IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 1 September 2023, accepted 15 September 2023, date of publication 20 September 2023,
date of current version 3 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3317799

RESEARCH ARTICLE

Analyzing Replay Attack Impact in DC Microgrid Consensus Control: Detection and Mitigation by Kalman-Filter-Based Observer

MD. ABU TAHER, (Graduate Student Member, IEEE), MOHD TARIQ, (Senior Member, IEEE), MILAD BEHNAMFAR, (Graduate Student Member, IEEE), AND ARIF I. SARWAT, (Senior Member, IEEE)
Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174, USA
Corresponding author: Arif I. Sarwat (asarwat@fiu.edu)

ABSTRACT This paper presents a Direct Current (DC) Microgrid with a consensus-based secondary control strategy to efficiently manage the microgrid, ensuring precise voltage regulation and fair power distribution among Distributed Energy Resources (DERs). The consensus approach employs a communication network to establish a Cyber layer for DER information exchange and harmonize the entire system to achieve a common goal. However, this cyber layer's vulnerability could destabilize the interconnected control system and lead to the whole system being unsynchronized. The paper explores replay attacks conducted in the path of the communication link between interconnected Distributed Generation Units (DGUs), demonstrating their impact on secondary control using simulations and real-time experiments. A method leveraging Distributed Kalman Filter observers for attack detection is proposed which requires low computational demand to suit the real-time application, while an attack mitigation technique using observer-generated residues with the optimal condition is implemented. Validation is conducted through both MATLAB simulations and real-time OPAL-RT emulation, confirming the proposed system's effectiveness.

INDEX TERMS Replay attack, dc microgrid, consensus control, Kalman filter based state observer, communication links, OPAL-RT.

NOMENCLATURE

AC	Alternating Current.
CPS	Cyber-Physical System.
DC	Direct Current.
DCmG	Direct Current microGrid.
DERs	Distributed Energy Resourses.
DGUs	Distributed Generation Units.
PCC	Point of Common Coupling.
SC	Subsystem Controller.
SCADA	Supervisory Control And Data Acquisition.
SM	System Model.

I. INTRODUCTION

DC microgrids have emerged as a novel concept in modern power systems, offering a new approach to energy distribution and management [1]. These microgrids are self-contained, localized systems that can operate independently or in coordination with the main grid, depending on the circumstances [2]. They have gained significance due to their potential to address several challenges faced by traditional AC grids, such as energy loss during transmission, voltage instability, and the integration of distributed energy resources (DERs) and renewable sources [3]. The integration of renewable energy sources, such as solar panels and wind turbines, has become increasingly important to transition towards a more sustainable and environmentally friendly energy mix [4]. However, the intermittent nature of these sources poses challenges for grid stability and reliability [5]. Challenges and instability during PV integration are addressed through a versatile system with five modes, including microgrid separation for sensitive loads during poor power quality [6]. DC microgrids offer a promising solution by allowing for better control over power flow and voltage

The associate editor coordinating the review of this manuscript and approving it for publication was Wonhee Kim.

regulation [7]. In DC microgrids, secondary control plays a crucial role in regulating power sharing and maintaining voltage stability [8]. Unlike primary control, which deals with instantaneous power adjustments to match supply and demand, secondary control focuses on fine-tuning power distribution and voltage levels over slightly longer time intervals [9]. This is essential for ensuring proper coordination among different DERs and loads within the microgrid [10]. By dynamically adjusting the power output of various sources and managing energy storage systems, secondary control helps to avoid voltage fluctuations and imbalances [11]. This aspect is especially critical in microgrids with a high penetration of variable renewable sources. The proper functioning of secondary control contributes to efficient energy utilization and enhances the overall stability of the microgrid [12], [13]. Moreover, the integration of distributed energy resources (DERs) and renewable sources is reshaping the landscape of power systems [4]. Traditionally dominated by centralized fossil-fuel-based power plants, modern power systems are now witnessing a shift towards a more decentralized and sustainable model [14]. DERs, which include solar panels, wind turbines, energy storage systems, and even electric vehicles, are being installed at various points in the grid, closer to the end-users. This not only reduces transmission losses but also allows for a more resilient and adaptable grid structure [15]. Renewable sources, in particular, are abundant and environmentally friendly, but their variability poses challenges for grid operators [16]. DC microgrids provide a platform to effectively integrate these DERs, enabling more efficient use of clean energy resources while ensuring grid stability [7]. The decentralized nature of DC microgrids offers several potential benefits, primarily centered around enhanced energy efficiency and resilience [17]. By operating independently or in a coordinated manner, these microgrids can optimize power distribution based on local demand and supply conditions. This localized decision-making reduces the need for extensive long-distance transmission, which is a common source of energy losses [18]. Furthermore, the ability of DC microgrids to island themselves from the main grid during disruptions enhances the resilience of the energy supply, making them suitable for critical facilities like hospitals, military bases, and remote communities. In the face of natural disasters or grid failures, DC microgrids can continue to provide power, thus improving overall energy security [19].

Consensus-based secondary control is a pivotal mechanism in achieving coordinated power sharing and voltage regulation in DER-based microgrids. This form of control involves a network of intelligent devices communicating and collaborating to make collective decisions [20]. Cooperative control ensures that power sources and loads work in harmony to maintain grid stability [21]. In a DC microgrid, consensus-based secondary control enables real-time adjustments of power outputs based on varying conditions. By sharing information and collectively agreeing on the optimal operating points, DERs can effectively respond to load changes and disturbances. This approach facilitates smooth power sharing and minimizes voltage fluctuations, contributing to reliable and efficient microgrid operation [22].

The functionality of a DC microgrid heavily relies on the interconnection of DERs and their communication link, forming a cyber-physical system (CPS) [20]. CPS integration allows for real-time monitoring, control, and data exchange between physical components and digital systems [23]. CPS-based microgrids enable sophisticated control strategies, predictive maintenance, and optimized energy management [24]. However, this relationship of physical and digital domains also introduces cybersecurity challenges. As the communication network becomes a critical component, the microgrid becomes susceptible to cyber threats that can disrupt its operation [25]. The evolving landscape of cyber threats poses a significant risk to CPS-based microgrids [26]. These threats range from cyberattacks targeting communication infrastructure to malware compromising the control systems [27]. As CPS systems become more complex and interconnected, the potential impact of cyberattacks becomes more severe. A breach in the communication link could lead to miscommunication among DERs, causing instability in power sharing and voltage regulation [25].

Moreover, a cyberattack could manipulate the data exchanged between physical components and control systems, leading to inaccurate decision-making and potentially catastrophic consequences [28]. The vulnerabilities of cyber-physical network (CPS) based control systems in DC microgrids are multifaceted [29]. First, the interconnected nature of DERs and their reliance on communication networks exposes them to potential unauthorized access and control [30]. Malicious actors could exploit vulnerabilities in communication protocols or gain unauthorized access to the control infrastructure [31]. Second, the real-time nature of CPS requires rapid data exchange and decision-making, leaving limited time for thorough cybersecurity checks. This urgency can be exploited by attackers seeking to compromise the system [32]. Third, the heterogeneity of devices and communication standards in a microgrid introduces compatibility and integration challenges, potentially leading to weak points that attackers can exploit [33].

