





Article

Enhancing Cyber-Physical Resiliency of Microgrid Control under Denial-of-Service Attack with Digital Twins

Mahmoud S. Abdelrahman , Ibtissam Kharchouf , Hossam M. Hussein , Mustafa Esoofally and Osama A. Mohammed * 

Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174, USA; mabde046@fiu.edu (M.S.A.); ikhar002@fiu.edu (I.K.); hhuss013@fiu.edu (H.M.H.); mesoo002@fiu.edu (M.E.)

* Correspondence: mohammed@fiu.edu; Tel.: +1-305-348-3040

Abstract: Microgrids (MGs) are the new paradigm of decentralized networks of renewable energy sources, loads, and storage devices that can operate independently or in coordination with the primary grid, incorporating significant flexibility and supply reliability. To increase reliability, traditional individual MGs can be replaced by networked microgrids (NMGs), which are more dependable. However, when it comes to operation and control, they also pose challenges for cyber security and communication reliability. Denial of service (DoS) is a common danger to DC microgrids with advanced controllers that rely on active information exchanges and has been recorded as the most frequent cause of cyber incidents. It can disrupt data transmission, leading to ineffective control and system instability. This paper proposes digital twin (DT) technology as an integrated solution, with new, advanced analytics technology using machine learning and artificial intelligence to provide simulation capabilities to predict and estimate future states. By twinning the cyber-physical dynamics of NMGs using data-driven models, DoS attacks targeting cyber-layer agents will be detected and mitigated. A long short-term memory (LSTM) model data-driven digital twin approach for DoS attack detection and mitigation is implemented, tested, and evaluated.

Keywords: smart grid; cyber-physical microgrid; digital twin; denial-of-service attack



Citation: Abdelrahman, M.S.; Kharchouf, I.; Hussein, H.M.; Esoofally, M.; Mohammed, O.A. Enhancing Cyber-Physical Resiliency of Microgrid Control under Denial-of-Service Attack with Digital Twins. *Energies* **2024**, *17*, 3927. <https://doi.org/10.3390/en17163927>

Academic Editor: Tek Tjing Lie

Received: 30 May 2024

Revised: 27 July 2024

Accepted: 28 July 2024

Published: 8 August 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Recently, electric power systems have transformed into intricately interlinked cyber-physical systems, relying significantly on sophisticated communications. This dependence stems from integrating networked physical and electronic sensing, monitoring, and control devices connected to an energy control and protection system's control center. This expansion has increased the susceptibility of power systems to numerous cyberattacks, which may have several negative repercussions and cascading failures, from the destruction of interconnected critical infrastructure to the loss of life [1]. Therefore, resilient, secure grid operation is even more critical because a disruption or loss of function could negatively impact the security and resilience of other crucial infrastructure sectors. In the near future, the number of devices owned and controlled by consumers will significantly expand as distributed energy resources (DER) become more widely used through microgrids or networked multi-microgrids [2]. However, while networked microgrids bring many advantages to future smart grids, they also pose numerous problems, including a lack of centric oversight and resilience against renewable uncertainties.

Furthermore, due to their heavy reliance on digital communication and control, the power system has become a cyber-physical power system (CPPS) with deep integration of information and physics, consequently more vulnerable to cyberattacks. The operation of microgrids is impacted by physical events and cyberattacks in the information system, or vice versa. For instance, if an attacker targets the control system by falsifying data or denying the service of an agent information, it will force the control or protection system to make a poor control decision that compromises the security of the power system [3].

Undoubtedly, the operation of power systems has been improved through proper integration and management of renewables, advanced control/protection schemes able to detect events, and reliable communication systems [4,5]. However, maintaining cyber-physical security and resilience under the rising frequency of successful cyberattacks is a significant challenge, enhanced using innovative techniques that can offer appropriate real-time or faster-than-real-time decisions. To deal with all these complex and critical challenges, we propose digital twin (DT) technology as an integrated solution that can cover every asset in the studied power system. A DT is defined as the virtual replicas or models of the physical object/thing with bidirectional real-time data flow between them [6]. These data include physical measurements, manufacturing data, operational data, and insights from analytics software. This allows the power system to enhance its operation by implementing advanced and innovative techniques to detect and mitigate physical and cyber events that target communication-based control and protection schemes.

The evolution of digitalization has gone through digital enablement, digitalization assistance, digital control and link, and cyber-physical integration [7]. The basis for DT cyber-physical interaction and data integration is created by the Internet of Things (IoT). To develop a DT for a physical or cyber asset, the following data should be collected: the asset's states, manufacturing data, and operating data. In [8], the authors examine and summarize commonly used enabling technologies and tools in the digital twin model to provide a reference for future digital twin applications and make it easier for researchers and practitioners to adopt DTs. However, digital twins are still far from reaching their full potential because of their complicated system and drawn-out procedure. DTs can offer more thorough support for decision-making on various activities by assessing current states, diagnosing historical issues, and predicting future trends [9].

To the best of our knowledge, there have been little need for more research in the power system security area, and the field has not been well examined despite growing concern about the benefits and technical problems of digital twins in power system applications. This emphasizes the importance of identifying alternative and smart countermeasures that can minimize these types of attacks when the target is a power grid system while maintaining the power system's reliability, resilience, and security. With new, advanced analytics such as machine learning and artificial intelligence, DT provides simulation capabilities to predict, optimize, and estimate future states. This strategic solution can be a fully integrated situational awareness platform for the system operator based on the digital twin shadow and the machine learning insights for cyber threat events.

This paper applies the digital twin concept to develop a DoS attack detection and mitigation approach. A digital twin is a digital simulation of a physical system that accurately calculates its characteristic outputs in real time. It could be model-based or data-driven, or a combination of both. The data-driven DT model uses a long short-term memory (LSTM) neural network in this work. The digital twin concept is relatively new for attack detection and mitigation in power systems and has yet to be applied to microgrid security. We present the modeling and validation of a digital twin approach for cyber event detection in a multi-agent control-based networked MG. The proposed approach performs DoS attack detection of each MG's agent and enhances the stability and resiliency of the overall networked microgrid system through the mitigation scheme.

2. Cyber-Physical Power System and Cyber-Attacks

Cyber-physical power systems underpin many of our society's critical infrastructures and are the backbone of economic activity. The increasing prevalence of consumer-owned and controlled devices is set to surge alongside the widespread adoption of distributed energy resources (DERs) facilitated by microgrids or networked multi-microgrids. This growth poses a resilience challenge amid uncertainties in renewable energy. Furthermore, the need for advanced communications becomes paramount. Consequently, this expansion amplifies the susceptibility of power systems to various cyber-attacks, including denial-of-service attacks. The main challenge is detecting and understanding these emerging smart

threats and system vulnerabilities linked with energy assets. This enables the development of intelligent and efficient countermeasures while ensuring the energy system's real-time operation remains reliable and secure.

2.1. Cyber-Physical System (CPS) Layers and Attack Modeling

A typical cyber-physical system (CPS) combines computational and communication components to control, protect, and manage physical assets, as shown in Figure 1. Understanding how cyber and physical components interact is critical for studying cyber-physical issues. Sensors, which establish communication with field devices such as generators and transmission lines, transmit measurements to control centers via dedicated communication protocols. The measurements $y(t)$ may encompass voltage, current, and frequency at the physical layer. These measurements undergo processing by a suite of computational protection and control algorithms operating within the control center, facilitating operational decision-making. Actuators are then given the decision $u(t)$ to alter the field devices. Figure 1 fully represents the interaction between physical and cyber layers in the CPPS.

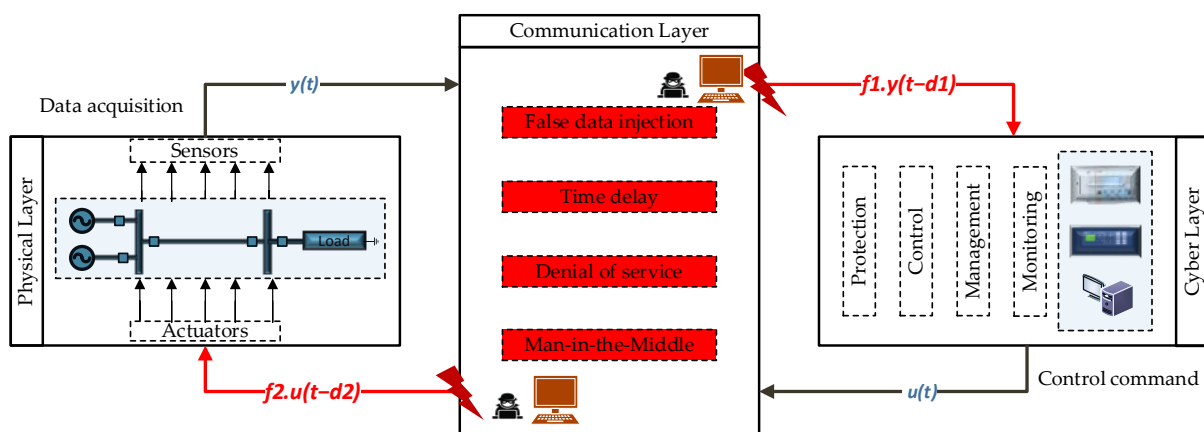


Figure 1. Cyber-physical layer data and interaction in power system.

A potential adversary could construct attack templates to modify the content of, introduce a time delay to, or deny the communication of these control/measurement signals by exploiting vulnerabilities along the communication channels. In this scenario, the sensor measurements employed as input to the control algorithm will deviate from the actual condition to $f1.y(t - d1)$. Similarly, the control decision output will be deviated from the correct one to $f2.u(t - d2)$. Given that such attacks can significantly jeopardize the security and reliability of the power system, it is imperative to research to comprehend and mitigate their effects. The impacts of these attacks can be measured in terms of load loss, frequency and voltage deviations, and their subsequent repercussions. Additionally, exploiting defenses against such attacks or strategies to mitigate their impacts will benefit from in-depth attack studies. Based on the modeling technique used, the attack can be simulated, emulated, or even the real agent [10].

2.2. Denial-of-Service Attack in Microgrids

A denial-of-service (DoS) attack happens when legitimate users are denied access to information systems, devices, or other network resources as a result of the actions of a malicious cyber threat actor. DoS has been recorded as the most frequent cause of cyber incidents. Compared with other attacks, DoS attacks are more devastating as they disrupt communication channels and cause significant delays [11]. According to several online reports and statistics, DoS attacks are common, and it is estimated that malicious hackers launch more than 7000 DoS attacks each day, with nearly 80% of electrical enterprises in 14 countries being victims of large-scale DoS attacks.

DoS attacks can target a smart grid in different sections, from generation, transmission, distribution, and consumption to control centers. DoS attacks can impede the transfer of measurement data to the control center, impact the control center's ability to update commands and delay the control signals transmitted to the actuator, ultimately degrading the operation of the power system [12]. DoS attacks can have disastrous consequences, such as a cascading blackout that could leave thousands, if not millions, of consumers without power for extended periods.

In DC MGs, the proper exchange of information significantly impacts its performance. With the complex controllers in DC MGs that rely on active information exchanges, DoS cyber-attacks can disrupt communication channels and jeopardize their stability, security, and resiliency [13,14]. DoS, also known as jamming attacks, primarily target data availability. DoS attacks aim to disrupt normal operations among networked MGs by overwhelming one or more physical agents (such as controllers, actuators, sensors, and/or communication channels) with excessive requests or data. DoS attacks with unlimited energy levels are intermittent and destabilize the system. During these attacks, the information exchange among the agents is disrupted and compromised, resulting in network topology change. Due to energy limitations, the attacker needs to enter inactive sleep intervals. Two-time sequences are needed to describe a DoS attack in the time domain: when the DoS attack occurred and the duration of each attack. Let $\Gamma_{DoS}^{(i,j)}$ be the total DoS time intervals between two agents as follows:

$$\Gamma_{DoS}^{(i,j)} = (t_1, t_2) \cap \left(\bigcup_{a=1}^{m_\mu} I_k^{(i,j)} \right) \quad (1)$$

The k th interval during which a DoS attack takes place is denoted as $I_k = [t_a, t_a + \tau_a]$, where t_a , $t_a + \tau_a$, and τ_a are the DoS attack's start time, end time, and duration, respectively. m_μ represents the number of DoS attacks that might occur during the interval $[t_1, t_2] \subset [0, \infty]$.

3. Background of Digital Twin Technology and Applications in Smart Grid

In the meantime, the Internet of Everything creates the framework for DT cyber-physical interaction and data integration. A DT essentially entails building a virtual model of a physical entity in a digital form to mimic entity behaviors, monitor ongoing status, recognize internal and external complexity, detect aberrant patterns, represent system performance, and forecast future trends. Digital twin concepts, paradigms, frameworks, applications, and technologies are increasingly debated and discussed in academic and industrial communities. The concept of a digital twin first appeared in 2003 and was proposed by Professor Grieves in the product life cycle management course at the University of Michigan. Later, the US Department of Defense introduced the concept of digital twins to issues such as the maintenance of spacecraft [15]. According to Michael Grieves in a white paper published in 2014 [16], "A Digital Twin concept model is constructed from three basic components: Physical items in real space, virtual products in virtual space, and connections of data and information that link the two together."

