On the Implementation of IoT-Based Digital Twin for Networked Microgrids Resiliency Against Cyber Attacks

Ahmed Saad, *Graduate Student Member, IEEE*, Samy Faddel, *Member, IEEE*, Tarek Youssef, *Member, IEEE*, and Osama A. Mohammed, *Life Fellow, IEEE*

***Abstract*—The increased rate of cyber-attacks on the power system necessitates the need for innovative solutions to ensure its resiliency. This work builds on the advancement in the IoT to provide a practical framework that is able to respond to multiple attacks on a network of interconnected microgrids. This paper provides an IoT-based digital twin (DT) of the cyber-physical system that interacts with the control system to ensure its proper operation. The IoT cloud provision of the energy cyber-physical and the DT are mathematically formulated. Unlike other cyber-security frameworks in the literature, the proposed one can mitigate an individual as well as coordinated attacks. The framework is tested on a distributed control system and the security measures are implemented using cloud computing. The physical controllers are implemented using single-board computers. The practical results show that the proposed DT is able to mitigate the coordinated false data injection and the denial of service cyber-attacks.**

***Index Terms*—Digital twin, networked microgrids, distributed control, industrial Internet of Things, cybersecurity.**

I. Introduction

THE RAPID penetration of Renewable Energy Resources (RES) and the recent trend of transportation electrification increase the growth of networked microgrids industries in the energy sector. The recent development of the Networked Microgrid (NMG) systems converted the electrical distribution grid from passive to active networks and transformed the consumers into prosumers, which significantly increases the complexity of these systems. On one hand, the NMG physical system becomes more composite by containing multiple two-way interconnected systems such as Distributed Energy Resources (DERs), Energy Storage Systems (ESSs), flexible loads (as electric vehicles), fixed loads, power electronics converters, transformers, cables, etc. On the other hand, the degree of the cyber system complexity is much greater due to the use of multiple infrastructures, communication protocols, controllers, Intelligent Electronics Devices (IED), smart meters, and phasor measurement units. This transforms the modern electric distribution system into a critical energy cyber-physical system (ECPS) [1]–[3].

The two-way power flow controllability and the transactive energy capabilities of the NMG depend mainly on a large number of bidirectional power electronic converters, which should have a flexible, fast, and stable response to support the grid during the normal operation and the disasters. To efficiently and safely operates the NMG, proper management and control methodologies should be developed. Modern networked control systems are linked from the downstream level (nanogrids) to the upstream level (distribution substation), which are considered as an Industrial Internet of Things (IIoT) based communication infrastructure. The IIoT enables the required flexible coordination and integration among the DER's controllers and also improves the overall system management. Being IoT technology-dependent, a large amount of data is harvested from the physical assets' sensors and the cyber assets' controllers, which lead to the efficient operation of the grid and securely minimizes the risk. Thus, the IoT is believed to revolutionize the way we understand the energy sector [4]–[7].

Usually, the control system of the NMG systems is developed as a hierarchical distributed architecture, which contains primary, secondary and tertiary control layers. The geographical distribution of the NMG gives incentives to the designers to use the distributed control strategy to reduce the communication bandwidth and ensures the plug-and-play flexible installation of the microgrids. Generally speaking, the coordination between agents in a distributed control system usually depends on consensus protocols [8]–[18].

Despite the reported benefits of the distributed control system in the literature [9]–[14], [19]–[21], it is more vulnerable to cyber threats. Due to the absence of the centric oversight and the low-security level at this layer of consumer system, more cyber-attacks are inevitable [1]. In this kind of control systems, typically, the data transaction is secured using two ways. The first track is provided by IT data encryption and

Manuscript received October 30, 2019; revised February 24, 2020 and April 28, 2020; accepted May 31, 2020. Date of publication June 9, 2020; date of current version October 21, 2020. This work was partially supported by grants for the Office of Naval Research. Paper no. TSG-01646-2019. *(Corresponding author: Osama A. Mohammed.)*

Ahmed Saad and Osama A. Mohammed are with the Energy Systems Research Laboratory, Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174 USA (e-mail: asaad009@fiu.edu; mohammed@fiu.edu).

Samy Faddel is with the Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL 32816 USA (e-mail: samy.faddel@ucf.edu).

Tarek Youssef is with the Department of Electrical and Computer Engineering, University of West Florida, Pensacola, FL 32514 USA (e-mail: tyoussef@uwf.edu).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2020.3000958

certificate authentication [19]. The second one focuses on the resiliency of the control system itself [1], [10]–[18], [20]–[24]. The authors in [1] presented an attack resilient control system for multiple DERs based on a neighbour watching mechanism to isolate the attacked control agent from the network graph. In [20], a resilient distributed control system is introduced to solve the packet loss problem while in [21], a distributed hierarchical control system was proposed. The controller was able to detect and gradually isolate the infected controller. In [10], a mathematical morphology technique was used to analyze the neighbour's dynamical features to detect, identify and mitigate the attacked agent. A trust-based and compensator-based control protocol were introduced in [15] and [16], respectively to guarantee the distributed system synchronization under sensor/actuator attacks. In [17], a reputation-based neighbourhood watches method was used to detect the data integrity attack on the distributed scheduling. For the same problem, the authors in [18] proposed a confidence level-based mechanism using on the top hidden communication network in parallel with the main distributed management system to detect and isolate the attack. Kullback-Leibler (KL) divergence technique was used in [22] to determine the trust level of the distributed controllers and then isolate the faulty data source according to the divergence rates.

Regardless of the efforts that were done so far, multiple coordinated attacks on the distributed secondary and/or tertiary control systems have not received enough attention. Coordinated attacks can easily disturb the consensus among the distributed controllers. Besides, regular solutions of mitigating these kinds of attacks by excluding it from the cyber graph cannot solve the problem because the excluded agent might be a vital agent that can disturb an entire microgrid cluster. Furthermore, mixing the coordinated attacks on both sensors and controllers alongside with communication network magnifies the security concerns and impose handicap on the IIoT benefits. Motivated by [24], the authors believe that the live data-driven model can discover the coordinated attack and provide the autonomous post-attack recovery.

In this paper, an IoT-based digital twin (DT) for the cyber-physical networked microgrids is introduced to enhance the resiliency against cyber attacks. The cloud-based DT platform is implemented to be a centric oversight for the NMG system. The cloud system hosts the controllers (cyber things) and the sensors (physical things) into the cloud IoT core in terms of the IoT shadow. The proposed DT covers the digital replica for both the physical layer, cyber layers and their hybrid interactions. The proposed framework ensures the proper and secure operation of the NMG. Also, it can detect false data injection (FDIA) and denial of service (DoS) attacks on the control system whether they are individual or coordinated attacks. Once an attack is detected, corrective action can be taken by the observer-based on What-If scenarios that ensure the safe and seamless operation of the networked microgrids (NMG). DT introduce a constructible active model to provide interaction between the defence mechanism and the attackers. In summary, the major contributions of this paper are:

1) New use of the concept of DT to secure the NMG.
2) Formulating the IoT shadow and cyber-physical DT mathematically.
3) Developing practical resilient control algorithms that are able to detect and mitigate FDIA attacks.
4) Deploying the cloud-based services to provide an IoT based implementation of the DT.
5) Validating the interaction between the cloud-based services and the physical entities of the control system.

II. Overall System Description

Recently, the IoT technologies and cloud computing advancements encourage the energy sector to utilize this digital transformation for better understanding and improving the energy system operation. The Digital Twin (DT) strategic technology is proposed to get the benefits of the IIoT, the ECPS models and the advanced data analytics to understand what is happening and what will happen for the ECPS. The DT is defined as digital replica/model that includes the last information matching a thing. The DT was successfully applied recently in the industry for manufacturing, power plants, healthcare and automotive sectors [6], [25], [26].

Fig. 1 shows the proposed DT architecture. The NMG (physical assets) under study is a DC networked microgrid (DCNMG) system in the physical space in the lower layer. The physical system is constructed by n interconnected DC microgrids clusters where each cluster contains m DCNMGs.

The interconnected clusters are connected to a main Medium Voltage DC (MVDC) bus. The NMG is aggregated at the point of common coupling (PCC) with grid through an interlinking DC/AC inverter and a step-up transformer. The primary controllers are assumed to be a part of the physical system as they are mainly responsible for the local control of the converters.

In the second layer, the edge control system consists of the distributed controllers and the tertiary controller. The secondary controllers are communicating and coordinating via a cyber combination IED-to-IED links to satisfy the objective control rule that is received from the tertiary controller at the PCC.

The tertiary control agent sends the required reference power-sharing factor to the secondary controllers' leaders for each cluster of microgrids. Then, the leader sends the control law to the cluster follower agents by the consensus protocol to make an agreement on the leader state. The control objective is to guarantees equal relative power-sharing among microgrids. The failure in ensuring the control objective due to a communication failure or a cyber-attack causes unfair power-sharing and can disturb/collapse the voltage regulation at the PCC. Since the NMG is ruled by the balancing between the NMGs power and the PCC power, the physical DT is implemented to represent the real-time balancing according to the physical living model of the interconnected system.

