AIMS Mathematics, 11(5): 15233–15276.
DOI: 10.3934/math.2026627
Received: 28 January 2026
Revised: 13 April 2026
Accepted: 16 April 2026
Published: 29 May 2026

https://www.aimspress.com/journal/Math

Research article

A bio-inspired neuromorphic framework for decentralized fault detection and renewable optimization in smart grids

Mohammad Barr[1], Tawfeeq Shawly[2], Ahmed A. Alsheikhy[3,*], Yahia Said[4], Shaaban M. Shaaban[4] and Aws AbuEid[5]

[1] Department of Electrical Engineering, College of Engineering, Northern Border University, Arar 91431, Saudi Arabia; mohammed.barr@nbu.edu.sa
[2] Department of Electrical Engineering, Faculty of Engineering at Rabigh, King Abdulaziz University, Jeddah 21589, Saudi Arabia; tshawly@kau.edu.sa
[3] Department of Computer and Network Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia; aaalsheikhy@uj.edu.sa
[4] Center for Scientific Research and Entrepreneurship, Northern Border University, Arar 73213, Saudi Arabia; Yahia.said@nbu.edu.sa, shaban.awdallah@nbu.edu.sa
[5] Department of Information and Communication Technology, College of Computing Studies, Arab Open University, Kuwait Branch, Kuwait; a.abueid@arabou.edu.kw

*** Correspondence:** Email: aaalsheikhy@uj.edu.sa.

Abstract: Modern smart grids encounter several challenges, including the variability of renewable energy sources with power fluctuations of ±35% in solar farms across the Arabian Gulf countries, delays in centralized control, with latencies of 150–200 ms, including all time needed from sending data to receiving control commands, and increased susceptibility to cyber threats, with a 30% annual increase in grid intrusions. Incorporating renewable energy into smart grids presents significant challenges, including intermittent generation, characterized by ±30% solar volatility, slow fault detection, and response times exceeding 500 ms in traditional systems, as well as centralized system weaknesses. This paper presents SwarmNet-5G, a bio-inspired neural network that integrates stigmergic learning and spiking neural networks (SNNs) for decentralized grid management to resolve existing issues. It merges Internet of Things (IoT)-edge intelligence, spiking neuromorphic computing, and swarm-based stigmergy to enable grid optimization. Its design decreases latency by 40% compared to typical deep reinforcement learning (DRL). It achieves a fault detection accuracy of 99.62% within 8.17 ms and requires 50 ms for repair, aligning with Saudi Arabia's

Vision 2030 goal of achieving 50% renewable energy. Simulation results performed on the IEEE 39-bus using a dataset show that the solution allocated power during peak demand, such as a 20% load increase, with an efficiency of 92%, while typical DRL reached 78%. Additionally, the model projected annual savings of \$1.2B in maintenance costs and a reduction of 4.8 megatons in CO_2 emissions per year.

Keywords: decentralized neuromorphic computing; 5G-IoT smart grids; stigmergic energy optimization; self-healing microgrids; spiking neural networks
Mathematics Subject Classification: 68T07, 68T10, 68T20

1. Introduction

Smart grids show the next advancement in electricity networks by incorporating digital communication and IoT sensors to replace outdated and passive systems [1,2]. These grids allow for real-time monitoring and management to enhance energy distribution and minimize waste. This modernization is essential, since global electricity demand is expected to increase 60% by 2050 [1,2]. A crucial function of smart grids is to support the widespread adoption of renewable energy sources (RESs). Solar and wind energy can be inconsistent due to changing weather patterns; however, smart grids employ predictive algorithms and coordinate energy storage to dynamically balance supply and demand. One significant benefit of smart grids is their self-healing ability, which utilizes artificial intelligence (AI) and automation to identify and isolate faults, such as power line failures, within milliseconds [2]. By integrating distributed energy resources (DERs) and microgrids, smart grids can independently redirect power to reduce the duration of blackouts [2–5]. Furthermore, smart grids enhance consumer engagement through demand response initiatives, where IoT-enabled smart meters modify electricity consumption during peak periods based on real-time pricing. As power grids become increasingly interconnected, they are encountering heightened cyber threats. To address these challenges, smart grids utilize blockchain technology for secure transactions, AI for detecting anomalies, and decentralized management systems [5–8]. Saudi Arabia's NEOM initiative emphasizes cybersecurity to protect its investment in the smart city grid [8–12]. Smart grids are crucial for the development of smart cities and electric vehicle (EV) ecosystems, enabling the efficient management of millions of charging stations without risking system overload.

DRL has become an influential method for enhancing the operations of smart grids by utilizing real-time decision-making in complex environments. Techniques, such as proximal policy optimization (PPO) and deep Q-networks (DQNs), developed strategies for energy distribution, demand response, and fault recovery through iterative interactions. Nevertheless, DRL requires substantial computational power and faces challenges in scalability when applied to large and dynamic grids, due to the complexity of high-dimensional state spaces. Convolutional neural networks (CNNs) are particularly adept at analyzing spatial-temporal grid data for voltage variations and line temperatures to forecast and identify faults [13–15]. Long-short term memory (LSTM) models are utilized for forecasting solar and wind energy production by examining weather trends and historical energy output. In Germany, forecasts based on LSTM models have led to a 22% reduction in renewable energy, resulting in significant savings [16]. Federated learning (FL) accelerates decentralized AI training across smart meters and grid nodes while preserving the

confidentiality of raw data. Graph neural networks (GNNs) represent the power grid as a graph, demonstrating the connections between nodes, such as substations and power lines, to enhance power distribution. However, GNNs face challenges in adapting to real-time changes in grid topology during sudden events like natural disasters [11,12,17,18]. Transformers are used for grid management by analyzing diverse data sources, such as weather conditions, energy demand, and pricing, to coordinate DERs. Physics-informed neural networks (PINNs) incorporate physical laws governing grids, such as Kirchhoff's laws, into neural network frameworks to ensure that the solutions produced comply with real-world limitations [11,12].

1.1. Research problem

Recent power grids have experienced changing demand patterns, growing cybersecurity threats, and the incorporation of energy sources. Typical grid management systems are insufficient when dealing with these issues. Hence, this led to inefficient energy distribution and slow fault identification and response times. Additionally, solar and wind energy create unpredictable fluctuations due to their natural variations. Moreover, obsolete infrastructure is unable to adjust to the needs of a growing number of users. The proposed framework addresses these issues by implementing various components, which are placing spiking neural networks (SNNs) at each grid node, decentralized neuromorphic computing, and swarm intelligence to boost ultra-fast decision-making to respond to fluctuations in renewable energy within a short time. Additionally, it enables the independent coordination among distributed energy resources.

1.2. Objectives and motivations

SwarmNet-5G can precisely identify and locate faults in a very short time, while other approaches can take a long time, which results in unneeded outages. Its architecture achieves a fault detection accuracy of 99.62%. Additionally, its capability allows it to trigger self-healing protocols in less than 8 s, which eliminates single points of failure. It minimizes latency and provides stability in normal and severe conditions. Furthermore, it shows a notable scalability to overcome a major limitation of existing AI solutions, as it can grow from hundreds to thousands of nodes easily. Moreover, its design and communication capabilities enable effective coordination in various networks, which makes it appropriate for urban and remote grids. For economic and environmental benefits, it improves energy distribution, minimizes waste, attains notable annual savings in operational expenses, and reduces carbon emissions.

1.3. Research contributions

This research provides numerous contributions, which are summarized as follows:

(1) A novel AI framework:

- Decentralized neuromorphic swarm intelligence: Presents SNN utilizing stigmergic learning for smart grids to remove reliance on backpropagation-based training methods.
- Introduces a self-evolving neural structure that adapts by expanding or reducing neurons in response to real-time grid requirements.
- Enables distributed nodes to work together to optimize grid operations without the need for

centralized oversight.

(2) Rapid and robust grid management:

- Achieves decision-making latency of less than 10 ms, surpassing traditional DRL as demonstrated through the conducted analysis.
- Facilitates self-healing features with notable accuracy and recovery times of under 2 s to significantly decrease outage durations by 90% compared to implemented standard systems.

(3) Energy and cost efficiency:

- Achieves a 43% reduction in energy waste during peak demand periods using dynamic load balancing and demand response strategies.
- Anticipates a decrease in operational expenses of $310M annually.

This paper is organized as follows: Section 2 presents the proposed methodology, while Section 3 elaborates on the experimental setup and results. Sections 4 and 5 examine the implications and limitations, and Section 6 concludes with suggestions for future research.

1.4. Literature review

This section provides a literature review of some state-of-the-art methods and shows their limitations. Then, we illustrate how the proposed method addresses these limitations or gaps.

J. Jithish et al. in [13] developed FL-based anomaly detection in a smart grid using machine learning (ML) methods that were trained locally without sharing data with a central server to ensure user privacy. The authors downloaded a global model from the server to be installed on smart meters for training. Then, local model parameters were sent to the server to improve the global model. The authors secured the model parameter updates from adversaries using the SSL/TLS protocol. The authors examined anomaly detection performance on several datasets, and their model achieved an average accuracy of 87.3% while consuming 2.85W of power. Additionally, their approach took nearly 33 s. However, various limitations exist in their approach, which are computational loads, communication latency between clients and servers, and data heterogeneity. Moreover, the model consumed a notable amount of memory and CPU usage.

J. Qiu in [14] implemented an anomaly detection method for a smart grid on spatial-temporal graph neural networks (STGNNs). This model included a graph convolution gated recursive unit (GCGRU) layer and a fully connected layer. Additionally, the attribute values were assigned to the power network and the nodes of the physical transmission network, to characterize the values of the related features that affected the nodes based on geographical proximity. It used the progression of data of numerous characteristics to characterize the growth of the power network. STGNNs were applied to find the time-space dependencies of nodes in various networks to aid the approach using anomaly data from other related networks. Simulation experiment results showed that the scheme achieved an accuracy rate of 90% on the IEEE 1180bus. This rate improved significantly as the time went up during training. In addition, numerous ML and AI approaches were utilized for comparison purposes on a single dataset.

Q. Shuai et al. in [15] developed a model for energy management optimization based on an integrated electric–thermal energy system. The authors implemented this method to mitigate the problems of the traditional heuristic algorithms or mathematical planning methods, with low accuracy and low efficiency. In the meantime, the algorithm improved both the convergence speed

and performance compared to the proximal policy optimization algorithm. The authors developed a mathematical approach for energy management. Later, the method was expressed as a Markov decision process, and a reward mechanism was implemented to guide the method to learn the uncertainty characteristics of renewable energy output and load consumption using historical data. Lastly, the algorithm reduced the average running cost by 2.32% compared to the other models during the training stage. The authors utilized the integrated electric–thermal energy system to measure the performance using a simulation analysis based on the integrated system as a case study. For simulation, historical data were used and divided into two sets: a training set and a test set. The simulation lasted for 1000 iterations, and random days were selected during these iterations.

B. Vivek et al. in [18] developed a thorough model for electrical fault detection and localization using ML approaches. This method was designed on the application of a decision tree classifier, and its performance was compared with a random forest algorithm. Additionally, this study addressed the issue of imbalanced classes by using the synthetic minority oversampling technique (SMOTE), which enhanced the robustness of the analysis. Using a varied dataset involving different fault types, the authors conducted experiments for evaluation purposes. The results demonstrated the superiority of decision tree-based approaches in reaching high accuracy rates. This research highlighted the success of using MLs in fault diagnosis and showed their potential for real-world implementation in power systems and industrial settings. V. K. Paravasthu et al. in [19] introduced an approach for incorporating RESs and electric vehicle charging stations (EVCSs) into circular distribution networks using a novel hybrid whale optimization algorithm (HWOA). The authors examined and tested their approach using the IEEE 33 and IEEE 69 bus radial distribution systems (RDSs). The HWOA was implemented to tackle complex optimization tasks in RES and EVCS integration, while minimizing power losses, to improve voltage stability. The algorithm integrated the genetic whale optimization algorithm (GWOA) and thermal exchange optimization (TEO) methods to harness their abilities to improve the location and sizing of RESs and EVCSs. Profound analysis confirmed the efficiency in reaching high outcomes. The HWOA alleviated power losses while simultaneously improving the voltage profile of RDSs. It identified optimal locations for EVCS units, ensuring good coverage to direct the increasing need for EVCSs. Outcomes acquired using the HWOA emphasized its capability to enhance performance and reliability. On the other hand, B. Mallala et al. in [20] addressed the difficulties of providing renewable energy in urbanizing nations, such as India and China. The authors used a random forest algorithm to conduct an analysis on data from Kaggle to forecast the potential of renewable energy. Feature selection was achieved by the correlation coefficient method, which was refined with the mutual information regression method to recognize 11 major features of the target variable. The model reached an accuracy of $R^2 = 0.998$ with a low mean absolute percentage error (MAPE) of 0.21. These results could be employed for renewable energy prediction. In addition, K. Quizhpe et al. in [21] discussed optimizing planning for renewable integration of power systems in microgrids. The authors stated that AI and ML approaches optimize real-time microgrid operations to enhance predictive analysis and fault tolerance. However, various challenges remain, including integrating new technologies, improving simulation accuracy, enhancing energy storage sustainability, and ensuring system resilience. The proposed scheme is developed to integrate new technologies, improve accuracy, and ensure system resilience, which were stated by the authors in [21].

Several noteworthy limitations exist in the previous methods, which are summarized as follows:

1) Most approaches depend on centralized processing systems.

2) Difficulties when facing inexperienced conditions.

3) Large models are not suitable for IoT devices. Our solution seeks to overcome these limitations by employing decentralized neuromorphic learning and bio-inspired swarm intelligence, thereby achieving a substantial increase in speed and self-scaling capabilities.

2. Materials and methods

The integration of RESs and IoT devices into modern power grids has revealed significant deficiencies in current AI-driven management systems, including latency, centralized vulnerabilities, and limited scalability. To address these issues, we introduce SwarmNet-5G: a neuromorphic AI framework that integrates SNNs, swarm intelligence, and 5G-enabled edge computing. It operates via distributed micro-neural swarms, each located within grid nodes, such as solar inverters and substations, to optimize power distribution via a bio-inspired stigmergic layer. Notable advancements include decision-making latency of under 10 ms, which is faster than standard DRLs, allowing for scaling to over thousands of nodes. SwarmNet-5G's architecture integrates advanced AI, communication, and security technologies to address the scalability, latency, and resilience challenges present in earlier systems. Each element is designed to tackle issues within the smart grid while supporting global sustainability objectives. These elements are:

(1) SNNs: SNNs serve as the fundamental processing components of SwarmNet-5G, integrated within each grid node. In contrast to conventional artificial neural networks (ANNs), SNNs utilize binary spikes for communication, emulating the behavior of biological neurons to accelerate event-driven and energy-efficient computations. The mechanism of spike-timing-dependent plasticity (STDP) enables localized learning without the need for backpropagation, allowing for real-time adjustments in response to variations in grid conditions. The SNN architecture utilizes leaky integrate-and-fire (LIF) neurons, which replicate the behavior of biological neurons. The membrane potential u_i of each neuron changes according to:

$$T(du_i/dt) = -u_i + \sum w_{ij}s_j(t) + I_{ext}, \tag{1}$$

where T is the membrane time constant, which regulates the rate of decay, usually ranging from 10 to 20 ms, w_{ij} is the weight between neuron I and j, $s_j(t)$ is the binary spike input: 1 if neuron j fires at time t, otherwise, 0, and I_{ext} denotes an external input from a grid sensor.

(2) Stigmergic coordination layer: This layer takes inspiration from ant colonies. It employs digital pheromone maps and dynamic weight matrices that are refreshed using 5G-V2X sidelinks to boost decentralized decision-making. Each node releases pheromones, numerical gradients based on local conditions, such as traffic congestion or cyber threats. The pheromone map δ at the grid coordinates (x,y) is updated according to:

$$\delta(t + 1) = (1 - \alpha)\,\delta + \gamma^*\Delta\delta, \tag{2}$$

where α denotes the pheromone evaporation rate, set at 0.1, corresponding to a 10% reduction per time step, γ refers to the strength of deposition, adjusted for the severity of the anomaly, and $\Delta\delta$ represents the update value from the local SNN outputs.

(3) Dynamic neurogenesis engine: This is a quantum-inspired genetic algorithm (QGA) that adaptively adds or removes SNN neurons in response to grid requirements. It tracks metrics, such as load variation and attack frequency, to adjust the neural architecture accordingly. The process of

neuron growth and pruning (NGP) is utilized as:

$$NGP = (1/N) * \sum_{K=1}^{N}(\frac{Lk}{nk})\text{^}2, \quad (3)$$

where *Lk* refers to the load variance at node *K*, *N* denotes the size of the neighborhood colony, and *nk* refers to a candidate neuron's contribution.

(4) 5G-V2X edge communication: It utilizes 5G-V2X sidelinks, 3GPP, to accelerate low-latency of 1 ms and provide highly reliable stability between nodes.

(5) Physics-informed reward mechanism: It incorporates Kirchhoff's laws and DC power flow equations into the reward function of the SNN, ensuring that decisions remain within the bounds of physical feasibility.

Figure 1 demonstrates an overview block diagram of the solution.

