DC-

link voltage regulation. Nevertheless, the method lacked any layer for detecting or mitigating cyberattacks, making it insufficient for today's intelligent and resilient microgrid environments. On the other hand, several studies have specifically addressed cybersecurity threats in power systems. In [5], it was demonstrated that False Data Injection Attacks (FDIAs) can disrupt the hierarchical control of microgrids, leading voltage and frequency irregularities. Similarly, research in [6] modeled Denial-of-Service (DoS) attacks and showed that such intrusions can severely affect power distribution and overall system stability. Although these studies highlighted the significance of cyber threats, none of them proposed a resilient control mechanism to ensure DC-link voltage stability under such conditions.

In this regard, studies such as [7] and [8] proposed adaptive neuro-fuzzy controllers for power converters and power quality enhancement, proving that the integration of neural networks with fuzzy logic can improve dynamic performance. However, these works were primarily concerned with local power quality and dynamic stability, without considering the cybersecurity dimension in their control design. Furthermore, study [9] employed Long Short-Term Memory (LSTM) networks to detect and mitigate FDIAs in fully converter-based microgrids, showing that replacing compromised setpoints can help maintain system voltage stability. While this approach proved effective in attack detection, it did not provide a dynamic control solution for sustaining DC-link stability.

Finally, researchers in [10] conducted a systematic review of cyber-resilience strategies in renewable-based microgrids and emphasized the necessity of co-designing control and security mechanisms. However, this contribution remained largely theoretical. Several other studies have also focused directly on improving DC-link voltage stability, reflecting the growing research interest in this area. In [11], several methods were explored to mitigate fluctuations caused by solar generation; however, cyberattack scenarios were not considered. Study [12] proposed a learning-based algorithm for the detection and mitigation of False Data Injection Attacks (FDIAs), yet the algorithm was not integrated into the DC-link voltage control loop and was confined to the detection level. Similarly, the neuro-fuzzy controllers presented in [13] and the deep reinforcement learning–based control approach in [14] improved voltage and power stability under normal conditions; nevertheless, the former was limited to power damping issues, while the latter incurred high data and retraining costs. In [15], a supervisory system for hybrid microgrids wasput forward, focusing primarily on energy management and economic optimization rather than the security of the DC-link voltage loop. Cybersecurity aspects were more prominently addressed in [16] and [17]. The former classified attacks targeting converters and analyzed their impact on system stability, while the latter investigated delay-induced attacks, emphasizing the need for real-time resilience mechanisms. Although these studies effectively modeled various threats, they did not develop a control design capable of maintaining DC-link voltage stability under active cyberattacks. Along the same line, [18] and [19] employed Adaptive Neuro-Fuzzy Inference Systems (ANFIS) to enhance the performance of boost converters and three-phase

inverters, resulting in better dynamic stability and power quality. However, neither study considered cybersecurity scenarios nor established a direct connection to the grid-side dq-frame control architecture.

In summary, a review of recent research reveals that despite significant progress in intelligent control and cyberattack analysis, a substantial gap still exists between attack detection and the design of a resilient control loop capable of maintaining DC-link voltage stability. The present work's originality lies precisely in its ability to bridge this gap. The proposed ANFIS-based controller, trained with both clean and compromised data, dynamically adjusts its neuro-fuzzy rules in real time. This capability enables stable DC-link voltage operation even under complex cyberattack scenarios, eliminating the need for precise system modeling or extensive retraining. Therefore, this research not only represents a more practical advancement compared to previous studies,but it also introduces a novel framework for improving the cyber-resilience of next-generation smart microgrids.

2 . Background and Conceptual Model of the Research

The growing use of renewable energy sources such as photovoltaic (PV) systems and wind turbines in modern power networks, has created new challenges to the dynamic stability of these systems. In contemporary microgrids, the DC-link voltage as a critical component of power converters plays a vital role in facilitating power exchange between AC and DC sub-networks. Any fluctuation or deviation in this voltage can lead to converter instability, deterioration of power quality, and a reduction in the overall reliability of the grid. At the same time, the growing dependence of power systems on communication infrastructures and digital control platforms has made them vulnerable to cyber–physical attacks. Attacks such as False Data Injection Attacks (FDIAs) and Denial-of-Service (DoS) can manipulate sensor data or control signals, thereby severely disrupting the stability of the DC-link voltage. Conventional methods, including PI controllers and even many modern intelligent approaches, exhibit limited effectiveness against such threats due to their reliance on precise modeling and lack of real-time adaptability. In response to these challenges, the present study proposes an intelligent framework based on an Adaptive Neuro-Fuzzy Inference System (ANFIS), which integrates the learning capabilities of neural networks with the robustness of fuzzy logic to enable real-time tuning of control parameters. By simultaneously analyzing both DC-link voltage error and output power error, the proposed controller can identify and compensate for the effects of cyberattacks as well as instantaneous network variations. As illustrated in Figure (1), the conceptual model of the research consists of three main layers, each responsible for a specific functional process within the adaptive and resilient control framework.