One specific threat that poses a significant risk to consensus-based secondary control in CPS-based microgrids is the replay attack [34]. A replay attack involves an attacker intercepting valid communication between devices and then replaying or resending those messages to deceive the system [35]. In the context of consensus-based control, replay attacks could lead to incorrect decisions being made by the DERs [36]. For instance, if an attacker replays a message indicating a high load demand, the DERs might increase their output unnecessarily, leading to an imbalance in power distribution. Similarly, voltage regulation commands could be replayed, causing erratic voltage levels. The potential disruption caused by replay attacks highlights the need

for robust cybersecurity measures in microgrid control systems [37].

The computational complexity of a Kalman filter-based observer is lower compared to machine learning algorithms. However, it comes with the drawback of being suitable only for simpler models and demanding more computational resources, potentially causing delays in real-time applications for machine learning algorithms. When it comes to predictive capabilities, the Kalman filter-based observer exhibits greater strength than machine learning algorithms. Furthermore, in terms of interpretability, the Kalman filter-based observer surpasses machine learning algorithms, offering a higher degree of clarity and understanding [38], [39] in attack detection and mitigation scenarios. Several machine learning algorithms have been suggested for forecasting cyber intrusions in microgrid networks. Nonetheless, a significant drawback of machine learning lies in its limited adaptability, along with its requirement for substantial computational resources and extensive training data.

While various studies have explored general cybersecurity concerns in microgrids, the specific threat of replay attacks and their potential to disrupt consensus-based control have not been thoroughly investigated, particularly within the context of DC Microgrid scenarios. Notably, Dan Li et al. [40] lack clear validation of their statistical method's efficacy in differentiating replay attacks from equipment faults in SCADA systems, while also omitting scalability considerations and complex system handling [41]. Similarly, another study briefly mentions replay attacks in DC microgrids but lacks in-depth impact analysis and practical defense strategies, with no empirical validation or simulation results [29]. Meanwhile, a paper utilizing recurrent neural networks for real-time intrusion detection in AC microgrids seems disconnected from the focus on replay attacks in DC microgrids, raising questions about the chosen model's relevance [42]. Furthermore, a separate paper addresses microgrid cyber threat resilience but overlooks specific analysis of replay attacks in DC microgrids and lacks robust validation of its proposed countermeasures [43].

Despite the growing recognition of cybersecurity challenges in CPS-based microgrids, there exists a research gap that centers on the lack of comprehensive security analysis of replay attacks in consensus-based secondary control. Addressing this research gap is crucial for developing effective countermeasures and safeguards that can protect CPS-based DC microgrids from replay attacks and ensure the reliable and secure operation of consensus-based secondary control systems to make the whole system harmonious.

The key contributions of this paper can be summarized as follows:

- Implementation of a consensus protocol establishes an intelligent control system, enabling microgrid generation units to achieve proportional power sharing aligned with their capacities.
- Introduction of a replay attack through the communication link effectively illustrates the performance of the consensus-based control system when confronted with attack scenarios.
- Incorporation of a state observer facilitates real-time monitoring of diverse transient conditions, encompassing load fluctuations and replay cyber attacks. Additionally, the successful integration of an attack detection method preemptively mitigates threats, strengthening system stability and reinforcing both resilience and security.

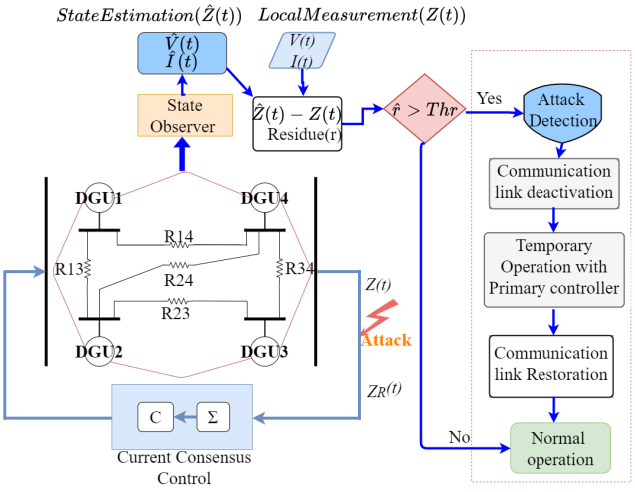

FIGURE 1. Flow diagram of procedure.

The paper is structured as follows: Section II provides a detailed overview of the system description and methodology, which is divided into five subsections. Subsection A covers the microgrid model, explaining its components and functioning. Subsection B discusses consensus or cooperative control, which is a key aspect of the proposed approach. Subsection C focuses on the replay attack model, describing the nature and characteristics of replay attacks in the context of the microgrid. Subsection D introduces the state observer, an essential component for accurate monitoring and control. Lastly, subsection E discusses attack detection and mitigation techniques employed in the system. In Section III, the paper presents the results and analysis of the proposed methodology, evaluating its performance and effectiveness. Following this, Section IV describes the experimental validation conducted to verify the feasibility and practicality of the proposed approach. Finally, in Section V, the paper concludes by summarizing the key findings and contributions of the study.

II. METHODOLOGY

DC Microgrid (DCmG) is defined as a network of distributed generation units (DGUs) as depicted in Fig.1 that are connected and controlled through current consensus loops to ensure proper load sharing across the units. In order to achieve this, each DGU's line current need to be communicated to the others. However, The central current consensus loop

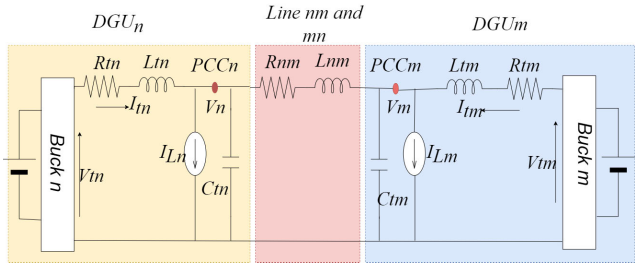

FIGURE 2. Microgrid model.

could be disrupted by attacks that introduce false information through this communication channel. Replay attacks are one type of such attack that involve delaying the communication channel's signals.

A. MICROGRID MODEL

The system involves a DC microgrid (DCmG) comprising of two interconnected distributed generation units, which have been modeled using DC-DC buck converter blocks(Buck n and Buck m), as shown in Figure 2. These sources are connected to each other via a line impedance(R_{mn} and L_{mn}) to form an autonomous DC microgrid, where each source is connected to a transmission line through a point of common coupling (PCC). Additionally, each source is supplied to a DC load. The voltage rating of the input sources is 100V, while the buck converter rating is 48V.