Using digital twins, the complexity of the real world is reduced to essential data. Because of this, the technology is welcomed by numerous industries. Twinning can be carried out within these industries on various scales, from a single component to a complete product to an operation to a system of systems. One of the most crucial and complex industries is the smart grid, with huge power generation, transmission, and distribution equipment. Figure 2a shows the three-dimensional digital twin model for the smart grid. By comparing the actual system behavior and the twinning behavior, different types of physical events and cyber-attacks can be detected and mitigated using the digital twin model, as shown in Figure 2b. In [6], the authors examine and summarize commonly used enabling technologies and tools in the digital twin model to provide a reference for future digital twin applications and make it easier for researchers and practitioners to adopt DTs. Most pertinent literature techniques discovered have been published within

the last three years, demonstrating how widespread and quickly growing DT use in smart grids is. However, because there is yet to be a common understanding of how DTs are implemented and integrated with power system applications, more efforts are still needed to comprehend and automate the operation of the grid.

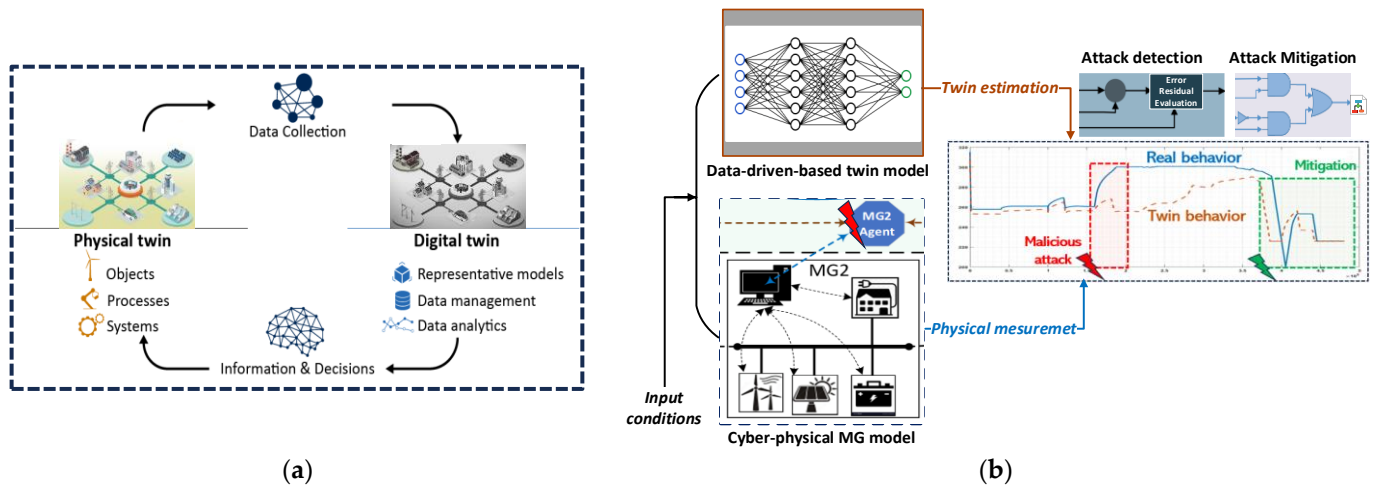


Figure 2. Digital twin model and its application in grid security: (a) three-dimensional digital twin model for smart grid; (b) microgrid security and resiliency using digital twin concept.

Regarding the use of DTs in power systems, there are different applications ranging from low-level concerns like asset model parameters to high-level coordination like microgrid power distribution. In [17], the authors proposed a transformer DT model to predict the parameters of the medium-voltage side based on the measurements received from the low-voltage side and validated with historical field data. The behavior of an induction machine was estimated in [18] using an analytical model based on an equivalent circuit. In [19], a potential DT structure that links small energy communities to the electrical grid was designed, with a brief discussion of the potential for modeling various system levels and the resulting different timescales. The multi-agent system concept was introduced to the DT system structure for control and management in power substations in [20]. Based on its autonomy, fault tolerance, and consistency, the system allows for agents to share data on a central database. In addition, DT technology offers a powerful tool that helps in microgrid design, control and management, fault diagnostics, and security [21]. The DT, which is a digital version of the physical MG, can be used in many hypothetical situations to capture the behavior observed and replicate that behavior under various normal or faulty operating conditions. As a result, necessary adjustments can be made early in the development process [22]. During MG operation, the DT can be employed as an effective tool for control and operation management that operates concurrently with the physical system [23]. The operators benefit from the DT's assistance in identifying critical operating conditions, evaluating system performance, and acting quickly to adapt to system changes. In the sense of fault diagnosis, a systematic comparison of the system's performance with the reference behavior can be used to identify instances of faulty operation. In [24], a controller-embedded DT-based diagnostics monitoring system is presented to identify anomalies in the physical subsystems of a power converter. From the aspect of grid security and resiliency, the DT can offer a platform for MG attack scenario identification and simulation. Therefore, by employing data-driven approaches or projecting the system's behavior using the DT-based simulation platform [25], it is possible to discover possible situations promptly that could result in insecure operation followed by necessary corrective measures to enhance the resiliency.

4. Proposed Multi-MGs with Multi-Agents Based Control Architecture

The microgrid concept is an efficient solution for integrating renewable energy sources and energy storage systems (ESSs). MGs operate either in islanded mode or grid-connected mode and offer increased flexibility and security of the electrical system [26]. Research into DC and AC microgrids has been intensively conducted over the past decade. DC microgrids present an appealing alternative to AC microgrids, efficiently integrating DC energy generations and loads without additional AC/DC conversion stages. In addition, DC microgrids avoid issues that exist in AC microgrids like frequency regulation, reactive power flow, and synchronization. Conventional control methods, such as droop control for DC MGs, have faced challenges, including bus voltage drop and inaccurate current sharing due to real power line impedance [27]. Therefore, hierarchical control methods have been introduced to overcome these issues and enhance system reliability, scalability, and resilience. At the secondary level, conventional centralized control strategies rely on a single central controller, which is set to collect information of each distributed generation (DG) and then provide the control signals [28]. However, centralized control strategies present several challenges due to their extensive computational requirements, inefficiency, and vulnerability to a single point of failure. Recognizing these limitations, decentralized control strategies distribute decision-making among multiple controllers or nodes, mitigating the risk of single points of failure and offering flexibility in managing diverse DERs. However, they may suffer from coordination challenges and increased communication overhead. In distributed secondary control methods, each DG communicates with only its neighboring agents, avoiding single points of failure and offering advantages in flexibility, scalability, and computing performance [29]. Figure 3 shows the cyber-physical model of three networked microgrids connected to the point of common coupling (PCC).

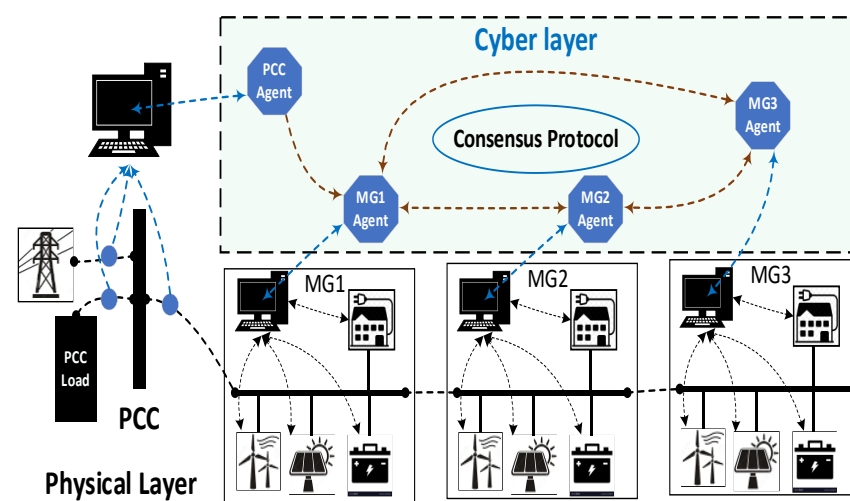


Figure 3. Cyber–physical architecture of networked MGs.

4.1. Physical Layer Modeling

An islanded DC microgrid is envisioned, featuring a comprehensive setup with multiple distributed generators (DGs). Each DG unit comprises an ideal DC voltage source, a DC/DC converter, and diverse load types. Initially, the focus is placed on a microgrid system housing two DGs, namely, DG i and DG j , interconnected via a distribution line denoted as ij , as illustrated in Figure 4. Depending on the application and voltage levels at the source and load ends, various converter types, such as boost and buck converters, may be employed within a DC microgrid. The average electrical models of buck and

boost converters are delineated in Figure 4. The dynamic equations governing the system, derived through the application of Kirchhoff’s circuit laws, are outlined as follows [30]:

$$DG_i : \begin{cases} \frac{dV_i}{dt} = \frac{1}{C_{ti}} I_{ti} - \frac{1}{C_{ti}} \hat{I}_{Li} + \frac{1}{C_{ti}} I_{ij} \\ \frac{dI_{ti}}{dt} = -\frac{1}{L_{ti}} V_i - \frac{R_{ti}}{L_{ti}} I_{Li} + \frac{d_i}{L_{ti}} V_{si} \end{cases} \quad (2)$$

where V_i signifies the voltage across the load and V_{si} stands for the voltage of the distributed generator (DG). The currents through the filter, load, and transmission line are denoted as I_{ti} , \hat{I}_{Li} , and I_{ij} , respectively. Further, d_i represents the duty cycle of the converter. The parameters L_{ti} , R_{ti} , and C_{ti} refer to the filter’s inductance, resistance, and capacitance, 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 follows:

$$Line_{ij} : \frac{dI_{ij}}{dt} = -\frac{R_{ij}}{L_{ij}} I_{ij} + \frac{1}{L_{ij}} V_j - \frac{1}{L_{ij}} V_i \quad (3)$$

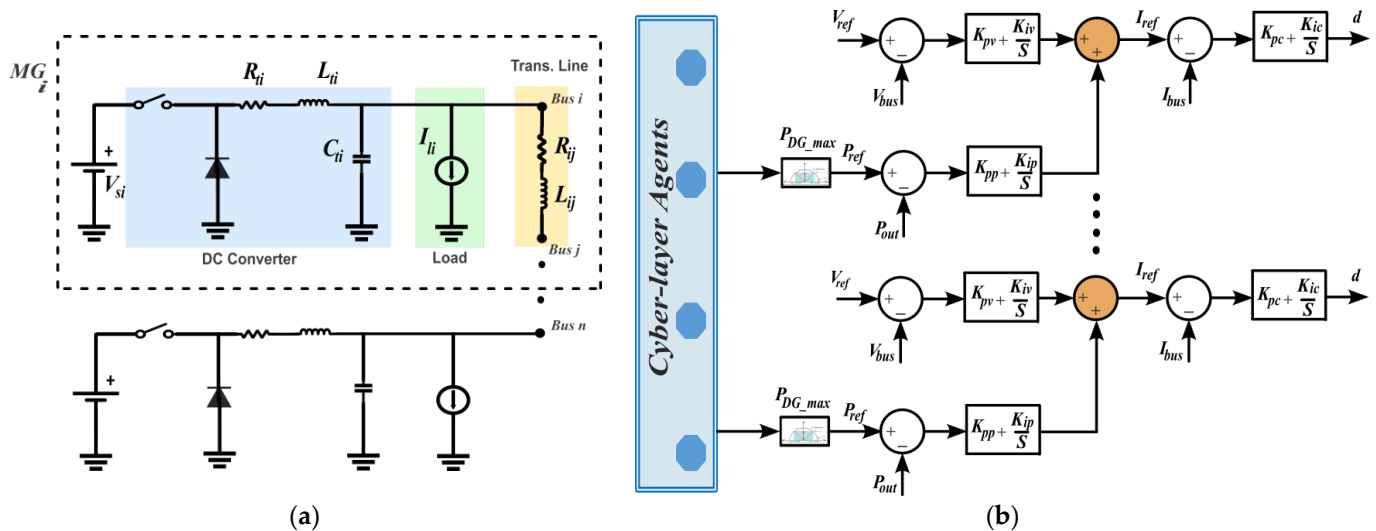


Figure 4. MG model and control: (a) equivalent circuit of DGs and loads in MG; (b) local controller in MG with cyber-layer connection.