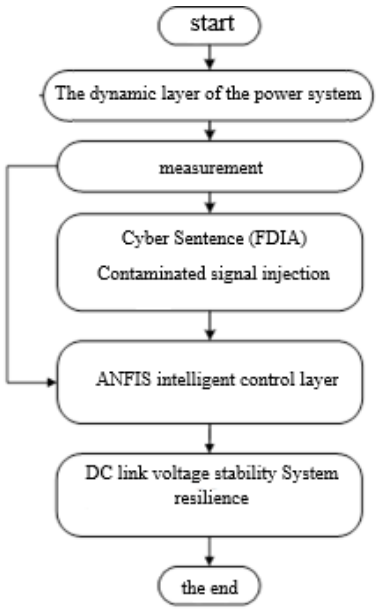

Fig. 1. Conceptual three-layer model of the proposed ANFIS-based framework for DC-link voltage stability in hybrid microgrids.

1. Power System Dynamics Layer – This layer represents the physical part of the system, including renewable energy sources, power converters, and the DC-link, which together define the dynamic behavior of the network.
2. Cyber–Physical Attack Layer – This layer models data-driven threats, simulating intrusion paths and attack mechanisms that can compromise communication and control signals within the system.
3. Intelligent ANFIS Control Layer – Relying on real-time input data (voltage and power errors) and fuzzy inference rules, this layer generates an adaptive corrective control signal to maintain the DC-link voltage at its reference value.

This three-layer structure establishes a novel framework that integrates cybersecurity, power stability, and adaptive learning, offering a unified and resilient control strategy for the next generation of smart microgrids.

3. Modeling and Problem Formulation

In accordance with the study's objectives which include enhancing DC-link voltage stability in grid-connected microgrids under cyber, physical attacks and developing an intelligent ANFIS-based controller to improve system resilience, the dynamic model of power converters and the DC-link voltage is first examined. Subsequently, the control problem and the proposed system structure are mathematically formulated to serve as the foundation for designing the adaptive controller.

3.1. DC-Link Dynamic Model

In grid-connected microgrids integrated with renewable energy sources, the DC-AC interlinking converter serves as the interface for energy transfer between the DC and AC subnetworks. The dynamic behavior of the DC-link voltage depends on the input current from renewable sources (such as PV or wind systems) and the output current injected into the power grid. The differential equation governing the DC-link voltage dynamics can be expressed as follows [18]:

$$C_{dc}\frac{dV_{dc}}{dt} = I_{in} - I_{out} \tag{1}$$

Where:

- C_{dc} : DC-link capacitance,
- V_{dc} : DC-link voltage,
- I_{in} : input current injected from the renewable energy source,
- I_{out} : output (or injected) current delivered to the AC grid.

Under steady-state conditions, the input and output currents are equal ($I_{in} = I_{out}$), and the DC-link voltage is constant at its reference value ($V_{dc,ref}$). Any deviation from this balance results in DC-link voltage oscillations, which can adversely affect system stability.

3.2. Grid-Side Converter Model

The grid-side converter (GSC) is responsible for controlling the active and reactive power injected into the grid. Its dynamic model in the synchronous rotating dq reference frame is expressed as follows [18]:

$$L_f\frac{di_d}{dt} = -R_f i_d + \omega L_f i_q + v_d - v_{gd} \tag{2}$$

$$L_f\frac{di_q}{dt} = -R_f i_q - \omega L_f i_d + v_q - v_{gq} \tag{3}$$

Where:

- i_d, i_q: The current components in the d and q axes,
- v_d, v_q :Converter output voltages,
- v_{gd}, v_{gq}: Network voltages,
- R_f, L_f Output filter inductance and resistance,
- ω : The angular velocity of the network is.

Active power and reactive injection are calculated from the following equation

$$P = \frac{3}{2}(v_d i_d + v_q i_q) \quad , \quad Q = \frac{3}{2}(v_q i_d - v_d i_q) \tag{3}$$

The controller aims to maintain the DC-link voltage at its reference value by regulating the active current, while the reactive current is used to control reactive power.

3.3. Cyber-physical attack model

To provide a better understanding for readers less familiar with cybersecurity modeling, the attack parameters used in this study are physically interpreted as follows: the magnitude represents the intensity or amplitude of the injected signal affecting the system, while the frequency range indicates how rapidly the attack signal varies over time. These parameters collectively characterize the severity and temporal behavior of potential attacks, allowing the reader to compare the modeled scenarios to real-worldcyber threats in power systems.

In this study, three types of data attacks are considered [20]:

1. Fixed fake data injection attack (Constant FDIA):

$$V_{dc}^{meas} = V_{dc}^{true} + \Delta \tag{4}$$

2. Sinusoidal oscillatory injection attack:

$$V_{dc}^{meas} = V_{dc}^{true} + A\,sin(\omega_a t) \tag{5}$$

3. Combined attack (Sinusoidal + Constant):

$$V_{dc}^{meas} = V_{dc}^{true} + \Delta + A\,sin(\omega_a t) \tag{6}$$

Where:

- V_{dc}^{meas} : Measured and contaminated quantity,
- V_{dc}^{true}: The actual voltage value,
- Δ : Fixed data injection bias,
- A: ω_a The range and frequency of attacks are.

These attacks lead to feedback signal distortion and malfunction of conventional controllers.

3.4. ANFIS Control Problem Formulation

The proposed ANFIS controller demonstrates a relatively low online computational burden, as the inference process mainly involves simple fuzzy rule evaluations and weighted summations. Once the ANFIS parameters are trained offline, the real-time implementation does not require iterative optimization or heavy numerical computations. Therefore, the proposed controller is well suited for real-time applications, particularly in power system control environments with limited computational resources and strict timing constraints.

