CAAI Transactions on Intelligence Technology

WILEY

The Institution of Engineering and Technology

ORIGINAL RESEARCH OPEN ACCESS

Cyberattack-Resilient Fractional-Order PPI Control for Frequency Regulation in PV-Integrated Power Systems

Bora Çavdar[1,2] | Erdinç Şahin[3,4] | Fatih Mehmet Nuroğlu[5]

[1]Graduate School of Natural and Applied Science, Karadeniz Technical University, Trabzon, Türkiye | [2]Energy Systems Engineering, Karadeniz Technical University, Trabzon, Türkiye | [3]Computer Engineering, Giresun University, Giresun, Türkiye | [4]Electrical and Computer Engineering, University of New Brunswick, Fredericton, New Brunswick, Canada | [5]Electrical and Electronics Engineering, Karadeniz Technical University, Trabzon, Türkiye

Correspondence: Erdinç Şahin (erdinc.sahin@giresun.edu.tr)

Received: 12 May 2025 | **Revised:** 5 April 2026 | **Accepted:** 21 May 2026

Keywords: artificial rabbits optimisation | cyberattack detection index | FOPPI controller | load-frequency control | PV-RT power system | stochastic loading conditions

ABSTRACT

Load-frequency control (LFC) comprises a primary process in interconnected electrical power systems, playing a critical role in maintaining the stability and reliability of the electrical grid. It is of paramount importance that the designed controller functions in an optimal manner, particularly with regard to the compression of area frequency and tie-line power deviations within the scheduled limits. In light of these considerations, this study puts forth the inaugural derivative-free and delay-based application of a predictive proportional-integral (PPI) and its fractional-order approach (FOPPI) controllers to address the LFC challenge in a PV-integrated two-area power system. To attain the most effective controller parameters of the PPI and FOPPI, the artificial rabbits optimisation (ARO) methodology is utilised by aiming to minimise the integral of the time-weighted absolute error (ITAE) performance measurement. The effectiveness of the proposed FOPPI controller is evaluated through a comparative analysis of existing controller structures in the literature and the classical PPI controller based on reported ITAE values in the literature. The proposed approach is validated through a series of detailed and systematic performance evaluations, such as time-domain analysis, uncertainty in system parameters, stochastic loading conditions, stability analysis and cyberattack performance of the proposed controllers. Furthermore, a cyberattack detection index for the controllers is considered together with a statistical analysis, and the dataset and simulation models supporting the study are made available as described in the Data Availability Statement. As evidenced by the outcomes of the performance assessments, the FOPPI controller, as conceptualised in this investigation, displays an augmented capacity for dynamic response and resilience in the face of specified scenarios when contrasted with alternative methodologies, including the PPI controller.

1 | Introduction

Today's electric power systems have become more complex and fragile with increasing energy demand, the integration of renewable energy sources, and the proliferation of communication-based automation systems. Therefore, maintaining stability and increasing the reliability of power systems should be addressed not only from the perspective of classical control methods but also from a cybersecurity perspective. In order to guarantee reliable and stable operation of the power system, it is essential to maintain the system frequency at the specified value or to quickly correct deviations caused by fluctuations in load supply or demand [1]. Sudden and unpredictable fluctuations in load demand

Abbreviations: ANA, antinuclear antibodies; APC, antigen-presenting cells; IRF, interferon regulatory factor.

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2026 The Author(s). *CAAI Transactions on Intelligence Technology* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology and Chongqing University of Technology.

can create an imbalance between the load and the generated power and cause changes in generator speed, which directly affects the system frequency. To overcome these challenges, the task of maintaining the balance between generation and consumption in power systems is provided by load frequency control (LFC) systems [2]. Although these systems were traditionally considered only physical processes, today, they have become cyber-physical systems (CPS) integrated with communication networks. Although this transformation has made LFC systems more flexible and centrally manageable, it has also brought serious cybersecurity risks. Attacks, such as false data injection (FDI) and denial of service (DoS), can threaten the stability of the system by disrupting the control loop. These attacks can directly lead to system frequency deviations, interarea imbalances, and even system blackouts. Therefore, today, LFC systems are expected to operate not only under nominal conditions but also under cyberattack in a stable and secure manner. However, when the studies conducted in this field in the literature are examined, it is seen that many studies remain limited in scope. There are very few studies that address both FDI and DoS attacks together [3–7]. In most studies, only one type of attack, such as FDI [8–23] or DoS [24–29], is addressed; the attack is usually applied to only one area, and scenario complexity is not provided. Moreover, existing cyberattack detection methods are mostly limited to observer-based frameworks such as Kalman filter (KF) [8], sliding mode observer (SMO) [9], model free observer (MFO) [10], linear matrix inequality-based observer (LMIO) [11] or unknown input observer (UIO) [12]. These methods are highly dependent on the system model, and detection performance can be severely degraded in the presence of model uncertainties or noise. Even small changes in observed parameters can affect residual generation, increasing the risk of false positive or negative alarms. Similarly, indirect–direct secure control (IDSC) [3], automatic intrusion mitigation unit (AIMU) [13] or residual-based detection (RD) [10, 14] units work in a very similar way to observer-based architectures; they detect attacks using the difference between real values and estimated or reference values. Although they do not directly use classical observer architectures, they can be considered as residual-based solutions. Therefore, such solutions have the same limitations as observer-based approaches, namely, model dependency, sensitivity to measurement noise and generalisability to real systems. In contrast, AI-based methods offer significant advantages in the model-independent recognition of complex structures, thanks to their data-driven learning capabilities. However, it is observed that very few studies include such deep learning-based detection methods [15–17], and the datasets used are generally limited in terms of both the number of scenarios [15, 17] and the size [15, 17]. In addition, the effect of load change on system behaviour is often modelled as a fixed value or a predefined profile, and random varying load conditions (VLC) are ignored [6, 7, 9–12, 14–20, 22–25]. However, in real systems, load change is sudden and unpredictable. In this respect, existing literature studies have serious limitations in terms of both data richness and realism. Table 1 summarises the shortcomings of the above-mentioned studies in the literature and what has been done in this study.

Although various control strategies, such as PID, fractional-order PID (FOPID) and model predictive controllers, have been investigated in LFC systems, controllers based on the derivative term exhibit a critical weakness in practical applications. By its very nature, the derivative operator amplifies high-frequency noise and sudden signal disturbances. To avoid these adverse effects, standard PI-type controllers without a derivative term are frequently preferred in real-world power systems and industrial applications. However, to address the slow dynamic response of classical PI controllers and improve system performance, employing a time-delayed (predictive) structure that operates without incorporating the risky derivative effect into the equation provides a significant advantage.

In a modern cyber-physical power system, the necessity of maintaining a derivative-free controller architecture becomes far more critical due to the nature of cyberattacks. FDI attacks introduce sudden and sharp anomalies into area control error (ACE) signals. Theoretically, a derivative-based controller (such as a PID) has the potential to aggressively amplify these malicious injections, instantly driving the system into instability. Due to this inherent structural vulnerability from a security perspective, adopting derivative-free architectures in cyber-resilient system designs is a much safer approach. Additionally, transmission delays naturally present in communication networks are intentionally prolonged during DoS attacks. Consequently, there is a significant research gap in the literature for a control strategy that can remain on a nonderivative basis to resist high-frequency FDI anomalies whilst also performing delay compensation to mitigate the weaknesses of classical PI and reduce dead times caused by DoS attacks. Based on these operational challenges, this study proposes a novel fractional-order predictive PI (FOPPI) controller. By completely eliminating the derivative term and integrating a fractional-order dead-time compensator, the proposed FOPPI uniquely addresses this gap; it offers superior resilience against combined cyberattack scenarios compared to traditional methods whilst naturally preventing noise amplification.

In this paper, to contribute to the shortcomings summarised in the literature, a novel controller design that is robust to cyberattacks is also proposed and cyberattack detection is performed on the system with the proposed controller. As an alternative to the classical PI and FOPPI controllers that are frequently encountered in the literature, a FOPPI controller, which is a fractional-order PPI controller with predictive structure, is proposed in this study. In its original form, the PPI controller is a model parameter-dependent controller; that is to say, it employs the system parameters as controller parameters and does not incorporate a derivative effect [30]. In the field of literature, the utilisation of this concept has been observed in the context of controlling wireless systems as well as first-, second- and third-order systems with small, medium and large death times (DTs) and first-order plus DT processes (FOPDT) with modifications such as fuzzy-based PPI (FBPPI), modified PPI (mPPI), generalised PPI (gPPI) and output PPI (oPPI) controllers [30–36]. Additionally, the fractional order PPI (FOPPI) controller has been the subject of investigation in literature. It has been employed to control of a real-time industrial process [37], processes with DTs and filters [38], wireless systems [39] and pH level systems [40]. In these studies, both model parameter-dependent and model parameter-independent implementations are presented for consideration. In model parameters-independent implementations, the controller parameters are tuned by metaheuristic algorithms [41, 42]. However, in these

TABLE 1 | A comparison table of the existing literature.

Ref	Year	Controller	Energy source	Area	SC	VLC	CAM	DS	CAD
[18]	2016	PI	Thermal	3	Low	✗	FDI	✗	✗
[8]	2018	PI	Thermal	2, 4	Low	✓	FDI	✗	KF
[26]	2020	IT2-TS fuzzy	Thermal	4	Low	✓	DoS	✗	✗
[19]	2020	RMPC	Thermal	3	Low	✗	FDI	✗	✗
[24]	2020	PI	Thermal	1, 2, 3	Low	✗	DoS	✗	✗
[14]	2020	SPMC	Battery, thermal	2	Low	✗	FDI	✗	RD
[13]	2021	FOPID	Thermal	2	Low	✓	FDI	✗	AIMU
[11]	2021	H∞-DOFC	Wind, solar, fuel cell, diesel, gas turbine, battery, flywheel	1	Low	✗	FDI	✗	LMIO
[27]	2021	PI + MDS	Thermal	3	Low	✓	DoS	✗	✗
[3]	2022	H∞-ROFC	Thermal	3	Low	✓	FDI and DoS	✗	IDSC
[15]	2022	PI	Wind, solar and thermal	2, 4	Medium	✗	FDI	24,000	FNN, NN, FPT and LSTM
[25]	2022	LQR	Thermal	3	Low	✗	DoS	✗	✗
[28]	2023	Fuzzy PD-(1+PI)	Wind, solar, diesel, fuel cell, battery, flywheel and EV	1	Low	✓	DoS	✗	✗
[20]	2023	IDSC-PI	Thermal	3	Low	✗	FDI	✗	✗
[9]	2023	SOF	Thermal, Wind and solar	2, 3, 4	Low	✗	FDI	✗	SMO
[21]	2024	RGADRC	Thermal, Wind and solar	2	Low	✓	FDI	✗	✗
[10]	2024	FOBEL	Thermal	2	Low	✗	FDI	✗	RD + MFO
[4]	2024	3DoF-TID–LADRC	Wind, solar, thermal and EV	3	Low	✓	FDI and DoS	✗	✗
[5]	2024	CPDμF-TI	Wind, solar, thermal, hydro and nuclear	2, 3	Low	✓	FDI and DoS	✗	✗
[6]	2024	DIT2FLC–FOTID	Biogas, biodiesel, solar and fuel cell	1	Low	✗	FDI and DoS	✗	✗
[12]	2024	I	Thermal	3	Low	✗	FDI	✗	UIO
[16]	2025	PDF + (0.75 + PI)	Solar, wind, thermal and EV	2	High	✗	FDI	200,001	LMFNN
[29]	2025	FOPID–FOI	Wind, hydro, thermal and EV	2	Low	✓	DoS	✗	✗
[17]	2025	No information	Solar and thermal	2	Medium	✗	FDI	7480	LMFNN
[22]	2025	$I^{\lambda}D^{1-\lambda}$	Wind, solar and thermal	2, 3	Low	✗	FDI	✗	✗
[23]	2025	RPID	Wind, solar and thermal	2	Low	✗	FDI	✗	✗
[7]	2025	SP-FPIDI	Wind, solar, thermal, flywheel, battery and ultra-capacitors	2, 3	Low	✗	FDI and DoS	✗	✗
This	—	FOPPI and PPI	Solar and thermal	2	High	✓	FDI and DoS	217,440	CNN

Abbreviations: CAD, cyberattack detection; CAM, cyberattack method; DS, dataset size; SC, scenario complexity; VLC, varying load conditions.

studies, the DT in the predictive term of an FOPPI controller is expressed by integer-order approximation. In this paper, FOPPI is presented as a novel controller by designing the DT approach in fractional order. In the tuning of the presented controller parameters, artificial rabbit optimiser (ARO), dream optimisation algorithm (DOA) and mirage search optimiser (MSO) are used. The high performance of the proposed controller is proved by time domain analysis as well as robustness random load

change and stability analyses. To measure the performance of the controller under cyberattack, a total of 720 scenarios with varying load conditions, including both FDI and DoS attacks, are generated. In addition, a one-dimensional convolutional neural network (1D-CNN) model is trained for cyberattack detection in the system with the proposed controller. The main contributions of this study to the literature are given below.

- *Benchmark dataset sharing (Random Varying Load Conditions + FDI/DoS)*: This study presents a cyberattack benchmark dataset created to enable researchers to compare different controller designs under fair and reproducible conditions on a PV–RT LFC system. The dataset is not based solely on a specific fixed/predefined load profile; instead, it contains hundreds of scenarios generated under random load variations. Furthermore, considering threats frequently encountered in the LFC control loop, FDI and DoS type attacks have been scenarioised with different severity and area combinations. Although existing studies in the literature frequently evaluate controller performance under cyberattacks, most studies address load input through a fixed or operation-specific profile and define the attack scenario internally. This makes it difficult to directly compare the results of different studies using a common reference dataset. With the presented benchmark, researchers will be able to test the cyberattack resilience of their own controllers under the same random load conditions and compare their results in a more equitable manner across methods.
- *Cyberattack detection infrastructure (1D-CNN baseline)*: The labelled dataset created is designed not only to measure controller robustness but also to support cyberattack detection studies in LFC systems. Although a significant portion of the literature on cyberattacks in the LFC context focuses on controller designs that mitigate the impact of attacks on performance, the attack detection side has been relatively less explored. This work provides labelled scenarios created under random load inputs, enabling researchers to train and test their artificial intelligence/deep learning-based detection models on the same dataset and compare methods in a fair and reproducible manner. Additionally, a 1D-CNN-based attack detection model was established on the dataset and reported as a baseline detection approach.
- *The unique structure of the FOPPI controller*: In this study, a fractional-order predictive PI controller has been developed for the PV–RT two-area LFC system. The fundamental innovation of the proposed structure is modelling the dead time effect in the predictive control structure within a fractional framework and integrating it into the controller design in this manner. Thus, compared to representing dead time with integer approaches, a more flexible and adjustable control structure is obtained, aiming to improve LFC performance.
- *Fair comparison and comprehensive validation (PPI baseline)*: To objectively demonstrate the benefits of the proposed FOPPI, the PPI controller was set up as a reference on the same PV–RT LFC model; both controllers were configured under the same performance metric and optimisation strategy. Subsequently, the controllers were evaluated not only under a single nominal condition but also through a systematic test set covering realistic conditions such as parameter uncertainty/robustness and random load variations; thus, the proposed approach was validated under different conditions.

Section 2, Methodology, includes the following subsections: PV–RT power system model, fractional-order FOPPI controller design, ARO algorithm, objective function, cyberattack design, dataset design, dataset preprocessing, conventional neural network and training process and model evaluation criteria. Section 3, Results and Discussion, presents the subsections: Time-Domain Analysis, Robustness Analysis, Random Load Change Analysis, Stability Analysis, Cyberattack Performance of Controllers, and Cyberattack Detection. Finally, Section 4 outlines the conclusions of the study.

2 | Methodology

2.1 | PV–RT Power System Model

The PV–RT power system used in this study is shown in Figure 1 and its parameters are given in Appendix A. This system has two areas, with the first area (A_1) having a PV system and the second area (A_2) including a reheat thermal system. In PV systems, PV cells are connected to form PV panels to generate DC power. PV panels are affected by temperature and solar radiation in electricity generation. It uses maximum power point tracking (MPPT) to ensure maximum power from solar radiation. Inverters convert the resulting DC power to AC power for transfer to the power system. At the output of the inverters, filters are used to eliminate harmonic distortion. In this way, the PV system is integrated into the power system. The mathematical model of the PV system consisting of PV panel, MPPT, inverter and filter is given in Equation (1).

$$G(s) = \frac{sb + a}{s^2 + sc + d}. \tag{1}$$

The reheat thermal system in A_2 of the PV–RT power system is mathematically modelled with four main components (blocks). The first of these components is the governor. Before the mathematical model of the governor, there is the block containing the speed regulation coefficient (R) of the generator shown in Figure 1. The governor controls the amount of steam entering the turbine according to changes in the generator speed. The mathematical model of the governor is drawn in Equation (2).

$$G(s) = \frac{1}{s\tau_G + 1}, \tag{2}$$

where τ_G is the time constant representing the response speed of the regulator. In addition to the conventional linear governor model in Equation (2), a governor dead-band (GDB) effect is also considered to reflect the practical nonlinearity in valve motion [43]. In this study, the dead-band nonlinearity is represented using an equivalent (linearised/describing-function-based) GDB model, whose transfer function is given in Equation (3). Accordingly, the nominal PV–RT model employs the linear governor for baseline analysis, whereas the PV–RT–GDB model incorporates the GDB block to investigate the impact of the governor dead-band on system dynamics.

