A Data-Driven Cyber-resilience Framework with Minimal Feature Learning for Frequency Restoration in Isolated Networked Microgrids

Subrata K. Sarker, *Student Member, IEEE,* Hamidreza Shafei, *Student Member, IEEE,* Li Li, *Senior Member, IEEE,* M. J. Hossain, *Senior Member, IEEE,* S M Muyeen, *Fellow, IEEE*

***Abstract*—Isolated networked microgrids (INMGs) provide a sustainable solution for future energy demands by leveraging modern communication technologies to facilitate efficient coordination among isolated microgrids (IMGs). However, reliance on communication networks brings cyber vulnerabilities, potentially undermining the overall performance and reliability of INMGs. Existing cyber-resilience solutions for IMGs are often inflexible, computationally expensive, and lack the adaptability needed for cyber-attack detection and mitigation. These challenges make them unsuitable for INMGs, where the interconnected IMG system complicates the detection of attacks. This paper introduces a scalable, data-driven intelligent framework designed for the concurrent detection and mitigation of attacks targeting the upper control layers of the INMG. The framework employs sparse Bayesian learning via the sequential Monte Carlo method to estimate the posterior distribution weights of the dynamic neural network model. This approach enhances sparsity by prioritizing key weights and filtering out insignificant ones, resulting in faster error estimation. This error identifies attacks, compromised IMGs, and communication channels, triggering timely attack mitigation for frequency restoration and cost-efficient operation of the INMG. Compared to existing strategies, the proposed approach offers significant improvements in computational efficiency and effectively manages the complexity of simultaneous attacks on multiple communication channels, distinguishing between malicious interference and normal system fluctuations, and enabling faster real-time mitigation. The proposed framework is validated using an INMG frequency-control model simulated in MATLAB and OPAL-RT under various attack scenarios. Results demonstrate its effectiveness in managing cyber-attacks and enhancing the adaptive frequency resilience of the INMG.**

***Index Terms*—Attack detection and mitigation, data-driven framework, frequency restoration, and networked microgrid.**

NOMENCLATURE

$\mathcal{M}(t)$	Estimated output vector at time t
$\mathcal{M}^*(t)$	Measured output at time t
$\mathcal{X}(t)$	Input vector at time t
Θ	Weight parameter matrix of the DNN
Ω	Coefficient matrix for auxiliary transformations
Φ	Bias term for each neural network layer
$f^{(l)}$	Activation function of the l-th layer
$g_m(\cdot)$	Auxiliary nonlinear transformation function
$d_{\mathcal{M}}$	Memory order for output variables
$d_{\mathcal{X}}$	Memory order for input variables
$P(\Theta)$	Prior probability of weight parameters
$P(\mathcal{X}\|\Theta)$	Likelihood of input data given weights
$P(\Theta\|\mathcal{X})$	Posterior probability of weights given data
λ	Sparsity parameter in the prior distribution
p	Total number of features
$\Theta_t^{(i)}$	i-th particle of weights at time t
$\mathcal{W}_t^{(i)}$	Weight of i-th particle at time t
$P_p(\cdot)$	Proposal prior distribution in SMC
$\delta(\cdot)$	Dirac delta function
Θ_{MAP}	Maximum a posteriori estimate of weights
$\mathcal{E}_i$	Estimation error for i-th IMG
$\mathcal{Z}_{c,i}(t)$	Attack-compensating signal for i-th IMG
K_p, K_i	Proportional and integral gains of PI controller
R_d	Droop coefficient
$\mathcal{T}_g$	Governor time constant
$\mathcal{T}_{Dg}$	Diesel generator turbine time constant (s)
$\mathcal{H}_m$	System inertia constant
$\mathcal{D}_l$	Load damping coefficient
$\mathcal{K}_r$	RES to fuel cell division gain
$\mathcal{K}_{sc}$	Secondary controller gain
$\mathcal{P}_{ter}$	Output power of TCL
$\mathcal{P}_{td}$	Total system demand
$\mathcal{P}_{nom}$	Nominal power generation
$\mathcal{P}_{Dg}$	Diesel generator power output
$\Delta\mathcal{F}$	Frequency deviation
$\Delta\mathcal{T}_{tie}$	Tie-line power exchange
$\Delta\mathcal{W}_g$	Speed deviation of the Governor
ϕ	Malicious attack signal
$\mathcal{E}_c$	Area control error
$\mathcal{P}_{ter}^*$	Manipulated target power under attack
$\mathcal{E}_c^*$	Manipulated ACE under attack
$\mathcal{N}_e$	Effective sample size in SMC resampling
$\mathcal{N}$	Total number of particles in the SMC method

S. K. Sarker, H. Shafei, Li Li and M. J. Hossain are with the School of Electrical and Data Engineering, University of Technology Sydney, Australia. S M Muyeen is with the Electrical Engineering Department, Qatar University, Doha, Qatar.

Email: subratakumar.sarker@student.uts.edu.au; hamidreza.shafei@student.uts.edu.au;Li.Li@uts.edu.au; Jahangir.Hossain@uts.edu.au; sm.muyeen@qu.edu.qa

I. Introduction

Isolated networked microgrid (INMG) leads a transformative techno-economic energy solution for the next-generation energy industry by maximizing the utilization of renewable energy sources (RESs). By incorporating RESs, the INMG contributes to sustainability by reducing its dependence on fossil fuels, lowering carbon emissions, and promoting energy resilience in remote areas [1]. However, their integration presents significant challenges, including intermittent resource availability, stability constraints, power quality issues, and the need for enhanced energy storage (ES) management. Furthermore, seamless interoperability among various RESs requires

advanced communication networks to achieve their growing penetration while meeting rising load demands. The balance between power demand and generation directly influences the operating frequency of INMG. When generation falls short of demand, frequency declines, which can result in power outages. Conversely, excess generation results in frequency increases, posing a risk of equipment damage [2].

To ensure the effective and safe operation of the INMG, it is crucial to regulate the frequency and maintain a balance between generation and demand output. Implementing a distributed hierarchical load frequency control (DHLFC) mechanism can achieve this objective by employing its upper and lower levels of control loops [3], [4]. The upper layer primarily implements secondary and tertiary control loops to minimize frequency deviation and set the optimal target power (OTP) for the lower control level of the local isolated microgrids (IMGs). The lower control layer generates command signals for the generator and ES systems of the local IMGs by utilizing data from the upper layer. The safe operation of these loops is essential for maintaining power balance and regulating system frequency in response to varying generation demands. However, they introduce stability challenges for INMGs, potentially causing delays due to transmission issues or cyberattacks that disrupt communication [5], [6]. These changes jeopardize the system's integrity, risking unsecured communications that undermine resilience and reliability. Such issues can degrade performance, resulting in operational delays, equipment damage, power outages, and compromised system integrity. Thus, dynamic cyber-resilient solutions are needed to maintain adaptive frequency restoration and secure INMG operations against cyber threats.

Researchers have focused on ensuring the safe operation of INMG through distributed control mechanisms for IMGs. A two-stage robust DHLFC mechanism based on day-ahead optimization was proposed in [7] for the resilient operation of IMGs. The primary objective of this mechanism is to achieve low operating costs by formulating a mixed-integer linear programming problem at the tertiary control layer (TCL). However, this study lacks an assessment of its resilience to cyber attacks. A modified two-stage DHLFC method based on frequency security for multi-microgrid clusters was formulated in [8]. This strategy outlines a joint energy and reserve scheduling issue aimed at the cost-effective operation of IMGs. However, it also fails to consider potential vulnerabilities, leaving the system susceptible to cyber attacks that could jeopardize its stability and security.

A cascaded proportional-integral-derivative (PID) controller optimized via the imperialist competitive algorithm was proposed in [9] to enhance frequency stability in multi-microgrids. While this controller improves the frequency response, it avoids measuring the cyber-resilience and cost-effective performance. The authors in [10] developed a hierarchical control system focusing on active power sharing and priority-based load management to enhance the dynamic performance of the INMG under steady-state load conditions. In [11], a modified version of the control mechanism discussed in [10] was introduced to validate the same level of performance of INMG while manipulating loads. While these approaches enhance the dynamic response of frequency stability over varying load conditions, they are limited in their applicability regarding cyber resilience. An intelligent hierarchical strategy leveraging a deep learning framework was introduced in [12] to optimize the frequency management of INMG. This method utilizes a traditional recurrent neural network (RNN) to determine optimal frequency regulation conditions in INMGs, but its performance is affected by attack-induced fluctuations, limiting real-time applicability. After thorough analysis, it's clear that while most of the research on INMG has focused on achieving optimal frequency regulation and cost efficiency, the interconnection of these systems highlights the need for cybersecurity measures. An attack, such as altering sensor data or manipulating control signals, could compromise the entire system, potentially leading to power outages or infrastructure damage. This highlights the need for an attack detection and mitigation (ADM) framework that works in tandem with the existing control systems to maintain cyber-safe operations. Without proper safeguards, even well-designed INMGs remain vulnerable, highlighting cybersecurity as a critical aspect of modern INMG design.

Numerous studies focus on developing cyber-resilient mechanisms to secure frequency regulation of IMG, aiming to mitigate the impact of cyber attacks on the secondary control layer (SCL). A control strategy utilizing bilinear matrix inequalities (BMI) to restore the frequency of IMGs under false data injection (FDI) attacks is examined in [13]. Similarly, an observer-based two-layer control approach was introduced in [14] for the adaptive frequency restoration of IMGs in response to FDI attacks. This method features an observer in the first layer to detect attack signals while the second layer works to reduce their impact. Furthermore, Ref. [15] explored a predictive control framework designed for cyber-resilient frequency regulation of IMGs, which integrates distributed integral action with a predictive component to improve resistance to attacks and enhance dynamic performance. However, these approaches are rigid and rely on complex mathematical derivations, limiting their suitability for INMG.