1) GRAPH THEORY

The connectivity among N DER agents in a communication network can be represented by a graph denoted as G = (V, E, A). The graph consists of a set of nodes V, where each node represents a communication agent for a DER, a set of edges E represents communication links for data exchange and A is the N × N weighted adjacency matrix of the graph, with elements $a_{ij} = a_{ji} \geq 0$. If the communication links are bidirectional, denoted as $(V_i, V_j) \in E$, then it implies that $(V_i, V_j) \in E$ for all nodes i and j, making the graph undirected. If the communication links are unidirectional, the graph is considered directed. A graph is said to have a spanning tree if there exists a root node from which there is a directed path to any other node in the graph. An adjacency matrix $A = \{a_{ij}\}_{N\times N}$ can be used to represent the graph, where each element a_{ij} in the matrix signifies the connectivity between nodes i and j [8] and a_{ij} can be defined as

$$a_{ij} = \begin{cases} 1, & \text{if } (\mathcal{V}_i, \mathcal{V}_j) \in \mathcal{E} \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

The time response depends on the size and topology of the communication network. Its behavior can be analyzed through the eigenvalues of the Laplacian matrix L, which is defined as L=D-A. Where A is the adjacency matrix, and D is a diagonal matrix formed by the sum of the elements in each row of the adjacency matrix A, i.e., $\mathbf{D} = \text{diag}\left\{\sum_{j=1}^{N} a_{ij}\right\}$.

The Laplacian matrix is represented as $L = \{l_{ij}\}_{N\times N}$, and the element l_{ij} is calculated from

$$l_{ij} = \begin{cases} -a_{ij}, & i \neq j \\ \sum_{i=1}^{N} a_{ij}, & i = j \end{cases} \tag{2}$$

If there exists a spanning tree rooted at node 0, it ensures that all the eigenvalues of the matrix L have positive real parts. Additionally, if the graph G is undirected, the matrix L becomes symmetrical, and all its eigenvalues are positive. Here, we denote these eigenvalues $0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_N$.

2) CONSENSUS PROTOCOL

The load sharing between the two sources has been achieved through the use of a consensus protocol, which distributes the load in proportion to each source's rating. To achieve proportional sharing of the current, the output current of each source has been divided by its rated current to obtain a per unit current value, which is then inputted into the consensus protocol. A PI controller has been employed to generate an additional voltage correction term, known as δv, which is added to the reference voltage to calculate a new adaptive reference point for each generation unit. Over time, convergence has been achieved as a result of the characteristic behavior of the consensus protocol, which facilitates the proportional sharing of the current based on each source's capacity. Equation (3) can be used to express the voltage set point for a single DG_i:

$$V_{refnew} = V_{ref} + \delta v_i \tag{3}$$

where δv_i represents the voltage correction term derived from equation (4):

$$\delta v_i = G_i(s)\left(V_{ref} - \bar{V}_i\right) \tag{4}$$

where $\bar{V}_i$ is the local estimation obtained from the observer given by equation (5) and $G_i(s)$ is the PI controller for producing the correction term of voltage restoration:

$$\bar{V}_i = V_i + C_E \int_0^t \sum_{i\in\mathcal{N}_i} a_{ji}\left(\bar{I}_j^{pu} - \bar{I}_i^{pu}\right) d\tau \tag{5}$$

In equation (5), V_i is the local measurement of the voltage at i,C_E represents the voltage coupling coefficient,a_{ji} is the adjacency matrix,N_i number of neighbors of i,$\bar{I}_i^{pu}$ is proportional unit current at i and $\bar{I}_j^{pu}$ is proportional unit current at neighbor j. Proportional unit current is defined as Proportional Unit Current =(Actual Current / Rated Current) at each source.

B. REPLAY ATTACK MODEL

A replay attack is a type of security attack that involves intercepting and recording communication signals in a system, and then later replays them to deceive the system into believing that the recorded signals are new and authentic. This type of attack is especially effective when the system

is in a steady state, as it can create the illusion of normal activity while causing significant damage or compromising the integrity of the system. In essence, a replay attack tricks a system into taking a particular action or providing access to sensitive information. It involves an attacker capturing data being sent between two parties and replaying that data back to the system later. Replay attacks can be carried out through various means, including intercepting wireless signals or capturing data packets transmitted over a network. The replay attack in this example has the following structure.

$$Z_R(t) = Z(t) + \beta\,(t - T_R)\,[-Z(t) + Z\,(t - t_0)] \quad (6)$$

In this case, the activation function $\beta\,(t - T_R)$ deviates the signal $Z(t)$ by t_0 and represents the modified signal as $Z_R(t)$.

C. STATE OBSERVER

The model computes the estimates of the model states using the following model and a linear Kalman filter.

$$\dot{V}_n(t) = \frac{1}{C_{tn}} I_{tn}(t) - \frac{1}{C_{tn}R_{nm}} V_n(t) + \frac{1}{C_{tn}R_{nm}} V_m(t) - \frac{1}{C_{tn}} I_{Ln}(t) \quad (7)$$

$$\dot{I}_{tn}(t) = -\frac{1}{L_{tn}} V_n(t) - \frac{R_{tn}}{L_{tn}} I_{tn}(t) + \frac{1}{L_{tn}} V_{tn}(t) \quad (8)$$

State space models represent dynamic systems using a collection of variables called ''states''. These states change over time in accordance with a set of equations. The state variables can be represented as a vector and their evolution equations can be written in matrix form.

$A_k = [-1/(R_{nm} * C_k),\quad 1/C_k;\quad -1/L_k, -R_k/L_k];$
$\mathrm{B_k} = [\theta;\quad 1/L_k];\ \mathrm{M_k} = [-1/\mathrm{C_k};\quad 0];$
$\mathrm{P_k} = \begin{bmatrix} 1 & 0 \end{bmatrix};\ B_m = [1/(R_{nm} * C_k); 0];\ \mathrm{B_{jl}} = [-1/C_k; 0];$
$\text{StateSpace Matrix} = ss(A_k, [B_k, B_m, B_{jl}], H_k, \theta);$

The ss function can be used to convert a system represented by matrices into state space form

D. ATTACK DETECTION AND MITIGATION

The Kalman filter is a recursive estimation algorithm used to estimate the state of a dynamic system based on noisy measurements. It operates on the principles of Bayesian filtering and combines the system dynamics model with the measurements to produce an optimal estimate of the true state. The state space representation of the Kalman filter describes the mathematical equations that define the evolution of the system's state and the estimation process [44].

The state space model for the Kalman filter can be expressed as follows:

State Transition Equation:

$$x(k) = A * x(k-1) + B * u(k) + w(k) \quad (9)$$

In this equation 7, x(k) represents the system state at time t, A is the state transition matrix that describes the evolution of the system state over time, x(k-1) is the previous state, B is the input control matrix, u(k) is the input control vector, and w(k) is the process noise that accounts for uncertainties in the system dynamics.