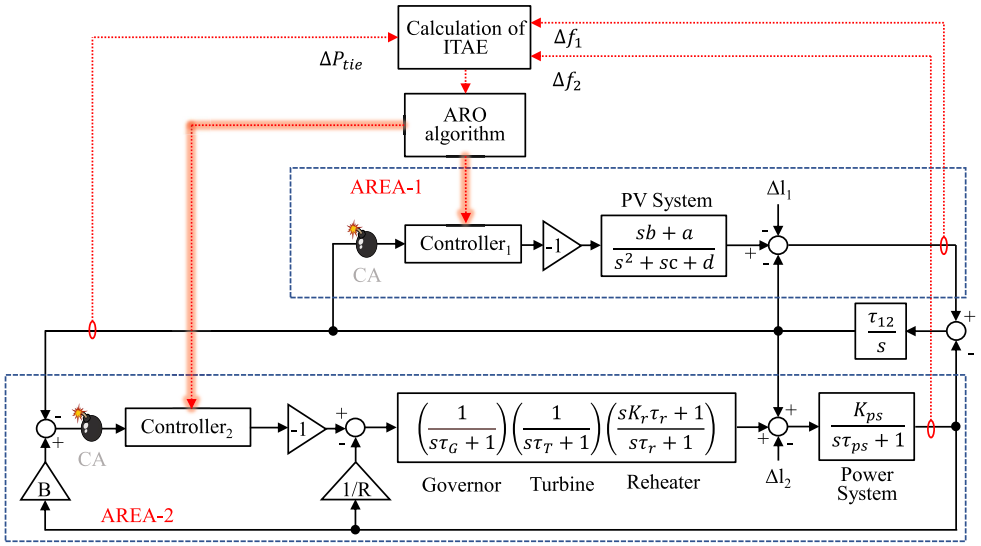


FIGURE 1 | Block diagram representation of the PV–RT power system.

$$G_{\mathrm{GDB}}(s)=\frac{0.8-\left(\frac{0.2}{\pi}\right)s}{s\tau_G+1}. \tag{3}$$

The second main component of the system, the turbine block, which follows the governor block, represents the conversion of steam energy into mechanical energy. Equation (4) shows the mathematical model of the turbine.

$$G(s)=\frac{1}{s\tau_T+1}, \tag{4}$$

where τ_T is the time constant of the turbine. Following the turbine block is the third main component of the system, the reheater block. This block represents the reheating of the steam from the turbine to generate more energy in the later phases of the turbine. Equation (5) shows the mathematical model of the reheater.

$$G(s)=\frac{sK_r\tau_r+1}{s\tau_r+1}, \tag{5}$$

where τ_r is the time constant of the reheat and K_r is the reheat gain. The power system block is the fourth component of the system after the reheater block. The mathematical model of this block is given in Equation (6). In this equation, τ_{ps} is the time constant of the power system and K_{ps} is the power system gain.

$$G(s)=\frac{sK_{ps}}{s\tau_{ps}+1}. \tag{6}$$

In the two-area system mentioned above, load changes in A_1 and A_2 are expressed as Δl_1 and Δl_2, respectively. The frequency changes are also expressed as Δf_1 and Δf_2 in A_1 and A_2, respectively. ΔP_{tie} is obtained according to the frequency changes of the areas. The mathematical expression of ΔP_{tie} is shown in Equation (7).

$$\Delta P_{tie}=\frac{T_{12}}{s}(\Delta f_1-\Delta f_2), \tag{7}$$

where T_{12} is the synchronisation coefficient of the tie line. Using ΔP_{tie} in both areas, the ACEs are obtained as the input signal of the controllers. Unlike the first area, in the second area the bias coefficient (B) and the frequency change in this area (Δf_2) also play a role in the ACE calculation. The ACE in A_1 and A_2 is obtained as in Equation (8).

$$ACE_1=\Delta P_{tie} \qquad ACE_2=B\Delta f_2-\Delta P_{tie}. \tag{8}$$

2.2 | Fractional-Order Predictive PI (FOPPI) Controller Design

As previously stated in the introduction, the PPI controller is comprised of two components. The first part is a classical PI controller, whereas the second part is a Smith predictor-based predictive part [30]. This segment incorporates a single integrator and a DT element. The difference between the control signal and its delayed version is then utilised, with the result being supplied to an integrator block. This signal is then multiplied by the integrator coefficient and subtracted from the PI controller output. The block diagram presentation of the PPI controller is given in Figure 2b, and its mathematical expression is depicted in Equation (9). Here, K_p and K_i are the classical PI controller parameters, whereas K_{pt} and τ_{pt} are the predictive term parameters. $U(s)$ and $E(s)$ represent the control and error signals in the Laplace domain, respectively.

$$U(s)=\left(K_p+\frac{K_i}{s}\right)E(s)-\frac{K_{pt}}{s}\left(1-e^{-(s\tau_{pt})}\right)U(s). \tag{9}$$

Using fractional calculus, it is possible to design a PPI controller as a fractional controller in order to increase the controller's flexibility. To do this, two integrator terms and one delay term must be expressed fractionally. After applying fractional convergence methods to the PPI controller, the resulting FOPPI controller with fractional-order DT (FODT) can be obtained as in equation (10) where λ, λ_{pt} and μ_{pt} are the fractional order of the FOPI's integrator, predictive term's integrator and DT, respectively. The block diagram of the obtained FOPPI controller is given in Figure 2a.

$$U(s)=\left(K_p+\frac{K_i}{s^{\lambda}}\right)E(s)-\frac{K_{pt}}{s^{\lambda_{pt}}}\left(1-e^{-(s\tau_{pt})^{\mu_{pt}}}\right)U(s). \tag{10}$$

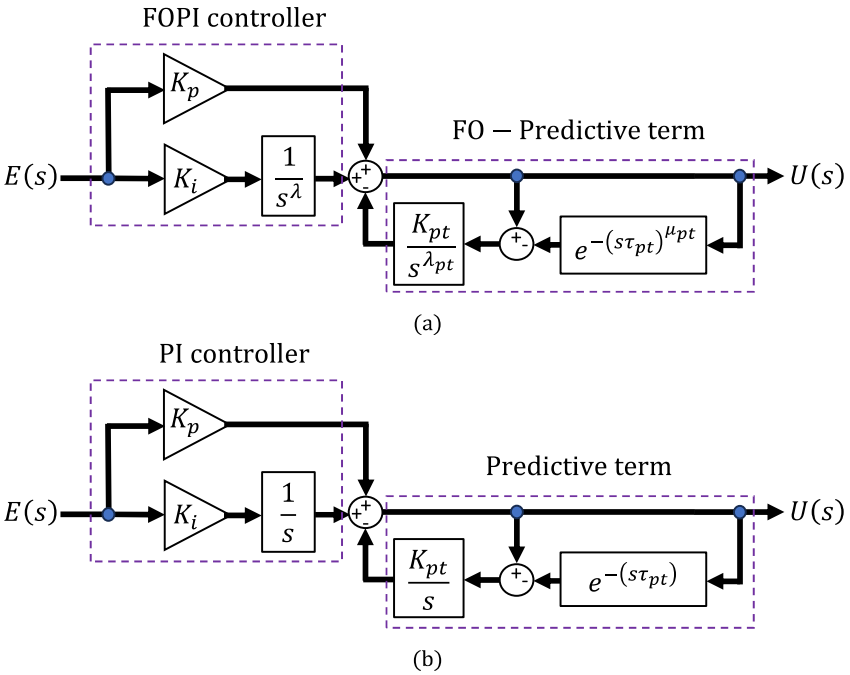


FIGURE 2 | Block diagram representation of the (a) FOPPI and (b) PPI controllers.

To implement the proposed FOPPI controller, two approximation methods are needed, one of which is for the FODT and the other is required for the fractional implementation of the integrator operators. In the design of the FODT, a Pade-approximation-based method is proposed in ref. [44]. With the help of this method, FODT can be expressed through a fractional-order transfer function. The detailed proofs and explanations can be found in ref. [44]. The second-order approximation equation of the FODT is given below.

$$\left(e^{-(s\tau)^{\mu}}\right) \approx \frac{(1/12)(s\tau)^{2\mu} - (1/2)(s\tau)^{\mu} + 1}{(1/12)(s\tau)^{2\mu} + (1/2)(s\tau)^{\mu} + 1}. \tag{11}$$

As the degree of approximation increases, the accuracy of system modelling is enhanced. Conversely, the analysis of the system becomes more intricate. In addressing these concerns, this study employs the second-order approximation for the FODT given in Equation (11) in system and controller designs as recommended in ref. [44].

In order to use fractional-order operators (FOO) in the time domain, a substantial amount of complex mathematical calculation is required. In many control applications, this is made easier by using approximate techniques. These techniques enable the approximation of FOOs or transfer functions using operators or transfer functions with an integer order over a defined frequency range. The study employs the refined Oustaloup as the second approximation method to implement derivative and integrator actions in a fractional order. The refined Oustaloup approximation method is the developed version of the classical Oustaloup method. It is generally preferred because of its high degree of accuracy across the desired frequency range. The refined Oustaloup approximation method is formulated in Equation (12) [45, 46].

$$s^{(\sigma)} \approx \left(\frac{d}{b}\omega_h\right)^{\sigma} \left(\frac{ds^2 + b\omega_h s}{d(1-\sigma)s^2 + b\omega_h s + d\sigma}\right) \prod_{k=-N}^{N} \left(\frac{s + \omega_l(\omega_h//\omega_l)^{\frac{k+N+0.5(1-\sigma)}{2N+1}}}{s + \omega_l(\omega_h//\omega_l)^{\frac{k+N+0.5(1+\sigma)}{2N+1}}}\right), \tag{12}$$

where the constants b and d are selected as 10 and 9, respectively as recommended in ref. [45]. N, ω_h and ω_l are the approximation number and the frequency range of the approximation, respectively. In this study, N is considered as 5 and the frequency ranges are set as $[\omega_h,\ \omega_l] = [10^3,\ 10^{-3}]$ *rad/s*.

2.3 | Artificial Rabbit Optimiser (ARO)

ARO is an MHS algorithm inspired by the natural life of rabbits. This algorithm basically consists of two strategies and a mechanism control the transition between them [47]. The first one is detour foraging and the second one is random hiding. The energy shrink mechanism provides the transition between these two strategies. These strategies provide the algorithm's exploration and exploitation capabilities, whereas the transition mechanism ensures to maintain a balance between them.

Detour Foraging: In this strategy, rabbits avoid foraging in the immediate neighbourhood and move to distant areas to hide the location of their burrows. It also assumes that rabbits move randomly towards other rabbits. This strategy corresponds to the global search phase, which represents the exploration capability of the ARO algorithm. The detour foraging strategy is defined mathematically as in Equation (13).

$$\vec{v}_i(t+1) = \vec{x}_j(t) + R\cdot(\vec{x}_i(t) - \vec{x}_j(t)) + round(0.5\cdot(0.05 + r_1))\cdot n_1, \quad i,j = 1, ..., n, \quad j \neq i, \tag{13}$$

where n_1 and r_1 are randomisation factors with normal distribution and uniform distribution, respectively. $\vec{x}_i(t)$ is the current position of the ith rabbit, whereas $\vec{x}_j$ is the position of the randomly selected rabbit. R is the main operator that determines how the rabbit moves. The mathematical expression of R is given in Equation (14).

$$R = \left(e - e^{\left(\frac{t-1}{T}\right)^2}\right)\cdot\sin(2\pi r_2)\cdot c, \tag{14}$$

where r_2 is the uniformly distributed randomisation factor and c is the mapping vector. t represents the current number of iterations, and T represents the maximum number of iterations. With the R operator, the step sizes of the rabbits are ensured to be larger at the beginning of the iteration process and smaller at the end of the iteration process. The mapping vector c determines the dimensions of movement. In other words, it determines the direction in which the rabbit moves. The mathematical expression of this vector is devised in Equation (15).

$$c(k) = \begin{cases} 1, & \text{if } k==g(l) \\ 0, & \text{otherwise} \end{cases} \quad k = 1, ..., d \text{ and } l = 1, ..., \lceil r_3\cdot d\rceil, \tag{15}$$

where r_3 is the randomisation factor with uniform distribution. $g(l)$ introduces randomness into the movement process by generating a random permutation of numbers from 1 to d, determining which dimensions will be updated.

Random Hiding: In this strategy, rabbits dig several burrows and hide in one random burrow at a time to avoid predators. This strategy corresponds to the local search phase, which represents the exploitation capabilities of the algorithm. The random hiding strategy is formulated mathematically as in Equation (16)

$$\vec{v}_i(t+1) = \vec{x}_i(t) + R\cdot\left(r_4\cdot\vec{b}_{i,r}(t) - \vec{x}_i(t)\right), \quad i = 1, ..., n, \tag{16}$$

where r_4 are randomisation factors with uniform distribution. $\vec{b}_{i,r}(t)$ represents the position of the randomly selected burrow. When choosing burrows to hide in, rabbits tend to choose larger areas at the beginning of the iteration process and narrower areas towards the end of the iteration process. The burrow selection process for rabbits is shown in Equation (17).

$$\vec{b}_{i,r}(t) = \vec{x}_i(t) + \left(\frac{T - t + 1}{T}\right)\cdot n_2\cdot g_r\cdot\vec{x}_i(t), \tag{17}$$

where n_2 represents the randomness factor with a normal distribution and g_r represents a vector that controls the burrow selection process. This vector, such as the mapping vector, determines which dimensions are changed. The mathematical expression of this vector is drawn in Equation (18).

$$g_r(k) = \begin{cases} 1, & \text{if } k==\lceil r_5\cdot d\rceil \\ 0, & \text{otherwise} \end{cases} \quad k = 1, ..., d, \tag{18}$$

where r_5 are randomisation factors with uniform distribution.

After both the devious foraging and random hiding strategies, the rabbits' new positions are compared with their old positions. If the rabbit's current position is better than its previous position, the rabbit stays in this position, otherwise, it returns to the other position. In equation (19), the position updates of the rabbits are expressed mathematically.

$$\vec{x}_i(t+1) = \begin{cases} \vec{x}_i(t), & \text{if } f(\vec{x}_i(t)) \leq f(\vec{v}_i(t+1)) \\ \vec{v}_i(t+1), & \text{if } f(\vec{x}_i(t)) > f(\vec{v}_i(t+1)). \end{cases} \tag{19}$$

Energy Shrink: This mechanism is a critical factor controlling the transition between the detour foraging and random hiding strategies mentioned above. At the beginning of the iteration process, the rabbits' energy is high, so the algorithm's exploration capability is high, whereas at the end of the iteration process, the rabbits' energy is low, so the algorithm's exploitation capability is high. This dynamic mechanism, which balances between exploration and exploitation depending on the iteration, is formulated as in Equation (20).

$$A(t) = 4\left(1 - \frac{t}{T}\right)\ln\left(\frac{1}{r}\right), \tag{20}$$

where r are randomisation factors with uniform distribution. In Equation (20), detour foraging is applied if $A(t) > 1$, whereas random hiding is applied if $A(t) < 1$. In other words, if $A(t) > 1$, the algorithm prioritises exploration, whereas if $A(t) < 1$, prioritises exploitation. Although $A(t)$ is determined randomly, it is more likely to be greater than 1 at the beginning of the iteration process and less than 1 towards the end.

2.4 | Dream Optimisation Algorithm (DOA)

DOA is a population-based metaheuristic inspired by the characteristics of human dreams [48]. In DOA, the dream quality is evaluated by the fitness function, and the search process is modelled through two main stages: an exploration stage (dreaming with group-dependent memory/forgetting) and an exploitation stage (development with population-wide best memory) [48]. In addition, a boundary-handling mechanism is employed to keep candidate solutions within the feasible search space.

Exploration phase: In the exploration phase, the population is divided into five groups ($q = 1, 2, 3, 4, 5$) to reflect different memory capabilities. Each group uses a distinct number of forgetting dimensions denoted by k_q (see Equation (27)). Before each dreaming session, individuals in a group are shown the best previous dream in that group by the memory strategy in Equation (21), and only the variables indexed by the randomly selected set $\{K_1, K_2, ..., K_{k_q}\}\subset\{1, ..., Dim\}$ are updated using either Equation (22) or Equation (23).

i. *Memory strategy*: For an individual $\vec{x}_i(t)$ in group q, its position is first reset to the best individual of that group as follows:

$$\vec{x}_i(t+1) = \vec{x}^{\,t}_{best,q}, \tag{21}$$

where $\vec{x}^{\,t}_{best,q}$ is the best individual in group q at iteration t.

ii. *Forgetting and supplementation strategy*: For the selected forgetting dimensions $j \in \{K_1, ..., K_{k_q}\}$, the update is performed as in Equation (22):

$$x_{i,j}(t+1) = x^t_{best,q,j} + \left(x_{\ell,j} + \text{rand}\left(x_{u,j} - x_{\ell,j}\right)\right) \frac{1}{2}\left(\cos\left(\pi \frac{t + T_{\max} - T_d}{T_{\max}}\right) + 1\right), \quad j = K_1, ..., K_{k_q}, \tag{22}$$

where $x^t_{best,q,j}$ is the jth component of the group-best solution and rand $\in [0, 1]$ is a uniform random number.

iii. *Dream-sharing strategy*: To improve escaping from local optima, DOA can alternatively replace the forgetting dimensions by acquiring information from another randomly selected individual $m \in \{1, ..., N\}$ as formulated in Equation (23):

$$x_{i,j}(t+1) = \begin{cases} x_{m,j}(t+1), & m \le i, \\ x_{m,j}(t), & i < m \le N, \end{cases} \qquad j = K_1, ..., K_{k_q}, \tag{23}$$

where the piecewise form reflects the sequential (individual-by-individual) update within the iteration.

During the exploration phase, a probability parameter u controls the selection between strategies (ii) and (iii): if rand $< u$ the forgetting-and-supplementation strategy in Equation (22) is executed; otherwise, the dream-sharing strategy in Equation (23) is applied.