The objective of designing the ANFIS controller is to maintain the stability of the DC-link voltage in the presence of cyberattacks and load variations. The input variables of the controller are as follows:

$$x_1 = e_{VDC} = V_{dc,ref} - V_{dc}^{meas} \quad , \quad x_2 = e_{Pload} = P_{ref} - P_{load} \tag{7}$$

which are fed to the ANFIS network to produce the adaptive control output (u(t)):

$$u(t) = f_{ANFIS}(x_1, x_2) \tag{8}$$

The control signal u(t) is applied to the converter, regulating the i_d current to maintain the DC-link voltage at its reference value. Gaussian membership functions are employed for the fuzzy logic system, and the network weights are updated using the Levenberg–Marquardt optimization algorithm to minimize the mean squared error (MSE).

$$MSE = \frac{1}{N}\sum_{k=1}^{N}\left(V_{dc,ref} - V_{dc}(k)\right)^2 \tag{9}$$

3.5. Control Optimization Objective

Ultimately, the control task is formulated as an optimization problem

$$minu(t) J = \int_0^T \left[(V_{dc,ref} - V_{dc})^2 + \lambda(u(t))^2\right] dt \tag{10}$$

Here, λ serves as a weighting factor to constrain the control signal within allowable limits. The ANFIS controller is trained to minimize the cost function J while simultaneously ensuring voltage stability and a fast system response.

4. Discussion and analysis of simulation results

To comprehensively evaluate the proposed solution, a series of simulations were conducted on the standard IEEE-13 bus network, where a photovoltaic (PV) unit and a wind farm are simultaneously connected to the grid. This configuration represents a realistic example of a distributed generation system connected to the network, in which the stability of the DC link voltage is crucial for ensuring reliable power transfer and the proper functioning of converters. Figure (2) illustrates the schematic of the system, depicting the power exchange pathways, converters' locations, and the placement of the DC link capacitor in the presence of renewable energy sources. The dynamic model of the grid-side converter is implemented within the framework described in the section "Modeling and Problem Formulation," and its connection with the dynamics of the DC link is established. Active/reactive power control is achieved through current i_d/i_q components to maintain the DC link voltage steady around a $V_{dc,ref}$ reference.

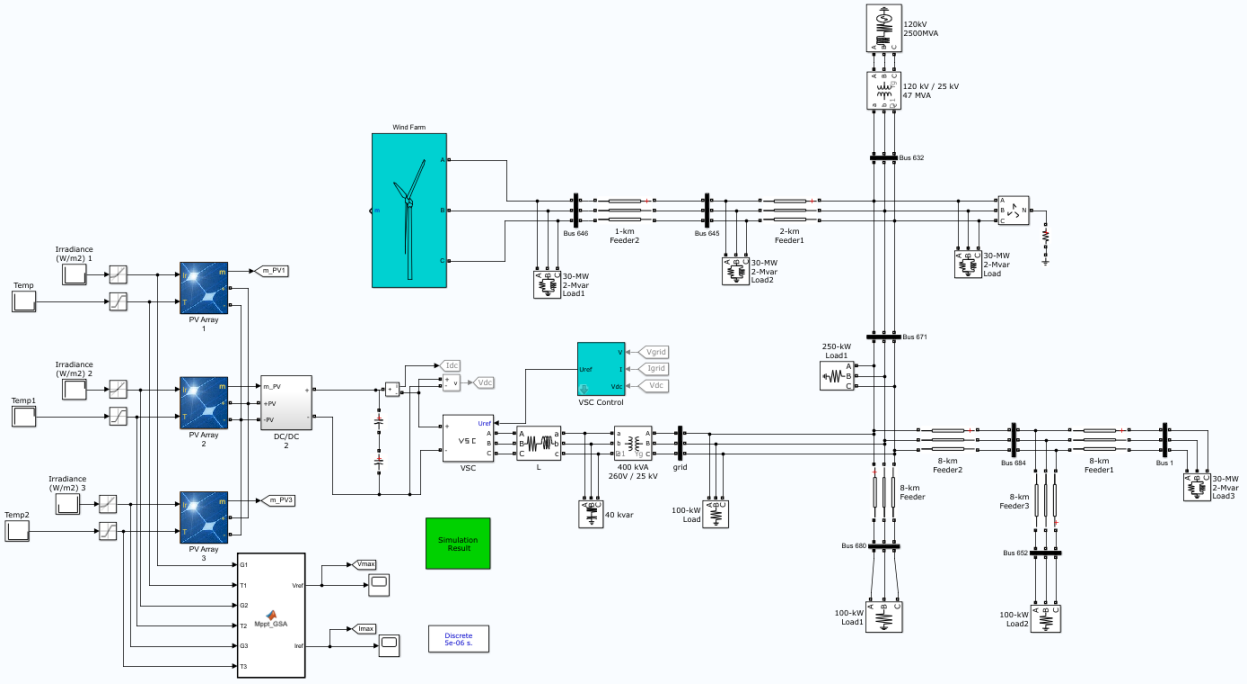

Fig. 2. Schematic view of the IEEE-13-bus test system with integration of photovoltaic and wind systems.