Measurement Equation:

$$z(k) = H(k) * x(k) + v(k) \quad (10)$$

here, z(k) represents the measurement obtained from the system at time k, H(k) is the measurement matrix that maps the system state to the measurement space, and v(k) is the measurement noise that captures the measurement inaccuracies. Initial State and Covariance:

$$x(0) \sim N(m(0), P(0)) \quad (11)$$

This equation represents the initial state distribution, where x(0) is the initial state vector, m(0) is the mean of the initial state, and P(0) is the covariance matrix that describes the uncertainty in the initial state.

State Prediction:

$$\hat{X(k)} = A * \hat{X(k-1)} + B * u(k) \quad (12)$$

In this equation, $\hat{X(k)}$ represents the predicted state estimate at time t, $\hat{X(k-1)}$ is the previous state estimate, A is the state transition matrix, B is the input control matrix, and u(k) is the input control vector.

Covariance Prediction:

$$P(k) = F(k) * P(k-1) * F(k)\hat{}T + Q(k) \quad (13)$$

here, P(k) is the predicted state covariance matrix at time t, P(k-1) is the previous state covariance matrix, A is the state transition matrix, and Q(k) is the process noise covariance matrix that accounts for the uncertainties in the process model.

Kalman Gain:

$$K = P(k) * H(k)\hat{}T^* \left(H(k) * P(k) * H(k)\hat{}T + R(k)\right)\hat{} - 1 \quad (14)$$

In this equation, K represents the Kalman gain at time t, P(k) is the predicted state covariance matrix, H(k) is the measurement matrix, and R(k) is the measurement noise covariance matrix.

Covariance Update:

$$P(k) = (I - K * H(k)) * P(k) \quad (15)$$

In this equation, P(k) is the updated state covariance matrix, I is the identity matrix, K is the Kalman gain, and H(k) is the measurement matrix.

By iteratively applying these equations, the Kalman filter recursively estimates the true state of the system based on the available measurements. At each time step, the filter predicts the system state and its covariance using the state transition matrix and the process noise covariance. Then, it incorporates the measurement information using the measurement matrix, measurement noise covariance, and the predicted state estimate.

The Kalman filter as in Figure 3 can also be used as a replay attack detection tool in microgrids. A replay attack involves

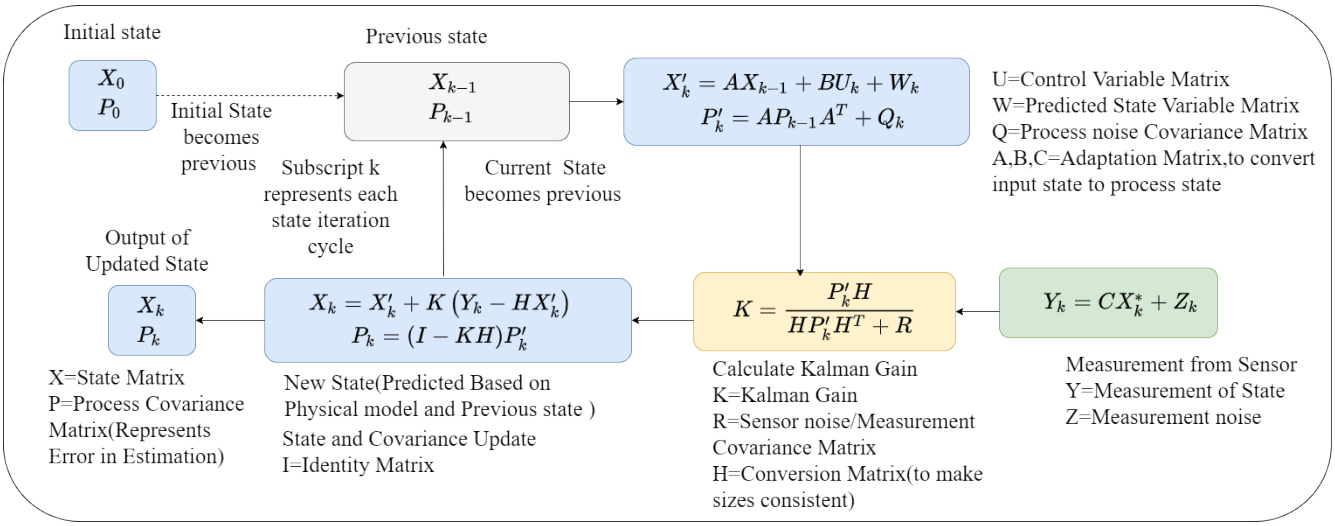

FIGURE 3. Kalman filter process steps for state estimation and error prediction.

an attacker recording legitimate signals or messages and then replaying them later to deceive the system. The Kalman filter can detect these attacks by comparing the received signals to the expected signals based on the system model. If there is a significant difference between the expected and received signals, the Kalman filter can raise an alarm to indicate a possible replay attack. The filter can be a useful tool for enhancing the security of microgrids against replay attacks.

During a cyber attack detected by the state observer, the secondary controllers in each Distributed Generation (DG) unit will be deactivated. This is achieved by temporarily deactivating the communication links that support secondary control. If the communication links are affected, the consensus control becomes unstable and cannot converge to a common point, and the secondary controller is deactivated once the error exceeds a predefined threshold. Once the secondary controllers are deactivated, the primary controllers in each DG unit work independently to supply the load. Once the communication links are restored, normal operation will resume. This approach helps to mitigate the effects of cyber-attacks and ensures that the DG units can continue to operate even in the presence of such attacks.

III. RESULT AND ANALYSIS

A. LOAD CHANGE AND NO ATTACK SCENARIO

In the normal scenario, shown in Figure 4, the initial load current is distributed between two generators, DG1 and DG2, in proportion to their capacity. DG1 supplies 3A and DG2 supplies 6A. At t=1s, the load at DG1 is reduced from 3A to 2A. The consensus control protocol ensures that load changes at one bus affect the generation of both DG units. Thus, both generators share the current proportionally based on their capacity. After 1s, DG1 and DG2 share the current such that the current sharing amounts become 2.3A and 4.7A, respectively. This current sharing ratio is approximately 1:2,

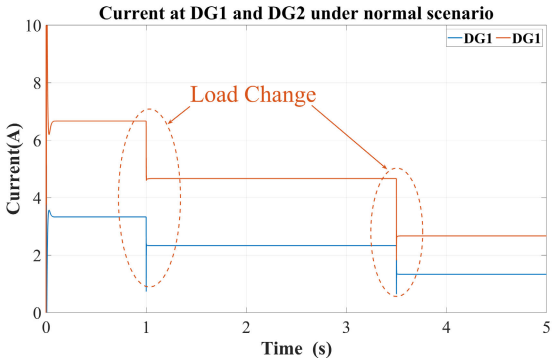

FIGURE 4. Current at DG1 and DG2 under normal scenario.

indicating that the consensus control protocol is effective in ensuring that the generators share the current according to their capacity. At t=3.5s, the load at DG2 is further reduced from 6A to 4.5A. The consensus control algorithm continues to operate and ensures that both generators share the current proportionally based on their capacity. The new current sharing amounts are calculated by the consensus control algorithm, and the current sharing ratio is maintained at approximately 1:2.

