Journal of Applied Technology and Innovation
Vol. 09, Issue 3, 2025, pp. 18-33
e-ISSN:2600-7304-ISSN
DOI: https://doi.org/10.65136/jati.v9i3.8

A Novel Control Strategy for Centralized and Decentralized Microgrids in Response to Cyber-Physical Attacks Using a Frequency Sensitivity Approach.

Elnaz Yaghoubi [1*], Elaheh Yaghoubi [1], Ahmed Khamees [2] Ashraf Alharam [2]

[1] Department of Electrical and Electronics Engineering, Istanbul Topkapi University, Istanbul, Turkey
[2] College of Science and Technology, Umm Al-Aranib, Libya
*Corresponding Author: elnaz.yaquobi@gmail.com

Abstract

Cyber-attacks present vital challenges to the stability and performance of power microgrids, making security and stability a serious concern. Current research on cyber-attacks in microgrids often focuses on artificial intelligence techniques, such as artificial neural networks, machine learning, and deep learning. Most of these studies concentrate on either centralized or decentralized control systems and often overlook the potential benefits of Fuzzy-PID controllers. This paper introduces a novel technique employing Fuzzy-PID controllers to address the shortcomings in islanded and grid-connected microgrid architectures. The work demonstrates the performance of both centralized and decentralized control systems while under physical cyber-attacks as a basis for the development of rapid response systems using frequency detection. The proposed strategy shows substantial improvements in stabilizing frequency and voltage and managing power fluctuations, thereby effectively maintaining overall system stability. This approach offers a robust and practical solution for strengthening microgrid resilience against cyber threats.

Keywords: *Microgrid, Cyber-Physical Attacks, Frequency Sensitivity, Centralized and Decentralized controller.*

1. Introduction

Security threats, particularly due to cyber-attacks, significantly affect the microgrid's stability and performance. For instance, DDoS can overwhelm the resources available within a microgrid (Taher et al., 2023; Wang et al., 2022), and interrupt the operation of this system while decreasing its accessibility (Kaur Chahal et al., 2019). There are vulnerabilities in software and hardware that hackers might take advantage of to infiltrate various systems unauthorizedly and then modify any critical data or commands(Ishtiaq et al., 2022).

Furthermore, communication protocol attacks, such as data injection and message tampering, can be conducted against the integrity of the control systems and data transmissions (Jegatheswarn & Juremi, 2021; Sridhar & Manimaran, 2010; Yang et al., 2022). Managing huge numbers of interconnected devices is already complex, and frequent configuration changes or updates to software become even more complicated (Iqbal et al., 2020; Yusupov et al., 2023). These pressing challenges call for the use of advanced detection methods to help reduce the impacts of cyber-attacks(Machap & Muaza, 2022). Specifically, this strategy requires a combination of centralized and decentralized controls, enabling the system to transition to islanded mode during a cyber-attack. This approach protects the system from further damage and ensures continuous operation. It is vital to ensure system stability and performance, especially in the event of an attack where central controllers might be compromised. Bringing together the various mechanisms of control, microgrids reach a robust operational framework that makes them resilient to cyber-attacks and reliable in-service delivery.

The literature is enriched with many studies on methods of cyber-attack detection in power systems, as can be evidenced by sources such as Reference (Suprabhath et al., 2023) which proposes a dual deep neural network (DDNN)-based approach for detecting and correcting cyber-attacks in direct current microgrids (DCMGs). Due to the existence of sensors and communication links in DCMG devices, they could be prone to cyber-attacks. A cyber-attack may trigger voltage instability and cause improper load sharing. In this respect, the proposed DDNN approach consists of two independent neural networks: a prediction network predicting the converter's duty cycle based on inputs like the DC bus voltage and reference voltage and a correction network that rectifies the duty cycle to mitigate false data injection attacks. Another paper (Aluko et al., 2022) is focused on island microgrids and their interaction with a microgrid control center (MGCC).

In this paper, the authors investigate the vulnerability of such microgrids to cyber-attacks, focusing on the so-called FDI attacks against frequency measurements. The proposed approach is based on dynamic state estimation by using an unknown input observer (UIO) for attack detection and identification. The UIO will then make an estimation of the microgrid's states and create a residual function that raises an alarm when an attack is detected. The practicality and efficiency of the method will be validated through real-time simulation tests on a real-world microgrid system, proving the capability of precisely detecting and identifying FDI attacks. The authors of reference (Bhusal et al., 2021) the application of this approach within decentralized control systems in islanded microgrids. They propose a two-layer machine learning-based scheme to detect and locate data falsification attacks against an islanded microgrid's distributed frequency control system. First, environmental inputs, such as solar irradiance, ambient temperature, and wind speed, are fed into a machine learning regressor to predict the active power output from distributed generators (DGs). Second, an application of logistic regression will compare this predicted active power with the measured one to detect and locate data falsification attacks in near real time. Moreover, Reference (Xia et al., 2023) proposes a deep neural network (DNN)-based methodology to improve tolerance against cyber-attacks in microgrids by using data-driven signal estimators, while RSD-based transfer learning is proposed to enhance generalization.

The problem considered in this paper is how to improve the resilience of the system against cyber-attacks within a decentralized secondary control framework. The research (Chang et al., 2021) proposes a new methodology of cybersecurity with the best solution for detecting cyber-attacks within the communication networks associated with both central and decentralized control systems in renewable microgrids. This study integrates Fast Fourier Transform with Deep Learning to enhance attack diagnosis efficiency, specifically focusing on the secondary control layer in microgrids. This approach effectively addresses the challenge of differentiating between malicious attacks and normal system variations, which can impact voltage regulation and current distribution. The article (Heidary et al., 2023) presents the impact of hybrid cyber-attacks, including denial of service and false data injection-based cyber-attacks on load frequency control in a low-emission shipboard microgrid (SMG). A centralized control scheme combining adaptive reinforcement learning with parallel attack detection is presented for effective management and mitigation of impacts from such cyber-attacks. another paper (Roshanzadeh et al., 2024) presents an unsupervised machine learning-based approach for detecting cyberattacks in AC microgrids with a distributed secondary control architecture. The method has the goal of detecting false data injection attacks that interfere with the operating frequency of inverter-based DGs. Utilizing a 1D Convolutional Autoencoder (CAE), the method employs unsupervised learning to reconstruct inputs and detect anomalies based on the correlation between the time-series data of DG operating frequency and active power ratios.