Given that the impedance of the lines within the DC network predominantly comprises resistance, i.e., $\frac{dI_{ij}}{dt} = 0$, the line dynamic in (3) is rewritten as follows [30]:

$$I_{ij} = \frac{V_j - V_i}{R_{ij}} \quad (4)$$

The combined assets are linked to a shared DC bus via LC filters with varying parameters, forming a multi-DG and load single-bus DC microgrid. Owing to the swift dynamic reactions of converters, the system dynamics can be modeled using LC-type output filters, as described in [31].

$$\begin{cases} v_o = \frac{\sum_{j=1}^n i_j}{\sum_{j=1}^n C_j} - \frac{1}{\sum_{j=1}^n C_j} i_{load} \\ i_j = -\frac{1}{L_j} v_o - \frac{R_j}{L_j} i_j + \frac{1}{L_j} v_j, j = 1, 2, \dots, n \end{cases} \quad (5)$$

where v_o is the DC bus voltage of the system, i_{load} represents total load current, i_j stands for the inductor current of the output filter, v_j signifies the control input of the converter, and L_j , R_j , and C_j refer to the inductance, inductance resistance, and capacitance of the LC output filter j . One major control objective of this study is to ensure the output bus voltage v_o tracks

a desired output trajectory v_{ref} during steady operation. More precisely, the output voltage needs to remain within the user-defined boundary, represented as $v_{min} \leq v_o \leq v_{max}$. The parameters v_{min} and v_{max} represent the lower and upper limits of the output voltage v_o , respectively, determined based on operational requirements adhering to the $\pm 5\%$ allowable standard deviation. Additionally, the load current $i_{load} = \sum_{j=1}^n C_j$ is anticipated to be equitably distributed among n DGs according to a predefined load-sharing strategy based on the varying capacities of DGs. The local control system comprises both inner and outer control loops responsible for regulating voltage and current. Proportional–integral (PI) controllers are employed in the inner voltage and outer current control loops. The output of each control loop can be computed as follows [32]:

Voltage control loop:

$$i_{ref} = \left(\frac{K_{iv}}{S} + K_{pv} \right) \cdot \underbrace{(v_{ref} - v_{dcbus})}_{\Delta v} + \left(\frac{K_{ip}}{S} + K_{pp} \right) \cdot \underbrace{(p_{ref} - p_{out})}_{\Delta p} \quad (6)$$

Current control loop:

$$d = \left(\frac{K_{ic}}{S} + K_{pc} \right) \cdot \underbrace{(i_{ref} - i_{Li})}_{\Delta i} \quad (7)$$

where S represents the Laplace operator, d stands for the duty ratio for the pulse width modulation signal, i_{ref} denotes the current reference, $v_{dc bus}$ represents the voltage reference, $v_{dc bus}$ and i_{Li} are the measured DC bus voltage and output current, Δv and Δi are the voltage and current error signals, K_{ic} and K_{pc} are the integral and proportional terms of the current PI controller, K_{iv} and K_{pv} signify the integral and proportional terms of the voltage PI controller and K_{ip} and K_{pp} are the integral and proportional terms of the power PI controller.

4.2. Communication Layer

This section briefly overviews graph theory properties as applied to microgrids. The networked microgrids are conceptualized as a multi-agent system (MAS), with each MG acting as a communicating agent or node. At the same time, communication links represent edges forming a sparse communication network [33]. Within this network, each MG can exchange information with its neighboring MGs. A directed (one-way) or undirected (two-way) communication graph can visually depict the communication. $\mathcal{G} = (\mathcal{V}, E, A)$ represents the graph, where $\mathcal{V} = \{v_1, v_2, \dots, v_N\}$ is a set of \mathcal{N} nodes, $E \subseteq \mathcal{V} \times \mathcal{V}$ is a set of edges, and $A \triangleq [a_{ij}] \in \mathbb{R}^{N \times N}$ is the adjacency matrix. The edge (v_j, v_i) indicates that node j transmits information to node i , with a weight of edge $a_{ij} > 0$ if $(v_j, v_i) \in E$; otherwise, $a_{ij} = 0$. Each node in a graph possesses an in-degree matrix $D \triangleq \text{diag}\{d_i\}$, where $d_i \triangleq \sum_{j \in \mathcal{N}_i} a_{ij} \forall i = j$. Additionally, the Laplacian matrix $L \triangleq D - A$ is defined as follows:

$$L \triangleq [\uparrow_{ij}] \quad \text{where} \quad \uparrow_{ij} \triangleq \begin{cases} d_i = \sum_{j \in \mathcal{N}_i} a_{ij} & \forall i = j \\ -a_{ij} & \forall i \neq j \end{cases} \quad (8)$$

4.3. Cyber Layer

The DC microgrid's power-sharing system depends heavily on the multi-agent control scheme. The power balance criteria are as follows:

$$P_{MG} + P_g - P_{LOAD} = 0 \quad (9)$$

$$P_{MG} = \sum_{m=1}^q P_{MG_m}, m \in 1, 2, 3, \dots, q \tag{10}$$

$$P_{LOAD} = \sum_{i=1}^{NI} P_{Li}, i \in 1, 2, 3, \dots, NI \tag{11}$$

where P_{MG} , P_g , and P_{LOAD} are the generation power from the m DC MGs, the power generated from the PCC, and the total load (NI) power connected to the DC buses and the PCC. The power constraints for each DCMG and the connected DGs are as follows:

$$\begin{cases} P_{MG_m}^{min} \leq P_{MG_m} \leq P_{MG_m}^{max} \\ V_{MG_m}^{min} \leq V_{MG_m} \leq V_{MG_m}^{max} \\ P_{DG_i}^{min} \leq P_{DG_i} \leq P_{DG_i}^{max} \end{cases} \tag{12}$$

where $P_{MG_m}^{min}$ and $P_{MG_m}^{max}$ are the minimum and maximum power limits of each DC MG, respectively. $P_{DG_i}^{min}$ and $P_{DG_i}^{max}$ are the power limits of the i th DG. The parameters $V_{MG_m}^{min}$ and $V_{MG_m}^{max}$ represent the lower and upper limits of the DC bus voltage for the m th MG. Considering these factors, a consensus algorithm is formulated to ensure that the microgrids generate their output power relative to the maximum capacities of their distributed generators (DGs) [34]. According to the consensus agreement protocol, the agents implement the following equation to solve the agreement problem, which is equivalent to the dynamical system $\dot{x} = u$ and $u = -Lx$:

$$\dot{x}_i = \sum_{j \in n} a_{ij}(x_j - x_i) + b_i(x_0 - x_i) \tag{13}$$

where b_i is the weight of the edge between the leader and an agent with the state x_i . The node with the state x_0 is called the leader, which is the PCC agent in this work. The PCC agent calculates the sharing factor and propagates as follows in (14) and (15):

$$\delta x_i = k_p \cdot \underbrace{(P_{ref} - P_{MG})}_{\Delta p} + k_v \cdot \underbrace{(V_{ref} - V_{MG})}_{\Delta v} \tag{14}$$

$$\dot{r}_{MGi} = \sum_{j \in n} a_{ij}(r_{MGj} - r_{MGi}) + b_i(R - r_{MGi}) \tag{15}$$

where k_p and k_v are the proportional gain of the power and voltage control. The contribution factor rule at the PCC is R , while r_{MGi} and r_{MGj} are the contribution factors at MG_i and MG_j , which is defined as the percentage of the maximum rating power available at each MG. P_{MG} and V_{MG} are the sharing power and bus voltage for each microgrid, respectively. Figure 5 shows the NMG cyber layer with the communication topology.

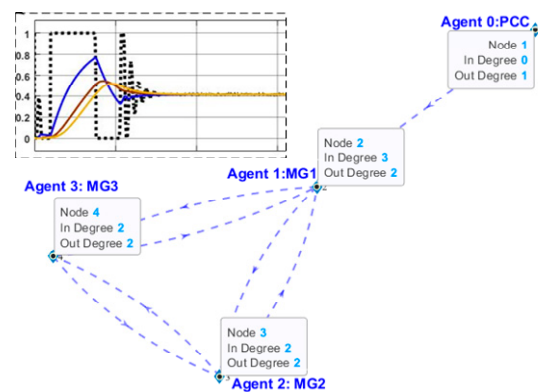


Figure 5. NMG cyber layer with communication topology.

5. Digital Twin-Based Attack Detection and Mitigation

The proposed framework for using a DT to enhance the security of microgrids and increase resiliency is shown in Figure 6. In networked microgrids, the complexity comes

from integrating different types of renewable resources and energy storage, which require proper control and protection to mitigate uncertainty, especially under physical or cyber threats. Strategies for attack detection have been explored to improve the security and cyber tolerance of complex systems. To ensure a resilient operation of the microgrids under a DoS attack, the DT comprises two functions: (1) attack detection, which is a binary decision on the occurrence of a cyber event, and (2) attack mitigation, which is the process of either adjusting the cyber-physical system’s operation or replacing functions. The successful detection and mitigation in the microgrid system enable online attack remediation, increasing the system’s resiliency and reliability.

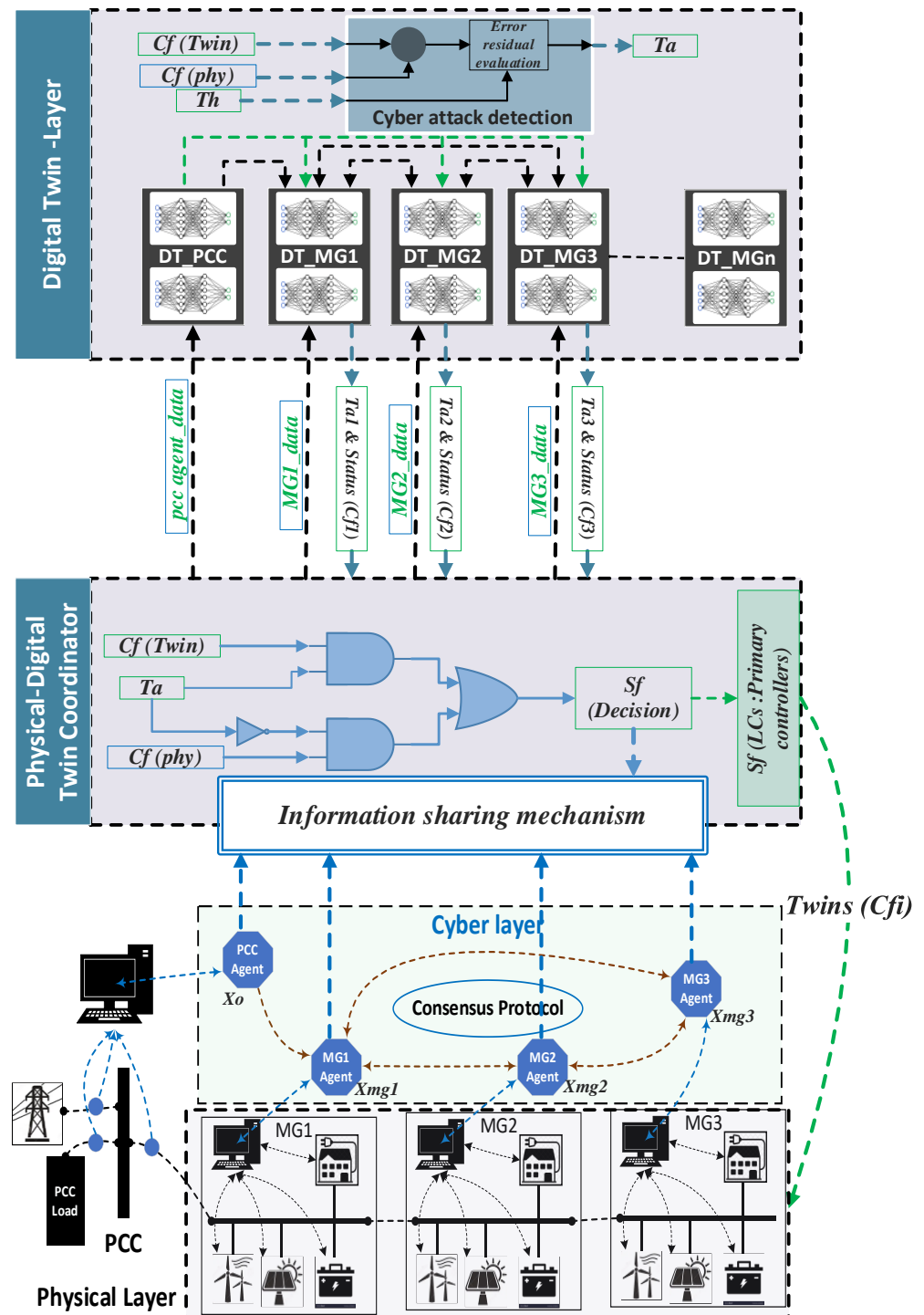


Figure 6. DT framework of NMGs for attack detection and mitigation.