In [16], a control method utilizing Hankel-norm approximation was designed to maintain stability and ensure the cyber-resilient performance of IMG. While this approach effectively restores frequency against attacks on local communication links, it fails to uphold safe regulation principles when the global communication network is compromised. Further, Ref. [17] explored a sliding mode-based observer capable of handling attacks on both local and global communication channels of the IMG. However, it depends on accurate system models, faces real-time implementation challenges, and is vulnerable to noise. Data-driven cybersecurity solutions offer a viable alternative by eliminating the need for precise system modeling and associated assumptions [18], [19]. Several approaches, such as Support Vector Machine (SVM) with reinforcement learning [20] and RNN-based attack detection [21], enhance cyber resilience in IMGs. While these methods surpass traditional models in many aspects, they often struggle with adaptability to dynamic conditions and require high computational resources due to slow convergence and structural constraints.

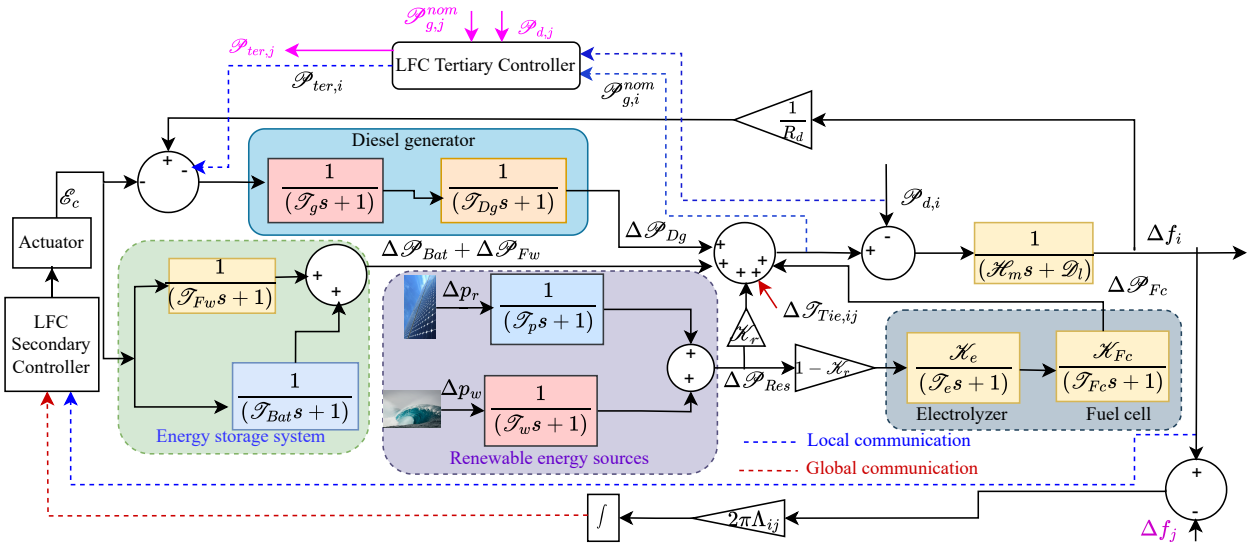


Fig. 1: Load frequency control model of isolated networked microgrid.

A. Motivations and contributions

Given the challenges of existing methods, there is a pressing need for an adaptive and computationally efficient ADM framework to ensure the effective and techno-economic operation of INMG, addressing current challenges while bridging the limitations of existing approaches. Now, existing literature primarily focuses on methods designed solely for ADM in SCL-driven IMGs. While several studies develop hierarchical control methods for the efficient and cost-effective operation of INMG, they often overlook the impact of cyber-attacks on the TCL and the performance of these methods under such conditions. Since the TCL requires information sharing among all IMGs within the INMG, an attacker can target this layer by tampering with the OTP for local IMGs. This temperament increases the operating fuel cost of INMG or forces the utilization of the ES system to maintain the power balance between generation and demand, which degrades the cost-effective performance of INMG. When an attacker exploits both control layers to inject attacks into the INMG, it can pose several additional challenges for existing methods in accurately detecting and mitigating threats, including:

- Manipulation of multiple layers, along with load changes, can obscure attack signatures, making detection more difficult.
- Load changes or attack scenarios at both layers increase challenges in differentiating their dynamic responses, hindering the identification of altered communication channels and triggering the mitigation mechanism.
- Existing data-driven techniques may address these challenges by training on multi-layer attack scenarios, which increases the number of features and results in slow convergence during training.

These challenges motivate us to modify the design strategy of existing approaches and develop a data-driven ADM approach for the cyber-safe and cost-effective operation of INMG. The proposed approach aims to simultaneously identify and mitigate attacks on the SCL and TCL of INMG while minimizing redundant features to increase its convergence during training. Unlike existing methods that mainly focus on a single control layer, the proposed approach employs a model-free DNN framework to detect and mitigate cyber-attacks on both the SCL and TCL simultaneously. It also accelerates convergence using sparse Bayesian learning optimized with SMC techniques, which removes redundant features and lessens computational resources. Moreover, a mitigation layer based on a PI controller is developed to ensure cyber-safe and cost-efficient frequency stabilization, especially in complex scenarios with multiple attack layers and dynamic load variations that are not fully addressed by existing solutions. These innovations highlight the newness of the proposed approach compared to existing solutions, and their deployment signifies a considerable advancement in cyber-resilient operations for INMG.

II. System Modelling with Cyber Attacks

An IMG incorporates RESs, such as photovoltaic (PV) and wave energy, which primarily serve as primary power sources for generation. In comparison, INMG refers to the integration of two or more IMGs. To enhance stability during significant disturbances, it also integrates an ES system that reduces the likelihood of frequency instability and power outages. However, traditional frequency stability assessments often overlook inter-machine oscillations and transmission system dynamics [22]. To streamline analysis, a simplified representation using an electrical machine, turbine, and governor is commonly adopted. As illustrated in Fig. 1, this reduced-order dynamic model effectively characterizes the interaction between active power and frequency while accounting for potential cyber-attack vulnerabilities. Studies in [23], [24] have validated this approach as a reliable framework for examining cyber-resilient frequency control support in IMGs. Fig. 1 depicts the studied system, which comprises two primary networks: an energy network and multiple communication networks utilized to send/receive information to/from both control layers. In the SCL, the communication network collects system measurements, including frequency deviations and power flows through the tie line, to generate the command signal $\mathcal{E}_c$,

sending it to the ES systems for restoring frequency deviation to its nominal value. Meanwhile, the TCL utilizes demand and generation data from all IMGs to compute the allocated OTP for each local IMG. This layer ensures efficient power distribution while maintaining overall system stability and cost-effective operation by adjusting the control signal of the governor. The adjustment in the speed governor's control signal $\Delta\mathcal{W}_g$ for i^{th} IMG is expressed as follows:

$$\Delta\mathcal{W}_{g,i} = \frac{1}{1+s\mathcal{T}_{g,i}}\left(\frac{1}{\mathcal{R}_{d,i}}\cdot\Delta\mathcal{F}_i - \mathcal{E}_{c,i} - \mathcal{P}_{ter,i}\right), \quad (1)$$

where $\mathcal{R}_d$, $\mathcal{T}_g$, and $\Delta\mathcal{F}_i$ indicate the droop coefficient for the primary control layer, the governor's time constant, and frequency deviation, respectively. In (1), $\mathcal{P}_{ter}$ is the output of the TCL that can be calculated for i^{th} IMG as:

$$\mathcal{P}_{ter,i} = \frac{P_{td}}{P_{tg}^{nom}} \times P_{g,i}^{nom}, \quad (2)$$

where $P_{\mathrm{g},i}^{nom}$ denotes the nominal power generation for the i^{th} IMG, while P_{td} and P_{tg}^{nom} indicate the total demand and nominal power generation of INMG. This ensures that the power distribution among IMGs is proportional to their respective nominal power generation, optimizing system-wide resource allocation while maintaining stability. Now, from Fig. 1, the output of SCL $\mathcal{E}_c$ for i^{th} IMG can be calculated as:

$$\mathcal{E}_{c,i}(t) = \mathcal{K}_{sc,i}\Big(\sum_{j=1,i\neq j}^{K}\Delta\mathcal{T}_{tie,ij} + \Delta\mathcal{F}_i\Big). \quad (3)$$

Here, $\mathcal{K}_{sc}$ and K denote the gain of the secondary controller and the total number of tie-lines, while $\Delta\mathcal{T}_{tie,ij}$ denotes the variation in tie-line power. Now, the turbine system is activated by the adjusted speed governor signal from (1), initiating power generation. Thus, the power $\mathcal{P}_{Dg}$ produced by the i^{th} IMG synchronous generator fluctuates as follows:

$$\Delta\mathcal{P}_{Dg,i} = \frac{1}{1+s\mathcal{T}_{Dg,i}}\cdot\Delta\mathcal{W}_{g,i}, \quad (4)$$

where $\mathcal{T}_{Dg}$ is the turbine time-constant of a diesel generator. This reinstates the IMG frequency, allowing the system to keep the frequency deviation $\Delta\mathcal{F}$ zero over the disturbances, which can be measured for i^{th} IMG as:

$$\Delta\mathcal{F}_i = \frac{1}{\mathcal{H}_{m,i}s+\mathcal{D}_{l,i}}[\mathcal{K}_r\Delta\mathcal{P}_{Res,i} + \Delta\mathcal{P}_{Bat,i} + \Delta\mathcal{P}_{Fw,i} + \Delta\mathcal{P}_{Fc,i} + \Delta\mathcal{T}_{tie,ij} + \Delta\mathcal{P}_{Dg,i} - \Delta\mathcal{P}_{l,i}], \quad (5)$$

