ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 2 - 2026

A Data-Driven Digital Twin-Based Framework for Attack Chain Modeling and Defense in Networked Microgrids

Peng Xiao[1], *Biao Bai*[1] *and Zijie Deng*[2,*]

[1] Information Center of China Southern Power Grid Yunnan Power Grid Co., Ltd., Yunan, 650000, China

[2] China Southern Power Grid Power Grid Group, Co., Ltd., Guangdong Province, 510000, China

SUMMARY: *In light of the digital transformation of power systems and the increasing integration of renewable energy, grid control architecture has gradually evolved into deeply coupled cyber-physical power systems (CPPS) with chain-like and coordinated security risks. A Digital Twin-Based Framework for Attack Chain Modelling and Defence Strategy Verification in Power Grids is proposed in this paper. A bidirectional mapping model of the physical and cyber layers is built in this way to detect abnormal behaviour in time and space, and then adjust. A data-driven digital twin model of LSTM networks is used to address typical denial-of-service (DoS) attack scenarios and realize attack detection, alert, and self-healing decision verification. According to the results of the simulation, the proposed method can effectively reconstruct the process of the attack chain and improve the robustness and adaptive recovery capabilities of the control system in multi-node parallel systems significantly.*

KEYWORDS: *Digital Twin; Grid Security; Attack Chain Modeling; Defense Verification; Long Short-Term Memory*

1 Introduction

The digitization of electric power systems is changing traditional electric grids into cyber-physical electric power systems (CPPSs). Inside these systems, the physical property objects are connected with the network layers through the high-speed communication and the intelligent control mechanisms [1]. This change makes the promotion of monitoring, automation, and the total efficiency. Nevertheless, this thing moreover expands the proneness that people suffer from network and coordinated attacks [2]. Along with the enlargement of the scale of distributed energy resources (DERs) and networked microgrids (NMGs), the dependence on the control which is based on communication and the exchange of data becomes stronger [3]. This increased dependence therefore lifts the danger of network attacks on key electric power infrastructure.

A network of microgrids (NMG), which are coordinated clusters of microgrids, have recently shown promise in enhancing the integration of renewable energy, operational flexibility and local energy security. Each microgrid can operate independently or work together in cooperation through multi-agent systems (MAS) to share information for voltage stability maintenance, power-sharing optimisation, and coordination of distributed generation (DG) units [4]. However, the above advantages are also accompanied by disadvantages; that is,

*zijiedeng2025@163.com
https://doi.org/10.65102/is2026854
Published: 30 April, 2026

the same communication network that supports intelligent coordination can also be used as a target for cyberattacks, such as data alteration, spoofing and denial-of-service (DoS) attacks. Such intrusions will interfere with the real-time operation of decision-making, be affected in various ways, and result in the complete collapse of the system due to a chain reaction of failures in interconnected platforms [5].

Early studies found that, due to the spread of cyber threats along communication lines, voltage fluctuations, power imbalances or even blackouts could occur in the physical power system. He and Yan [6] have studied the impact of False Data Injection (FDI) attacks on distributed control systems and found that modifications to measurement data can cause a large deviation in the output of distributed generation (DG). Liu and others [7] have modeled the coordinated FDI and DoS attack, showing that they can compromise the consensus control mechanism of a microgrid. Li and others [8] have proposed a fault-tolerant distributed secondary control algorithm based on consensus reconfiguration to improve voltage recovery; however, it is still sensitive to communication failures. Xing et al. [9] proposed an adaptive control reallocation scheme under cyber disruptions, but this method required full state observability and thus was not suitable for large-scale networked systems.

With the development and spread of applications for multi-agent-based control in microgrids, many studies have recently investigated how to improve the robustness and security of such systems at various levels. Arani et al. [10] have presented a cyber-physical co-simulation framework to analyze DoS attacks on DC microgrids and have identified core weaknesses in agent synchronisation. At the same time, Wang et al. [11] put forward a resilient distributed control strategy based on event-triggered communication to reduce DoS effects by reducing bandwidth consumption, but it did not detect stealthy data falsification attacks. Zhang and others [12] have put forward an anomaly-based intrusion detection mechanism that improves detection through Kalman filtering and residual evaluation. However, this way was constrained by the linearity of the system's dynamics and thus not suitable for converter-dominated nonlinear systems. More recently, Ali et al. [13] have combined artificial intelligence (AI) with cybersecurity for microgrid operation to use a convolutional neural network (CNN) to detect DoS attack signatures. Although the improved accuracy is due to CNNs, they cannot handle the time-series nature of the attack well. Zhou and others [14] have applied a graph neural network (GNN)-based method for anomaly detection in multi-agent networks to enhance spatial feature extraction, but it is relatively computationally expensive for real-time operation.

Recently, Digital Twin (DT) technology has begun to be used to improve the situational awareness, predictive monitoring and real-time control capabilities of CPPSs. Fuller et al. [15] proposed DTs (dynamic, data-driven models) that can simulate the real-time behaviour of a physical system by using a two-way information exchange. Tao et al. [16] have examined the application of DTs in smart manufacturing and extended the potential for smart grid applications; at the same time, they are suitable for predicting failures and identifying abnormal conditions in smart grids. Qi and Tao [17] have also proposed DT architectures for cyber-physical systems and pointed out the need for high-fidelity modelling and real-time data synchronisation. Chen et al. [18] have built a DT-based fault diagnosis model for microgrids that integrates data-driven and physics-based methods to identify converter faults, and while improving diagnostic accuracy, it has not shown robustness against cyber disturbances. He and others [19] put forward a hierarchical DT framework for real-time energy management in multi-microgrids, but only used it for operational optimisation and did not add cyberattack detection and mitigation. Ranawaka et al. [20] extended DT technology to power system stability analysis and developed a real-time simulation environment using reinforcement learning. Although it

has improved the problem of control optimisation, it has not addressed the issue of communication-layer security directly.

With the development of machine learning, some scholars have begun to apply artificial intelligence technology to solve the problem of cyber-attack detection. Chen and others [21] have used recurrent neural networks (RNNs) to predict power system abnormalities from time-series data and thus enhanced the early warning function of the traditional fixed model. Based on the above, Hussain et al. [22] have applied a Long Short-Term Memory (LSTM)-based method to detect coordinated FDI and DoS attacks in AC microgrids. The Model has high detection accuracy but is not very explainable and slow. Alshahrani and others [23] put forward a hybrid LSTM-CNN model for anomaly detection; although it is more robust against false alarms, the training difficulty has increased. Although there have been some progress, most of the current AI-based methods are still data-hungry and tailored to a single type of grid. They are generally not connected to control modules, so they cannot automatically address the detected problems.

Although many studies have been conducted on the detection of cyberattacks, improvements in resilience and the application of digital twin modelling in power systems still face several basic problems:

Most DT frameworks focus on physical fault diagnosis and optimisation, and have paid little attention to cyberattack detection and response in networked microgrids.

Existing research has separated the cyber and physical layers and thus has failed to address the necessity of real-time mutual dependence.

LSTM networks have shown some promise for analysing sequence data, but their application in DT architectures for dynamic cyberattack detection is still in its early stages.

Many of the current methods only trigger after detecting an attack and do not have the predictive ability to prevent performance degradation before the system fails.

Based on the above deficiencies, this paper proposes a new data-driven digital twin framework for cyberattack chain modelling and mitigation in networked microgrids.

The first few are as follows:

(1) Development of an LSTM-based digital twin architecture capable of accurately replicating cyber–physical dynamics across both communication and control layers.

(2) Design of a real-time cyberattack detection mechanism leveraging temporal residual analysis between digital and physical twins.

(3) Introduction of an autonomous mitigation scheme in which digital twins replace compromised agents to restore operational stability.

(4) Validation of the proposed model under simulated DoS attack scenarios, demonstrating enhanced resilience, reliability, and low computational overhead.

This paper builds an all-encompassing digital twin-based cybersecurity system for next-generation intelligent microgrids and integrates deep learning, cyber-physical modelling and autonomous control to achieve resilient, self-healing power networks.

2 A Multi-Agent Control Architecture for Multi-Microgrid (MG) Systems

The concept of microgrids (MGs) is an economical way to connect renewable energy resources and energy storage facilities (ESSs) for greater flexibility and stability of the electrical system. MGs can operate in either islanded or grid-connected modes and are suitable for both energy management and grid stability. With the growth of demand for distributed power systems, in recent years, both DC and AC microgrid research has expanded at an accelerated pace. DC

microgrids are relatively easy to connect with DC systems and do not require a DC-AC converter because both are inherently DC, simplifying the connection to an existing DC network. DC microgrids do not have the same problems as AC systems, such as frequency regulation issues and reactive power flow problems, etc. The old control method of droop control is not suitable for DC microgrids because of bus voltage drop and inaccurate current sharing when there is a real power line impedance. Given the above problems, in order to improve the stability, scalability and robustness of the system, a hierarchical control mode has been chosen. Traditional centralised control methods at the secondary level use a single central controller to collect information from all distributed generation (DG) units and then issue control signals. Although this way can form a single-control structure, it has the following deficiencies: a large amount of computation, low efficiency, and a single point of failure. In light of the above problems, a distributed control method distributes the decision-making responsibility among multiple controllers or nodes to reduce the risk of a whole-system failure and enhance the flexibility of managing various distributed energy resources (DERs). Decentralised control methods also have coordination problems and increased communication overhead because each DG only communicates with its neighbours. These ways, however, are more flexible and scalable, perform better in computation, do not have a single point of failure, and support the addition of new distributed energy resources (DERs). Figure 1 is the cyber-physical model of three networked microgrids connected to a point of common coupling (PCC), and the interconnectedness and communication paths among the system are shown.