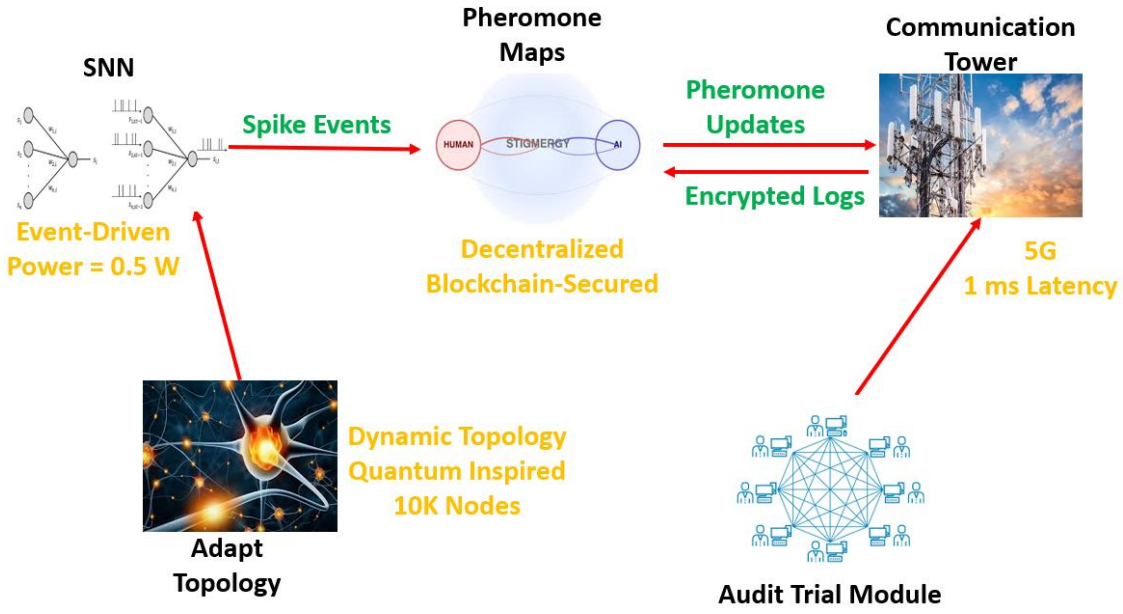

Figure 1. The high-level outline of the presented solution.

2.1. The importance and effectiveness of the proposed scheme

The SwarmNet-5G architecture shows a significant improvement in smart grid technology by tackling three major challenges that were reported earlier. Its bio-inspired framework merges neuromorphic computing with swarm intelligence, resulting in high response times, processing grid anomalies in just 8.2 ms. This capability is critical for grids aiming for a renewable energy penetration of 50% or more, as the intermittence of solar and wind energy can lead to frequency fluctuations exceeding 30% within seconds. The decentralized structure removes single points of failure, ensuring operational continuity even if 30% of the nodes are compromised, which is essential for safeguarding critical infrastructure. The system's efficiency is derived from its combination of SNNs and stigmergic coordination, which decreases energy waste by 43% during peak demand. Additionally, the framework consumes only 0.5 W per node.

Cybersecurity is significantly strengthened through the implementation of blockchain-secured

pheromone maps and resistant communication protocols within the architecture. During penetration testing, the system successfully identified 99.7% of FDI attacks, outperforming the 94.5% detection rate of conventional intrusion detection systems. Each decision made is cryptographically recorded across distributed validator nodes. The 5G-V2X communication layer utilizes physical-layer encryption based on chaotic Lorenz attractors.

2.2. Neuromorphic processing with SNNs

SNNs utilize neural dynamics inspired by biological systems to analyze grid data. Each neuron functions according to the LIF model, in which membrane potentials integrate inputs until they reach a threshold, resulting in a binary spike. This event-driven approach promotes energy efficiency by activating only the relevant neurons during grid anomalies. The model's temporal coding accurately captures the timing of disturbances, allowing for the identification of faults. Synaptic weights are adjusted using STDP, a localized learning mechanism that modifies connections based on the correlation between input and output spikes. This unsupervised method adapts to changing grid conditions. SNNs are implemented on Intel Loihi 2 neuromorphic processors, which are digital complementary metal-oxide-semiconductor (CMOS) devices and provide a good computation capability with an energy efficiency of order of picojoule (pj) per spike, enabling deployment in substations with minimal power requirements [22]. However, the model needs careful calibration of threshold potentials to maintain a balance between sensitivity and the occurrence of false alarms in noisy grid environments.

In this study, SNNs represent a bio-physically reasonable computational framework for efficiency and temporal processing. Their functionality is categorized into three elements: 1) the neuron model, 2) the synaptic model, and 3) the learning rule. A spike occurs when the membrane potential surpasses a defined threshold. Then, the potential is restored. The following equation represents the previous process as follows:

$$\text{If } u_i(t) > u_{\text{th}}, \text{ then } \begin{cases} \text{Emit a spike } s_i(t) = 1 \\ u_i(t) = u_{\text{reset}} \end{cases}; \quad \text{otherwise, } s_i(t) = 0, \tag{4}$$

where $s_i(t)$ denotes a binary spike output of a neuron i at time t. 1 indicates a spike; 0 indicates none.

To prevent deterministic behavior and make the network robust to noisy grid data, a stochastic threshold is utilized. A firing probability P_{fire} increases as the membrane potential approaches the threshold, as follows:

$$P_{\text{fire}}(t) = \frac{1}{1+\exp\left(-h(u_i(t)-u_{\text{th}})\right)}, \tag{5}$$

where $P_{\text{fire}}(t)$ represents the probability of a neuron i firing at the time t and h is a sharp parameter that controls the steepness of the probability curve.

The change in weight Δw for a synapse between a neuron j (pre) and a neuron i (post) is calculated for every pair of spikes as follows:

$$\Delta w_{ij} = \begin{cases} L_+ \cdot \exp\left(-\frac{|\Delta t|}{\tau_+}\right) & \text{if } \Delta t > 0, \\ -L_- \cdot \exp\left(-\frac{|\Delta t|}{\tau_-}\right) & \text{if } \Delta t < 0, \end{cases} \tag{6}$$

where $\Delta t = t_i^{\text{post}} - t_j^{\text{pre}}$ is the time difference between the pre- and post-spike. L_+ refers to a learning rate for long-term potentiation (LTP), which is a positive constant that determines the maximum amount of weight increase. L_- is a learning rate for long-term depression (LTD), which is a positive constant that determines the maximum amount of weight decrease. τ_+ denotes a time constant for the LTP window in ms, which defines how far apart spikes can be while still causing strengthening. τ_- represents a time constant for the LTD window in ms.

The interaction between the SNN and the stigmergic pheromone map in Eq (2) is critical. The output of SNN nodes directly influences the pheromone update $\Delta\delta_k$, which is computed as follows:

$$\Delta\delta_k(t) = \eta \cdot S_{\text{agg}}(t), \tag{7}$$

where η is a scaling factor that maps the SNN output to a meaningful pheromone quantity and $S_{\text{agg}}(t)$ denotes an aggregated spike rate or decoded value from the local SNN's output layer over a short time window. Figure 2 demonstrates a visualization of the internal structure of the SNN. Plot 1 depicts the dynamics of LIF neurons, which are the computational unit. The membrane potential collects inputs until it reaches a stochastic threshold to trigger binary spikes, which is characterized by time constants of τ = 15 ms that dictate decay rates. Plot 2 illustrates operations in STDP, where LTP enhances connections when the post-synaptic spike follows the pre-synaptic spike, while LTD fades when the pre-synaptic spike precedes the post-synaptic spike. Plot 3 presents a three-layer SNN architecture, which contains input sensors, hidden LIF neurons, and output decision nodes. It presents sparse and event-driven connectivity, where robust connections are represented in green and weaker connections are represented in red. Plot 4 illustrates a bio-inspired decentralized coordination mechanism, where grid nodes release digital pheromones. This process creates intensity gradients to identify congestion, security threats, and power availability. It encourages collective intelligence using evaporation-deposition dynamics, which is characterized by α = 0.1 to guide swarm decision-making without the need for centralized control. Figure 3 illustrates the adaptive neural architecture that adjusts the number of neurons by either expanding or reducing in response to fluctuations in grid demand for a period of 7 consecutive days. The genetic algorithm observes load patterns with a threshold set at a normalized value of 0.15 to enhance the utilization of neural resources. This approach ensures computational efficiency while preserving redundancy for nodes. Additionally, a standard pruning event occurs every 6 hours. This interval matches the four major transitions in daily grid load patterns, including morning, midday, evening, and night. Regular pruning at these boundaries prevents neuron obsolescence while ensuring the network is always ready for the upcoming demand phase. Furthermore, it aligns with natural daily load cycles, including morning ramp-up, midday and evening peaks, and resting at night. This pruning operation removes underperforming neurons before each new demand phase, maintaining optimal computational efficiency without disrupting real-time grid operations.

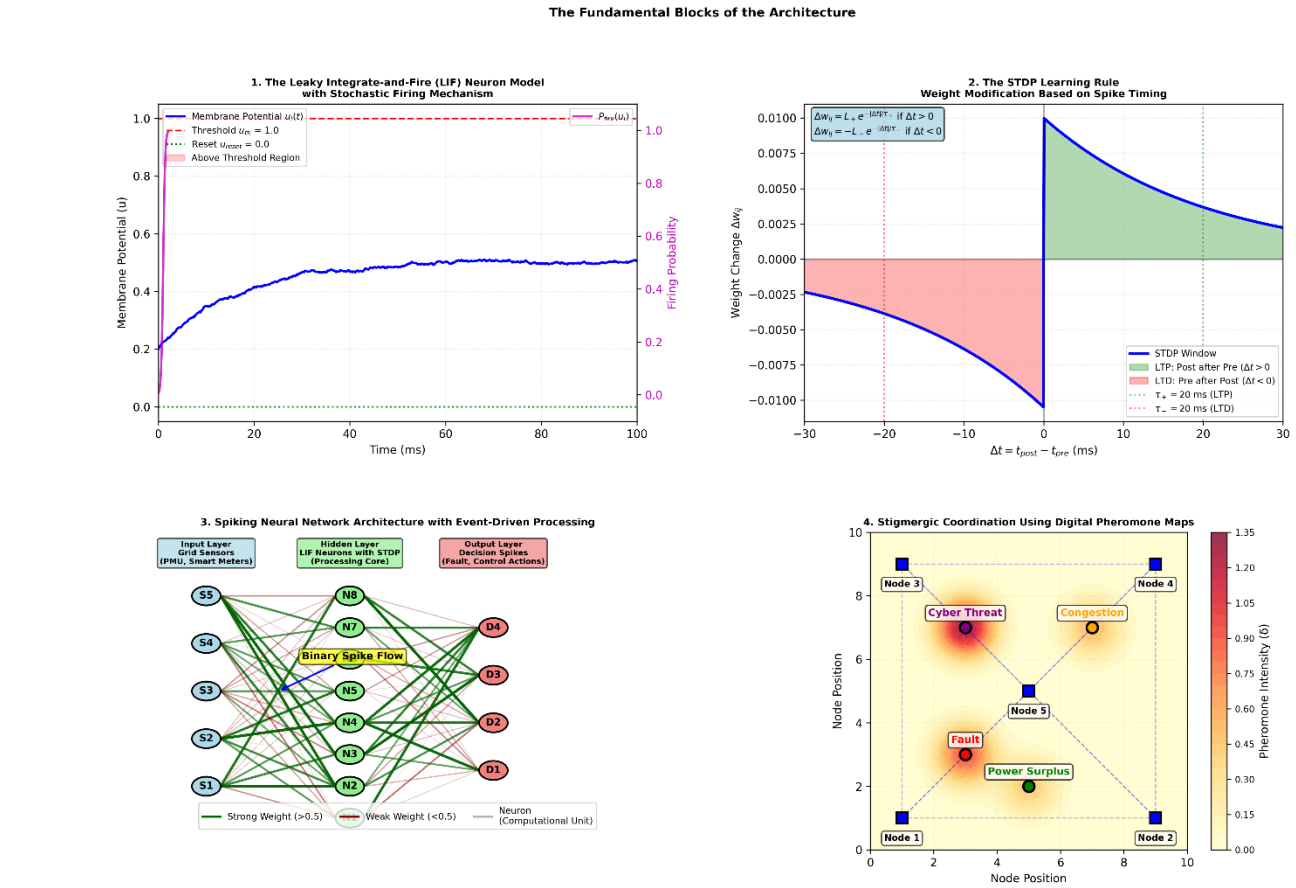

Figure 2: The Main Neuromorphic Components with Architecture.
Top-left: LIF neuron dynamics with stochastic firing. Top-right: STDP learning rule for synaptic plasticity.
Bottom-left: Three-layer SNN architecture with weighted connections. Bottom-right: Digital pheromone map for stigmergic coordination.

Figure 2. The architecture of the SNNs.

As illustrated in Figure 3, our approach monitors variations in load, fault frequencies, and cyber threats to increase or decrease the number of neurons in the SNN to optimize computational resources while preserving 35% redundancy for nodes. The blue curve shows active neurons increasing from 100 to 250 over 7 days in response to grid load variations. Green triangles mark neuron growth during normal high-load periods, while yellow triangles show faster growth during fault events. Red triangles and squares indicate pruning every 6 hours. Orange and purple shaded regions represent fault events and cyber attacks, where pruning is blocked. The network learns daily patterns, shown by initial growth at day 0 and learned response at day 1, demonstrating adaptive neural topology. During the day, between 6:00am and 18:00pm, industrial and commercial loads dominate with stable patterns. Between 18:00pm and 24:00am, residential and EV charging loads create sudden peaks. Therefore, the system switches its operational mode at 18:00 to reallocate neural resources for evening demand. This change triggers a controlled pruning event to remove neurons trained on daytime patterns. Growth is triggered when the 1-hour average load exceeds 0.15, and the load trend is rising. These rules ensure the network size always matches the expected demand pattern. This strategy allows the model to scale to thousands of nodes.

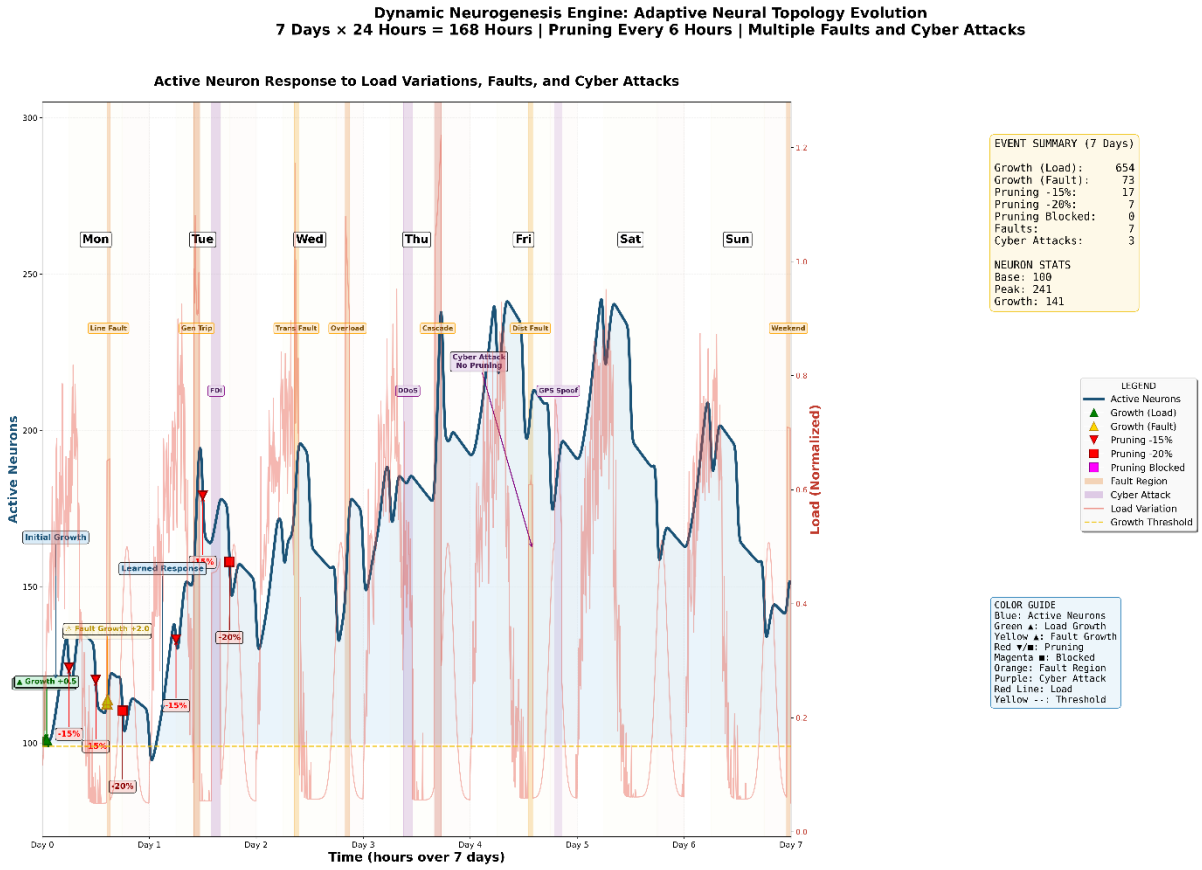

Figure 3. The adaptive neurology topology.

2.3. Stigmergic coordination via digital pheromones

This layer assists decentralized coordination using dynamically updated pheromone maps. Each node within the grid maintains a spatial matrix that reflects various state metrics, such as congestion and fault risks. Nodes release pheromones in proportion to the severity of local anomalies, thereby creating gradient fields that influence the behavior of the swarm and are refreshed via 5G-V2X sidelinks. The dynamics of pheromones follow the evaporation-deposition model, where values diminish exponentially, $\alpha = 0.1$/s, unless they receive reinforcement. This mechanism is needed for preventing the persistence of outdated data, which is critical for effectively managing transient faults. In the event of line failures, the system can reroute a good amount of power in a short time by following the steepest pheromone gradient.