where $\Delta\mathcal{P}_{Res,i}$, $\Delta\mathcal{P}_{Fw,i}$, $\Delta\mathcal{P}_{Fc,i}$, $\Delta\mathcal{P}_{Bat,i}$, $\Delta\mathcal{T}_{Tie,ij}$ $\Delta\mathcal{P}_{Dg,i}$, and $\Delta\mathcal{P}_{l,i}$ represent the per-unit power variations corresponding to the RESs, flywheel, FC, battery, tie-line power, diesel generator, and load for the i^{th} IMG, respectively. The detailed parameter description of (5) can be found in [21]. However, both control layers are particularly vulnerable to cyber threats due to their dependence on communication and sensor networks. Notably, other components of the system shown in Fig. 1 do not require direct interaction with the control centers, significantly reducing their risk of cyber compromise. In an INMG, attackers exploit communication signals by injecting various types of cyber-attacks, with FDI attacks being among the most prevalent. This attack poses severe risks to system performance, leading to erroneous control decisions, instability, power losses, communication failures, and overall integrity degradation. By targeting communication networks, attackers can alter the area control error (ACE) $\mathcal{E}_c$ and the target power adjustment $\mathcal{P}_{tar}$, ultimately compromising the cost-effectiveness of frequency control in the INMG. Now, consider attackers can manipulate the frequency signal or tie-line power to modify the $\mathcal{E}_c$ signal as:

$$\mathcal{E}_c^* = \mathcal{K}_{sc,i}\big((\Delta\mathcal{F}_i(t)+\phi_i(t)) + \sum_{j=1,j\neq i}^{K}\Delta\mathcal{T}_{\mathrm{tie},ij}(t)\big), \quad (6)$$

$$\mathcal{E}_c^* = \mathcal{K}_{sc,i}\big(\Delta\mathcal{F}_i(t) + \sum_{j=1,j\neq i}^{K}\big(\Delta\mathcal{T}_{\mathrm{tie},ij}(t)+\phi_{ij}(t)\big)\big), \quad (7)$$

Similarly, for the TCL, the target power for the i^{th} IMG under the attack condition can be manipulated as:

$$\mathcal{P}_{ter,i}^* = \frac{P_{td}}{P_{tg}^{nom}+\phi_i(t)} \times (P_{g,i}^{nom}+\phi_i(t)), \quad (8)$$

where ϕ, $\mathcal{E}_c^*$, and $\mathcal{P}_{ter}^*$ represent the malicious signal injected into the communication pathway, manipulated ACE signal, and allocated OTP, respectively. If the system remains free from attacks, it adheres to the following communication principle:

$$\begin{aligned}\Delta\mathcal{T}_{tie,ij} &= \Delta\mathcal{T}_{tie,ij}^S = \Delta\mathcal{T}_{Tie,ij}^R,\\ \Delta\mathcal{F}_i &= \Delta\mathcal{F}_i^S = \Delta\mathcal{F}_i^R,\\ P_{g,i}^{nom} &= P_{g,i}^{nom,S} = P_{g,i}^{nom,R},\end{aligned} \quad (9)$$

where the superscript S and R denote the sending and receiving end signals, respectively, as transmitted by the system and received by the control center for the corresponding parameters.

Remark 1: Since this study primarily focuses on detecting and mitigating cyber-attacks across both control layers of the INMG while distinguishing between load changes and attack scenarios, it assumes that the power generated by the TCL represents the OTP allocated for the local IMG.

TABLE I: System parameters for real-time simulation.

Parameter	Description	Area 1	Area 2
$\mathcal{T}_{Dg}$	Diesel generator time constant (s)	1	1
$\mathcal{T}_g$	Governor time constant (s)	2	2
Λ	Synchronizing coefficient	0.25	
$\mathcal{T}_p$	PV time constant (s)	0.5	0.5
$\mathcal{T}_{Bat}$	Battery time constant (s)	0.1	0.1
$\mathcal{T}_e$	Electrolyzer time constant (s)	0.5	0.3
$\mathcal{T}_w$	Wave energy time constant (s)	0.5	0.5
$\mathcal{K}_{Fc}$	FC gain	0.002	0.001
$\mathcal{T}_{Fc}$	FC time constant (s)	0.5	0.3
$\mathcal{K}_e$	Electrolyzer gain	0.002	0.001
$\mathcal{T}_{Fw}$	Flywheel time constant (s)	0.1	0.1
$\mathcal{R}_d$	Droop constant (Hz/p.u.MW)	0.6	0.75
$\mathcal{K}_r$	RESs to FC division gain	0.6	0.5
$\mathcal{H}_m$	System inertia (s)	0.2	0.3
$\mathcal{D}_l$	Load damping coefficient (p.u.MW/Hz)	0.012	0.03

III. Proposed Methodology

This paper develops a scalable data-driven cyber ADM framework to enhance the cyber-resilience frequency support of INMG. The proposed framework utilizes sparse learning through SMC to approximate the posterior distribution

weights of the DNN model. This strategy enhances sparsity by emphasizing relevant weights while filtering out the less significant ones. The work in [25] develops a cyber-resilient framework based on the DNN without integrating sparse learning. While this method effectively addresses cyber issues on DC microgrids, it requires substantial computational resources, which may limit its real-time application. However, implementing SMC-based posterior approximation within the Bayesian framework of the proposed model improves its computational efficiency by introducing sparsity. This enables quicker updates and recalibrations of the model weights as new data arrives, making the proposed framework a powerful tool for real-time threat detection. The detailed formulation of the proposed model is outlined in the parts below.

A. Modeling of the dynamic neural network

A DNN adapts its structure and parameters based on input data and feedback. Unlike static neural networks with fixed architectures, DNNs evolve, making them ideal for real-time learning and adaptive forecasting. Numerous intelligent control applications of IMGs depend on data-driven neural networks, emphasizing the necessity of choosing the right type of DNN modeling, which is mainly influenced by the relationship between the inputs and outputs of the system. Feed-forward DNN functions well for systems exhibiting stable, static input-output relationships [26]. Conversely, RNNs, which have memory capabilities, thrive in situations where outputs are influenced by the historical values of inputs and outputs, such as in the frequency control of IMGs [27]. The developed DNN framework represents a unique variety of RNNs that offer substantial advantages in terms of accuracy and learning capability. While other RNN variations may reach similar performance levels, they often have slower convergence rates, which can limit their use in real-time scenarios.

Consider a conventional DNN used for time-series prediction at time t, which depends on prior outputs and inputs by mapping their relationship as follows:

$$\begin{aligned}\mathcal{M}(t) = f(&\mathcal{M}(t-1), \mathcal{M}(t-2)\ldots, \mathcal{M}(t-d_{\mathcal{M}}),\\ &\mathcal{X}(t-1), \mathcal{X}(t-2), \ldots, \mathcal{X}(t-d_{\mathcal{X}}); \Theta),\end{aligned} \quad (10)$$

where $\mathcal{X}(t) = [\Delta\mathcal{F}_i \ \sum_{j=1, i\neq j}^{K} \Delta\mathcal{T}_{tie,ij}]$ indicates the input while $\mathcal{M}(t) = [\mathcal{E}_c^* \ \mathcal{P}_{ter}^*]$ indicates the output at time t estimated by using the previous output $\mathcal{M}(t-1)$ and input $\mathcal{X}(t-1)$, scaled by the weight parameter Θ connecting to the corresponding neurons. In addition, $d_{\mathcal{M}}$ and $d_{\mathcal{X}}$ are positive integers indicating the memory order of the network's outputs and inputs. In this work, the developed DNN consists of an input layer, a hidden layer, and an output layer with a specified number of neurons through which data flows via the subsequent transformation:

$$\mathcal{M}^{(l)} = f^{(l)}\Big(\sum_{m=1}^{n^{(l-1)}} \Theta_m^{(l)} \mathcal{M}_m^{(l-1)} + \sum_{m=1}^{q^{(l)}} \Omega_m^{(l)} g_m(\mathcal{M}_m^{(l-1)})\Big) + \Phi^{(l)},$$

where $\mathcal{M}^{(l)}$ carries the output of l^{th} layer after transformations and the utilization of non-linear activation function $f^{(l)}$. Additionally, $\sum_{m=1}^{n^{(l-1)}} \Theta_m^{(l)} \mathcal{M}_m^{(l-1)}$ indicates the weighted sum of the output from $n^{(l-1)}$ neurons in the $(l-1)^{\text{th}}$ layer, whereas $\sum_{m=1}^{q^{(l)}} \Omega_m^{(l)} g_m(\mathcal{M}_m^{(l-1)})$ determines the output resulting from $q^{(l)}$ auxiliary nonlinear transformations $g_m(.)$, scaled by coefficients $\Omega_m^{(l)}$. This weighted sum, along with the bias term $\Phi^{(l)}$, enhances the transformation complexity by adding more non-linearity. This increase in complexity allows the model to learn more intricate relationships within the data, thus improving its ability to make precise estimations. This work considers the following activation function:

$$f^{(l)} = \frac{e^{\mathcal{M}^{(l)}} - e^{-\mathcal{M}^{(l)}}}{e^{\mathcal{M}^{(l)}} + e^{-\mathcal{M}^{(l)}}}.$$

Now, the initial stage in estimating the output of the proposed DNN involves training a network with one hidden layer h. This trained network then utilizes the following mathematical mapping to estimate target variables:

$$\mathcal{M}(t) = f^{ou}(\Theta^{ou}(\Theta^{(h)}\mathcal{X}^{(h)}(t-1) + \Phi^{(h)}) + \Phi^{ou}), \quad (11)$$

where Θ^{ou}, Φ^{ou}, $\Theta^{(h)}$, and $\Phi^{(h)}$ denote the weighted matrix and biasing factors for the output and hidden layer, respectively. Given that the model consists of only one hidden layer, the transformation g_m is directly applied to the output of this layer, thereby increasing the complexity of the output by adding more non-linearity. Additionally, $\mathcal{X}_{t-1}^{(h)}$ represents the mapping of the input and target variables as follows:

$$\mathcal{X}^{(h)}(t-1) = \begin{bmatrix} \mathcal{M}(t-1) & \cdots & \mathcal{M}(t-d_{\mathcal{M}}), \\ \mathcal{X}(t-1) & \cdots & \mathcal{X}(t-d_{\mathcal{X}}) \end{bmatrix}^T.$$