Moreover, the methodology proposed in reference (El-Ebiary et al., 2024) employs a Kalman Filter to estimate the terminal voltages and currents accurately; therefore, cyber-attack-induced inconsistencies can be effectively detected and corrected. A decentralized control approach has been considered with emphasis on the performance of the Kalman filter in minimizing current sharing error and voltage deviations against other methods. The reference (Zhang et al., 2021) presents a model-based method for cyber-attack detection against voltage source converters (VSCs) in islanded microgrids(Maghami et al., 2025). In the proposed approach, the Harmonics State Space Matrix is employed to synthesize a closed-loop transfer function that aids in the estimation of grid voltage and control reference. Subsequently, using the model, residuals are computed using the Space Phase Model to detect any anomalies that cyber-attacks can cause. Another work (Guo et al., 2021) deals with cyber-attack detection in grid-connected photovoltaic farms whose power electronics converters interface with the grid.

This paper uses a magnitude-based residual in the frequency domain and time-domain mean current vector-based features for fault/cyber-attack identification. Deep learning methods are applied for threat detection and compared to other methods, such as μPMU-based detection. Research on cyberattacks and microgrids exposes significant gaps. While current studies often focus on artificial intelligence (AI) techniques such as artificial neural networks, machine learning, and deep learning (Elaheh Yaghoubi, Elnaz Yaghoubi, Ahmed Khamees, et al., 2024), they typically emphasize either centralized or decentralized control systems and frequently overlook the application of Fuzzy-PID controllers. Although conventional PID controllers are able to accommodate a wide range of process dynamics, including those systems with significant disturbances and nonlinearity, fairly typical in most industrial settings (Suprabhath et al., 2023; Yusupov et al., 2022), Fuzzy-PID controllers offer a significant advantage. Fuzzy-PID controllers mitigate sudden changes in the system due to abrupt variations in error or input range. Thus, instability is avoided, and the whole system's performance is improved (Wang et al., 2019).

This paper outlines new ideas and some practical concepts to overcome the shortcomings, specifically by considering both operational modes of MGs to address both islanded and grid-connected configurations, and by the inclusion of both centralized and decentralized controllers to evaluate their performance during physical cyber-attacks. Furthermore, the study implements fast response mechanisms enhancing the responsiveness of the proposed model based on a frequency detection approach, while using a Fuzzy-PID controller in both modes of MG to be more convenient for industrial conditions. Those are unique features that underline the novelty and advanced capabilities of this research in advancing power systems and microgrid studies.

The rest of the paper is organized as follows: Section II presents a detailed background to the conceptual model. A brief description of the proposed methodology for cyber-attack detection is given in Section III. Problem formulation and modeling approaches are discussed in Section IV. Section V handles the simulation process and result analysis. Finally, the conclusions of the study are given in Section VI.

2. Research Background and Conceptual Model

There are different types of buses used to model a power system with respect to power flow and system control aspects. A PQ bus or load bus specifies active power, P, and reactive power, Q, at the bus. The voltage magnitude and phase angle are determined as functions of the power injections and load characteristics, so this bus could represent loads or generation units whose power demands are already known. In contrast, a PV bus specifies independent variables: active power, P, and voltage magnitude, V. In this case, the reactive power, Q, and voltage angle are determined by power injections and voltage control mechanisms. This type of bus is normally used to model generators where the voltage is controlled to some set value, and the reactive power adjusts to maintain this voltage. Finally, the V/F bus, called a slack or reference bus, sets the voltage magnitude and frequency. The active and reactive powers are finally assessed based on system balance and control requirements. This bus is used with voltage and frequency being pre-defined values used by systems such as in islanded microgrids or during faults in a system.

There are two major types of controllers for microgrids, each suited to different scenarios. In normal conditions, a microgrid is operated with a centralized control system, having overarching decision-making and coordination across different elements (Rasoulnia et al., 2026; Elnaz Yaghoubi et al., 2024; Elaheh Yaghoubi, Elnaz Yaghoubi, Ziyodulla Yusupov, et al., 2024). However, the transition changes to a decentralized and localized control mode once a cyber-attack or critical conditions are detected. In this mode, every single unit or a group of units independently works to allow for autonomous decision-making and localized responses to maintain system stability and resilience (Shahrbejari et al., 2025; Wazirali et al., 2023; Elaheh Yaghoubi, Elnaz Yaghoubi, Ahmed Khamees, et al., 2024).

Figure 1 illustrates the MG under study, which involves photovoltaic panels, loads, and an upstream grid. In this configuration, an inverter is interfaced with the photovoltaic system. The initial state of the figure represents that before any cyberattack, the grid is operated connectedly under a centralized controller. If a cyberattack occurs, the MG will switch to island mode, which can supply power to the loads. In these settings, when the system is grid-connected, the associated inverter of the photovoltaic system acts as a PQ bus. However, if the same system is operated in island mode, it behaves as a V/F bus.