A data-driven-based digital twin is developed for each MG, including the physical, and cyber layers. The digital and physical twins' outputs are compared to generate an error residual vector, producing alarms if one of these residual errors exceeds a specific threshold. Each microgrid (MG) is twined with two models: (1) the first model embodies the physical layer of each MG, encompassing the local controller response and the behavior of physical components; (2) the second model simulates the cyber layer, incorporating multi-agent control and communication network topology. The set of predicted parameters from the data-driven-based digital twin of each cyber-physical MG is $C_{f_MGi(twin)}$, $V_{MGi(twin)}$, and $P_{MGi(twin)}$. In this work, the focus is on detecting and mitigating the DoS attack on the multi-agent control in the cyber layer. Therefore, the contribution factors generated from the cyber twin layer $C_{f_MGi(twin)}$ are considered in this work as the reference behavior of the twin agent. Hence, any observed deviation in the contribution factor generated by the physical agent from the contribution factor predicted by the twin agent indicates a cyber event (cyber-attack). Accordingly, the three main elements of the cyber-attack detection and mitigation approach are (1) a digital twin, which estimates the measurable characteristic outputs $C_{f_twin}(t)$ of each MG in real time; (2) an error residual vector $Error(t)$, which is the difference between the estimated outputs and the measured outputs $C_{f_phy}(t)$, and an alarm methodology, which triggers alarm $Ta = [Ta_1 Ta_2 Ta_3]$ for attack detection in MG1, MG2, or MG3 based on comparing the $Error(t)$ with a threshold Th ; and (3) a physical–digital twin coordinator (PDTC) for obtaining the appropriate decision for attack mitigation. These elements are described in detail in the subsequent sections.

5.1. Black-Box Model of Microgrids Based on LSTM

Over the years, considerable effort has been made to understand the dynamics of microgrids and describe them using complex models. Modeling a system can be approached in two ways: (i) the physics-based approach and (ii) the empirical/data-driven approach. A physics-based model, often called the first principle or white-box model, is used when detailed system physics is available. This approach uses mathematical equations to establish model dynamics. Creating an accurate mathematical model of a complicated power system (MGs) is difficult due to the nonlinear structure of components and their relationships. Therefore, establishing a digital twin using model-based approaches is challenging [35]. The empirical or data-driven approach, sometimes called the black-box model, uses data to demonstrate a statistical correlation between input and output variables, thereby explaining microgrid behavior. System identification and neural networks are two widely used data-driven modeling methodologies.

A long short-term memory (LSTM) network is a sophisticated type of recurrent neural network (RNN) utilized in deep learning. Traditional RNNs suffer from a significant limitation known as vanishing gradients, where the network parameters primarily capture short-term dependencies, causing information from earlier time steps to diminish. Additionally, the problem of exploding gradients can occur, leading to drastic increases in error with each time step.

LSTM networks are designed to address the vanishing gradient problem through gates that selectively retain pertinent information and discard irrelevant data. This mechanism allows LSTM networks to maintain lower sensitivity to time gaps, making them more effective than simple RNNs for analyzing sequential data. Consequently, LSTMs excel in learning, processing, and classifying sequential information [36]. The cell state is crucial in long short-term memory (LSTM) networks because it permeates every neural network (NN) link. This unique feature enables LSTMs to retain information across extended sequences, allowing data to flow freely along the cell state for as long as necessary. The movement of information into and out of the cell state is regulated by specialized units known as gates. As illustrated in Figure 7, the LSTM cell consists of an input gate i_t , a forget gate f_t , an output gate o_t , and a memory cell with two outputs: the long-term state c_t and the short-term state h_t . The input gate determines the extent to which the current input data should be saved to the cell state; the forget gate decides how much of the previous unit

state should be retained for the current moment; and the output gate controls the amount of the current cell state that should be passed on to the current output value [30].

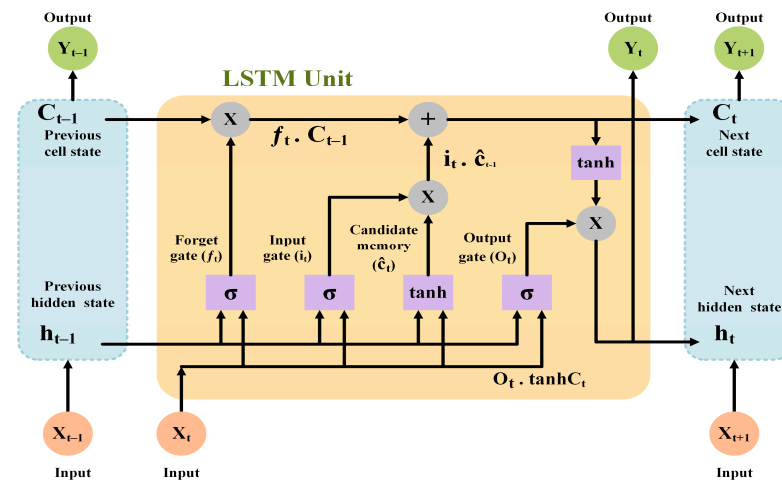


Figure 7. Long short-term memory (LSTM) architecture.

To grasp the functioning of the LSTM, let us begin with the input signal x_t . It is important to note that h_{t-1} and c_{t-1} are inputs from the LSTM at the previous timestep. Usually, the input signal x_t comprises a sequence of features extracted from the time series of sensor measurements. The forget gate f_t governs the removal of information from the previous long-term state c_{t-1} as follows:

$$f_t = \sigma_g(W_f \times x_t + U_f \times h_{t-1} + b_f) \quad (16)$$

Following that, the input gate i_t regulates which values are to be updated. Subsequently, a hyperbolic tangent (\tanh) function generates a vector of new candidate values, c'_t , that could potentially be incorporated into the following state [35]:

$$i_t = \sigma_g(W_i \times x_t + U_i \times h_{t-1} + b_i) \quad (17)$$

$$c'_t = \sigma_c(W_c \times x_t + U_c \times h_{t-1} + b_c) \quad (18)$$

$$c_t = f_t \cdot c_{t-1} + i_t \cdot c'_t \quad (19)$$

The output gate o_t governs the creation of the current short-term state h_t using information from the current long-term state c_t . Thus, the output o_t is calculated as follows [37]:

$$o_t = \sigma_g(W_o \times x_t + U_o \times h_{t-1} + b_o) \quad (20)$$

$$h_t = o_t \cdot \sigma_c(c_t) \quad (21)$$

The dot (\cdot) and addition ($+$) operators employed in Equations (4) and (6) represent the Hadamard product or element-wise product. Additionally, W_f , W_i , W_o , W_c , U_f , U_i , U_o , and U_c denote the weight matrices while b_f , b_i , b_o , and b_c signify biases that are time-independent variables. Finally, σ_g and σ_c represent sigmoid and \tanh functions, respectively [38].

5.2. Data-Driven Digital Twin Model of Microgrids

The digital twinning framework comprises three essential components: the physical system, the virtual system, and the data exchange between these two entities. Constructing a digital twin involves integrating high-fidelity models with diverse data sources, including sensor readings, historical records, technical specifications, and maintenance logs. These data enable the development of accurate models of the physical system, ensuring a realistic

and up-to-date representation of its operational state for analysis and decision-making. However, maintaining model accuracy poses a significant challenge due to the dynamic nature of operating conditions and environmental factors. For example, in microgrids, shifts in power consumption patterns stemming from socioeconomic changes, weather variations, and technological advancements can lead to disparities between modeled and actual system outputs [39]. Addressing this challenge necessitates continuous model updates to reflect evolving conditions accurately. The LSTM model offers a solution by capturing complex phenomena and leveraging extensive historical data that are difficult to incorporate into physics-based models. LSTMs have become indispensable because they can handle sequential data, establish connections across distant events within time series, and retain longer-term patterns. As research in this field progresses, leveraging AI for the analysis of longitudinal data, the significance of LSTMs is expected to escalate further.

Based on substantial research into deep neural networks (DNNs), it is clear that the deep learning framework has significant potential as a viable alternative to traditional modeling and control methodologies, particularly in circumstances with a limited understanding of system dynamics. To the author's knowledge, there has been no prior research on implementing a time-series LSTM network-based digital twin for complex cyber-physical networked microgrids. In this work, the digital twin of a cyber-physical MG using an LSTM network is presented, with more focus on the cyber twin model. As shown in Figure 8, each MG will be twinned by two connected LSTM models: (1) a cyber-layer twin, which simulates the cyber-layer asset behavior, including the multi-agent communication protocol, communication topology, and output control decisions; (2) physical-layer twin, which includes the local (primary) controller behavior, DG unit operation, and the DC/DC converter. The physical-layer twin's correct response reflects the cyber-layer twin's proper modeling. Therefore, this response will be used for performance evaluation of the model. However, for attack detection and mitigation, the cyber-layer twin features output of each MG will be used without consideration of the physical-layer twin.

In the cyber layer, the primary input is the data and control input (R) from the PCC agent. The PCC agent calculates this control input based on the measured DC bus voltage, MG output power, and load requirements. Any change in one of these parameters, such as load increase or DG capacity decrease, leads to a new or updated control signal. Accordingly, the cyber agents calculate the contribution factors based on the consensus protocol of each MG and send these parameters to the local controllers to adjust the associated converter output. In this regard, the cyber-layer twin input parameters are the control input R from the PCC agent, and the expected output parameters are $C_f(twin)$ for the three agents. However, in the training stage, relying only on one input showed low accuracy in the model. To solve this problem, the rate of change of the contribution factors produced by the physical agents $dC_f(phy)/dt$ are used as an additional input to reflect the agent dynamics. Nevertheless, during the testing and operation of the twin model with the physical system, these inputs were replaced by the feedback loop from the twin model $dC_f(twin)/dt$ as shown in Figure 9. This is because cyber events such as the DoS attack in this work will impact the behavior of the physical agents; consequently, they will mislead the twin model and impact the detection mechanism. In the physical layer, the local controllers receive the cyber agents' decisions to actuate the outputs based on the converters' calculated switching duties (d). To create the LSTM model of the physical layer, the input parameters considered in this work are the cyber twin's calculated $C_f(twin)$, reference parameters, controller parameters, and DG ratings. The output parameters of each physical-layer twin are MG output power, MG voltage, and DG output.

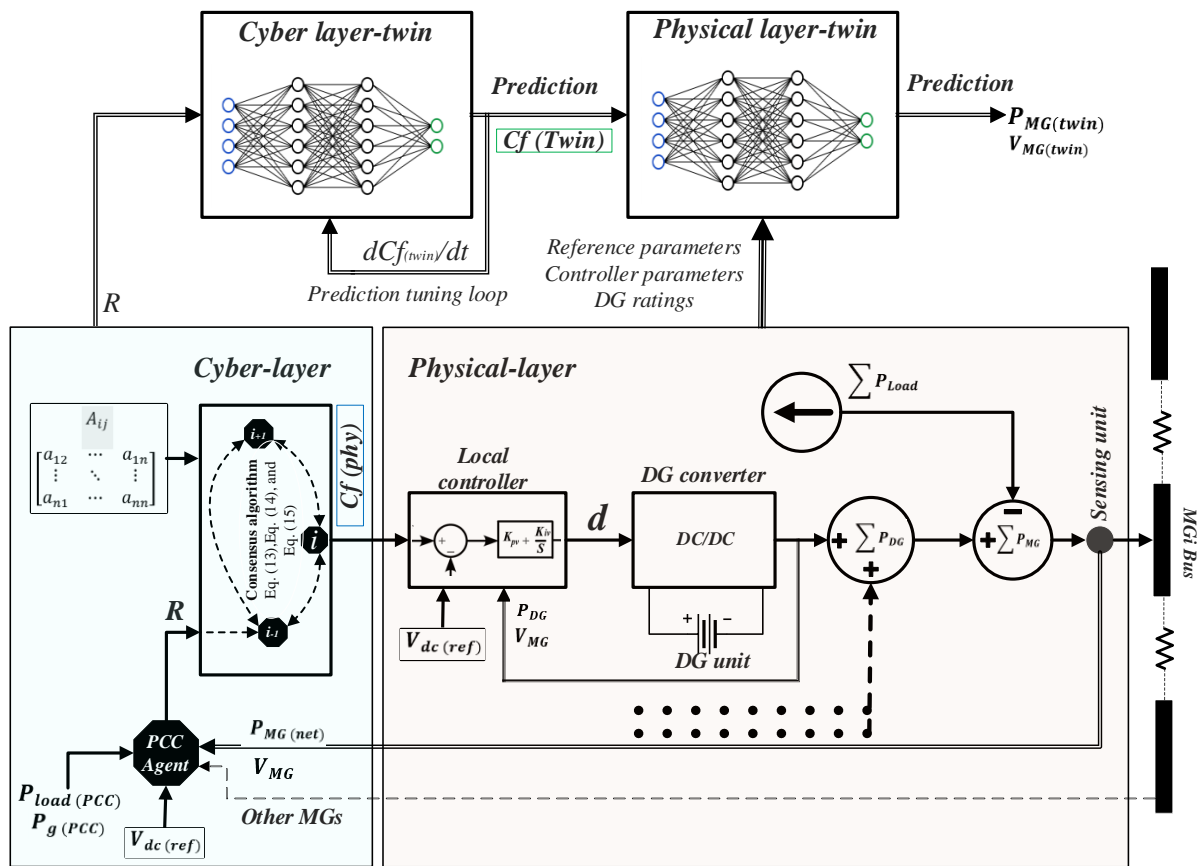


Figure 8. Cyber–physical layer of the MG and their digital twin models.