As indicated in (11), the output of the DNN relies on time-sensitive information; therefore, a Bayesian learning approach is used to model the proposed DNN. This approach is essential for time-series prediction, providing a robust probabilistic framework for time-dependent data. It integrates prior knowledge to incorporate historical data and domain expertise, especially when data is limited. A key benefit is its ability to quantify uncertainty with complete posterior distributions, improving decision-making. Regularization through priors and likelihoods helps resist overfitting, making it suitable for sparse datasets. It adeptly manages non-stationary time series data by updating distributions with new data, which is critical for dynamic systems. Now, as per the Bayesian rule, we can define the notation of posterior distribution for the given weight parameters Θ and input data $\mathcal{X}$ as follows:

$$P(\Theta|\mathcal{X}) = \frac{P(\mathcal{X}|\Theta)P(\Theta)}{P(\mathcal{X})}, \quad (12)$$

where $P(\Theta)$, $P(\mathcal{X}|\Theta)$, and $P(\Theta|\mathcal{X})$ are the prior probability, likelihood, and the posterior probability, respectively. The denominator of (12) represents the marginal likelihood probability, computed as the normalizing constant of maximizing the posterior distribution. This work utilizes the SMC approach for the maximization of the posterior distribution $P(\Theta|\mathcal{X})$ while incorporating a sparsity-promoting prior for the feature minimization by iteratively focusing on the most informative features. Now, consider the sparsity-promoting prior as:

$$P(\Theta) \propto \exp(-\lambda \sum_{j=1}^{p} |\Theta_j|), \quad (13)$$

In (13), $\lambda > 0$ maintains the level of sparsity while p measures the total number of features. The objective of this prior is to encourage the many elements of Θ to shrink towards zero, effectively reducing the influence of less important features. Also, the sparsity-based prior assists in normalizing the weights to approximate the maximum posterior $P(\Theta|\mathcal{X})$.

Now, consider that SMC approximates $P(\Theta|\mathcal{X})$ by utilizing a set of $\mathcal{N}$ weighted particles $\left\{\Theta_t^{(i)}, \mathcal{W}_t^{(i)}\right\}_{i=1}^{\mathcal{N}}$, where $\Theta_t^{(i)}$ denotes the i-th particle at time t, and $\mathcal{W}_t^{(i)}$ is its corresponding weight. Thus, initializing the $\mathcal{N}$ set of particles for (13) as:

$$\Theta_0^{(i)} \sim P(\Theta) \propto \exp(-\lambda \sum_{j=1}^{p} |\Theta_j|), \tag{14}$$

with uniform weights as $\mathcal{W}_0^{(i)} = \frac{1}{\mathcal{N}}$. In (14), the particle $\Theta_0^{(i)}$ is sampled from the $P(\Theta)$, which is proportional to $\exp\left(-\lambda \sum_{j=1}^{p} |\Theta_j|\right)$. Once initialization is complete, the subsequent step entails weight propagation, where new particles of $\Theta_t^{(i)}$ are generated from the previous location of particles $\Theta_{t-1}^{(i)}$ and compare it with proposal prior distribution, $P_p(\Theta_t \mid \Theta_{t-1}, \mathcal{X}_t)$, which governs the evolution of the particles. Thus, each new particle $\Theta_t^{(i)}$ at time t can be sampled from the proposal distribution as:

$$\Theta_t^{(i)} \sim P_p(\Theta_t \mid \Theta_{t-1}^{(i)}, \mathcal{X}_t), \tag{15}$$

The next step involves updating the weights to refine the set of particles, ensuring that they more accurately reflect the accurate posterior distribution. By integrating the likelihood and prior, this weight adjustment prioritizes the more relevant particles in later steps, resulting in a closer approximation of the posterior. Thus, updating the weights of each particle using the posterior distribution as:

$$\mathcal{W}_t^{(i)} \propto \mathcal{W}_{t-1}^{(i)} \cdot \frac{P(\mathcal{X}_t \mid \Theta_t^{(i)}) P(\Theta_t^{(i)})}{P_p(\Theta_t^{(i)} \mid \Theta_{t-1}^{(i)}, \mathcal{X}_t)}, \tag{16}$$

When the weights are updated in this phase, the normalization factor is considered for the subsequent normalization step. Therefore, the proposal distribution does not influence the relative weights among particles; it merely directs the generation of particles. Now, using (13), we can modify (16) as:

$$\mathcal{W}_t^{(i)} \propto \mathcal{W}_{t-1}^{(i)} \cdot P(\mathcal{X}_t \mid \Theta_t^{(i)}) \cdot \exp\left(-\lambda \sum_{j=1}^{p} |\Theta_j|\right), \tag{17}$$

with normalized weights as $\hat{\mathcal{W}}_t^{(i)} = \frac{\mathcal{W}_t^{(i)}}{\sum_{j=1}^{\mathcal{N}} \mathcal{W}_t^{(j)}}$. As particles evolve, some may have minimal weights, indicating a slight contribution to the posterior approximation. Eventually, particle degeneracy occurs when most particles have insignificant weights, leading to a few particles dominating the approximation. This results in an ineffective representation of the posterior distribution. To prevent particle degeneracy, an effective sample size of $\mathcal{N}_e$ needs to be measured, indicating that duplicates of high-weighted particles replace particles having lower weights than $\mathcal{N}_e$ that can be calculated as:

$$\mathcal{N}_{\mathrm{e}} = \left(\sum_{i=1}^{\mathcal{N}} \left(\hat{\mathcal{W}}_t^{(i)}\right)^2\right)^{-1}, \tag{18}$$

The resampled particle from (18) is utilized to approximate the posterior distribution as:

$$P(\Theta \mid \mathcal{X}) \approx \sum_{i=1}^{\mathcal{N}} \hat{\mathcal{W}}_t^{(i)} \delta(\Theta - \Theta_t^{(i)}), \tag{19}$$

where $\delta(\Theta - \Theta_t^{(i)})$ is the Dirac delta function that is zero everywhere except at the point where its argument is zero, indicating the posterior distribution is concentrated at the particles' locations. Thus, the maximum a posteriori (MAP) estimate, Θ_{MAP}, which corresponds to the value of Θ that maximizes the posterior distribution, can be approximated as:

$$\Theta_{\mathrm{MAP}} = \arg\max_{\Theta_t^{(i)}} \hat{\mathcal{W}}_t^{(i)}.$$

From (13), features that contribute minimally to the likelihood $P(\mathcal{X}_t|\Theta_t^{(i)})$ lead to smaller values of Θ_j. This occurs because the term λ compels the model to reduce Θ_j values. When the likelihood shows relative insensitivity to changes in Θ_j, the gradient of the likelihood concerning Θ_j approaches zero. Consequently, the value of Θ_j will experience less

Algorithm 1 Pseudocode for implementing the proposed framework

Inputs: Data $\mathcal{X}(t)$
Output: Estimate attacked signal $\mathcal{M}_i(t)$
Initialize: Select values for weights, biases, prior distributions, and sparsity parameter
Model Specification: Define $f^{(l)}$, $P(\Theta|\mathcal{X})$ and $P(\Theta)$
Training Process: Initialize hidden layers and neurons
repeat
  for each time step t **do**
    for each layer l **do**
      Update the output of each layer using (11)
    end for
    Estimate the target output $\mathcal{M}_i(t)$ using (12).
    Weight Optimization: Initialize a set of $\mathcal{N}$ particles $\left\{\Theta_0^{(i)}, \mathcal{W}_0^{(i)}\right\}_{i=1}^{\mathcal{N}}$
    for each particle $\Theta_t^{(i)}$ **do**
      Propagate each particle based on (16)
      Update the weight $\mathcal{W}_t^{(i)}$ using (17)
    end for
    Calculate $\hat{\mathcal{W}}_t^{(i)} = \frac{\mathcal{W}_t^{(i)}}{\sum_{j=1}^{\mathcal{N}} \mathcal{W}_t^{(j)}}$ and $\mathcal{N}_e$
    if $\mathcal{N}_e < \mathcal{N}$ **then**
      Resample particles based on $\hat{\mathcal{W}}_t^{(i)}$
    end if
    Approximate the $P(\Theta|\mathcal{X})$ using (20)
    Compute the MAP estimate Θ_{MAP}
  end for
until convergence
End

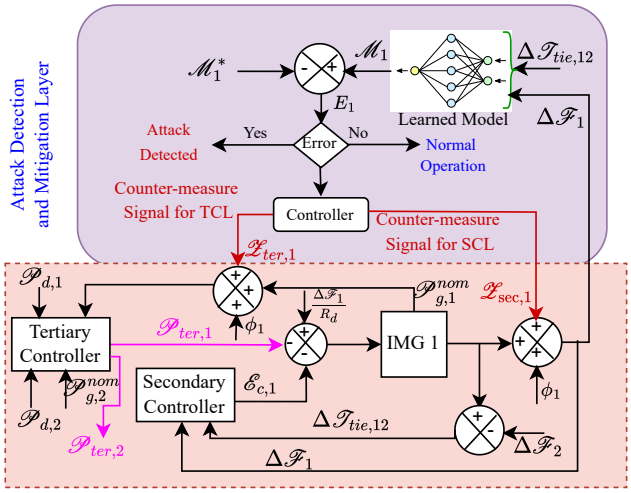


Fig. 2: Proposed ADM for the IMG 1 of the INMG.

significant updates, and due to the sparsity prior, it will naturally decrease towards zero [28], [29]. Thus, we get:

$$\Theta_j \to 0, \quad \text{if} \quad \frac{\partial P(\mathcal{X}_t|\Theta)}{\partial \Theta_j} \approx 0.$$

Thus, the proposed DNN effectively ignores irrelevant features by reducing their corresponding parameters Θ_j to zero or nearly zero, thereby removing them from the model. A pseudocode for the implementation of the proposed framework is illustrated in Algorithm 1.