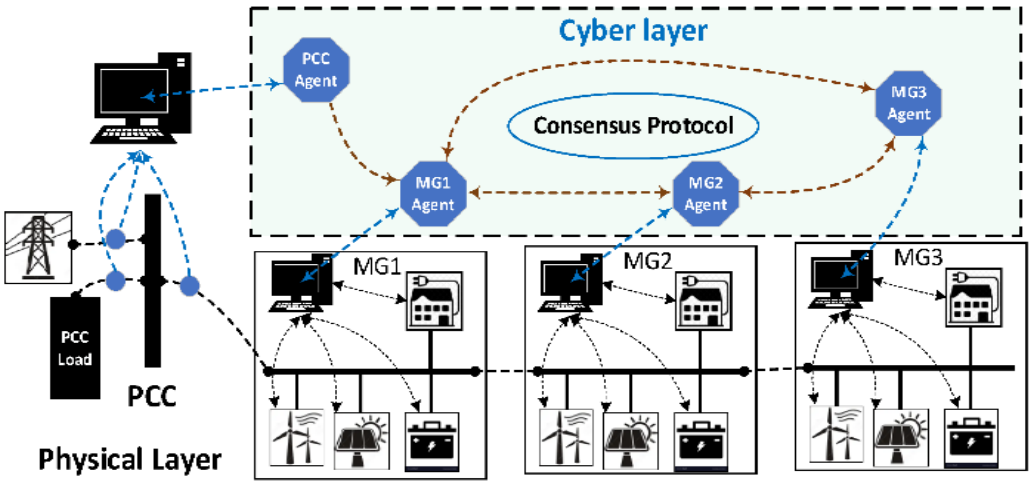

Figure 1: Cyber-Physical Architecture of Networked MGs.

2.1 Physical Layer Modeling

A concept that is about an isolated direct current microgrid is put forward, which possesses an all-round structure with very many distributed power generators (DGs). Each DG unit is composed by one ideal DC voltage source, one DC/DC converter, and many different sorts of loads. In the beginning, the focus is put on a microgrid system that includes two DGs, which are called DG i and DG j, they are connected via a distribution line marked as ij, just like what is shown in Figure 2. According to the application situation and the voltage magnitude on the source side and the load side, many kinds of converters, such as raise-voltage and lower-voltage converters, may be utilized inside a DC microgrid. The average electricity model graphs of step-down and step-up converters are shown in the Figure 2. The motion equations which control the system, got through using Kirchhoff's circuit rules, are written as what follows[24].

For DGi:

$$\frac{dV_i}{dt} = \frac{1}{C_{ti}} I_{ti} - \frac{1}{C_{ti}} \widehat{I_{Li}} + \frac{1}{C_{ti}} I_{ij} \tag{1}$$

$$\frac{dI_{ti}}{dt} = -\frac{1}{L_{ti}} V_i - \frac{R_{ti}}{L_{ti}} I_{Li} + \frac{d_i}{L_{ti}} V_{si} \tag{2}$$

where $V_i$represents the voltage across the load, and V_{si}represents the voltage of the distributed generator (DG). The currents through the filter, load, and transmission line are denoted as I_{ti}, $\widehat{I_{Li}}$and I_{ij}, respectively. Additionally, $d_i$represents the duty cycle of the converter, and L_{ti}, R_{ti}, and C_{ti} are the inductance, resistance, and capacitance of the filter, respectively. The transmission line connecting any two different nodes i and j can be typically represented with the impedance of line resistance and inductance, R_{ij} and L_{ij}. Hence, the current flowing between these two nodes can be expressed as:

$$\frac{dI_{ij}}{dt} = -\frac{R_{ij}}{L_{ij}} I_{ij} + \frac{1}{L_{ij}} V_j - \frac{1}{L_{ij}} V_i \tag{3}$$

The above equations show the dynamic connection of distributed generators, filters, currents, loads and transmission lines in a DC microgrid. A model is constructed to study how different parameters in a system, such as voltage and current, are connected, and thus how to optimize control and operation of a microgrid.

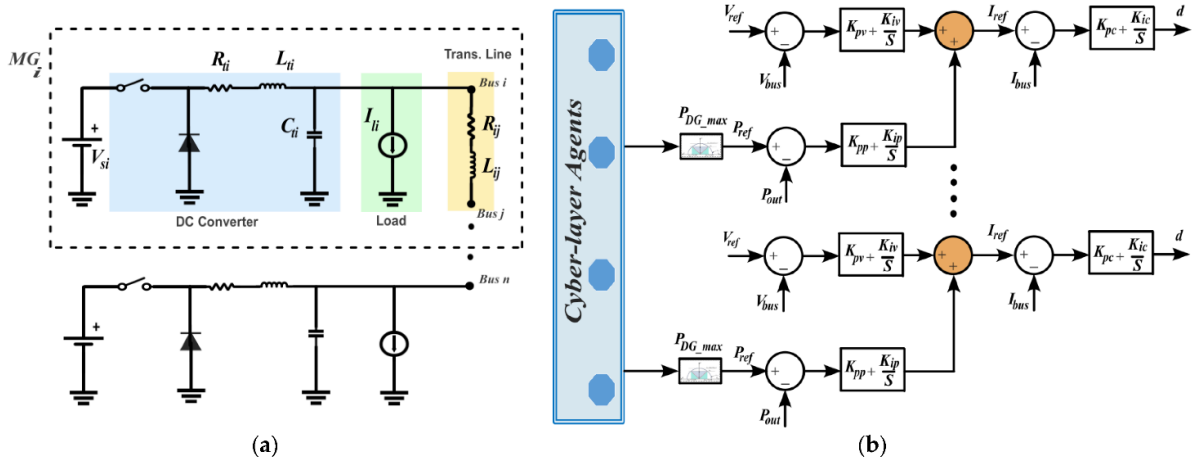

Figure 2: Micro-grid (MG) Model Building and Control: (a) The equal value electric circuit of Distributed Generation units (DGs) and load devices inside the micro-grid; (b) The local control unit that is inside the microgrid which has a cyber-layer connecting link.

The Control Strategy of a Microgrid Needs to ensure that both Voltage and Current remain stable during operation. Therefore, PI controllers are used to regulate both the inner and outer control loops for voltage and current in this study. The control equation for the voltage control loop is set to regulate the DC bus voltage, maintain it close to the desired reference value, and consider power output:

$$i_{\text{ref}} = \left(K_{iv}S + K_{pv}\right) \cdot \left(v_{\text{ref}} - v_{\text{dcbus}}\right) + \left(K_{ip}S + K_{pp}\right) \cdot \left(p_{\text{ref}} - p_{\text{out}}\right) \tag{4}$$

where:v_{ref} is the desired voltage reference,v_{dcbus} is the measured DC bus voltage, p_{ref} is the

power reference, $p_{\text{out}}$is the measured output power, $K_{iv}, K_{pv}$are the integral and proportional terms of the voltage PI controller, K_{ip}, K_{pp} are the integral and proportional terms of the power PI controller.

The terms Δv and Δp represent the voltage and power error signals respectively. These errors are used to drive the control action, with the goal of minimizing the difference between the measured and desired values. The controllers adjust the duty cycle of the converter to correct the system's behavior, ensuring that the voltage remains within the predefined operational limits (e.g., within ±5% deviation from the reference value).

The current control loop will regulate the current at the load and keep it within a reasonable range based on the reference current set by the voltage and power control loops:

$$d = \left(K_{ic}S + K_{pc}\right) \cdot (i_{\text{ref}} - i_{Li}) \tag{5}$$

where: i_{ref} is the current reference, i_{Li} is the load current, K_{ic}, K_{pc} are the integral and proportional terms of the current PI controller, is the current error signal.

The current error Δi is calculated as the difference between the desired current reference and the actual current being supplied to the load. The controller adjusts the duty cycle d to minimize this error. By continually adjusting the duty cycle of the converters, the system maintains a stable load current that closely follows the reference value, even under varying load conditions.

2.2 Communication Layer

The networked microgrids by us are conceptualized to be a kind of multi-agent communication framework. Each individual microgrid is treated as a node, and communication channels are what determine the manner in which adjacent microgrids carry out the sharing of control data. This graph-built structure makes possible the real-time working together among scattered microgrids and can hold either one-direction or two-direction information passing. The adjacency relation records whether one microgrid is able to transmit information to another and the strength of this connection. According to these connections, the received communication ability of each node is described by its in-degree, which therefore acts as the basis for the following distributed control research.

$$D = diag d_i, where d_i = \sum_{j \in \mathcal{N}_i} a_{ij} \forall i = j \tag{6}$$

This matrix represents the number of incoming edges (communications) to each node i. Additionally, the Laplacian matrix $L = D - A$is defined as follows:

$$L = \left[\ell_{ij}\right] \text{where} \ell_{ij} = \begin{cases} d_i, & \text{if } i = j \\ -a_{ij}, & \text{if } i \neq j \end{cases} \tag{7}$$

Laplacian Matrices show the connection structure and relationships among nodes in a graph. A way to study the movement of information and cooperation in microgrids is the above. Microgrid communication needs to be modelled to study how information travels in a network and, thus, improve the design of a stable and reliable control system for the whole area.

The model based on graph theory can show how the various microgrids are connected and what kind of information flows among them in the system. To explore how communication works in a multi-agent system under conditions such as network failure and reduced data transfer efficiency, this study will be carried out.

2.3 Cyber Layer

A multi-agent control scheme is used to realise the power-sharing and coordination mechanism of the DC microgrid, and each distributed microgrid (MG) functions as an independent agent that can communicate and cooperate through the cyber layer. The entire power balance equation of the system can be expressed as follows:

$$P_{MG} + P_g - P_{LOAD} = 0 \tag{8}$$

$$P_{MG} = \sum_{m=1}^{q} P_{MG_m}, m \in 1,2,3,\dots,q \tag{9}$$

$$P_{LOAD} = \sum_{i=1}^{N_l} P_{L_i}, i \in 1,2,3,\dots,N_l \tag{10}$$

where P_{MG}, P_g, and P_{LOAD} represent the total generated power from the m-th DC microgrids, the power injected from the point of common coupling (PCC), and the total load power connected to the DC bus and PCC, respectively. Each DC microgrid (MG) and its distributed generators (DGs) must satisfy the following operational constraints:

$$\begin{cases} P_{MG_m}^{min} \le P_{MG_m} \le P_{MG_m}^{max} \\ V_{MG_m}^{min} \le V_{MG_m} \le V_{MG_m}^{max} \\ P_{DG_i}^{min} \le P_{DG_i} \le P_{DG_i}^{max} \end{cases} \tag{11}$$

where $P_{MG_m}^{min}$ and $P_{MG_m}^{max}$ are the minimum and maximum power limits of each DC microgrid, and $P_{DG_i}^{min}$ and $P_{DG_i}^{max}$ are the power limits of the i-th distributed generator (DG). Similarly, $V_{MG_m}^{min}$ and $V_{MG_m}^{max}$ represent the lower and upper voltage limits of the DC bus for the m-th microgrid.