In addition, the cyber DT represents the multi-agent consensus convergence rules to guarantee the matching between the tertiary control system and the secondary control system. The hybrid CPS replica enhances the centric oversight by ensuring that the mismatch between the cyber and physical system

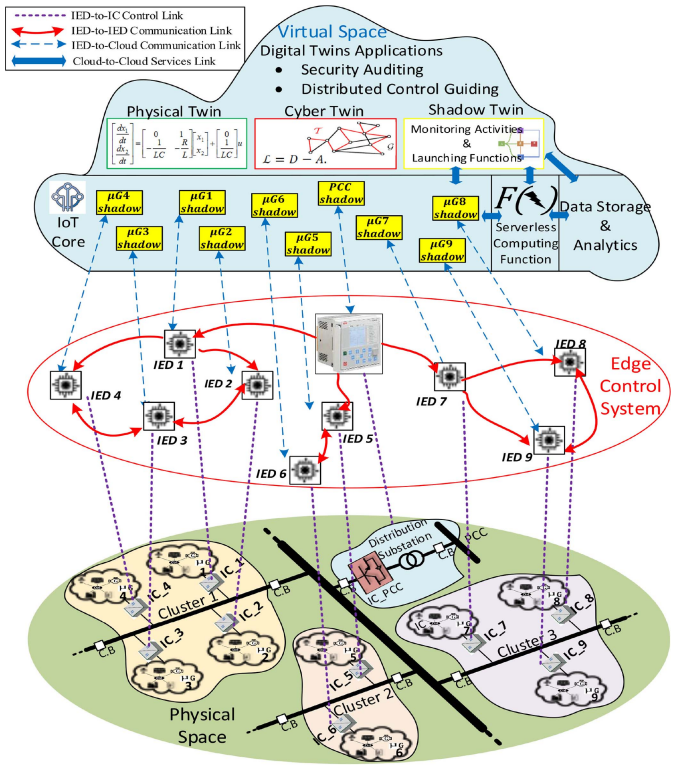

Fig. 1. The overall system architecture of the proposed DT platform for ECPS.

components is decaying to zero. If the mismatch between the DT and the real-time measurements exists, the CPS failure or attack can be detected, estimated and mitigated. Both the physical system states and the cyber control agents are connected to the virtual layer (cloud system) through the IoT core as a shadow of things. Things' shadows have the last states of the controllers/sensors, which are updated periodically by the edge controller to notify the cloud of the new states. A serviceless computing function is utilized to launch certain applications/measures according to the status of the shadow states. The main focus of this paper is the resiliency of the NMG against the cyber-attacks on the physical sensors and/or control agents.

III. Digital Twin Living Model

The Degree of complexity and the accuracy of the DT is defined according to the application and the type of analysis or the outputs that are required to be implemented. The purpose of the DT in this paper is to discover the physical balancing mismatch, the cyber control system convergence and the hybrid CPS consistency. Therefore, the system models are implemented for the DT as follows.

A. Physical Twin Model

In this work, the intra-microgrids dynamics are ignored for the control system since the objective is the power transaction and the power balancing rule among the microgrids and the PCC. Therefore, the implemented physical twin model emphases mainly on the bidirectional DC/DC converters because they are the things that control the power flow transaction and regulates the system parameters [27].

Generally, the DCNMG dynamics of i^{th} microgrids can be described by,

$$\left.\begin{aligned} L_i \frac{d\tilde{I}_i}{dt} &= E_i^* - r_i\tilde{I}_i - v_i^t \\ C_i \frac{dv_i^t}{dt} &= \tilde{I}_i - I_i^t \end{aligned}\right\} \tag{1}$$

where $\tilde{I}_i$ is the i^{th} microgrid converter average inductor current, E_i^* is the reference voltage at the i^{th} microgrid v_i^t is the microgrid terminal voltage and I_i^t is the transmitted current from/to microgrid i to the grid. In addition, R_i, L_i and C_i are the equivalent resistance, inductance and capacitance of each microgrid.

It is assumed that the microgrid output is controlled by the reference signals of the terminal voltage $V_i^{t,ref}$ and the output reference power P_i^{ref} using the droop control characteristics as follows,

$$E_i^* = V_i^{t,ref} - k_i\left(P_i^{ref} - P_i\right) \tag{2}$$

where k_i is droop coefficient and the output power can be represented in terms of power-sharing factors $P_i = P_{i,max}x_i$. Therefore, if $\beta_i = k_iP_{i,max}$, the controlled voltage in (2) can be rewritten as,

$$E_i^* = V_i^{t,ref} - \beta_i\left(x_i^{ref} - x_i\right) \tag{3}$$

The microgrid terminal t_i is connected to the distribution grid nodes g_j which has voltages $v_o^g = [v_o^g, \ldots, v_m^g]$ and the transmitted current to the grid nodes can be described as,

$$I_i^t = \sum_{j\subset m} I_j^g = \sum_{j\subset m} y_{ij}^{tg}\left(v_i^t - v_j^g\right) \tag{4}$$

where y_{ij}^{tg} is the line or cable admittance between the nodes t_i and g_j. Since the balancing and power flow is the purpose of the model, the electromagnetic transients are ignored which leads that the grid interconnection model is represented as follows,

$$\begin{bmatrix} I^t \\ I^g \end{bmatrix} = \begin{bmatrix} Y^{tt} & Y^{tg} \\ Y^{gt} & Y^{gg} \end{bmatrix} \begin{bmatrix} V^t \\ V^g \end{bmatrix} \tag{5}$$

According to (1) and (3)-(5), the balancing dynamics in matrix notation can be written as,

$$\left.\begin{aligned} L\frac{d\tilde{I}}{dt} &= V^{t,ref} - \beta X^{ref} - R\tilde{I} - V^t \\ C\frac{dV^t}{dt} &= \tilde{I} - I^t \\ I^t &= Y^{tt}V^t + Y^{tg}V^g \\ I^g &= Y^{gt}V^t + Y^{gg}V^g \end{aligned}\right\} \tag{6}$$

where the power sharing states $X^{ref} = [x_1^{ref}, \ldots, x_n^{ref}]^T$, and the reference terminal voltages, $V^{t,ref} = [v_1^{t,ref}, \ldots, v_n^{t,ref}]^T$.

To ensure the equilibrium of the dynamics, (6) is analyzed in steady-state such that $V^t = V^{t,ref} - \beta X^{ref} - RI^t$ as,

$$\left.\begin{aligned} I^t &= Y^{tt}V^{t,ref} - \beta Y^{tt}X^{ref} - RY^{tt}I^t + Y^{tg}V^g \\ I^g &= Y^{gt}V^{t,ref} - \beta Y^{gt}X^{ref} - RY^{gt}I^t + Y^{gg}V^g \end{aligned}\right\} \tag{7}$$

whose re-arranging yields,

$$\left.\begin{aligned} I^t &= \left(Y^{tt^{-1}} + R\right)^{-1} V^{t,ref} - \beta\left(Y^{tt^{-1}} + R\right)^{-1} X^{ref} \\ &\quad + Y^{tg}\left(1 + RY^{tt}\right)^{-1} V^g \\ I^g &= \left(Y^{gt} - Y^{gt}R\left(Y^{tt^{-1}} + R\right)^{-1}\right) V^{t,ref} \\ &\quad - \left(\beta Y^{gt} - Y^{gt}R\beta\left(Y^{tt^{-1}} + R\right)^{-1}\right) X^{ref} \\ &\quad \left(Y^{gg} - Y^{gt}Y^{tg}R\left(1 + RY^{tt}\right)^{-1}\right) V^g \end{aligned}\right\} \quad (8)$$

The system achieves the equilibrium if the controlled values $V^{t,ref}$ and X^{ref} are chosen to guarantee that the system in (6) is solvable. A physical asset $\varphi \in \Phi$ is represented by the physical set of states, which is measured by a sensor $\psi \in \Psi$. The physical system is represented in state-space form as,

$$\left.\begin{aligned} \dot{X}^{\Psi} &= A^{\Phi}X^{\Psi} + B^{\Phi}U^{\Psi} \\ Y^{\Psi} &= C^{\Phi}X^{\Psi} \end{aligned}\right\} \quad (9)$$

where the physical system states are $X^{\Psi} = [\tilde{I}, V^t]^T$, and the inputs are $U^{\Psi} = [V^{t,ref}, X^{ref}, I^t]^T$. The physical system dynamical parameters are derived from (6) as follows,

$$A^{\Phi} = \begin{bmatrix} -RL^{-1} & -L^{-1} \\ C^{-1} & 0_n \end{bmatrix}, \quad C^{\Phi} = [I_n]$$
$$B^{\Phi} = \begin{bmatrix} L^{-1} & -\beta L^{-1} & 0_n \\ 0_n & 0_n & -C^{-1} \end{bmatrix}. \quad (10)$$

As an illustration, The NMG system under study is DC microgrids with two microgrids clusters, which are interconnected by z_c tie-lines. As shown in Fig. 2, the first cluster has five microgrids and the second cluster has three microgrids. The two clusters are connected to the PCC by the lines z_{c1}, z_c8. Each microgrid has a bidirectional DC/DC converter and the controlled variables are the voltages, which should be maintained at $1p.u.$ and the power-sharing factor that is provided by the secondary control layer.

B. Cyber Twin Model

The distribution system that contains NMG can be considered as a virtual power plant. The aggregated power from the NMG is controlled by the tertiary controller at PCC (leader) and the multi-agent cooperated controllers at each microgrid (followers) [1], [9], [15]–[18]. The PCC tertiary controller objective is to satisfy the energy management optimal update, which is the reference power-sharing P_{pcc}^{ref} by aggregating it from the NMGs sharing P_i. Since the NMG contains different scales of microgrids, the sharing capability of each microgrid is different. Therefore, the PCC agent (agent 0) is described by the sharing factor $x_0 = P_0/P_{0,\max}$ and each microgrid sharing capability is defined as $x_i = P_i/P_{i,\max}$. The PCC agent control objective is to achieve certain reference common power-sharing factor as follows,

$$\min_x \left(x_0^{ref} - x_0(x_i)\right)$$
$$\text{s.t. } 0 \le x_0 \le 1, \quad 0 \le P_0 \le P_{0,max} \quad (11)$$

where $P_{0,max}$ is the maximum power-sharing capability at the PCC.