B. Attack detection and mitigation layer

As illustrated in Fig. 1, malicious entities can initiate unwanted signals aimed at compromising the communication infrastructures for the SCL and TCL. To counter these threats, a dynamic approach is essential for swiftly detecting and mitigating the attack signals, minimizing their adverse effects, and supporting frequency stability restoration in the system. This study introduces a cybersecurity framework composed of detection and mitigation layers. The detection layer continuously monitors the discrepancy between the measured and estimated output of upper control layer to identify potential cyber attacks. These estimations are done based on the local frequency deviation and the tie-line power exchange with the neighboring IMG. Under attack scenarios, the output of the proposed framework is routed through an error block to produce the error signal for the i^{th} IMG, which detects the appearance of the attack signal as follows:

$$\mathcal{E}_i = \mathcal{M}_i - \mathcal{M}_i^*, \tag{20}$$

where $\mathcal{M}^*$ defines the measured output. When the system encounters any attack signal within the communication signals, the estimation error fails to reach zero, instead exhibiting a persistent error. Therefore, the system's behavior under attack conditions is as follows:

$$\lim_{t\to\infty} \mathcal{E}_i(t) \neq 0 \quad . \tag{21}$$

The PI controller in the mitigation layer utilizes the estimated error signal to generate an attack-compensating signal $\mathcal{Z}_{c,i}(t) = [\mathcal{Z}_{sec,i}(t)\ \mathcal{Z}_{ter,i}(t)]$, which is then combined with the corrupted communication signals before being sent to the SCL ($\mathcal{Z}_{sec,i}(t)$) and TCL ($\mathcal{Z}_{ter,i}(t)$) layer. This enables a coordinated response to mitigate the effects of the attacks. Thus, the local communication signal for the SCL satisfies:

$$\lim_{t\to\infty}(\Delta\mathcal{F}_i^{*R}(t) - \Delta\mathcal{F}_i^S(t)) = \lim_{t\to\infty}(\Delta\mathcal{F}_i^S(t) + \phi_i(t)$$
$$+\mathcal{Z}_{sec,i}(t) - \Delta\mathcal{F}_i^S(t)) = \lim_{t\to\infty}(\mathcal{Z}_{sec,i}(t) + \phi_i(t)) = 0, \tag{22}$$

Likewise, the proposed methodology can ensure the effective cyber-secured operation for global communication channels within the SCL and the TCL. By utilizing the efficiency of the PI controller, the information processed by both control units remains consistent with the transmitted data. This consistency is achieved through the proposed approach, which ensures that the condition outlined in (22) is satisfied, even in the presence of an attack signal. The dynamic behavior of $\mathcal{Z}_{c,i}(t)$ leads a critical role in detecting attack signals. Specifically, during an attack on the i^{th} IMG, $-\mathcal{Z}_{c,i}(t)$ tends to reflect the dynamics of the attack. Conversely, when no attack occurs, $-\mathcal{Z}_{c,i}(t)$ approaches zero. This design guarantees the secure operation of the INMG, as described in (9), irrespective of the presence of an attack. The ADM for INMG using the proposed approach is illustrated in Fig. 2.

Remark 2: When an INMG experiences an attack on the SCL, the estimator for the affected IMG will exhibit a prominent estimation error characterized by a sharp spike during the initial sampling phase, followed by either a stabilization of the error or an inability to converge to zero. In contrast, spikes induced by load changes will eventually diminish and converge to zero over time. However, the identification of the compromised channel depends on the nature of the observed spikes. Specifically, the spikes observed in the initial sampling within the local IMG estimator response solely identify an attack on the local communication channel. In contrast, both area estimators show sharp spikes when breaching the global channel, with one potentially converging to zero.

Remark 3: When the INMG experiences an attack on the TCL, the estimator for the affected IMG will show an estimation error, followed by either a stabilized error or failure to converge to zero, while the estimators for other IMGs will converge to zero. The spikes observed during initial sampling indicate the compromised channel. It is important to note that the proposed approach operates on a centralized detection model. This means that the detection of attacks and compromised channels require the estimation of the errors i^{th} IMG, E_i, in (20), while their inputs are completely distributed.

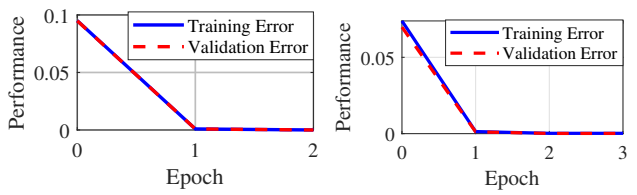
TABLE II: Training results of the proposed framework.

IMG	Training time (s)	Epochs	MAE	RMSE
1	4.0835	2	0.0072	1.72×10^{-5}
2	3.8704	2	0.0081	2.042×10^{-5}

IV. Results and Discussion

A. Efficacy of the faster convergence of the proposed method

The proposed sparse-guided DNN framework for detecting injected attacks and compromised channels in INMG critically relies on system data acquisition. The system depicted in Fig. 1 is simulated in MATLAB using the parameters listed



(a) Training error for IMG 1 (b) Training error for IMG 2

Fig. 3: Training performance of the proposed framework.

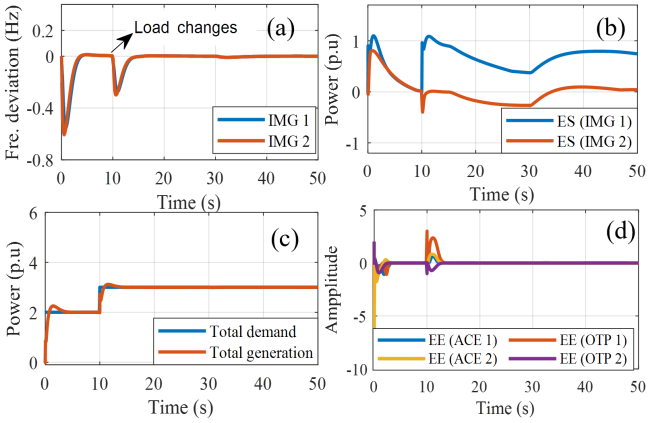


Fig. 4: Performance of the proposed framework for INMG: (a) Frequency response, (b) ES system response, (c) Total demand and generated power, and (d) Estimation error.

in Table I. To enable data collection, relevant input and target variables for the DNN are defined and simulated under standard operating conditions, including load variations. The input data for local DNN comprises $\Delta\mathcal{F}$ measurements from the local IMG and its associated $\Delta\mathcal{T}_{tie}$ power signals. At the same time, the target variable of local DNN consists of the $\mathcal{E}_c$ and the $\mathcal{P}_{tar}$ signal for the local IMG. As the proposed system identifies injected attacks by estimating the target variable through an intensive training process, data are generated via a simulation of 50 s under normal operating conditions, resulting in a dataset containing $1,000,000$ input-output pairs. This extensive dataset is then utilized to train the proposed DNN framework, enabling it to accurately detect attack signals in the communication channels of the INMG. Fig. 3 shows the training efficacy of the proposed DNN method for both IMGs, as indicated by the training and validation errors, while Table II lists their quantitative error measurements. These responses exhibit the high computational efficiency of the proposed DNN framework, especially in terms of training time and accuracy. The model reaches minimal training error in only two epochs for both IMGs, taking about 4 s, which underscores the quick convergence of the proposed framework. Moreover, the reduced mean absolute error (MAE) and root mean square error (RMSE) further confirm the framework's efficacy in estimating the target variables.

B. Efficacy of the proposed DNN under load changes

The proposed DNN framework is integrated into the centralized ADM framework of INMG after completing its training phase. In this configuration, each IMG features a local estimator that estimates regional targets, such as the ACE and OTP. A key indicator for detecting attacks and compromised

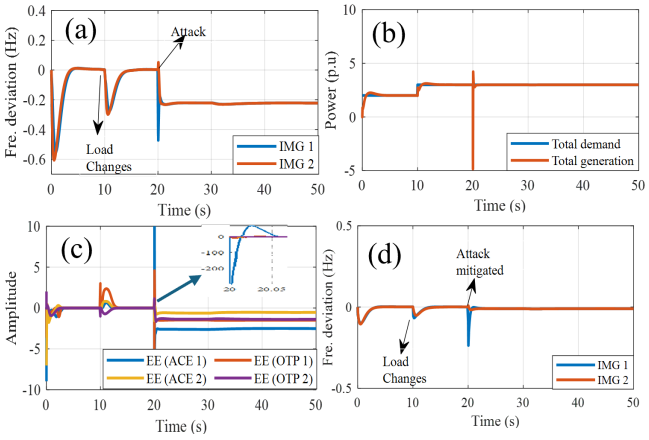


Fig. 5: Proposed framework performance under constant FDI attack on the SCL local channel at $t = 20$ s: (a) Frequency without mitigation, (b) Total demand vs. generation, (c) Estimation error, (d) Frequency post-mitigation.

channels is the estimation error (EE), representing the difference between the estimated and actual target values. The responses from this implementation are illustrated in Fig. 4, where Fig. 4(a) shows the frequency deviation response for both IMGs following sudden load changes in IMG 1 at $t = 10$ s. Despite the abrupt change, both IMGs quickly return to frequency stability. This rapid recovery is achieved through the coordinated action of the controller, which activates support from the ES systems, as shown in Fig. 4 (b), by adjusting the local control signal. This modification enables the INMG system to maintain effective coordination between total nominal generation and load demand, ensuring that the INMG system maintains energy balance, as shown in Fig. 4(c). The response in Fig. 4(d) is the key to understanding the dynamic behavior of the proposed trained DNN. Here, the estimator experiences a spike in estimation error for both ACE and OTP variables right after the load changes. However, these spikes quickly diminish to zero, ensuring that the proposed DNN correctly identifies this error as a natural disruption, like load changes, based on Remark 2. These outcomes demonstrate the excellent estimation accuracy of the proposed framework in identifying the dynamics of load changes.