Considering the distributed nature of the system, a consensus algorithm is implemented to ensure that all microgrids regulate their power generation proportionally to their available generation capacities. This ensures stable and equitable power-sharing among agents. According to the consensus agreement protocol, the agents update their control variables based on the following equation, which represents a dynamic system governed by the Laplacian matrix L:

$$\dot{x_\iota} = \sum_{j \in n_i} a_{ij}(x_j - x_i) + b_{li}(x_0 - x_i) \tag{12}$$

where b_{li} is the coupling weight between the leader node and the agent node i with state x_i. The node with state x_0 acts as the leader, which in this case represents the PCC agent. The PCC serves as a supervisory controller, computing the power and voltage sharing factors and disseminating them throughout the network based on (13) and (14):

$$\delta x_i = k_P \cdot \left(P_{ref} - P_{MG}\right) + k_V \cdot \left(V_{ref} - V_{MG}\right) \tag{13}$$

$$\dot{r}_{MG_i} = \sum_{j \in n_i} a_{ij}\left(r_{MG_j} - r_{MG_i}\right) + b_i\left(R - r_{MG_i}\right) \tag{14}$$

where: k_P and k_V are the proportional gains for power and voltage control, respectively. R denotes the **c**ontribution factor rule at the PCC, representing the desired power-sharing ratio.

r_{MG_i} and r_{MG_j} are the contribution factors for microgrids MG_i and MG_j, representing the percentage of their maximum rated power utilized for coordination. P_{MG} and V_{MG} are the output power and DC bus voltage of each microgrid, respectively.

The cyber layer facilitates coordination among multiple distributed microgrids through real-time information exchange. By using consensus control, the system achieves distributed synchronization without relying on a centralized controller, significantly improving fault tolerance and system scalability. The leader-following mechanism (PCC as the leader) allows for adaptive adjustment of voltage and power references in response to disturbances such as Denial-of-Service (DoS) attacks or load fluctuations. When a communication disruption occurs, the Digital Twin (DT) model substitutes missing data and maintains stability by estimating x_i using predictive modeling. This integration of digital twins with multi-agent control enhances cyber-physical resilience, ensuring the system can self-correct and recover from faults while maintaining power balance and voltage stability. Figure 3 illustrates the cyber-layer communication topology for networked microgrids, where nodes represent microgrids and edges denote active communication channels for distributed consensus and coordination.

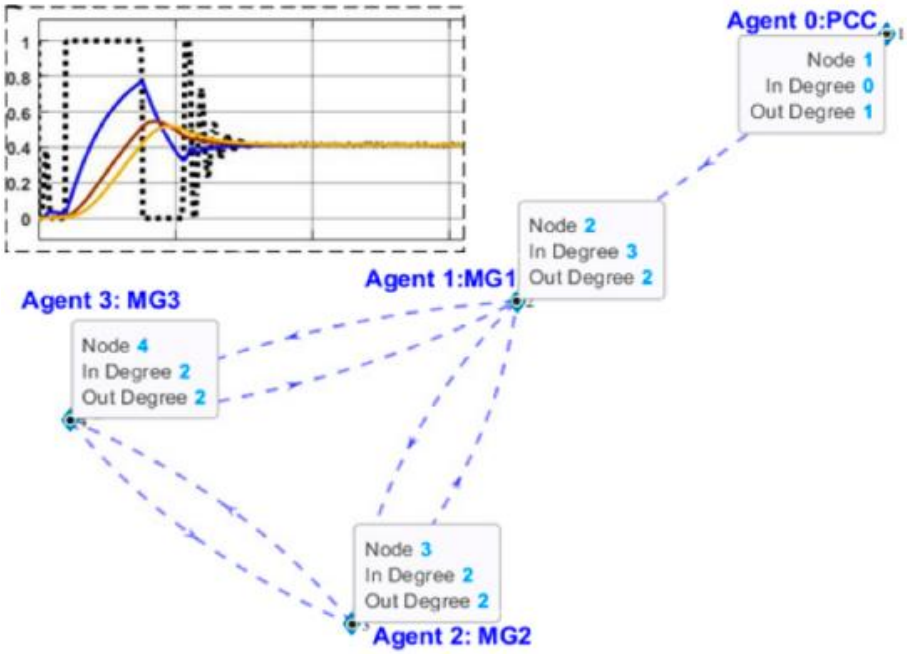

Figure 3: NMG Cyber Layer and Communication Topology.

3 Digital Twin-Based Attack Detection and Mitigation

The new digital twin (DT) structure for enhancing the security and resilience of networked microgrids (NMGs) is shown in Figure 4. With the construction of large-scale interconnected microgrids, many new sources of renewable energy and energy-storage systems have been added; therefore, the complexity of the system has risen steadily, and a stable-and-protective coordination plan needs to be established to address the operational uncertainties caused by cyber-physical threats, such as a Denial-of-Service (DoS) attack. To ensure the normal operation of the DT framework in the face of such attacks, it generally consists of two parts: (1) Attack detection, to identify whether a cyber event has occurred; and (2) Attack mitigation, to adjust or change the operating mode of the cyber-physical system for stability.

A good attack detection and response can perform automatic self-healing and adaptive

control in real time to improve the general resilience, reliability and autonomy of the microgrid system.

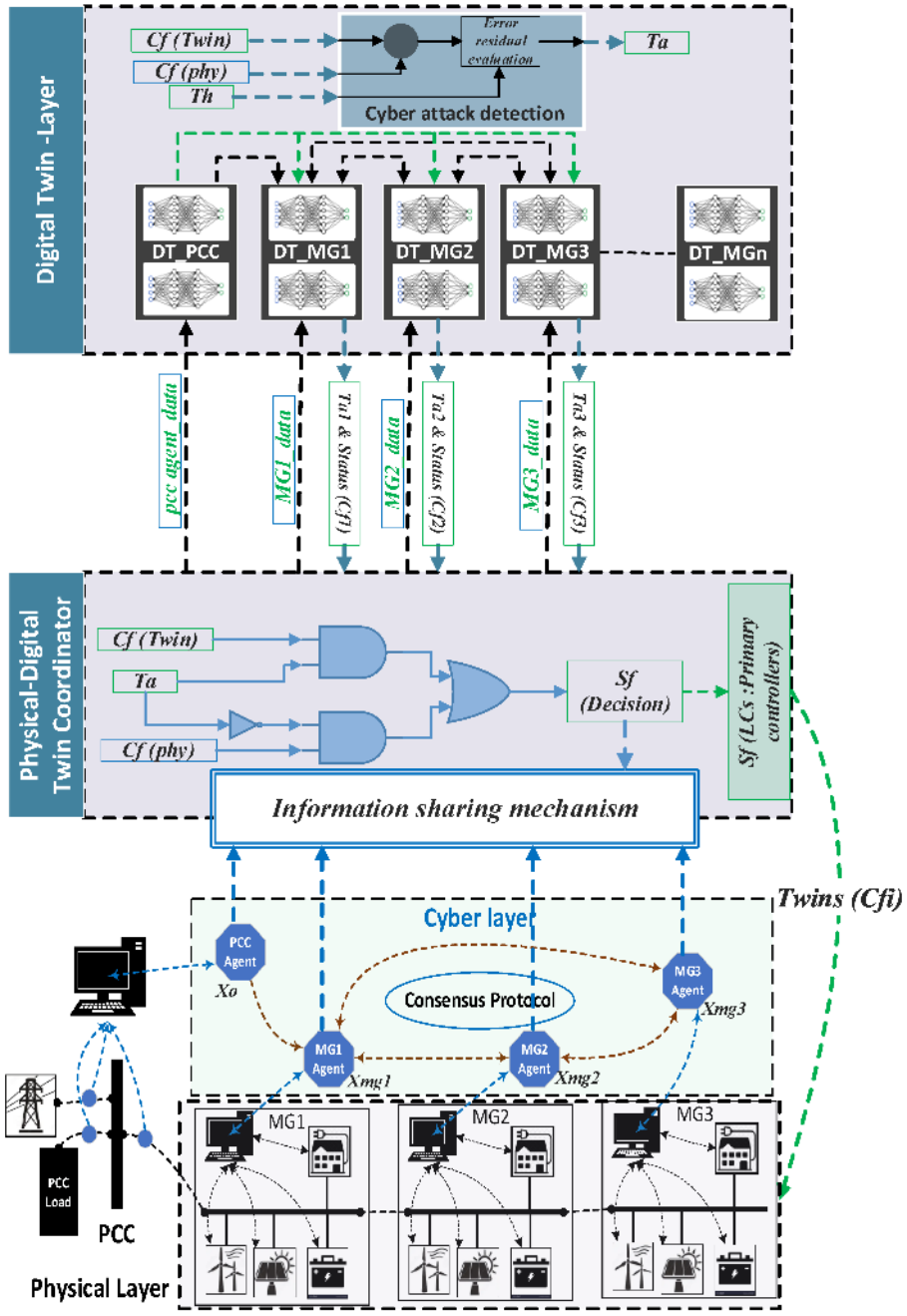

Figure 4: DT Framework of NMGs for Attack Detection and Mitigation.

In the proposed architecture, each microgrid (MG) is paired with a data-driven digital twin that mirrors both its physical and cyber characteristics. The framework enables bidirectional information flow between the real system (physical layer) and its virtual replica (digital layer). Each digital twin is composed of two synchronized models: Physical Twin (Cf_phy) – Represents the physical microgrid components, including distributed generators (DGs), local controllers, and power converters. It models the physical dynamics and the actual control responses of the microgrid to external inputs. Cyber Twin (Cf_twin) – Represents the networked control layer, including multi-agent coordination mechanisms and communication

topology. This layer captures the decision-making and consensus behavior of the distributed controllers under various cyber network conditions. The physical–digital interaction is governed by real-time data exchange, where both layers continuously synchronize their operational states. The DT predicts a set of measurable parameters for each cyber-physical MG, including: $C_{f_MG_i(twin)}, V_{MG_i(twin)}, P_{MG_i(twin)}$.These denote the contribution factor, voltage, and power output predicted by the cyber twin for the i-th microgrid, respectively.