Exploitation phase: In the exploitation (development) phase, grouping is no longer used. All individuals are guided by the best solution found by the entire population through the memory strategy in Equation (24) and the update rule in Equation (25).

i. *Memory strategy*: The position of each individual is first reset to the global best solution as follows:

$$\vec{x}_i(t+1) = \vec{x}^{\,t}_{best}, \tag{24}$$

where $\vec{x}^{\,t}_{best}$ denotes the best individual of the whole population at iteration t.

ii. *Forgetting and supplementation strategy*: In the development phase, the number of forgetting dimensions is denoted by k_r (see Equation (28)), and the set of forgetting dimensions is selected as $\{K_1, ..., K_{k_r}\} \subset \{1, ..., Dim\}$. For $j \in \{K_1, ..., K_{k_r}\}$, the update is given by Equation (25):

$$x_{i,j}(t+1) = x^t_{best,j} + \left(x_{\ell,j} + \text{rand}\left(x_{u,j} - x_{\ell,j}\right)\right) \frac{1}{2}\left(\cos\left(\pi \frac{t}{T_{\max}}\right) + 1\right), \quad j = K_1, ..., K_{k_r}. \tag{25}$$

Parameter settings: The exploration length is set as in Equation (26):

$$T_d = \frac{9}{10} T_{\max}. \tag{26}$$

The number of forgetting dimensions for each group in the exploration phase is determined by Equation (27):

$$k_q = \text{randi}\left(\left\lceil \frac{Dim}{8q} \right\rceil, \ \max\left\{2, \left\lceil \frac{Dim}{3q} \right\rceil\right\}\right), \qquad q = 1, 2, 3, 4, 5, \tag{27}$$

and the number of forgetting dimensions in the exploitation phase is set by Equation (28):

$$k_r = \text{randi}\left(2, \ \max\left\{2, \left\lceil \frac{Dim}{3} \right\rceil\right\}\right). \tag{28}$$

The strategy selection parameter is typically set to $u = 0.9$.

Boundary handling: DOA uses two boundary-handling approaches depending on the problem dimensionality. For low-dimensional problems ($Dim \le 15$), any violated component is re-initialised randomly using Equation (29):

$$x_{i,j}(t+1) = x_{\ell,j} + \text{rand}\left(x_{u,j} - x_{\ell,j}\right). \tag{29}$$

For high-dimensional problems ($Dim > 15$), boundary violations are corrected using a dream-sharing-like update in Equation (30):

$$x_{i,j}(t+1) = \begin{cases} x_{m,j}(t+1), & m < i, \\ x_{m,j}(t), & i < m \le N, \end{cases} \tag{30}$$

where $m \in \{1, ..., N\}$ is a randomly selected index different from i.

2.5 | Mirage Search Optimiser (MSO)

MSO is a population-based metaheuristic inspired by the physical phenomenon of mirage formation [49]. In MSO, the superior mirage mechanism is modelled as a global search strategy (exploration), whereas the inferior mirage mechanism is modelled as a local search strategy (exploitation) [49]. The algorithm updates candidate solutions by combining these two strategies and balancing their usage throughout the iterations.

Superior mirage strategy: In the superior mirage search mode, MSO performs global exploration by updating individuals using a displacement derived from a reflection-based mirage model. The horizontal displacement of the exploration point is expressed as in Equation (31):

$$\Delta x_{\text{lower}} = \frac{\sin B \cdot h \cdot \sin C}{\sin D \cdot \sin A}, \tag{31}$$

where h denotes the vertical distance term, and A, B, C and D are angles defined by the mirage geometry in Equation (31).

To facilitate escaping from local optima, h is adaptively controlled using the global best solution. For the jth component, h_j is computed according to Equation (32):

$$h_j = \left|gbest_j - x_{i,j}\right| \cdot rand + 1, \tag{32}$$

where $gbest_j$ is the jth component of the global best solution, $x_{i,j}$ is the jth component of the current individual and $rand \in [0, 1]$. The range of h_j is bounded as in Equation (33):

$$1 \le h_j \le 10 \cdot \text{arctanh}\left(\frac{t}{t_{\max}} + 1\right) + 1, \tag{33}$$

where t is the current iteration number and $t_{\max}$ is the maximum number of iterations in Equation (33).

The incident-angle related parameters α and β are generated as in Equation (34):

$$\begin{cases} \alpha = rand \cdot \dfrac{\pi}{4}, \\ \beta = rand \cdot \left(\dfrac{\pi}{4} - \dfrac{\alpha}{2} \right), \end{cases} \tag{34}$$

The superior mirage displacement is computed via three cases. The individual step size in the superior mirage search mode is given by Equations (35–37).

$$\Delta x_{\text{lower}} = a \cdot \frac{\sin(\pi - 2\alpha - 2\beta) \cdot h \cdot \sin\left(\frac{\pi}{2} + \beta\right)}{\sin(\alpha - \beta)\sin(\alpha - 2\beta)}, \tag{35}$$

$$\Delta x_{\text{lower}} = a \cdot \frac{\sin(\pi - 2\alpha + 2\beta) \cdot h \cdot \sin\left(\frac{\pi}{2} - \beta\right)}{\sin(\pi - \alpha + \beta)\sin(\alpha - 2\beta)}, \tag{36}$$

$$\Delta x_{\text{lower}} = a \cdot \frac{\sin(-\pi + 2\alpha - 2\beta) \cdot h \cdot \sin\left(\frac{\pi}{2} - \beta\right)}{\sin(\pi - \alpha + \beta)\sin(\pi - \alpha + 2\beta)}, \tag{37}$$

where $a \in \{+1, -1\}$ indicates the left/right orientation with respect to the horizontal datum normal in Equations (35–37). After computing Δx_{lower} from Equation (31) and the case expressions Equations (35–37), the position component is updated as in Equation (38):

$$x_{i,j}^{t+1} = x_{i,j}^{t} + \Delta x_{\text{lower}}. \tag{38}$$

Inferior mirage strategy: The inferior mirage strategy performs exploitation based on a refraction-inspired model. Two cases are considered depending on whether the current individual is the best one as given in Equations (39) and (40).

Case 1: if the current individual is not the optimal individual of the population, the local parameters are computed according to Equation (39):

$$\begin{cases} h_j = |gbest_j - x_{i,j}| \cdot rand, \\ D = \dfrac{(gbest_j - x_{i,j}) \cdot rand}{h_j}, \end{cases} \tag{39}$$

Case 2: if the current individual is the optimal individual of the population, the local parameters are computed according to Equation (40):

$$\begin{cases} h_j = | \pm 0.05 \cdot rand|, \\ D = \dfrac{\pm 0.05 \cdot rand}{h_j}, \end{cases} \tag{40}$$

where $D \in \{+1, -1\}$ in Equations (39) and (40).

The angle between the refractive-index layered line and the stratified reference line is initialised by Equation (41):

$$\gamma = \frac{\pi\,(t_{\max} - t)}{2t_{\max}} \cdot rand, \tag{41}$$

The angle φ between the incident light and the normal to the observation position is generated as in Equation (42):

$$\varphi = \left(\arctan\left(\frac{1}{2\tan\gamma} \right) - \arctan\left(\frac{\sin\gamma\cos\gamma}{1 + \sin^2\gamma} \right) \right) \cdot rand + \arctan\left(\frac{\sin\gamma\cos\gamma}{1 + \sin^2\gamma} \right). \tag{42}$$

The refraction angle is then obtained by Equation (43):

$$\omega = \arcsin\left(\frac{n_2}{n_1} \sin(\varphi + \gamma) \right), \tag{43}$$

where n_1 and n_2 denote the refractive indices below and above the stratification line, respectively (with $n_1 < n_2$) as used in Equation (43).

Using the local parameter definitions Equations (39) and (40) and the angle relations Equations (41–43), the displacement in the inferior mirage mode is computed as in Equation (44):

$$\Delta x_{\text{upper}} = \frac{h}{\tan\gamma} - \frac{\left(\frac{h}{\sin\gamma} - \frac{h\sin\varphi}{\cos(\varphi+\gamma)} \right)\cos\omega}{\cos(\omega - \gamma)}, \tag{44}$$

and the local update rule is given by Equation (45):

$$x_{i,j}^{t+1} = x_{i,j}^{t} + D\,\Delta x_{\text{upper}}. \tag{45}$$

Balancing exploration and exploitation: MSO ranks individuals so that the current best solution is placed at the top. The number of individuals selected (excluding the best) for global updating is controlled by Equation (46):

$$n = \left\lceil 20 \cdot \frac{t_{\max} - t}{t_{\max}} \right\rceil, \tag{46}$$

which yields $1 \le n \le 20$ and gradually decreases as t approaches $t_{\max}$ according to Equation (46).

Execution outline: At each iteration, MSO updates a subset of individuals (excluding the current best) using the superior mirage strategy via the displacement and update rules in Equations (31–38) and then updates individuals using the inferior mirage strategy via Equations (39–45). The population is re-sorted based on fitness values, and the best individual is retained for the next iteration.

2.6 | Objective Function

ITAE is a performance criterion defined as the integral of the time-weighted absolute error, and it is frequently used as an objective function in LFC studies. In this study, the ITAE is selected as the objective function because of its popularity and advantages on time-domain response compared to the other well-known integral of error-based fitness functions. A further rationale for utilising ITAE is its application in studies that are subjected to comparative analysis. In LFC, the error value is not calculated on a single signal. Instead, changes in areas and inter-area lines are taken into account. Since the system used in this study is a two-area system, the error value is calculated

using the Δf_1, Δf_1 and ΔP_{tie} signals. The mathematical expression of the ITAE performance criterion is presented in Equation (47) where t and t_{sim} represent the time and total simulation time, respectively.

$$ITAE = \int_0^{t_{sim}} t\left(|\Delta f_1| + |\Delta f_2| + |\Delta P_{tie}|\right)dt. \tag{47}$$

2.7 | Cyberattack Design

Cyberattacks can be used to manipulate the LFC mechanism in power systems. In this study, FDI and DoS cyberattacks are applied to the ACE signal entering the controllers. As mentioned earlier, the ACE signal in the LFC system is calculated by considering the variations in system frequency and tie-line power. The signal obtained as a result of this calculation is changed/delayed, causing the controller to react incorrectly. For FDI attacks, instead of distorting the signal by directly adding to the real ACE signals in both areas of the power system, attacks are performed by proportionally distorting the signals. In this way, cyberattack designs more similar to the real ACE signals of the system are obtained. The FDI cyberattacks applied to the areas can be expressed as in Equation (48).

$$\begin{aligned} ACE_1^{FDI}(t) &= \Delta P_{tie}(t) \times \alpha \\ ACE_2^{FDI}(t) &= \left(B\Delta f_2 - \Delta P_{tie}(t)\right) \times \beta. \end{aligned} \tag{48}$$

The severity of the attack is adjusted with the α and β variables shown in equation (48). If these variables take the value 1, there is no attack, and if they take the value 2, the severity of the attack is maximised. In other words, these coefficients regulate the attack by varying the magnitude of the ACE signals from 0% to 100%.

In a DoS cyberattack, ACE signals are delayed from reaching the controllers. In this attack, the delay time is set between 0.001 and 0.09 s. The mathematical expression of the DoS cyberattack is shown in Equation (49).

$$\begin{aligned} ACE_1^{DoS}(t) &= ACE_1(t - \tau_1) \\ ACE_2^{DoS}(t) &= ACE_2(t - \tau_2). \end{aligned} \tag{49}$$

2.8 | Dataset Design

This study generates a dataset including cyberattacks and normal conditions for the PV–RT power system controlled by the FOPPI controller. The dataset contains 1440 scenarios in total, 720 normal and 720 attacked scenarios. These scenarios are obtained by running the system for 15 s. The sampling time is set to 0.1 s, resulting in a total of 151 rows of data for each scenario. The 7 features recorded in the scenarios are used in the training process. These features are the scenarios' ID numbers, Δl_2, Δf_1, Δf_2, ΔP_{tie}, time and the label information for the attack and normal condition. As a result, the size of the total dataset is 217,440 rows × 7 columns. Randomly selected examples from the normal and cyberattack scenarios created in the study are shown in Figure 3. In this figure, the green colour represents normal scenarios, the blue colour represents FDI cyberattack scenarios and the red colour represents DoS cyberattack scenarios.

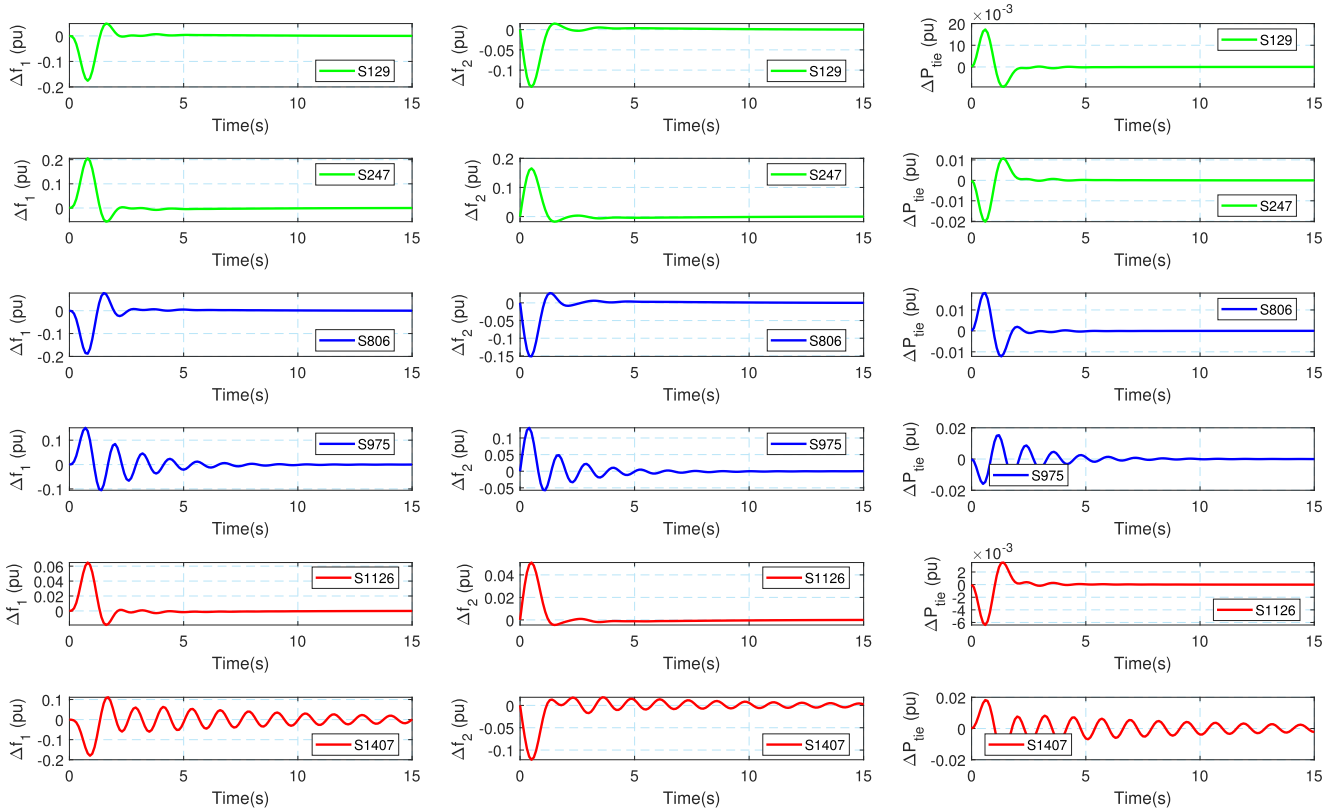


FIGURE 3 | Examples of cyberattack and normal scenarios.

In all scenarios, the load change in the second area is set to include randomness. This is realised as a uniform distribution of ±10%. In this way, ACE signals with different magnitudes are obtained both in cyberattack scenarios and in normal scenarios. In addition, the cyberattack scenarios do not destabilise the system as in normal scenarios. Both the load change in the scenarios and the scenarios not destabilising the system make it difficult to detect attack scenarios. In addition to load change, the severity of cyberattacks in the scenarios also involves randomness. Cyberattacks are divided into 18 sub-scenarios, each with 40, according to attack severity and attack areas. Cyberattacks are designed to occur in one or both areas. According to the rate of FDI attacks, low-severity attack designs occur between 1.01 and 1.25, medium-severity attack designs occur between 1.25 and 1.50 and high-severity attack designs occur between 1.50 and 2.00. According to the duration of DoS attacks, low-severity attack designs are implemented between 0.001 and 0.02 s, medium-severity attack designs are implemented between 0.02 and 0.05 s and high-severity attack designs are implemented between 0.05 and 0.09 s. Both FDI and DoS attacks are uniformly randomly generated at the intervals specified for each sub-scenario. Sub-scenarios with cyberattack specifications are given in Table 2.

2.9 | Dataset Preprocessing

In this section, the preprocessing steps necessary for the dataset to be used in cyberattack detection are performed. Before the preprocessing steps are performed, duplicated data analysis, missing data analysis and infinite data analysis are performed on the dataset. As a result of these analyses, it is determined that there is no duplicate, missing or infinite data in the dataset. After these analyses, the dataset is divided into training and test. In the training dataset (360 scenarios), 50% of the normal scenarios are used. The reason for using only normal scenarios in the training dataset is that it is not possible to know cyberattack scenarios in advance and cyberattacks do not have to be of certain standards. In the test dataset (1080 scenarios), 50% of the normal scenarios and all scenarios involving cyberattacks are used. Then, for the training dataset to be used in the deep learning process, the mean and standard deviation of Δf_1, Δf_2 and ΔP_{tie} features are calculated and the scaling process is performed with the Z-score method. This method is expressed mathematically in Equation (50).

$$X = \frac{X_{original} - \mu}{\sigma}, \tag{50}$$

where μ represents the mean and σ the standard deviation. X and $X_{original}$ represent the scaled data and the original data, respectively. In addition to the features scaled by the Z-score method, the time and Δl_2 features are handled by the min–max scaling method. The time feature starts from the 0th second and goes up to the 15th second. The Δl_2 feature changes between −0.1 and 0.1. In this way, these features are easily scaled between 0 and 1 with the min–max scaling method. Equation (51) shows the mathematical expression of this method.

$$X = \frac{X_{original} - \min(X_{original})}{\max(X_{original}) - \min(X_{original})}. \tag{51}$$

2.10 | Conventional Neural Network and Training Process

This section presents the design and training process of the 1D-CNN model for cyberattack detection. The design of the 1D-CNN model used in this study includes an input layer,

TABLE 2 | Cyberattack sub-scenarios.