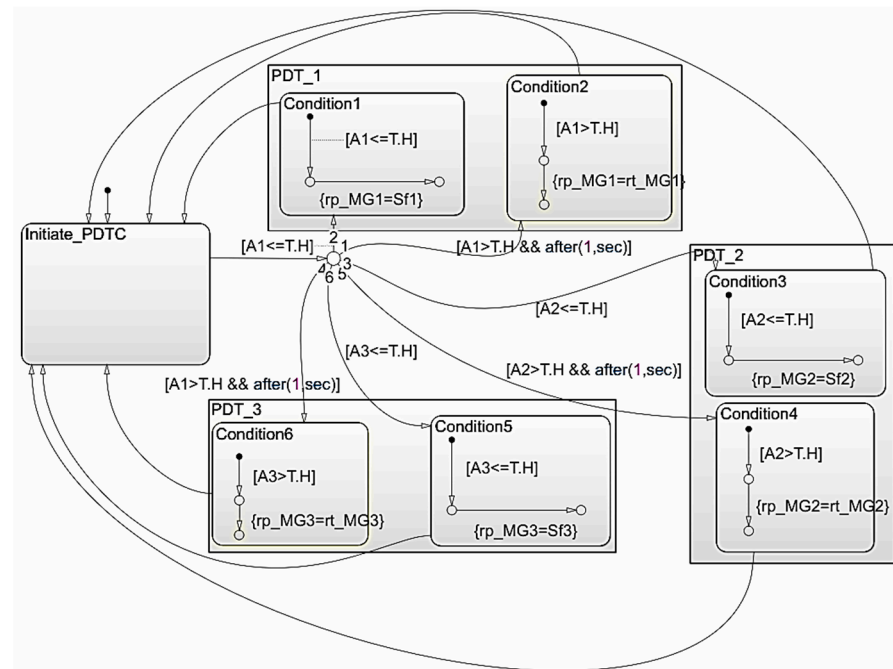


Figure 9. Updating the shared information among the agents using PDT coordinator.

5.3. Training and Learning

Creating a digital twin begins with acquiring large-scale datasets that cover the whole operational range of the system through several runs. To capture the complicated nonlinear dynamics of microgrid parameters, input parameters are mapped to output parameters

using a deep neural network. A deep neural network (DNN) consists of numerous layers of LSTM cells trained by modifying hyperparameters to minimize the error between experimental and predicted output measurements across large datasets. The first step in this phase is data collection and normalization. This dataset was acquired through multiple runs using various input parameters that covered all operational scenarios using MATLAB/SIMULINK (2023a) runs, intending to predict the output parameters of both cyber and physical layers of each MG. Each run lasts approximately 20 min, and the data are logged at 100 milliseconds. Various load conditions have been considered by varying the loads at each MG or changing the load requirements at the PCC point, and the MG input/output data are logged. The assumption is that the PCC agent is running in an ideal condition without any impact of cyber-attacks or physical events, and no malfunction occurs during the data collection process in training and testing. The features of the MG parameters selected for building the twin model are expressed in different units. Therefore, the digitized measurements from the MG model are normalized and prepared as input vectors to the LSTM network. The framework of the standard LSTM neural network model is built using Python 3.12.3. This work uses the ADAM optimizer to train the LSTM neural network model, and ReLU activation function and it utilizes MSE as the loss function. The LSTM neural network is trained over 10 million pieces of datum with the length of the time sequence as $t = 20$ s. The pre-processed data are partitioned into two sets: 60% of the data are featured randomly for training, and 40% are kept for testing. The cyber-physical twin model can be obtained via training after gathering training and validation data.

5.4. Physical–Digital Twin Coordinator for Attack Mitigation

In this study, the networked microgrid (NMG) system comprises multiple local controllers, each responsible for managing the operation of inverter-based resources within their respective microgrids (MGs). The coordination of each MG's operation is facilitated through agents $\{X_{mg1}, X_{mg2}, X_{mg3}\}$, which communicate with one another to ensure the stability of the NMG. A typical twin model of these NMGs is also implemented to enable precise control action selection during disturbances or attack scenarios. To achieve this, a physical–digital twin coordinator (PDTC) is proposed. The primary objective of the PDTC is to enhance information sharing among these agents to efficiently manage the power distribution among available resources and maintain system stability during contingencies or attack scenarios. The PDTC comprises multiple physical–digital twin (PDT) units, designated as PDT_{MG1} , PDT_{MG2} , and PDT_{MG3} , each associated with a specific MG. As detailed in this study, the NMG consists of three microgrids, each incorporating its local controllers, loads, sources, and converters, which are connected to the main DC bus via appropriate DC/DC converters. The contribution factors generated from the physical agents, $C_{f(phy)} = \{r_{P_MG1}, r_{P_MG2}, r_{P_MG3}\}$, are transmitted between the local agents and the PDTC through an information-sharing mechanism. This mechanism is designed to facilitate the switching between the physical agents and their twin agents if the system is subjected to a DoS attack. In addition, it provides a gateway for the information exchanges between the physical agents and the digital twin layer. Similarly, the estimated contribution factors from the twin agents are $C_{f(twin)} = \{r_{T_MG1}, r_{T_MG2}, r_{T_MG3}\}$.

Each physical–digital twin (PDT) unit is tasked with generating the appropriate control action based on its input signals, as illustrated in Figure 9. However, the final control action S_f by each PDT unit is not solely dependent on the presence of an alarm signal but also on the duration of this signal. For example, discrepancies between the physical and twin models during normal operation may arise due to communication traffic. Consequently, a time delay is implemented before selecting the appropriate control action in such scenarios, as described below:

$$S_f = \begin{cases} C_{f(phy)}, & error < TH \\ C_{f(twin)}, & error \geq TH, \end{cases} \quad for \tau s. \quad (22)$$

If the error signal remains below the threshold value during normal operation, the shared signals will be the normal physical measurements. When an alarm is triggered, the PDT will wait for a predefined duration τ seconds before updating the S_f signal. This delay allows for the PDT to confirm the occurrence of an abnormal condition before the system reaches an instability state. If the alarm persists, indicating that the error remains constant or increases, this signifies abnormal operating conditions. Consequently, the physical $C_{f(phy)}$ signal will be replaced with the latest $C_{f(twin)}$ twin signal as a major solution to deal with the DoS attack in the mitigation mechanism. The mitigation scheme consists of two stages: firstly, the twin agent will replace the attacked agent in terms of sending the control signals to the local controller to show the impact on the physical layer, and secondly, the twin agent will replace the function of the attacked agent in terms of sharing the information with its neighbor agents in the cyber layer.

6. Simulation of the Proposed System Under Normal Operation and DoS Attack

This section includes the simulation and validation response obtained from the LSTM network-based digital twin for the cyber-physical layer of the NMGs under normal operation. The root mean squared error (RMSE) is used as a prediction performance evaluation metric. In addition, the response of the cyber-layer twin is tested to detect the DoS attack on one of the physical agents in the cyber layer. Then, the evaluation of the mitigation mechanism with the aid of the designed PDT is presented. Table 1 provides the parameters of the three NMGs in terms of power ratings of DG units, system voltages, and load power at each MG and PCC. The local loads connected to MG1, MG2, and MG3 are P_LD1, P_LD2, and P_LD3, respectively.

Table 1. NMG parameters.

Parameter	Description	Value
MG1 Parameters		
P_{rated} (DG1)	DG1 rating	10 kW
P_{rated} (DG2)	DG2 rating	5 kW
P_LD1	Load power	7 kW
MG2 Parameters		
P_{rated} (DG3)	DG3 rating	8 kW
P_{rated} (DG4)	DG4 rating	7 kW
P_LD2	Load power	6 kW
MG3 Parameters		
P_{rated} (DG5)	DG5 rating	8 kW
P_LD3	Load power	6 kW
V	MG voltage	3 kV
P_{load} (PCC)	PCC load power	5 kW

6.1. Twin Models Performance Results

The final stage in creating an LSTM network-based digital twin is to test the trained network on a new dataset. Once the performance is adequate, the weights and biases can be frozen, and the trained network for the cyber and physical layers can be used to forecast the MG's dynamic behavior for a given physical or cyber pattern/events. In this section, the behaviors of the cyber-physical layer output and their twin models using LSTM are compared and evaluated under different loading conditions. The model performance is evaluated during the testing process using the point-to-point absolute error and the mean square error (RMSE) as the evaluation index and is calculated as follows:

$$Error = \left| Y_i - Y_{i_p} \right| \quad (23)$$

$$RMSE = \sqrt{\frac{1}{N_s} \sum_{i=1}^{N_s} (Y_i - Y_{i_p})^2} \quad (24)$$

where Y_i , Y_{i_p} , and N_s are the simulated value using the physical twin model, the output of the proposed LSTM DT model at time step I , and the sample size in the dataset, respectively? To evaluate the created data-driven DT model's accuracy, the four main output parameters for the DT that represent cyber-layer and physical-layer behaviors are compared with the output of the physical model. Figure 10 shows the response of the data-driven cyber twin agents and physical agents under different loading conditions. In the top panel, the measured control signal R from the physical PCC agent is plotted (red line), considered the main input for the cyber twin model. The variation in R is based on the loading conditions at each MG and the PCC point. In this scenario, the blue line does not represent the twin behavior of the PCC agent since we considered this agent the main source of information for the cyber twin. This blue line shows the expected response of the PCC agent if the twin agents fully controlled the NMGs instead of the physical agents. The contribution factors of the physical and twin agents are recorded and compared in the same figure using the absolute error metric for each MG. The results show a match between the DT model's behavior and the physical model with very small errors.

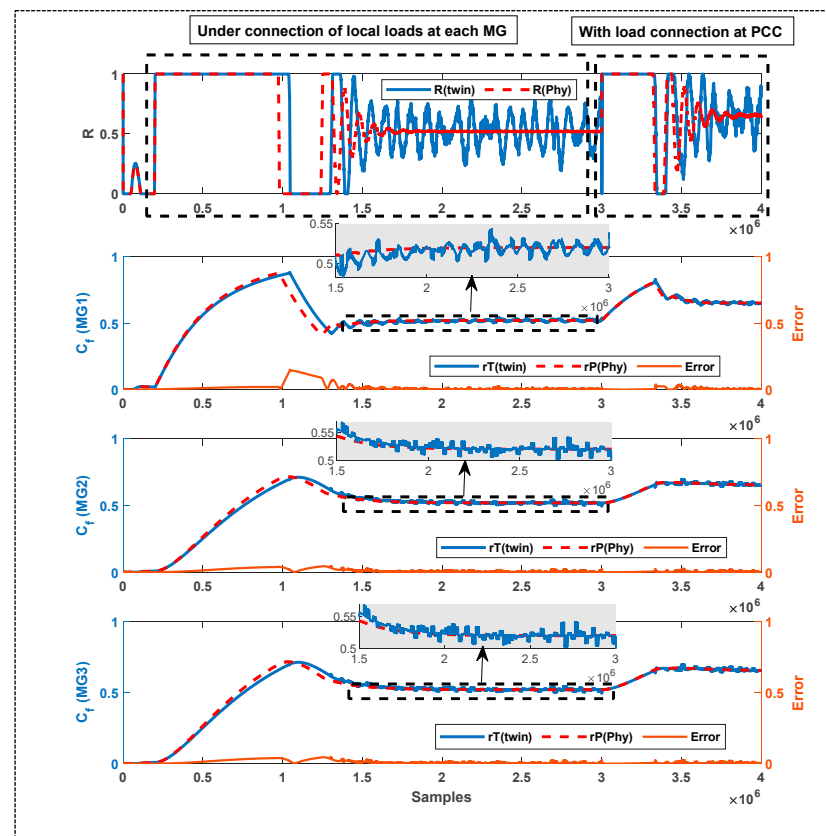


Figure 10. Cyber twin agents and physical agents' response under different loading conditions.