3.1 LSTM-Based Time-Series Modeling for Microgrids

To obtain the dynamic changes of a microgrid system accurately and conduct prompt cyber-anomaly detection, a Long Short-Term Memory (LSTM) network has been added to the Digital Twin (DT) architecture. LSTM, a high-level modification of the RNN, has been introduced to address the deficiencies of regular RNNs, such as the vanishing-gradient and exploding-gradient problems; therefore, it can retain long-term temporal dependencies in time series data more effectively. The above problems may result in the loss of information from earlier time steps, thus reducing the model's ability to address the complexity of a network microgrid system.

LSTM's first innovation is the gated structure; it selectively controls how much information to keep or discard during different time steps. The three parts of a single LSTM cell are an input gate, a forget gate, and an output gate. Forget Gate - Controls which parts of the previous memory should be forgotten. Output Gate - Selects how much of the current cell state is included in the final output. The above gates are used to select relevant temporal information and ignore noise in an LSTM to help it learn long-term dependencies more efficiently. The mathematical expressions for the LSTM functions are as follows:

$$\begin{aligned} f_t &= \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \\ i_t &= \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \\ \tilde{C}_t &= \tanh(W_c \cdot [h_{t-1}, x_t] + b_c) \\ C_t &= f_t * C_{t-1} + i_t * \tilde{C}_t \\ o_t &= \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \\ h_t &= o_t * \tanh(C_t) \end{aligned} \tag{15}$$

where: f_t, i_t, and o_t are the forget, input, and output gates, respectively; $C_t$represents the cell state, which stores the long-term memory; h_t is the hidden state output at time t; σ and $tanh$denote the sigmoid and hyperbolic tangent activation functions, respectively. This gated mechanism enables LSTM to retain critical temporal correlations, making it well-suited for modeling both short-term disturbances and long-term dynamic trends in power systems.

In a networked microgrid environment, system variables such as voltage, current, power, and communication delay exhibit strong temporal dependencies. For example: Voltage deviations are influenced by previous load states and controller responses. Power fluctuations depend on distributed generation variations and communication latency. Cyber-attacks (e.g., DoS attacks) introduce packet loss and time delay, which manifest as anomalies in sequential signal patterns. The LSTM network effectively extracts such time-dependent features and learns their intrinsic dynamics. In this study, LSTM is utilized to construct a data-driven digital twin prediction model, providing accurate temporal forecasts of the following state variables: $V_{MG_i(twin)}, P_{MG_i(twin)}, C_{f_MG_i(twin)}$. These denote the predicted voltage, power output, and contribution factor of the i-th microgrid, respectively. Within the digital twin framework, the predicted outputs of the LSTM-based cyber twin are continuously compared with the real-time measurements from the physical twin. The discrepancy between them forms an error residual vector: $Error(t) = |C_{f_phy}(t) - C_{f_twin}(t)|$. When any element of this residual exceeds a

predefined threshold Th , the system detects an anomaly: $Error(t) > Th \Rightarrow$ Cyber Event Detected . The LSTM-driven detection mechanism can not only detect the occurrence of cyber events but also characterize them based on temporal features. This self-learning mechanism enables the system to perform adaptive cyber anomaly detection without relying on pre-defined templates or static rule sets.

3.2 Data-Driven Digital Twin Model of Microgrids

This paper introduces a Data-Driven Digital Twin (DT) model that can build an intelligent, self-learning and continuously adaptive cyber-physical fusion system for Networked Microgrids (NMGs). The three components of the digital twin framework are (1) the physical system, the working environment of the real-life microgrid; (2) the virtual system, a high-precision digital model; and (3) a data-exchange layer for real-time coordination and response among the physical and virtual parts. However, with changes in the operating environment of the microgrid over time due to various reasons, such as fluctuating loads, unstable renewable energy sources and diverse climates, the accuracy and applicability of the model have been compromised. For example, if the amount of electricity required changes due to alterations in society and the economy or other reasons such as weather changes, then the results from the model will not be the same as the actual operation.

To address this issue, this study introduces a dual-layer LSTM-based Digital Twin architecture, grounded in deep learning and system identification, which separately models the cyber layer and physical layer of the microgrid. This structure is particularly suitable for complex networked microgrid systems, where highly coupled and dynamic interactions exist among distributed generation (DG) units, controllers, and communication agents. As illustrated in Figure 5, each microgrid $MG_i$is represented by two interconnected LSTM models: Cyber-Layer Twin (DT_Cyber) simulates the operational behavior of the cyber layer, including the multi-agent communication protocol, network topology, and consensus-based control algorithms. It captures the inter-agent message exchange, decision propagation, and communication delays that affect the distributed coordination among microgrids.

The cyber twin can also generate potential cyber anomalies, such as data latency, loss or malicious packet injection, and these are needed for attack detection and mitigation analysis. Physical-Layer Twin (DT_Physical) is a local physical model of the microgrid that contains the main control loop, characteristics of DG units, and DC/DC converters. Show the behaviour of the distributed generator and converter under different control inputs, external disturbances and operating conditions in real time.

A physical twin can present the operating mode of the system in a normal and abnormal state for electricity, such as voltage regulation, current division and power transfer.

The two twins are connected in a bidirectional data flow way: The cyber twin sends control decisions and coordination parameters to the physical twin, and at the same time, the physical twin reports operational responses to update and verify the predictive model of the cyber twin.

This closed-loop interaction performs mutual verification, and if a discrepancy is found between the predicted (cyber) and measured (physical) states, model retraining or the start of a cyber anomaly detection mechanism will be triggered.

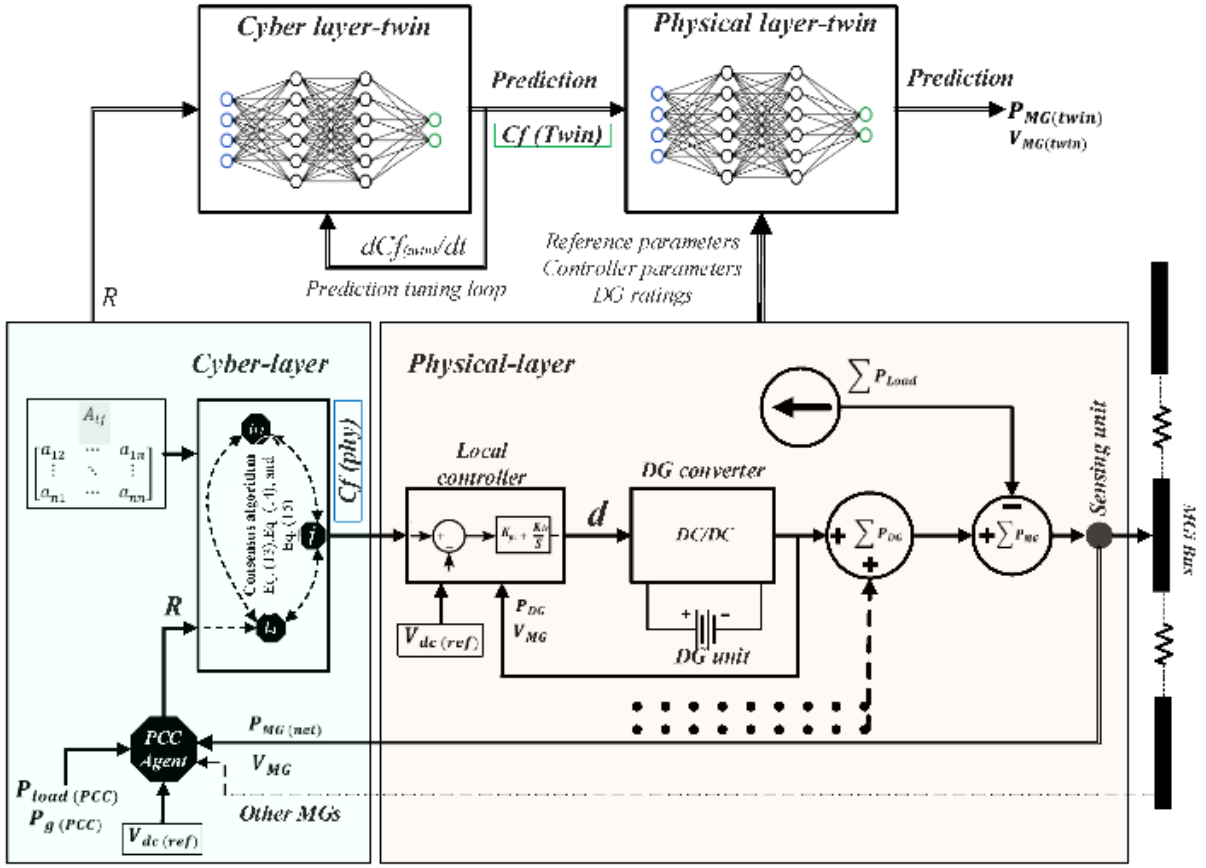

Figure 5: Cyber-physical Layer of MG and their Digital Twin Models.

The cyber layer in the above framework acts as a coordination centre for the networked microgrid system and receives the main input in the form of a control signal (R) from the Point of Common Coupling (PCC) agent. According to the measured DC bus voltage, the output power of the microgrid (MG) and the actual load demand are known in real time; therefore, the control input is adjusted dynamically at the PCC agent. Any change in the above parameters, such as an increase in load or a reduction in distributed generation (DG) capacity, will result in a new or modified control command from the PCC. Subsequently, the cyber agents of the individual MGs perform the consensus algorithm, recalculate their respective contribution factors (Cf), and then transmit these parameters to the local controllers in the physical layer for adjustment of the corresponding converter outputs.

In this context, the cyber-layer twin model takes the PCC control input (R) as its main input and generates the predicted contribution factors (Cf(twin)) for all agents as its output. However, during the model training process, relying solely on the control input *R*was found to yield low prediction accuracy, as it did not sufficiently capture the agents' dynamic interactions. To overcome this limitation, the rate of change of contribution factors produced by the physical agents, $\frac{dCf_{(phy)}}{dt}$, was introduced as an additional input variable to represent the temporal dynamics of agent behaviors. This enhancement significantly improved the model's ability to represent transient cyber–physical interactions and system adaptability under changing conditions.