The proposed ANFIS-based controller was validated from both structural and performance perspectives. From a structural standpoint, the control inputs were defined as the DC link voltage error and the output power error, allowing the controller to respond simultaneously to voltage deviations and load changes. From a performance perspective, a series of scenarios were executed, including load variations (small/medium/large steps), fluctuations in the power injected by renewable sources, measurement noise, and, importantly, data-driven cyber-physical attacks. The ANFIS algorithm utilized Gaussian membership functions and updated parameters based on Levenberg-Marquardt optimization to produce the modified control signal at each moment. This arrangement enables the controller to adjust the system's behavior in the presence of disturbances and attacks without relying heavily on an accurate model or requiring costly retraining. To assess performance, the following evaluation metrics were monitored during the simulations: settling time V_{dc} defined as the time taken to return to the vicinity of the reference after a disturbance; maximum overshoot M_p to measure the risk of transient overvoltage; steady-state error e_{ss} as a metric for regulation accuracy; voltage/current ripple in the power frequency band (as a power quality index); and control cost $\int u^2 dt$ which indicates the balance between performance and control effort. These metrics were measured both under normal conditions and during data-driven attacks, and they were compared across three scenarios: "proposed ANFIS controller," "conventional PI controller," and "no adaptive control." In the first step, the system's behavior under normal operating conditions was examined. The results showed that the ANFIS controller quickly dampens voltage fluctuations in the DC link caused by

variations in PV wind power and load steps, remaining short in such a way that T_s remains short and M_p limited and the residual error is negligible. This behavior can be observed in Figures (3) and (4): the DC link voltage stabilizes around the reference, currents are maintained within permissible limits, and the active output power remains consistent and free from large-scale fluctuations. In the same scenarios, using only PI control results in longer settling times and greater sensitivity to converter parameter variations; particularly in the presence of measurement noise, voltage ripple, and persistent deviations increase, indicating the limitations of linear methods when dealing with the nonlinear dynamics of the AC/DC link.

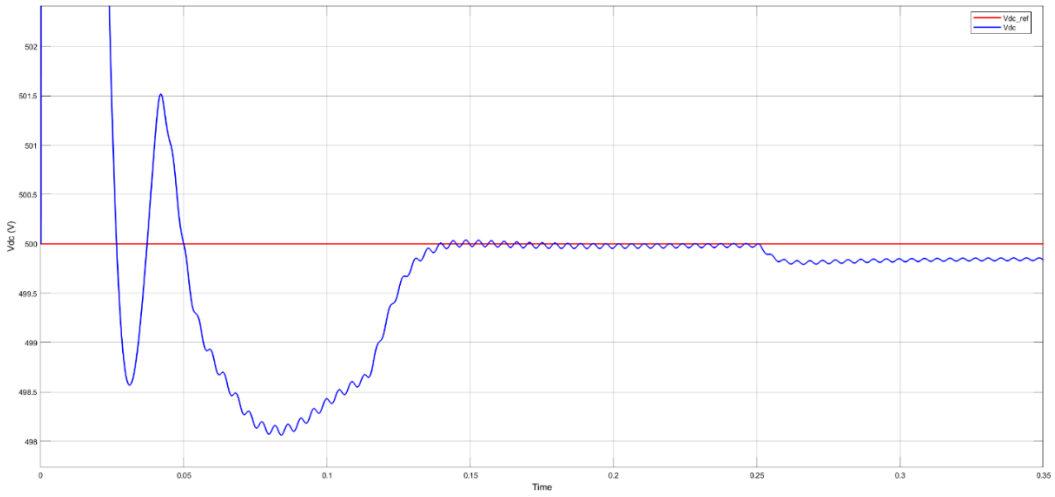

Fig. 3. DC link voltage response in the presence of the proposed ANFIS-based controller.

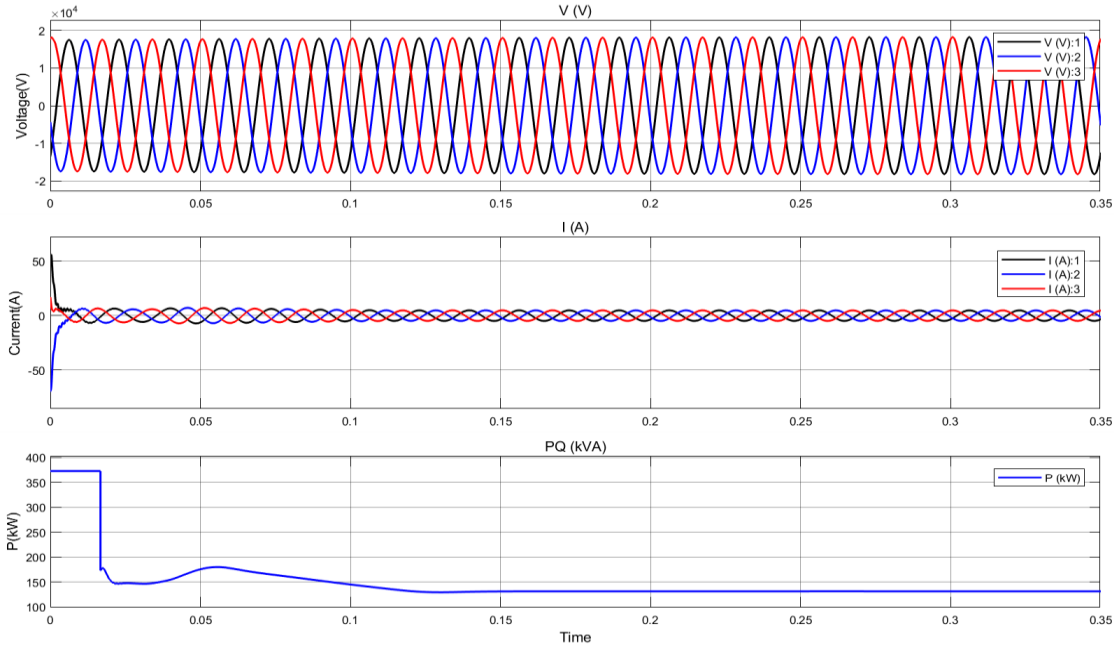

Fig. 4. Voltage, current, and active power of the system in the presence of the ANFIS controller under cyber-attack.