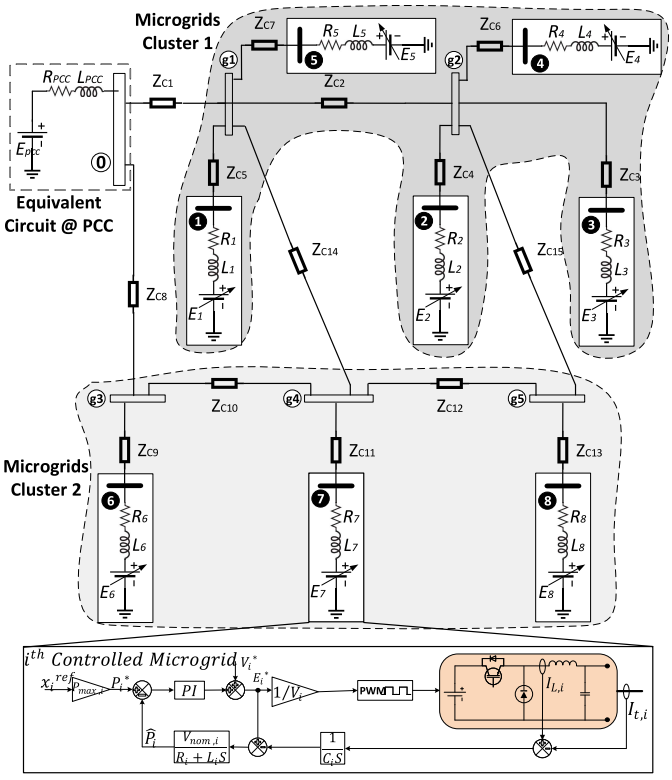

Fig. 2. NMG equivalent circuit for the physical system model.

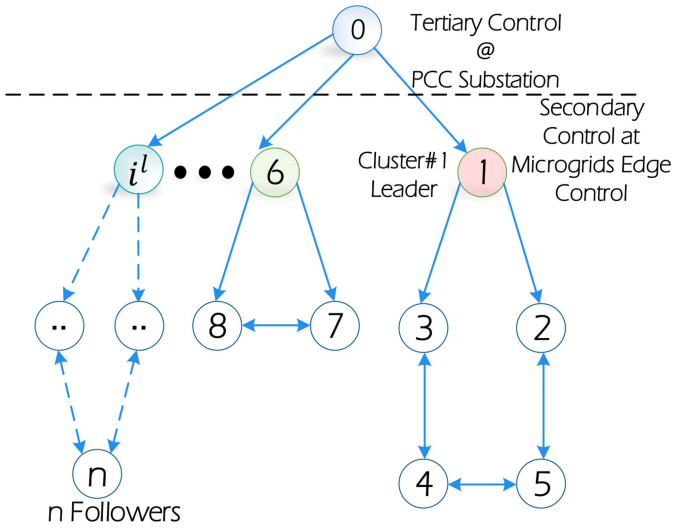

Fig. 3. NMG cyber graph topology.

The secondary distributed controllers cooperate to achieve a consensus on the main leader control objective. According to the graph theory, the cyber communication is a graph $\mathcal{G} = (\mathcal{V}, \varepsilon)$ that determines the cyber state coupling of the agents' dynamics where $\mathcal{V} = \{0, 1, \ldots, n\}$ is the vertex set with a set of edges $\varepsilon \subseteq \mathcal{V} \times \mathcal{V}$ is the coupling between the control agents. Figure 3 shows the communication network cyber graph topology. Agent 0 is the main leader for the system, and it is connected to the leaders of microgrids clusters i^l, which is connected to several i followers.

The edge $(i,j) \in \mathcal{E}$ represents the cyber state of i^{th} agent will influence the dynamics of j^{th} agent according to weighing factor w_{ij}, which is represented as a global adjacency matrix $\mathcal{A} \in \mathbb{R}^{(n+1)\times(n+1)}$, which is described as [8], [15]–[17],

$$[\mathcal{A}]_{ij} = \begin{cases} w_{ij} > 0 & \text{if } i,j \in \mathcal{E} \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

The graph Laplacian matrix is defined as $\mathcal{L} = \mathcal{D} - \mathcal{A}$, were $\mathcal{D} = \text{diag}\{d_i\}$, is the in-neighbours degree matrix and $d_i = \sum_{j\in n_i} w_{ij}$.

Remark 1: The leader-follower consensus protocol can be implemented in the following discrete-time form for k^{th} samples to achieve an agreement on the steady-state control leader such that, $\lim_{k\to\infty} x_i(k) = x_0^{ref} \forall i \in n$ that is provided by the tertiary controller as formulated in Algorithm A2 in [28],

$$\delta_{ij}(k+1) = \delta_{ij}(k) + w_{ij}\big(x_j(k) - x_i(k)\big) \tag{13}$$

$$x_i(k+1) = \varepsilon.\delta_{ij}(k+1) + g_i \cdot x_0 \tag{14}$$

where δ_{ij} is an intermediate updating of the control law for an agent i by j^{th} neighbours, ε is a constant to regulate the consensus speed and g_i is the pinning gain, which characterizes the spanning tree at the leader.

The dynamics of the consensus protocol can be modelled as a set of interacting agents that achieve a common goal x_0. The local neighbourhood tracking error e_i of a controller i is formulated as,

$$e_i = \dot{x}_i = \sum_{j\in n_i} w_{ij}\big(x_j - x_i\big) + g_i \cdot (x_0 - x_i) \tag{15}$$

$$\dot{X} = -(\mathcal{L} + G) \cdot X + G\underline{1}x_0 \tag{16}$$

The leader takes the role of controlling the graph in a distributed manner using the consensus protocol $u_i = \iota e_i$, were ι is a constant gain, which is chosen to ensure the synchronization among agents. The synchronization error with the leader can be represented as $\delta_i = x_i - x_0$. The consensus is achievable under the input u_i to the leader state x_0 and the synchronization error with the leader is decaying to zero, $\delta_i \to 0$ if the dynamical matrix of the cyber graph is stabilizable. The global dynamical error under the control mechanism u_i be formulated as,

$$\left.\begin{aligned} \dot{\delta} &= \dot{X} - \dot{X}_0 \\ &= ((I_n \otimes \mathcal{A}) - \iota(\mathcal{L} + G))\delta \\ &= A^c\delta \end{aligned}\right\} \tag{17}$$

were A^c represent the error closed dynamical matrix. The solution is written as,

$$\delta(t) = e^{A^c t}\delta(0) \tag{18}$$

A cyber thing θ represents a controller state $x^\theta \in X^\Theta$, which uses the sensor measurement and the cyber graph $\mathcal{G}$ to control the physical asset φ. The cyber system dynamics is given by,

$$\left.\begin{aligned} \dot{X}^\Theta &= A^\Theta X^\Theta + B^\Theta U^\Theta \\ Y^\Theta &= C^\Theta X^\Theta \end{aligned}\right\} \tag{19}$$

where the cyber states $X^\Theta = X^{ref}$, the graph control input $U^\Theta = X_0$, the cyber system dynamics are $A^\Theta = -(\mathcal{L} + G)$, $B^\Theta = \iota G\underline{1}$, $C^\Theta = I_n$.

The IoT cyber edge system is vulnerable to different types of attacks that can threaten the communication links or the controllers itself. A cyber-attack against control systems is usually classified into three different properties/resources available for the attack: model knowledge, disclosure resources, and disruptive resources. The following assumptions hold.

Assumption 1: An attacker can acquire at least the local data to launch an attack to disturb the consensus. Also, the link between the secondary and primary controller is a part of the local controller. If an attack launched on the PCC agent or its communication link with the leaders can mislead the entire distribution system. Also, if an attacker knows the distributed control systems, consensus protocol and the network topology, he can launch a multiple coordinated attacks, which can easily mislead the distributed observers.

Assumption 2: If an attack was successfully launched on the PCC agent or the leader agents of clusters and the attack is detected, the isolation of the attacked agent cannot retrofit the consensus as that will exclude also the healthy follower agents.

Mathematically, the attack on the controller can be on the control actuator signal to the physical system and/or on the cyber graph states as follows,

$$\left.\begin{aligned} u_i^f &= u_i + \gamma_i u_i^a \\ x_i^f &= x_i + \alpha_i x_i^a \end{aligned}\right\} \tag{20}$$

where u_i, u_i^f are the healthy and the attacked actuator signal to the physical system. Also, x_i, x_i^f are the healthy and faulty states sent to neighbourhood controllers from the physical system. The Boolean signals γ_i, α_i is representing the presence of the attack vector u_i^a, x_i^a.

Theorem 1: Suppose the cyber system (19) is under attack (20) and let Assumptions 1-2 are applied. If an agent i is the attacked, then all intact agents j^{th}, the tertiary control objective cannot be satisfied.

Proof: According to attack model (20) and by applying the error dynamics (15) and substituting in the cyber system (19), the combined system dynamics is represented as,

$$\left.\begin{aligned} \dot{x}_i^\theta &= A^\theta x_i^\theta + B^\theta u_i^\theta + B^\theta \xi_i^\theta \\ \xi_i^\theta &= \gamma_i u_i^a - \iota\Big(\textstyle\sum_{j\in n_i} w_{ij}\Big(\alpha_i x_i^a - \alpha_j x_j^a\Big) + g_i\alpha_i x_i^a\Big) \end{aligned}\right\} \tag{21}$$

By calculating the error dynamics with respect to the leader state and rewriting (21) in matrix form,

$$\left.\begin{aligned} \dot{\delta} &= \dot{X} - \dot{X}_0 = A^c\delta + \big(I_n \otimes B^\theta\big)\xi^\theta \\ \xi^\theta &= -\iota(\mathcal{L} + G)(\boldsymbol{\alpha} \otimes I_n)X^a + (\boldsymbol{\alpha} \otimes I_n)U^a \end{aligned}\right\} \tag{22}$$

by combining (17) and (22), the error dynamics becomes,

$$\begin{aligned} \dot{\delta} = A^c\delta &- \iota\big(I_n \otimes B^\theta\big)(\mathcal{L} + G)(\boldsymbol{\alpha} \otimes I_n)X^a \\ &+ \big(I_n \otimes B^\theta\big)(\boldsymbol{\alpha} \otimes I_n)U^a \end{aligned} \tag{23}$$

let the attack is launched at time τ, the solution of (23) is,

$$\delta(t) = e^{A^c t}\delta(0) + \int_0^t e^{A^x(t-\tau)}X^a dt + \int_0^t e^{A^u(t-\tau)}U^a dt \tag{24}$$

However, the first term is decaying to zero, the second and the third term is nonzero and their steady-state values depends on the attack vectors alongside cyber system connectivity. Therefore, the PCC control objective cannot be satisfied. ■

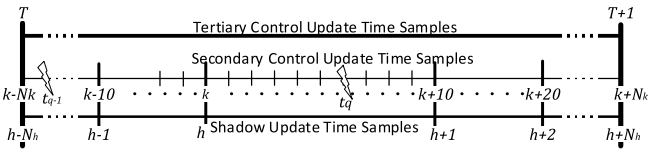

Fig. 4. Overall time-scales discrimination.