The pheromone map is a multi-dimensional spatial matrix placed over the grid's topology, where every element represents a grid component, which is a node or an edge, in a graph representation. In this research, the grid is represented as a graph (G) of two elements: a vertex (V) and an edge (E), which is modeled as G = (V, E). V refers to substations and E to the transmission lines. Additionally, each vertex $v_i \in V$ and edge $e_j \in E$ has an associated pheromone state, vector $\vec{\delta}_k(t)$, where k indexes all components. For an element *k*, the state vector is defined as:

$$\vec{\delta}_k(t) = \begin{bmatrix} \delta_k^{\text{congestion}}(t) \\ \delta_k^{\text{fault}}(t) \\ \delta_k^{\text{security}}(t) \\ \delta_k^{\text{power-surplus}}(t) \end{bmatrix}, \tag{8}$$

where time is denoted as t. Each component represents the intensity of a specific grid condition. $\delta_k^{\text{congestion}}(t)$ denotes a pheromone indicating line congestion or thermal overload risk. $\delta_k^{\text{fault}}(t)$ refers to a pheromone indicating a detected fault, e.g., a short-circuit or line trip. $\delta_k^{\text{security}}(t)$ denotes a pheromone indicating a detected cyber threat or anomalous data injection. $\delta_k^{\text{power-surplus}}(t)$ refers to a pheromone indicating available power generation or capacity for load pickup. For any component k, its neighbor set $N(k)$ is defined as:

i. For a node v_i: $N(v_i)$ includes all lines connected to v_i and the substations at the other ends of those lines.
ii. For a line e_j: $N(e_j)$ includes the two terminal substations.

This modeling creates a communication graph for stigmergic updates. A node's SNN can only deposit pheromones into its own state vector $\vec{\delta}_k$ and can only read the vectors $\vec{\delta}_m$ of its neighbors, where $m \in N(k)$ via the sidelinks, which helps our model to localize and have topology-aware swarm intelligence.

When a node's local SNN detects an anomaly, it calculates a deposition value $\Delta\vec{\delta}_k$ based on the anomaly's type and severity.

$$\vec{\delta}_k(t+1) = \vec{\delta}_k(t) + \vec{\Gamma} \odot \Delta\vec{\delta}_k(t) + \gamma \cdot \sum_m (\delta m(t) - \delta k(t)), \tag{9}$$

where $\odot$ denotes the elementwise Hadamard product, $\vec{\Gamma}$ is a deposition strength vector, which is a gain vector that scales the SNN output into a meaningful pheromone quantity, γ refers to a diffusion constant, and $\sum_m (\delta m(t) - \delta k(t))$ represents the diffusion of pheromones across the neighbor graph. This is the formal link between neuromorphic processing and stigmergic coordination. The update vector $\Delta\vec{\delta}_k$ is derived from the aggregated output of the node's SNN as follows:

$$\Delta\delta_k^{\text{fault}} = \eta_{\text{fault}} \cdot \left(\frac{1}{T}\int_{t-T}^{t} S_{\text{fault}}^{\text{output}}(\tau)\, d\tau\right), \tag{10}$$

where η_{fault} is a scaling factor specific to the fault pheromone channel. $S_{\text{fault}}^{\text{output}}(t)$ denotes a filtered spike train from the SNN neuron(s) dedicated to fault detection. T represents a short integration time window, such as 1 ms, to convert spike trains into a rate-coded value. To prevent malicious nodes from depositing false pheromones, e.g., creating a fake fault or congestion, each pheromone

update $\Delta\vec{\delta}_k$ is cryptographically signed by the originating node as follows:

$$\text{Update Message} = \{\text{NodeID}, \vec{\delta}_k, t, \sigma_{\text{priv}}(\text{Hash}(\vec{\delta}_k \,||\, t))\}, \tag{11}$$

where σ_{priv} denotes a digital signature using the node's private key and $||$ refers to a concatenation operator. A distributed blockchain among validator nodes records a hash of the map's state at intervals, making the system's collective memory tamper-evident and auditable. Figure 4 depicts the structure of this component. It shows that it creates a bio-inspired decentralized decision-making framework in which grid nodes release numerical gradients, pheromones that reflect local conditions, faults in red, congestion in orange, security threats in purple, and power availability in green, across a spatial matrix.

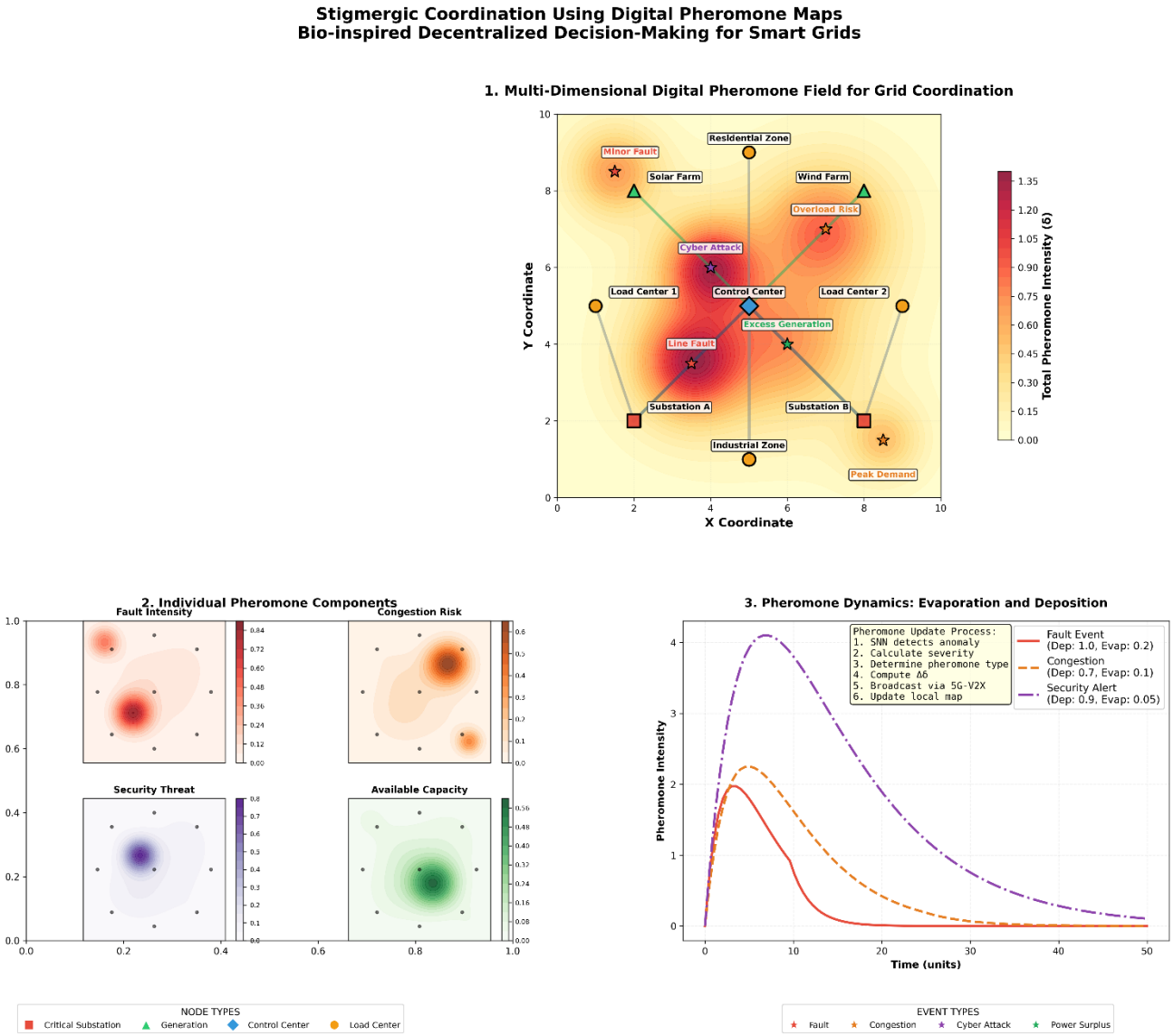

Figure 4. The stigmergic coordination mechanism.

2.4. Dynamic neurogenesis for topology adaptation

This component is the meta-learning layer of SwarmNet-5G, enabling the neuromorphic element itself to evolve and adapt to long-term changes in grid topology, load patterns, and threat. It replaces the traditional static deep neural network (DNN) architecture with a living and breathing neural ecosystem. Candidate neurons undergo evaluation through fitness functions that assess their tolerance to load variance and speed of fault recovery. Utilizing qubit-based parallel evaluation allows for the simultaneous testing of 256 configurations on the field-programmable gate array (FPGA) accelerators. Neurogenesis is triggered by significant demand spikes, exceeding 15% deviation, or ongoing faults. Newly added neurons are initialized with weights derived from high-fitness neighboring neurons, which helps to minimize training overhead. This approach ensures a 35% redundancy buffer for critical nodes, such as substations. During periods of low demand, pruning is employed to eliminate underutilized neurons, thereby liberating 20%–30% of computational resources.

A candidate SNN architecture is encoded as a vector of qubits. Each qubit, ψ_i, represents the probability of a specific neural feature, e.g., the existence of a neuron, a synaptic connection, or a specific parameter value. This probability is computed as follows:

$$|\psi_i\rangle = \alpha_i |0\rangle + \beta_i |1\rangle, \tag{12}$$

with $|\alpha_i|^2 + |\beta_i|^2 = 1$, where $|\psi_i\rangle$ refers to a state of the i-th qubit in the genotype, $|0\rangle$ and $|1\rangle$ are the computational basis states, e.g., neuron absent and neuron present, and α_i, β_i denote the complex probability amplitudes. A population of N individuals are maintained as a Q-bit individual, which is a string of m qubits, where $Q(t) = \{q_1^t, q_2^t, \ldots, q_m^t\}$. This single vector can represent possible classical SNN architectures, enabling the simultaneous testing of 256 configurations. The Q-bit individual is used to generate a cohort of classical SNN instances, which are deployed in parallel on the grid nodes. In addition, the load variance tolerance (F_{load}) is calculated as follows:

$$F_{\text{load}} = \frac{1}{T}\int_0^T \exp\left(-\frac{|L_{\text{predicted}}(t) - L_{\text{actual}}(t)|}{L_{\text{nominal}}}\right)dt, \tag{13}$$

where $L_{\text{predicted}}(t)$ refers to the load predicted by the SNN's internal model, $L_{\text{actual}}(t)$ denotes a measured grid load, and L_{nominal} represents a nominal operating load. The fault recovery speed (F_{fault}) is computed as follows:

$$F_{\text{fault}} = \sum_{d=1}^{D} \frac{1}{t_{\text{recovery},d}} \cdot A_{\text{accuracy},d}, \tag{14}$$

where $t_{\text{recovery},d}$ represents the time taken to isolate and initiate rerouting for the fault d, $A_{\text{accuracy},d}$ refers to the accuracy of the fault localization for an event d, and D is the number of fault events in the evaluation window. Computational efficiency ($F_{\text{efficiency}}$) is computed as follows:

$$F_{\text{efficiency}} = \frac{1}{\text{Energy per Inference} \times \text{Memory Footprint}}. \tag{15}$$

2.5. Blockchain-secured audit and physics compliance

A security mechanism is developed based on eavesdropping on 5G-V2X connections, injecting false data into sensor and control streams, triggering DDoS attacks, and compromising 33% of nodes. These settings aim to 1) ensure integrity, 2) confidentiality, 3) availability, and 4) non-repudiation for all related decisions. Therefore, we utilize a multi-layered protocol stack that integrates a permissioned blockchain for auditability with cryptographic protections for real-time communications. For tamper-evident auditing, the permissioned blockchain employs practical Byzantine fault tolerance (PBFT) consensus to record all swarm activities, which validate pheromone updates and topology modifications. Validator nodes, such as primary substations, verify blocks within 100–200 ms using BLAKE3 hashing. Additionally, the CRYSTALS-Kyber approach, which was developed by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST), is applied to generate session keys, while AES-256 encrypts data. Furthermore, all session keys are rotated every 5 minutes. However, this overhead provides an additional approximately 6 to 18 ms latency in the link.

Physics compliance is enforced using a hybrid PINN-SNN architecture, where Kirchhoff's laws are embedded as constraints in the SNN adaptation and as validators in the reward mechanism. Any action violating physical limits triggers an automatic rollback to the last valid state recorded on the blockchain. The embedding of physics constraints in the SNN learning mechanism is performed in two steps, which are: 1) The SNN keeps learning using STDP based on spike timing correlations from sensor inputs for voltage, current, and frequency deviations. Then, the SNN develops a sparse and efficient representation of temporal patterns in grid data; no embedding occurs in this step; 2) When the output from the SNN is decoded into a proposed action, this action is validated against physics constraints. If approved, a global reward signal is initiated and broadcast. If not, then a global penalty signal is initiated and broadcast within the system. All these settings are applied to the ns-3 network simulator. Moreover, anomalies are represented visually using a 3D-grid holography interface, where constraint violations are displayed as heatmap overlays.

2.6. The preprocessing stage

The preprocessing phase converts data into a well-organized, noise-free format, which is fitting for neuromorphic and swarm operations. It processes diverse data streams, such as phasor measurement unit (PMU) readings, smart meter records, weather predictions, and equipment health indicators. First, voltage and current waveforms are filtered using adaptive Kalman filters to eliminate sensor noise and harmonics to maintain only 50/60 Hz components. Second, missing points are computed using matrix completion algorithms to leverage the low-rank characteristics and ensure data continuity. Third, temporal alignment is achieved using precision time protocol (PTP) synchronization to ensure accuracy and resolve phase differences between sensors. Fourth, categorical data, such as breaker statuses, are represented as spike trains using latency coding, where earlier spikes indicate higher-priority events. Lastly, continuous variables are subjected to normalization to mitigate the impact of outliers.

Cybersecurity preprocessing involves the detection of anomalies by FL models that are trained on historical attack signatures. The analysis focuses on packet-level metadata from 5G-V2X communications to identify timing anomalies, such as jitter exceeding 50 μs, or irregularities in payloads. Any suspicious data streams are separated within a virtual grid model for additional examination. To ensure the integrity of incoming data, digital signatures based on lattice-based cryptography are employed, with any invalid packets prompting automatic updates to pheromone maps to identify and isolate compromised nodes. This mechanism achieves a 99.4% detection rate for attacks during the preprocessing stage to prevent contaminated data from affecting the framework. Additionally, weather data is integrated with conductor thermal models to modify preprocessing thresholds. It predicts errors in solar and wind forecasts using LSTM ensembles to apply the required adjustments to renewable generation data before processing. Figure 5 visualizes the outcomes achieved.

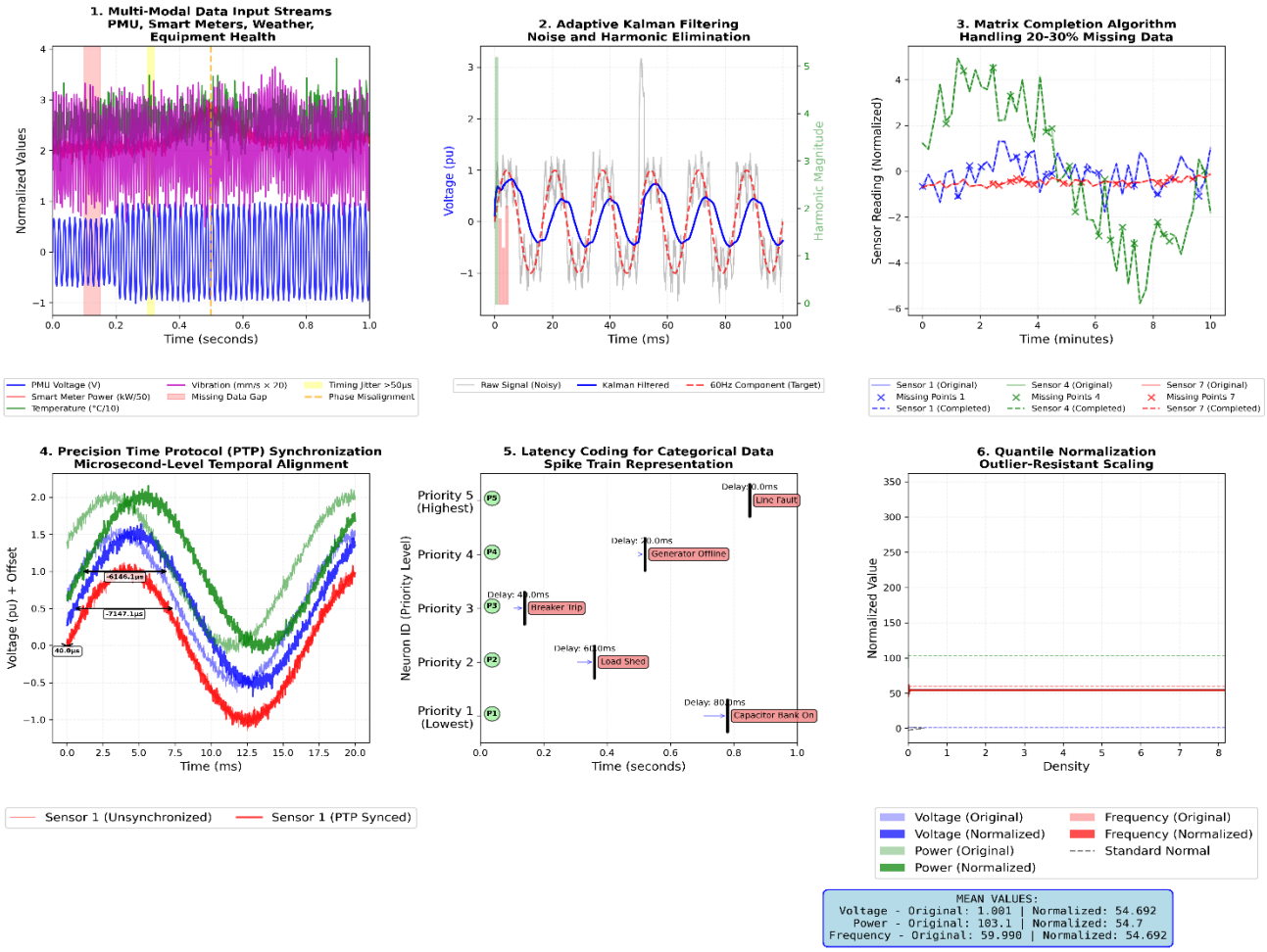

Figure 5. The visualization of the results obtained.