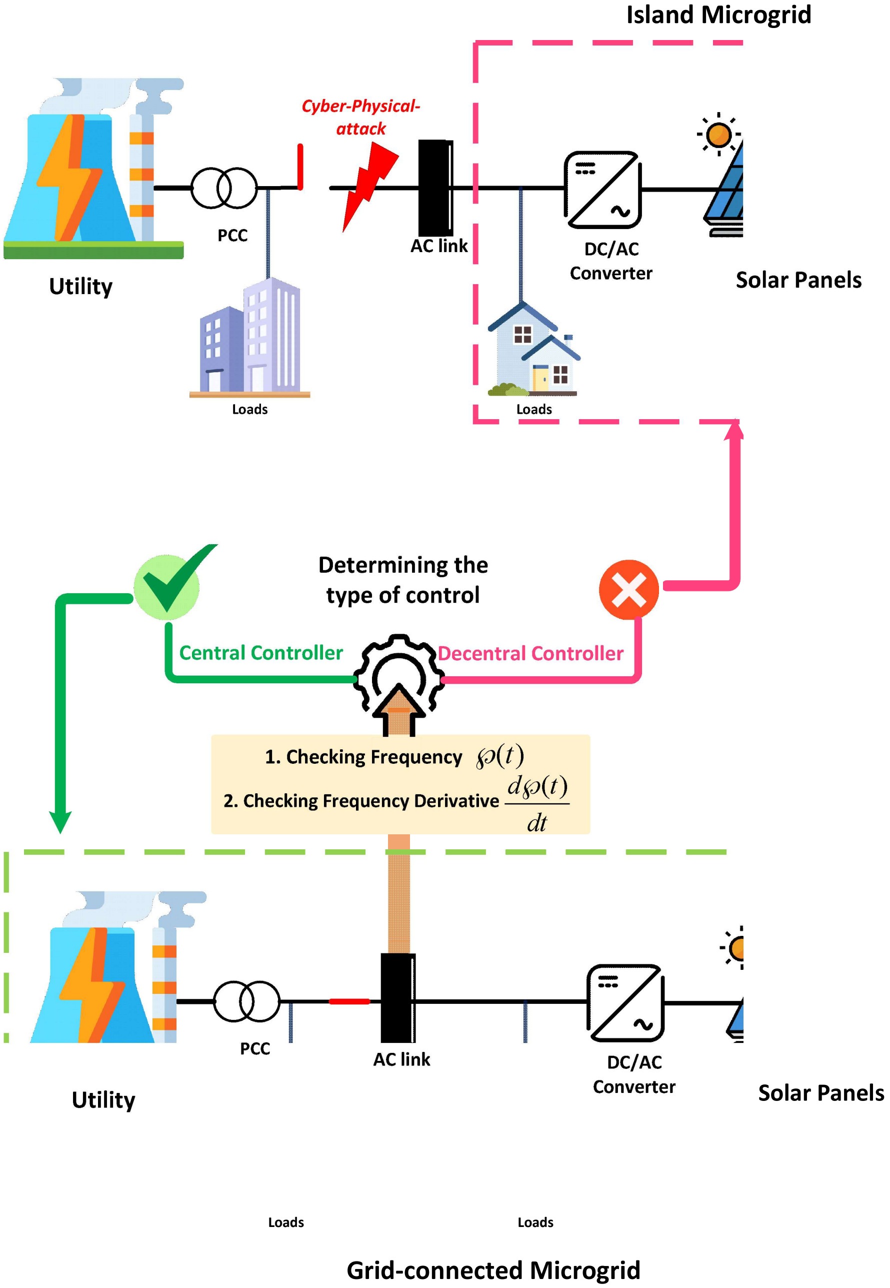

Figure 1. Conceptual model of MG with the central controller and the decentral controller during the cyberattack.

3. Cyber Physical Attack Detection Using Sensitivity Frequency Analysis

Frequency-based cyber-attack detection involves monitoring electrical systems and power distribution networks for abnormalities by analyzing changes in their frequency patterns. This method is specifically designed to identify cyber-attacks that could severely impact the performance of the power system. Frequency monitoring is currently the most advanced and effective approach for safeguarding power systems and microgrids against cyber threats. Electrical systems continuously track frequency to ensure that voltage and frequency remain within acceptable limits. Any significant deviation from normal frequency ranges could indicate a potential cyber-attack (Jahromi et al., 2025; Mohan et al., 2020; Pinto et al., 2023).

In this paper, frequency changes and their rate of change are employed to detect anomalies that may compromise system security or operational integrity. These changes are analyzed to prevent situations that could jeopardize the system. The frequency derivative is assessed based on the rate of change, which can help identify attacks or severe disturbances characterized by rapid frequency fluctuations. This measure provides insight into the dynamics of frequency deviations, facilitating the detection of sudden changes that may indicate catastrophic events affecting security or functionality. Specifically, it focuses on the rate of change, as even minimal initial variations can escalate, potentially destabilizing the system. Thus, calculating the frequency derivative aids in detecting rapid changes and maintaining system stability. The method proposed in this paper detects cyberattacks by means of formulas that analyze changes in frequency and their derivatives, which help to set thresholds and introduce corrections into the control mode. In the first step, (1) is used in the evaluation of the calculation of a change in frequency.

$$\Delta\wp(t) = \frac{\wp(t) - \wp(t-1)}{\Delta t} \qquad (1)$$

Where $\wp(t)$ represent the frequency of the system at time t, and computing the change in frequency is shown by $\Delta\wp(t)$. the $\wp(t-1)$ is the frequency at a previous time step $t - \Delta t$. then the frequency derivative $\frac{d\wp(t)}{dt}$ is calculated by (2).

$$\frac{d\wp(t)}{dt} = \lim_{t \to 0} \frac{\Delta\wp(t)}{\Delta t} \qquad (2)$$

Equation (2) provides the rate of change of the frequency change. This can be computed numerically using finite difference methods, where $\Delta\wp(t)$ is the frequency change over Δt. After this step, the maximum allowable rate of frequency change denoted as $\Delta\wp_{max}$ is established. This value represents the highest permissible rate at which the system's frequency can change before it is deemed to be in a critical state. Moreover, the maximum allowable rate of frequency change, denoted as $\frac{d\wp_{max}}{dt}$, is also determined. This value represents the maximum rate at which the frequency derivative can change and is used to identify if the system is experiencing abrupt changes.

3.1. Control Mode Switching Algorithm

Under normal conditions, in the absence of significant disturbance or potential cyber-attack in the system, the microgrid is operated in grid-connected mode and follows the central controller. On detection of a cyber-attack or suspicious condition, though, the microgrid switches to island mode and adopts a decentralized controller when $\Delta\wp(t) > \Delta\wp_{max}$ and $\frac{d\wp(t)}{dt} > \frac{d\wp_{max}}{dt}$.

Algorithm 1 provides an exact, practicable pseudocode of the control mode switching mechanism. It explains how the system will shift from one control mode to another based on the detected frequency once a cyber-attack is detected.

Algorithm 1: Control Mode Switching

```
START
Define threshold parameters
DEFINE DELTA_F_MAX ≤Threshold value for frequency change rate
DEFINE DF_DT_MAX ≤Threshold value for frequency derivative
Function to calculate the rate of frequency change
FUNCTION CalculateDeltaF(currentFreq, previousFreq, deltaT):
    RETURN (currentFreq - previousFreq) / deltaT
Function to calculate the derivative of frequency
FUNCTION CalculateDFDT(deltaF, deltaT):
    RETURN deltaF / deltaT
Function to switch to decentralized control mode
FUNCTION SwitchControlMode ():
    Switching to decentralized control mode
Activate decentralized control mode
IMPLEMENT DECENTRALIZED CONTROL MODE
Main loop
WHILE True:
    Read frequency data from sensors (AC link)
    currentFreq = READ_SENSOR (current_frequency)
    previousFreq = READ_SENSOR (previous_frequency)
    deltaT = READ_SENSOR (time_interval)
    Calculate the rate of frequency change and its derivative
    deltaF = CalculateDeltaF (currentFreq, previousFreq, deltaT)
    dfDT = CalculateDFDT (deltaF, deltaT)
    Check conditions for mode switching
    IF deltaF > DELTA_F_MAX AND dfDT > DF_DT_MAX THEN
        SwitchControlMode ()
    END
    Update previous data
    previousFreq = currentFreq
    Delay for the next iteration
    WAIT (deltaT)
END
```

In Algorithm 1, the first step is to set threshold values for the rate of frequency change and its derivative. These thresholds will be used to detect abnormal conditions. The next phase involves computing these parameters: CalculateDeltaF computes the rate of frequency change, while CalculateDFDT computes the frequency derivative. Control mode settings are adjusted in the final step. If the frequency or its derivative exceeds the defined thresholds, the system shifts to a decentralized control mode. In this main loop, pseudocode runs continuously, monitoring frequency data, performing the necessary calculations, and checking whether the conditions for a mode switch are met. If so, it triggers a shift to decentralized control. The process then updates the previous frequency data and repeats regularly to ensure continuous monitoring and response.