IV. IoT Shadow and DT Representation

The CPS hybrid models are combined into a single concatenation dynamical model from both systems (9) and (19) to represent the overall system behaviour. The series concatenation operation is performed [29]. The hybrid system model is represented as,

$$\begin{bmatrix} \dot{X}^{\Theta} \\ \dot{X}^{\Psi} \end{bmatrix} = \begin{bmatrix} A^{\Theta} & \mathbf{0} \\ B^{\Phi}C^{\Theta} & A^{\Phi} \end{bmatrix} \begin{bmatrix} X^{\Theta} \\ X^{\Psi} \end{bmatrix} + \begin{bmatrix} B^{\Theta} \\ \mathbf{0} \end{bmatrix} \begin{bmatrix} U^{\Theta} \end{bmatrix} \quad (25)$$

$$\begin{bmatrix} Y^{\Theta\Psi} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & C^{\Phi} \end{bmatrix} \begin{bmatrix} X^{\Theta} \\ X^{\Psi} \end{bmatrix} \quad (26)$$

where $Y^{\Theta\Psi}$ is the hybrid model output.

A. IoT Shadow Representation

The shadow states represent the monitored cyber and physical states for provisioning the CPS activity every h time instant. A chosen physical sensor ψ transmits its local microgrid measurements to the virtual space (cloud) and the transmitted state is subjected to noise σ^{Ψ}. The shadow of the physical states $\mathcal{Z}^{\Psi}$ is provisioned by matrix S^{Φ} as follows,

$$z^{\Psi}(h) = S^{\Phi}C^{\Phi}X^{\Psi}(h) + \sigma^{\Psi}(h) \quad (27)$$

Similarly, the cyber system controller state φ is reported as a cyber shadow state $\mathcal{Z}^{\Theta}$ to the cloud by provisioning matrix S^{Θ} as follows,

$$\mathcal{Z}^{\Theta}(h) = S^{\Theta}C^{\Theta}X^{\Theta}(h) + \sigma^{\Theta}(h) \quad (28)$$

where the transmitted data has noise σ^{Θ}.

In addition to the periodic shadow update every sample time h, the occurrence of an event q is assumed to update the shadow to $\mathcal{Z}(t_q)$ that has the following representation,

$$z_i(h) = \left\{ z_i\left(t_{q-1}\right), z_i\left(t_q\right), t_{q-1}, t_q, z_{\varrho}\left(t_q\right) \right\} \quad (29)$$

where t_{q-1}, t_q are the times of the last two consequence events and $\mathcal{Z}^{\varrho}(t_q)$ is the reported malicious neighbour agents of i^{th} agent. Figure 4 shows the discrimination between the different time scales of secondary, tertiary and shadow updating rates.

The tertiary controller and the secondary controllers update the control input every T and k time instances, respectively. The shadow updates occur every h time instance and/or every event trigger instant t_q. To monitor the security of the system activity and reduce the communication burden with the cloud system, the shadow update is assumed to be $T \gg h > k$ during the normal periodic update.

B. Luenberger Observer (LO) Based DT Constructor

Using the LO, *multi-What-If* scenarios are constructed and tested to authenticate the healthy desired control state. Given the linear system, which represents the dynamics of the CPS in (9), (19), (25)-(26), the LO is constructed firstly for the full healthy state as,

$$\left.\begin{aligned} \widehat{\mathcal{X}}_i(h+1) &= \Lambda\widehat{\mathcal{X}}_i(h) + \Gamma\mathcal{U}_i(h) + \ell_i\Big(\mathcal{Y}_i(h) - \hat{\mathcal{Y}}_i(h)\Big) \\ \hat{\mathcal{Y}}_i(k) &= \Upsilon\widehat{\mathcal{X}}_i(h) \end{aligned}\right\} \quad (30)$$

where $\widehat{\mathcal{X}}_i$ is the estimated state that is calculated according to the control input $\mathcal{U}_i$ and the measurement $\mathcal{Y}_i$. The LO is constructed by assigning the control input and the measured output based on the shadow states of the cyber and physical systems such that Λ and Υ are full ranked. According to the realtime CPS topology, the observer parameters Λ, Γ and Υ are built to represent the last shadow state. The LO gain ℓ_i is selected such that the eigenvalues of $(\Lambda - \ell\Upsilon)$ is stabilizable. During the normal healthy operation, the observer input is set to the desired state at the PCC, $\mathcal{U}_i(h) = \mathcal{Z}_0(h)$ and the observer measured output is set to the reported shadow states $\mathcal{Y}_i(h) = \mathcal{Z}_i(h)$. Also, the observation error $\|\mathcal{Z}_i(h) - \mathcal{O}_i\widehat{\mathcal{X}}_i(h)\|_2^2$ is decaying to zero, where $\mathcal{O}_i = [\Upsilon_i, \Upsilon_i\Lambda, \ldots, \Upsilon_i\Lambda^{t-1}]^T$ is the block of the output parameter for the set of shadow states during time period t. The LO observer is rewritten as,

$$\left.\begin{aligned} \widehat{\mathcal{X}}_i(h+1) &= \widetilde{\Lambda}\widehat{\mathcal{X}}_i(h) + \tilde{\Gamma}\tilde{\mathcal{U}}_i(h) \\ \widetilde{\Lambda} &= \Lambda - \ell_i\Upsilon_i \\ \tilde{\Gamma} &= \begin{bmatrix} \Gamma & \ell_i \end{bmatrix} \\ \tilde{\mathcal{U}}_i &= \begin{bmatrix} \mathcal{Z}_0 & \mathcal{Z}_i \end{bmatrix}^T \end{aligned}\right\} \quad (31)$$

If a set of the observed states are non-decaying to zero error, these states' indices are recorded in ϱ. Then, the LO is reconstructed to checking the satisfiability such that,

$$\lim_{h\to\infty} \operatorname{supp} \left\| \mathcal{Z}_i(h) - \mathcal{O}_i\widehat{\mathcal{X}}_i(h) \right\|_2^2 \leq TH \quad (32)$$

for constant TH, which is selected based on the composite noise from the cyber edge to the cloud. The observer gain ℓ_i is chosen such that $\widetilde{\Lambda}$ has the characteristic polynomial $d(s) = s^n + a_1 s^{n-1} + \cdots + a_n$ of the healthy case. To guarantee that condition, a linear coordination transformation of the observer parameter matrices is applied as [30, Proposition 2.3] as,

$$\begin{aligned} \widetilde{\Lambda}^t &= I_n \otimes \begin{bmatrix} -a_1 & -a_2 & \cdots & -a_{n-1} & -a_n \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \\ \tilde{\Gamma}^t &= I_n \otimes \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \end{bmatrix}^T \end{aligned} \quad (33)$$

Remark 2: The LO purpose is to estimate the suspicious data source of each set of shadow states. After that, the suspicious indices vectors are compared logically, which eventually defines the bad data source which will be discussed in Algorithm 1 and 2. The presence of the adversarial input ξ, the LO can be defined as follows,

$$\widehat{\mathcal{X}}_i(h+1) = \widetilde{\Lambda}\widehat{\mathcal{X}}_i(h) + \widetilde{\Gamma}\tilde{\mathcal{U}}_i(h) + \tilde{B}\xi(h) \quad (34)$$

which leads to the error dynamics can be derived from (22)-(23),

$$\dot{\delta}_i = \widetilde{\Lambda}\tilde{\delta}_i + \widetilde{B}\xi_i \quad (35)$$

Algorithm 1 Digital Twin Algorithm on Cloud

Initialize *DT* model and import auxiliary functions
Connect to *IoT* Core and Shadow Service
Construct full state *DT* using *LO* such that:
$\tilde{\mathcal{U}}_i = \begin{bmatrix} \mathcal{Z}_0 & \mathcal{Z}_i \end{bmatrix}^T$, $rk(\tilde{\Lambda})$ is full
Initialize security event function $q = 0$
while *True* **do**
  Estimate the full state, $\widehat{\mathcal{X}}_i(h+1) = \widetilde{\Lambda}\widehat{\mathcal{X}}_i(h) + \widetilde{\Gamma}\tilde{\mathcal{U}}_i(h)$
  if $\exists\ i$ s.t $\left\| \mathcal{Z}_i(h) - \mathcal{O}_i\widehat{\mathcal{X}}_i(h) \right\|_2^2 \leq TH \vee q \neq 0$ **then**
    Launch security authentication and audit function,
    $\Xi_{t_q+1}(\eta, \widetilde{\Lambda}, \tilde{\Gamma}, \widehat{\mathcal{X}}) = \text{AuthAudit}\left(\mathcal{Z}_{t_q}, \varrho_{t_q}\right)$
    Reconstruct *DT* with the healthy model Ξ_{t_q+1}
  else
    Keep the full *DT* $\Xi_{t_q+1} = \Xi_{t_q}$
  Update $\mathcal{Z}_i^{des}(h)$ ▷ update desired shadow → edge

The residual estimate that resulted from adversarial input is estimated as,

$$\pi_i(h) = \left\| \mathcal{Z}_i(h) - \mathcal{O}_i\widehat{\mathcal{X}}_i(h) \right\|_2^2 - TH \tag{36}$$

under an attack, $\pi_i(h)$ is non-decaying to zero according to [31, Th. 2].

V. Digital Twin Based Secured Control

The proposed cloud-based DT provides an end to end security audit solution for the ECPS even with multiple coordinated attack scenarios. The proposed solution has two parts; the first one is implemented on the cyber edge and the second part is built as a function on the cloud. The following subsections discuss the two parts.