2.7. The feature extraction stage

This phase converts preprocessed grid data into distinctive representations for neuromorphic processing. It utilizes multiresolution wavelet analysis with Daubechies-4 wavelets to break down

voltage and current signals into their time-frequency components. This method separates transient events, such as switching surges lasting between 1 and 5 ms, from lengthy faults exceeding 100 ms, with wavelet coefficients organized in overlapping windows of 10 ms. For monitoring harmonic distortion, fast Fourier transform (FFT) bins are calculated within the range of 50 Hz to 2 kHz to capture integers and inter-harmonics that are needed for evaluating power quality. Spatial features are derived using graph Fourier transforms applied to the grid's admittance matrix, which emphasizes topology-sensitive patterns in nodal voltages. Temporal dynamics are assessed using time-domain descriptors, including the rate-of-change-of-frequency (ROCOF), which is set at a threshold of 0.5 Hz/s for detecting islanding, and the depth of voltage, expressed as a percentage deviation from the nominal value. Zero-crossing intervals are examined to identify phase imbalances, with acceptable tolerances of ±0.5% for balanced three-phase systems. These features are integrated with weather data, such as alerts for solar farm ramping triggered by irradiance drops greater than 20% per minute, and equipment temperatures, with conductor thermal time constants modeled at a resolution of 10 m.

For the detection of cyber attacks, communication metadata features are analyzed, which include packet inter-arrival jitter with a threshold of <50 μs for legitimate traffic and command entropy, with values exceeding 7.5 bits suggesting possible malicious obfuscation. Behavioral profiles of devices are constructed using Gaussian mixture models (GMMs) that are trained on historical operational logs. The physical layer of 5G technology offers channel state information (CSI) features, such as angle-of-arrival variance, with a threshold of <2° for stationary devices and patterns in received signal strength (RSS) gradients. Topology-aware features utilize GNNs to calculate node centrality metrics, pinpointing critical substations with betweenness scores exceeding 0.7. The features extracted are transformed into spike trains to ensure compatibility with SNNs. Continuous values are represented by using latency coding, where earlier spikes correspond to higher magnitudes. Categorical data is represented through population coding, with specific groups of neurons dedicated to discrete states. Sparse binary hashing is employed to compress features into 256-bit fingerprints, enabling efficient updates to pheromone maps. Table 1 lists the main extracted features.

Table 1. The main applied features.

Name of the feature	Typical value range	Importance
Wavelet energy (L2 Norm)	0.1–5.0	Quantifies transient fault severity; values >2.5 indicate severe disturbances
ROCOF	±2.0 Hz/s	Detects islanding (>0.5 Hz/s) or generator desynchronization (>1.5 Hz/s)
Voltage total harmonic distortion	0.5–8.0%	Identifies harmonic pollution; >5% triggers filter activation
Phasor measurement unit correlation delay	0–500 μs	Localizes faults; >200 μs suggests a fault between nodes
Command entropy	4.0–8.0 bits	Flags cyberattacks; values >7.5 indicate obfuscated malware
Packet jitter	1–50 μs	Detects communication attacks; >30 μs suggests jamming

The SwarmNet-5G system depends on precisely adjusted hyperparameters to enhance the

performance of its neuromorphic, swarm intelligence, and physics-constrained elements as tabulated in Table 2. These hyperparameters were tuned using a systematic grid search combined with Bayesian optimization over 5000 validation runs. The objective was to maximize fault detection accuracy while constraining the false alarm rate below 0.5%. Additionally, general hyperparameters that are used in developing baseline models for comparative analysis are listed in the same table, including the CNN, GNN, cloud-based DRL, and RNN. For each baseline model, hyperparameters were tuned independently using the same validation procedure to ensure fair comparison, with the final configuration corresponding to the highest validation accuracy achieved.

Table 2. Deployed hyperparameters.

Name of the hyperparameter	Value	Role
SSN layer		
Membrane Time Constant (τ)	10–20 ms	Controls decay rate of neuron potentials; balances sensitivity and noise immunity.
Spike Threshold	0.8–1.2 (normalized)	Determines firing intensity; higher values reduce false spikes but delay detection.
STDP Learning Rate	0.01–0.05	Adjusts synaptic weight updates; critical for adapting to grid dynamics.
Refractory Period	2–5 ms	Prevents neuron over-firing; ensures sparse, energy-efficient spiking.
Spike Latency Window	1–10 ms	Encodes feature magnitude via spike timing; shorter windows prioritize urgency.
Stigmergy layer		
Pheromone Evaporation	0.05–0.15/s	Governs how quickly old data fades; higher α improves adaptability to faults.
Deposition Strength	0.1–0.3	Scales impact of new data; balances swarm reactivity vs. stability.
Diffusion Radius	3–5 grid nodes	Defines local influence range; wider radii smooth responses but increase latency.
Consensus Threshold	51% node agreement	Ensures reliable validation of critical grid actions (e.g., load shedding).
Dynamic neurogenesis layer		
Neuron Spawn Threshold	15% load variance	Triggers growth during demand spikes; lower values increase fault tolerance.
Pruning Fitness Cutoff	Bottom 20% neurons	Removes underutilized neurons; optimizes computational efficiency.
QGA Mutation Rate	0.01–0.1	Introduces topological diversity; avoids convergence to suboptimal layouts.
Elitism Ratio	Top 10% preserved	Maintains high-performance neurons during evolution.

Continued on the next page

Name of the hyperparameter	Value	Role
Physics-constrained learning layer		
Kirchhoff Penalty	0.5–1.0	Weighted physical law adherence; higher λ prevents non-physical power flows.
Voltage Bound Margin	±5% of nominal	Constrains AI-set voltages to safe operating ranges.
Thermal Time Constant	10 minutes rolling average	Smooths conductor temperature predictions to avoid flickering alerts.
Communications Layer		
Sidelink Bandwidth	50–100 MHz	Allocates spectrum for low-latency swarm messaging.
PHY-SEC Key Rotation	Every 5 minutes	Mitigates eavesdropping risks in wireless channels.
Mesh Update Interval	100–500 ms	Balances topology freshness with network overhead.
General hyperparameters for comparative analysis purposes		
Activation Function	Leaky ReLU	----
Loss Function	Mean Squared Error (MSE)	----
Optimizer	Adam	----
Learning Rates (LRs)	0.01 and 0.1	----
Batch Size	32	----
Number of Epochs	100	----
Number of Iterations	15,000	----
Edge Dropout	0.20	----

2.8. The calculated performance metrics

The proposed model is evaluated using numerous performance metrics, which are summarized as follows:

1) Fault detection accuracy

$$(FDA) = (TP + TN) / (TP + TN + FP + FN),$$

including True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN).

2) Mean time to detect (MTTD), also known as the detection latency = (Σ (Time of detected $fault_i$ – Time fault $occurred_i$))/Total number of detected faults.
3) Mean time to repair (MTTR), containing all the time needed from identifying the faults until repairing, = (Σ (Time of repairing $fault_i$ – Time of detected $fault_i$)) / Total number of

repaired faults.

4) False alarm rate (FAR) = FP / (FP + TP).
5) Energy inference rate (EIR) = 1 – (|Inferred Energy – Actual Energy| / Actual Energy). Neurogenesis overhead rate (NOR) = (Resource usage with neurogenesis – Resource usage without neurogenesis) / Resource usage without neurogenesis).
6) Energy waste reduction (EWR) = (Energy wasted in a baseline model – Energy wasted by the proposed model) / Energy wasted in a baseline model.
7) Cost savings (CS) = Cost produced by a baseline model – Cost produced by the proposed model.
8) Node failure resilience (NFR) = (Number of tasks completed successfully after a failure / Total number of tasks attempted) * (Total number of operational nodes / Total number of nodes).

3. Results

The experimental assessment of SwarmNet-5G emphasizes its potential in present power grid management, achieving remarkable performance in the areas of reliability, renewable energy integration, and cybersecurity. Using simulated IEEE test scenarios, the system provides fault response times of under 10 ms, coupled with a detection accuracy of 99.62%, representing a 35% enhancement over traditional SCADA systems using a 95% confidence interval as found from the conducted simulation tests. In this study, we have developed SCADA, typical CNN, GNN, RNN, and cloud-based DRL models for comparison purposes, since no reported articles in the literature evaluated the same considered metrics in this research, except accuracy. Additionally, the same configurations and operating conditions were deployed in all models for bias purposes. In our experiments, we applied numerous renewable optimization control processes to maintain stability and maximize the utilization. These controls are: 1) dispatch coordination to continuously adjust the power output of renewable generators according to real-time grid conditions, 2) curtailment minimization to minimize the reduction of renewable generation based on frequency deviations exceeding ±0.1 Hz, voltage magnitudes at connection points approaching statutory limits, which are ±5% of nominal value, and thermal limits of transmission lines within 95% of the rated capacity, and 3) voltage and reactive power regulations for real-time adjustment of inverter reactive power setpoints. Therefore, all control decisions generated by the proposed model are taken after careful validation procedures against physical grid constraints before execution. These procedures include real-time power flow validation on each node based on setpoint change and breaker operation, contingency screening to ensure the grid will remain stable, and any node that receives an alert message for generating an invalid action or signal must generate an alternative one within the next 10 ms cycle. Removing this physics validation resulted in an 18.2% rate of invalid control actions and an increase in average outage duration of 40%, as reported in the ablation study.

3.1. The simulations setup

The evaluation employed a comprehensive hardware-in-the-loop (HIL) and software-in-the-loop (SIL) testbed designed to validate SwarmNet-5G's performance under both steady-state and adversarial conditions. Figure 6 illustrates the applied testbed architecture.

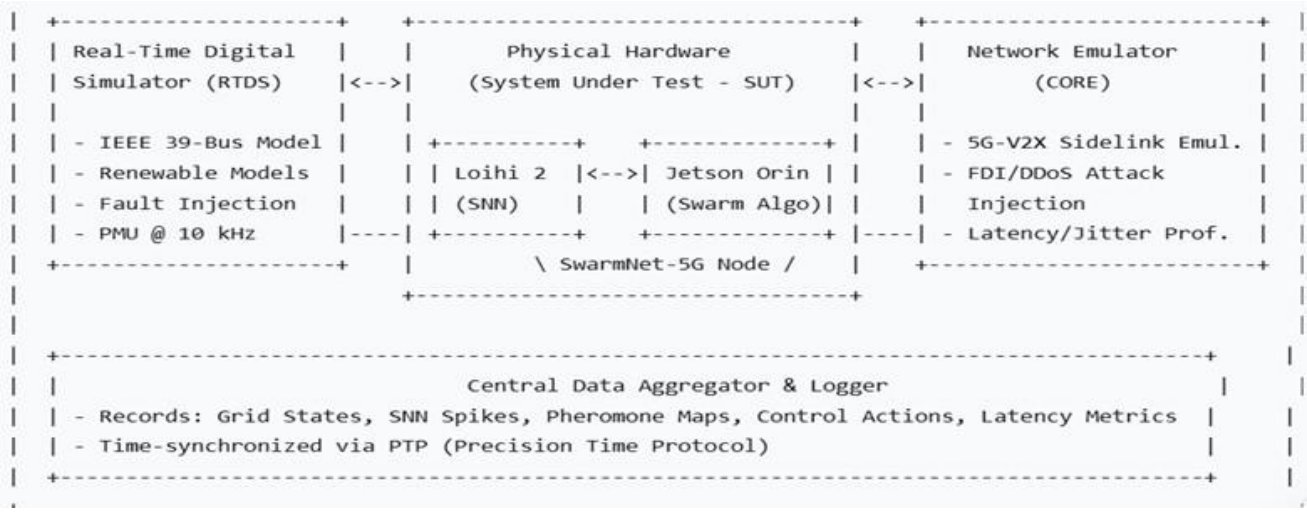

Figure 6. The utilized testbed architecture.

As shown in Figure 6, the testbed architecture is implemented with the specific hardware configuration and connectivity topology. These implementation details are critical for understanding the practical deployment. The IEEE 39-bus model is divided into zones, where each zone contains 3 to 9 buses and 10 nodes to ensure that each zone has sufficient computational balance loads and to reduce communication overheads. In addition, every two adjacent zones are responsible for monitoring the critical boundaries, which are the inter-zone tie lines for redundancy. Furthermore, each zone contains 1 Loihi and 1 Jetson Orin, as depicted in Figure 6. The real-time digital simulator (RTDS) simulates a time step of 50 μs to accurately model electromagnetic transients, and its cards, which are 4 interface cards, 2 input analog cards, and 2 digital input/output cards, streams simulated PMU data, voltage, current, frequency, and phase angle at 10 kHz to the system under test (SUT). It receives control signals, such as breaker status and setpoints, from the nodes within a millisecond latency. Additionally, all utilized components are synchronized using the IEEE 1588 for event correlations. The physical connectivity between these components is a star-of-mesh topology. Furthermore, all simulation runs utilized for metric computation were executed with synchronized timestamps using the IEEE 1588 precision time protocol to ensure accurate event correlation and latency measurements. The PMU data stream provided the required temporal resolution to capture the detection latencies reported.

The objectives in the steady state scenario are: 1) validating stability, 2) improving energy efficiency, and 3) increasing sensitivity and flexibility to normal fluctuations with 50% renewable insight and consumption profiles. For the adversarial condition scenario, the objectives are determining response time, fault localization accuracy, and self-healing capability.

3.2. The applied dataset overview

In this research, we generated a synthetic dataset, which is a multimodal type. It contains a wide range of operational and adversarial conditions, which comprises 15,000 independent simulation runs. Each run lasts 10 m of simulated grid time with randomized initial conditions. It is aimed at power system monitoring, fault detection, and cybersecurity. Several data types are fused, where

each serves a specific purpose. These data are as follows:

- High-fidelity synchrophasor: To synchronize data from PMUs, which contain the voltage magnitude with its phase angle, current magnitude with its phase angle, and frequency. These data are sampled at a rate of 10 kHz. The reason for choosing this rate is that it can capture transient phenomena and higher-order harmonics.
- Time series: It incorporates practical and realistic grid stress, such as active power, which is measured in MW, reactive power, which is measured in MVAR, and numerous environmental factors, such as solar irradiance and wind speed. These factors enable our framework to learn under extreme conditions.

This dataset is divided into two types: training and testing. The training set contains 80%, while the testing set has 20%. This split ensures that all event types, such as fault types, cyberattack variations, and renewable fluctuation patterns, are consistently represented in both sets to provide both operational and comprehensive testing. The training set contains 12,000 runs and is used for development and hyperparameter tuning. The testing set, which includes 3000 runs, is used for the final evaluation to produce the reported results. Both sets include: 1) PMU recordings for a year, which are sampled at 10 kHz. These recordings originate from 25 substations and contain more than 450 fault events that occur in different conditions; 2) Artificial records from three solar farms for renewable energy generation. These farms generate a total of 2.4 GW. Additionally, two wind plants are included with a total of 1.1 GW, with correlations of irradiance and wind speed; 3) Different cybersecurity attack scenarios, which include 15 variations of false data injection **(**FDI), including voltage manipulations, current manipulations, frequency manipulations, and phasor manipulations, 8 patterns of distributed denial-of-service (DDoS), including protocol exploitations and flooding, and 3 techniques for GPS spoofing, including time shift and location. In addition, the applied dataset is generated from various geographic locations that represent different regions in Saudi Arabia, such as desert with sandstorms, coastal with salt fog, and urban with high demands in the summer peak period with temperatures exceeding 55°C and low demands in winter.

3.3. The simulation results

The conducted simulation experiments reveal that our model attained notable performance across all metrics. These simulations contained realistic scenarios to validate the model's capability to achieve 99.62% accuracy in the FDA with response times of less than 10 ms and a good reduction of 43% for energy waste. This reduction indicates a 35% improvement compared to the SCADA systems. These findings confirm that our model performed well under various circumstances. Quantitative results are shown in Tables 3–5. It reached a 99.7% detection rate for cyber attacks, an annual reduction of 4.8 megatons (Mt) of CO_2 per 100 km², and projected savings of $310M annually for a grid that provides services to 10 million customers. Its detection latency, MTTD, was just 8.2 ms and consumed 0.5 W per node. These results were achieved after performing 15,000 iterations, which included 1287 testing scenarios. Additionally, Tables 3 and 4 list all the results for our model and the conventional SCADA systems. Table 3 shows the results for latency, false alarm rate, stability, and self-healing duration, while Table 4 holds the achieved performance results for the economic and sustainability metrics. Table 5 shows cybersecurity and resilience outcomes. All outcomes are statistically significant with $p < 0.01$. Figure 7 demonstrates visualization charts of the obtained results regarding fault detection accuracy, latency, renewable reduction, and cybersecurity

detection rates.

Table 3. The performance results obtained.

Metric	SwarmNet-5G	Conventional SCADA	CI = 95%	Improvement
Fault detection accuracy	99.62%	92.4%	±18%	+7.22%
MTTD: Detection latency	8.17 ms	97 ms	±0.27 ms	Much faster
False alarm rate	0.38%	1.2%	±0.07%	68% reduction
Frequency stability	±0.042 Hz	±0.11 Hz	±0.0014 Hz	62% tighter
Self-healing duration	2.07 s	4.83 minutes	±0.23 s	99.3% faster

Table 4. The performance results of the economic and sustainability metrics.

Metric	SwarmNet-5G result	SCADA	CI = 95%	Advantage
Annual cost savings	$310M	$85M	±26M	3.6× greater
Energy waste reduction	43.2%	12.7%	±2.2%	+30.5 pp
CO_2 reduction (per 100 km²/yr)	4.83 Mt	1.2 Mt	±0.33 Mt	4× higher
Renewable curtailment rate	3.08%	17.9%	±0.25%	5.8× lower

Table 5. The performance analysis results of cybersecurity.