In the second step, the cyber resilience of the controller was assessed. According to the defined scenario, at time t = 0.25s , a False Data Injection Attack (FDIA) was applied to the measured voltage signal of the DC link. This attack diverts the feedback path by adding a constant bias and/or oscillatory component $V_{dc\,ref}$ to the signal, steering the control loop towards incorrect command execution. In the presence of the ANFIS controller, the transient reaction of the DC link voltage indicates that the controller immediately detects the effect of the attack in the "error signal" and reconfigures the command i_d by adaptively adjusting the fuzzy rules. As a result, the voltage quickly returns to around the reference level, and the oscillations caused by the attack are dampened. Even after the attack is injected, the voltage and current of the network remain stable and do not deviate from stability limits, and the active power delivered from PV and wind sources remains continuous. This behavior demonstrates the controller's ability to simultaneously compensate for both bias and oscillatory disturbances caused by the attack, preventing error accumulation in the loop. In contrast, in the absence of the ANFIS controller (Figs 5 and 6), the FDIA leads to a persistent deviation in the feedback signal, preventing the control loop from restoring the DC-link voltage to its reference value. As a result, sustained oscillations emerge and the voltage/current ripple increases, degrading power quality and perhaps posing a risk of grid disconnection. A qualitative comparison of the performance indices indicates that, in this case, T_s values increase significantly; $M_p$the voltage ripple rises markedly and a noticeable steady-state error appears. Moreover, the control effort either increases ineffectively or loses its effectiveness due to actuator saturation or operational constraints. These findings highlight the inherent vulnerability of classical controllers when confronted with data-driven attacks and underscore the necessity of intelligent adaptive control mechanisms.

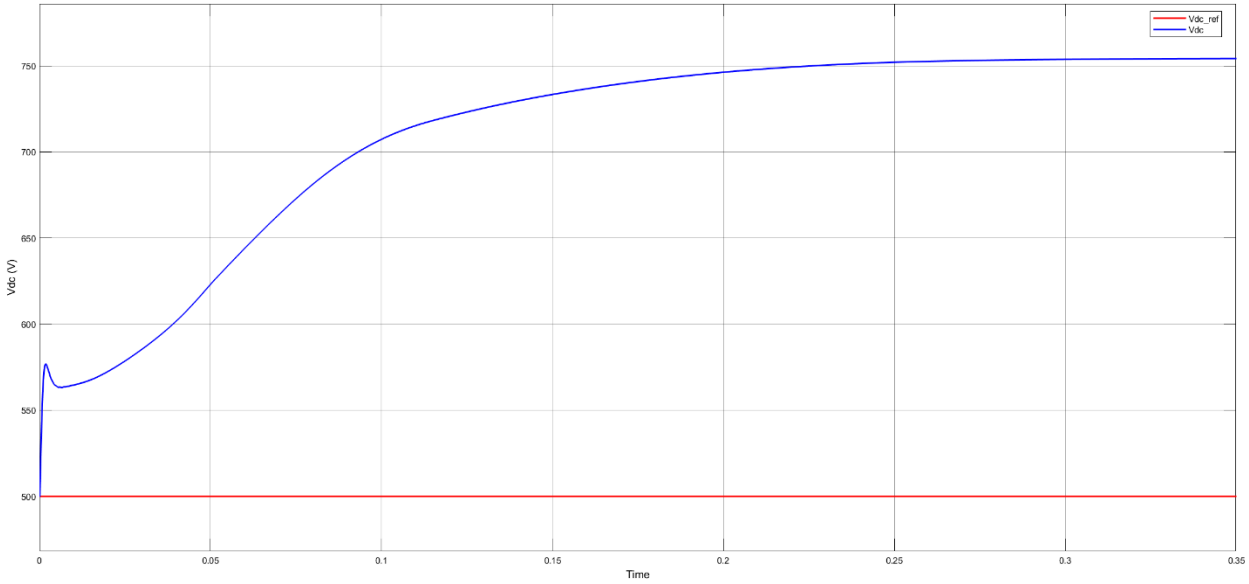

Fig. 5. Unstable DC link voltage response without using the proposed controller.