A. DT Cloud Algorithms

The physical, cyber and cyber-physical twin models are built as auxiliary functions as discussed in the previous sections. Algorithm 1 shows the DT algorithm that is implemented on the cloud. The DT models' functions are imported and the connection with IoT core and shadow services are launched. Then, the DT is constructed based on the LO by mapping the shadow states to the LO input vector. The system is assumed to be secure initially by setting $q = 0$. The DT loop starts by continuously estimating the ECPS full states. If a conflict between the shadow states and the estimated state is detected or a security audit is requested by a control agent, the authentication and auditing functions will be initiated at t_q. This function is discussed in Algorithm 2. The purpose of the function is to return the secured observer and states, which are used to reconstruct the healthy model after the event Ξ_{t_q+1}. The healthy desired state is updated on the IoT shadow, which will be used later by the edge controllers.

To guarantee a healthy estimation of the desired control action and to discriminate between the healthy and the attacked state, Algorithm 2 is used. The shadow states $\mathcal{Z}_{t_q}$ and the conflicted agents ϱ_{t_q} that were determined in Algorithm 1 are utilized to define the malicious agents and their number

Algorithm 2 AuthAudit $\left(\mathcal{Z}_{t_q}, \varrho_{t_q}\right)$

Input $\mathcal{Z}_i^{\Psi}(t_q), \mathcal{Z}_i^{\Theta}(t_q), \mathcal{Z}_i^{\varrho}(t_q)$ ▷ from *IoT* shadow
Define ϱ, N_ϱ and $\tilde{\mathcal{U}}_\varrho$ ▷ parallel *DT* observers
for $\varrho \in 1, 2, \ldots, N_\varrho$ **do**
  Construct *DT* for conflict case ϱ with $\tilde{\mathcal{U}}_\varrho$ such that,
  $rk(\tilde{\Lambda})$ is full
  Compute the residues for i^{th} shadow state,
  $\pi_i(t_q) = \left\| z_i(t_q) - \mathcal{O}_i\widehat{\mathcal{X}}_i(t_q) \right\|_2^2 - TH$
  Normalize the residues, $\pi_i = \pi_i / \|\mathcal{O}_i\|_2^2$
  Sort the residues ascendingly, $\pi_{sort}\ \forall i$
  Choose maximum residues indexes,
  $\mathcal{J} = \text{Max}(\pi_{\text{sort}}).\text{Index}$
  Convert non-zero indices $\mathcal{J}$ into Boolean vector Ω_ϱ
  Store $\mathcal{J}$, Ω_ϱ and $\widehat{\mathcal{X}}_\mathcal{J}$
Confirm the attacked agents/sensors indices,
$\mathcal{F} = \text{supp}\left[\Lambda_{\varrho=1}^{N_\varrho}\Omega_\varrho\right], \eta = \neg\mathcal{F}$
Transform $\widetilde{\Lambda}, \widetilde{\Gamma}$ according to η and (33)
Return $\eta, \widetilde{\Lambda}, \tilde{\Gamma}, \widehat{x}_\eta$

ϱ and N_ϱ. Then, parallel DT observers will run by configuring the inputs with the malicious data sources $\tilde{\mathcal{U}}_\varrho$. For each malicious data source, the residues (36) is calculated, normalized and sorted ascendingly to choose the most suspicious data source indices $\mathcal{J}$.

For each iteration, the indices $\mathcal{J}$, its Boolean representation Ω_ϱ and their estimated states $\tilde{\mathcal{X}}_\mathcal{J}$ are stored. Finally, the indices of the confirmed attacked agents $\mathcal{F}$ are calculated as,

$$\mathcal{F} = \text{supp}\left[\bigwedge_{\varrho=1}^{N_\varrho}\Omega_\varrho\right] \tag{37}$$

and the equivalent secured LO is rebuilt using the healthy states η based on (33) to be returned to Algorithm 1.

B. Resilient Distributed Control Algorithm

In the NMG, the leader nature is different as compared with the follower's nature. The attack on the leader can cause a complete disruption for the microgrid cluster. Therefore, the proposed methodology in this paper is to have maximum security level by authenticating every incoming update from the PCC agent. However, the followers depend on their neighbours to estimate the control update and the isolation of the attacked follower can retrofit the control system back to consensus. Consequently, one algorithm for the leaders and a different one for the followers are proposed to guarantee the system security without increasing the system complexity or utilizing higher communication bandwidth.

1) Cluster's Leader Agent Algorithm: Algorithm 3 shows the secured control for the leader i^l of MG cluster. Firstly, the agent is initialized by assuming a secure state. The leader subscribes on edge for the main leader (PCC) state. If a change in the leader state or a security event is triggered, the desired shadow state $\mathcal{X}_{i^l}^{des}$ is received from the IoT shadow. Either the received PCC state from the edge does not match the DT desired or the DT already confirmed that agent 0

Algorithm 3 Cluster's Leader Resilient Control Algorithm

Initialize *MG* cluster's leader i^l agent, $x_{i^l}, \varrho_{i^l}, \omega_{0,i^l}$
$k = 0$
while *True* **do**
  Receive *PCC* agent 0 state,
  $x_0(k)$ ▷ subscribe on edge
  if $(|\Delta x_0(k)| > 0) \vee (q = 1)$ **then**
    Control update event triggered,
    Receive desired shadow state,
    $\mathcal{Z}_{i^l}^{des} = \left\{\widehat{\mathcal{X}}^{des}(h), \mathcal{F}\right\}$ ▷ get *IoT* Shadow
    if $\left(x_0(k) \neq \hat{\mathcal{X}}^{\text{des}}(h)\right) \vee (\mathcal{F} = PCC)$ **then**
      Declare *PCC* agent attacked and excluded,
      Cloud *DT* is tertiary controller,
      $x_{i^l}(k+1) = \widehat{\mathcal{X}}^{des}(h)$
    else
      PCC state accepted, $x_0(k)$
      $x_{i^l}(k+1) = x_0(k)$
    Send new state to neighbours,
    $x_{i^l}(k+1)$ ▷ publish to edge
    Send reported state, $\mathcal{Z}_{i^l}$ ▷ update IoT shadow
    Send secured state to i^l primary controller
  else
    No Update, $x_{i^l}(k+1) = x_{i^l}(k)$
  $k = k + 1$

is attacked. The PCC is excluded and the DT on the cloud became a tertiary controller temporary by directly utilizing the DT estimated desired $x_{i^l} = \widehat{\mathcal{X}}^{des}$. If the PCC healthy, the edge update is accepted. Afterwards, the updated state is published to the edge, the cloud IoT shadow is updated and the primary controller of this MG is actuated by this healthy control action.

2) Followers Agent Algorithm: Algorithm 4 is implemented on the follower agents. After initialization and receiving the neighbour's data from the edge, the update event is checked by watching if the neighbour's states change exceeds ϵ or the security event q is triggered. Then, The Kullback-Leibler divergence KL_i is used to check if the neighbours diverge from the consensus.

$$KL_i\big(x_j \| x_{j+1}\big) = \sum_{j \in n_i} x_j \cdot \log\left(\frac{x_j}{x_{j+1}}\right) \tag{38}$$

where x_j and x_{j+1} are the neighbours of the follower i. An auditing request q will be activated if $KL_i > \aleph$. The desired estimated state by DT is received from the IoT shadow $\hat{\mathcal{X}}^{des}$. A neighbour agent is marked as a malicious agent if it has the highest *KL*. Then, the shadow is updated by states $\mathcal{Z}_{i^f}^{\Psi}, \mathcal{Z}_{i^f}^{\Theta}$ and the candidate malicious index $\mathcal{Z}_{i^f}^{\varrho}$. The cloud DT feedback is received from Algorithm 1 and 2 that ensures the healthy desired state $\mathcal{Z}_{i^f}^{des}$. The adjacency matrix wights are modified according to $\mathcal{F}$. Finally, using the healthy state, the consensus is updated by (13) and (14) and the secured final state is published to the edge and updated on the cloud IoT shadow.

Algorithm 4 Followers Resilient Control Algorithm

Initialize *MG* follower i^f agent, $x_{i^f}, \varrho_{i^f}, \omega_{i^f,j^f}$
$k = 0$
while *True* **do**
  Receive $j^f h$ follower agent state,
  $x_j(k)\ \forall j = \{1, 2, ..., n_i\}, j \neq i$ ▷ subscribe on edge
  if $\left(|\Delta x_j(k)| > \epsilon\right) \vee (q = 1)$ **then**
    Control update event triggered,
    Estimate Kullback-Leibler divergence KL_i, (38)
    if $|KL_i| > \aleph$ **then**
      Malicious activity detected, DT audit request,
      $\widehat{\mathcal{X}}^{des}(h)$ ▷ get *IoT* Shadow
      Find diverged neighbours from desired $\widehat{\mathcal{X}}^{des}$
      Send reported state to the cloud,
      $\mathcal{Z}_{i^f} = \left\{\mathcal{Z}_{i^f}^{\Psi}, \mathcal{Z}_{i^f}^{\Theta}, \mathcal{Z}_{i^f}^{\varrho}\right\}$ ▷ update IoT shadow
      Receive the desired state and attacked agent,
      $\mathcal{Z}_{i^f}^{des} = \left\{\widehat{\mathcal{X}}^{des}(h), \mathcal{F}\right\}$ ▷ get *IoT* Shadow
      Exclude the attacked agent, $\omega_{i^f,\mathcal{F}} = 0$
    else
      Neighbours state $x_j(k)$ accepted, $\omega_{i^f,j^f} = 1$
    Information update until consensus using (13)-(14)
    Send new state to neighbours,
    $x_{i^f}(k+1)$ ▷ publish to edge
    Send reported state, $\mathcal{Z}_{i^f}$ ▷ update IoT shadow
    Send secured state to i^f primary controller
  else
    No Update, $x_{i^f}(k+1) = x_{i^f}(k)$
  $k = k + 1$

VI. Digital Twin Implementation

The proposed system is implemented practically by developing two main platforms. Locally, the distributed controllers are implemented on embedded single board computers. Remotely, cloud computing is implemented on AWS cloud vendor. Figure 5 shows the practical implementation.

A. Embedded Distributed Control Platform

The distributed controllers use the onboard WiFi modules to communicate locally with each other via UDP protocol and to communicate with the upper cloud layer via TCP/IP protocol. The networked control algorithms and the communication interface settings are applied on embedded *Raspberry-Pi3B+* toolkits as control agents using Python Programming.