4. Mathematical Modelling and Problem Formulation

This section presents the objectives and limitations of the proposed methodology, highlighting key technical aspects like frequency, voltage, active power, and reactive power. A detailed study regarding mathematical formulations and constraints that concern modeling the main grid and the photovoltaic sources shall be provided. In addition to this, the application of Fuzzy-PID controllers in applications where quick response is necessary will be introduced. All this shall be explained in detail to enable a proper understanding of the approach.

4.1. Modeling of solar panels

The power output of solar (PV) panels can be determined using the following equations:

$$P_{solar\_panels} = \mathbb{N}_{solar\_panels} \times \hbar \times V \times I \quad (3)$$

$$\hbar = \frac{V_{MPP} \times I_{MPP}}{V_{oc} \times I_{sc}} \quad (4)$$

$$V = V_{oc} - Kv\left(aT + sol_{Rad}(\frac{N_{oT} - 20}{0.8})\right) \quad (5)$$

$$I = sol_{Rad}(I_{sc} + Kv(T - 25)) \quad (6)$$

Where $\mathbb{N}_{solar\_panels}$ is donate to number of solar panels and $\hbar$ refer to fill factor. sol_{Rad} is solar radiation and ambient temperature is represented by aT. A comprehensive examination of these factors, along with other pertinent attributes, is thoroughly discussed in the reference (Azizi et al., 2022). Table I organizes the key parameters of the PV array and its modules, allowing for easy reference in simulations or performance evaluations.

Table 1. Key Parameters of PV Array and Modules for Simulation and Performance Evaluation.

Parameter	Value
Parallel Strings	66
Series-Connected Modules per String	5
PV Module Model	SunPower SPR-305E-WHT-D
Maximum Power (Pmax)	305.226 W
Cells per Module (Ncell)	96
Open Circuit Voltage (Voc)	64.2 V
Short-Circuit Current (Isc)	5.96 A
Voltage at Maximum Power Point (Vmp)	54.7 V
Current at Maximum Power Point (Imp)	5.58 A
Temperature Coefficient of Voc	-0.2727 %/°C
Light-Generated Current (IL)	5.9657 A
Diode Saturation Current (I0)	6.3076×10^{-12} A
Diode Ideality Factor	0.94489
Shunt Resistance (Rsh)	393.2054 Ω

4.2. Dynamic Model of Power Microgrid

It is evident that active power changes significantly affect system frequency, whereas reactive power shows much less sensitivity to frequency changes and is mainly influenced by voltage magnitude variations. This indicates that active and reactive power are controlled through different mechanisms. Active power and frequency are regulated within the Load Frequency Control (LFC) loop, while reactive power and voltage magnitude are regulated within the Automatic Voltage Regulator (AVR) loop. As interconnected systems expand, LFC becomes increasingly important for their effective operation. This effort focuses on both the LFC and AVR loops. The controllers are tuned for specific operating conditions, enabling the system to handle small load changes and maintain frequency within specified limits. Small changes in active power are primarily influenced by variations in rotor angle, which ultimately affect system frequency. Some of the equations governing the LFC loop, as presented in the equations, illustrate how changes in frequency relate to changes in active power.

$$\Delta\wp(s) = \frac{1}{Re(\, s)}[\Delta P_{gen}(s) - \Delta P\iota(s)] \quad (7)$$

Where, $\Delta\wp(s)$ is frequency deviation in the s-domain, while $Re(\, s)$ represent frequency response characteristic. Deviation in generator active power is shown by $\Delta P_{gen}(s)$ and deviation in load active power is depicted by $\Delta P\iota(s)$. Equation (8) represents the dynamic response of the active power control.

$$\Delta P_{gen}(s) = \frac{K_P}{T_i s + 1}\Delta\wp(s) \quad (8)$$

Here K_P is proportional gain and $T_i s$ shows integral time constant. The AVR loop controls reactive power and maintains voltage magnitude within specified limits. The key equations are:

$$\Delta V(s) = \frac{1}{K_v(s)}[\Delta Q_{gen} - \Delta Q_\iota(s)] \quad (9)$$

Where $\Delta V(s)$ is the Voltage deviation in the s-domain. Voltage response characteristic is donated by $K_v(s)$. Deviation in generator reactive power and Deviation in load reactive power are shown by ΔQ_{gen} and $\Delta Q_\iota(s)$, respectively. Equation (10) captures the dynamic response of the reactive power control.

$$\Delta Q_{gen} = \frac{K_{vp}}{T_v s + 1}\Delta V(s) \quad (10)$$

Here K_{vp} is proportional gain for voltage control and $T_v s$ shows integral time constant for voltage.

4.3. Voltage and Frequency Control in Microgrids

Some sources with variable DC output, especially those with unstable or high frequency compared to the grid, are unsuitable for direct connection to a low-voltage grid(Maghami & Mutambara, 2022). To address this, power electronic converters are employed to link such sources with the grid. This work focuses on voltage and frequency control in microgrids. These controls are applied whether the system is in islanded or grid-connected mode, and they are managed through power electronic converters. Depending on the control mode, specific control strategies are applied. When the microgrid is connected to the main grid, all sources follow the grid's voltage and frequency, operating in power control mode. However, when the microgrid disconnects from the grid, one converter switches to voltage control mode, while the remaining converters continue to regulate power. To define the input-output relationships for controllers, it is essential first to establish the power and voltage relationships for distributed generation sources when connected to the microgrid (Yusupov et al., 2022), as illustrated in Figure 2.