In Figure 5, the voltage is maintained at a reference voltage of 48V, regardless of any changes in the load or current sharing ratio. This shows that the consensus control algorithm not only ensures proportional current sharing among the generators but also maintains the voltage at a stable and desired level.

B. ATTACK SCENARIO

However, in the Replay attack scenario shown in Figures 6 and 7, When the load changes, this attack exhibits unwanted behavior. Due to the communication channel delay

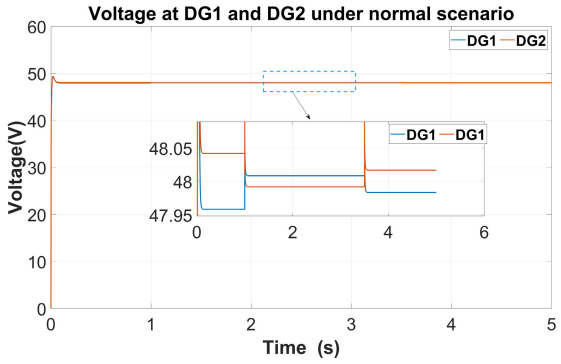

FIGURE 5. Voltage at DG1 and DG2 under normal scenario.

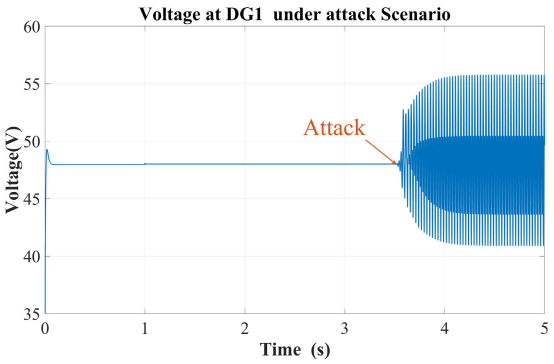

FIGURE 8. Voltage at DG1 under attack scenario.

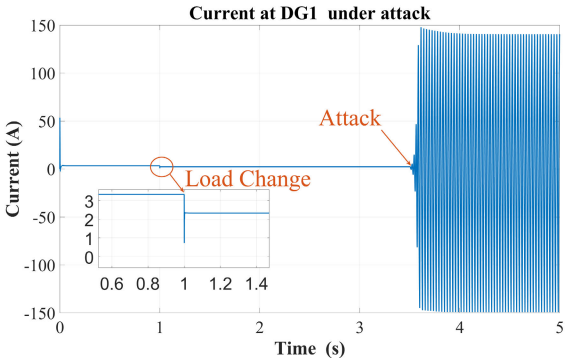

FIGURE 6. Current at DG1 under attack scenario.

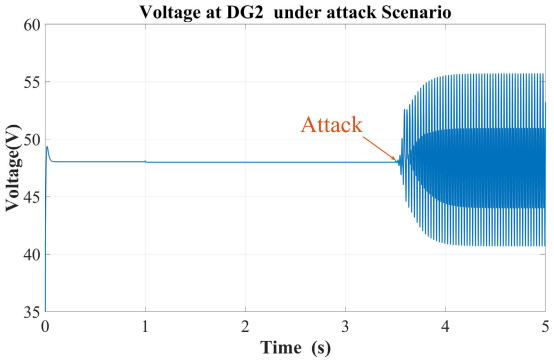

FIGURE 9. Voltage at DG2 under attack scenario.

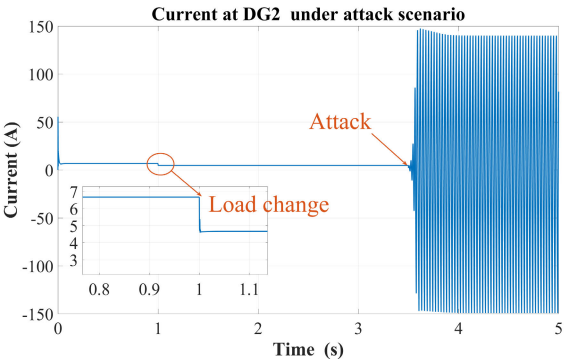

FIGURE 7. Current at DG2 under attack scenario.

implemented by the replay attack, the current consensus control is unable to detect changes in the line current. The attack begins at t = 3s, but it goes undetected while the system is in a steady state. As soon as the load changes at t = 3.5s, the incorrect measurements at the consensus controller result in an unstable system. Within a millisecond of the load change, the line currents go uncontrolled, as depicted in Figures 6 and 7, exceeding the rated capacity which creates a significant risk of harm to the local DGU and other machinery. Figures 8 and 9 show that the current consensus control has failed, leading to uncontrolled current sharing among DG units. This results in the reference voltage deviating from the predefined values, causing it to exceed the 48V limit. As a result, the entire system becomes unstable and uncontrollable. The residual plots, as shown in Figures 10 and 11, provide insight into the response of the system to the attack that occurred at t = 3s. Specifically, these plots show the difference between the observed voltage and line currents and their expected values. Figure 10 reveals that the observed line currents in both DGUs differ from their expected values, and this difference crosses specified thresholds within 4 milliseconds. The attack was directed at the signals from DGU 1, as evidenced by Figure 11 that DGU 2's voltage residueÂ is zero. Figure 11 shows that the observed voltage in DGU 1 differs from its expected value, with the difference crossing a specified threshold within 4 milliseconds.

C. ATTACK MITIGATION SCENARIO

Figures 12 and 13 demonstrate the normal operation of the microgrid without secondary control, where each DG unit serves its individual load. When a load change occurs in one DG unit, the load change is addressed by that particular unit only while the other unit is unaffected as the secondary control of each unit is deactivated due to the deactivation of the communication link. The system stability and security are maintained by ensuring that the current flowing in each DG unit is within the control limit. This highlights the importance

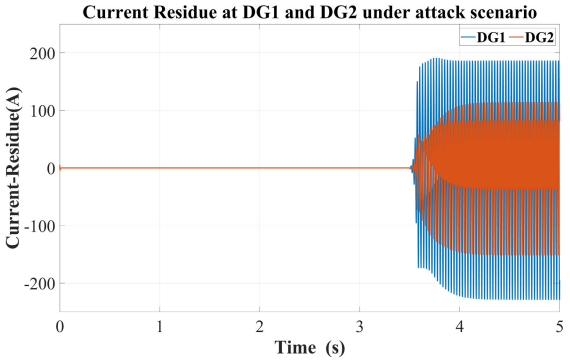

FIGURE 10. Current residue at observer under attack scenario.

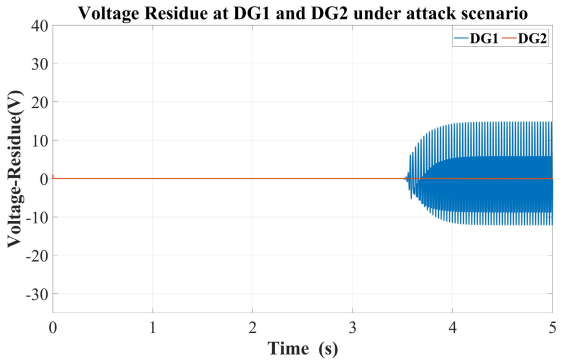

FIGURE 11. Voltage residue at observer under attack scenario.