Attack category	Attack type	Attack area		Attack severity	Attack value
		Area-1	Area-2		
FDI	I	✗	✓	Low	1.01–1.25
	II	✓	✗	Low	1.01–1.25
	III	✓	✓	Low	1.01–1.25
	IV	✗	✓	Medium	1.25–1.50
	V	✓	✗	Medium	1.25–1.50
	VI	✓	✓	Medium	1.25–1.50
	VII	✗	✓	High	1.50–2.00
	VIII	✓	✗	High	1.50–2.00
	IX	✓	✓	High	1.50–2.00
DoS	X	✗	✓	Low	0.001–0.02 s
	XI	✓	✗	Low	0.001–0.02 s
	XII	✓	✓	Low	0.001–0.02 s
	XIII	✗	✓	Medium	0.02–0.05 s
	XIV	✓	✗	Medium	0.02–0.05 s
	XV	✓	✓	Medium	0.02–0.05 s
	XVI	✗	✓	High	0.05–0.09 s
	XVII	✓	✗	High	0.05–0.09 s
	XVIII	✓	✓	High	0.05–0.09 s

convolution layers, fully connected layers and an output layer. These layers are described below.

Input Layer: In this layer, the dataset prepared in the previous section and passed through certain preprocessing steps is given to the CNN model as input. The input data is given in Equation (52) as the X representing the time series data.

$$X \in \mathbb{R}^{B\times C\times T}, \tag{52}$$

where B is the batch size, C is the number of features and T is the time step.

Convolution Layers: The data set transmitted from the input layer goes through a series of operations in the convolution layer. This layer is used many times in different parts of the network to extract features. With this layer, a feature map of the filtered data set is created. In the part of the network used after the input layer, simple features are usually extracted, whereas complex feature extraction occurs towards the output of the network. The convolution layer for 1D-CNN is expressed as in Equation (53).

$$S(i) = \sum_{j=0}^{k-1} X(i+j)\cdot W(j) + b, \tag{53}$$

where $W(j)$ is the convolution kernel, b is the bias term and k is the length of the filter. There are three convolution layers in this study. The outputs of these layers use the *ReLU* activation function. The outputs and their sizes are given in Equation (54).

$$\begin{aligned} X_1 &= ReLU(S(X, W_1)), \quad X_1 \in \mathbb{R}^{B\times C_1\times T} \\ X_2 &= ReLU(S(X_1, W_2)), \quad X_2 \in \mathbb{R}^{B\times C_2\times T} \\ X_3 &= ReLU(S(X_2, W_3)), \quad X_3 \in \mathbb{R}^{B\times C_3\times T}. \end{aligned} \tag{54}$$

Fully Connected Layers: This layer takes the features from all previous layers and prepares them for the output layer. In this layer, the feature maps are flattened into a single vector. The flattening vector is given in Equation (55).

$$X_{flat} = Flatten(X_3), \quad X_{flat} \in \mathbb{R}^{B\times D}, \tag{55}$$

where D is the product of C_3 and T. After this process, fully connected layers are used as shown in Equation (56).

$$\begin{aligned} X_4 &= ReLU\left(X_{flat}W_4 + b_4\right), \quad X_4 \in \mathbb{R}^{B\times M_1} \\ X_5 &= X_4W_5 + b_5, \quad X_5 \in \mathbb{R}^{B\times M_2}. \end{aligned} \tag{56}$$

Output Layer: For use in cyberattack detection, the output after the fully connected layers must be the same size as the input data. For this reason, the size of the output is rearranged. In this way, the output of the model is obtained as in Equation (57).

$$\hat{Y} = Reshape(X_5, (B, C, T)), \quad \hat{Y} \in \mathbb{R}^{B\times C\times T}. \tag{57}$$

Information about the layers of the CNN model mentioned above is summarised in Table 3. In the training process of the CNN model, Adam optimiser was used as the optimisation algorithm and 0.0001 was selected as the learning rate by fine-tuning. Also at this process, the number of epochs and batch size were used as 500 and 32, respectively. In addition, the mean square error (MSE) shown in Equation (58) is used as the loss function.

$$\mathcal{L}_{MSE} = \frac{1}{N}\sum_{i=1}^{N}\left(Y_i - \hat{Y}_i\right)^2, \tag{58}$$

where Y_i represents the actual value, $\hat{Y}_i$ is the predicted value and N is the total number of samples.

2.11 | Cyberattack Detection via Reconstruction–Error Anomaly Score

In this study, cyberattacks are identified using an anomaly detection mechanism based on the reconstruction capability of the trained 1D-CNN model. Given the input time-series tensor $X \in \mathbb{R}^{B\times C\times T}$ in Equation (52), the model produces the reconstructed output $\hat{Y} \in \mathbb{R}^{B\times C\times T}$ as in Equation (57). Under normal operating conditions, the reconstruction error between X and $\hat{Y}$ remains small, whereas FDI/DoS attacks distort the system behaviour and lead to noticeably larger reconstruction errors. Therefore, an anomaly score is defined for each sample in a batch as the mean squared reconstruction error averaged over all channels and time steps as defined in Equation (59):

$$s_b = \frac{1}{CT}\sum_{c=1}^{C}\sum_{t=1}^{T}\left(X_{b,c,t} - \hat{Y}_{b,c,t}\right)^2, \qquad b = 1, 2, ..., B. \tag{59}$$

A binary decision rule is then applied according to Equation (60):

$$\hat{y}_b = \begin{cases} 1, & s_b > \tau, \\ 0, & s_b \le \tau, \end{cases} \tag{60}$$

where $\hat{y}_b = 1$ denotes 'attack' and $\hat{y}_b = 0$ denotes 'normal'. The threshold τ is determined using normal test scenarios that are not used during training, and it is chosen to ensure that all those normal test samples are classified as normal (i.e., zero

TABLE 3 | Layer details of the CNN model.

No	Type	Parameters	Input shape	Output shape
1	Conv1D + BatchNorm + ReLU	(5 → 32), kernel = 3, padding = 1	(Batch, 5, 151)	(Batch, 32, 151)
2	Conv1D + BatchNorm + ReLU	(32 → 64), kernel = 3, padding = 1	(Batch, 32, 151)	(Batch, 64, 151)
3	Conv1D + BatchNorm + ReLU	(64 → 128), kernel = 3, padding = 1	(Batch, 64, 151)	(Batch, 128, 151)
4	Flatten	—	(Batch, 128, 151)	(Batch, 19,328)
5	Fully connected layer I	19,328 → 64	(Batch, 19,328)	(Batch, 64)
6	Fully connected layer II	64 → 755	(Batch, 64)	(Batch, 755)
7	Reshape	View (x, batch, 5, 151)	(Batch, 755)	(Batch, 5, 151)

false alarms on the normal test set). Let $\mathcal{D}_{N,\text{test}}$ denote the normal-only test subset and let s_i be the anomaly score of the ith sample. The threshold is selected according to Equation (61) as follows:

$$\tau = \max_{i \in \mathcal{D}_{N,\text{test}}} s_i, \tag{61}$$

which enforces $s_i \leq \tau$ for all $i \in \mathcal{D}_{N,\text{test}}$ and therefore yields FP = 0 and FPR = 0 on the normal test set by construction.

2.12 | Model Evaluation Criteria

The metrics used to evaluate the performance of the CNN-based cyberattack detection model are discussed in this section. These metrics are necessary to analyse how accurately the model detects cyberattacks and misclassification rates. In this study, the model is evaluated using 'Accuracy', 'Precision', 'Recall', 'F1-score', 'False Positive Rate (FPR)' and 'False Negative Rate (FNR)'. In addition, the confusion matrix is used to understand the decision mechanism of the model. All these metrics are calculated based on four basic criteria. These criteria are briefly summarised below.

- True Positive (TP): Correct classification of cyberattacks
- True Negative (TN): Correct classification of normal conditions
- False Positive (FP): Classifying normal conditions as cyberattacks
- False Negative (FN): Classification of cyberattacks as normal conditions

The confusion matrix is represented by the matrix representation of the four criteria mentioned above. Other metrics are calculated by combining these criteria in different ways. The description and mathematical expressions of these metrics are given below.

Accuracy: This metric measures the overall classification success of the model. This metric calculates the ratio of all correct predictions to total predictions as given in Equation (62).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}. \tag{62}$$

Precision: This metric measures how many cyberattack predictions are actually cyberattacks. A precision value close to one indicates that the model is unlikely to give false alarms. The mathematical expression of this metric is shown in Equation (63).

$$Precision = \frac{TP}{TP + FP}. \tag{63}$$

Recall: This metric shows how many actual cyberattacks are detected. A recall value close to one indicates that the model is unlikely to miss cyberattacks. The mathematical expression of this metric is drawn in Equation (64).

$$Recall = \frac{TP}{TP + FN}. \tag{64}$$

F1−Score: This metric represents the balance of the precision and recall metrics. Equation (65) shows the mathematical expression of this metric.

$$F1 - Score = \frac{2 \times Precision \times Recall}{Precision + Recall}. \tag{65}$$

FPR: This metric, given in Equation (66), shows how many normal conditions are incorrectly classified as cyberattacks.

$$FPR = \frac{FP}{FP + TN}. \tag{66}$$

FNR: This metric, illustrated in Equation (67), shows how many cyberattacks are incorrectly classified as normal conditions.

$$FNR = \frac{FN}{FN + TP}. \tag{67}$$

3 | Results and Discussions

In this section, the performance of the optimally designed PPI and FOPPI controllers is compared in terms of time domain analysis, robustness analysis and random load change analysis. In addition, the performance of the optimally designed PV–RT power system with the FOPPI controller under cyberattack is presented and cyberattack detection in this system is considered. During the optimal design of the PPI and FOPPI controllers, the load change of the system is applied as 10% in the second area based on the literature [50–57]. In this design, the parameters of PPI and FOPPI controllers are obtained within defined ranges by ARO algorithm. The parameter ranges used in the optimum controller design were determined based on similar studies in the literature [54–57]. The parameter ranges used in the optimum controller design are given in Table 4.

With optimally designed PPI and FOPPI controllers, the ITAE values obtained at the end of 30 s of simulation time are 1.3137 and 0.8976, respectively. The controller parameters that provide these ITAE values are given in Table 5.

3.1 | Time-Domain Evaluation of the Optimisation Algorithms for PV-RT System

The transient response performance of the system is evaluated in the time domain. Using the optimum parameters reported in Table 5, Figures 4 and 5 present the frequency deviations (Δf_1, Δf_2) and the tie-line power deviation (ΔP_{tie}) of the PV-RT power system for the PPI and FOPPI controllers, respectively. In addition, three optimisers (ARO, DOA and MSO) were compared, and their transient response metrics are provided in Table 6. Since the best overall results (minimum ITAE) were obtained with ARO, the numerical comparisons and discussions below correspond to the ARO-tuned PPI and FOPPI controllers. Compared to PPI, the FOPPI controller reduces the overshoot of Δf_1 from 0.0887 p.u to 0.0645 p.u (27.3% reduction) and the overshoot of Δf_2 from 0.0409 p.u to 0.0198 p.u (51.6% reduction). For ΔP_{tie}, the overshoot decreases from 0.0338 p.u to 0.0230 p.u (32.0% reduction). In terms of undershoot magnitude, FOPPI improves Δf_2 from 0.2060 p.u to 0.1884 p.u (8.5% reduction) and ΔP_{tie} from 0.0257 p.u to 0.0123 p.u (52.1% reduction), whereas the Δf_1 undershoot remains essentially unchanged (0.2337 p.u vs. 0.2339 p.u). Moreover, FOPPI shortens the settling time (0.2% criterion) for Δf_1 from 10.22 to 9.34 s (8.6%), for Δf_2 from 9.84 to 9.28 s (5.7%) and for ΔP_{tie} from 3.58 to 1.92 s (46.4%). These results, together with the optimiser-

TABLE 4 | Parameter ranges for the design of optimal controllers in PV-RT power system.

Controller	$K_{p_{1/2}}$	$K_{i_{1/2}}$	$K_{pt_{1/2}}$	$\tau_{pt_{1/2}}$	$\lambda_{1/2}$	$\lambda_{pt_{1/2}}$	$\mu_{pt_{1/2}}$
PPI	0.001–2	0.001–2	0.001–2	0.001–2	1	1	1
FOPPI	0.001–2	0.001–2	0.001–2	0.001–2	0.1–1	0.1–1	0.1–1

TABLE 5 | Optimal PPI and FOPPI controller parameters in PV–RT power system obtained by different optimisers.

Optimiser	Controller	Area	K_p	K_i	K_{pt}	τ_{pt}	λ	λ_{pt}	μ_{pt}	ITAE
ARO	PPI	A_1	1.9999	0.1128	1.1298	1.0290	1.0000	1.0000	1.0000	1.3137
		A_2	1.2459	2.0000	0.0003	0.0326	1.0000	1.0000	1.0000	
DOA	PPI	A_1	1.9996	0.1133	1.1246	1.0306	1.0000	1.0000	1.0000	1.3147
		A_2	1.2558	1.9980	0.0020	0.0374	1.0000	1.0000	1.0000	
MSO	PPI	A_1	2.0000	0.1120	1.1310	1.0294	1.0000	1.0000	1.0000	1.3137
		A_2	1.2473	2.0000	0.0001	0.0001	1.0000	1.0000	1.0000	
ARO	FOPPI	A_1	1.9412	1.9982	1.5134	1.3598	0.0171	0.9896	0.8913	0.8976
		A_2	1.9984	1.9976	0.1328	1.4528	0.8477	0.0185	0.9991	
DOA	FOPPI	A_1	1.7367	1.8391	2.0000	1.9872	0.0337	0.9998	0.7910	0.9057
		A_2	1.9983	1.9967	0.2070	1.5363	0.8410	0.0635	0.9915	
MSO	FOPPI	A_1	1.8917	1.8906	1.2522	1.2270	0.0637	0.9757	0.9596	0.9195
		A_2	2.0000	2.0000	0.1193	1.2099	0.8629	0.0775	0.9992	

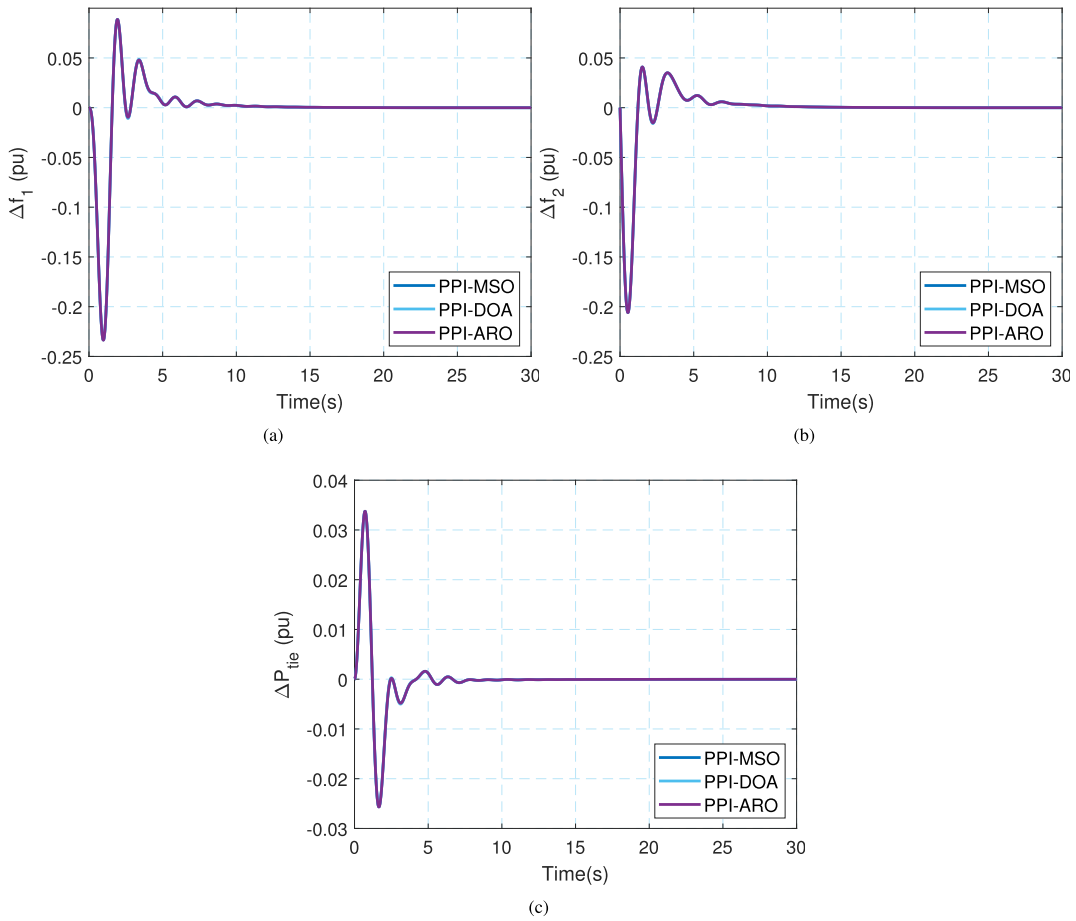


FIGURE 4 | Transient responses of PV–RT power system with PPI and FOPPI controllers for (a) Δf_1, (b) Δf_2 (c) ΔP_{tie}.