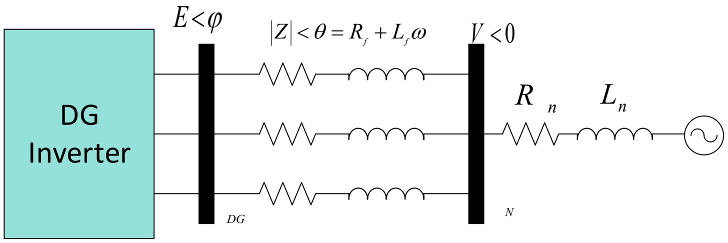

Figure 2. Schematic diagram of connecting distributed generation to a microgrid

With these definitions in mind, the active and reactive power generated by a distributed generation source and injected into the microgrid are defined in the Park coordinate system, as depicted in Figure 2 and detailed (Yusupov et al., 2022) by (11) and (12).

$$P_n = \frac{3}{2}(V_{nd}I_{nd} + V_{nq}I_{nq}) \quad (11)$$

$$Q_n = \frac{3}{2}(V_{nq}I_{nd} - V_{nd}I_{nq}) \quad (12)$$

The active and reactive power relationships at the inverter terminals for the case of a three-phase sinusoidal system are defined as follows:

$$P_{DG} = \left(\frac{\mathrm{EV}}{Z}\cos\phi - \frac{V^2}{Z}\right)\cos\theta + \frac{\mathrm{EV}}{Z}\sin\phi\sin\theta \quad (13)$$

$$Q_{DG} = \left(\frac{\mathrm{EV}}{Z}\cos\phi - \frac{V^2}{Z}\right)\sin\theta - \frac{\mathrm{EV}}{Z}\sin\phi\cos\theta \quad (14)$$

where Z and θ represent the magnitude and phase of the impedance of the connection line between the source and the microgrid. The difference in voltage size (V) and phase (ϕ) between the bus voltage and the converter's output voltage (E). It is obvious from equations, and that active and reactive powers are not controlled in separate channels. However, since the line impedance is predominantly inductive in practice ($\mathrm{Z} = \mathrm{X}\measuredangle\frac{\pi}{2}$), the relationships may be summarized as:

$$P_{DG} = \frac{\mathrm{EV}}{X}\sin\phi \quad (15)$$

$$Q_{DG} = \frac{\mathrm{EV}}{X}\cos\phi - \frac{V^2}{X} \quad (16)$$

This assumption can be checked by using the output filter impedance of the converter, generally of LC or LCL type, and subsequently incorporating a virtual impedance into the output control loop of the converter. Equations (15) and (16) include nonlinear parts, however, in the case of small phase difference ϕ these nonlinear parts may be neglected. In that case:

$$P_{DG} \approx \frac{\mathrm{EV}}{X}\phi \quad (17)$$

$$Q_{DG} \approx \frac{V}{X}(E - V) \quad (18)$$

$$\frac{d\phi}{\mathrm{dt}} = \Delta\omega \quad (19)$$

Therefore, combining (17) to (19), frequency and voltage relations can be written as:

$$\omega = \omega_0 - m_d P_{DG} \rightarrow P_{DG} = \frac{\Delta\omega}{m_d} \quad (20)$$

$$E = E_0 - n_d Q \rightarrow \quad Q_{DG} = \frac{-\Delta E}{n_d} \quad (21)$$

In the above equations, the E and E_0 are the instantaneous voltage magnitude and nominal converter output voltage respectively. ω represents the instantaneous frequency and $\omega_0$is nominal network output frequency. The coefficients $m_d$and $n_d$are the droop coefficients for frequency and voltage, respectively. These droop constants can be selected from the nominal value as:

$$m_d = \frac{\Delta\omega_{max}}{P_{max}} \quad (22)$$

$$n_d = \frac{\Delta E_{max}}{Q_{max}} \quad (23)$$

In the above equations, $\Delta\omega_{max}$, P_{max}, ΔE_{max}, Q_{max} represent the maximum variations in frequency, voltage, active power, and reactive power of DG, respectively. On the other hand, voltage relationships at the point of interconnection of DG to the grid may be formulated as shown in the following:

$$E_d = -(R_f I_{nd} + L_f \omega I_{nd}) + \omega L_f I_{nq} + V_{nd} \qquad (24)$$

$$E_q = -(R_f I_{nq} + L_f \omega I_{nq}) - \omega L_f I_{nd} + V_{nq} \qquad (25)$$

Now, from (11), (12), (20), and (21), the voltage and frequency relationships in relation to currents and voltages in the Park coordinate system can be written as:

$$\frac{\Delta\omega}{-m_d} = \frac{3}{2}(E_d I_{nd} + E_q I_{nq}) \qquad (26)$$

$$\frac{-\Delta E}{n_d} = \frac{3}{2}(E_q I_{nd} - E_d I_{nq} \qquad (27)$$

Since the networks are balanced, $V_{nq} = 0$ and $E_q = 0$, the relationships (26) and (27) can be rewritten as (28) and (29), respectively.

$$\frac{\Delta\omega}{-m_d} = \frac{3}{2} E_d I_d \qquad (28)$$

$$\frac{-\Delta E}{n_d} = \frac{3}{2} E_d I_q \qquad (29)$$

The final forms are then given by equations, from these, (30) and (31):

$$\Delta\omega = -m_d \frac{3}{2} I_{nd}\big(-(R_f I_{nd} + L_f \omega I_{nd}) + \omega L_f I_{nq} + V_{nd}\big) \qquad (30)$$

$$\Delta E = -n_d \frac{3}{2} I_q\big(-(R_f I_{nq} + L_f \omega I_{nq}) - \omega L_f I_{nd}\big) \qquad (31)$$

From (30) and (31), the block diagram of the voltage and frequency control circuit is drawn as shown in Figure 3:

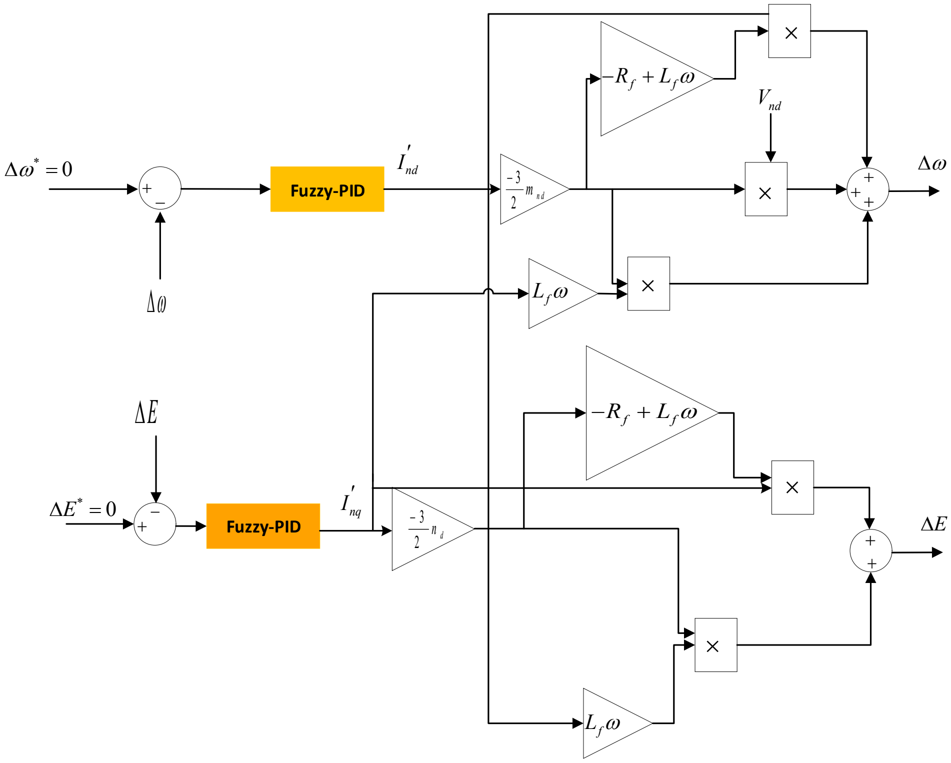

Figure 3. Block diagram of the voltage and frequency control circuit

4.4. Fuzzy-PID Controller

In a Fuzzy-PID controller, fuzzy logic adjusts the PID parameters as a function of error and its rate of change. Equations (32) to (34) describe the adjustment of the proportional gain, integral gain, and derivative gain, respectively. The interested reader can find more details about it in (Hajighorbani et al., 2014; Mohan & Sinha, 2006).

$$K_p(t) = K_{p,nom} + \Delta K_p \qquad (32)$$

$$K_i(t) = K_{i,nom} + \Delta K_i \qquad (33)$$

$$K_d(t) = K_{d,nom} + \Delta K_d \qquad (34)$$

IF e is "Large" AND $e^{\bullet}$ is "Positive" THEN ΔK_p is "Increase" AND ΔK_d is "Decrease". Here, e is the error, and $e^{\bullet}$is the rate of change of error. The fuzzy outputs become defuzzification to obtain the real PID parameter adjustment. There are commonly:

- Centroid Method

$$\Delta K_p = \frac{\sum Kp. Membership\ Degree}{\sum Membership\ Degree} \qquad (35)$$

- Weighted Average

$$\Delta K_p = \frac{\sum w_i. \Delta K_{p,i}}{\sum w_i} \qquad (36)$$

Where w_i represents the weights of the fuzzy rules.

In the system, there exist three different Fuzzy-PID controllers:

- Active Power Controller: The Fuzzy-PID controller regulates the active power of the system to operate within the defined operational limits. The output in controlling active power is determined using (37) below:

$$\mathbb{C}(z) = \rho + \frac{I.T_s}{2-1}\frac{1}{z-1} + D\frac{N}{1+N.T_s}\frac{z^{-1}}{1-z^{-1}} \qquad (37)$$

Where ρ is 0.09, I is 0.05 and the D is zero. N is the filter coefficient is 100.

- Reactive Power Controller: This Fuzzy-PID controller is always monitoring the reactive power to ensure that its levels are within the levels required for system performance. Equation (38) shows the expressed controlling reactive power

$$\mathbb{C}(z) = \rho + \frac{I}{T_s}\frac{2-1}{z-1} + D\frac{N}{1+N.T_s}\frac{z-1}{1-z^{-1}} \qquad (38)$$

Where ρ is -0.02, I is -0.0045 and the D is zero. N is the filter coefficient is 100.

- Current Regulator: This third Fuzzy–PID is used for regulating the current to ensure stable and very accurate control of the current flowing through the system:

$$\mathbb{C}(z) = \rho + I\frac{T_s}{z-1} \qquad (39)$$

Where ρ is 0.3, I is 20.

5. Simulation and Results

As shown in Figure 4, before the 15th second, the MG is in grid-connected mode and works normally with an active power input of 40 (kW)and a reactive power of -15 (kVar). In this case, the system generation and consumption of power are well-balanced, and so is the frequency ($P_{generation} = P_{consumption} \Rightarrow \frac{d\wp}{dt} = 0$). However, at the 15th second, a cyber-attack is launched and results in increased frequency by the 16th second. This results from the load being partially disrupted by the attack, hence creating a situation where the amount of generated power is more than that being consumed therefore resulting in increased frequency ($P_{generation} > P_{consumption} \Rightarrow \frac{d\wp}{dt} \neq 0 \uparrow$). In this case, the proposed strategy detects the cyberattack within one second and quickly transfers the system from PQ mode to island mode (V/F).

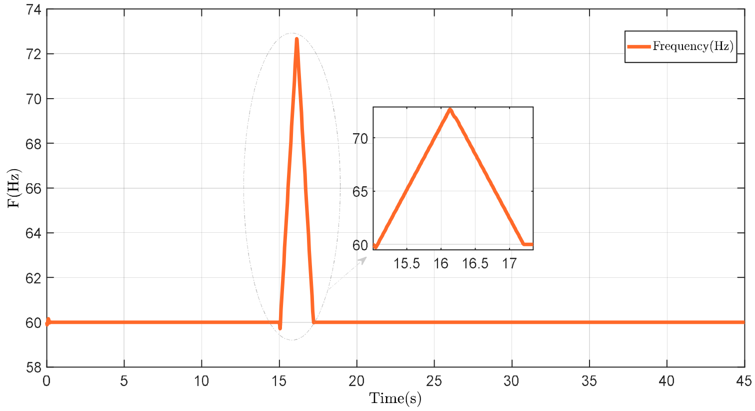

Figure 4. Frequency Control of the Network by Both Centralized and Decentralized Controllers During a Cyber Attack.

As shown in Figure 5, at 15 seconds, the voltage collapse occurred due to a cyberattack. However, one second later, the proposed technique successfully stabilized the voltage back to its steady state (1 pu).

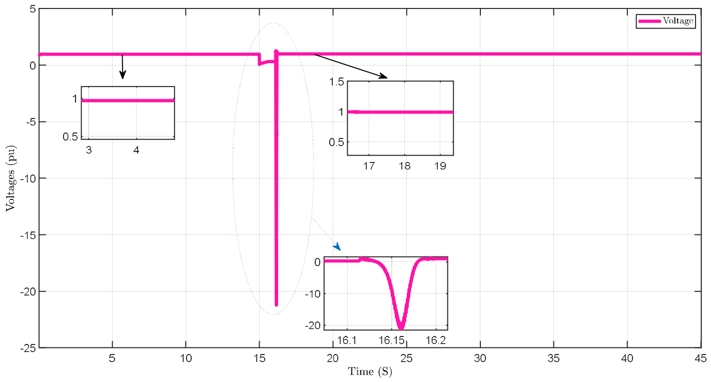

Figure 5. Voltage Stability in the Network Managed by Centralized and Decentralized Controllers During a Cyber Attack.

As illustrated in Figure 6, the active power in grid-connected mode was 40 kW before 15 seconds. At 16 seconds, the system transitioned to island mode, where decentralized control switched the microgrid to V/F bus mode, resulting in an increase in active power to 1060 kW.