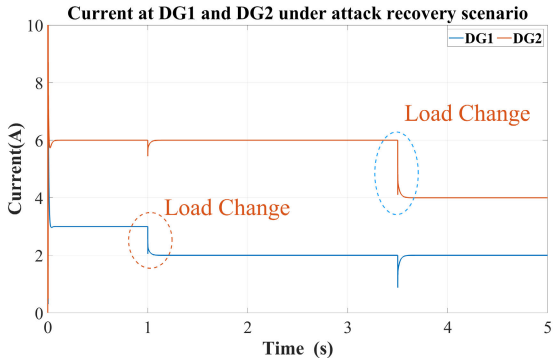

FIGURE 12. Current at DG1 and DG2 under attack recovery scenario.

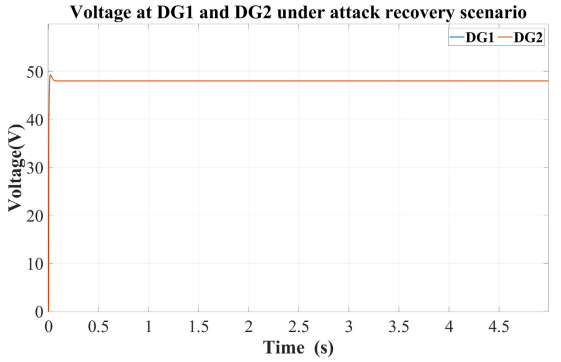

FIGURE 13. Voltage at DG1 and DG2 under attack recovery scenario.

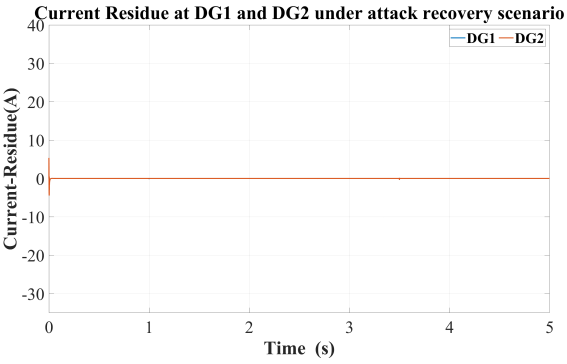

FIGURE 14. Current residue at observer under attack recovery scenario.

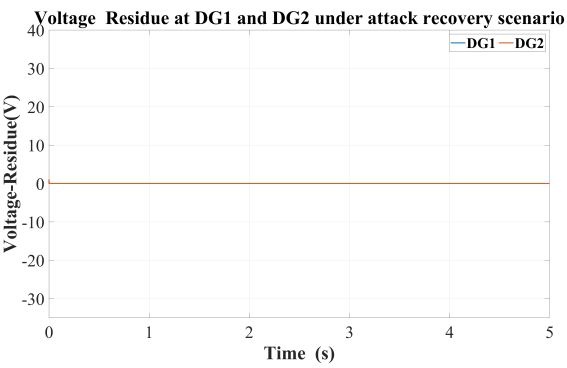

FIGURE 15. Voltage residue at observer under attack recovery scenario.

of controlling and monitoring the current flow to prevent any overloading or instability in the system.

The residual plot shown in Figures 14 and 15 further demonstrates that the system is operating normally during attacks or unusual conditions. These findings provide valuable guidance for designing and managing microgrids in the future.

IV. REAL-TIME VALIDATION

The real-time validation setup using OPAL-RT, MATLAB, and Simulink involves configuring a host PC with MATLAB 2021b and RT-LAB 2023 as in depicted in Figure 16. The Simulink model is developed on the host PC, comprising SM (System Model) and SC (Subsystem Controller) subsystems. Next, the RT-LAB software is installed on the host PC. This software allows for real-time simulation of the Simulink models. The experimental setup is connected to an OP5700 OPAL-RT target, which is a hardware device designed for emulating real-time simulations. The Simulink model, including the SM and SC subsystems, is then loaded onto the OP5700 OPAL-RT target. This step transfers the simulation model from the host PC to the real-time hardware for execution. Once the setup is loaded onto the OPAL-RT target, the simulation is executed in real-time. The control

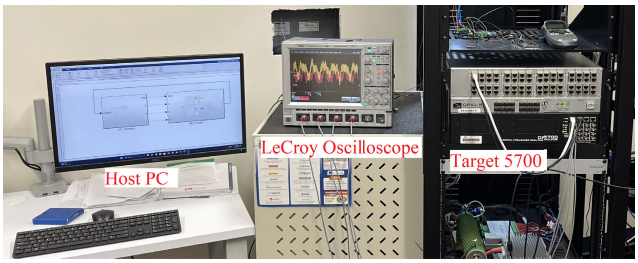

FIGURE 16. Real time validation setup by OPAL-RT.

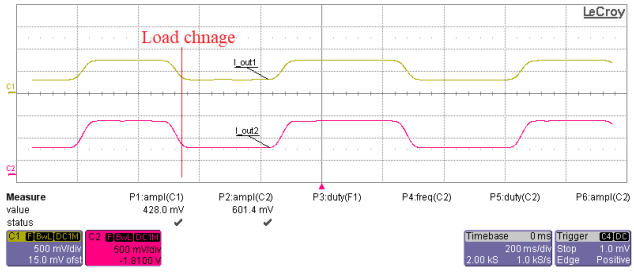

FIGURE 17. Load change with consensus secondary control.

algorithms and system dynamics defined in the Simulink model are now executed on the OPAL-RT target. To capture real-time data for validation, an OPAL board connected to the OPAL-RT target is used to configure a LeCroy oscilloscope. This configuration enables the oscilloscope to capture real-time data from the experimental setup. During the execution of the simulation, the oscilloscope captures real-time data, which can be used for reference and validation. This data allows for comparing the simulated results with the actual behavior of the system.

In Figure 17, the functionality of secondary consensus control for two DG units under load variation is depicted. When one unit experiences a load reduction, the secondary consensus controller ensures that the load in the other unit is proportionately reduced based on their respective capacity. Similarly, if there is an increase in load demand in one unit, the controller increases the load current in the other unit to achieve cooperative control of the entire system. This approach enables the DG units to work together and maintain system stability and balance. Moving on to Figure 18, it illustrates a normal scenario followed by a replay attack in the communication channel. The system becomes immediately unstable after the attack is initiated. The current flowing through the line becomes excessively high, posing a risk of damaging electrical equipment beyond its rated capacity. Figure 19 demonstrates the residual output under the attack scenario, obtained using a Kalman filter. The local measurements are compared with the predicted values based on the system configuration. The residual value is then utilized to initiate a mitigation plan to restore system stability before it worsens.