C. Case 1: Detecting and mitigating attacks on the local channel of SCL using the proposed method

A scenario involving a constant FDI attack and load variations is simulated at the INMG terminal to assess the efficacy of the proposed DNN. Here, the attack is introduced through the local communication channel (frequency channel) of SCL in IMG 1, and the resulting dynamic responses are shown in Fig. 5. As illustrated in Fig. 5(a), both IMGs exhibit a coordinated and stable frequency response following the initial load change at $t = 10$ s. However, a notable deviation occurs at $t = 20$ s, followed by a sustained offset. This clearly indicates a cyber attack compromising the operation of the INMG and highlights the necessity for effective detection and mitigation mechanisms. Furthermore, as shown in Fig. 5(b), the total generation momentarily collapses at the onset of the attack, reflecting a breakdown in distributed control

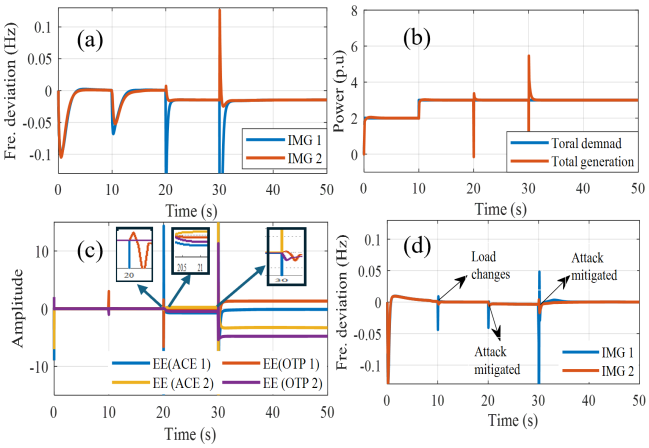


Fig. 6: Proposed framework performance under constant FDI attack on the SCL local and global channels: (a) Frequency without mitigation, (b) Total demand vs. generation, (c) Estimation error, (d) Frequency post-mitigation.

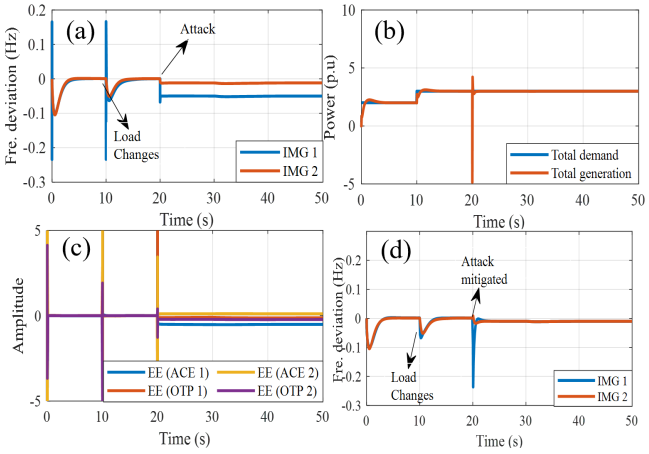


Fig. 7: Proposed framework performance under constant FDI attack on the SCL local channels with increasing system parameters by up to 15%: (a) Frequency without mitigation, (b) Total demand vs. generation, (c) Estimation error, (d) Frequency post-mitigation.

coordination within the INMG. Fig. 5(c) presents the EE generated by the proposed framework based on (20). As noted in Remark 2, the estimator associated with IMG 1 exhibits a sharp spike in ACE 1 at the moment of the attack, followed by a prominent negative error, confirming that the attack is confined to the local communication channel of SCL in IMG 1. In contrast, the EEs resulting from earlier load perturbations are transient and quickly converge to zero, demonstrating the framework's ability to distinguish between normal load variations and cyber attack scenarios. Based on the EEs, the controller in the mitigation layer uses the EE to generate a counter-attack signal, allowing IMG 1 to quickly suppress the frequency deviation. Consequently, system stability is restored across both IMGs. This highlights the framework's capability to detect and localize attacks while enabling timely corrective actions to maintain operational integrity of the INMG.

D. Case 2: Detecting and mitigating attacks on the local and global SCL channels using the proposed method

This experiment evaluates the efficacy of the proposed framework under simultaneous constant FDI attacks, targeting the local (frequency) channel at $t = 20$ s and the global (tie-line power) channel at $t = 30$ s of the SCL in INM 1. Fig. 6(a) illustrates the frequency deviation responses of the INMG when IMG 1 is subjected to attacks on both communication channels of the SCL. Additionally, Fig. 6(b) shows a transient disturbance in generated power due to the breakdown of coordinated control actions during the attack. This underscores the need for ADM to restore frequency stability and ensure reliable operation of the INMG. The EEs for both IMGs are shown in Fig. 6(c), indicating that the attack at $t = 20$ s causes a distinct spike in the EE of the ACE signal for IMG 1. This error fails to converge to zero and remains prominently negative until the second attack occurs. According to Remark 2, this behavior confirms that the local communication channel in the SCL of IMG 1 is compromised by the attack. Similarly, at $t = 30$ s, the ACE signal for estimators of both IMGs exhibits simultaneous sharp spikes at the onset of attack, consistent with a breach in the global communication channel, as detailed in Remark 2. Although dual-targeted attacks can be complex, the framework effectively distinguishes between authentic system dynamics and malicious actions. Fig. 6(d) illustrates that the controller in the mitigation layer generates countermeasure signals against attacks by leveraging EE, thereby reducing the impact of dual attacks. This guarantees the reliable and safe operation of the INMG, even when facing coordinated FDI attacks.

E. Sensitivity analysis of the proposed framework

Sensitivity analysis evaluates how the variations in parameters, such as weights Θ or input values, influence the output $M(t)$. However, altering the weights might not affect the estimated output as SMC optimization tries to reach the same optimal solution under fixed input of the proposed framework. Therefore, sensitivity is measured by varying the input parameters, which involves increasing system parameters by up to 15%. The performance of the proposed framework is illustrated in Fig. 7 under the study of Case 1, with increasing system parameters, shown in Table I. The results indicate that the proposed DNN framework is minimally affected by parameter variations when successfully detecting and mitigating cyber-attacks based on Remark 2.

F. Scalability of the proposed framework

The scalability of the proposed framework is further validated through a simulation involving six IMGs connected as shown in Fig. 8(a). An attack is triggered at t = 20 s in the local channel of IMG 1. The frequency response of the INMG is depicted in Fig. 8(b). The error estimation from the local estimator, shown in Fig. 8(c), demonstrates that the attack injected into IMG 1 is easily detectable, as the local estimator for IMG 1 displays a notable error, as explained in Remark 2. Finally, the mitigated performance is shown in Figure 8(d), which demonstrates that the proposed framework can effectively reduce the impact of attacks across multiple IMGs. This assessment confirms that the framework

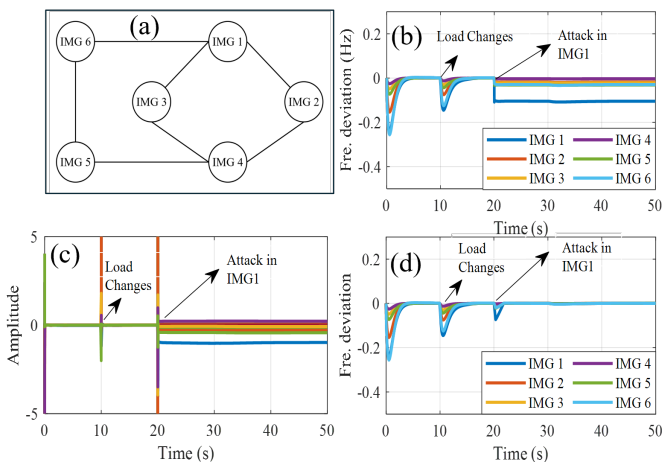


Fig. 8: Scalability assessment of the proposed framework under constant FDI attack: (a) Configuration of INMG, (b) Frequency response, (c) Estimation error, (d) Frequency post-mitigation.

successfully detects and mitigates attacks in a scalable way across a larger network.