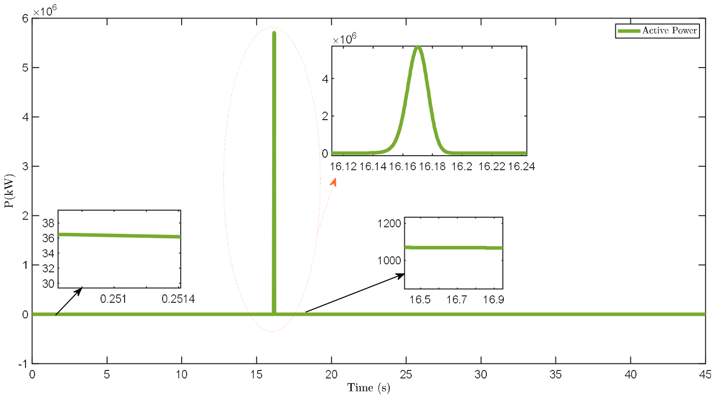

Figure 6. Active Power Control in the Network by Centralized and Decentralized Controllers During a Cyber Attack.

Additionally, Figure 7 shows that the reactive power was -15 kVAR before the cyber-attack and dropped to nearly zero by 16 seconds. This increase in both active and reactive power (Figure 6 and Figure 7), driven by the decentralized controller, is designed to maintain effective control over frequency and voltage.

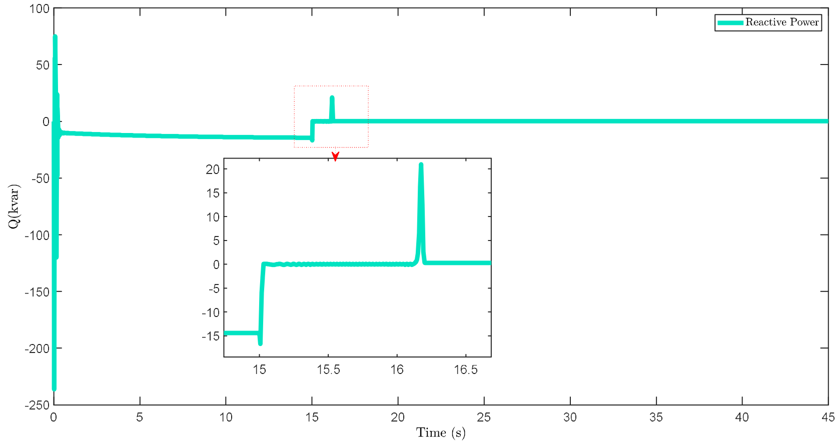

Figure 7. Reactive Power Control in the Network by Centralized and Decentralized Controllers During a Cyber Attack.

A comparison was conducted with the methodologies outlined in references (Xia et al., 2023) and (Heidary et al., 2023) to validate the proposed strategy, as shown in Table II. The results demonstrate that the proposed method restored the frequency to near its original condition, 97.5% faster than the method in reference (Heidary et al., 2023) and 80% faster than the method in reference (Xia et al., 2023). This indicates a substantial improvement in response time with the proposed approach. Additionally, the proposed method exhibited a frequency deviation of 0.833%, which is significantly better than the 1.67% deviation observed with the method in reference (Heidary et al., 2023), reflecting an improvement of approximately 49.8%. Although the method in reference (Xia et al., 2023), achieved a frequency deviation that was 99.5% lower, it required a considerably longer time to reach stability. This extended stabilization period could lead to sustained instability in the network, making the proposed method more advantageous due to its faster and more reliable stabilization capabilities.

Table 2. Performance Comparison of Frequency Sensitivity in Proposed Method and Existing Approaches.

Method	**Maximum Frequency Deviation**	**Main Time to Frequency Stability Point**
Proposed Approach	0.833%	1 second
(Xia et al., 2023)	0.004%	5 second
(Heidary et al., 2023)	1.67%	40 seconds

6. Conclusions

This paper significantly improves microgrid control by solving some of the critical limitations that exist in the current research on cyber-attacks. Adopting Fuzzy-PID controllers into the proposed control strategy makes it an effective and practical way of managing islanded and grid-connected microgrid modes during cyber-attack scenarios. This strategy can stabilize voltage and control power fluctuation while also maintaining the general stability of a system. The introduction of Fuzzy-PID controllers is one of the key innovations of this study. These controllers have been proven to be very good at handling instabilities caused by abrupt changes and sudden islanding conditions occurring during physical cyber-attacks. In this case, the application of Fuzzy-PID controllers helps to prevent sudden variations in error or input range, hence circumventing system instability and enhancing overall performances.

The proposed method outperformed these with a maximum frequency deviation of ±0.833% and a fast stabilization time of just 1 second. Thus, this approach constitutes an improvement over other methods that exhibit higher deviations or a longer stabilization time. Therefore, the proposed fuzzy-PID method provides a cost-effective and strong solution for practical applications in the real world and has given valuable insights to enhance microgrid control. Future studies need to be oriented to enhance the mechanisms of cyber-attack detection and response so that they can handle the complexities and dynamics of modern microgrids more effectively by building upon the achievements made in this work.

Declarations

Funding

This research received no external funding.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability

The data supporting the findings of this study are available from the corresponding author upon request.

References

Aluko, A. O., Carpanen, R. P., Dorrell, D. G., & Ojo, E. E. (2022). Real-time cyber attack detection scheme for standalone microgrids. *IEEE Internet of Things Journal, 9*(21), 21481–21492.

Azizi, A., Karimi, H., & Jadid, S. (2022). Daily operation of multi-energy systems based on stochastic optimization considering prediction of renewable energy generation. *IET Renewable Power Generation, 16*(2), 245–260.

Bhusal, N., Gautam, M., & Benidris, M. (2021). Cyber-attack detection on distributed frequency control of islanded MGs using machine learning. In *2021 IEEE Industry Applications Society Annual Meeting (IAS)*.

Chang, Q., Ma, X., Chen, M., Gao, X., & Dehghani, M. (2021). A deep learning based secured energy management framework within a smart island. *Sustainable Cities and Society, 70*, 102938.

El-Ebiary, A. H., Attia, M. A., Awad, F. H., Marei, M. I., & Mokhtar, M. (2024). Kalman filters based distributed cyber-attack mitigation layers for DC microgrids. *IEEE Transactions on Circuits and Systems I: Regular Papers*.

Guo, L., Zhang, J., Ye, J., Coshatt, S. J., & Song, W. (2021). Data-driven cyber-attack detection for PV farms via time-frequency domain features. *IEEE Transactions on Smart Grid, 13*(2), 1582–1597.