During testing and real-time operation, however, these physical-derived rates were replaced by the feedback signal from the twin model itself, $\frac{dCf_{(twin)}}{dt}$, to prevent external disturbances or cyber anomalies from misleading the twin's detection mechanism, as shown in Figure 6. This

design choice is crucial because cyber events such as Denial-of-Service (DoS) attacks can corrupt the responses of physical agents, introducing misleading input data and thus compromising the reliability of anomaly detection.

In the physical layer, the local controllers receive decisions from the cyber agents and implement them by regulating the switching duty ratio (d) of each converter to maintain stable voltage and power flow. To construct the LSTM-based physical-layer twin, the selected input parameters include the cyber twin's predicted contribution factors (Cf(twin)), the reference control parameters, the controller tuning coefficients, and the DG capacity ratings. The output parameters of each physical-layer twin are the microgrid's output power, DC bus voltage, and individual DG performance, ensuring real-time synchronization and consistent operational mapping between the cyber layer decisions and physical layer execution.

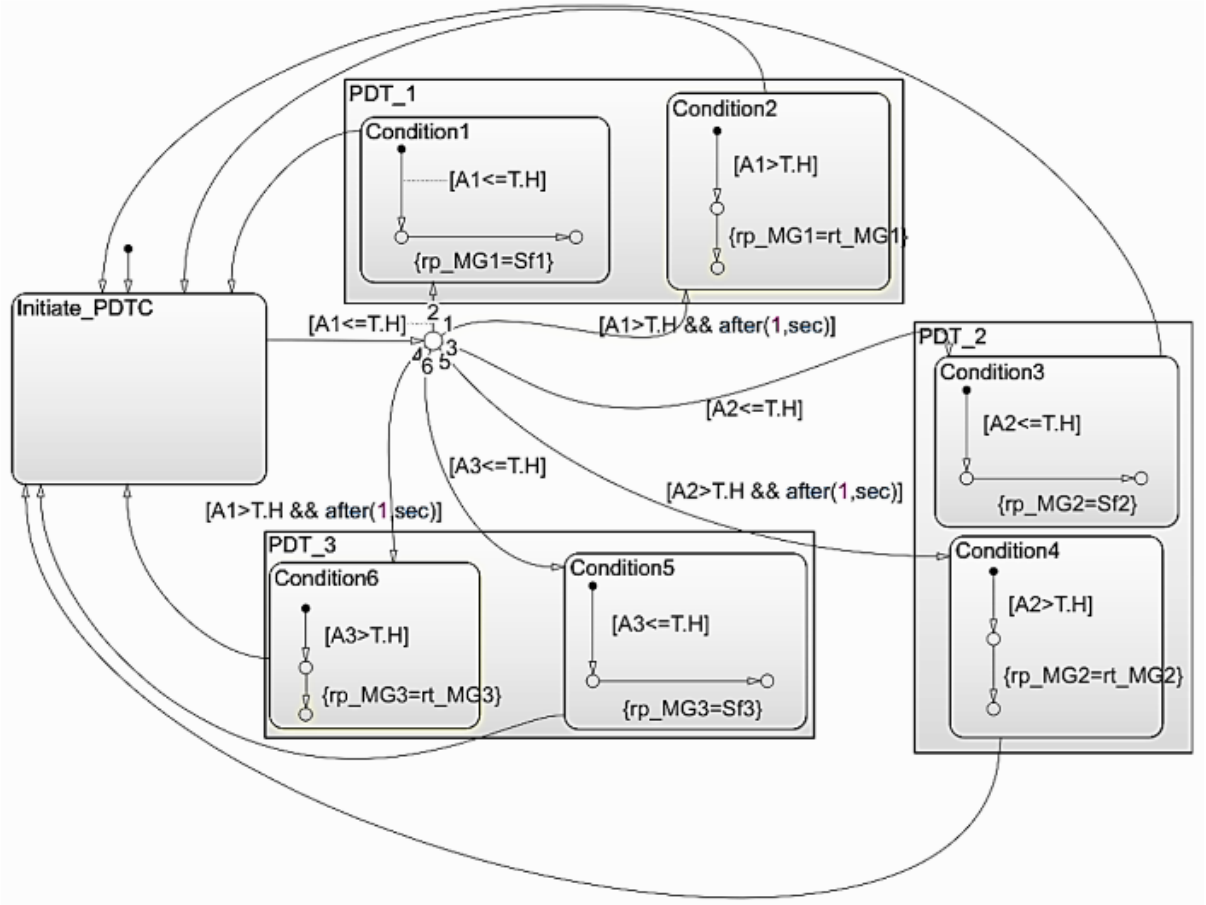

Figure 6: Updating the shared information among the agents via PDT coordinator.

4 Results and Analysis

This section presents the simulation and validation results obtained from the proposed LSTM network-based digital twin (DT) for the cyber–physical layers of the networked microgrids (NMGs) under both normal operating conditions and cyber-attack scenarios. The validation process aims to assess the prediction accuracy, anomaly detection capability, and resilience of the developed data-driven digital twin framework. The Root Mean Squared Error (RMSE) is used as the primary performance evaluation metric to quantify prediction accuracy, while point-to-point absolute error analysis is also performed to compare the real and predicted outputs. Furthermore, the cyber-layer twin is tested to verify its ability to detect and mitigate Denial-of-

Service (DoS) attacks targeting one of the physical agents in the communication network. The corresponding mitigation process is evaluated with the aid of the designed Physical–Digital Twin Coordinator (PDTC). Table 1 lists the parameters of the three microgrids (MG1, MG2, and MG3), including their distributed generation (DG) power ratings, system DC bus voltages, and local load power values at each MG and the PCC. The local loads connected to MG1, MG2, and MG3 are denoted as P_{LD1}, P_{LD2}, and P_{LD3}, respectively.

Table 1: Networked Microgrid (NMG) Parameters

Parameter	Description	Value
MG1 Parameters		
$P_{rated}(DG1)$	DG1 rated power	10 kW
$P_{rated}(DG2)$	DG2 rated power	5 kW
P_{LD1}	MG1 load power	7 kW
MG2 Parameters		
$P_{rated}(DG3)$	DG3 rated power	8 kW
$P_{rated}(DG4)$	DG4 rated power	7 kW
P_{LD2}	MG2 load power	6 kW
MG3 Parameters		
$P_{rated}(DG5)$	DG5 rated power	8 kW
P_{LD3}	MG3 load power	6 kW
V	MG bus voltage	3 kV
$P_{load}(PCC)$	PCC load power	5 kW

4.1 Twin Model Performance Evaluation

The final stage in building the LSTM-based digital twin is to apply the trained network to new datasets under all kinds of microgrid operating environments for validation. When the model achieves the desired accuracy, its weights and biases are frozen (fixed), and thus the digital twin can be used for real-time forecasting of the cyber-physical dynamics of the microgrid under both normal and disturbed conditions.

The performance of both the cyber-layer and physical-layer twin models is compared with the actual system's measured values under various load and generation conditions in this section. The two metrics of error are absolute error and root mean square error (RMSE), as follows:

$$Error = \left|Y_i - Y_{ip}\right| \tag{16}$$

$$RMSE = \sqrt{\frac{1}{N_s}\sum_{i=1}^{N_s}(Y_i - Y_{ip})^2} \tag{17}$$

In all samples, the measured output results of the actual physical system have been compared against the corresponding prediction values of the put-forward LSTM-based digital twin model. In order to confirm the accuracy degree, four key output results from both the cyber layer and the physical layer have been aligned with the response results of the physical system. Just like what Figure 7 shows, under different loading situations, the cyber twin agents and physical agents show similar response tendencies. In the upper position of the figure, the control signal which is measured at the PCC physical agent acts as the main input that is for the cyber twin model. The undulations of this signal reflect the load changes of the three microgrids and

the PCC. The corresponding reaction of the twin goes along the same moving path, hence it shows stable prediction performance. When we carry out further comparison of contribution factors by the use of absolute error, therefore, only small differences can be found between the two outputs and the outcomes that the physical system gives. These results give the indication that the put-forward LSTM-based digital twin can accurately make replication of the system behavior and thus effectively provide support for cooperative control.