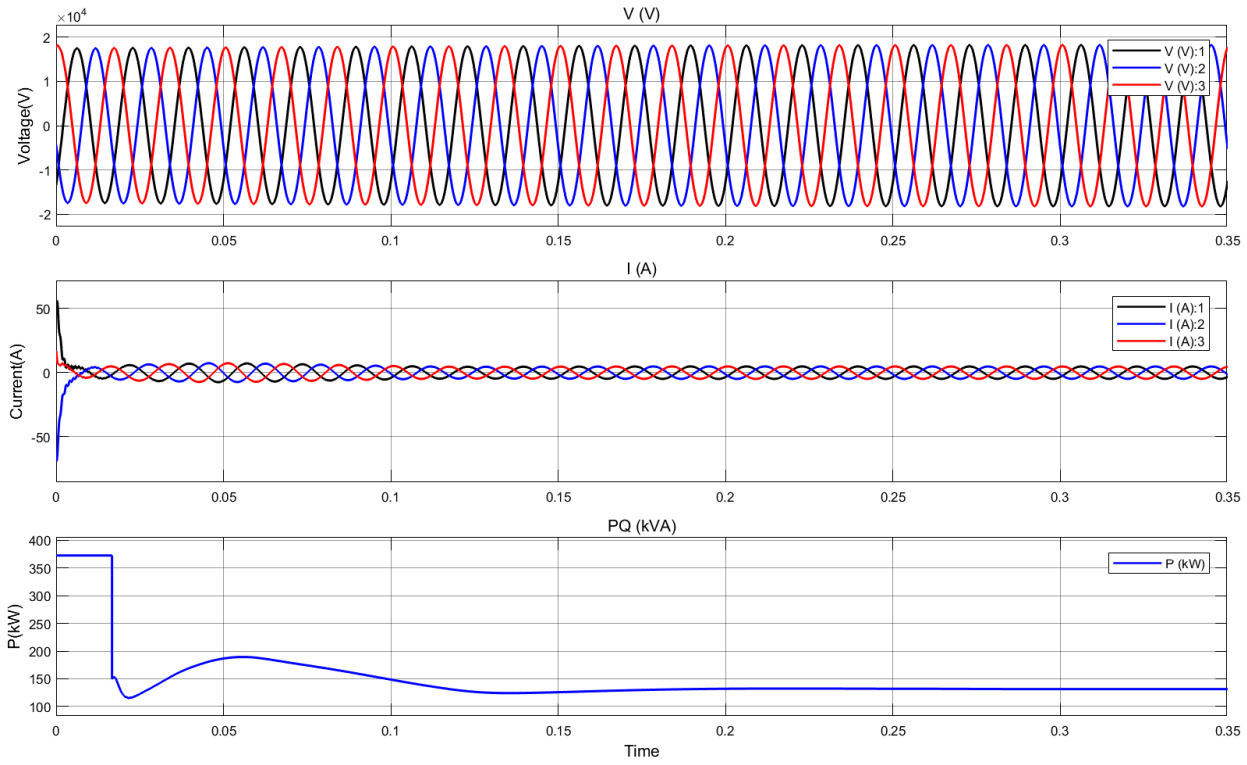

Fig. 6. Voltage, current, and active power of the system without adaptive control under cyber-attack conditions.

To enhance the reliability of the results, additional sensitivity analyses were conducted. First, measurement noise was injected into the V_{dc} signal to evaluate the controller's robustness against sensor noise. The results demonstrated that, owing to fuzzy interpolation and online parameter learning, the ANFIS controller exhibits greater resilience to measurement noise than the PI controller, maintaining the e_{ss} index and ripple within acceptable limits. Second, parametric drift in the converter filter elements (a relative variation of L_f R_f was considered) to assess the impact of model uncertainty; the system response indicated that the proposed controller is less dependent on an accurate model and is able to preserve DC-link voltage stability even under moderate parameter variations. Third, slow–fast variations in PV/wind power generation were applied in the form of ramps and quasi-atmospheric disturbances to evaluate reference tracking under variable loading conditions. Under these scenarios as well, the ANFIS controller prevented large overshoots through online adaptation of fuzzy rules and maintained smooth and stable output power.

An integrated examination of the results (as shown in Figs. 3–6) consistently demonstrates that the proposed approach simultaneously enhances three key performance components. First, DC-link voltage stability is improved through reduced recovery time and effective suppression of overshoot. Second, power quality is enhanced by regulating voltage/current ripple and maintaining the stability of the delivered active power. Third, cyber resilience is strengthened by rapidly neutralizing the effects of data-driven attacks along the

feedback path. The proposed method outperforms conventional approaches because ANFIS can bridge the gap between disturbance/attack detection and effective control action; rather than relying on extensive retraining or highly accurate modeling, it exploits a learning–fuzzy mechanism to achieve online parameter readjustment. In summary, the simulation results demonstrate that the ANFIS-based intelligent controller provides an effective solution for stabilizing the DC-link voltage in grid-connected distributed generation systems. Even in the presence of cyber–physical threats and severe generation/load fluctuations, the controller rapidly restores the voltage to the vicinity of its reference value, maintains voltage and current within stable operating limits, and ensures smooth output power delivery. Accordingly, practical adoption of this approach can enhance cyber resilience, improve operational security, and reduce the risk of grid disconnection in modern microgrids, thereby facilitating the development of sustainable and reliable smart grids. To quantitatively evaluate the performance of the proposed controller, key indices—including settling time T_s, maximum overshoot M_p, steady-state error e_{ss}, DC-link voltage ripple, control cost $\int u^2 dt$, and total harmonic distortion (THD)—were analyzed. These metrics were examined under two primary conditions: first, during normal operating conditions, and second, in the presence of a false data injection attack (FDIA) occurring at t=0.25s. The comparative results are summarized in Tables (1) and (2).