To evaluate the physical layer twin model, the selected output parameters from each MG are recorded and compared with the twin outputs. These parameters include the normalized MG voltage, normalized MG output power, and the normalized generated power from each DG in the MG. Figures 11–13 compare the physical and twin models of MG1, MG2, and MG3, respectively. These figures depict a close relationship between the data-driven digital twin estimated outputs and the physical model measurements. Figure 14 shows the RMSE for all cyber and physical parameters in each MG. It calculates the average difference between the projected and actual values to measure the model

prediction accuracy. The RMSE values of contribution factors, shared powers, and the bus voltages of the three MGs are shown in the left figure, and the RMSE of the power generated from each DG unit is shown in the right figure. The twin models show low values in the range of 0.2–3.5%. This presents the ability of the created DT model using the LSTM network to mimic the cyber-physical response of the NMGs.

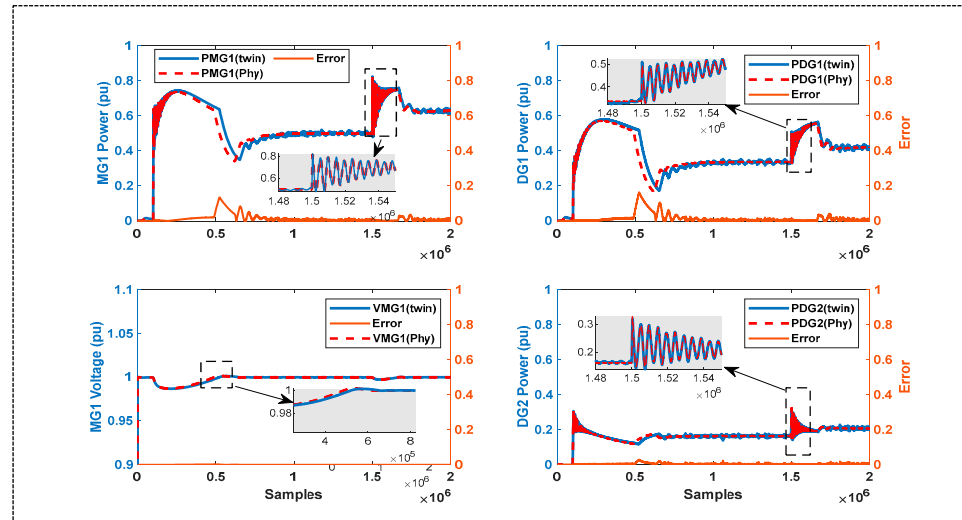


Figure 11. Voltage and power output comparison for the physical and twin models of MG1.

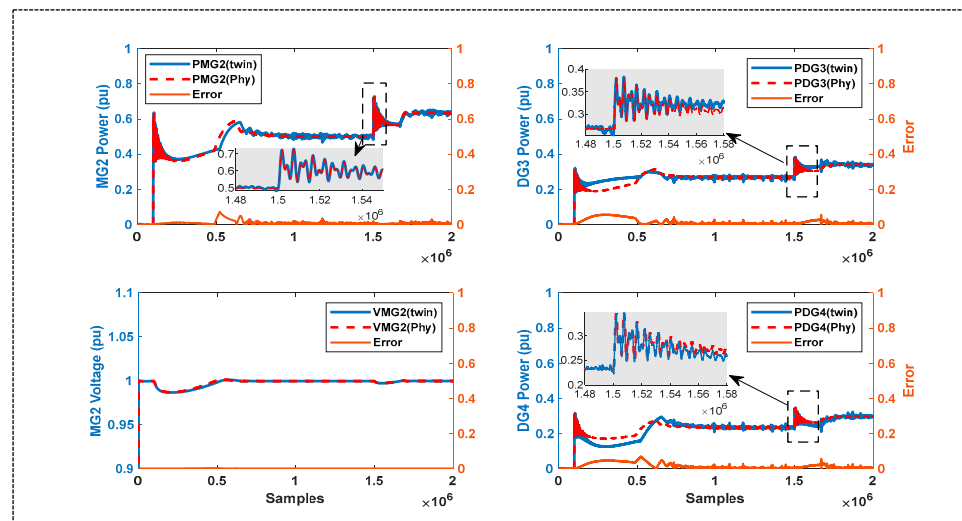


Figure 12. Voltage and power output comparison for the physical and twin models of MG2.

6.2. Results and Evaluation of the Proposed DT Response under DoS Attack

This section evaluates the networked microgrid system's resilience to cyber-attacks. The simulation results illustrate the effectiveness of the digital twin framework in enhancing the security and resiliency of microgrid cyber-physical systems. Figure 15 shows load profiles at various points: the point of common coupling (PCC), each microgrid (MG1, MG2, and MG3), and the total load. The total load increased at $t = 1$ s and $t = 15$ s. Figure 16 shows the response of the physical agents and their associated cyber twin agents under normal load conditions, connecting the load at the PCC, DoS attack, and attack detection and mitigation. The sequence of events is as follows: at $t = 1$ s, the load at each MG is connected; then, at $t = 15$ s, the load at the PCC is energized; after that, a DoS attack targeting the cyber agent of the MG2 is initiated. As shown in Figure 16, the twin and physical agent responses are closely matched. However, when the system is subjected to

the DoS attack, there is a considerable deviation between the agent’s behavior and a notable change in the PCC agent’s behavior. This is because, after the detection, the attacked physical is substituted by its twin agent, as described in Figure 11. The following is a detailed description of how the DT model detects the attacked agent and mitigates it with the help of the PDT coordinator, showing the impacts of the NMG resiliency on both the physical and cyber layers.

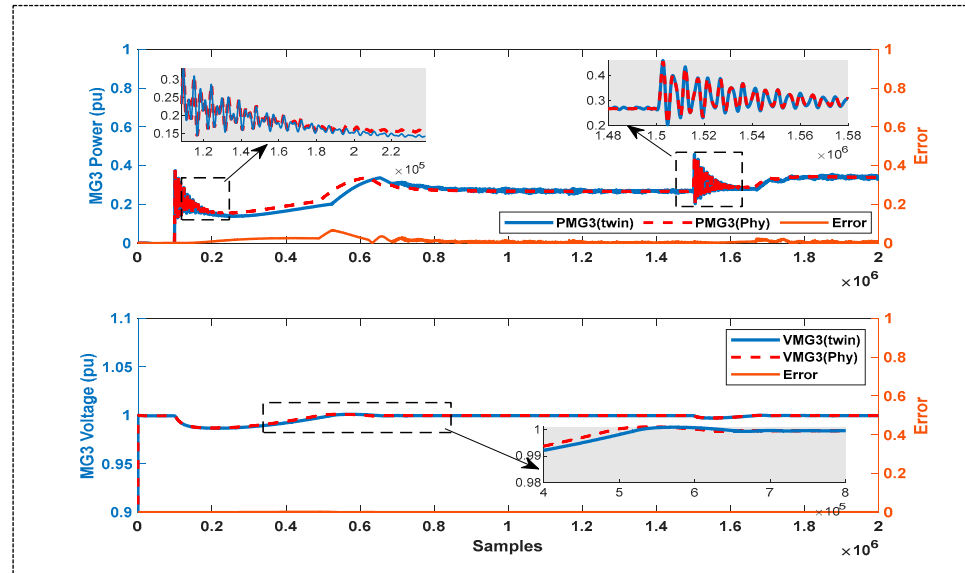


Figure 13. Voltage and power output comparison for the physical and twin models of MG3.

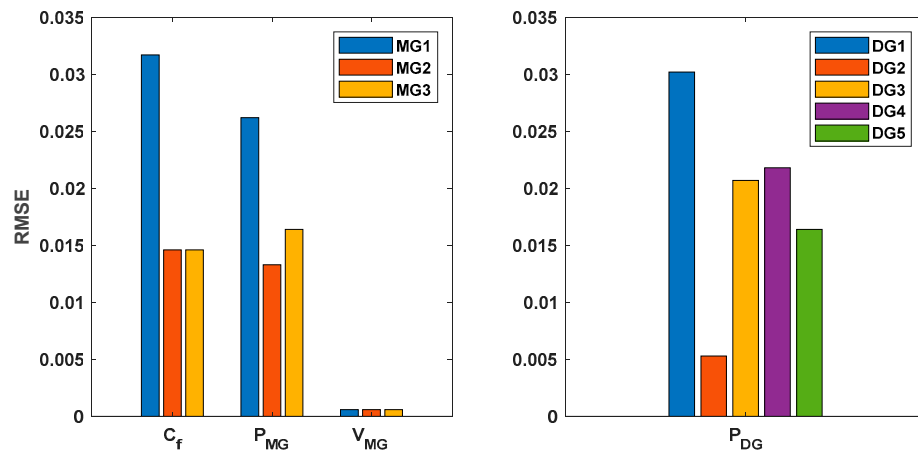


Figure 14. RMSE metric for the cyber and physical twin models of the NMGs.

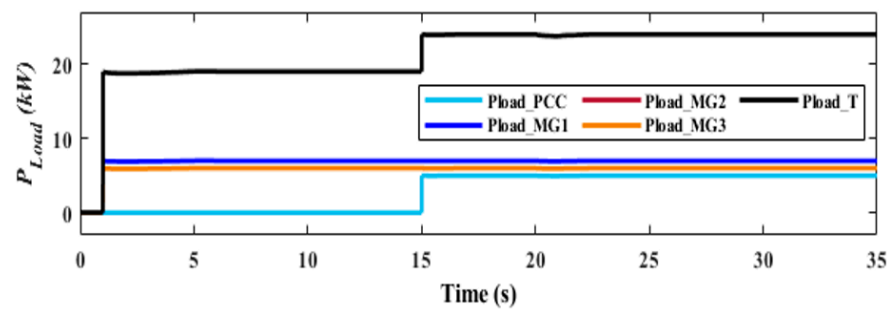


Figure 15. Local loads and PCC load profiles.

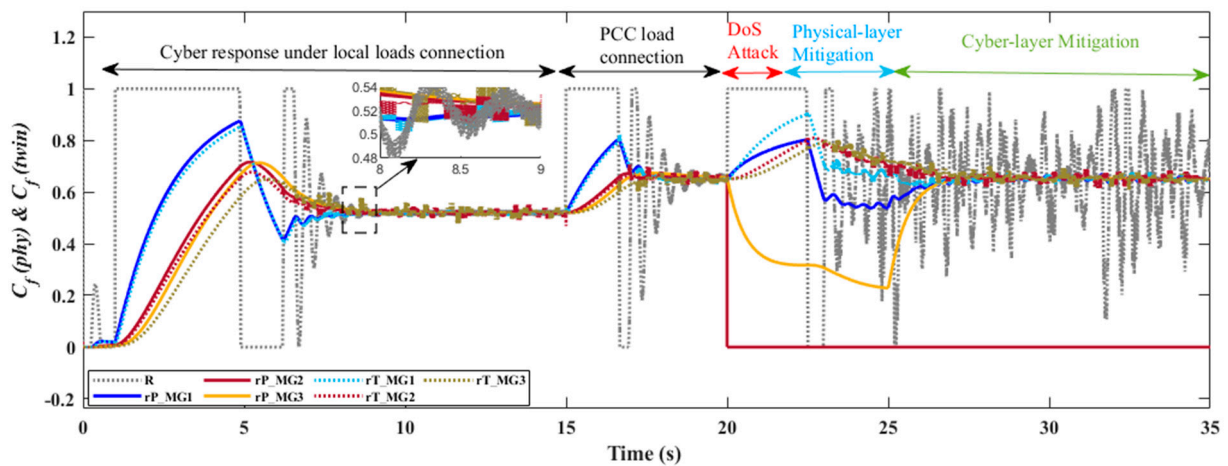


Figure 16. The response of the physical agents and their associated cyber twin agents.

As shown in Figure 17, all MGs operate normally in the beginning at no load. Following an increase in total load at each MG around $t = 1$ s, the contribution factor (C_f) from both the physical agents and their digital twins for each MG rises accordingly to meet the demand. The cyber-layer twin output $C_{f(twin)} = \{r_{T_MG1}, r_{T_MG2}, r_{T_MG3}\}$ (blue lines) and physical agent $C_{f(phy)} = \{r_{P_MG1}, r_{P_MG2}, r_{P_MG3}\}$ (red lines) closely aligned, reflecting accurate power-sharing and minimal error. At $t = 15$ s, a further increase in PCC load resulted in additional adjustments in $C_{fs(phy)}$ and $C_{fs(twin)}$ for MG1, MG2, and MG3 to handle the increased demand based on the consensus protocol with no alarms initiated by the digital twins. The system continued to operate smoothly until $t = 20$ s, when a denial of service (DoS) attack targeted the cyber agent of MG2 (X_{m2}), as shown in Figure 17c. This attack disrupted the communication between the attacked agent and its local controller as well as its neighboring agents, causing its corresponding C_f to drop to zero and resulting in a sharp increase in the error signal exceeding the setting threshold $TH2 = 0.2$. The system responded instantly with twin alarm 2, as shown in Figure 17a, activating and switching control from the compromised physical agent to the twin agent 1 s from the alarm activation. Shortly after the attack on agent X_{m2} , MG3 experienced similar behavior, with twin alarm 3 activating and its control also shifting to the twin agent after 1 s from the alarm activation. During this period, MG1 exhibited a slow increase in error due to its reliable information exchange with the PCC agent and the neighboring agents. Between $t = 21$ s and $t = 25$ s, the local controller exchanged information with DT of agent 2 instead of the attacked agent through the PDT coordinator. However, the cyber layer faced disruptions, since agent 2 was out of service. At $t = 25$ s, the twin had fully replaced the attacked agent in the cyber layer, restored the power-sharing objectives, and maintained system stability. In summary, this case showed that the DoS attack on agent 2 disrupted the system's overall behavior. The digital twin framework quickly identified the issue, triggered alarms, and switched control from the compromised physical agents to the twin agents. Also, it fully replaced agent 2 in the cyber layer, sharing reliable information with MG1 and MG3.