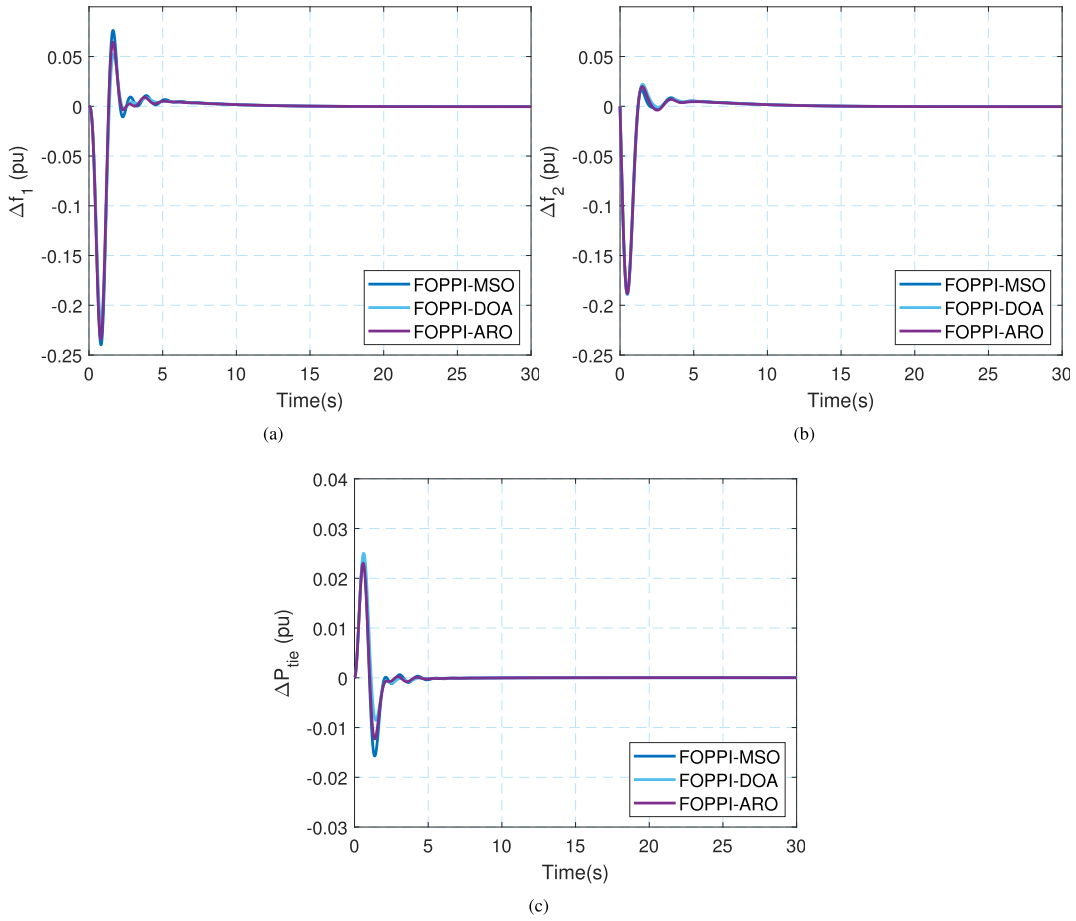


FIGURE 5 | Transient responses of PV–RT power system with PPI and FOPPI controllers for (a) Δf_1, (b) Δf_2 (c) ΔP_{tie}.

TABLE 6 | Transient responses of PV–RT power system with PPI and FOPPI controllers obtained by different optimisers.

		Settling time (0.2%)			Undershoot (p.u)			Overshoot (p.u)		
Controller	**Optimiser**	Δf_1	Δf_2	ΔP_{tie}	Δf_1	Δf_2	ΔP_{tie}	Δf_1	Δf_2	ΔP_{tie}
PPI	ARO	10.22	9.84	3.58	−0.2337	−0.2060	−0.0257	0.0887	0.0409	0.0338
	DOA	10.24	9.85	3.57	−0.2334	−0.2056	−0.0256	0.0886	0.0405	0.0337
	MSO	10.22	9.84	3.58	−0.2335	−0.2059	−0.0257	0.0886	0.0409	0.0338
FOPPI	ARO	9.34	9.28	1.92	−0.2339	−0.1884	−0.0123	0.0645	0.0198	0.0230
	DOA	9.34	9.28	1.91	−0.2166	−0.1894	−0.0086	0.0527	0.0222	0.0250
	MSO	9.57	9.54	1.89	−0.2398	−0.1877	−0.0157	0.0763	0.0165	0.0236

wise comparison in Table 6, confirm that FOPPI provides faster damping with lower oscillations than PPI.

3.2 | Comparative Time-Domain Analysis for PV–RT System

To fairly compare the performance of the proposed nonderivative and predictive controller architectures with existing methods in the literature, this section presents a comprehensive time-domain analysis. Table 7 lists the parameters of the PI controllers previously proposed in the literature and optimised using various heuristic algorithms (GA, FA, SFLA, WOA, WCA, BWOA, SSA, RIME and SHO) on the same PV–RT power system benchmark, along with the parameters of the PPI–ARO and FOPPI–ARO controllers proposed in this study. Although classical PI controllers possess only proportional and integral gains, it is observed that the predictive and fractional-order parameters included in the proposed structures provide the system with high control flexibility.

The transient responses of the proposed controllers under nominal conditions, compared with existing PI methods in the literature, are illustrated in Figure 6. The numerical performance metrics (settling time, overshoot and undershoot values) calculated based on the 0.2% settling band for these responses are presented in a comparative manner in Table 8.

Upon examining Figure 6 and Table 8, it is clear that classical PI controllers exhibit high-amplitude oscillations (overshoot/undershoot) due to the system's inertia and that their settling times

TABLE 7 | Optimal parameters of the proposed controllers and existing PI methods in the literature for PV–RT power system.

Controller	Area	K_p	K_i	K_{pt}	τ_{pt}	λ	λ_{pt}	μ_{pt}
PI-GA [50]	A_1	0.5663	0.4024	—	—	1.0000	—	—
	A_2	0.5127	0.7256	—	—	1.0000	—	—
PI-FA [50]	A_1	0.8811	0.5765	—	—	1.0000	—	—
	A_2	0.7626	0.8307	—	—	1.0000	—	—
PI-SFLA [51]	A_1	0.5156	0.9012	—	—	1.0000	—	—
	A_2	0.7896	0.8965	—	—	1.0000	—	—
PI-WOA [52]	A_1	0.4563	0.2254	—	—	1.0000	—	—
	A_2	0.8967	0.9865	—	—	1.0000	—	—
PI-WCA [53]	A_1	0.5737	0.0521	—	—	1.0000	—	—
	A_2	0.9312	0.7287	—	—	1.0000	—	—
PI-BWOA [54]	A_1	0.6671	0.5477	—	—	1.0000	—	—
	A_2	2.0000	0.8470	—	—	1.0000	—	—
PI-SSA [55]	A_1	0.7715	0.0483	—	—	1.0000	—	—
	A_2	1.0837	0.8929	—	—	1.0000	—	—
PI-RIME [56]	A_1	0.4540	0.0935	—	—	1.0000	—	—
	A_2	2.0000	0.9436	—	—	1.0000	—	—
PI-SHO [57]	A_1	0.6701	0.5371	—	—	1.0000	—	—
	A_2	2.0000	0.8476	—	—	1.0000	—	—
PPI–ARO (proposed)	A_1	1.9999	0.1128	1.1298	1.0290	1.0000	1.0000	1.0000
	A_2	1.2459	2.0000	0.0003	0.0326	1.0000	1.0000	1.0000
FOPPI–ARO (proposed)	A_1	1.9412	1.9982	1.5134	1.3598	0.0171	0.9896	0.8913
	A_2	1.9984	1.9976	0.1328	1.4528	0.8477	0.0185	0.9991

are quite long. Even in the WCA and RIME algorithms—which yield the best results in terms of dynamic performance among existing methods in the literature—these times can only be reduced to the 14–15-s range. In contrast, the proposed FOPPI–ARO controller, despite not incorporating the risky derivative effect into the equation, has demonstrated a superior damping profile thanks to the fractional-order dead-time compensator it contains. FOPPI–ARO has significantly outperformed existing methods in the literature by reducing the settling times of Δf_1 and Δf_2 to 9.34 and 9.28 s, respectively and the settling time of ΔP_{tie} to 1.92 s. Similarly, overshoot values have also been minimised compared to other PI controllers in the literature.

3.3 | Time Domain Analysis for PV-RT Governor Dead Band System

The transient response performance of the PV–RT–GDB power system is evaluated in the time domain. Using the optimum parameters reported in Table 9, Figure 7 depicts the frequency deviations (Δf_1, Δf_2) and tie-line power deviation (ΔP_{tie}) under PPI and FOPPI controllers. Compared to PPI, the FOPPI controller significantly reduces the overshoot of Δf_1 from 0.1303 p.u to 0.0873 p.u (33.0% reduction)s and the overshoot of Δf_2 from 0.0519 p.u to 0.0404 p.u (22.2% reduction). Similarly, the overshoot of ΔP_{tie} decreases from 0.0398 p.u to 0.0316 p.u (20.6% reduction). In terms of undershoot magnitude, FOPPI improves Δf_1 from 0.2955 p.u to 0.2845 p.u (3.7% reduction), Δf_2 from 0.2456 p.u to 0.2356 p.u (4.1% reduction) and ΔP_{tie} from 0.0333 p.u to 0.0170 p.u (48.9% reduction). Moreover, FOPPI shortens the settling time (0.2% criterion) for Δf_1 from 10.82 to 10.57 s (2.3%) and for ΔP_{tie} from 5.12 to 2.31 s (54.9%), whereas the settling time of Δf_2 remains comparable (10.45 vs. 10.50 s). These quantitative results, summarised in Table 10, confirm that FOPPI provides faster damping with reduced oscillations compared to PPI for the PV–RT–GDB case.

3.4 | Robustness Analysis

In a system, system parameters can change instantaneously or gradually due to internal and external effects. This may adversely affect the performance in controlling the system and may even lead the system to instability. For this reason, controllers designed for a system are expected to be robust against system parameter changes. In this section, the robustness of the PPI and FOPPI controllers against system parameter changes is analysed. In this analysis, system parameters τ_G, τ_T, τ_{12}, B and R are changed by $\pm$ 50%. As a result of this change, the transient response performances of the PV–RT power system with PPI and FOPPI controllers for $\Delta f_1, \Delta f_2$ and ΔP_{tie} are given in Tables 11 and 12, respectively. When the transient responses of the systems with both controllers are analysed, it is seen that the systems are not unstable and even the transient state is damped and the response settles. In addition, comparing Tables 11 and 12, it can be said that the system with the FOPPI controller has shorter settling times than the system with the PPI controller and performs better in undershoot/overshoot. Quantitatively, when all $\pm$ 50% parameter variations are considered, the average settling times of the PPI-controlled system are 11.08, 10.90 and 5.15 s

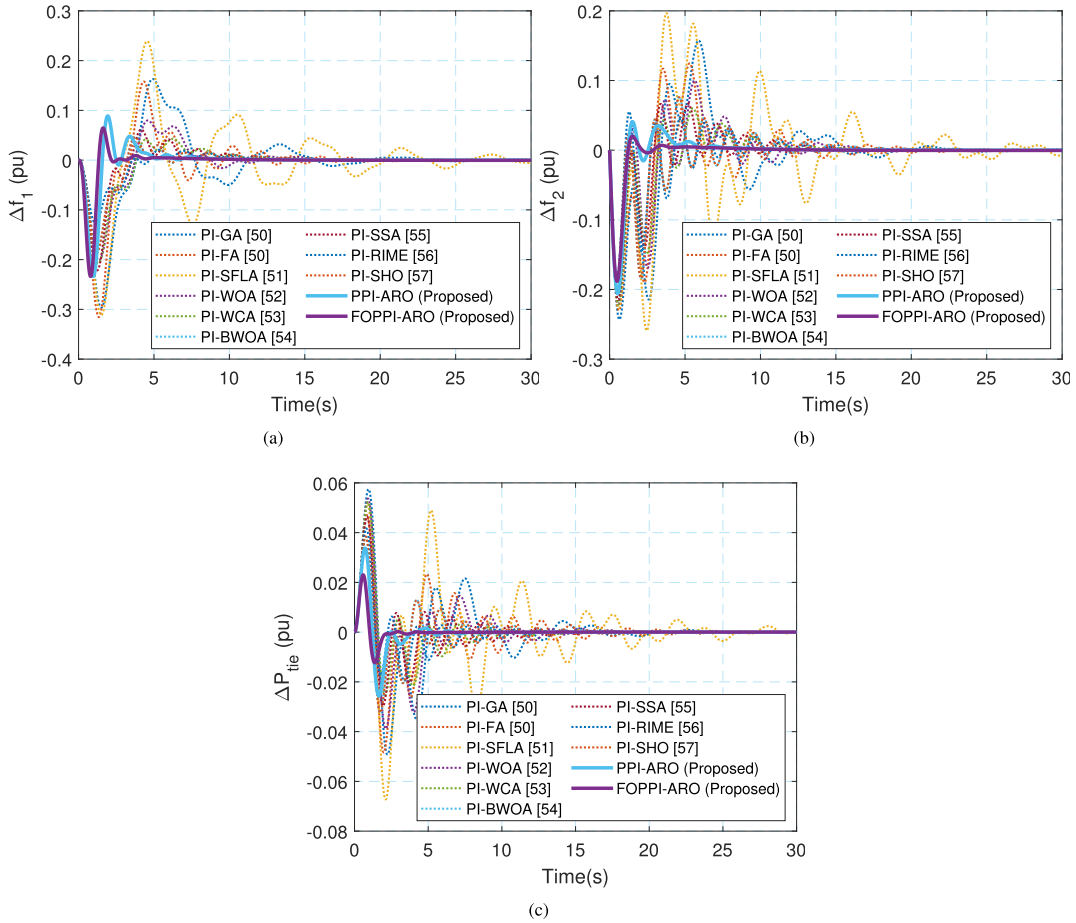


FIGURE 6 | Transient responses of PV–RT power system comparing the proposed PPI/FOPPI controllers with the existing PI controllers in the literature for (a) Δf_1, (b) Δf_2 (c) ΔP_{tie}.

TABLE 8 | Comparative transient responses of PV–RT power system using the proposed controllers and existing PI methods in the literature.

	Settling time (0.2%) (s)			Undershoot (p.u)			Overshoot (p.u)		
Controller	Δf_1	Δf_2	ΔP_{tie}	Δf_1	Δf_2	ΔP_{tie}	Δf_1	Δf_2	ΔP_{tie}
PI-GA [50]	25.67	24.66	16.41	−0.2965	−0.2431	−0.0492	0.1630	0.1574	0.0575
PI-FA [50]	22.03	23.16	16.66	−0.3154	−0.2302	−0.0483	0.1579	0.1246	0.0470
PI-SFLA [51]	38.75	39.33	28.34	−0.3115	−0.2592	−0.0673	0.2390	0.1967	0.0515
PI-WOA [52]	15.36	17.94	12.60	−0.2020	−0.2212	−0.0388	0.0797	0.0999	0.0536
PI-WCA [53]	14.69	15.74	10.11	−0.2074	−0.2217	−0.0253	0.0429	0.0600	0.0523
PI-BWOA [54]	17.18	19.71	10.99	−0.1872	−0.1867	−0.0326	0.0470	0.0767	0.0384
PI-SSA [55]	15.65	16.73	11.40	−0.2216	−0.2150	−0.0297	0.0614	0.0666	0.0465
PI-RIME [56]	15.67	16.71	8.70	−0.1280	−0.1861	−0.0195	0.0209	0.0553	0.0417
PI-SHO [57]	17.17	19.70	10.99	−0.1868	−0.1867	−0.0324	0.0460	0.0759	0.0384
PPI-ARO (proposed)	10.22	9.84	3.58	−0.2337	−0.2060	−0.0257	0.0887	0.0409	0.0338
FOPPI-ARO (proposed)	**9.34**	**9.28**	**1.92**	**−0.2339**	**−0.1884**	**−0.0123**	**0.0645**	**0.0198**	**0.0230**

Note: The bold values indicate the best performance results among the compared methods.

TABLE 9 | Optimal PPI and FOPPI controller parameters in PV–RT–GDB power system obtained by ARO.