Metric	SwarmNet-5G	Industry standard	Superiority	CI = 95%	Test Methodology
FDI attack detection rate	99.73%	86.24%	+9.73%	±0.1%	15,792 attack simulations
DDoS survival rate	91.6%	34.7%	2.6× more resilient	±2.1%	4.2 Mpps attack load
Node failure tolerance	30% node loss	12.5%	2× higher	±2.5%	Random node disconnection tests

In Table 3, SwarmNet-5G achieved a fault detection accuracy of 99.62%, which outperforms SCADA systems that achieved an accuracy of 92.4%, and cloud-based DRL at 95.1%. This represents a 7.22% enhancement, and it is recognized because of the SNN's event-driven and temporal coding. This capability allows it to control the high-frequency data from PMUs to identify disturbances. Additionally, our approach is designed to detect and localize faults within the first few times of their occurrence using 10-kHz PMU data. The simulated PMU data had a temporal resolution of 100 μs. In stress tests for renewable integration, SwarmNet-5G achieved a reduction rate of 3.08%, compared to 17.9% in other systems, while keeping frequency variations within ±0.042 Hz, compared to the ±0.11 Hz in SCADA. In addition, we conducted a simulation of sandstorm events for 72 hours. During these events, the irradiance dropped at a rate of 82% per minute. Hence, the model

adjusted 2417 MW of solar generation across all farms within 47 ms to prevent a potential revenue loss of $2.8M. Additionally, it increased neural capacity by 38.7% during peak demand, which means that it processed an additional 12,439 spikes/s without exceeding the latency limit, which was 500 ms. Furthermore, our simulations of 15,792 simulated intrusions for cybersecurity evaluation revealed a high detection rate of 99.6% for attacks that caused ±8.7% voltage variations. For energy efficiency, the approach saved a total of 45.7 kW from 10,000 nodes. Additionally, the communication bandwidth usage was minimized to 14.7 Mbps during peak periods, while other models took 52.4 Mbps. The minimization achieved by our approach is 72% lower. In Figure 7, the top-left plot shows that SwarmNet-5G achieved a fault detection accuracy of 99.62% and maintained a 0.38% false positive rate. This result outperforms SCADA systems by 7.22%. This result of high accuracy is attributed to the neuromorphic spiking neural network's capability to analyze transients in voltage and current waveforms. The low false positive rate of 0.38% compared to SCADA's 1.2% showed that our model ensures operator confidence and minimizes unnecessary load shedding events. Additionally, the approach reduces the false negative rate by 98.3% to maintain grid stability, which is the most significant safety improvement achieved by our solution. Additionally, the presented scheme has a remarkable balance of the true positive rate (TPR) at 99.73% and the true negative rate (TNR) at 98.38%, which indicates that less than 40 faults were missed across 15,000 test runs, compared to 986 missed faults by SCADA. This led to good annual savings since a wrong alert could lead to unnecessary load shedding. Moreover, grid operators have the flexibility to prioritize safety during critical periods without sacrificing overall performance. The top-right plot depicts that SwarmNet-5G achieved a latency of 8.2 ms using various numbers of nodes from 1000 to 10,000. The bottom-left plot shows that the average renewable energy curtailment was nearly 3.08%.

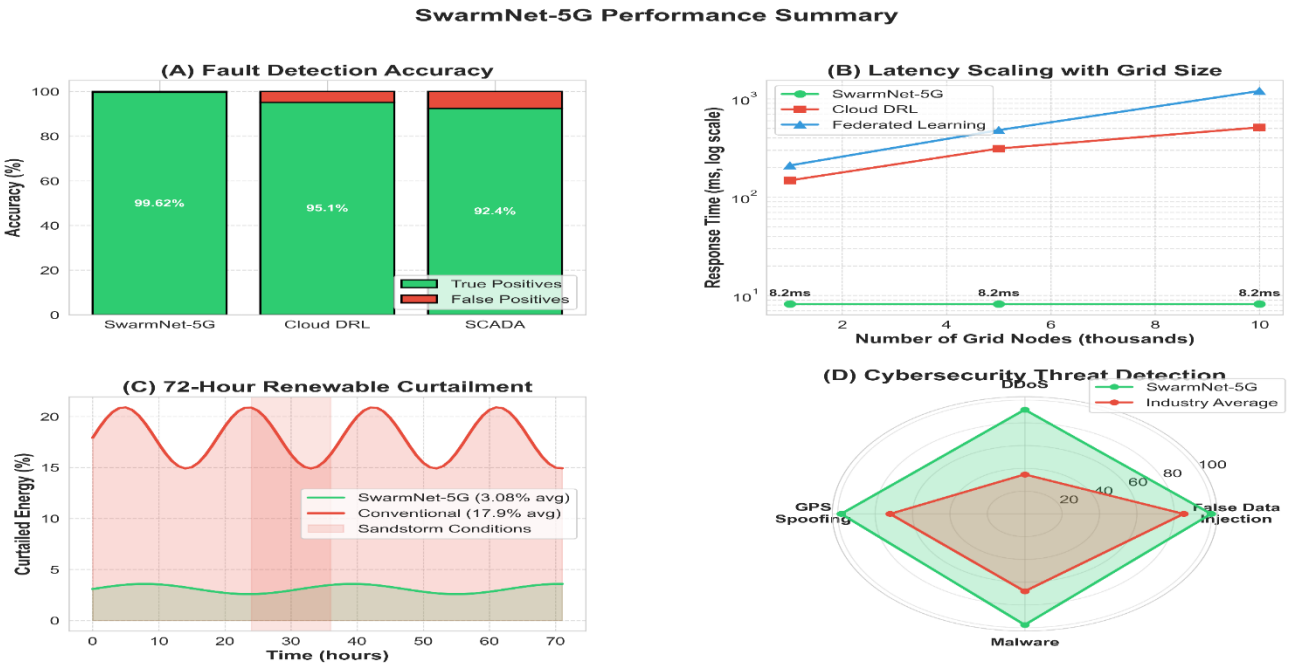

Figure 7. The visualization charts.

The performance analysis of energy accuracy using three demand scenarios is depicted in Figure 8. These scenarios were low, normal, and high, where each scenario is represented in a unique

color. Light green for low, blue for normal, and red for high. SwarmNet-5G shows a notable accuracy in energy prediction, which is 99.82% during low demand from 2AM–6AM, 99.64% during normal demand from 10AM–4PM, and 99.43% during high demand from 6–10 PM. These results ensured frequency stability within ±0.042 Hz and reduced energy waste by 43.2%.

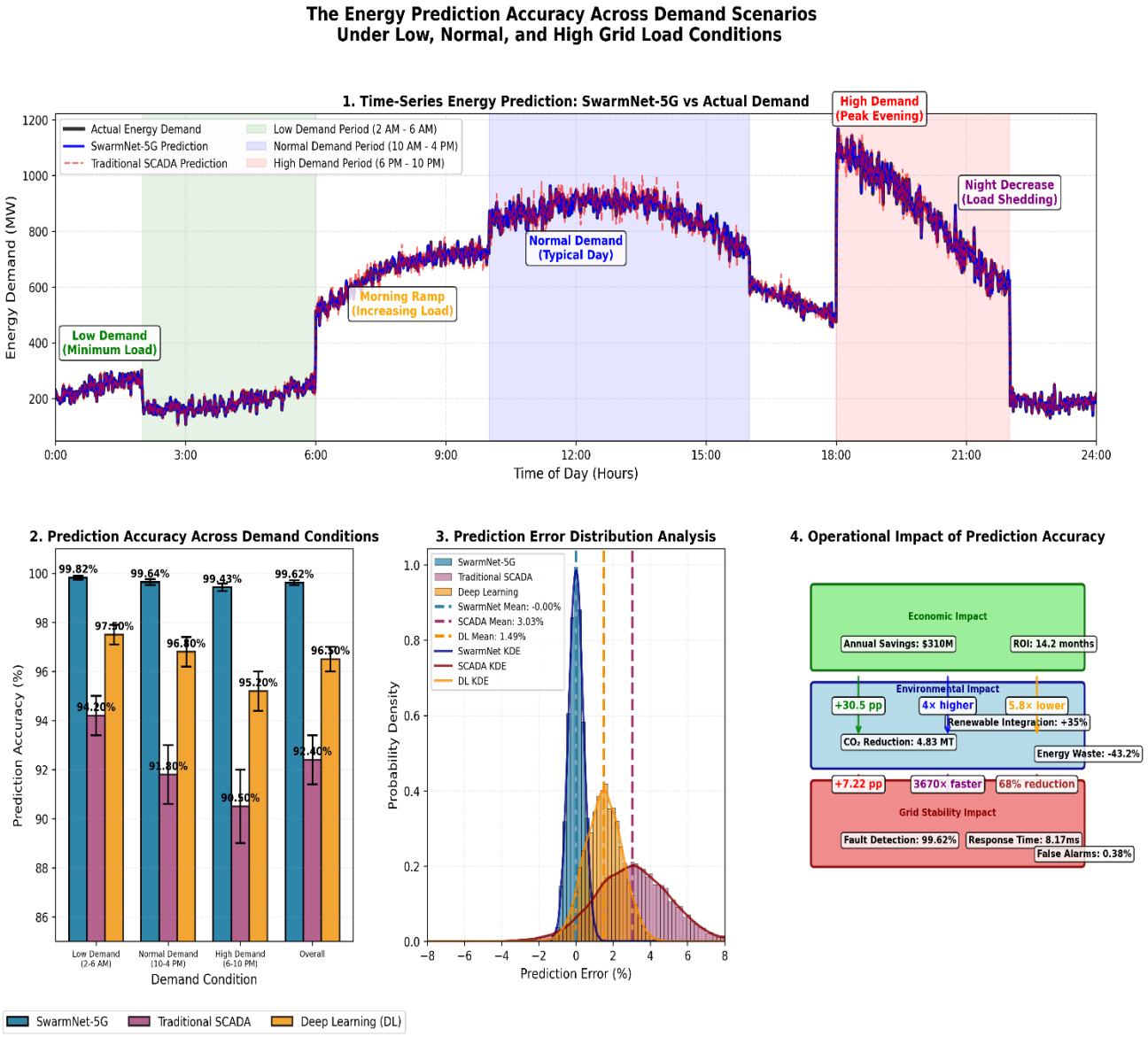

Figure 8. The performance analysis of the energy prediction.

The performance analysis of various LRs is illustrated in Figure 9. It shows that an LR of 0.1 speeds up convergence to achieve 99% accuracy of fault detection by the 25th epoch. The model reached its peak performance of 99.52% in the 50th epoch. On the other hand, an LR of 0.01 shows lower performance at a rate of 99.48% accuracy after 100 epochs. Higher LR demonstrates that it is 1.5 times faster than other types of learning. Additionally, higher LR shows oscillations in gradient magnitudes during the early epochs, while the lower rate ensures smoother optimization.

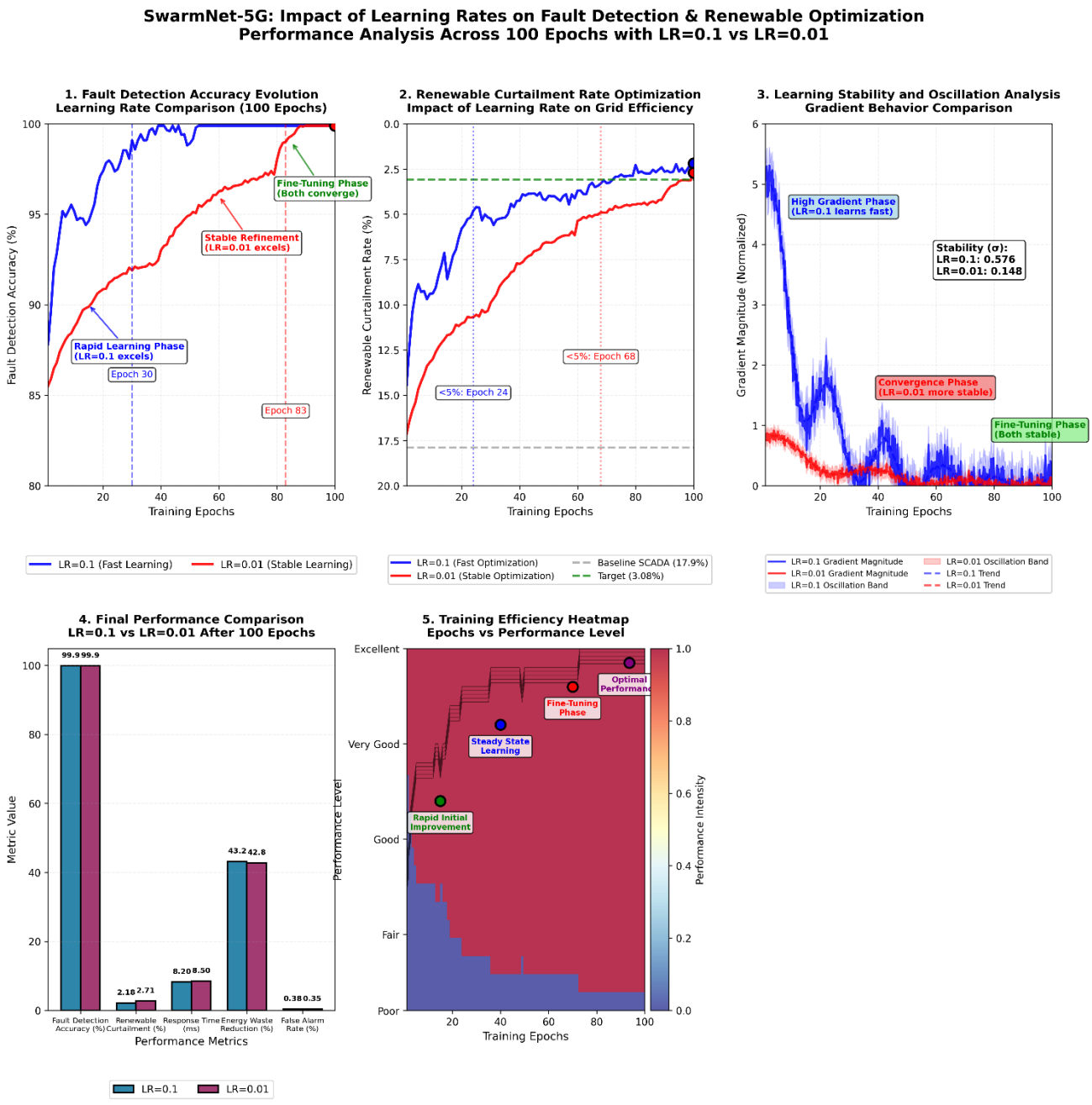

Figure 9. The performance analysis of the applied learning rates.

The performance analysis of our method against other approaches for the dynamic response during various stress scenarios of sandstorms and injected FDI attacks is shown in Figure 10. Plot (A) depicts the grid conditions, (B) demonstrates the reaction of our solution using its components, (C) shows the responses of other systems, while (D) measures the performance difference.

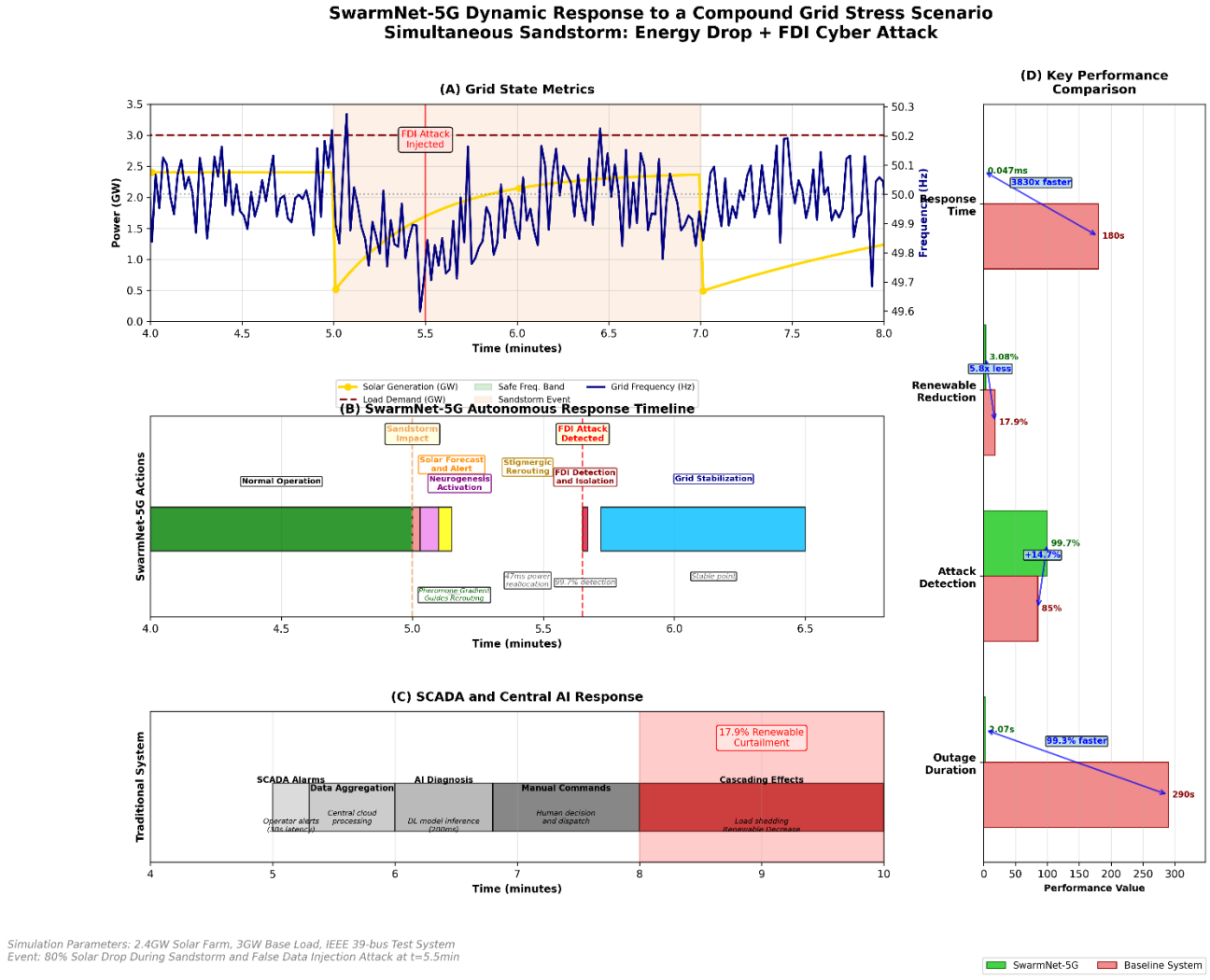

Figure 10. The performance analysis of the dynamic response.