Figure 18 shows the microgrid system's response to an increased load scenario and a subsequent DoS attack in terms of voltages and power-sharing from each MG. As shown in Figure 18a, the voltage levels shown highlight minor drops during load increases as well as during the DoS attack. The voltage control is decentralized in the local controllers, which is why it shows low impact during the DoS attack. Finally, Figure 18b depicts the power outputs of the three microgrids. The power outputs increase to meet the higher load demand. However, significant disturbances occurred in the power outputs of the three microgrids due to the DoS attack at $t = 20$ s. The system started to recover as the twin took over in the physical layer by sending information to the local controller of MG2 at $t = 21$ s and in the cyber layer by sharing the healthy information with the cyber agents at $t = 25$ s, respectively.

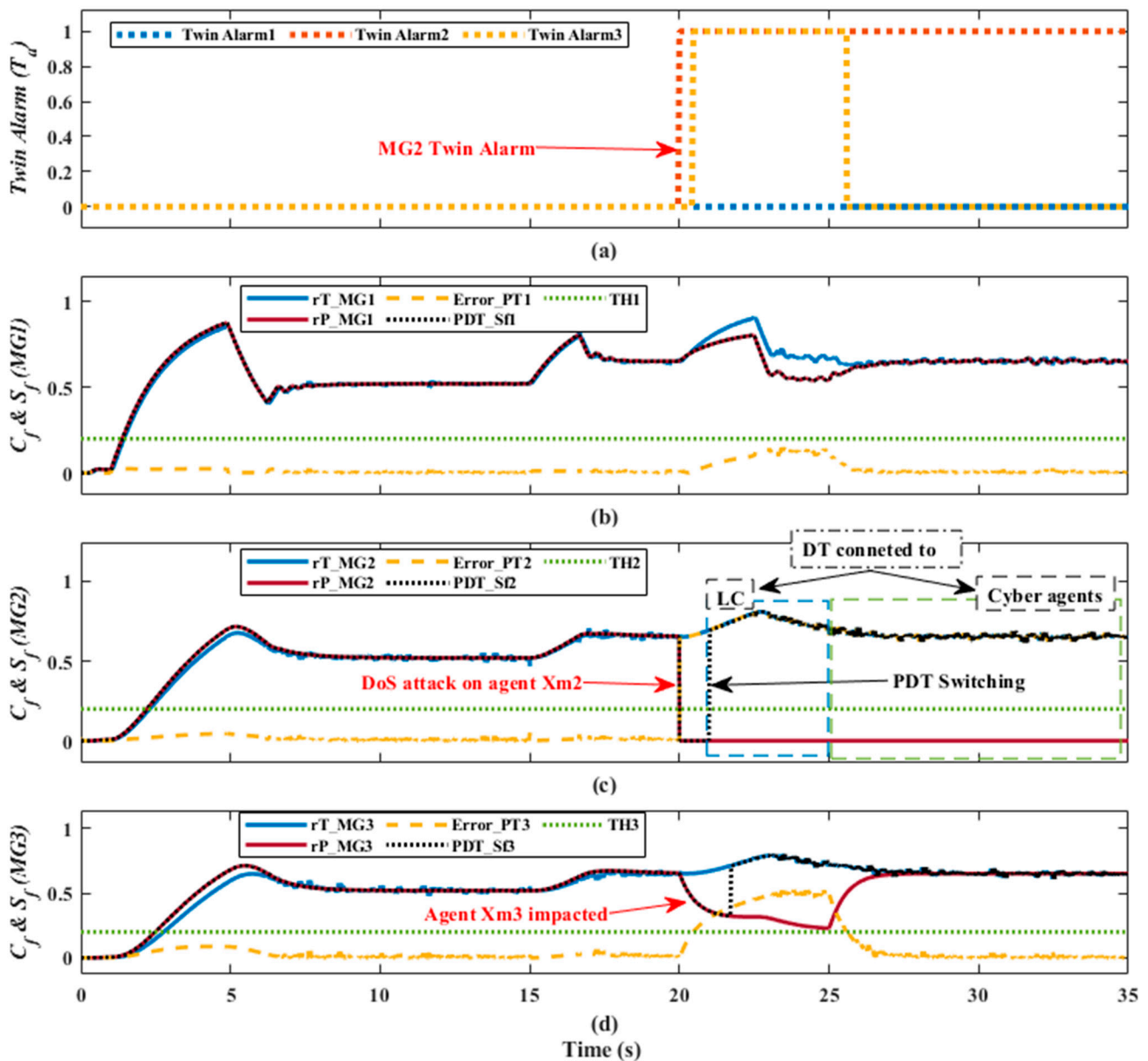


Figure 17. Contribution factors of physical and twin agents with attack detection and mitigation: (a) twin alarms; (b) contribution factors for MG1; (c) contribution factors for MG2; and (d) contribution factors for MG3.

The detailed response of the power outputs from the distributed generators and the power loads within each of the three microgrids (MG1, MG2, and MG3) over time, highlighting their response to the increased load demand and the denial of service (DoS) attack is shown in Figure 19. In Figure 19a, MG1 initially showed stable operation, with power outputs from DG1 and DG2 increasing at $t = 1$ s and $t = 15$ s to meet rising load demands. After $t = 20$ s, MG1 experienced fluctuations in the DG outputs due to the DoS attack but maintained relative stability compared to the others. Figure 19b, representing MG2, revealed a similar initial stability and load response, but at $t = 20$ s, DG3 and DG4 showed severe fluctuations and instability due to the attack, highlighting MG2's significant disruption. Figure 19c shows MG3's response, DG5 adjusted to the load increase. After $t = 20$ s, MG3 also experienced notable fluctuations in power output, reflecting the attack's impact. Overall, this figure illustrates the microgrids' coordinated effort to manage increased load demands and recover from cyber-attacks, demonstrating the critical

role of the digital twin framework in mitigating disruptions and restoring stability across the network.

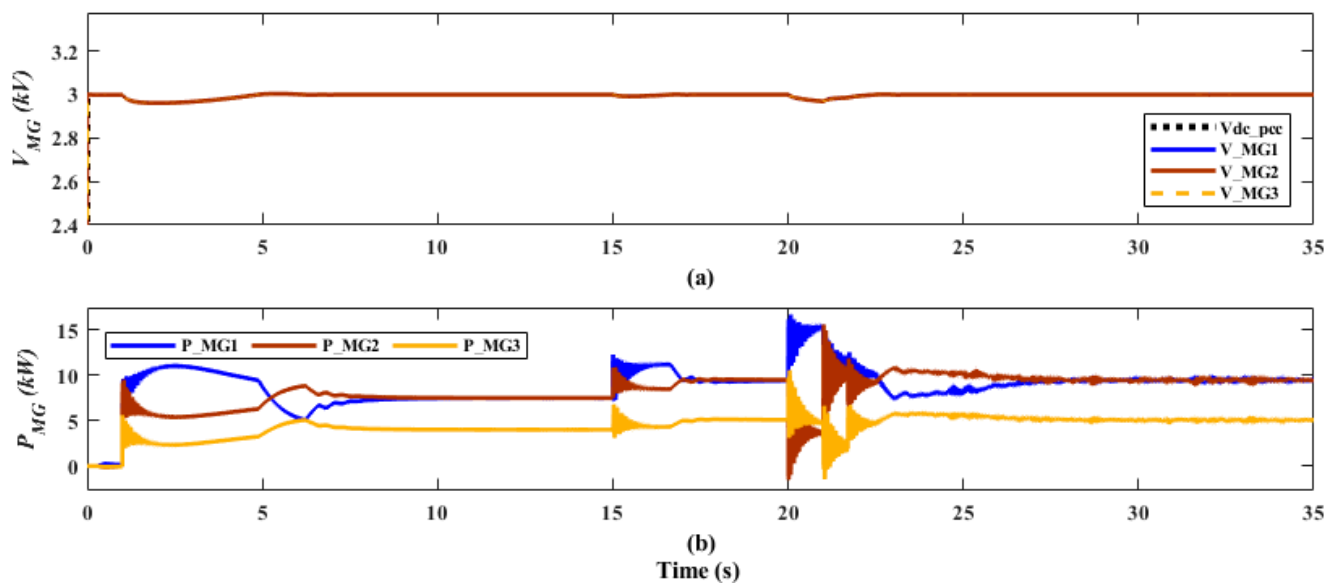


Figure 18. Voltage and power sharing response of each MG: (a) voltage measurements; and (b) power sharing from each MG.

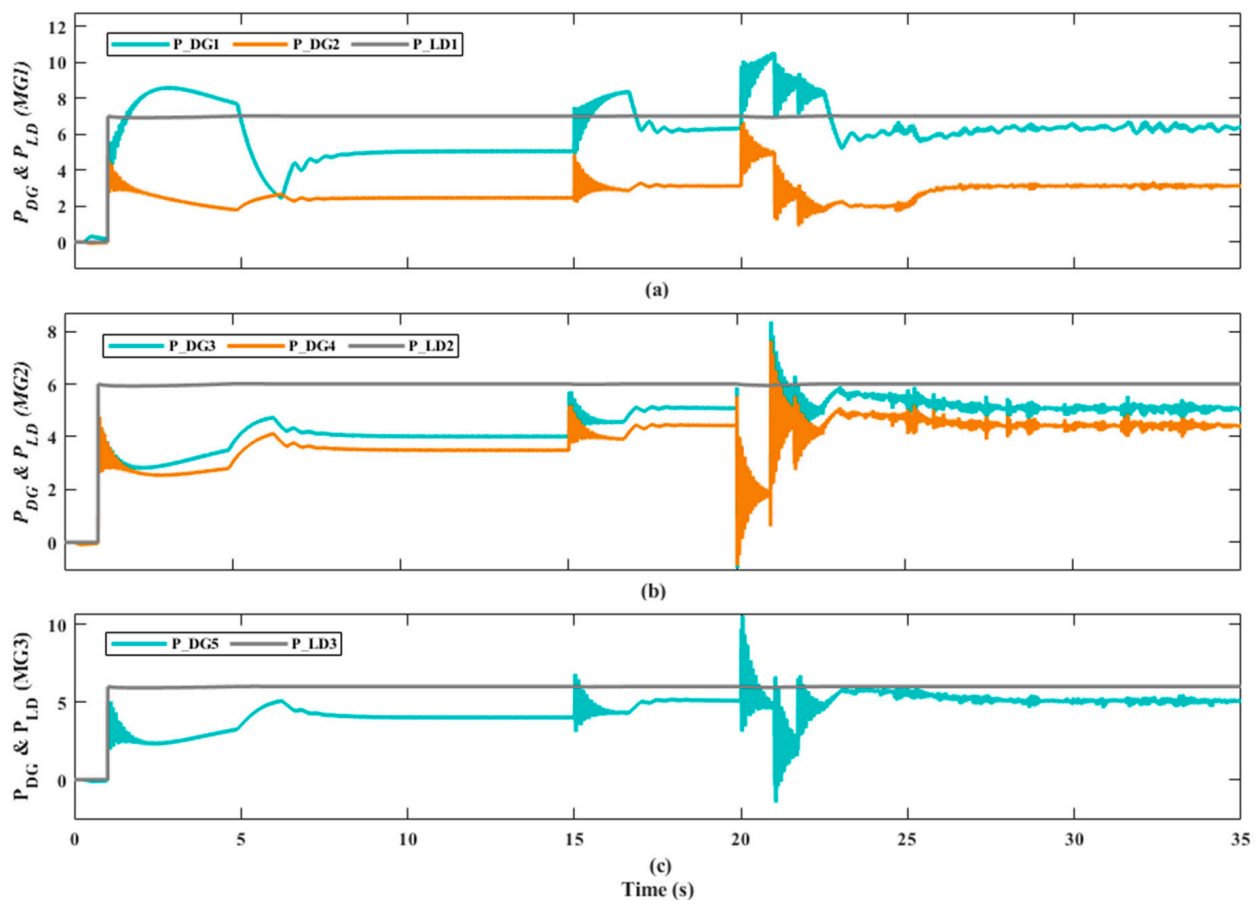


Figure 19. Power output of each DG and local loads in the NMGs: (a) power outputs of DG1 and DG2 for MG1; (b) power outputs of DG3 and DG4 for MG2; and (c) power output of DG5 for MG3.