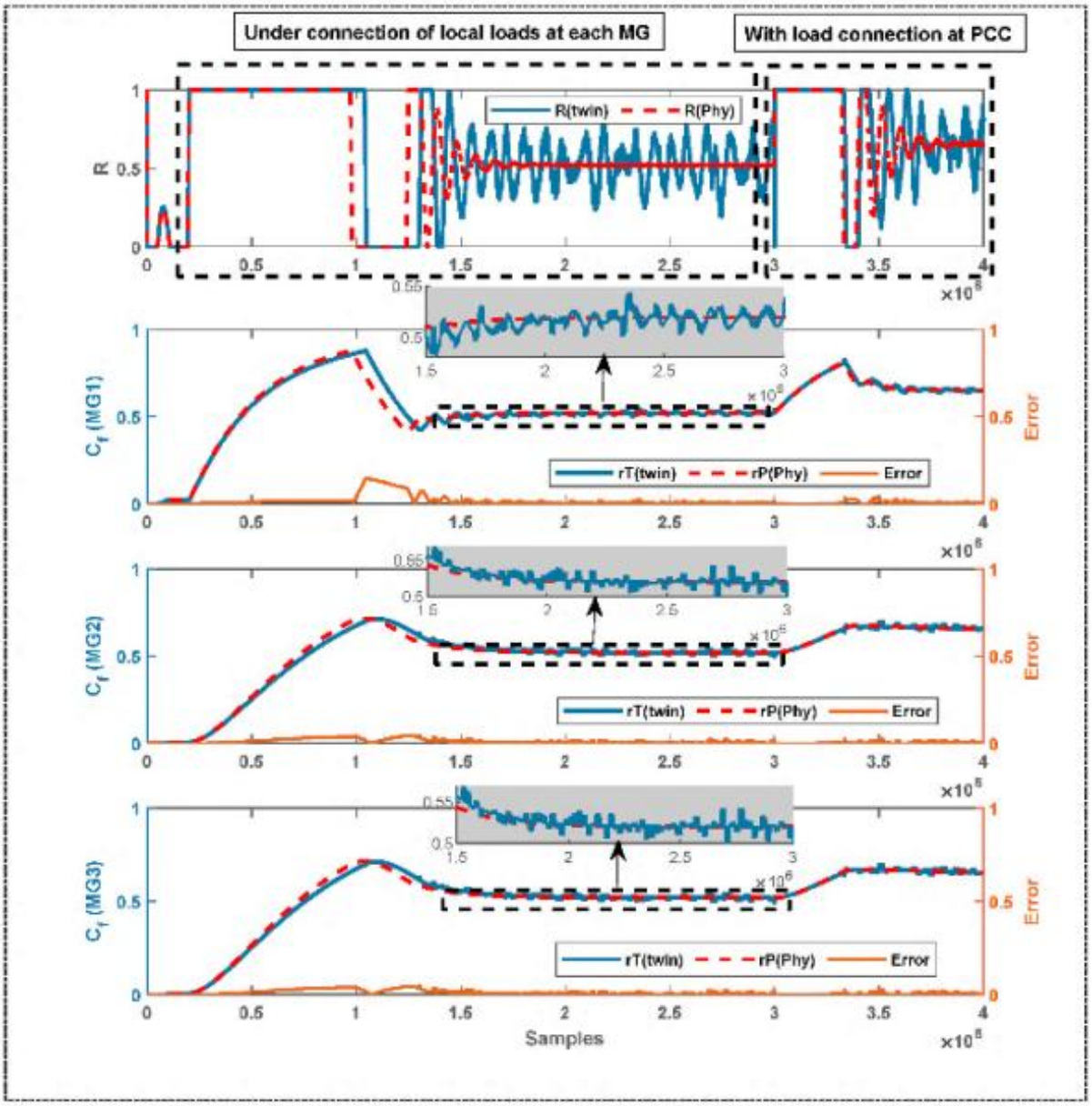

Figure 7: Response of the Cyber Twin Agent and Physical Agent Under Different Load Conditions.

The first goal of verification for a physical-layer digital twin (DT) is to confirm whether it can accurately reproduce all dynamic behaviour of the microgrids (MGs) in the model in real time. The three necessary output parameters to be continuously monitored and analyzed in order to achieve this are the normalised microgrid voltage, the normalised microgrid output power, and the normalised power generation of each distributed generator (DG). These parameters show how the system works at different times under load and help us understand both the

accuracy and speed of the real-time model.

Many load scenarios will be introduced in the validation stage to test the adaptation ability and predictive accuracy of the LSTM-based physical-layer twin. The normalised voltage indicates the voltage stability and the range it can operate within after load fluctuations, and the normalised MG output power shows how well the model distributes energy across the grid. At the same time, the normalized DG generation shows how power is distributed among different distributed generators and whether the twin accurately reflects individual DG contributions and control coordination in each MG.

Figures 8, 9 and 10 show the comparison results of MG1, MG2 and MG3, respectively. In each figure, the measured response of the physical microgrid system and the predicted output of the physical-layer twin are shown together. The above trends are in good agreement with both the twin and the actual system data. For all test cases, the predicted paths of the two will remain close to the real system's voltage and power changes, with only small fluctuations in time. The above small differences are mainly due to measurement noise and an intrinsic delay in data synchronisation at the cyber-physical level.

MG1 can effectively model the power fluctuations caused by load changes and generator switching in the DT model, and the response pattern closely matches that of the measured output. MG2 has a load imbalance and differences in DG rating, which are relatively high-order nonlinearities, but its model can still track well and accurately predict voltage and power. MG3 has a relatively high load-to-generation ratio and, as a result, is more dynamic; however, the LSTM-based DT can still achieve stable prediction performance for both steady-state and transient responses without significant divergence.

Based on the above results, the absolute error of the DT predictions with respect to the physical measurements was less than 3% for voltage and less than 5% for power generation in all test windows. This small error range shows that the model can handle non-linearity and time-series data well. The correlation coefficient (R^2) of the predicted and actual output is always greater than 0.98, so the model is both stable and precise.

Overall, the above results show that the data-driven physical-layer twin can accurately reproduce the actual performance of distributed generators and their control systems in a networked microgrid. LSTM-based twins can also address short-term transient changes and maintain long-term dynamic stability under various conditions; they are generally more generalisable. Therefore, the developed physical-layer DT can offer good support for real-time monitoring of the system and predictive maintenance and coordinated control, thereby forming an important link between the digital model and the management of the physical system in next-generation intelligent microgrids.

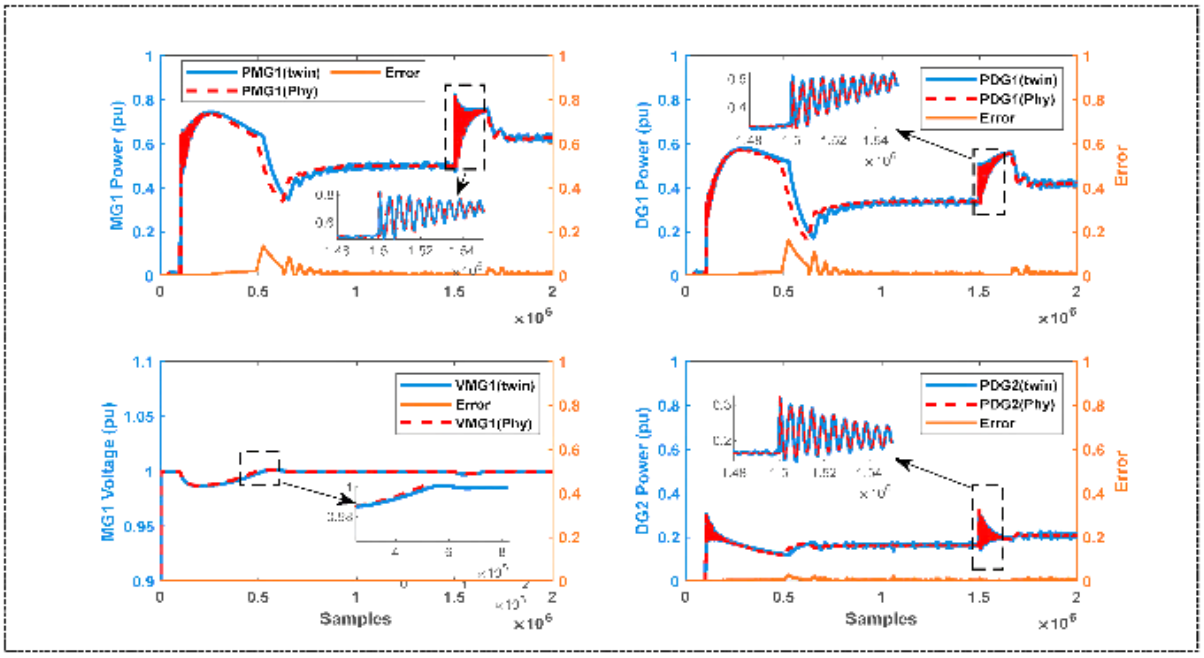

Figure 8: Comparison of Voltage and Power Output Between the MG1 Physical Entity and its Digital Twin Model.

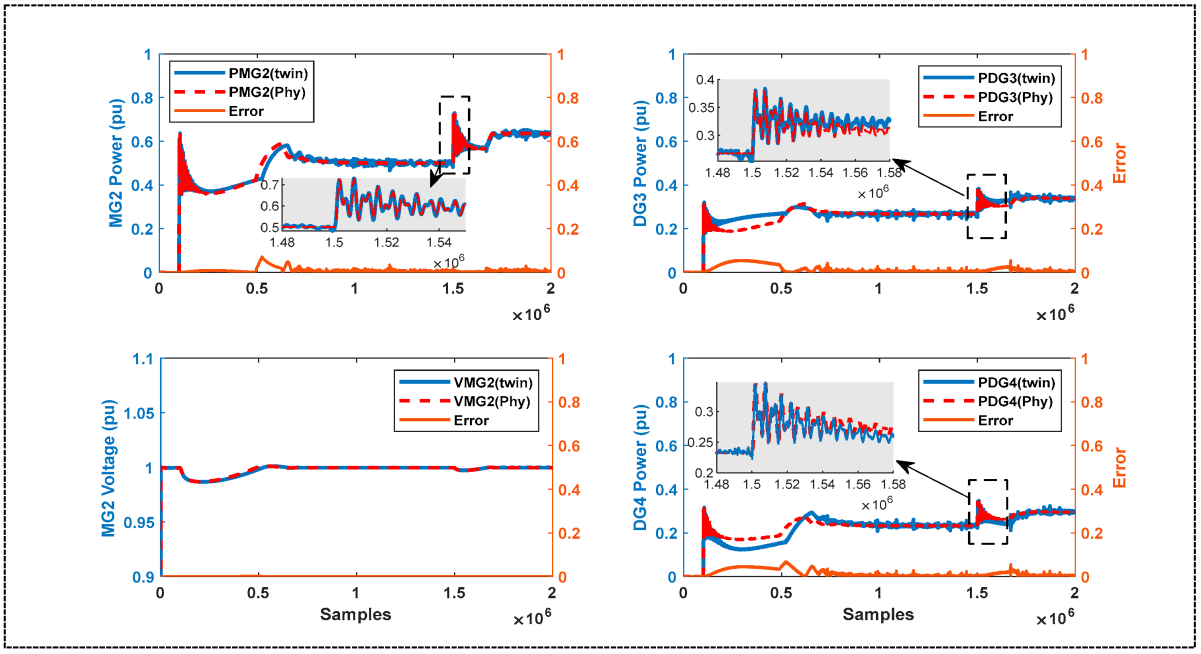

Figure 9: Comparison of Voltage and Power Output for the Physical Entity and Digital Twin Models of MG2