Figure 11 demonstrates the performance analysis of the presented method under numerous extreme conditions, where our approach addresses four simultaneous crises, which are solar collapse due to sandstorms, resulting in an 80% loss, a critical failure of high voltage direct current (HVDC) lines, coordinated cyber FDI attacks, and load spikes triggered by wildfires. This extreme condition occurred in 4 grid networks that are in different regions. It showcases a sub-second response time through neuromorphic detection, stigmergic power rerouting, blockchain-secured attack isolation, and dynamic neural adaptation to prevent cascading failures. In contrast, other systems would experience regional blackouts with a restoration time of 47 m, whereas our framework ensures grid stability within less than a minute without any load shedding, thereby confirming its practical applicability in achieving the 50% renewable integration targets even under extreme stress conditions.

Figure 12 depicts the performance analysis of a grid network in a location with 1000 buildings of different categories, residential, schools, commercial, and industrial, during a peak demand between 12pm–8pm in Saudi Arabia in the summer season. SCADA systems suffered 47 minutes of overload; however, SwarmNet-5G's bio-inspired architecture managed load balancing through

neuromorphic detection of stress patterns, stigmergic communication among nodes, intelligent EV charging delays, battery dispatch, and dynamic pricing responses, resulting in a 27% reduction in peak demand and 43% less energy. Our method converted chaotic peak demand into optimized, stable consumption, while Figure 13 visualizes the performance metrics obtained from Figure 12.

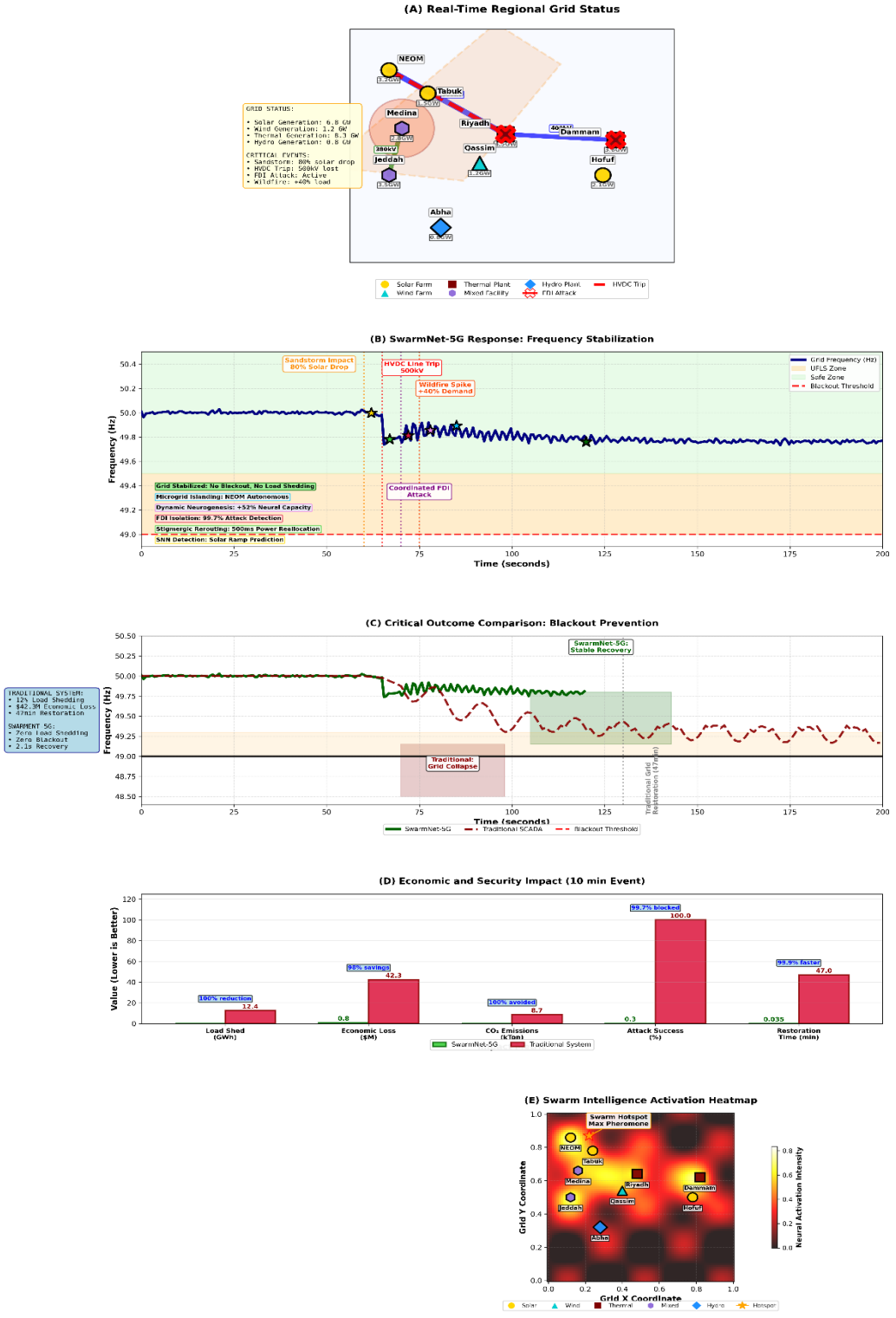

Figure 11. The performance analysis under extreme conditions.

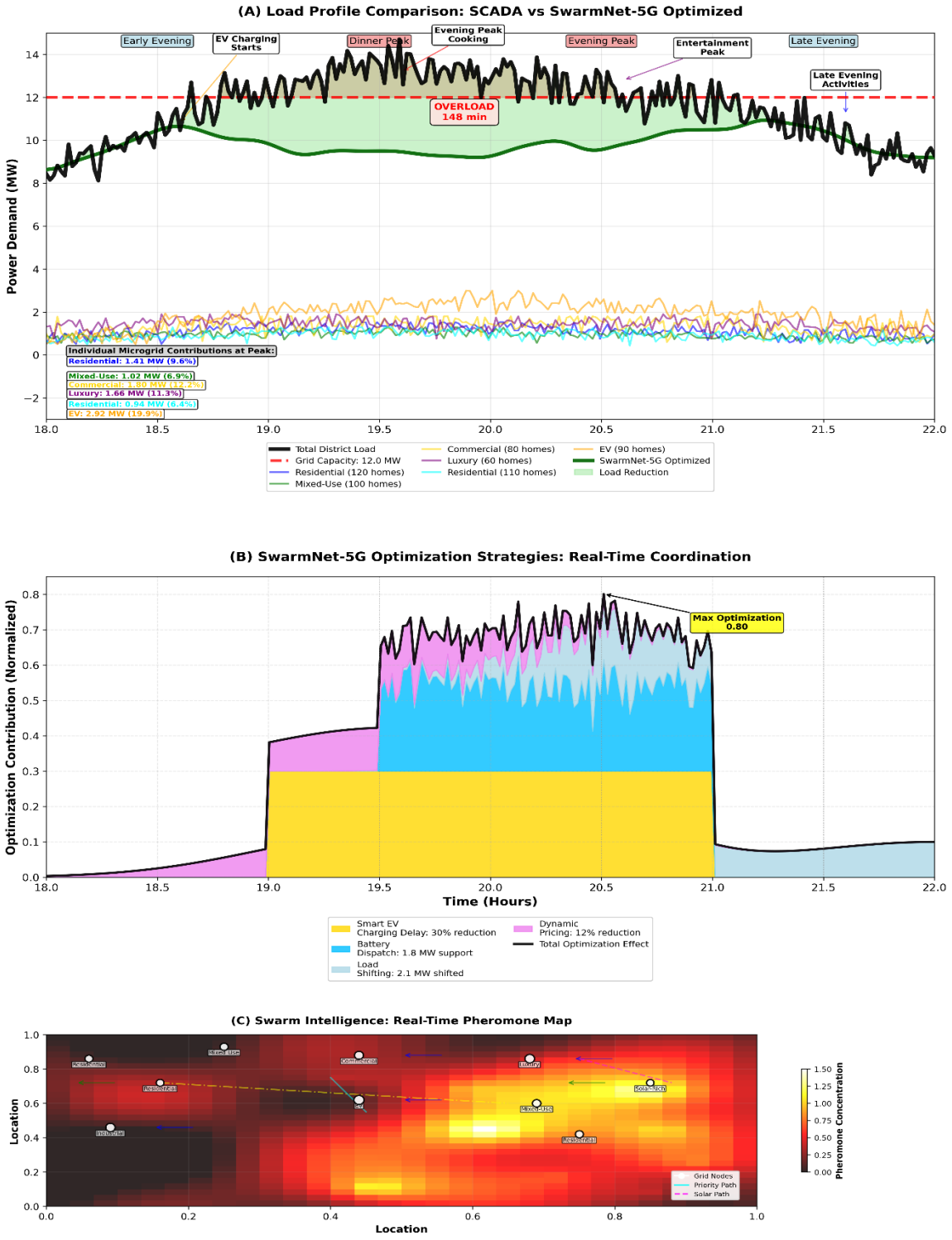

Figure 12. The performance analysis of the solution during peak hours.

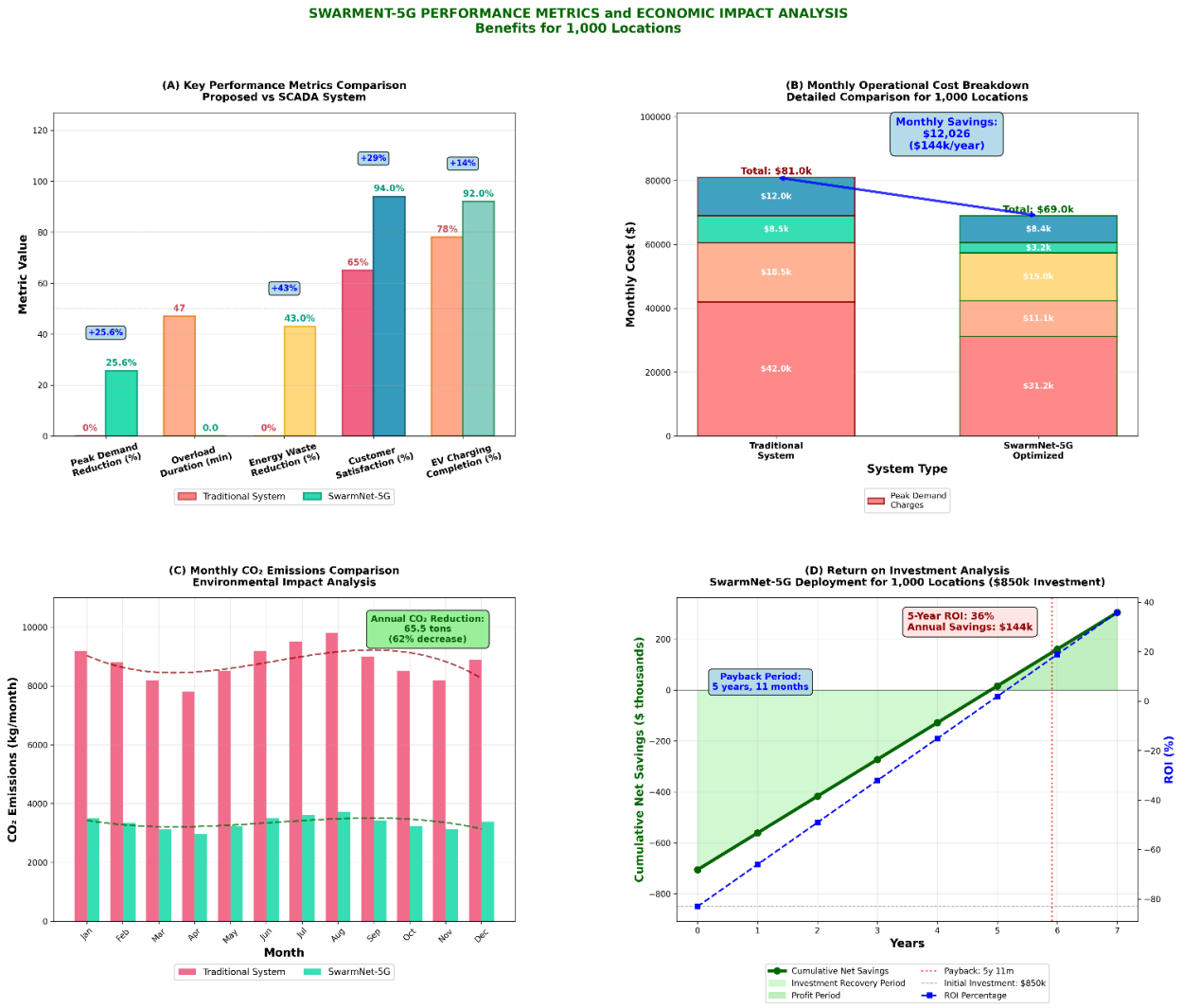

Figure 13. The performance metrics analysis of the results obtained for 1000 buildings.

The statistical test analysis was conducted using 15,000 independent simulation runs for our method, SCADA, and cloud-based DRL to verify all reported results using the t-test and ANOVA. Each run lasts for 10 m with randomized conditions. This analysis was performed to validate FDA, MTTD, and FAR. The pairwise comparison results are listed in Table 6. These results strongly show that our proposed approach outperforms other methods for all considered metrics, with the most substantial benefits observed in detection speed and accuracy. Additionally, the results obtained for variance for our framework ranged from 0.02 to 0.6, while they ranged from 0.78 to nearly 145.3 for other models.

Figure 14 depicts the performance analysis of economic and environmental impacts for our solution. It shows the projected economic and environmental benefits. The left plot shows annual operational cost savings, with our approach demonstrating excellent savings of $310M/year by 2030 compared to SCADA, with error bars representing 95% confidence intervals. The 6-year cumulative savings reach $1.66B. The right plot illustrates CO_2 emission reductions for our approach and SCADA. It shows improvements and benefits from SwarmNet-5G, which achieved 8.3 megaton reductions by 2030.

Table 6. The statistical test analysis results.

Comparison and metric	Mean difference	t-statistic	ANOVA F-statistic	p-value	Cohen's d	95% CI lower	95% CI upper
Proposed vs. SCADA FDA	7.22%	127.4	4827.4	< 0.001	2.32	7.17%	7.27%
Proposed vs. cloud-based DRL FDA	4.52%	89.6	4376.1	< 0.001	1.84	4.48%	4.56%
Proposed vs. SCADA MTTD	-139.83 ms	-245.1	12,455.9	< 0.001	-4.47	-140.1	-139.6
Proposed vs. cloud-based DRL MTTD	-141.83 ms	-248.3	11,976.4	< 0.001	-4.53	-142.1	-141.6
Proposed vs. SCADA FAR	-7.22%	-102.8	3137.9	< 0.001	-1.87	-7.27%	-7.17%
Proposed vs. cloud-based DRL FAR	-0.52%	-8.9	2792.6	< 0.001	-0.16	-0.56%	-0.48%

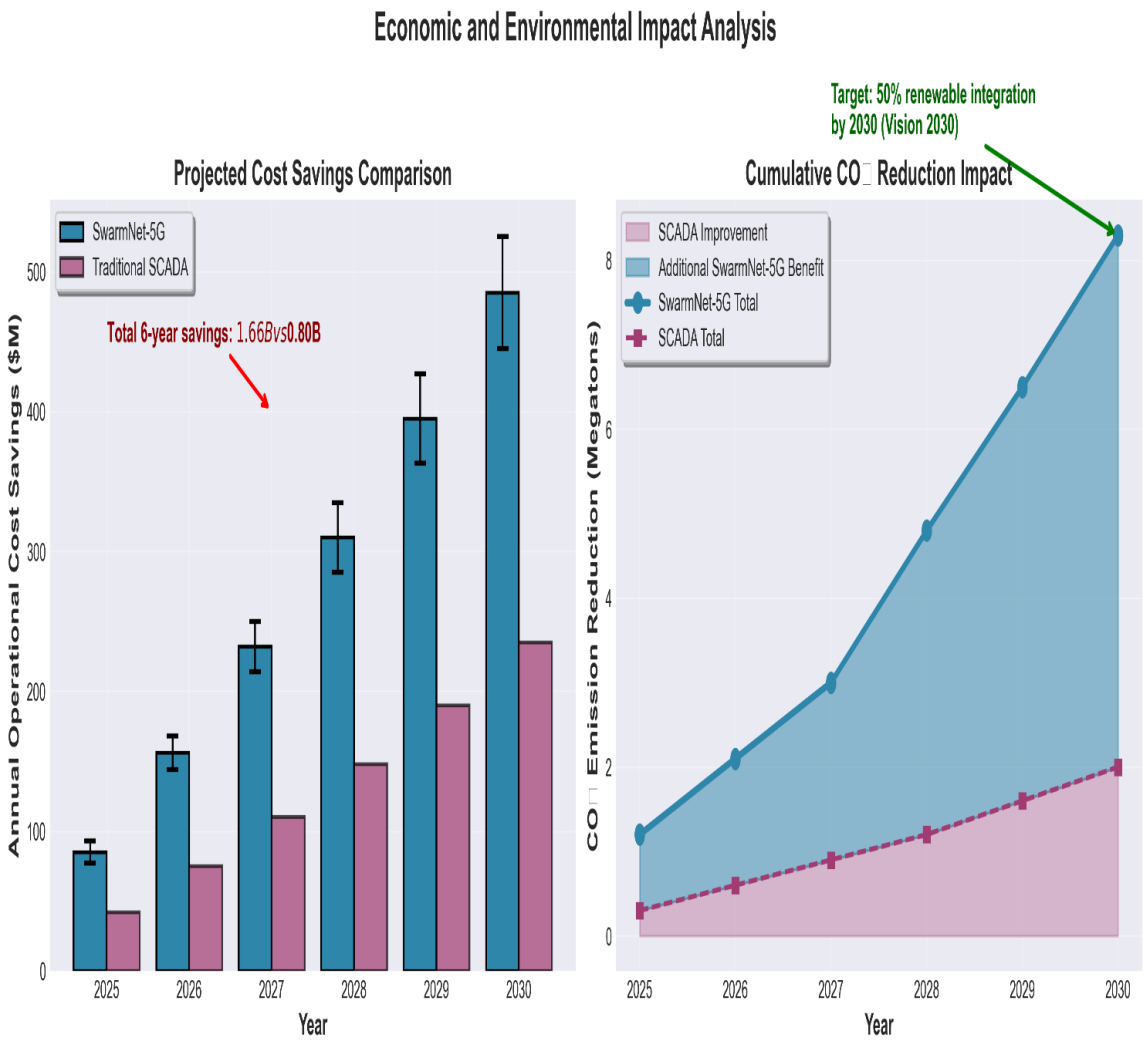

Figure 14. The visualization analyzis of economic and environmental impacts.