Table 1. Performance under normal operating conditions (no attack)

Evaluation index	ANFIS (Proposed)	PI (custom)	No adaptive control
settling time (T_s) (seconds)	0.08	0.22	0.35
maximum overshoot (M_p) (%)	3.1	9.4	15.7
voltage ripple (V_{dc})(% of nominal value)	0.4	1.2	2.3
control cost $\int u^2 dt$ (p.u.)	0.90	1.00	1.30

Under standard operating conditions, the ANFIS-based intelligent controller outperforms both the PI controller and the non-adaptive configuration in terms of stability, speed, and accuracy. It quickly restores the DC-link voltage to its reference value while maintaining the lowest levels of ripple and steady-state error among the three methods. The reduced settling time and overshoot reflect the controller's effectiveness in damping transient fluctuations. By comparison, the PI controller, due to its linear nature, exhibits slower response and reduced precision when dealing with the nonlinear dynamics of power converters. Meanwhile, the non-adaptive system experiences persistent oscillations and noticeable steady-state error, which can compromise overall power quality.

Table 2. Performance in the presence of a fake data injection attack (FDIA) at (t = 0.25s)

Post-attack index	ANFIS (Proposed)	PI (custom)	No adaptive control
settling time after attack ($T_s^{(\text{atk})}$)(seconds)	0.12	0.60	(unsuccessful)
overshoot after the attack ($M_p^{(\text{atk})}$) (%)	4.5	22.0	—
Permanent error at (t=1s) (volts)	0.3	3.5	(>) 5
voltage ripple (V_{dc})(% of nominal value)	0.6	2.8	(>) 4.5
THD Network flow (%)	2.1	5.9	9.8
Forced power reduction (Curtailment, %)	0	6	12
Sustainability outcome	Stable	Borderline/Poorly stable	Unstable

When cyberattacks are introduced, the advantages of the ANFIS-based controller become distinctly apparent compared with the two alternative strategies. Leveraging adaptive fuzzy inference mechanisms combined with neural learning capabilities, the controller promptly identifies abnormalities in the sensed DC-link voltage and dynamically adjusts the control action in response. Consequently, voltage fluctuations remain tightly bounded, and the DC-link voltage is restored to its reference level within a short recovery interval. In addition, the total harmonic distortion of the grid current is maintained at approximately 2%, reflecting high power quality and stable output voltage behavior. By contrast, the PI-controlled system exhibits substantial voltage deviations under attack, along with prolonged recovery times and noticeable current ripple. In the absence of adaptive control, the feedback loop is pushed beyond its stable operating region, rendering the system unable to mitigate the effects of the attack or re-establish normal operating conditions. A quantitative evaluation further confirms that the proposed ANFIS strategy surpasses conventional approaches not only in dynamic response characteristics like settling time (T_s) and peak overshoot (M_p, but also in power quality indicators and robustness under abnormal scenarios. The controller effectively balances fast dynamic response, precise voltage regulation, and cyber resilience, whereas classical control methods tend to deteriorate when subjected to data-driven perturbations. Accordingly, the proposed ANFIS controller constitutes a reliable and resilient solution for DC-link voltage regulation in grid-connected renewable energy systems.

4. Conclusion

This work presents an intelligent control framework based on an Adaptive Neuro-Fuzzy Inference System (ANFIS) for DC-link voltage regulation in grid-connected microgrids under fluctuating load, variable renewable generation, and cyber–physical attacks. The framework comprises three layers: the power system dynamics layer, a data-driven attack layer, and an intelligent control layer, enabling comprehensive analysis of DC-link voltage behavior under disturbances and security threats. Simulations on the IEEE 13-bus test system with integrated photovoltaic and wind sources demonstrate that the ANFIS controller provides

superior performance compared to classical approaches such as PI control, delivering faster response, higher stability, and improved accuracy. In normal operating conditions, the controller brings the DC-link voltage back to its reference with minimal overshoot and reduced settling time. Under false data injection attack (FDIA) scenarios, adaptive tuning of control parameters ensures system stability. Quantitative metrics, including reductions in steady-state error, voltage ripple, and grid current total harmonic distortion (THD), further confirm the superiority of the ANFIS-based method over non-adaptive controllers. The proposed approach simultaneously enhances cyber resilience, dynamic stability, and power quality by combining neural network learning with fuzzy logic robustness. This ANFIS-based strategy offers a practical and effective solution for sustainable microgrid operation amid renewable integration and cyber threats, with the potential to expand to multilayer robust controllers and hybrid Deep-ANFIS architectures for next-generation power networks.

Authors' contributions

Omar Mohammad: Data curation, Writing- Original draft preparation, Investigation

Mehdi Ahmadi Jirdehi: Supervision, Methodology, Software, Writing- Reviewing and Editing

Funding

The authors did not receive support from any organization for the submitted work.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Availability of data and materials

All data, models, or code generated or used during the study are available in a repository or online.

Reference

[1] S. Sarwar, D. Kirli, M. M. Merlin, and A. E. Kiprakis, "Major challenges towards energy management and power sharing in a hybrid AC/DC microgrid: a review," Energies, vol. 15, no. 23, p. 8851, 2022, https://doi.org/10.3390/en15238851

[2] S. Rajendran, V. Thangavel, N. Krishnan, and N. Prabaharan, "DC link voltage enhancement in DC microgrid using PV based high gain converter with cascaded fuzzy logic controller," Energies, vol. 16, no. 9, p. 3928, 2023, https://doi.org/10.3390/en16093928

[3] C. A. Beltrán, L. H. Diaz-Saldierna, D. Langarica-Cordoba, and P. R. Martinez-Rodriguez, "Passivity-based control for output voltage regulation in a fuel cell/boost converter system," Micromachines, vol. 14, no. 1, p. 187, 2023, https://doi.org/10.3390/mi14010187