A Data Distribution Service (DDS) [20] middleware interface is used to share the control parameters locally within the control edge. The DDS is machine-to-machine connectivity that can be implemented locally without message broker. We used rticonnextdds-connector Python package [32] to configure the publish/subscribe connectivity on each embedded controller. Both the connectivity and the communication QoS are configured using an XML configuration file. This configuration guarantees lower latency, packet-loss mitigation and IT security batches.

To communicate with the cloud, an MQTT client is created using AWSIoTPython SDK to exchange messages. On

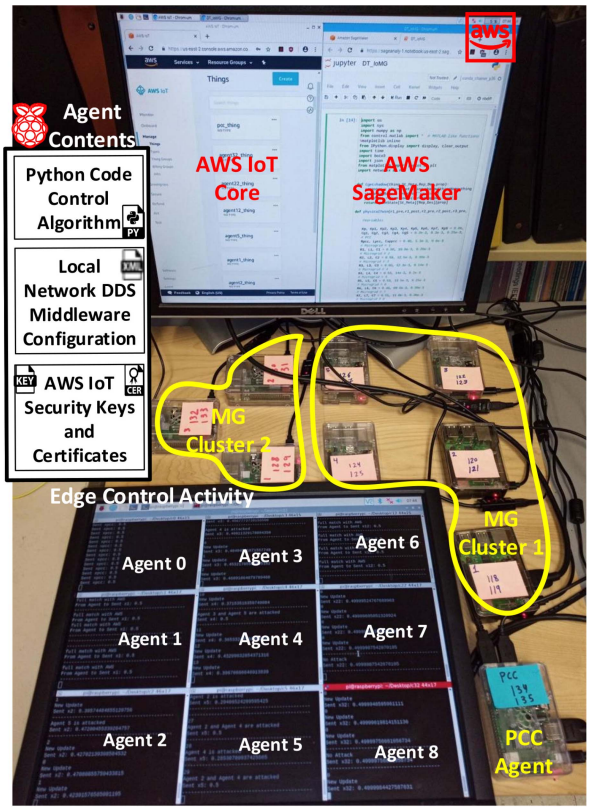

Fig. 5. Practical distributed control and DT implementation.

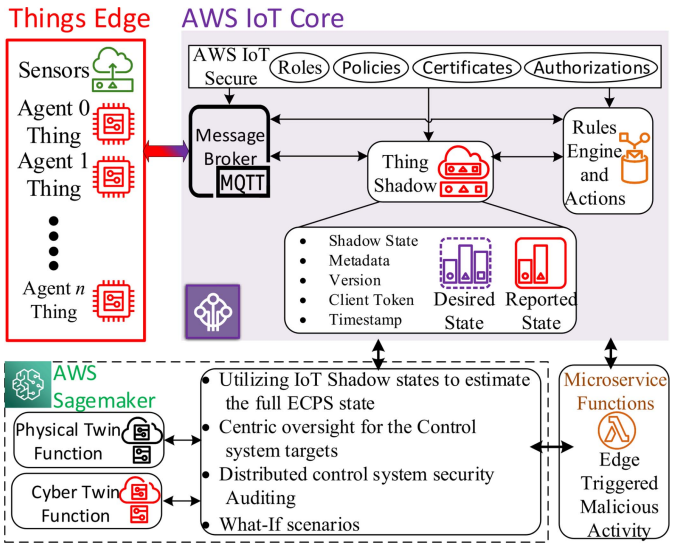

Fig. 6. Digital Twin Description.

AWS, HTTPS, WebSockets and MQTT protocols are available to interact with the cloud. The MQTT is selected due to its low latency for small messages [33]. On each device, the generated keys and certificates are attached and configured to define the device on the AWS cloud computing platform [18]. Those authentication files are generated during the creation of each thing on AWS IoT Core. Each device has a detailed model for its microgrid to emulate the real physical system. We implemented an event-based callback function to trigger the data interaction based on the events. The cloud communication has higher latency compared to edge communication. Performance analysis of the local DDS communication and the remote MQTT communication will be discussed in the next section. It is worth mentioning that the sampling rate of the edge control system and the shadow sampling rate are assumed to be $k = 0.2s$ and $h = 2s$, respectively. The thresholds are set as $\epsilon = 0.01$, $\aleph = 0.035$ and $TH = 0.05$.

B. Cloud Computing Platform

Numerous components involved in the ECPS requires a flexible, reliable and integrated system which can deal with the IoT complexities. The cloud computing services cover these needs by including computing servers, databases, networking, analytics, intelligence over the Internet. Figure 6 shows the functional block diagram of the implemented services.

1) AWS IoT Core: The IoT Core is a cloud service that enables things to connect securely and interact with different cloud services and applications. Each thing is registered on the cloud. The IoT policy is created to control the access and allows/denies a predefined service to be accessed by the thing. Then, the created policies are attached to each thing's certificate. On the edge of the things, each sensor/controller is configured by attributing the generated keys and certificates to its device. One of the default settings in the thing policy is the access of the MQTT message broker to the thing. The MQTT communication protocol is used to interact (get and update) with the shadow of the things on the AWS cloud. The thing shadow is a JSON payload that is used to store and retrieve the things' last states. The contents of the shadow file are shadow states, asset metadata, update version, client token and the timestamp of the last transaction. The shadow has two categories; the reported states $\mathcal{Z}_i$ and the desired states $\mathcal{Z}_i^{des}$. The metadata holds a tuple of the constant parameter of each microgrid as the power and voltage ratings, the location, the owner and the updated version. Also, one of the main IoT core components is the rule engine, which is the filters, that takes actions on the fly based on predefined rules. The actions can be activated by a cloud microservice function, which is the AWS Lambda function.

2) AWS Lambda Function: The AWS lambda-Function is a service less computing function that can trigger a computing service in response to a detected event or a predefined logic/task. In this paper, the security audit event q is managed by the lambda-function. Besides, it can update the tertiary control and management objective, launch a response to grid ancillary service during a contingency, guide the secondary control layer or response to restoration request after a blackout.

3) AWS SageMaker: The AWS SageMaker is integrated and managed computing service. In this paper, the physical twin, the cyber twin and the hybrid ECPS models are implemented as functions to be imported by different tasks and applications. In addition to the centric oversight and security auditing applications, the Sagemaker is used to guide the distributed controllers and runs what-if scenarios using LO based DT.

C. Attack Emulation

The false data injection attacks are artificially soft coded and is implemented on each controller to emulate the attacker. The attacked agent, attack vector, and the attack time instant are predefined according to the required emulation. For the attacks on the edge controllers, the artificial attack agent is can join the network, subscribe on data and publish under the topic name of the infected real agent. Also, it has been designed to be able to publish/subscribe on/to the cloud messages. According to the required study, the attacker agents can be configured to launch an attack on the link between the infected agent and its neighbor(s). Also, the attacker agent is configured to mislead the cloud by reporting a healthy state to it while publishing faulty data to the edge. By the same emulator, the multi-coordinated attacks can be launched on multiple agents to degrade the consensus. This can be done by activating the soft-coded attacks on multiple agents simultaneously. The Denial of Service (DoS) attacks, network delay and the packet loss emulation are implemented using a network emulation software. In this paper, NETEM tool is utilized. The network corruption, the switched delay and the packet loss probability functions are used to implement the DoS, the delay and the packet loss, respectively.

VII. Results and Discussion

To validate the effectiveness and the performance of the proposed methodology, multiple scenarios are tested.

A. False Data Injection Attack

Figure 7 shows the first scenario of multiple coordinated attacks on the first cluster's leader (agent 1) and agent 4, at $k = 55$ and $k = 75$, respectively. Figure 7(a) shows the states on the edge cyber system. The edge system detected a malicious activity and the suspected agents were 1, 4 and 5. The left axis in Fig. 7(b) shows the reported IoT shadow states and the desired state. On the right-hand axis of the second subplot, the attacked agents are depicted. Agent 5 has been temporarily declared as an attacked during $h = 3$ to 4 because of the delay produced by the algorithms' initialization. In addition, the divergence of Agent 5 away from the desired state at $h = 10$ to 12 is resulted by the attack on agent 4. The DT based authentication is able to find the new healthy desired state and confirm that Agents 1 and 4 are attacked. Therefore, even though Agent 5 has been subjected to the delay and misleading, the agent succeeded to use the estimated healthy PCC desired state. to retrofit its consensus dynamics by comparing both neighbors with the DT desired state and mitigate the attack by excluding Agent 4 from the cyber graph. As shown in Fig. 7(c), The DT estimations for the injected power from each microgrid and the voltage at the PCC are very close to the actual simulation. Figure 8 shows the second scenario where Agent 4 is attacked by injecting $x_4 = 0.95$ instead of $x_{i,s.s} = 0.5$.

However, the actual value of $0.5p.u.$ was sent to the cloud to mislead the algorithm by reporting the healthy state. On the edge control system, the attack disturbed the consensus

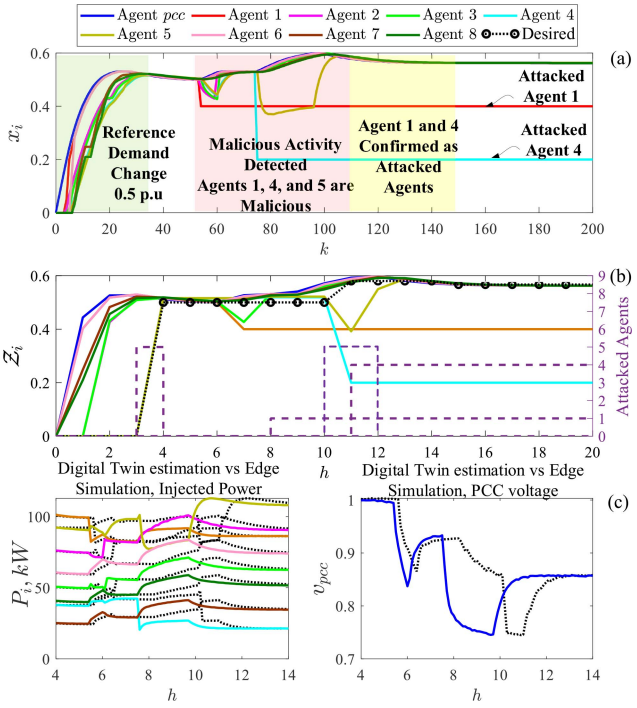

Fig. 7. Response under the multiple attacks on agents 1 and 4 with mitigation.