Hajighorbani, S., Radzi, M. M., Ab Kadir, M., Shafie, S., Khanaki, R., & Maghami, M. (2014). Evaluation of fuzzy logic subsets effects on maximum power point tracking for photovoltaic system. *International Journal of Photoenergy, 2014*(1), 719126.

Heidary, J., Oshnoei, S., Gheisarnejad, M., Khalghani, M. R., & Khooban, M. H. (2023). Shipboard microgrid frequency control based on machine learning under hybrid cyberattacks. *IEEE Transactions on Industrial Electronics*.

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet of Things Journal, 7*(10), 10250–10276.

Ishtiaq, S., Azlina Abd Rahman, N., & Shajaratuddur Harun, K. (2022). Cyber security and threats: Deepfakes impacts and risks. *Journal of Applied Technology and Innovation, 6*(2).

Jahromi, M. Z., Yaghoubi, E., & Yaghoubi, E. (2025). Optimal generation and distribution planning in smart microgrids under conditions of multi-microgrid disconnection using a hierarchical control strategy. *Electrical Engineering*, 1–20.

Jegatheswarn, R., & Juremi, J. (2021). The impact of data analytics in cyber security. *Journal of Applied Technology and Innovation, 5*(2).

Kaur Chahal, J., Bhandari, A., & Behal, S. (2019). Distributed denial of service attacks: A threat or challenge. *New Review of Information Networking, 24*(1), 31–103.

Machap, K., & Muaza, A. (2022). Use of network and cyber security tools to counter the security obstacles. *Journal of Applied Technology and Innovation, 6*(1), 5.

Maghami, M. R., & Mutambara, A. G. O. (2022). Optimum power flow with respect to the capacitor location and size in distribution network. *Processes, 10*(12), 2590.

Maghami, M. R., Mutambara, A. G. O., & Gomes, C. (2025). Assessing cyber attack vulnerabilities of distributed generation in grid-connected systems. *Environment, Development and Sustainability*, 1–27.

Mohan, A. M., Meskin, N., & Mehrjerdi, H. (2020). A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems. *Energies, 13*(15), 3860.

Mohan, B., & Sinha, A. (2006). The simplest fuzzy PID controllers: Mathematical models and stability analysis. *Soft Computing, 10*, 961–975.

Pinto, S. J., Siano, P., & Parente, M. (2023). Review of cybersecurity analysis in smart distribution systems and future directions for using unsupervised learning methods for cyber detection. *Energies, 16*(4), 1651.

Rasoulnia, M., Yaghoubi, E., Yaghoubi, E., Hussain, A., & Kamwa, I. (2026). A comprehensive systematic and bibliometric review of technologies and measurement tools for power quality events detection, classification, and fault location in smart grids. *Renewable and Sustainable Energy Reviews, 226*, 116302.

Roshanzadeh, B., Choi, J., Bidram, A., & Martínez-Ramón, M. (2024). Multivariate time-series cyberattack detection in the distributed secondary control of AC microgrids with convolutional neural network autoencoder ensemble. *Sustainable Energy, Grids and Networks, 38*, 101374.

Shahrbejari, A. N., Sani, M. H. E., Jahromi, M. Z., Yaghoubi, E., Yaghoubi, E., & Maghami, M. R. (2025). Optimal multi-objective energy management of decentralized demand response incorporating uncertainties. *PLOS ONE, 20*(7), e0328838.

Sridhar, S., & Manimaran, G. (2010). Data integrity attacks and their impacts on SCADA control system. In *IEEE PES General Meeting*.

Suprabhath, K. S., Prasad, M. V. S., Madichetty, S., & Mishra, S. (2023). A deep learning based cyber attack detection scheme in DC microgrid systems. *CPSS Transactions on Power Electronics and Applications, 8*(2), 119–127.

Taher, M. A., Iqbal, H., Tariq, M., & Sarwat, A. I. (2023). 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)*.

Wang, B., Sun, Q., Wang, R., & Dong, C. (2022). Vulnerability analysis of secondary control system when microgrid suffering from sequential denial-of-service attacks. *IET Energy Systems Integration, 4*(2), 192–205.

Wang, L., Wang, W., Du, Y., & Huang, Y. (2019). A novel adaptive fuzzy PID controller based on piecewise PID controller for dynamic positioning of sandglass-type FDPSO. *Journal of Marine Science and Technology, 24*, 720–737.

Wazirali, R., Yaghoubi, E., Abujazar, M. S. S., Ahmad, R., & Vakili, A. H. (2023). State-of-the-art review on energy and load forecasting in microgrids using artificial neural networks, machine learning, and deep learning techniques. *Electric Power Systems Research, 225*, 109792.

Xia, Y., Xu, Y., Mondal, S., & Gupta, A. K. (2023). A transfer learning-based method for cyber-attack tolerance in distributed control of microgrids. *IEEE Transactions on Smart Grid*.

Yaghoubi, E., Yaghoubi, E., Khamees, A., Razmi, D., & Lu, T. (2024a). A systematic review and meta-analysis of machine learning, deep learning, and ensemble learning approaches in predicting EV charging behavior. *Engineering Applications of Artificial Intelligence, 135*, 108789.

Yaghoubi, E., Yaghoubi, E., Yusupov, Z., & Maghami, M. R. (2024b). A real-time and online dynamic reconfiguration against cyber-attacks to enhance security and cost-efficiency in smart power microgrids using deep learning. *Technologies, 12*(10), 197.

Yaghoubi, E., Yaghoubi, E., Yusupov, Z., & Rahebi, J. (2024c). Real-time techno-economical operation of preserving microgrids via optimal NLMPC considering uncertainties. *Engineering Science and Technology, an International Journal, 57*, 101823.

Yang, K., Wang, H., & Sun, L. (2022). An effective intrusion-resilient mechanism for programmable logic controllers against data tampering attacks. *Computers in Industry, 138*, 103613.

Yusupov, Z., Almagrahi, N., Yaghoubi, E., Yaghoubi, E., Habbal, A., & Kodirov, D. (2022). Modeling and control of decentralized microgrid based on renewable energy and electric vehicle charging station. In *World Conference Intelligent System for Industrial Automation*.

Yusupov, Z., Yaghoubi, E., & Yaghoubi, E. (2023). Controlling and tracking the maximum active power point in a photovoltaic system connected to the grid using the fuzzy neural controller. In *2023 14th International Conference on Electrical and Electronics Engineering (ELECO)*.

Zhang, J., Ye, J., & Guo, L. (2021). Model-based cyber-attack detection for voltage source converters in island microgrids. In *2021 IEEE Energy Conversion Congress and Exposition (ECCE)*.