[4] A. Tian et al., "Two-stage PV grid-connected control strategy based on adaptive virtual inertia and damping control for DC-link capacitor dynamics self-synchronization," Journal of Energy Storage, vol. 72, p. 108659, 2023, https://doi.org/10.1016/j.est.2023.108659

[5] S. Das, "Modeling and mitigating power grid vulnerabilities: A comprehensive analysis of renewable energy integration, cascading failures, and microgrid resilience," 2024, https://doi.org/10.25772/Q6SF-4M59

[6] M. A. Taher, H. Iqbal, M. Tariq, and A. I. Sarwat, "Disruptive effects of denial-of-service (DoS) attacks on microgrid distributed control: Altered communication topology, voltage stability, and accurate power allocation," in 2023 IEEE International Conference on Energy Technologies for Future Grids (ETFG), 2023: IEEE, pp. 1-6, https://doi.org/10.1109/ETFG55873.2023.10407127

[7] S. Shanmugam and A. Sharmila, "An intelligent adaptive neuro-fuzzy based control for multiport DC-AC converter with differential power processing converter for hybrid renewable power generation systems," Frontiers in Energy Research, vol. 12, p. 1471265, 2024, https://doi.org/10.3389/fenrg.2024.1471265

[8] B. Rekha, "Novel MLI-based DVR and DSTATCOM with ANFIS control for enhanced power quality improvement," Electric Power Systems Research, vol. 235, p. 110838, 2024, https://doi.org/10.1016/j.epsr.2024.110838

[9] M. Beikbabaei, M. Montano, A. Mehrizi-Sani, and C.-C. Liu, "Mitigating false data injection attacks on inverter set points in a 100% inverter-based microgrid," in 2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2024: IEEE, pp. 1-5, https://doi.org/10.1109/ISGT59692.2024.10454181

[10] S. H. Rouhani, C.-L. Su, S. Mobayen, N. Razmjooy, and M. Elsisi, "Cyber resilience in renewable microgrids: A review of standards, challenges, and solutions," Energy, vol. 309, p. 133081, 2024, https://doi.org/10.1016/j.energy.2024.133081

[11] S. Imtiaz, L. Yang, H. M. Munir, Z. A. Memon, H. Kilic, and M. N. Naz, "DC‐link voltage stability enhancement in intermittent microgrids using coordinated reserve energy management strategy," IET Renewable Power Generation, vol. 19, no. 1, p. e13197, 2025, https://doi.org/10.1049/rpg2.13197

[12] A. Basati, J. M. Guerrero, J. C. Vasquez, N. Bazmohammadi, and S. Golestan, "A data-driven framework for FDI attack detection and mitigation in DC microgrids," Energies, vol. 15, no. 22, p. 8539, 2022, https://doi.org/10.3390/en15228539

[13] D. Petković, M. Issa, N. D. Pavlović, L. Zentner, and Ž. Ćojbašić, "Adaptive neuro fuzzy controller for adaptive compliant robotic gripper," Expert Systems with Applications, vol. 39, no. 18, pp. 13295-13304, 2012, https://doi.org/10.1016/j.eswa.2012.05.072

[14] M. Sravani and P. V. Sobhan, "Deep reinforcement learning-based controller for DC-link voltage regulation and voltage sag compensation in a solar PV-integrated UPQC system," Scientific Reports, vol. 15, no. 1, p. 25800, 2025, https://doi.org/10.1038/s41598-025-08729-1

[15] S. Vendoti et al., "Grid tied hybrid PV fuel cell system with energy storage and ANFIS based MPPT for smart EV charging," Scientific Reports, vol. 15, no. 1, p. 27392, 2025, https://doi.org/10.1038/s41598-025-09626-3

[16] N. Eswaran, J. Sivarajah, K. Karunakaran, L. Velmanickam, S. Kumarawadu, and C. Wanigasekara, "Cyberattack Detection and Classification of Power Converters in Islanded Microgrids Using Deep Learning Approaches," Electronics, vol. 14, no. 17, p. 3409, 2025, https://doi.org/10.3390/electronics14173409

[17] S. J. Pinto, P. Siano, M. Parente, and G. Ozdemir, "Resilience and stability analysis of distributed secondary controllers in DC microgrids under cyber attacks and communication delays," IEEE Access, vol. 11, pp. 132296-132311, 2023, https://doi.org/10.1109/ACCESS.2023.3335131

[18] D. B. Aeggegn, G. N. Nyakoe, and C. Wekesa, "ANFIS‐Controlled Boost and Bidirectional Buck‐Boost DC‐DC Converters for Solar PV, Fuel Cell, and BESS‐Based Microgrid Application," International Transactions on Electrical Energy Systems, vol. 2024, no. 1, p. 6484369, 2024, https://doi.org/10.1155/2024/6484369

[19] E. N. Odonkor, A. O. Akumu, and P. M. Moses, "Design of a Three-Phase Inverter ANFIS-Based Control System for Grid-Tied PV Plant and Battery Energy Storage Systems to Enhance Grid Distribution Network Synchronization," Next Research, p. 100723, 2025, https://doi.org/10.1016/j.nexres.2025.100723

[20] A. Sahu, T. Nguyen, K. Chen, X. Zhang, and M. Hassanaly, "Detection of False Data Injection Attacks (FDIA) on Power Dynamical Systems with a State Prediction Method," IEEE Access, 2024, https://doi.org/10.48550/arXiv.2409.04609