Controller	Area	$K_{p_{1/2}}$	$K_{i_{1/2}}$	$K_{pt_{1/2}}$	$\tau_{pt_{1/2}}$	$\lambda_{1/2}$	$\lambda_{pt_{1/2}}$	$\mu_{pt_{1/2}}$
PPI	A_1	2.0000	0.1068	0.9607	1.0666	1.0000	1.0000	1.0000
	A_2	1.3928	2.0000	0.0052	0.0054	1.0000	1.0000	1.0000
FOPPI	A_1	1.9697	1.7930	1.7792	1.9770	0.1857	0.9226	0.8293
	A_2	1.9558	1.9964	0.1917	1.2994	0.8757	0.3046	0.9796

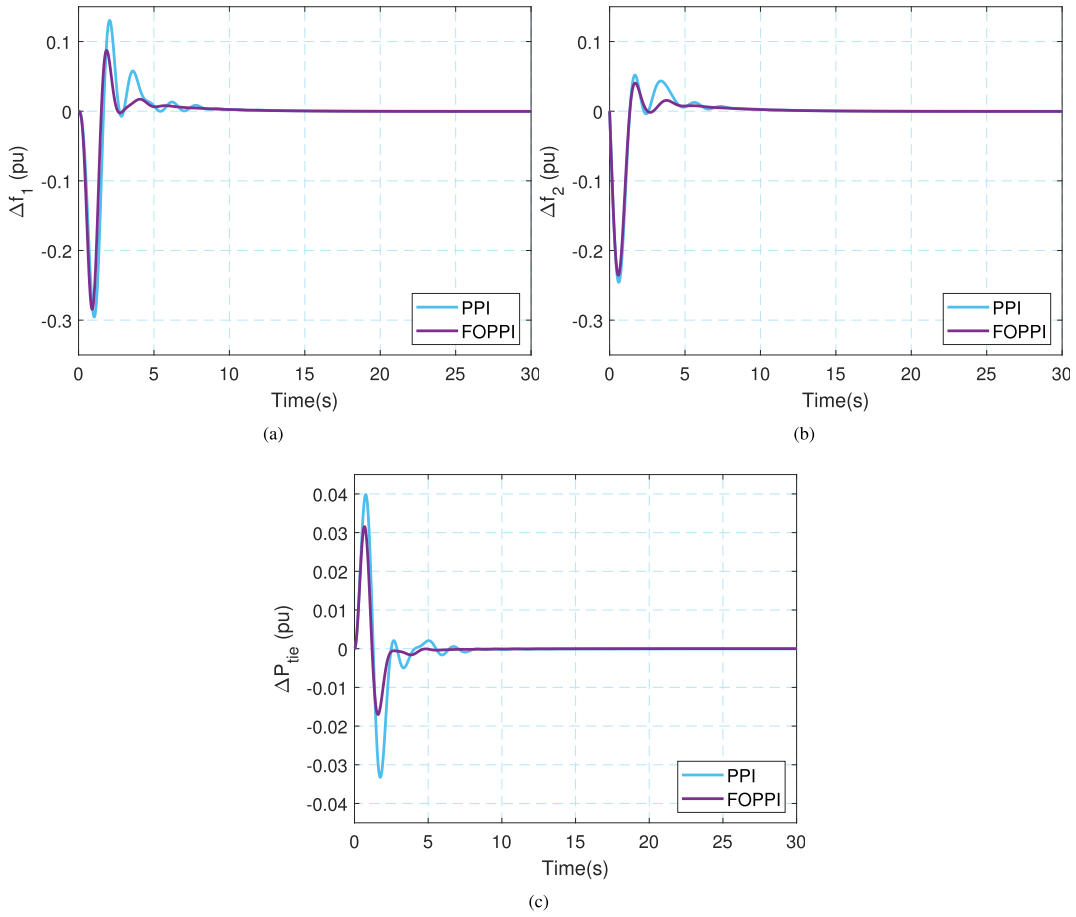


FIGURE 7 | Transient responses of PV–RT–GDB power system with PPI and FOPPI controllers for (a) Δf_1, (b) Δf_2 (c) ΔP_{tie}.

TABLE 10 | Transient responses of PV–RT–GDB power system with PPI and FOPPI controllers.

	Settling time (0.2%)			Undershoot (p.u)			Overshoot (p.u)		
Controller	Δf_1	Δf_2	ΔP_{tie}	Δf_1	Δf_2	ΔP_{tie}	Δf_1	Δf_2	ΔP_{tie}
PPI	10.82	10.45	5.12	−0.2955	−0.2456	−0.0333	0.1303	0.0519	0.0398
FOPPI	10.57	10.50	2.31	−0.2845	−0.2356	−0.0170	0.0873	0.0404	0.0316

TABLE 11 | Robustness performance of PV–RT power system with PPI controller.

		Settling time (0.2%)			Undershoot (pu)			Overshoot (pu)		
p	**RoC %**	Δf_1	Δf_2	ΔP_{tie}	Δf_1	Δf_2	ΔP_{tie}	Δf_1	Δf_2	ΔP_{tie}
τ_G	+50	10.19	9.81	4.97	−0.2472	−0.2161	−0.0298	0.1139	0.0608	0.0355
	−50	10.22	9.87	3.41	−0.2193	−0.1942	−0.0214	0.0638	0.0283	0.0318
τ_T	+50	9.12	10.18	5.25	−0.2632	−0.2253	−0.0318	0.1284	0.0720	0.0371
	−50	11.14	10.59	4.27	−0.1947	−0.1784	−0.0157	0.0514	0.0258	0.0289
τ_{12}	+50	14.05	12.22	7.60	−0.2427	−0.1931	−0.0228	0.0616	0.0348	0.0374
	−50	13.13	14.53	8.51	−0.1967	−0.2245	−0.0224	0.0812	0.1150	0.0260
B	+50	10.29	9.76	4.55	−0.1987	−0.1863	−0.0288	0.1192	0.0772	0.0300
	−50	12.14	12.13	4.60	−0.2855	−0.2362	−0.0171	0.0511	0.0455	0.0390
R	+50	10.21	9.85	4.97	−0.2423	−0.2114	−0.0267	0.0940	0.0438	0.0347
	−50	10.35	10.02	3.41	−0.2110	−0.1921	−0.0233	0.0768	0.0375	0.0312

for Δf_1, Δf_2 and ΔP_{tie}, respectively. In contrast, the FOPPI controller achieves average settling times of 9.44, 9.35 and 2.65 s, corresponding to average reductions of 14.8%, 14.2% and 48.7%. Moreover, the worst-case settling time of ΔP_{tie} decreases from 8.51 s (PPI) to 3.78 s (FOPPI), that is, a 55.6% improvement. Regarding oscillatory behaviour, the average overshoot is reduced from 0.0841 to 0.0616 p.u for Δf_1 (26.8%), from 0.0541 to 0.0310 p.u for Δf_2 (42.7%) and from 0.0332 to 0.0227 p.u for ΔP_{tie} (31.7%).

In addition to the transient responses of the system given in the tables as a result of the robustness analysis, the performance of the system with the PPI and the FOPPI controllers under variations of parameter B is illustrated graphically in Figures 8 and 9 to better observe the transient behaviour. Since presenting figures for all five parameters would require excessive space, only the responses corresponding to B are provided as B yields one of the most pronounced changes in transient characteristics according to Tables 11 and 12.

TABLE 12 | Robustness performance of PV–RT power system with FOPPI controller.

		Settling time (0.2%)			Undershoot (pu)			Overshoot (pu)		
p	RoC %	Δf_1	Δf_2	ΔP_{tie}	Δf_1	Δf_2	ΔP_{tie}	Δf_1	Δf_2	ΔP_{tie}
τ_G	+50	9.33	9.28	2.01	−0.2480	−0.1994	−0.0148	0.0899	0.0428	0.0242
	−50	9.39	9.32	2.44	−0.2180	−0.1757	−0.0096	0.0392	0.0057	0.0216
τ_T	+50	9.45	9.29	3.34	−0.2620	−0.2090	−0.0151	0.1009	0.0692	0.0252
	−50	9.49	9.43	2.53	−0.1943	−0.1597	−0.0072	0.0192	0.0068	0.0197
τ_{12}	+50	9.26	9.28	2.57	−0.2414	−0.1794	−0.0089	0.0345	0.0272	0.0252
	−50	9.58	9.18	3.78	−0.2002	−0.2015	−0.0122	0.0754	0.0646	0.0183
B	+50	7.74	7.68	2.73	−0.2007	−0.1672	−0.0158	0.1025	0.0443	0.0205
	−50	11.6	11.55	2.88	−0.2831	−0.2241	−0.0061	0.0228	0.0091	0.0265
R	+50	9.33	9.28	2.11	−0.2399	−0.1925	−0.0122	0.0638	0.0241	0.0235
	−50	9.27	9.23	2.06	−0.2176	−0.1775	−0.0127	0.0681	0.0162	0.0218

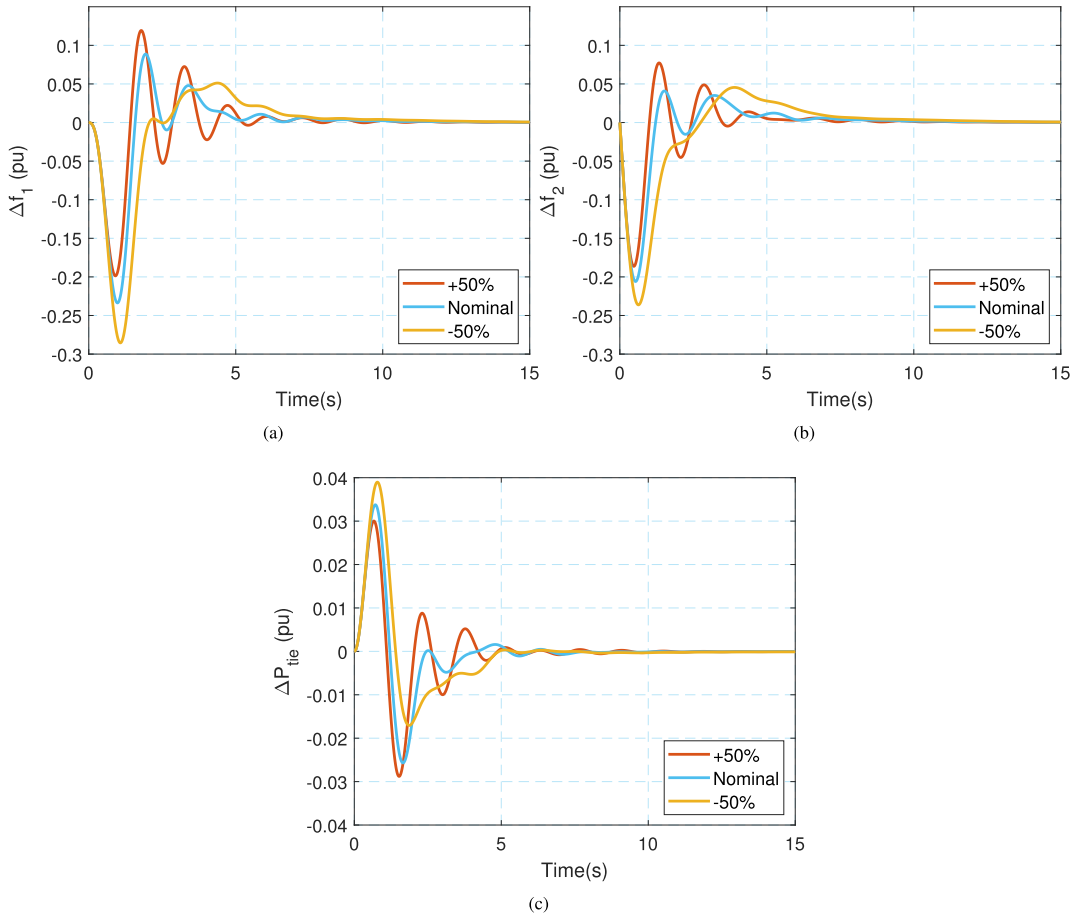


FIGURE 8 | Robustness performance of PV–RT power system with PPI controller for (a) Δf_1, (b) Δf_2 (c) ΔP_{tie}.

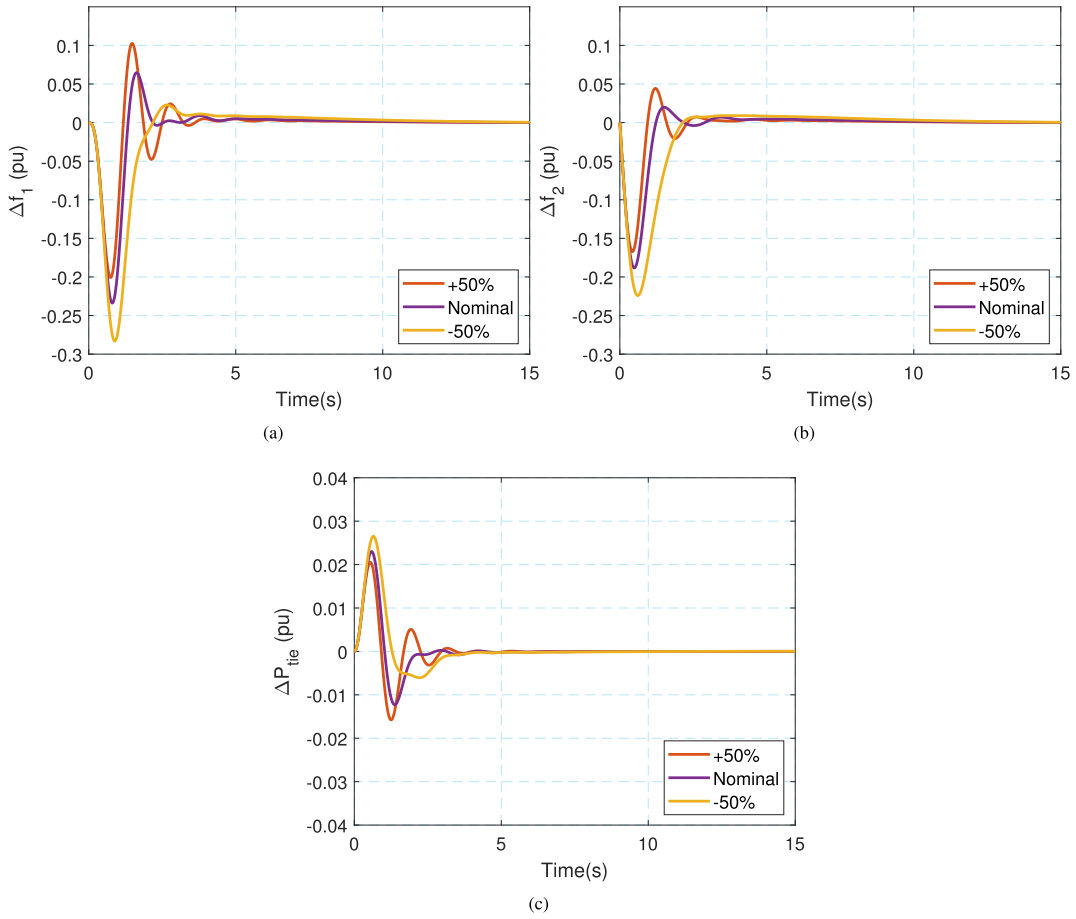


FIGURE 9 | Robustness performance of PV–RT power system with FOPPI controller for (a) Δf_1, (b) Δf_2 (c) ΔP_{tie}.

3.5 | Random Load Change Analysis

Two distinct random load signals have been applied to both energy units under this subtitle, and the performances of the proposed controllers are analysed. The load signals are generated with the blocks of band-limited white noise, first-order transfer function, constant and mathematical operations accessed in MATLAB/Simulink library. The load signals applied to the PV and reheat thermal power units are shown in Figure 10a. A numerical analysis employing maximum deviation (MD) and ITAE value is tabulated in Table 13. The system responses are depicted in Figure 10b–d. It is evident from the results obtained that the ITAE value with FOPPI and PPI controller is calculated as 200.2 and 238.8, respectively. This constitutes a 16.2% improvement with the FOPPI controller. Moreover, it has been demonstrated that the MD values for Δf_1, Δf_2 and ΔP_{tie} attained with the FOPPI controller is less than the PPI controller.

3.6 | Stability Assessment and Angular Consistency Analysis

The stability of the proposed two-area PV-integrated LFC system is evaluated through a dual-perspective approach: eigenvalue analysis of the rationalised model and an angular consistency check based on fractional-order (FO) stability theory. Since the system is linearised around the nominal operating point, the results characterise the local asymptotic stability (LAS) of the equilibrium.

First, the FO operators in the FOPPI controller are implemented using the Oustaloup recursive approximation (ORA) within a frequency range of $\omega \in [10^{-3}, 10^{3}]$ rad/s with $N = 5$. This yields a high-order rationalised integer-order model that represents the controller's practical implementation. To ensure stability, the complete eigenvalue spectrum of the augmented system matrix was computed. It was verified that all eigenvalues lie in the open left-half of the s-plane ($\Re\{s_k\} < 0, \forall k$), confirming that the rationalised closed-loop model is locally asymptotically stable within the valid frequency range of the ORA.

Second, to align the numerical results with fractional-order control principles, the distribution of the characteristic roots is evaluated against the FO stability sectors. Although the overall system exhibits incommensurate dynamics due to the combination of integer-order plant models and distinct fractional orders (λ, μ), the locations of the dominant roots provide a significant measure of stability margins. According to FO stability theory, the stable region in the complex plane is defined by an angular sector determined by the commensurate order q. For the proposed FOPPI–ARO scheme, the dominant roots are identified at $s_{1,2} = -0.2975 \pm j1.7913$. The phase angle of these roots is analytically calculated in Equation (68) as follows:

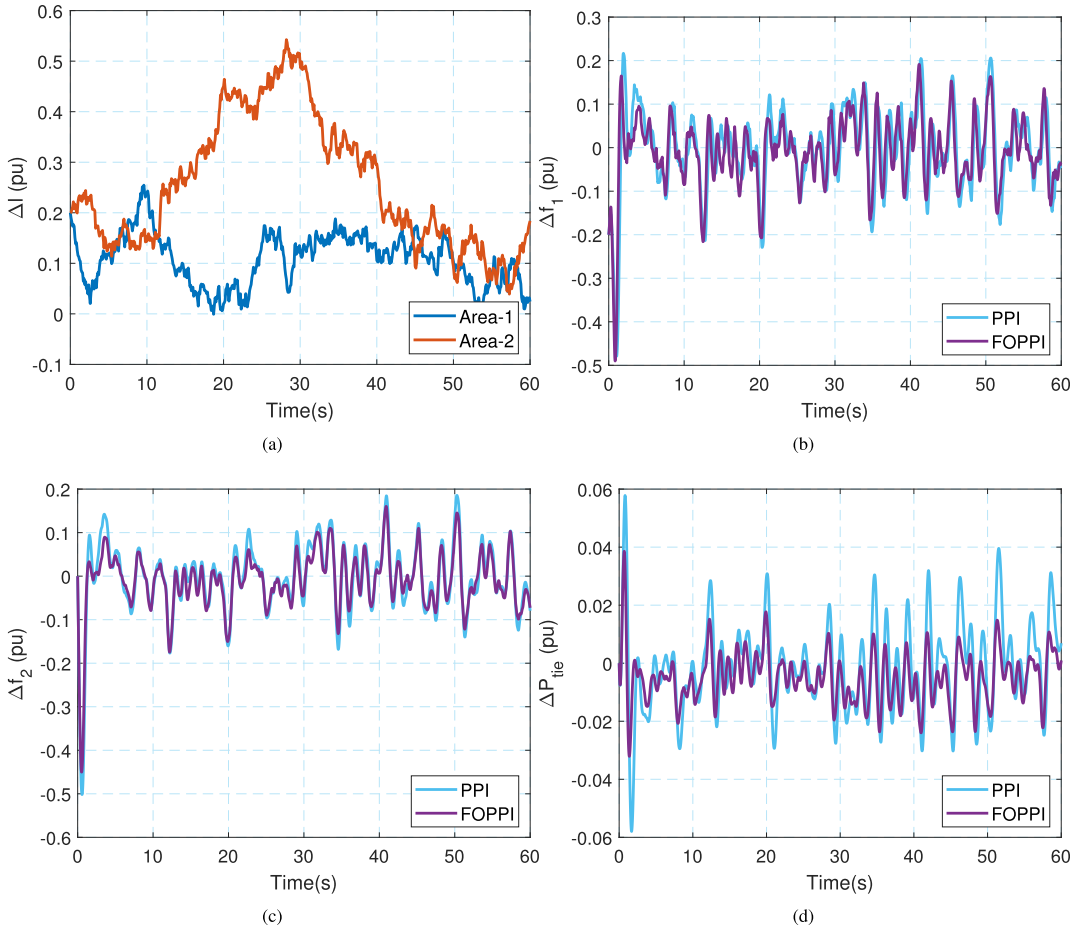


FIGURE 10 | (a) RLC signal and RLC performance of PV–RT power system with PPI and FOPPI controllers for (b) Δf_1, (c) Δf_2 (d) ΔP_{tie}.