In this study case, a long-term DoS attack is assumed, which makes the physical agent unavailable for a long time. Traditional DoS attack mitigation schemes are typically short-term solutions by adjusting controls or removing the attacked agent and recalculating the new operating point based on the available healthy agents. Providing a substitute twin agent is crucial to deal with this attack. Based on the results, replacing the attacked agent, the twin agent retrofitted all agents to their original, healthy state, hence increasing the control scheme's resiliency by replacing the agent's functions under a DoS attack. However, using the DT in attack detection and mitigation is limited by the need for a high-fidelity model, assumptions of existing of trusted points, and security check measures before replacing the attacked agent with its twin agent.

7. Conclusions

The digital twin, a dynamic virtual replica of a physical system, is a rapidly growing technology that can provide solutions for cyber-physical system monitoring and cyber-attack detection. This paper presents a methodology for designing data-driven-based digital twin models for both cyber and physical layers of a networked DC microgrid system using an LSTM network. The design methodology, mathematical analysis, and simulation study of a data-driven digital twin approach for DoS attack detection and mitigation are presented. The proposed study is unique in that the LSTM-based digital twin of the NMG's operation efficiently predicts the behavior of the physical and cyber parameters by mapping a smaller number of input/output parameters over the whole working range of the MG. The performance of the twin model is tested and evaluated. It effectively anticipates the dynamic behavior of cyber-physical dynamics under diverse load conditions and cyber incidents. In addition, the proposed attack detection and mitigation scheme based on the DT model enhanced the cyber-physical resiliency of the control system under a DoS attack.

Author Contributions: Conceptualization, M.S.A. and O.A.M.; Methodology, M.S.A., I.K. and H.M.H.; Software, M.S.A. and M.E.; Validation, M.S.A. and H.M.H.; Formal analysis, M.S.A. and H.M.H.; Investigation, O.A.M.; Resources, O.A.M.; Writing—original draft, M.S.A., H.M.H. and I.K.; Writing—review and editing, O.A.M.; Visualization, M.S.A. and I.K.; Supervision, O.A.M. All authors have read and agreed to the published version of the manuscript.

Funding: The work in this article was partially funded by grants from the US Department of Energy and National Science Foundation.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Krause, T.; Ernst, R.; Klaer, B.; Hacker, I.; Henze, M. Cybersecurity in power grids: Challenges and opportunities. *Sensors* **2021**, *21*, 6225. [[CrossRef](#)] [[PubMed](#)]
2. Zhou, B.; Zou, J.; Chung, C.Y.; Wang, H.; Liu, N.; Voropai, N.; Xu, D. Multi-microgrid energy management systems: Architecture, communication, and scheduling strategies. *J. Mod. Power Syst. Clean Energy* **2021**, *9*, 463–476. [[CrossRef](#)]
3. Jafari, M.; Rahman, M.A.; Paudyal, S. Optimal false data injection attacks against power system frequency stability. *IEEE Trans. Smart Grid* **2023**, *14*, 1276–1288. [[CrossRef](#)]
4. Choi, I.-S.; Hong, J.; Kim, T.-W. Multi-agent based cyber attack detection and mitigation for distribution automation system. *IEEE Access* **2020**, *8*, 183495–183504. [[CrossRef](#)]
5. Ashok, A.; Govindarasu, M.; Wang, J. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proc. IEEE* **2017**, *105*, 1389–1407. [[CrossRef](#)]
6. Fuller, A.; Fan, Z.; Day, C.; Barlow, C. Digital twin: Enabling technologies, challenges and open research. *IEEE Access* **2020**, *8*, 108952–108971. [[CrossRef](#)]
7. Tao, F.; Qi, Q.; Wang, L.; Nee, A. Digital twins and cyber-physical systems toward smart manufacturing and industry 4.0: Correlation and comparison. *Engineering* **2019**, *5*, 653–661. [[CrossRef](#)]
8. Qi, Q.; Tao, F.; Hu, T.; Anwer, N.; Liu, A.; Wei, Y.; Wang, L.; Nee, A. Enabling technologies and tools for digital twin. *J. Manuf. Syst.* **2021**, *58*, 3–21. [[CrossRef](#)]
9. Guo, J.; Lv, Z. Application of digital twins in multiple fields. *Multimed. Tools Appl.* **2022**, *81*, 26941–26967. [[CrossRef](#)]

10. Abdelrahman, M.S.; Kharchouf, I.; Nguyen, T.L.; Mohammed, O.A. A Hybrid physical co-simulation smart grid testbed for testing and impact analysis of cyber-attacks on power systems: Framework and attack scenarios. *Energies* **2023**, *16*, 7771. [[CrossRef](#)]
11. Cheng, Z.; Yue, D.; Hu, S.; Huang, C.; Dou, C.; Chen, L. Resilient load frequency control design: Dos attacks against additional control loop. *Int. J. Electr. Power Energy Syst.* **2020**, *115*, 105496. [[CrossRef](#)]
12. Li, Y.; Zhang, P.; Ma, L. Denial of service attack and defense method on load frequency control system. *J. Frankl. Inst.* **2019**, *356*, 8625–8645. [[CrossRef](#)]
13. Liu, Y.; Peng, Y.; Wang, B.; Yao, S.; Liu, Z. Review on cyber-physical systems. *IEEE/CAA J. Autom. Sin.* **2017**, *4*, 27–40. [[CrossRef](#)]
14. Kim, K.-D.; Kumar, P.R. Cyber-physical systems: A perspective at the centennial. *Proc. IEEE* **2012**, *100*, 1287–1308. [[CrossRef](#)]
15. Glaessgen, E.; Stargel, D. The digital twin paradigm for future NASA and us air force vehicles. In Proceedings of the 53rd AI-AA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference 20th AIAA/ASME/AHS Adaptive Structures Conference 14th AIAA, Honolulu, HI, USA, 23–26 April 2012; p. 1818.
16. Grieves, M. *Digital Twin: Manufacturing Excellence through Virtual Factory Replication*; A White Paper; Michael Grieves, LLC: Melbourne, FL, USA, 2014.
17. Moutis, P.; Alizadeh-Mousavi, O. Digital Twin of Distribution Power Transformer for Real-Time Monitoring of Medium Volt-age From Low Voltage Measurements. *IEEE Trans. Power Deliv.* **2021**, *36*, 1952–1963. [[CrossRef](#)]
18. Mukherjee, V.; Martinovski, T.; Szucs, A.; Westerlund, J.; Belahcen, A. Improved Analytical Model of Induction Machine for Digital Twin Application. In Proceedings of the 2020 International Conference on Electrical Machines (ICEM), Gothenburg, Sweden, 23–26 August 2020; IEEE: Piscataway, NJ, USA, 2020.
19. Nguyen-Huu, T.A.; Tran, T.T.; Tran, M.Q.; Nguyen, P.H.; Slootweg, J. Operation Orchestration of Local Energy Communi-ties through Digital Twin: A Review on suitable Modeling and Simulation Approaches. In Proceedings of the 2022 IEEE 7th International Energy Conference (ENERGYCON), Riga, Latvia, 9–12 May 2022; IEEE: Piscataway, NJ, USA, 2022.
20. Yuan, J.; Sun, M.; Xie, J.; Su, D.; Guo, J.; Guo, Y.; Wang, S. A Multi-agent System Construction Method for Substation Digital Twin. In Proceedings of the 2022 2nd International Conference on Electrical Engineering and Mechatronics Technology (ICEEMT), Hangzhou, China, 1–3 July 2022; IEEE: Piscataway, NJ, USA, 2022.
21. Bazmohammadi, N.; Madary, A.; Vasquez, J.C.; Mohammadi, H.B.; Khan, B.; Wu, Y.; Guerrero, J.M. Microgrid digital twins: Concepts, applications, and future trends. *IEEE Access* **2022**, *10*, 2284–2302. [[CrossRef](#)]
22. Madni, A.M.; Madni, C.C.; Lucero, S.D. Leveraging Digital Twin Technology in Model-Based Systems Engineering. *Systems* **2019**, *7*, 7. [[CrossRef](#)]
23. Jiang, H.; Tjandra, R.; Soh, C.B.; Cao, S.; Soh, D.C.L.; Tan, K.T.; Tseng, K.J.; Krishnan, S.B. Digital Twin of Microgrid for Pre-dictive Power Control to Buildings. *Sustainability* **2024**, *16*, 482. [[CrossRef](#)]
24. Milton, M.; De La, C.O.; Ginn, H.L.; Benigni, A. Controller-Embeddable Probabilistic Real-Time DTs for Power Electronic Converter Diagnostics. *IEEE Trans. Power Electron.* **2020**, *35*, 9850–9864. [[CrossRef](#)]
25. Saad, A.; Faddel, S.; Youssef, T.; Mohammed, O.A. On the implementation of IoT-based digital twin for networked mi-crogrids resiliency against cyber attacks. *IEEE Trans. Smart Grid.* **2020**, *11*, 5138–5150. [[CrossRef](#)]
26. Liu, X.-K.; Wang, S.-Q.; Chi, M.; Liu, Z.-W.; Wang, Y.-W. Resilient secondary control and stability analysis for dc microgrids under mixed cyber attacks. *IEEE Trans. Ind. Electron.* **2024**, *71*, 1938–1947. [[CrossRef](#)]
27. Fan, B.; Guo, S.; Peng, J.; Yang, Q.; Liu, W.; Liu, L. A Consensus-based algorithm for power sharing and voltage regulation in DC microgrids. *IEEE Trans. Ind. Inform.* **2020**, *16*, 3987–3996. [[CrossRef](#)]
28. Yohanandhan, R.V.; Elavarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications. *IEEE Access* **2020**, *8*, 151019–151064. [[CrossRef](#)]
29. Mohiuddin, S.M.; Qi, J. Attack resilient distributed control for ac microgrids with distributed robust state estimation. In Proceedings of the 2021 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2–5 February 2021; pp. 1–6. [[CrossRef](#)]
30. Shafiee-Rad, M.; Sadabadi, M.S.; Shafiee, Q.; Jahed-Motlagh, M.R. Robust decentralized voltage control for uncertain DC microgrids. *Int. J. Electr. Power Energy Syst.* **2021**, *125*, 106468. [[CrossRef](#)]
31. Wang, C.; Duan, J.; Fan, B.; Yang, Q.; Liu, W. Decentralized high-performance control of dc microgrids. *IEEE Trans. Smart Grid* **2019**, *10*, 3355–3363. [[CrossRef](#)]
32. Meng, L.; Dragicevic, T.; Roldan-Perez, J.; Vasquez, J.C.; Guerrero, J.M. Modeling and sensitivity study of consensus algorithm-based distributed hierarchical control for dc microgrids. *IEEE Trans. Smart Grid* **2016**, *7*, 1504–1515. [[CrossRef](#)]
33. Kharchouf, I.; Mohammed, O.A. Controller hardware-in-the-loop testbed of a distributed consensus multi-agent system control under deception and disruption cyber-attacks. *Energies* **2024**, *17*, 1669. [[CrossRef](#)]
34. Saad, A.A.; Faddel, S.; Mohammed, O. A secured distributed control system for future interconnected smart grids. *Appl. Energy* **2019**, *243*, 57–70. [[CrossRef](#)]
35. Saad, A.; Faddel, S.; Mohammed, O. IoT-based digital twin for energy cyber-physical systems: Design and implementation. *Energies* **2020**, *13*, 4762. [[CrossRef](#)]
36. Wu, Z.; Li, J. A framework of dynamic data driven digital twin for complex engineering products: The example of air-craft engine health management. *Procedia Manuf.* **2021**, *55*, 139–146. [[CrossRef](#)]
37. He, J.; Xiang, T.; Wang, Y.; Ruan, H.; Zhang, X. A Reinforcement learning handover parameter adaptation method based on LSTM-aided digital twin for UDN. *Sensors* **2023**, *23*, 2191. [[CrossRef](#)] [[PubMed](#)]

38. Hussein, H.M.; Esoofally, M.; Donekal, A.; Rafin, S.M.S.H.; Mohammed, O. Comparative study-based data-driven models for lithium-ion battery state-of-charge estimation. *Batteries* **2024**, *10*, 89. [[CrossRef](#)]
39. Jafari, M.; Kavousi-Fard, A.; Chen, T.; Karimi, M. A Review on digital twin technology in smart grid, transportation system and smart city: Challenges and future. *IEEE Access* **2023**, *11*, 17471–17484. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.