In Figure 20, a load change scenario is shown after recovering from the attack. The load changes are depicted

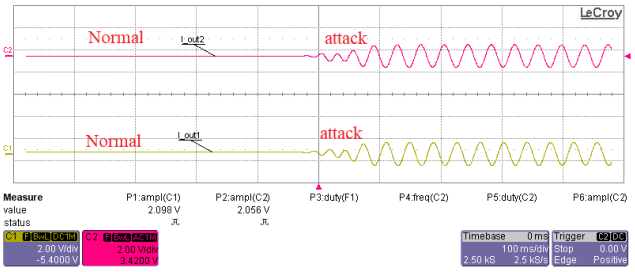

FIGURE 18. Normal scenario followed by attack.

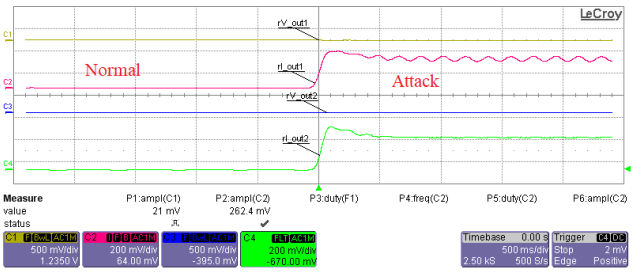

FIGURE 19. Residual increment after attack.

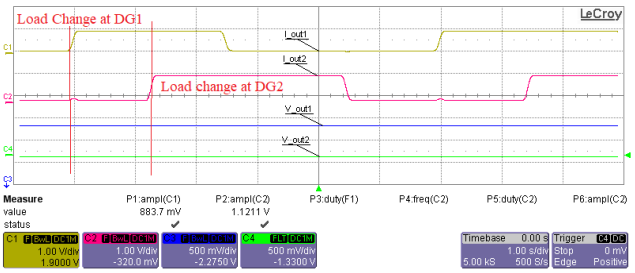

FIGURE 20. Load change at attack recovery scenario.

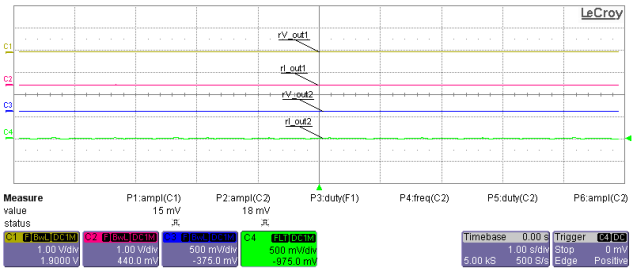

FIGURE 21. Residual at attack recovery scenario.

separately in both DGs, and the system operates well without one unit's load change significantly impacting the other unit. Figure 21 displays the residual scenario after recovering the system from the attack. The absence of residue indicates that the system is under control and the effects of the attack have been mitigated. Overall, the figures depict various aspects of the system's behavior and response in different scenarios, highlighting the importance of secondary consensus control, the impact of attacks, the effectiveness of

mitigation measures, and the system's ability to recover and maintain stability.

V. CONCLUSION

In conclusion, our findings confirm that a reduction in load on a particular bus connected to one DG unit leads to a proportional decrease in generation from other DG units, thus validating the effectiveness of consensus control. Furthermore, this paper shows that a Replay attack, when introduced into the communication link, remains dormant until alterations occur in the system information, typically triggered by load changes. Once activated, this attack disrupts the system's ability to maintain a stable voltage setpoint for reliable operation. Moreover, the line current exhibited a surge of over a hundredfold when compared to its typical value. We identify the attack by observing a rise in residue, and we consider it resolved when the residue returns to zero. Additionally, we propose that future research should extend its horizons by considering diverse attack scenarios and communication network structures, including AC microgrids with multiple generation units that incorporate delays and quality-of-service requirements.

REFERENCES

[1] A. Khalid, A. Stevenson, and A. I. Sarwat, "Overview of technical specifications for grid-connected microgrid battery energy storage systems," *IEEE Access*, vol. 9, pp. 163554–163593, 2021.

[2] A. Debnath, S. Roy, T. O. Olowu, I. Parvez, and A. Sarwat, "A unified controller for hybrid PV-battery system with DC microgrid voltage regulation in grid-connected and islanding-mode," in *Proc. IEEE Ind. Appl. Soc. Annu. Meeting (IAS)*, Oct. 2022, pp. 1–6.

[3] A. Debnath, S. Roy, A. Stevenson, T. O. Olowu, and A. Sarwat, "ANN-based dynamic frequency regulation of PV-based hybrid microgrid system," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Jan. 2023, pp. 1–5.

[4] A. Q. Al-Shetwi, "Sustainable development of renewable energy integrated power sector: Trends, environmental impacts, and recent challenges," *Sci. Total Environ.*, vol. 822, May 2022, Art. no. 153645.

[5] A. Sundararajan and A. I. Sarwat, "Hybrid data-model method to improve generation estimation and performance assessment of grid-tied PV: A case study," *IET Renew. Power Gener.*, vol. 13, no. 13, pp. 2480–2490, Oct. 2019.

[6] D. P. Simatupang and J. Choi, "Integrated photovoltaic inverters based on unified power quality conditioner with voltage compensation for submarine distribution system," *Energies*, vol. 11, no. 11, p. 2927, Oct. 2018.

[7] P. Montegiglio, G. Acciani, M. Dicorato, G. Forte, and F. Marasciuolo, "A decentralized power and bus voltage regulation approach for DC microgrids," *IEEE Trans. Ind. Appl.*, vol. 59, no. 4, pp. 4773–4785, Jul./Aug. 2023.

[8] E. Espina, R. Cárdenas-Dobson, J. W. Simpson-Porco, M. Kazerani, and D. Sáez, "A consensus-based distributed secondary control optimization strategy for hybrid microgrids," *IEEE Trans. Smart Grid*, early access, Mar. 29, 2023, doi: 10.1109/TSG.2023.3263107.

[9] Y. Han, K. Zhang, H. Li, E. A. A. Coelho, and J. M. Guerrero, "MAS-based distributed coordinated control and optimization in microgrid and microgrid clusters: A comprehensive overview," *IEEE Trans. Power Electron.*, vol. 33, no. 8, pp. 6488–6508, Aug. 2018.

[10] M. Tucci, L. Meng, J. M. Guerrero, and G. Ferrari-Trecate, "Stable current sharing and voltage balancing in DC microgrids: A consensus-based secondary control layer," *Automatica*, vol. 95, pp. 1–13, Sep. 2018.

[11] Y.-W. Wang, Y. Lei, T. Bian, and Z.-H. Guan, "Distributed control of nonlinear multiagent systems with unknown and nonidentical control directions via event-triggered communication," *IEEE Trans. Cybern.*, vol. 50, no. 5, pp. 1820–1832, May 2020.

[12] X. Lu and J. Lai, "Communication constraints for distributed secondary control of heterogeneous microgrids: A survey," *IEEE Trans. Ind. Appl.*, vol. 57, no. 6, pp. 5636–5648, Nov. 2021.