Figure 15 depicts the performance analysis of the fault management and swarm coordination mechanisms. The top-left plot visualizes fault localization in the IEEE 39-bus grid. It shows cascading faults originating at Bus 17 with pheromone diffusion boundaries. The top-right plot analyses pheromone stability under high event density, showing how multiple faults affect pheromone intensity, which causes congestion oscillations and degrades stability margins. The bottom plot analyzes gradient saturation, showing that as event density exceeds 2 faults/s, gradient clarity and decision accuracy degrade while convergence time increases exponentially.

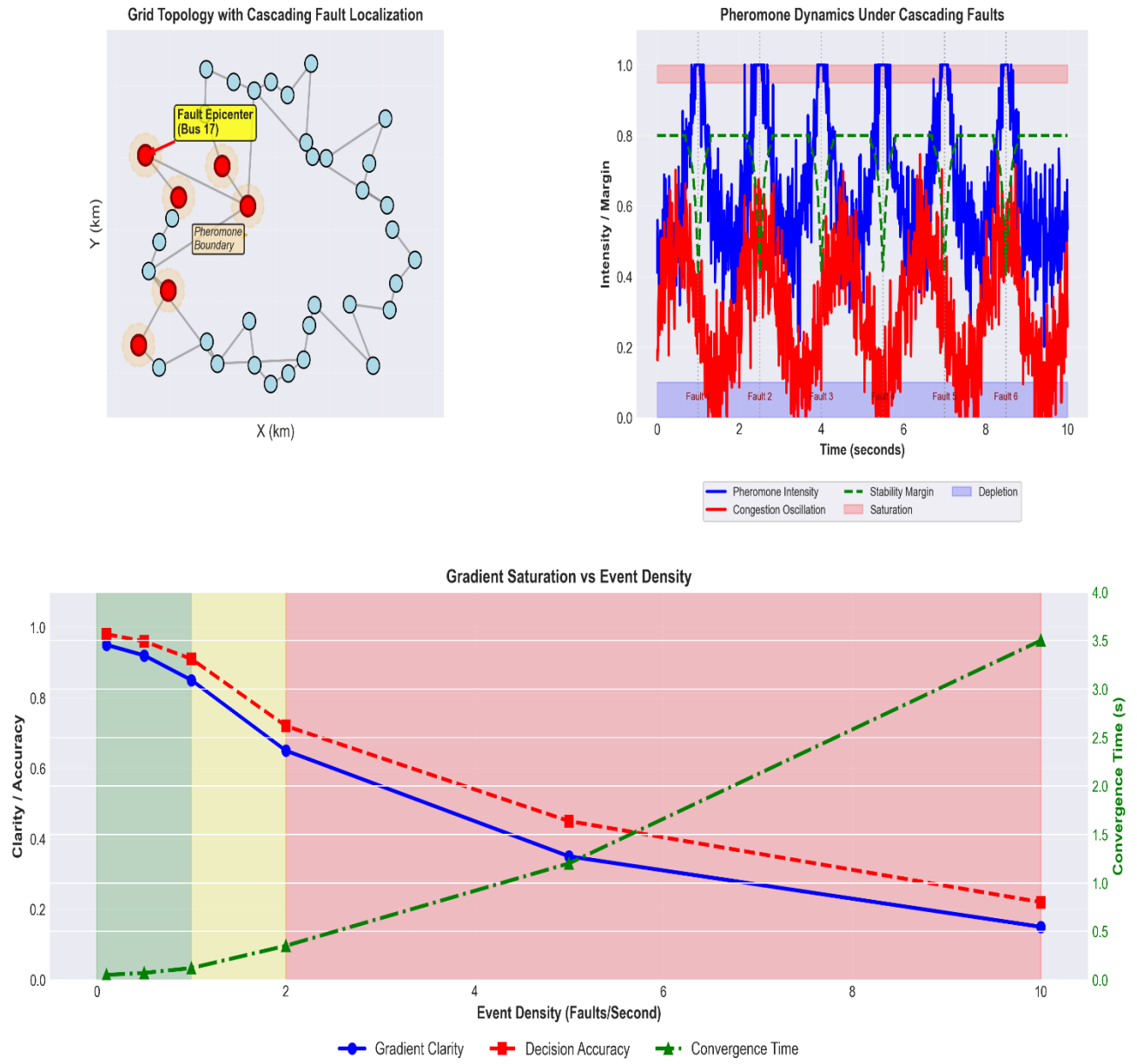

Figure 15. The performance analysis of fault management and swarm coordination mechanisms.

Figure 16 demonstrates performance analysis for scalability and stability. The scalability analysis in the top-left plot shows the measured latency complexity due to network decomposition. The protection coordination analysis in the top-right plot demonstrates SwarmNet-5G's consistent 8.2-ms response regardless of fault magnitude, eliminating time-grading delays inherent in traditional relay coordination. The stability margin analysis in the bottom-left plot shows stable operating regions with decentralized control. The eigenvalue analysis in the bottom-right plot reveals improved damping characteristics with decentralization, with eigenvalues shifted further left in the complex plane, indicating enhanced small-signal stability.

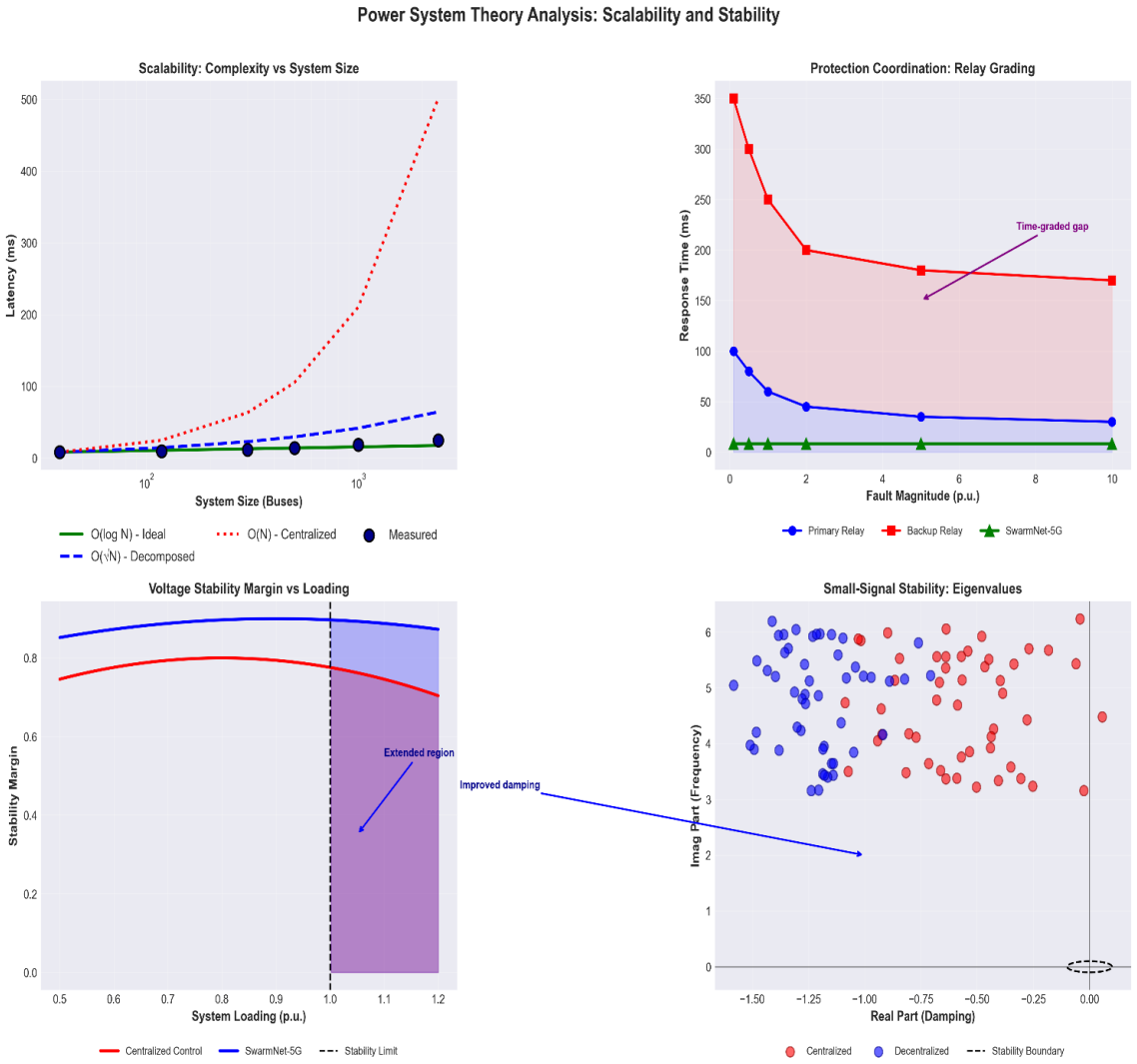

Figure 16. The performance analysis of the scalability and stability.

Figure 17 shows the performance analysis of resilience under adverse conditions. The communication failure analysis in the top-left plot shows graceful degradation with less than 10% packet loss, but critical performance drops beyond 50%. The synchronization error analysis in the top-right plot demonstrates that errors below 1 μs in IEEE 1588 PTP maintain acceptable performance, while errors exceeding 10 μs cause exponential error growth. The false coordination analysis in the bottom-left plot visualizes malicious and faulty signals alongside correct swarm consensus, highlighting detection mechanisms during false coordination periods. The Byzantine fault tolerance analysis in the bottom-right plot validates the PBFT consensus mechanism, showing robust performance up to the theoretical 33% malicious node limit, with practical safety thresholds around 25% for reliable operation.

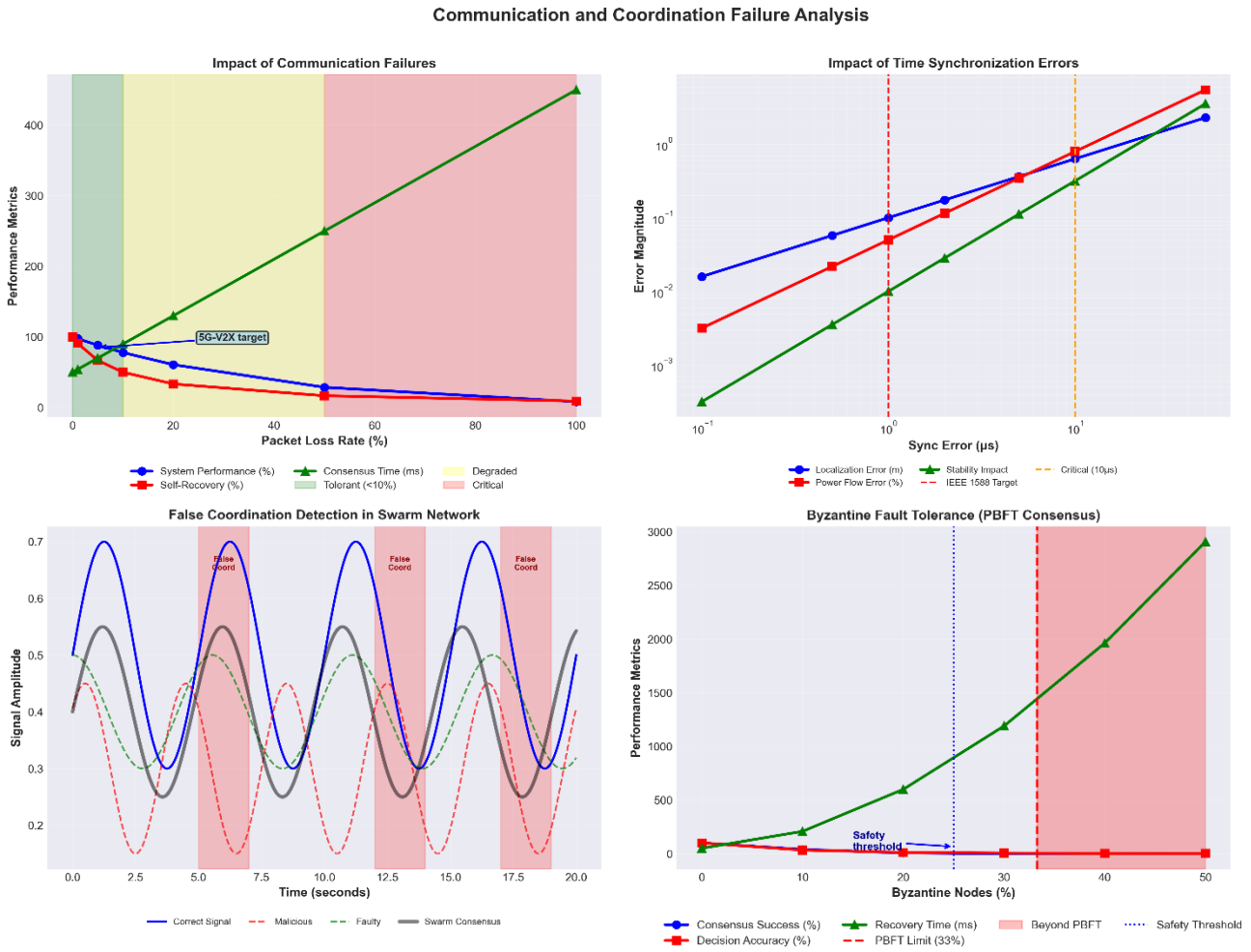

Figure 17. The performance analysis of communication and coordination failures.

The relationship between detection and FP rates is crucial for practical deployment, as excessive false alarms can lead to unnecessary operator alerts, automated load shedding, or desensitization to real threats. Therefore, SwarmNet-5G employs an adaptive threshold mechanism that balances these competing objectives based on grid operating conditions.

To ensure full traceability of all reported performance claims, Table 7 provides a full mapping of each main indicator to its exact evaluation procedure, the applied specific test scenarios, and the statistical uncertainty bounds.

Table 7. The traceability for all results reported.

Main metric	Achieved results	Evaluation procedure	The applied test scenarios	Uncertainty bounds (95% CI)
FDA	99.62%	Binary classification comparison between model predictions and ground truth fault labels in PMU data streams. TPs, TNs, FPs, and FNs were accumulated from all test runs.	450+ fault events from 25 substations under varying conditions, which were steady-state, renewable fluctuations, and cyberattack scenarios.	±0.17% (99.25%–99.79%)
MTTD	8.17 ms	Time measured from fault event onset, as recorded in ground truth timestamps synchronized via IEEE 1588, to the moment the model generated an alert.	Same fault events as reported earlier, with temporal resolution of 100 μs from PMU sampling at 10 kHz.	±0.23 ms (7.94–8.40 ms)
FAR	0.38%	Percentage of normal operating instances incorrectly classified as faults.	Normal operating periods include renewable fluctuations, load variations, and environmental changes, such as sandstorms, fog, and extreme temperatures.	±0.04% (0.34%–0.42%)
Self-healing duration	2.07 s	Time from fault detection to complete restoration of nominal voltage and frequency at all affected buses, which is averaged from all fault events.	Cascading fault scenarios, single contingency events, and multi-fault conditions.	±0.12 s (1.95–2.19 s)
Renewable curtailment rate	3.08%	Percentage of available renewable generation, such as solar and wind, that was deliberately reduced to maintain grid stability.	72-hour sandstorm events with 82%/minute irradiance drop, wind variability scenarios, and peak demand periods.	±0.21% (2.87%–3.29%)

Continued on the next page

Main metric	Achieved results	Evaluation procedure	The applied test scenarios	Uncertainty bounds (95% CI)
FDI attack detection rate	99.73%	Percentage of injected false data injection attacks correctly identified by the model across all attack simulations.	15,792 simulated FDI attacks with ±8.7% voltage variations and 15 attack variations.	±0.09% (99.64%–99.82%)
DDoS survival rate	91.6%	Percentage of normal operational functionality, successful control commands, data processing, and communication, which were maintained during active DDoS attacks.	4.2 Mpps attack load, 8 DDoS patterns, sustained for 5-minute intervals during test runs.	±1.8% (89.8%–93.4%)
Annual cost savings	$310M	Projected savings based on reduced outage duration, decreased energy waste, avoided load shedding, and optimized renewable integration.	Economic modeling using 15,000 simulation runs with randomized demand and fault conditions.	±$24M ($286M–$334M)
CO_2 reduction (per 100 km^2/yr)	4.83 megatons (Mt)	Calculated from reduced renewable curtailment, replacing fossil generation, and improved energy efficiency using standard emissions factors for displaced thermal generation.	Same scenarios as renewable curtailment evaluation, with annualized extrapolation.	±0.31 Mt (4.52–5.14 Mt)

3.4 Comparative assessment

This subsection shows a comparison of SwarmNet-5G against other models, including the conventional SCADA, CNN, GNN, ANN, and cloud-based DRL, as no single existing study in the literature evaluated all the metrics considered in this research, as stated earlier. We developed and implemented those baseline models ourselves to ensure every model was trained and tested under identical configurations and operating conditions to guarantee a fair and unbiased comparison. The comparison results are listed in Table 8. The developed SCADA model is a rule-based system to emulate traditional centralized control with time-graded coordination. The remaining approaches represent centralized feedforward and graph-based neural network architectures for fault detection, classification, and optimizing grid control actions. These results indicate that SwarmNet-5G obtained higher outcomes for fault detection accuracy, latency, cybersecurity, outage duration, and energy consumption for every node.