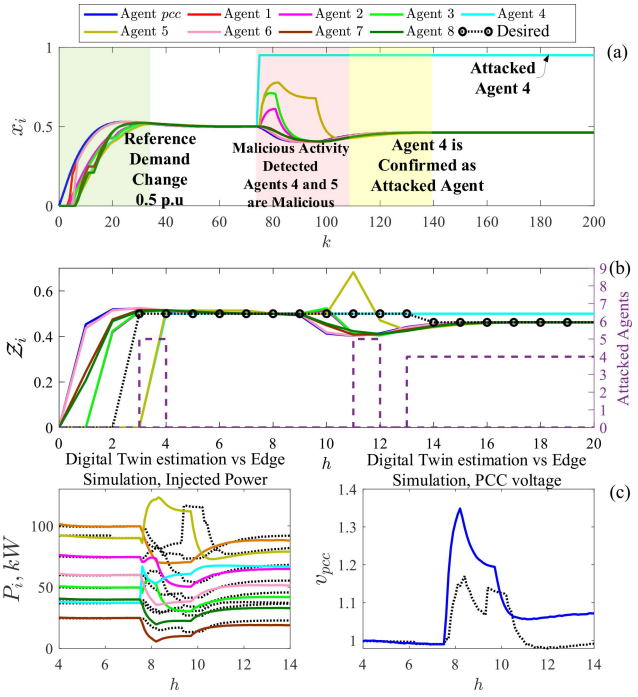

Fig. 8. Response for the attack on agent 4 and cloud misleading with mitigation.

between $k = 75$ to 110. On the cloud, the DT succeeded to calculate the healthy desired sharing factor state.

Based on the ECPS twin model, the DT realized that the edge control system is attacked. It authenticated that the PCC tertiary control shadow state and the PCC sensor state are matching. However, until this time, the DT suspected only Agent 5 (healthy agent). Between $h = 12$ to 13, the DT had no

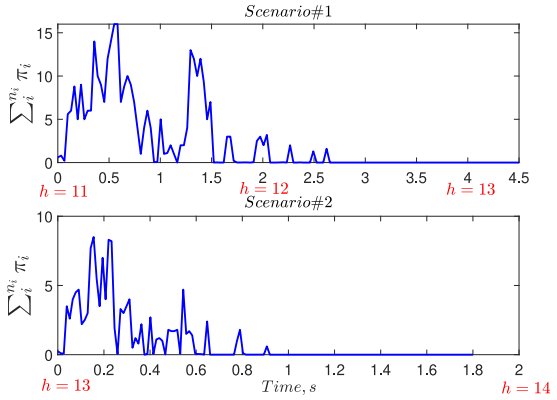

Fig. 9. Total residues during DT based security audit for Scenarios 1, 2.

ability to know the attacked agent because Agent 4 is still misleading them by submitting the healthy state. On the other side, the security auditing algorithm is running. Both Agent 5 and 3 used the desired state and ensured that Agent 4 is attacked. Based on that reported malicious activity, the DT confirmed the attack regardless of the deception. Finally, the neighbor agents succeeded to isolate the attacked agent. The proposed algorithm was able to discriminate between the healthy and the attacked agents even with multiple attacks and the cloud DT is misled.

Figure 9 depicts the summation of total residues of ECPS states for the LO based DT that running during the security audit analysis. The first scenario has higher residues as compared to scenario#2 because the malicious agents in scenario#1 are higher than scenario#2 and the execution time to decay to zero residues is higher in the first scenario.

B. Denial of Service Attack

Scenario # 3, DoS attack is tested on the communication link between the PCC and the leaders. The tertiary controller at PCC requested 40% increase in sharing power but this new command is intercepted by corrupting the communication between the PCC agent and the leaders (agent 1 and 6) as shown in Fig. 10. Primarily, all agents reported a malicious activity due to the difference between the DT shadow state and the edge state, which triggers the PCC authentication function (Algorithm 2). The LO based DT is reconstructed for the reported measurements. The DT observation is used to check the residuals and the healthy desired value is estimated according to Algorithm 1 and 2. Fig. 10(b) shows the shadow of the sharing factors on the cloud and the detected malicious agents using the DT algorithms.

Almost all agents after the attack was a suspicious agent between $h = 6$ and $h = 12$ without certain definition of the infected agent. However, at $t = 13$ the DT algorithms were able to ensure that the PCC agent is the infected source of information. Finally, the proposed platform succeeded to declare that the PCC-to-MG's leader communication links are attacked, and the cloud-based DT became the tertiary controller temporarily and all agents are retrofitted to the healthy state.

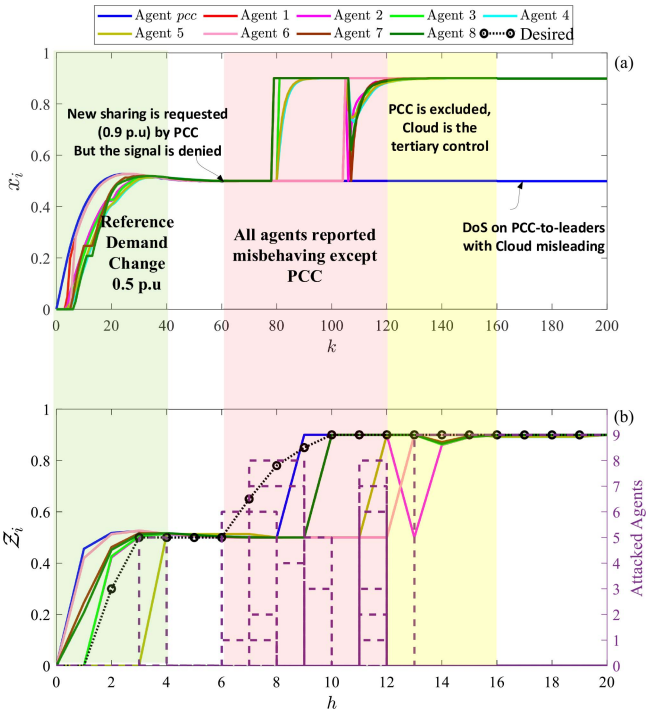

Fig. 10. Response for DoS attack on link between the PCC and leader agents.

C. Communication Platform Performance

The performance of the communication platform is tested for both intra-edge communication (DDS) and edge-to-cloud communication (MQTT). The average intra-edge latency for all agents during previously discussed scenarios is shown in Fig. 11. As shown, the maximum latency recorded in this test is $594\mu s$, which ensures the message delivery using DDS near to the real-time. To estimate the edge-to-cloud communication delay, two events case study is demonstrated to measure the latency. As shown in Fig. 12, the reference sharing factor changes from 0% to 50% at $t = 1s$, then at $t = 21s$ the tertiary command is updated from 50% to 90%. Also, to test the effect of a large delay and packet loss on the performance, the NETEM network emulation tool is used to emulate a delay and packet loss on published data from Agent 2 to both the edge and the cloud. The packet loss is emulated randomly during the whole test to be 5% and $2s$ delay is added intentionally between $t = 24s$ and $t = 26s$. Also, the test is made more challenging by setting the update reporting rate between the edge and the cloud to be one second only.

As illustrated in Fig. 12(a), the edge controllers normally follow the leaders without any noticeable effect of the packet loss on the consensus. Although the $2s$ delay causes a slight disturbance in the consensus dynamics, the communication graph connectivity remains stable and achieved an agreement. Also, the same effect is reflected in the cloud shadow as shown in Fig. 12(b). To measure precisely the delay between the edge and the cloud. The output data from Agent 2 is stamped by the departure time and the arrival time. The difference between the two timestamps is depicted in Fig. 12(c) and zoomed in Fig. 12(d). Except for the 2s delay period, the measured delay between the edge and the cloud did not exceed $300ms$. Another

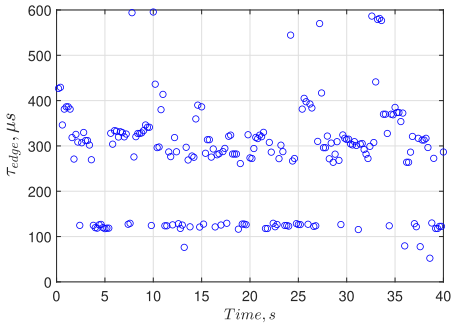

Fig. 11. Average agent-to-agent time delay in the edge (DDS communication).

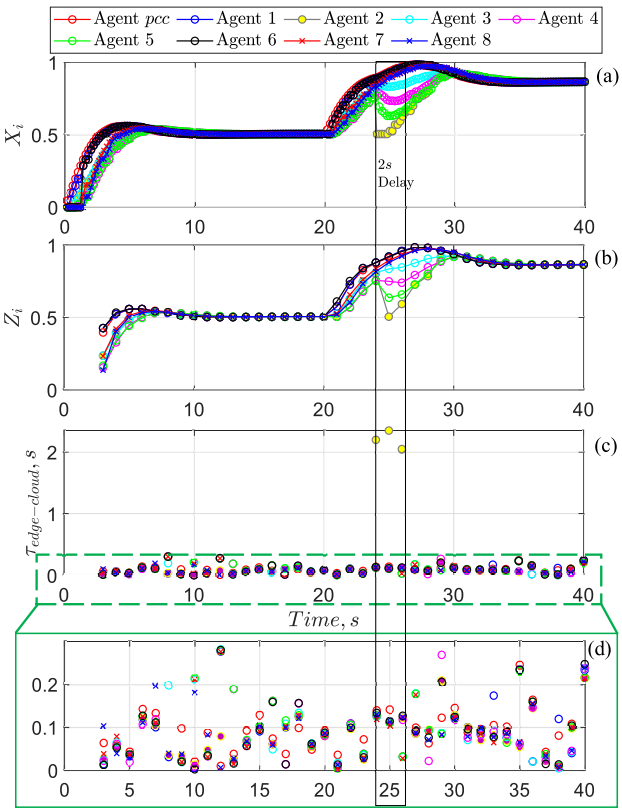

Fig. 12. The performance under 2s delay and 5% packet loss on the communication output from agent 2 to the edge and the cloud channels.