TABLE 13 | RLC performance of PV–RT power system with PPI and FOPPI controllers.

	MD			
Controllers	Δf_1	Δf_2	ΔP_{tie}	**ITAE**
FOPPI	0.6815	0.6105	0.0707	200.2
PPI	0.6962	0.6875	0.1158	238.8

$$|\arg(s_{1,2})| = \pi - \arctan\left(\frac{1.7913}{0.2975}\right) \approx 99.43^\circ \tag{68}$$

Although the dominant roots are highlighted in Table 14 for illustration, the entire root spectrum was verified to lie within the stability sector. Given that 99.43° significantly exceeds the 90° boundary (the sector limit for the maximum possible order $q = 1$), the root placement is highly consistent with Matignon-type stability conditions. This multifaceted assessment confirms that the system is numerically stable in its implemented form and theoretically aligned with the sectorial stability requirements of fractional-order dynamics.

3.7 | Cyberattack Performance of Controllers

In order for the analysis discussed in this section to be applied in studies using a similar system, the MATLAB/Simulink file and the.xlsx file containing the attack scenarios can be accessed from the link given in the abstract. In this section, the performance of the PV–RT power system with optimally tuned PPI and FOPPI controllers under cyberattack is discussed. To measure the performance of systems with PPI and FOPPI controllers, 720 cyberattack scenarios are used. These scenarios are applied to the system and the performance metric ITAE values are recorded. The statistical analysis of the total 720 ITAE scores obtained for each controller system by calculating the mean, standard deviation, median, max and min values are given in Table 15. Table 15 shows that the mean ITAE of the system with the FOPPI controller is about half of the mean ITAE of the system with the PPI controller. Table 15 also shows that the standard deviation of ITAE values is small in the FOPPI controller system.

In addition to the statistical values in Table 15, Figure 11 shows the histograms and box plots for the ITAE values obtained using the FOPPI and PPI controllers. When the histogram graph shown in Figure 11a is analysed, it is seen that the ITAE values are more spread out in the graph in the system with the PPI

TABLE 14 | Eigenvalue-based stability metrics and phase angle analysis for PPI and FOPPI controllers.

Controller	Dominant Root(s)	$\Re\{s_{\max}\}$	Phase angle $\lvert\arg(s)\rvert$
FOPPI–ARO	$-0.2975 \pm j1.7913$	-0.2975	99.43°
PPI–ARO	-0.1038	-0.1038	180.00°

TABLE 15 | Statistical analysis of PV–RT power system with PPI and FOPPI controllers under cyberattack.

Controllers	Mean	Standard deviation	Median	Max	Min
FOPPI	0.4521	0.4358	0.3943	5.4377	0.0007
PPI	0.8787	0.7302	0.7509	5.9786	0.0011

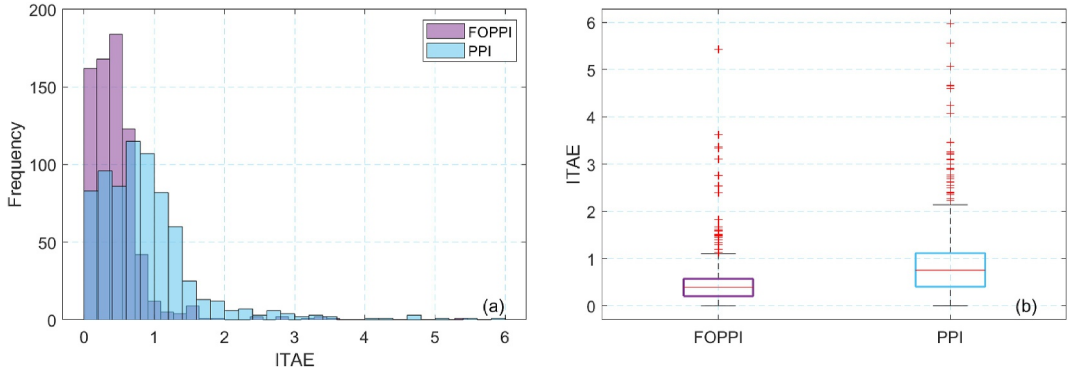


FIGURE 11 | Histograms and box plots for PV–RT power system with PPI and FOPPI controllers.

controller and the ITAE values are gathered between 0 and one in the system with the FOPPI controller. Figure 11b shows that the box plot obtained for the system with the FOPPI controller is closer to 0 and more stable than the system with the PPI controller.

3.8 | Cyberattack Detection

In the trained CNN model, a threshold value is set using test data with 360 normal scenarios and those exceeding this threshold are detected as cyberattacks. The threshold is set to ensure that all normal scenarios in the test data are detected as normal (i.e., zero false alarms on the normal test set). Thanks to this model and the threshold value, 668 out of 720 cyberattack scenarios are detected as cyberattacks (recall = 668/720 = 0.9278). The remaining 52 cyberattack scenarios are detected as normal (FNR = 52/720 = 0.0722). According to these results, TP, TN, FP and FN metrics are 668, 360, 0 and 52, respectively. The performance metrics obtained using TP, TN, FN and FP metrics are given in Table 16. The high accuracy rate (0.9518) in Table 16 demonstrates the overall classification success. In addition, the precision rate (1), which reveals how many of the detected cyberattacks are actually cyberattacks, and the recall rate (0.9278), which reveals how many of the cyberattacks can be detected, prove the successful performance of the trained model (FP = 0 over 360 normal scenarios implies FPR = 0 and 100% specificity). The table also shows the performance of the trained model by sharing the F1 score, FPR and FNR values (F1 score = 0.9625).

In addition to all the results shared in this section, the scenario IDs determined as FN are shared in Table 17 as it will be useful for further studies in this field. This table provides information on the change of load, which areas have been cyber attacked, the severity of the cyberattacks and the attack type. It should be noted that the undetected set contains 52 scenarios (i.e., 7.22% of the 720 cyberattack test cases). Among these FN cases, 38 scenarios are DoS-only (73.1%) and 14 scenarios are FDI-only (26.9%). It is seen that those that are cyberattacks but not detected are generally low-severity attacks, and if the attack severity is high, the load change is low. This observation is also supported by the magnitude of the load change in Table 17: Seventy-five percent of the FN cases have $|\Delta l_2| \leq 0.02$, indicating that most missed attacks cause relatively small load variations. In other words, because the disruptive impact of the attack on the system is low, the detector does not detect these attacks as a threat.

4 | Conclusion

In this study, the FOPPI controller is proposed as a novel structure by modelling the dead-time approach within a fractional-order framework. The parameter tuning of the PPI and FOPPI controllers is carried out using the ARO, DOA and MSO optimisation algorithms, and the consistency of the obtained settings under different optimisation strategies is also assessed. The effectiveness of the controllers is validated through time-domain analysis, robustness under parameter uncertainty, random load change conditions and closed-loop stability analysis. In addition, a total of 720 cyber-attack

TABLE 16 | Performance metrics.

Accuracy	Precision	Recall	F1−score	FPR	FNR
0.9518	1	0.9278	0.9625	0	0.0722

TABLE 17 | Undetected cyberattacks.

ID	FDI-A1	FDI-A2	DoS-A1	DoS-A2	Δl_2	ID	FDI-A1	FDI-A2	DoS-A1	DoS-A2	Δl_2
737	1	1.0464	0	0	−0.0031	1111	1	1	0	0.0027	−0.0489
740	1	1.0320	0	0	0.0062	1113	1	1	0	0.0022	0.0896
741	1	1.0352	0	0	−0.0189	1114	1	1	0	0.0064	0.0169
767	1.0543	1	0	0	0.0111	1115	1	1	0	0.0046	0.0655
770	1.0852	1	0	0	0.0116	1116	1	1	0	0.0085	−0.0115
813	1.1626	1.2382	0	0	0.0011	1120	1	1	0	0.0042	0.0142
828	1.0760	1.0697	0	0	0.0060	1130	1	1	0.0089	0	0.0174
845	1	1.2706	0	0	0.0024	1140	1	1	0.0152	0	−0.0135
872	1	1.3579	0	0	0.0003	1144	1	1	0.0199	0	0.0036
887	1.4237	1	0	0	−0.0015	1154	1	1	0.0111	0	0.0160
902	1.3724	1	0	0	0.0008	1156	1	1	0.0113	0	−0.0136
982	1	1.8064	0	0	0.0008	1157	1	1	0.0013	0	0.0425
1017	1.7928	1	0	0	0.0016	1159	1	1	0.0059	0	−0.0043
1036	1.8532	1	0	0	−0.0010	1163	1	1	0.0087	0.0044	−0.0058
1084	1	1	0	0.0055	0.0579	1170	1	1	0.0113	0.0069	0.0086
1085	1	1	0	0.0118	−0.0104	1172	1	1	0.0012	0.0184	−0.0073
1087	1	1	0	0.0052	0.0285	1173	1	1	0.0010	0.0016	0.0285
1092	1	1	0	0.0124	0.0241	1188	1	1	0.0031	0.0087	0.0215
1093	1	1	0	0.0027	−0.0655	1196	1	1	0.0040	0.0166	−0.0163
1096	1	1	0	0.0054	0.0450	1217	1	1	0	0.0298	0.0046
1097	1	1	0	0.0164	0.0152	1229	1	1	0	0.0262	0.0082
1100	1	1	0	0.0022	0.0023	1278	1	1	0.0356	0	0.0001
1102	1	1	0	0.0168	0.0059	1350	1	1	0	0.0762	−0.0015
1105	1	1	0	0.0031	0.0504	1358	1	1	0	0.0746	−0.0001
1107	1	1	0	0.0195	0.0049	1391	1	1	0.0760	0	0.0003
1108	1	1	0	0.0069	0.0421	1408	1	1	0.0662	0.0569	0.0009

scenarios, including both FDI and DoS attacks, are generated, and the controller performance is statistically analysed under these attacks. Moreover, a 1D-CNN-based model is developed for cyberattack detection and its performance is reported. Overall, this study provides both a benchmark dataset enabling fair comparisons and a reusable detection infrastructure, and it quantitatively demonstrates the impact of the derivative-free PPI approach as an alternative to the PI structure and its fractional-order extension (FOPPI) on dynamic performance and resilience. The main quantitative findings are summarised below in a bullet-point form.

- In the time-domain analysis (0.2% settling band), the proposed FOPPI controller reduces both oscillations and settling times compared to PPI. For the ARO-tuned case, the overshoot decreases by 27.3% for Δf_1 (0.0887 → 0.0645 p.u), by 51.6% for Δf_2 (0.0409 → 0.0198 p.u) and by 32.0% for ΔP_{tie} (0.0338 → 0.0230 p.u). The settling times improve from 10.22 to 9.34 s for Δf_1 (8.6%), from 9.84 to 9.28 s for Δf_2 (5.7%) and from 3.58 to 1.92 s for ΔP_{tie} (46.4%) (Table 6, Figures 4–5).
- Under the governor dead-band condition (PV–RT–GDB), FOPPI further improves transient performance, particularly for the tie-line power. The overshoot is reduced by 33.0% for Δf_1 (0.1303 → 0.0873 p.u), by 22.2% for Δf_2 (0.0519 → 0.0404 p.u) and by 20.6% for ΔP_{tie} (0.0398 → 0.0316 p.u). Moreover, the ΔP_{tie} undershoot magnitude decreases by 48.9% (0.0333 → 0.0170 p.u), and the 0.2% settling time of ΔP_{tie} is shortened from 5.12 to 2.31 s (54.9%) (Table 10, Figure 7).
- In the robustness study with ±50% variations in $(\tau_G, \tau_T, \tau_{12}, B, R)$, both controllers preserve stability, whereas FOPPI achieves shorter settling times and improved oscillatory behaviour. Averaged over all ±50% variations, the settling times are reduced from 11.08 to 9.44 s for Δf_1 (14.8%), from 10.90 to 9.35 s for Δf_2 (14.2%) and from 5.15 to 2.65 s for ΔP_{tie} (48.7%). In addition, the worst-case settling

time of ΔP_{tie} decreases from 8.51 s (PPI) to 3.78 s (FOPPI) corresponding to a 55.6% improvement (Tables 11 and 12).

- Under random load change conditions, FOPPI improves the ITAE from 238.8 to 200.2, yielding a 16.2% improvement, and produces lower maximum deviation (MD) values for all outputs (Δf_1: 0.6962 → 0.6815, Δf_2: 0.6875 → 0.6105 and ΔP_{tie}: 0.1158 → 0.0707) (Table 13, Figure 10).
- The closed-loop stability analysis based on dominant (rightmost) poles confirms internal stability for both controllers. The FOPPI-controlled system exhibits dominant poles at $-0.2975 \pm j1.7913$, whereas the PPI-controlled system has a dominant pole at -0.103757. The relative stability margin increases from $\alpha = 0.1038$ (PPI) to $\alpha = 0.2975$ (FOPPI), that is, approximately a 2.87-fold improvement, indicating faster decay characteristics with FOPPI (Table 14).
- Across 720 cyberattack scenarios, FOPPI yields a lower and more consistent ITAE distribution than PPI. The mean ITAE decreases from 0.8787 to 0.4521 (48.5% improvement), the median decreases from 0.7509 to 0.3943 and the standard deviation reduces from 0.7302 to 0.4358, indicating enhanced robustness under attacks (Table 15, Figure 11).
- For cyberattack detection, the threshold is selected to yield zero false alarms on 360 normal test scenarios (FPR = 0). The detector correctly identifies 668 out of 720 attack scenarios, achieving 95.18% accuracy, 1.00 precision, 0.9278 recall and a 0.9625 F1 score. The remaining 52 missed attacks correspond to 7.22% of the attack test set; among these false negatives, 73.1% are DoS-only and 26.9% are FDI-only and 75% satisfy $|\Delta l_2| \leq 0.02$ (Tables 16 and 17).

In future work, we aim to validate the proposed PPI/FOPPI-based approach on more realistic and higher-order power-system models. In this context, benchmark systems that better represent parameter heterogeneity and include a large number of generation units (e.g., the IEEE 39-bus system) will be considered to systematically investigate load–frequency dynamics, inter-area interactions and the impact of diverse generator/governor–turbine parameters on closed-loop performance. In addition, real-time tests will be conducted on real-time simulator platforms to demonstrate the practical implementability of the proposed controllers. Along with these extensions, the benchmark methodology introduced in this study, based on randomly varying load conditions and scenarioised FDI/DoS attacks, will be expanded to higher-order systems to support fair and reproducible comparisons for both controller robustness and AI-based cyberattack detection studies [58].

Acknowledgements

Erdinç Şahin would like to thank the support provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK) BİDEB 2219 under application number 1059B192301365. Bora Çavdar would like to thank the Scientific and Technological Research Council of Türkiye (TÜBİTAK) for the support provided through the 2211-C program.

Funding

This work was supported by open access funding from the Scientific and Technological Research Council of Türkiye (TÜBİTAK).

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The dataset and simulation models used in this study are publicly available through Zenodo and GitHub. These files include the data and models required to evaluate the performance of the proposed and comparative controllers under cyberattack scenarios. The archived repository is available at: https://doi.org/10.5281/zenodo.20379710, and the development repository is available at: https://github.com/Bora-Cavdar/Fractional-Order-PPI-Cyberattack-Dataset-Cyberattack-Test-Benchmark-for-PV-RT-Power-Systems.git.

References

1. H. Saadat, *Power System Analysis*, 2 (McGraw-Hill, 1999).

2. O. I. Elgerd, *Electric Energy Systems Theory: An Introduction*, 2nd ed. (McGraw-Hill, 1982).

3. X. Chen, S. Hu, Y. Li, D. Yue, C. Dou, and L. Ding, "Co-Estimation of State and FDI Attacks and Attack Compensation Control for Multi-Area Load Frequency Control Systems Under FDI and Dos Attacks," *IEEE Transactions on Smart Grid* 13, no. 3 (2022): 2357–2368, https://doi.org/10.1109/tsg.2022.3147693.

4. U. Raj, R. Shankar, S. Rani, and M. Ranjan, "Enhanced Load Frequency Regulation in Cyberattack Triggered Grids With Renewable Energy and Electric Vehicles," *Electrical Engineering* 107, no. 6 (2024): 1–19, https://doi.org/10.1007/s00202-024-02925-4.