V. Real-time Simulation

The effectiveness of the proposed DNN is further validated through real-time simulation of the studied system in Fig. 1. The simulation is performed using the OPAL-RT OP5700 simulator, which interfaces with the host computer via an Ethernet connection, as illustrated in Fig. 9. To enable communication between the host and target systems, a shared IP address is configured, allowing both to operate within the same subnetwork. In this experiment, a constant FDI attack is intentionally applied to TCL at $t = 25$ s to modify the OTP via altering the nominal generation of IMG 2. The dynamic responses from the real-time simulation under this scenario are illustrated in Fig. 10. Fig. 10(a) shows the frequency deviation of both IMGs, where a significant frequency deviation is observed following the attack. However, this disruption stabilizes after a short transient, as the lower-level control system autonomously redistributes control efforts to the unaffected IMGs and adjusts the generator or ES output power to restore the stable frequency. Again, the total nominal generation and demand power of the INMG is shown in Fig. 10(b), where it can be observed that the generation suddenly increases at $t = 25$ s while the demand remains unchanged. This disrupts the cost-effective operation of the INMG, resulting in inefficient energy dispatch. Fig. 10(c) illustrates the EEs, revealing that the estimator for the IMG 2 experiences a sudden EE in estimation at $t = 25$ s and fails to converge to zero, while the estimators for the other IMGs successfully converge to zero. This behavior confirms that an attack signal is presented on the TCL of IMG 2, as noted in Remark 3, which needs to be addressed for the cost-effective functioning of INMG. Like in other scenarios, the controller within the mitigation layer processes the EE and generates a counterattack signal to neutralize the impact of attacks. Fig. 10(d) illustrates the frequency deviation following the attack mitigation. There is a noticeable reduction in frequency deviation, characterized

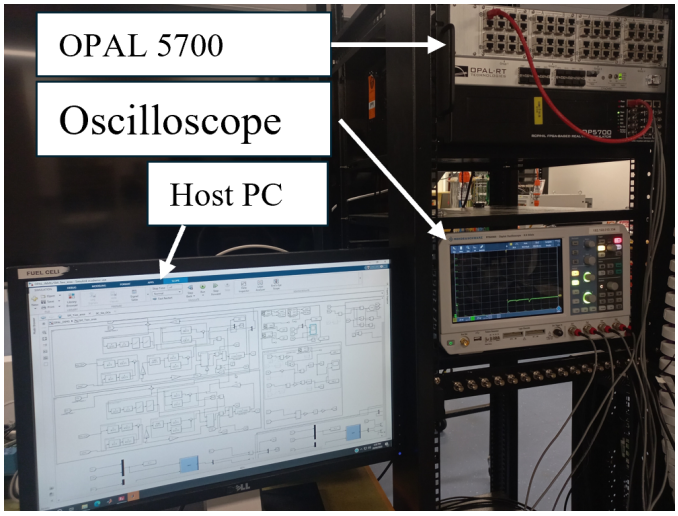


Fig. 9: Real-time testing setup.

by a swift recovery, which signifies effective mitigation. This allows the system to revert to a balanced operation, thereby improving the operational reliability and economic efficiency of the INMG even after facing a cyber attack on TCL.

A. Comparative analysis

In Table III, we present a comparative analysis of the proposed DNN against several recent state-of-the-art methods regarding the cyber-resilience frequency performance of IMGs. Due to the inherent variability in system dynamics, operational configurations, and attack types across different studies, a direct quantitative evaluation lacks meaning and consistency. Instead, we conduct a qualitative feature-based comparison to highlight the distinct advantages of the proposed method. Unlike existing approaches, the proposed framework is uniquely capable of detecting cyberattacks targeting the TCL, identifying compromised IMGs and communication channels, and achieving rapid convergence in training. These features are either absent or underexplored in the compared methods. Additionally, the proposed DNN exhibits real-time responsiveness and learning-based scalability, further solidifying its adaptability to evolving threats and dynamic conditions. While all compared methods support ADM on the SCL, only the proposed approach achieves comprehensive cyber-resilient performance by integrating detection, localization, and fast adaptation mechanisms across both control layers. Overall, the proposed framework provides a scalable and intelligent solution for ensuring secure and cost-effective IMG operations in the face of cyber-physical disruptions.

VI. Assumptions and Limitations

While the proposed framework exhibits promising outcomes in cyber-resilience for INMG, it is essential to acknowledge certain underlying assumptions and limitations that may influence its actual real-world applicability. The proposed model assumes that the power calculated from the TCL accurately indicates the OTP for local IMGs. It is also assumed that the communication networks are initially dependable, and the system dynamics are influenced solely by cyber-attacks or load

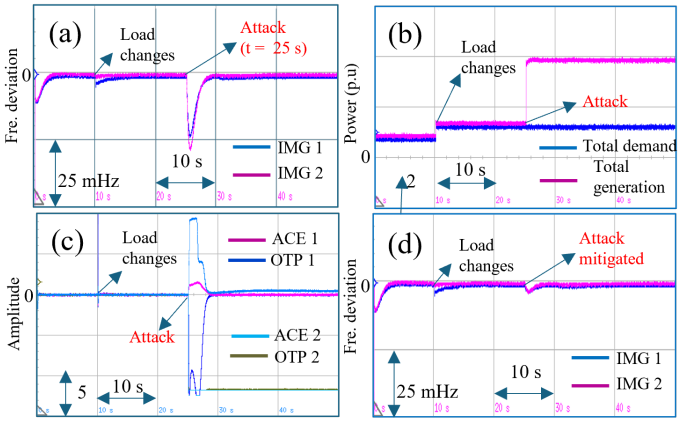


Fig. 10: Proposed framework performance under constant FDI attack on the TCL channel in IMG 2 at $t = 25$ s: (a) Frequency without mitigation, (b) Total demand vs. generation, (c) Estimation error, (d) Frequency post-mitigation.

TABLE III: Comparison of the proposed method with others.

FeaturesMethods	[13]	[24]	[16]	[21]	[30]	Proposed
Attack on TCL	×	×	×	×	×	✓
Learning-based scalability	N/A	✓	N/A	✓	N/A	✓
Attack mitigation	✓	✓	✓	✓	✓	✓
FDI attack detection on SCL	✓	✓	✓	✓	✓	✓
Compromised IMGs detection	×	×	×	×	×	✓
Compromised channel detection	×	×	×	×	×	✓
Rapid convergence	N/A	×	N/A	×	N/A	✓
Real-time response	×	✓	×	✓	✓	✓

changes, while other disruptions or faults are not considered. As the proposed model lacks mechanisms for noisy inputs, its performance may decline when noise is present. Still, its effectiveness has been evaluated under parameter uncertainty, providing insights into how it responds to parameter changes. However, further improvements are needed to develop methods for robustly managing input noise.

Furthermore, while the proposed framework is effective in identifying and mitigating FDI attacks, stealthy attacks that subtly alter system behaviour without causing noticeable errors still pose a challenge. Future studies based on the measurement of probabilistic confidence may focus on enhancing the detection mechanism to identify these subtle attack signatures, as it can quantify the certainty of the model's predictions. When the confidence falls below a specific threshold, it may indicate the presence of a stealthy attack. The proposed framework may also encounter challenges in precisely detecting and mitigating attacks when delays in estimator updates arise, which could be attributed to network latency or communication bottlenecks. Overcoming this limitation may require optimizing communication protocols for efficiently managing delays in control system updates. These integrations will further enhance the robustness and scalability of the proposed framework, supporting more resilient operations in dynamic real-world environments.

VII. Conclusion

This paper presented a sparse-guided DNN framework for ensuring cyber-resilience and cost-effective frequency support in an INMG facing FDI attacks. The framework was designed based on an RNN architecture, informed by sparse Bayesian learning principles, and enhanced through SMC techniques to tackle key issues like slow convergence and high computational costs. The performance of the proposed framework was evaluated through both real-time and MATLAB simulations across multiple scenarios, including attacks on the SCL and TCL, as well as varying load conditions. Results demonstrate that the proposed framework effectively detects and mitigates attacks while maintaining stable frequency in the INMG, even under coordinated attacks on SCL. Additionally, the sparse learning foundation contributed to accelerated convergence, while the integration of SMC optimization enabled efficient resource utilization. It achieves minimal training error within just two epochs for both IMGs, with training times of approximately 4 seconds, underscoring the rapid convergence of the proposed framework. Thus, the proposed method offers several benefits, including low computational resource requirements, rapid convergence, and enhanced security, thereby ensuring efficient, resilient, and cost-effective operation in dynamic settings. Additionally, the proposed framework provides a solid foundation for real-time distributed attack detection in future energy grids. Looking to the future, the proposed strategy is highly applicable to the next-generation INMGs, which will increasingly rely on RESs and complex communication networks. Its scalability and ability to quickly adapt to evolving cyber threats make it ideal for large-scale deployments in remote and interconnected energy systems.

In the future, we plan to include a stability analysis along with the detailed convergence proof for the proposed framework, providing further theoretical validation of the rapid convergence observed in the simulation results. Furthermore, this work can be extended to develop a robust distributed attack detection framework based on probabilistic confidence measures, aimed at restoring load frequency in the INMG under noisy and uncertain operating conditions. Additionally, optimizing the LFC controller will be explored, focusing on enhancing its performance under dynamic conditions and achieving a more efficient response time. Future work will also include a more comprehensive analysis of the demerits of the current system, such as increased computational complexity and sensitivity to parameter variations, and propose potential solutions for mitigating these challenges.

References

[1] J. De La Cruz, Y. Wu, J. E. Candelo-Becerra, J. C. Vásquez, and J. M. Guerrero, "Review of networked microgrid protection: architectures, challenges, solutions, and future trends," *CSEE Journal of Power and Energy Systems*, vol. 10, no. 2, pp. 448–467, 2023.

[2] N. Khosravi, "Finite-time control scheme for effective voltage and frequency regulation in networked microgrids," *International Journal of Electrical Power & Energy Systems*, vol. 165, p. 110481, 2025.

[3] T. Ma, M.-J. Li, H. Xu, R. Jiang, and J.-W. Ni, "Study on multi-time scale frequency hierarchical control method and dynamic response characteristics of the generation-grid-load-storage type integrated system under double-side randomization conditions," *Applied Energy*, vol. 367, p. 123436, 2024.

[4] Z. Tang, Y. Liu, T. Liu, G. Qiu, and J. Liu, "Distributed data-driven frequency control in networked microgrids via voltage regulation," *IEEE Transactions on Smart Grid*, 2024.

[5] H. Shafei, M. Farhangi, L. Li, R. P. Aguilera, H. H. Alhelou, *et al.*, "A novel cyber-attack detection and mitigation for coupled power and information networks in microgrids using distributed sliding mode unknown input observer," *IEEE Transactions on Smart Grid*, 2024.

[6] S. K. Sarker, H. Shafei, T. Shi, L. Li, M. Hossain, and R. P. Aguilera, "A data-driven multivariable adaptive cybersecurity framework for isolated microgrids," in *2024 IEEE 34th Australasian Universities Power Engineering Conference (AUPEC)*. IEEE, 2024, pp. 1–6.