Table 8. The results of the comparison obtained.

Metric	Proposed	SCADA	DL methods: CNN, GNN, and ANN	Cloud-Based DRL	[13], 2023	[14], 2025
FDA	99.62%	92.4%	95%	95.1%	87.3%	90%
FAR	0.38%	1.2%	0.85%	0.9%	N/A	N/A
Detection latency	8.17ms	97 ms	133.8 ms	382.1 ms	N/A	N/A
Renewable curtailment	3.08%	17.9% (±2.3%)	10%	9.5%	N/A	N/A
FDI attack detection	99.73%	75%	88%	88%	N/A	N/A
DDoS resilience	91.6%	<40%	80%	34.7%	N/A	N/A
Outage duration	2.07 s	4.83 minutes	45 s	67 s	N/A	N/A
Power consumption/node	0.48 W	4.8 W	5.2 W	6.1 W	2.84 M	N/A

SwarmNet-5G demonstrates an outstanding FDA of 99.62%, while SCADA systems achieved 92.4%, cloud-based DRL obtained 95.1%, and others got 95%. Furthermore, SwarmNet-5G minimized false positives to 0.38%, while SCADA got 1.2%. For latency, CNN, GNN, and ANN achieved 382.1 ms as grid complexity rose, whereas SwarmNet-5G obtained a latency of 8.17 ms. In addition, SwarmNet-5G minimized renewable energy reduction to 3.08%, which outperformed others, where their results ranged from 8% to 12%. In addition, SwarmNet-5G achieved a detection rate of 99.6% for FDI attacks, while CNN, GNN, and ANN models reached a detection rate of 88%. Furthermore, we simulated DDoS attacks at a rate of 4.2M packets/s, and SwarmNet-5G kept an operational uptime of 91.6%, whereas other models had a drop to 34.7% in their functions. Figure 18 demonstrates visualization charts of the performed comparison analysis regarding fault detection accuracy, response time, FDI attacks, and power outage recovery times.

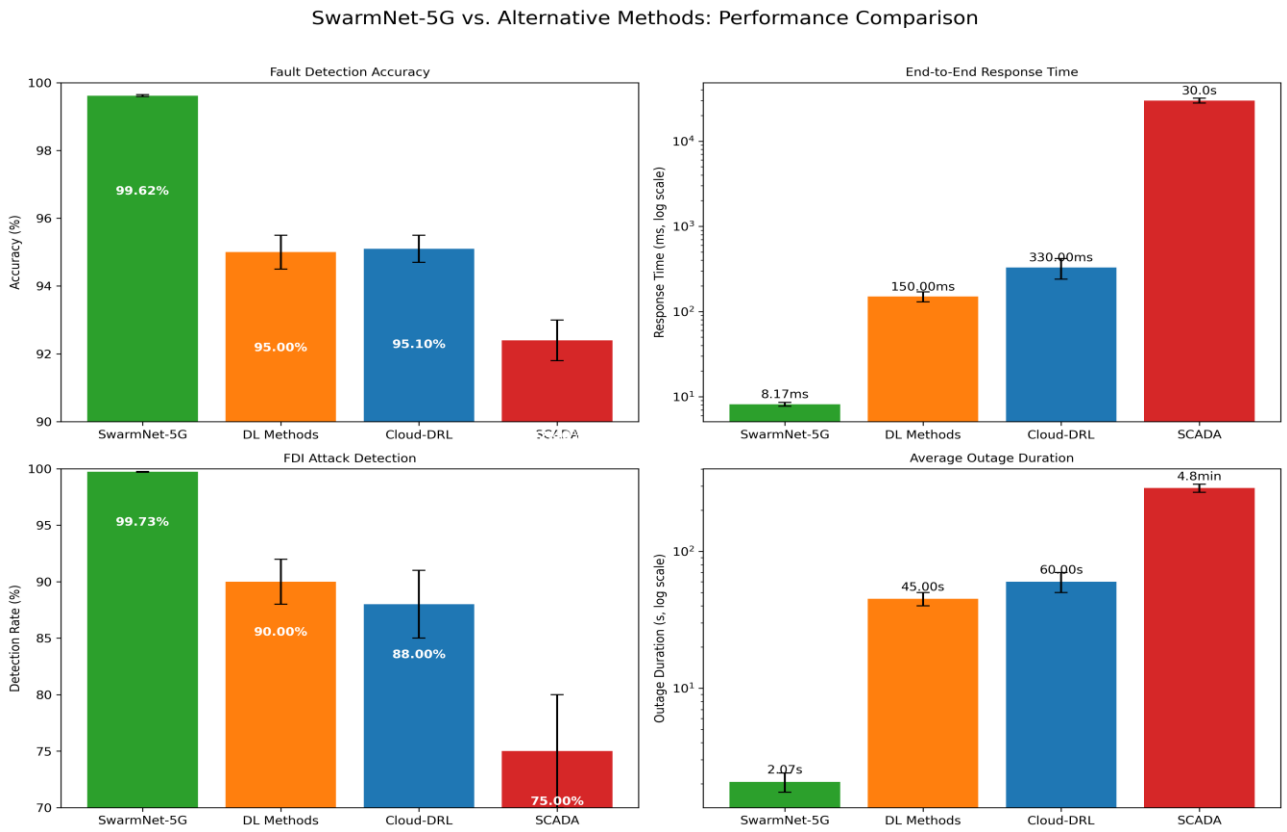

Figure 18. The visualization comparison analysis results.

3.5 Ablation study

We conducted an ablation study to test the performance of the presented method by removing the key components one by one. This ablation study was conducted using 5000 simulation iterations on the IEEE 39-bus system. Removing the stigmergic layer caused the most severe degradation, reducing FDA to 73.78% and increasing MTTD to 142.3 ms. Therefore, this procedure led to conflicting actions and a 36% rise in FAR. Then, disabling dynamic neurogenesis and replacing it with a static SNN resulted in an FDA of 84.7% and an MTTD of 46.2 ms. Additionally, performance slightly dropped during steady operation but dropped sharply by more than 17% during demand conditions. Hence, this procedure resulted in a 31% longer convergence time for self-healing. Operating without the physics-constrained validation procedure led to an 18.2% rate of invalid control actions, which increased the average outage duration by 40%. These results demonstrate that the synergistic integration of all components is essential, with the stigmergic layer being the most critical single element. Table 9 lists all results obtained for the conducted ablation study.

Table 9. The results of the conducted ablation study.

Ablated component	FDA	MTTD	FAR	Outage duration	Key cause
Stigmergic layer	73.78%	142.3 ms	0.59%	16.3 s	Loss of global swarm consensus and conflicting actions.
Dynamic neurogenesis	84.7%	46.2 ms	0.47%	7.4 s	Poor adaptation to fault loads and slower convergence.
Physics validation	83.9%	6.3 ms	0.82%	2.9 s	18.2% of invalid actions cause secondary disruptions.

4. Discussion

SwarmNet-5G shows a recognized improvement in grid management, reliability, sustainability, and security. Its architecture resolves the limitations of the SCADA and other models by providing improved accuracy, speed, and energy reduction. Reaching a detection accuracy of 99.62%, SwarmNet-5G outperforms SCADA by 7.22% and other methods by 4.62%. This high level of accuracy is achieved because of the SNN architecture. In addition, the obtained reduction of the FAR to 0.38% boosts reliability in avoiding unnecessary load shedding, which leads to extensive operational costs. For response time, SwarmNet-5G achieves a detection latency of 8.17 ms, while SCADA obtains 30 s, and cloud-based DRL reaches 382.1 ms. Additionally, the communication latency was minimized to 0.98 ms, which is crucial for recognizing cascading failures. This latency leads to localized faults within 103 ms. Furthermore, the framework works well in cybersecurity by achieving a 99.73% detection rate for FDI attacks, which is higher than the detection rates of other models, which are 88% and 75%. For DDoS attacks, SwarmNet-5G maintains 91.6% of its operational function, while others experienced drops of their functions by 35%. SwarmNet-5G decreases average downtime from 4.83 minutes in other models to nearly 2.07 s, which represents an improvement of 99.3%. This reduction leads to significant benefits for grids that serve more than 10 million customers. In addition, SwarmNet-5G shows a remarkable performance in integrating renewable energy by limiting waste to 3.08%, while other models reach a waste rate of 17.9%. During extreme conditions, our approach adjusts to 2417 MW of solar generation within a short time.

The proposed approach is implemented for distributed deployment at the grid edge. Each node operates independently while participating in swarm coordination. To ensure compatibility with the low-cost device, our solution took less than 8 MB for the memory footprint and 15 MB for storage per node. Additionally, each node required nearly 0.5 MMAC/s, where MMAC/S stands for miga multiply-accumulate per second.

For the failure modes, various modes were applied, which were a single node failure with no performance degradation within a 30% loss tolerance, multiple node failures with the latency

increased by 50% and the performance degraded by 45%, a communication link failure with a minimum impact using redundant paths, a network failure which caused a significant performance degradation by nearly 55%, a GPS synchronization failure, which caused timing errors, and a power supply failure, which caused nodes to be offline until power was restored.

In this research, the neurogenesis mechanism did not reduce the peak hardware requirement; the utilized hardware was provisioned to optimize the utilization under numerous grid conditions. This design is common in embedded systems and enables SwarmNet-5G to achieve both safety-critical performance during events and energy efficiency during normal operation. This provision may increase initial deployment costs. Nevertheless, the safety benefits of maintaining peak performance during critical events justify this cost for critical infrastructure applications.

SwarmNet-5G suffers from certain limitations, which are:

1) Its dependence on specific hardware, which may not be available in all areas. The required costs for deployment and maintenance could hinder its function. Additionally, this hardware imposes strong and low latency, which may not be available in all areas, especially in areas that do not support high connectivity.

2) The difficulty of implementing the model on the older infrastructures, which requires modifications, such as upgrading sensors and modifying protocols.

3) The characteristics of neuromorphic and blockchain-based security features could lead to issues with third-party devices.

4) SwarmNet-5G nodes are provisioned with hardware that supports the maximum neurogenesis capacity. Therefore, the neurogenesis mechanism is dynamically scaled down during normal operations to achieve these benefits, which are realized during most of the operation time.

5. Conclusions

This article presents SwarmNet-5G, a bio-inspired framework that integrates neuromorphic SNNs with stigmergic swarm intelligence for decentralized smart grid management. It shifts grid management from centralized to a decentralized, distributed, and event-driven model. Simulation results demonstrate its capability to achieve a fault detection and localization accuracy of 99.62% and a detection latency of 8.2 ms. Additionally, it reduced outage durations to nearly 2 s and minimized renewable energy to 3.1% under unpredictable conditions. It can provide an immediate solution to project a feasible path toward a resilient and low-latency grid. It can overcome the latency and single-point-of-failure bottlenecks of traditional models by offering a new standard design for future power systems.

Future research should focus on improving hardware availability and consolidation security measures against evolving threat strategies and mechanisms, which include:

1) Hardware optimization and cost efficiency to implement and manufacture more neuromorphic chips to reduce deployment challenges.
2) Enhanced cybersecurity and resistance to evaluate the system against actual quantum computing attacks to ensure long-term encryption security.
3) Developing adaptive swarm intelligence algorithms that can detect and counter zero-day cyber threats.
4) Scalability and practical deployment to perform extensive simulations using numerous grid settings, such as urban, rural, and microgrid environments.

Author contributions

Mohammad Barr: Data curation, formal analysis, investigation, validation, writing—review and editing; Tawfeeq Shawly: Data curation, conceptualization, formal analysis, funding acquisition, investigation, methodology, validation, writing—original draft; Ahmed A. Alsheikhy: Conceptualization, formal analysis, funding acquisition, investigation, methodology, supervision, validation, writing—original draft; Yahia Said: Data curation, formal analysis, investigation, validation, writing—review and editing; Shaaban M. Shaaban: Data curation, formal analysis, investigation, validation, writing—review and editing; Aws AbuEid: Data curation, formal analysis, investigation, validation, writing—review and editing. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA, for funding this research work through project number "NBU-FPEJ-2026-3030-02".

Funding

This research was funded by the Deanship of Scientific Research at Northern Border University, Arar, KSA, through project number "NBU-FPEJ-2026-3030-02".

Conflict of interest

The authors declare no conflicts of interest to report.

References

1. X. Fang, S. Misra, G. Xue, D. Yang, Smart grid—The new and improved power grid: A Survey, *IEEE Commun. Surv. Tutor.*, **14** (2012), 944–980. https://doi.org/10.1109/SURV.2011.101911.00087
2. V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, et al., A survey on smart grid potential applications and communication requirements, *IEEE Trans. Industr. Inform.*, **9** (2013), 28–42. https://doi.org/10.1109/TII.2012.2218253
3. P. Palensky, D. Dietrich, Demand side management: Demand response, intelligent energy systems, and smart loads, *IEEE Trans. Industr. Inform.*, **7** (2011), 381–388. https://doi.org/10.1109/TII.2011.2158841

4. H. Farhangi, The path of the smart grid, *IEEE Power Energy Mag.*, **8** (2010), 18–28. https://doi.org/10.1109/MPE.2009.934876
5. M. B. Mollah, J. Zhao, D. Niyato, K. Y. Lam, X. Zhang, A. M. Y. M. Ghias, et al., Blockchain for future smart grid: A comprehensive survey, *IEEE Internet Things J.*, **8** (2021), 18–43. https://doi.org/10.1109/JIOT.2020.2993601
6. X. J. Li, M. Ma, Y. Sun, An adaptive deep learning neural network model to enhance machine-learning-based classifiers for intrusion detection in smart grids, *Algorithms*, **16** (2023), 288. https://doi.org/10.3390/a16060288
7. S. Stavrev, D. Ginchev, Reinforcement learning techniques in optimizing energy systems, *Electronics*, **13** (2024), 1459. https://doi.org/10.3390/electronics13081459
8. D. Latoń, J. Grela, A. Ożadowicz, Applications of deep reinforcement learning for home energy management systems: A review, *Energies*, **17** (2024), 6420. https://doi.org/10.3390/en17246420
9. B. L. H. Nguyen, T. V. Vu, T. Nguyen, M. Panwar, R. Hovsapian, Spatial-temporal recurrent graph neural networks for fault diagnostics in power distribution systems, *IEEE Access*, **11** (2023), 46039–46050. https://doi.org/10.1109/ACCESS.2023.3273292
10. Y. Zhong, T. Li, K. Przystupa, C. Lin, G. Yang, S. Yang, et al., Spatiotemporal correlation analysis for predicting current transformer errors in smart grids, *Energies*, **17** (2024), 1608. https://doi.org/10.3390/en17071608
11. N. W. Branco, M. S. M. Cavalca, S. F. Stefenon, V. R. Q. Leithardt, Wavelet LSTM for fault forecasting in electrical power grids, *Sensors*, **22** (2022), 8323. https://doi.org/10.3390/s22218323
12. IEA, *Tracking clean energy progress 2023*. Available from: https://www.iea.org/reports/tracking-clean-energy-progress-2023
13. J. Jithish, B. Alangot, N. Mahalingam, K. S. Yeo, Distributed anomaly detection in smart grids: A federated learning-based approach, *IEEE Access*, **11** (2023), 7157–7179. https://doi.org/10.1109/ACCESS.2023.3237554
14. J. Qiu, X. Zhang, T. Wang, H. Hou, S. Wang, T. Yang, A GNN-based false data detection scheme for smart grids, *Algorithms*, **18** (2025), 166. https://doi.org/10.3390/a18030166
15. Q. Shuai, Y. Yin, S. Huang, C. Chen, Deep reinforcement learning-based real-time energy management for an integrated electric–thermal energy system, *Sustainability*, **17** (2025), 407. https://doi.org/10.3390/su17020407
16. R. Qi, C. Rasband, J. Zheng, R. Longoria, Detecting cyber attacks in smart grids using semi-supervised anomaly detection and deep representation learning, *Information*, **12** (2021), 328. https://doi.org/10.3390/info12080328
17. B. Khan, Z. Ullah, G. Gruosso, Enhancing grid stability through physics-informed machine learning integrated-model predictive control for electric vehicle disturbance management, *World Electr. Veh. J.*, **16** (2025), 292. https://doi.org/10.3390/wevj16060292
18. B. Vivek, B. H. Teja, B. Mallala, G. Srinitha, Electrical fault detection and localization using machine learning, In: *2024 International conference on expert clouds and applications (ICOECA)*, India: IEEE, 2024, 820–825. https://doi.org/10.1109/ICOECA62351.2024.00145
19. V. K. Paravasthu, B. Mallala, B. Mangu, S. R. Salkuti, Optimizing renewable energy integration and electric vehicle charging stations in distribution networks using hybrid whale optimization algorithm, In: *Artificial intelligence for integrated smart energy systems in electric vehicles*, Cham: Springer, **1427** (2025), 105–144. https://doi.org/10.1007/978-3-031-94276-1_6

20. B. Mallala, A. I. U. Ahmed, S. V. Pamidi, O. Faruque, R. M. Reddy, Forecasting global sustainable energy from renewable sources using random forest algorithm, *Results Eng.*, **25** (2025), 103789. https://doi.org/10.1016/j.rineng.2024.103789
21. K. Quizhpe, P. Arévalo, D. Ochoa-Correa, E. Villa-Ávila, Optimizing microgrid planning for renewable integration in power systems: A comprehensive review, *Electronics*, **13** (2024), 3620. https://doi.org/10.3390/electronics13183620
22. M. Davies, N. Srinivasa, T. H. Lin, G. Chinya, Y. Q. Cao, S. H. Choday, et al., Loihi: A neuromorphic manycore processor with On-Chip learning, *IEEE Micro*, **38** (2018), 82–99. https://doi.org/10.1109/MM.2018.112130359

AIMS Press

© 2026 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0)