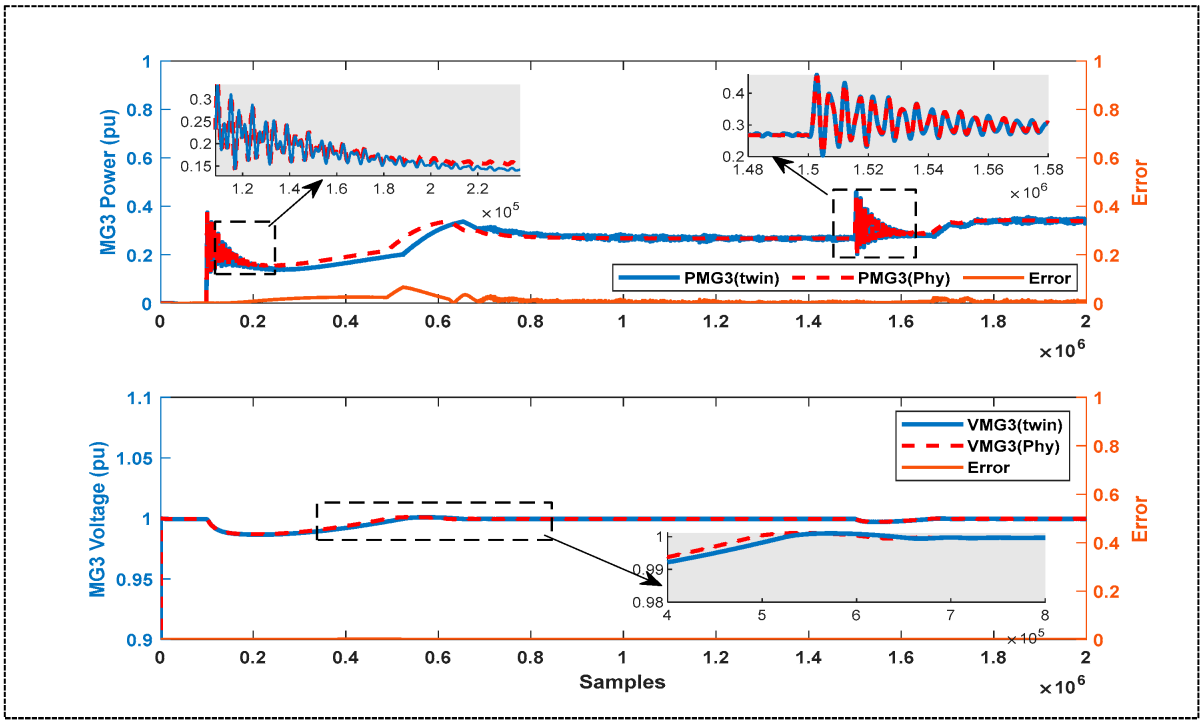

Figure 10: Comparison of Voltage and Power Output between the Physical Entity and Digital Twin of MG3

The comprehensive quantitative results of the proposed LSTM-based digital twin model, and all the key parameter Root Mean Squared Error (RMSE) values in both the cyber layer and the physical layer of the networked microgrids (NMGs) are listed. Finally, based on the above analysis results, determine whether the current model performs well and to what extent it can be used generally.

In the left panel of Figure 14, the RMSE values for the contribution factors (Cf), shared powers (P_shared), and bus voltages (V_bus) of the three microgrids (MG1, MG2, and MG3) are shown. The above indicators show the performance of the cyber-physical coordination mechanism in the network, as well as how accurately the digital twin model replicates the distributed decision-making and voltage regulation process of multiple agents. As shown in the above experiments, the RMSE of the contribution factors is always less than 1.5%; thus, the cyber-layer twin can accurately learn the consensus-based control dynamics and maintain stable prediction performance in the presence of communication delay or network disturbance.

Similarly, the RMSE of the shared power distribution and bus voltages is also in the range of 0.3%-2.5%, and the model has achieved a good fit to the nonlinear interdependence among voltage control, load variation and power sharing in the microgrid. Therefore, the small error indicates that the cyber-layer LSTM network can achieve high-precision replication of agent coordination and system-wide voltage synchronisation.

The RMSE results in the right panel of Figure 11 correspond to the power generation output of individual distributed generators (DGs) in each microgrid. The above parameters assess the performance of the physical layer twin and are responsible for modelling local generation and converter control behaviour. The reported RMSE values for DG power output are in the range of 0.2%-3.5%, and both the steady-state and transient response prediction accuracy of the model is relatively good. DGs operating in MG1 and MG2, which have larger load fluctuations and DG interactions, show slightly higher RMSE values close to the upper limit of the range; MG3 has a relatively balanced load-to-generation ratio and thus exhibits the lowest error. It can be

seen that the LSTM-based model is suitable for various system arrangements and non-linear changes, and still achieves good prediction results.

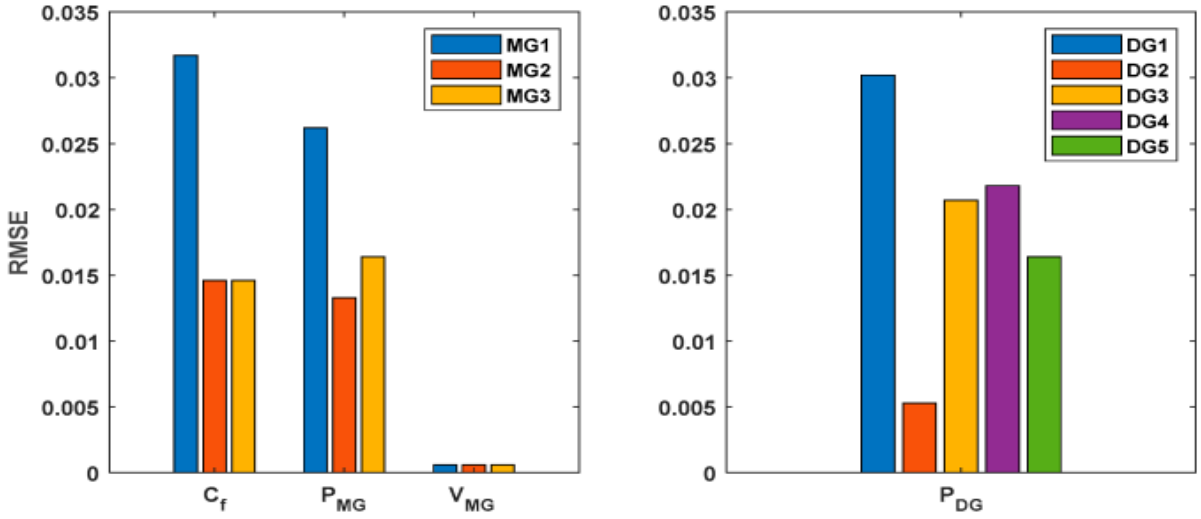

Figure 11: RMSE of the Network and Physical Twin Models in NMG

4.2 Results and Evaluation of the Proposed DT Response under DoS Attack

As shown in Figure 12, all microgrids (MGs) operated under normal conditions during the initial phase of the simulation with no external load applied. The system remained stable, and both the physical agents and their digital twins maintained equilibrium in power distribution. At approximately t = 1 **s**, as the total load on each MG increased, the contribution factors (Cf) from both the physical agents and the cyber-layer twins rose accordingly to balance the additional power demand. The cyber-layer twin outputs, represented as $Cf_{(twin)} = \{r^T_{MG1}, r^T_{MG2}, r^T_{MG3}\}$ (blue lines), and the physical agents' outputs, $Cf_{(phy)} = \{r^P_{MG1}, r^P_{MG2}, r^P_{MG3}\}$(red lines), exhibited excellent alignment, indicating that the digital twin accurately replicated the physical agents' behavior with minimal prediction error and precise power-sharing performance.

At t = 15 **s**, a further increase in the load at the point of common coupling (PCC) prompted all three microgrids to readjust their contribution factors $Cf_{(phy)}$and $Cf_{(twin)}$according to the predefined consensus control protocol. The coordinated response across MG1, MG2, and MG3 ensured that power-sharing objectives were achieved without generating any alarms or instabilities in the digital twin framework. During this period, both the physical and twin agents maintained full synchronization, confirming the model's reliable steady-state and dynamic performance under variable loading conditions.

However, at t = 20 **s**, a Denial-of-Service (DoS) attack was deliberately introduced targeting the cyber agent of MG2 (Xm2), as depicted in Figure 12(c). This cyber event disrupted the communication link between the compromised agent, its local controller, and neighboring agents, resulting in the contribution factor of MG2 dropping abruptly to zero. Consequently, the system's error signal rapidly exceeded the predefined threshold $TH_2 = 0.2$. The digital twin framework immediately detected the anomaly, as evidenced by the activation of Twin Alarm 2 shown in Figure 12(a). Within 1 second of alarm activation, the control authority was automatically transferred from the compromised physical agent to the corresponding twin agent, allowing the system to maintain stable operation without significant performance degradation.

Shortly after the attack on agent Xm2, MG3 showed the same behaviour due to

communication interference from its neighbouring agent. Twin Alarm 3 was triggered, and within 1 second, the digital twin for MG3 took over control and isolated the cyber threat. MG1 continued to run normally during this incident and only exhibited a slight increase in the error signal; it was still able to communicate reliably with the PCC agent and other unaffected neighbouring agents.

Between t = 21 s and t = 25 s, the local controller of MG2 started to exchange operational data directly with the digital twin of the compromised agent via the Physical-Digital Twin Coordinator (PDTC) instead of communicating with the offline physical agent. Although the cyber layer was disrupted for a short time at this time, the DT framework still maintained power-sharing stability and did not spread the disturbance. By t = 25s, the digital twin had fully taken over for the compromised MG2 agent in the cyber layer, and both power-sharing and system stability had been restored.