[7] M. Mohiti, H. Monsef, A. Anvari-Moghaddam, and H. Lesani, "Two-stage robust optimization for resilient operation of microgrids considering hierarchical frequency control structure," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 11, pp. 9439–9449, 2019.

[8] M. Mazidi, N. Rezaei, F. J. Ardakani, M. Mohiti, and J. M. Guerrero, "A hierarchical energy management system for islanded multi-microgrid clusters considering frequency security constraints," *International Journal of Electrical Power & Energy Systems*, vol. 121, p. 106134, 2020.

[9] P. C. Nayak, U. C. Prusty, R. C. Prusty, and S. Panda, "Imperialist competitive algorithm optimized cascade controller for load frequency control of multi-microgrid system," *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, vol. 47, no. 1, pp. 5538–5560, 2025.

[10] S. Chakraborty, S. Kar, and S. R. Samantaray, "Hierarchical dual loop voltage and frequency control in stand alone microgrid with priority based intelligent load management," *Electric Power Systems Research*, vol. 220, p. 109339, 2023.

[11] S. Chakraborty and S. Kar, "Hierarchical control of networked microgrid with intelligent management of tcls: A case study approach," *Electric Power Systems Research*, vol. 224, p. 109787, 2023.

[12] N. Khosravi, M. Dowlatabadi, and K. Sabzevari, "A hierarchical deep learning approach to optimizing voltage and frequency control in networked microgrid systems," *Applied Energy*, vol. 377, p. 124313, 2025.

[13] 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*, vol. 16, no. 1, pp. 1021–1031, 2021.

[14] M. R. Khalghani, J. Solanki, S. K. Solanki, M. H. Khooban, and A. Sargolzaei, "Resilient frequency control design for microgrids under false data injection," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 3, pp. 2151–2162, 2020.

[15] K. Han, K. Zhang, Z.-P. Wang, and R. Su, "Resilient predictive load frequency control of multi-area interconnected power systems with privacy preserving and active detection against stealthy cyber attacks," *IEEE Internet of Things Journal*, 2024.

[16] T. Kerdphol, I. Ngamroo, and T. Surinkaew, "Enhanced robust frequency stabilization of a microgrid against simultaneous cyber-attacks," *Electric Power Systems Research*, vol. 228, p. 110006, 2024.

[17] M. I. Ibraheem, M. Edrisi, H. H. Alhelou, M. Gholipour, and A. Al-Hinai, "A sophisticated slide mode controller of microgrid system load frequency control under false data injection attack and actuator time delay," *IEEE Transactions on Industry Applications*, 2023.

[18] J. Li and T. Zhou, "Data-driven fully distributed load frequency control for an iot-based interconnected grid considering a performance-based frequency regulation market," *IEEE Internet of Things Journal*, 2024.

[19] A. Nandakumar, Y. Li, Z. Xu, and D. Huang, "Enhancing transient dynamics stabilization in islanded microgrids through adaptive and hierarchical data-driven predictive droop control," *IEEE Transactions on Smart Grid*, 2024.

[20] T. Tabassum, S. Lim, and M. R. Khalghani, "Artificial intelligence-based detection and mitigation of cyber disruptions in microgrid control," *Electric Power Systems Research*, vol. 226, p. 109925, 2024.

[21] J. Heidary, S. Oshnoei, M. Gheisarnejad, M. R. Khalghani, and M. H. Khooban, "Shipboard microgrid frequency control based on machine learning under hybrid cyberattacks," *IEEE Transactions on Industrial Electronics*, 2023.

[22] M. Zhang, S. Dong, P. Shi, G. Chen, and X. Guan, "Distributed observer-based event-triggered load frequency control of multiarea power systems under cyber attacks," *IEEE Transactions on Automation Science and Engineering*, vol. 20, no. 4, pp. 2435–2444, 2022.

[23] X. Liu, Q. Jiao, S. Qiao, Z. Yan, S. Wen, and P. Wang, "A hybrid monotonic neural network approach for multi-area power system load frequency control against fgsm attack," *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2024.

[24] A. Saxena, R. Shankar, C. Kumar, and S. Parida, "A resilient frequency regulation for enhancing power system security against hybrid cyber-attacks," *IEEE Transactions on Industry Applications*, 2024.

[25] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "Detection of false data injection cyber-attacks in dc microgrids based on recurrent neural networks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5294–5310, 2020.

[26] H. Saxén and F. Pettersson, "Method for the selection of inputs and structure of feedforward neural networks," *Computers & Chemical Engineering*, vol. 30, no. 6-7, pp. 1038–1045, 2006.

[27] V. Veerasamy, L. P. M. I. Sampath, S. Singh, H. D. Nguyen, and H. B. Gooi, "Blockchain-based decentralized frequency control of microgrids using federated learning fractional-order recurrent neural network," *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 1089–1102, 2023.

[28] R. Tibshirani, "Regression shrinkage and selection via the lasso," *Journal of the Royal Statistical Society Series B: Statistical Methodology*, vol. 58, no. 1, pp. 267–288, 1996.

[29] F. Caron, L. Bornn, and A. Doucet, "Sparsity-promoting bayesian dynamic linear models," *arXiv preprint arXiv:1203.0106*, 2012.

[30] S. Hu, X. Ge, X. Chen, and D. Yue, "Resilient load frequency control of islanded ac microgrids under concurrent false data injection and denial-of-service attacks," *IEEE Transactions on Smart Grid*, vol. 14, no. 1, pp. 690–700, 2022.

Subrata K. Sarker (Student Member, IEEE) is currently pursuing a Master by Research degree at the University of Technology Sydney (UTS), Australia. He received his Bachelor of Science degree in Mechatronics Engineering from the Rajshahi University of Engineering and Technology (RUET), Rajshahi, Bangladesh, in December 2018. In September 2019, he joined the Department of Electrical and Electronic Engineering at Varendra University (VU), Rajshahi, Bangladesh, as a Lecturer. He served there until June 2021, when he joined the Department of Mechatronics Engineering, Rajshahi University of Engineering and Technology (RUET), as a Lecturer. He has authored or coauthored more than 110 papers in various journals and international conferences. He also serves as an Editor or Associate Editor for several prestigious journals from Wiley, Springer, and other publishers, including International Transactions on Electrical Energy Systems, International Journal of Computational Intelligence Systems, and International Journal of Intelligent Systems. His research interests include cybersecurity, intelligent control theory and applications, robotics, mechatronic systems, and power system control. He is currently on study leave from RUET to pursue his higher studies.

Hamidreza Shafei (Member, IEEE) received his B.Sc. degree in Mechanical Engineering from Kerman University, Iran, in 2011, and his M.Sc. degree in Mechanical Engineering (Dynamics and Control) from Amirkabir University of Technology, Iran, in 2014. He completed his Ph.D. degree with the School of Electrical and Data Engineering at the University of Technology Sydney (UTS), Australia, in 2025. His research interests include nonlinear control, dynamic state estimation, power systems, power system cybersecurity, microgrids, and robotics.

Li Li (Senior Member, IEEE) received his B.S. degree from Huazhong University of Science and Technology in 1996, M.S. degree from Tsinghua University in 1999, and Ph.D. degree from University of California, Los Angeles in 2005 respectively, all in Electrical Engineering. From 2005 to 2007 he was a research associate at the University of New South Wales at the Australian Defence Force Academy (UNSW@ADFA). From 2007 to 2011, he was a researcher at the National ICT Australia, Victoria Research Laboratory, Department of Electrical and Electronic Engineering, The University of Melbourne. He joined the University of Technology Sydney in 2011, and currently he is an Associate Professor. Dr Li held several visiting positions at various universities. His research interests are power systems and control theory. He is presently serving as an Associate Editor of IEEE Transactions on Industry Applications, IET Renewable Power Generation, and IET Generation, Distribution and Transmission.

Jahangir Hossain (M'10-SM'13) received the B.Sc. and M.Sc. Eng. degrees from Rajshahi University of Engineering and Technology (RUET), Bangladesh, in 2001 and 2005, respectively, and the Ph.D. degree from the University of New South Wales in 2010, Australia, all in electrical and electronic engineering. He is currently a Professor with the School of Electrical and Data Engineering, University of Technology, Sydney, Australia. Before joining there, he served as an Associate Professor in the School of Engineering, Macquarie University, Senior Lecture and a Lecturer in the Griffith School of Engineering, Griffith University, Australia for five years and as a Research Fellow in the School of Information Technology and Electrical Engineering, University of Queensland, Brisbane, Australia. He worked as lecturer and assistant professor for more than six years at RUET. He is a senior member of IEEE and AEr of two IEEE Trans. His research interests include renewable energy integration and stabilization, voltage stability, micro grids and smart grids, robust control, electric vehicles, building energy management systems, and energy storage systems.

S M Muyeen (S'03–M'08–SM'12–F'24) is a full professor in the Electrical Engineering Department of Qatar University. He received his B.Sc. Eng. Degree from Rajshahi University of Engineering and Technology (RUET), Bangladesh, formerly known as Rajshahi Institute of Technology, in 2000 and M. Eng. and Ph.D. Degrees from Kitami Institute of Technology, Japan, in 2005 and 2008, respectively, all in Electrical and Electronic Engineering. His research interests are power system stability and control, electrical machine, FACTS, energy storage system (ESS), Renewable Energy, and HVDC system. He has been a Keynote Speaker and an Invited Speaker at many international conferences, workshops, and universities. He has published more than 500+ articles in different journals and international conferences. He has published seven books as an author or editor. He served as Editor/Associate Editor for many prestigious Journals from IEEE, IET, and other publishers, including IEEE Transactions on Energy Conversion, IEEE Power Engineering Letters, IET Renewable Power Generation and IET Generation, Transmission & Distribution, etc. Dr. Muyeen is a Fellow of IEEE, Chartered Professional Engineers, Australia, and a Fellow of Engineers Australia.