5. P. K. Vidyarthi, A. Kumar, and S. Raj, "Chaos Quasi-Opposition Sea-Horse Based Modified New Tilt Controller Designed for Multi-Area Deregulated AGC Using Deep Learning Against Cyber-Attacks," *Chaos, Solitons & Fractals* 188 (2024): 115542, https://doi.org/10.1016/j.chaos.2024.115542.

6. S. Yıldız, B. Yildirim, and M. T. Özdemir, "Enhancing Load Frequency Control and Cybersecurity in Renewable Energy Microgrids: A Fuel Cell-Based Solution With Non-Integer Control Under Cyber-Attack," *International Journal of Hydrogen Energy* 75 (2024): 438–449, https://doi.org/10.1016/j.ijhydene.2024.02.145.

7. D. Kumar, G. L. Raja, M. Alkhatib, A. K. Deep, and U. R. Muduli, "Smith Predictor Based Fractional LFC Strategy for Storage Supported Thermal Power System Amid Communication Dead Time and Cyber Threats," *IEEE Transactions on Industry Applications* 61, no. 3 (2025): 4515–4529, https://doi.org/10.1109/TIA.2025.3549020.

8. M. Khalaf, A. Youssef, and E. El-Saadany, "Joint Detection and Mitigation of False Data Injection Attacks in AGC Systems," *IEEE Transactions on Smart Grid* 10, no. 5 (2018): 4985–4995, https://doi.org/10.1109/tsg.2018.2872120.

9. A. D. Syrmakesis, H. H. Alhelou, and N. D. Hatziargyriou, "A Novel Cyber Resilience Method for Frequency Control in Power Systems Considering Nonlinearities and Practical Challenges," *IEEE Transactions on Industry Applications* 60, no. 2 (2023): 2176–2190, https://doi.org/10.1109/tia.2023.3332702.

10. S. Oshnoei, M. R. Aghamohammadi, and M. H. Khooban, "Smart Frequency Control of Cyber-Physical Power System Under False Data Injection Attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers* 71, no. 12 (2024): 5582–5595, https://doi.org/10.1109/TCSI.2024.3396703.

11. H. Javanmardi, M. Dehghani, M. Mohammadi, S. Siamak, and M. R. Hesamzadeh, "BMI-Based Load Frequency Control in Microgrids Under False Data Injection Attacks," *IEEE Systems Journal* 16, no. 1 (2021): 1021–1031, https://doi.org/10.1109/jsyst.2021.3054947.

12. X. Zhao, Z. Ma, X. Shi, and S. Zou, "Attack Detection and Mitigation Scheme of Load Frequency Control Systems Against False Data Injection Attacks," *IEEE Transactions on Industrial Informatics* 20, no. 8 (2024): 9952–9962, https://doi.org/10.1109/TII.2024.3390549.

13. F. R. Badal, Z. Nayem, S. K. Sarker, et al., "A Novel Intrusion Mitigation Unit for Interconnected Power Systems in Frequency Regulation to Enhance Cybersecurity," *Energies* 14, no. 5 (2021): 1401, https://doi.org/10.3390/en14051401.

14. K. Pan, E. Rakhshani, and P. Palensky, "False Data Injection Attacks on Hybrid AC/HVDC Interconnected Systems With Virtual Inertia—Vulnerability, Impact and Detection," *IEEE Access* 8 (2020): 141932–141945, https://doi.org/10.1109/access.2020.3013889.

15. Z. Chen, J. Zhu, S. Li, Y. Liu, and T. Luo, "Detection of False Data Injection Attacks on Load Frequency Control System With Renewable Energy Based on Fuzzy Logic and Neural Networks," *Journal of Modern Power Systems and Clean Energy* 10, no. 6 (2022): 1576–1587, https://doi.org/10.35833/mpce.2021.000546.

16. H. Ahmad, M. M. Gulzar, G. Mustafa, A. Q. Khan, S. Habib, and I. Ahmed, "AI-Enabled Frequency Synchronization Control Considering FDI Attack Using Metaheuristic Algorithm," *Neural Computing & Applications* 37, no. 22 (2025): 1–30, https://doi.org/10.1007/s00521-024-10961-1.

17. H. Ahmad, M. M. Gulzar, G. Mustafa, and S. Habib, "AI-Based Approach for Detecting FDI Attacks in Load Frequency Control for Centralized Multi-Area Power Systems," *Computers and Electrical Engineering* 123 (2025): 110060, https://doi.org/10.1016/j.compeleceng.2025.110060.

18. C. Peng, J. Li, and M. Fei, "Resilient Event-Triggering H_∞ Load Frequency Control for Multi-Area Power Systems With Energy-Limited DoS Attacks," *IEEE Transactions on Power Systems* 32, no. 5 (2016): 4110–4118, https://doi.org/10.1109/TPWRS.2016.2634122.

19. Y. Liu, Y. Chen, and M. Li, "Dynamic Event-Based Model Predictive Load Frequency Control for Power Systems Under Cyber Attacks," *IEEE Transactions on Smart Grid* 12, no. 1 (2020): 715–725, https://doi.org/10.1109/tsg.2020.3022094.

20. Z. Cheng, X. Bu, J. Liang, and J. Liu, "Indirect–Direct Secure Load Frequency Control Against False Data Injection Attacks," *IEEE Transactions on Industrial Informatics* 20, no. 3 (2023): 4850–4862, https://doi.org/10.1109/tii.2023.3330235.

21. P. Kumari and S. Pan, "Enhanced Load Frequency Control Using Predictive Reduced Order Generalized Active Disturbance Rejection Control Under Communication Delay and Cyber-Attack," *Electrical Engineering* (2024): 1–15, https://doi.org/10.1007/s00202-024-02713-0.

22. P. Aryan, G. L. Raja, U. Mehta, T. R. Chelliah, and U. R. Muduli, "A Resilient Tri-Parametric Fractional Frequency Control for Cybersecurity Threats amid Latency," *IEEE Transactions on Industry Applications* 61, no. 4 (2025): 5597–5611, https://doi.org/10.1109/TIA.2025.3546173.

23. A. K. Deep, G. L. Raja, and G. D. Meena, "Robust Moments-Matching Load Frequency Control Strategy for Cyber–Physical Power System amid Communication Time Delay," *Applied Energy* 382 (2025): 125251, https://doi.org/10.1016/j.apenergy.2024.125251.

24. K. D. Lu, G. Q. Zeng, X. Luo, J. Weng, Y. Zhang, and M. Li, "An Adaptive Resilient Load Frequency Controller for Smart Grids With DoS Attacks," *IEEE Transactions on Vehicular Technology* 69, no. 5 (2020): 4689–4699, https://doi.org/10.1109/tvt.2020.2983565.

25. X. C. Shangguan, Y. He, C. K. Zhang, et al., "Resilient Load Frequency Control of Power Systems to Compensate Random Time Delays and Time-Delay Attacks," *IEEE Transactions on Industrial Electronics* 70, no. 5 (2022): 5115–5128, https://doi.org/10.1109/tie.2022.3186335.

26. Z. Hu, S. Liu, W. Luo, and L. Wu, "Resilient Distributed Fuzzy Load Frequency Regulation for Power Systems Under Cross-Layer Random Denial-of-Service Attacks," *IEEE Transactions on Cybernetics* 52, no. 4 (2020): 2396–2406, https://doi.org/10.1109/tcyb.2020.3005283.

27. A. Kazemy and M. Hajatipour, "Event-Triggered Load Frequency Control of Markovian Jump Interconnected Power Systems Under Denial-of-Service Attacks," *International Journal of Electrical Power & Energy Systems* 133 (2021): 107250, https://doi.org/10.1016/j.ijepes.2021.107250.

28. R. Pachaiyappan, E. Arasan, and K. Chandrasekaran, "Improved Gorilla Troops Optimizer-Based Fuzzy PD-(1+ PI) Controller for Frequency Regulation of Smart Grid Under Symmetry and Cyber Attacks," *Symmetry* 15, no. 11 (2023): 2013, https://doi.org/10.3390/sym15112013.

29. D. K. Gupta, A. V. Jha, P. Sahu, et al., "Load Frequency Control Analysis of Cyber-Physical Power System With Denial-of-Service Attack in Deregulated Power Markets," *Smart Grids and Sustainable Energy* 10, no. 1 (2025): 1–23, https://doi.org/10.1007/s40866-025-00250-8.

30. T. Hagglund, "A Predictive PI Controller for Processes With Long Dead Times," *IEEE Control Systems Magazine* 12, no. 1 (1992): 57–60, https://doi.org/10.1109/37.120455.

31. P. Airikka, "Another Novel Modification of Predictive PI Controller for Processes With Long Dead Times," *IFAC Proceedings Volumes* 45, no. 3 (2012): 507–511, https://doi.org/10.3182/20120328-3-it-3014.00086.

32. P. Airikka, "Stability Analysis of a Predictive PI Controller," in *Proceedings of the 2013 21st Mediterranean Conference on Control and Automation (MED)* (IEEE, 2013), 1380–1385, https://doi.org/10.1109/MED.2013.6608900.

33. O. A. Briones, A. J. Rojas, and D. Sbarbaro, "Generalized Predictive PI Controller: Analysis and Design for Time Delay Systems," in *Proceedings of the 2021 American Control Conference (ACC)* (IEEE, 2021), 2509–2514, https://doi.org/10.23919/ACC50511.2021.9482789.

34. S. M. Hassan, R. Ibrahim, N. Saad, V. S. Asirvadam, and T. D. Chung, "Predictive PI Controller for Wireless Control System With Variable Network Delay and Disturbance," in *Proceedings of the 2016 2nd IEEE International Symposium on Robotics and Manufacturing Automation (ROMA)* (IEEE, 2016), 1–6, https://doi.org/10.1109/ROMA.2016.7847802.

35. W. Lo, A. Rad, and K. Tsang, "Auto-Tuning of Output Predictive PI Controller," *ISA Transactions* 38, no. 1 (1999): 25–36, https://doi.org/10.1016/s0019-0578(98)00042-1.

36. R. S. Ranganathan, H. A. Malki, and G. Chen, "Fuzzy Predictive PI Control for Processes With Large Time Delays," *Expert Systems* 19, no. 1 (2002): 21–33, https://doi.org/10.1111/1468-0394.00186.

37. P. A. M. Devan, F. A. Hussin, R. Ibrahim, K. Bingi, and H. Abdulrab, "Design of Fractional-Order Predictive PI Controller for Real-Time Pressure Process Plant," in *Proceedings of the 2021 Australian & New Zealand Control Conference (ANZCC)* (IEEE, 2021), 86–91, https://doi.org/10.1109/ANZCC53563.2021.9628377.

38. P. A. M. Devan, F. A. B. Hussin, R. Ibrahim, K. Bingi, and H. Q. Abdulrab, "Fractional-Order Predictive PI Controller for Dead-Time Processes With Set-Point and Noise Filtering," *IEEE Access* 8 (2020): 183759–183773, https://doi.org/10.1109/access.2020.3029068.

39. P. A. M. Devan, R. Ibrahim, M. Omar, K. Bingi, M. Nagarajapandian, and H. Abdulrab, "A Novel Fractional-Order Dead-Time Compensating Controller for the Wireless Networks," *Scientific Reports* 13, no. 1 (2023): 17658, https://doi.org/10.1038/s41598-023-44515-7.

40. J. S. Mary, P. Hemavathy, and S. Kiran, "Fractional Order Predictive Proportional Integral Control of pH in Effluents of Industrial Plants," *International Journal of Environmental Health Engineering* 13, no. 1 (2024): 2, https://doi.org/10.4103/ijehe.ijehe_31_22.

41. P. A. M. Devan, R. Ibrahim, M. Omar, K. Bingi, and H. Abdulrab, "A Novel Hybrid Harris Hawk-Arithmetic Optimization Algorithm for

Industrial Wireless Mesh Networks," *Sensors* 23, no. 13 (2023): 6224, https://doi.org/10.3390/s23136224.

42. P. A. M. Devan, F. A. Hussin, R. B. Ibrahim, K. Bingi, M. Nagarajapandian, and M. Assaad, "An Arithmetic-Trigonometric Optimization Algorithm With Application for Control of Real-Time Pressure Process Plant," *Sensors* 22, no. 2 (2022): 617, https://doi.org/10.3390/s22020617.

43. D. Kumar, G. L. Raja, O. Al Zaabi, M. Alkhatib, and U. R. Muduli, "Resilient PID Controller for Communication Latency in Interconnected Power Systems," in *Proceedings of the 2024 IEEE Energy Conversion Congress and Exposition (ECCE)* (IEEE, 2024), 1653–1658, https://doi.org/10.1109/ECCE55643.2024.10861882.

44. M. M. Ozyetkin, "An Approximation Method and PID Controller Tuning for Systems Having Integer Order and Non-Integer Order Delay," *Alexandria Engineering Journal* 61, no. 12 (2022): 11365–11375, https://doi.org/10.1016/j.aej.2022.05.015.

45. D. Xue, C. Zhao, and Y. Q. Chen, "A Modified Approximation Method of Fractional Order System," in *Proceedings of the 2006 IEEE International Conference on Mechatronics and Automation (ICMA 2006)* (IEEE, 2006), 1043–1048, https://doi.org/10.1109/ICMA.2006.257769.

46. A. Oustaloup, F. Levron, B. Mathieu, and F. M. Nanot, "Frequency-Band Complex Noninteger Differentiator: Characterization and Synthesis," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 47, no. 1 (2000): 25–39, https://doi.org/10.1109/81.817385.

47. L. Wang, Q. Cao, Z. Zhang, S. Mirjalili, and W. Zhao, "Artificial Rabbits Optimization: A New Bio-Inspired Meta-Heuristic Algorithm for Solving Engineering Optimization Problems," *Engineering Applications of Artificial Intelligence* 114 (2022): 105082, https://doi.org/10.1016/j.engappai.2022.105082.

48. Y. Lang and Y. Gao, "Dream Optimization Algorithm (DOA): A Novel Metaheuristic Optimization Algorithm Inspired by Human Dreams and Its Applications to Real-World Engineering Problems," *Computer Methods in Applied Mechanics and Engineering* 436 (2025): 117718, https://doi.org/10.1016/j.cma.2024.117718.

49. J. He, S. Zhao, J. Ding, and Y. Wang, "Mirage Search Optimization: Application to Path Planning and Engineering Design Problems," *Advances in Engineering Software* 203 (2025): 103883, https://doi.org/10.1016/j.advengsoft.2025.103883.

50. S. M. Abd-Elazim and E. S. Ali, "Load Frequency Controller Design of a Two-Area System Composing of PV Grid and Thermal Generator via Firefly Algorithm," *Neural Computing & Applications* 30, no. 2 (2018): 607–616, https://doi.org/10.1007/s00521-016-2668-y.

51. R. K. Khadanga, A. Kumar, and S. Panda, "A Hybrid Shuffled Frog-Leaping and Pattern Search Algorithm for Load Frequency Controller Design of a Two-Area System Composing of PV Grid and Thermal Generator," *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields* 33, no. 1 (2020): e2694, https://doi.org/10.1002/jnm.2694.

52. R. K. Khadanga, A. Kumar, and S. Panda, "A Novel Modified Whale Optimization Algorithm for Load Frequency Controller Design of a Two-Area Power System Composing of PV Grid and Thermal Generator," *Neural Computing & Applications* 32, no. 12 (2020): 8205–8216, https://doi.org/10.1007/s00521-019-04321-7.

53. M. Barakat, A. Donkol, G. M. Salama, and H. F. Hamed, "Optimal Design of Fuzzy Plus Fraction-Order-Proportional-Integral-Derivative Controller for Automatic Generation Control of a Photovoltaic–Reheat Thermal Interconnected Power System," *Process Integration and Optimization for Sustainability* 6, no. 4 (2022): 883–900, https://doi.org/10.1007/s41660-022-00257-z.

54. P. Dahiya and A. K. Saha, "Frequency Regulation of Interconnected Power System Using Black Widow Optimization," *IEEE Access* 10 (2022): 25219–25236, https://doi.org/10.1109/access.2022.3155201.

55. E. Çelik, N. Öztürk, and E. H. Houssein, "Influence of Energy Storage Device on Load Frequency Control of an Interconnected Dual-Area Thermal and Solar Photovoltaic Power System," *Neural Computing & Applications* 34, no. 22 (2022): 20083–20099, https://doi.org/10.1007/s00521-022-07558-x.

56. S. Ekinci, Ö Can, M. Ş Ayas, D. Izci, M. Salman, and M. Rashdan, "Automatic Generation Control of a Hybrid PV-Reheat Thermal Power System Using RIME Algorithm," *IEEE Access* 12 (2024): 26919–26930, https://doi.org/10.1109/access.2024.3367011.

57. C. Andic, S. Ozumcan, M. Varan, and A. Ozturk, "A Novel Sea Horse Optimizer Based Load Frequency Controller for Two-Area Power System With PV and Thermal Units," *International Journal of Robotics and Control Systems* 4, no. 2 (2024): 606–627, https://doi.org/10.31763/ijrcs.v4i2.1341.

58. B. Cavdar, E. Sahin, E. Sesli, O. Akyazi, and F. M. Nuroglu, "Cascaded Fractional Order Automatic Generation Control of a PV-Reheat Thermal Power System Under a Comprehensive Nonlinearity Effect and Cyber-Attack," *Electrical Engineering* 105, no. 6 (2023): 4339–4360, https://doi.org/10.1007/s00202-023-01943-y.

Appendix A: PV–RT Power System Parameters [53, 58]

$a = 900, b = -18, c = 100, d = 50, \tau_{12} = 0.545, B = 0.8, R = 2.5, \tau_G = 0.08, \tau_T = 0.3, K_r = 0.33, \tau_r = 10, K_{ps} = 120, \tau_{ps} = 20$