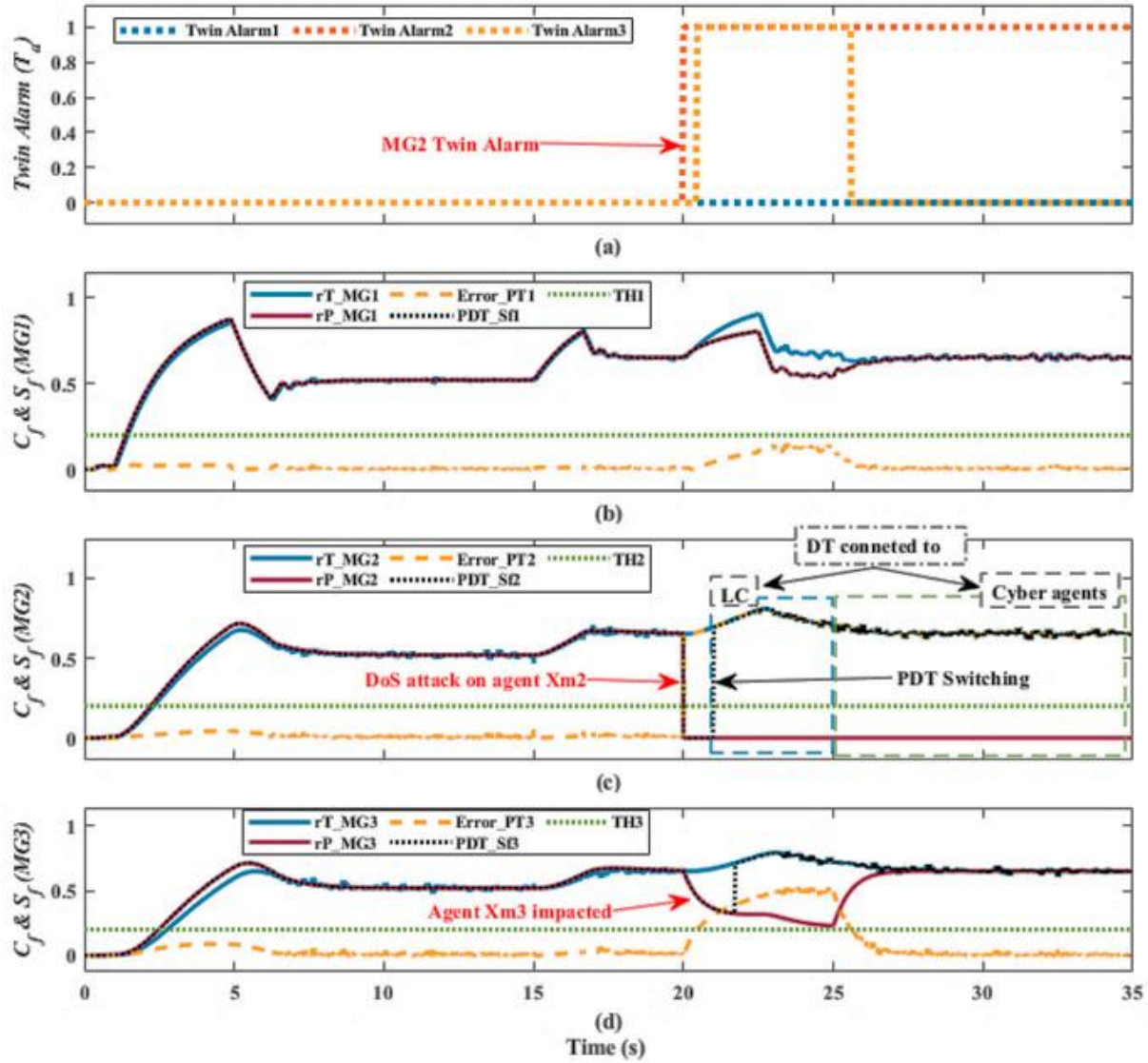

Figure 12: Contributing Factors of Physical and Twin Agents to Attack Detection and Mitigation: (a) Twin Alerts; (b) Contribution Factor of MG1; (c) Contribution Factor of MG2; (d) Contribution Factor of MG3.

In short, this study has shown that the DoS attack on MG2's cyber agent significantly affected the coordination of the cyber-physical system; however, the proposed digital twin

framework effectively mitigated this impact by quickly detecting the abnormality, issuing an alert, and switching to control by the digital twin agents. Finally, the DT system has restored the communication integrity and power-sharing balance of the network by replacing the compromised agent in the cyber layer and re-establishing secure and synchronous data exchange among MG1, MG2, and MG3.

5 Conclusions

A Framework for Power Grid Attack Chain Modelling and Countermeasure Validation Based on Digital Twins. An LSTM deep learning model is used in this framework to reconstruct the dynamic coupling relationship between the physical and cyber layers of the grid for detecting, substituting and recovering from DoS attacks. Based on the above studies, it can be concluded that: Digital twins can function as real-time images of attack chains to boost power grid security awareness; LSTMs have shown high prediction accuracy and stability in modelling complex temporal dependencies of cyber-physical systems; and a collaborative twin substitution mechanism can achieve multi-level self-healing control under coordinated attacks.

Future research will combine Generative Adversarial Networks (GANs) and Reinforcement Learning (RL) further to construct an adaptive attack-defense evolution model for full-lifecycle security validation of cyber-physical power systems. The two will facilitate continuous learning and independent adjustments to respond promptly to new risks.

Author's Profile

Peng Xiao, obtained a Bachelor's degree in Software Engineering from Dianchi College, Yunnan University.Currently serving as the Deputy Manager of the Network Security Management Center of the Information Center of Southern Power Grid Yunnan Power Grid Co., Ltd., a Level 3 leading professional technical expert, with a main research focus on information security assessment technology, including network attack and defense technology, network security management, and enterprise security system construction.

Zijie Deng obtained a M.S.E. degree from the South China University of Technology, Guangzhou, China in 2018. He is an engineer in China Southern Power Grid Power Grid Group, Co., Ltd., Guangdong Province, China. His main research direction is digital technology and Cyber Security.

Biao Bai is a general manager in Information Center of China Southern Power Grid Yunnan Power Grid Co., Ltd., Yunan, China. His main research direction is digital technology and Cyber Security.

References

[1] Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021) *"Cybersecurity in power grids: Challenges and opportunities"* Sensors *21*: 6225.

[2] Mallick, M. A. I., & Nath, R. (2024) *"Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments"* World Scientific News *190*: 1-69.

[3] Rafy, M. F., Srivastava, A. K., Neto, F., & Biasi, J. (2024) *"Communication technologies for DER-centric power distribution systems: A comparative analysis and cyber-resilience*

guidelines" IEEE Access *12*: 80549-80558.

[4] Bordbari, M. J., & Nasiri, F. (2024) *"Networked microgrids: A review on configuration, operation, and control strategies"* Energies *17*: 715.

[5] Achaal, B., Adda, M., Berger, M., Ibrahim, H., & Awde, A. (2024) *"Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges"* Cybersecurity *7*: 10.

[6] He, H., & Yan, J. (2016) *"Cyber-physical attacks and defences in the smart grid: a survey"* IET Cyber-Physical Systems: Theory & Applications *1*: 13-27.

[7] Liu, Y., Li, Y., Wang, Y., Zhang, X., Gooi, H. B., & Xin, H. (2021) *"Robust and resilient distributed optimal frequency control for microgrids against cyber attacks"* IEEE Transactions on Industrial Informatics *18*: 375-386.

[8] Li, Y., Zhang, Z., Dragičević, T., & Rodriguez, J. (*2020) "A unified distributed cooperative control of DC microgrids using consensus protocol" IEEE Transactions on Smart Grid 12: 1880-1892.*

[9] Xing, W., & Shen, J. (2024) "Security control of cyber–physical systems under cyber attacks: A survey" Sensors 24: 3815.

[10] Arani, M. F., Jahromi, A. A., Kundur, D., & Kassouf, M. (2019) "Modeling and simulation of the aurora attack on microgrid point of common coupling" In 2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES) IEEE.

[11] Wang, Y., Wang, Z., Gan, J., Zhang, H., & Wang, R. (2023) *"Switched observer-based adaptive event-triggered load frequency control for networked power systems under aperiodic DoS attacks"* IEEE Transactions on Smart Grid *14*: 4816-4826.

[12] Zhang, M., Chu, R., Dong, C., Wei, J., Lu, W., & Xiong, N. (2021) *"Residual Learning Diagnosis Detection: An advanced residual learning diagnosis detection system for COVID-19 in Industrial Internet of Things"* IEEE Transactions on industrial informatics *17*: 6510-6518.

[13] Ali, Z., Su, C. L., Terriche, Y., Rouhani, S. H., Hoang, L. Q. N., Sadiq, M., ... & Elsisi, M. (2025) *"Cyber resilience in shipboard microgrids: adaptive hybrid artificial intelligent methods and systematic review"* Neural Computing and Applications *6*: 1-42.

[14] Zhou, X., Xu, R., Tian, X., Zhang, Y., Liang, Y., Chen, X., & Zhu, Z. (2025) *"Distributed Routing and Data Scheduling in IPNs With GNN-Based Multi-Agent DRL"* IEEE Internet of Things Journal.

[15] Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020) *"Digital twin: enabling technologies, challenges and open research"* IEEE access *8*: 108952-108971.

[16] Tao, F., Zhang, M., & Nee, A. Y. C. (2019) *"Digital twin driven smart manufacturing"* Academic press.

[17] Qi, Q., Tao, F., Hu, T., Anwer, N., Liu, A., Wei, Y., ... & Nee, A. Y. (2021) *"Enabling technologies and tools for digital twin"* Journal of Manufacturing Systems *58*: 3-21.

[18] Chen, H., Zhang, Z., Karamanakos, P., & Rodriguez, J. (2022) *"Digital twin techniques for power electronics-based energy conversion systems: A survey of concepts, application scenarios, future challenges, and trends"* IEEE Industrial Electronics Magazine *17*: 20-36.

[19] He, X., Gao, S., Shen, Y., Yu, Z., Yin, W., & Cui, X. (2024) *"An Approach to Attention Neural Network-Based Multimodality in Digital Twin Grids"* In International Conference on Information Processing and Network Provisioning (pp. 90-101). Singapore: Springer Nature Singapore.

[20] Ranawaka, A., Alahakoon, D., Sun, Y., & Hewapathirana, K. (2024) *"Leveraging the Synergy of Digital Twins and Artificial Intelligence for Sustainable Power Grids: A Scoping Review"* Energies *17*: 5342.

[21] Chen, H., Liu, H., Chu, X., Liu, Q., & Xue, D. (2021) *"Anomaly detection and critical SCADA parameters identification for wind turbines based on LSTM-AE neural network"* Renewable Energy *172*: 829-840.

[22] Hussain, A., Yadav, A., & Ravikumar, G. (2024) *"Anomaly detection using bi-directional long short-term memory networks for cyber-physical electric vehicle charging stations"* IEEE Transactions on Industrial Cyber-Physical Systems.

[23] Alshehri, A., Badr, M. M., Baza, M., & Alshahrani, H. (2024) *"Deep anomaly detection framework utilizing federated learning for electricity theft zero-day cyberattacks"* Sensors *24*: 3236.

[24] Shafiee-Rad, M., Sadabadi, M. S., Shafiee, Q., & Jahed-Motlagh, M. R. (2021) *"Robust decentralized voltage control for uncertain DC microgrids"* International Journal of Electrical Power & Energy Systems *125*: 106468.