TABLE I
COMMUNICATION PERFORMANCE UNDER DELAY FOR 256B MESSAGES

Middleware	Unicast/Multicast	QoS	$\tau_{,av}$ (ms)	$\tau_{\max}$ (ms)
Edge-edge, DDS	Unicast	Best effort	0.252	0.454
	Multicast	Best effort	0.275	0.622
Edge-cloud, MQTT	Unicast	Level 1	105	301

test is performed to study the effect of the message size, a 256B JSON message is tested.

The average and maximum recorded delay under best QoS effort are shown in Table I for both DDS and MQTT middleware.

VIII. CONCLUSION

In this paper, mathematical formulation and implementation of an IoT based digital twin (DT) for the resiliency of interconnected microgrids was developed. The proposed DT was validated using a practical setup of the distributed control system and Amazon Web Services (AWS). The proposed framework was able to quickly detect and mitigate a different kind of attacks such as false data injection, denial of service, and coordinated attacks. Future research of this work will consider the fusion of deep learning and LO to enhance the speed, accuracy and predictability of the attacks.

REFERENCES

[1] Y. Liu, H. Xin, Z. Qu, and D. Gan, "An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2923–2932, Nov. 2016.
[2] A. Saad, T. Youssef, A. T. Elsayed, A. Amin, O. H. Abdalla, and O. Mohammed, "Data-centric hierarchical distributed model predictive control for smart grid energy management," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4086–4098, Jul. 2019.
[3] R. Moghaddass, O. A. Mohammed, E. Skordilis, and S. Asfour, "Smart control of fleets of electric vehicles in smart and connected communities," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6883–6897, Nov. 2019.
[4] M. H. Yaghmaee Moghaddam and A. Leon-Garcia, "A fog-based internet of energy architecture for transactive energy management systems," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1055–1069, Apr. 2018.
[5] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital twin in industry: State-of-the-art," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2405–2415, Apr. 2019.
[6] D. CeArley, B. Burke, S. Searle, and M. J. Walker, "Top 10 strategic technology trends for 2018," *Top*, vol. 10, pp 1–34, 2016.
[7] J. Poon, P. Jain, I. C. Konstantakopoulos, C. Spanos, S. K. Panda, and S. R. Sanders, "Model-based fault detection and identification for switching power converters," *IEEE Trans. Power Electron.*, vol. 32, no. 2, pp. 1419–1430, Feb. 2017.
[8] M. M. Shabestary and Y. A. I. Mohamed, "Autonomous coordinated control scheme for cooperative asymmetric low-voltage ride-through and grid support in active distribution networks with multiple DG units," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2125–2139, May 2020.
[9] S. Sahoo and S. Mishra, "An adaptive event-triggered communication-based distributed secondary control for DC microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6674–6683, Nov. 2018.
[10] A. A. Saad, S. Faddel, and O. Mohammed, "A secured distributed control system for future interconnected smart grids," *Appl. Energy*, vol. 243, pp. 57–70, Jun. 2019.
[11] M. Yazdanian and A. Mehrizi-Sani, "Distributed control techniques in microgrids," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2901–2909, Nov. 2014.
[12] H. Zhang, S. Kim, Q. Sun, and J. Zhou, "Distributed adaptive virtual impedance control for accurate reactive power sharing based on consensus control in microgrids," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1749–1761, Jul. 2017.
[13] X. Wu *et al.*, "A two-layer distributed cooperative control method for islanded networked microgrid systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 942–957, Mar. 2020.
[14] L. Yang, Y. Zhao, C. Wang, P. Gao, and J. Hao, "Resilience-oriented hierarchical service restoration in distribution system considering microgrids," *IEEE Access*, vol. 7, pp. 152729–152743, 2019.
[15] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731–6741, Nov. 2018.
[16] N. M. Dehkordi and S. Z. Moussavi, "Distributed resilient adaptive control of islanded microgrids under sensor/actuator faults," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2699–2708, May 2020.
[17] J. Duan and M.-Y. Chow, "A resilient consensus-based distributed energy management algorithm against data integrity attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4729–4740, Sep. 2019.
[18] Y. Liu, H. B. Gooi, Y. Li, H. Xin, and J. Ye, "A secure distributed transactive energy management scheme for multiple interconnected microgrids considering misbehaviors," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 5975–5986, Nov. 2019.

[19] Y. Kim, V. Kolesnikov, and M. Thottan, "Resilient end-to-end message protection for cyber-physical system communications," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2478–2487, Jul. 2018.
[20] D. Zhang, L. Liu, and G. Feng, "Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1501–1511, Apr. 2019.
[21] L. Meng, T. Dragicevic, J. Roldán-Pérez, J. C. Vasquez, and J. M. Guerrero, "Modeling and sensitivity study of consensus algorithm-based distributed hierarchical control for DC microgrids," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1504–1515, May 2016.
[22] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, "Detection and mitigation of data manipulation attacks in AC microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2588–2603, May 2020.
[23] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.
[24] F. Wei, Z. Wan, and H. He, "Cyber-attack recovery strategy for smart grid based on deep reinforcement learning," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2476–2486, May 2020.
[25] "IoT: Developer guide. Amazon Web services," AWS Inc., Seattle, WA, USA, Rep. B07JBRCWWZ, 2018.
[26] G. Bachelor, E. Brusa, D. Ferretto, and A. Mitschke, "Model-based design of complex aeronautical systems through digital twin and thread concepts," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1568–1579, Jun. 2020.
[27] J. Liu, W. Zhang, and G. Rizzoni, "Robust stability analysis of DC microgrids with constant power loads," *IEEE Trans. Power Syst.*, vol. 33, no. 1, pp. 851–860, Jan. 2018.
[28] M. Kriegleder, "A correction to algorithm A2 in 'asynchronous distributed averaging on communication networks,'" *IEEE/ACM Trans. Netw.*, vol. 22, no. 6, pp. 2026–2027, Dec. 2014.
[29] J. Climent, D. Napp, R. Pinto, and R. Simões, "Series concatenation of 2D convolutional codes," in *Proc. IEEE 9th Int. Workshop Multidimensional (nD) Syst. (nDS)*, 2015, pp. 1–6.
[30] B. De Schutter, "Minimal state-space realization in linear system theory: An overview," *J. Comput. Appl. Math.*, vol. 121, nos. 1–2, pp. 331–354, 2000.
[31] W. Chen, W. Chen, M. Saif, M. Li, and H. Wu, "Simultaneous fault isolation and estimation of lithium-ion batteries via synthesized design of luenberger and learning observers," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 1, pp. 290–298, Jan. 2014.
[32] RTIcommunity. (2019). *Rticonnextdds-Connector*. [Online]. Available: https://github.com/rticommunity/rticonnextdds-connector-py
[33] AWS. (2020). *Aws IoT Device SDK for Python*. [Online]. Available: https://github.com/aws/aws-iot-device-sdk-python

Ahmed Saad (Graduate Student Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from Helwan University, Cairo, Egypt, in 2007 and 2012, respectively. He is currently pursuing the Ph.D. degree in electrical engineering with Florida International University, Miami, FL, USA. Since 2009, he has been a Teacher and a Research Assistant with the Department of Electrical Power and Machines Engineering, Helwan University. His research interests include integration of renewable energy in smart grids, optimal distributed control and optimization, cyber-physical security, machine learning, Internet of Things, and digital twin.

Samy Faddel (Member, IEEE) received the B.Sc. degree in electrical engineering from Assiut University, Egypt, in 2011, the M.Sc. degree in electrical engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2015, and the Ph.D. degree in electrical and computer engineering from Florida International University, Miami, Fl, USA, in 2019. In 2012, he joined GAEB, Egypt, as an Electrical Engineer up to 2013, where he worked with KFUPM as a Research Assistant. He is currently a Postdoctoral Research Associate with the University of Central Florida. His research interests include integration of renewable energy and energy storage in smart grids, demand response, power system operation, optimization, and control.

Tarek Youssef (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Florida International University, Miami, FL, USA, in 2017. In 2018, he joined the University of West Florida Pensacola, FL, where he is currently an Assistant Professor with the Electrical and Computer Engineering Department. He was a Researcher in several projects funded by the Department of Energy and the Office of Naval Research. He was a Postdoctoral Researcher with Florida International University. His current research interests include focus on cyber-physical security, energy management, and intelligent control of smart grid.

Osama A. Mohammed (Life Fellow, IEEE) received the master's and Doctoral degrees in electrical engineering from Virginia Tech, Blacksburg, VA, USA, in 1981 and 1983, respectively. He is currently a Distinguished Professor and an Associate Dean of Research with the College of Engineering and Computing, Florida International University (FIU), Miami, FL, USA. He is also the Director of the Energy Systems Research Laboratory, FIU and a Professor of electrical and computer engineering. He has authored nearly 800 articles in refereed journals and other refereed international conference records. He has also authored a book and several book chapters and holds 16 patents awarded or filed. He has made numerous keynotes and invited presentations at academic and industrial organizations and conferences worldwide in addition to being general chair of 10 major IEEE international conferences. He is a world-renowned expert on various topics in power and energy systems. Specifically, he has interests in design optimization and physics-based modeling in electric drive systems and other low-frequency environments, electromagnetic signatures, wide band gap devices and switching, and ship power systems modeling and analysis, energy storage systems, and power electronics. Recent research projects included smart-grid distributed control, interoperability, and energy cyber-physical systems. He currently has active research projects with several federal agencies in these areas. He is a recipient of the prestigious IEEE Power and Energy Society Cyril Veinott Electromechanical Energy Conversion Award and the Outstanding Research Award from FIU in 2012, and the 2017 Outstanding Doctoral Mentor at FIU. He is a Fellow of the Applied Computational Electromagnetic Society.