[13] H. Iqbal, M. Tariq, M. Sarfraz, A. I. Sarwat, W. Alhosaini, O. Aldosari, and A. Aziz, "Selective harmonic mitigation based two-scale frequency control of cascaded modified packed U-cell inverters," *Energy Rep.*, vol. 8, pp. 1009–1020, Nov. 2022.

[14] K. Hargroves, B. James, J. Lane, and P. Newman, "The role of distributed energy resources and associated business models in the decentralised energy transition: A review," *Energies*, vol. 16, no. 10, p. 4231, May 2023.

[15] M. Pasetti, S. Rinaldi, and D. Manerba, "A virtual power plant architecture for the demand-side management of smart prosumers," *Appl. Sci.*, vol. 8, no. 3, p. 432, Mar. 2018.

[16] S. Algarni, V. Tirth, T. Alqahtani, S. Alshehery, and P. Kshirsagar, "Contribution of renewable energy sources to the environmental impacts and economic benefits for sustainable development," *Sustain. Energy Technol. Assessments*, vol. 56, Mar. 2023, Art. no. 103098.

[17] Y. Wang, A. O. Rousis, and G. Strbac, "Resilience-driven optimal sizing and pre-positioning of mobile energy storage systems in decentralized networked microgrids," *Appl. Energy*, vol. 305, Jan. 2022, Art. no. 117921.

[18] A. M. Jasim, B. H. Jasim, V. Bureš, and P. Mikulecký, "A new decentralized robust secondary control for smart islanded microgrids," *Sensors*, vol. 22, no. 22, p. 8709, Nov. 2022.

[19] Y. Mi, J. Guo, Y. Fu, C. Wang, and P. Wang, "Accurate power allocation of multienergy storage island DC microgrid based on virtual power rating," *IEEE Trans. Power Electron.*, vol. 38, no. 1, pp. 261–270, Jan. 2023.

[20] S. Majumder, A. Vosughi, H. M. Mustafa, T. E. Warner, and A. K. Srivastava, "On the cyber-physical needs of DER-based voltage control/optimization algorithms in active distribution network," *IEEE Access*, vol. 11, pp. 64397–64429, 2023.

[21] S. Garip, M. Bilgen, N. Altin, S. Ozdemir, and İ. Sefa, "Reliability analysis of centralized and decentralized controls of microgrid," in *Proc. 11th Int. Conf. Renew. Energy Res. Appl. (ICRERA)*, Sep. 2022, pp. 557–561.

[22] N. Khosravi, R. Baghbanzadeh, A. Oubelaid, M. Tostado-Véliz, M. Bajaj, Z. Hekss, S. Echalih, Y. Belkhier, M. A. Houran, and K. M. Aboras, "A novel control approach to improve the stability of hybrid AC/DC microgrids," *Appl. Energy*, vol. 344, Aug. 2023, Art. no. 121261.

[23] H. Riggs, M. Khan, A. Amir, F. Barranco, S. Tufail, I. Parvez, and A. I. Sarwat, "Cyber physical systems applications with a case study of intelligent dispatch of PV," in *Proc. SoutheastCon*, Mar. 2021, pp. 1–7.

[24] X.-G. Dong, M.-F. Ge, Z.-W. Liu, and X. Ai, "Distributed CPS-based model predictive compensator for DC microgrids with cyber-layer constraints," *Int. J. Electr. Power Energy Syst.*, vol. 143, Dec. 2022, Art. no. 108463.

[25] L. Sheng, G. Lou, W. Gu, S. Lu, S. Ding, and Z. Ye, "Optimal communication network design of microgrids considering cyber-attacks and time-delays," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3774–3785, Sep. 2022.

[26] T. O. Olowu, S. Dharmasena, A. Hernandez, and A. Sarwat, "Impact analysis of cyber attacks on smart grid: A review and case study," in *New Research Directions in Solar Energy Technologies*. New York, NY, USA: Springer, 2021, pp. 31–51.

[27] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad, K. K. Yen, and A. I. Sarwat, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Trans. Ind. Electron.*, vol. 67, no. 9, pp. 7951–7962, Sep. 2020.

[28] J. Zhou, Q. Yang, X. Chen, Y. Chen, and J. Wen, "Resilient distributed control against destabilization attacks in DC microgrids," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 371–384, Jan. 2023.

[29] P. S. Tadepalli and D. Pullaguram, "Distributed control microgrids: Cyber-attack models, impacts and remedial strategies," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 8, pp. 1008–1023, 2022.

[30] A. A. Khan and O. A. Beg, "Cyber vulnerabilities of modern power systems," in *Power Systems Cybersecurity: Methods, Concepts, and Best Practices*. New York, NY, USA: Springer, 2023, pp. 47–66.

[31] N. Sheykhi, A. Salami, J. M. Guerrero, G. D. Agundis-Tinajero, and T. Faghihi, "A comprehensive review on telecommunication challenges of microgrids secondary control," *Int. J. Electr. Power Energy Syst.*, vol. 140, Sep. 2022, Art. no. 108081.

[32] J. Lai, X. Lu, Z. Dong, and S. Cheng, "Resilient distributed multiagent control for AC microgrid networks subject to disturbances," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 1, pp. 43–53, Jan. 2022.

[33] A. Vosughi, A. Tamimi, A. B. King, S. Majumder, and A. K. Srivastava, "Cyber–physical vulnerability and resiliency analysis for DER integration: A review, challenges and research needs," *Renew. Sustain. Energy Rev.*, vol. 168, Oct. 2022, Art. no. 112794.
[34] A. Naha, A. Teixeira, A. Ahlén, and S. Dey, "Sequential detection of replay attacks," *IEEE Trans. Autom. Control*, vol. 68, no. 3, pp. 1941–1948, Mar. 2023.
[35] M. Liu, C. Zhao, J. Xia, R. Deng, P. Cheng, and J. Chen, "PDDL: Proactive distributed detection and localization against stealthy deception attacks in DC microgrids," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 714–731, Jan. 2023.
[36] A. J. Gallo, M. S. Turan, F. Boem, G. Ferrari-Trecate, and T. Parisini, "Distributed watermarking for secure control of microgrids under replay attacks," *IFAC-PapersOnLine*, vol. 51, no. 23, pp. 182–187, 2018.
[37] P. S. Sarker, S. Majumder, M. F. Rafy, and A. K. Srivastava, "Impact analysis of cyber-events on distributed voltage control with active power curtailment," in *Proc. IEEE Int. Conf. Power Electron., Drives Energy Syst. (PEDES)*, Dec. 2022, pp. 1–6.
[38] M. Liu, C. Zhao, Z. Zhang, R. Deng, P. Cheng, and J. Chen, "Converter-based moving target defense against deception attacks in DC microgrids," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3984–3996, Sep. 2022.
[39] A. Aflaki, M. Gitizadeh, R. Razavi-Far, V. Palade, and A. A. Ghasemi, "A hybrid framework for detecting and eliminating cyber-attacks in power grids," *Energies*, vol. 14, no. 18, p. 5823, Sep. 2021.
[40] K. Zhang, C. Keliris, T. Parisini, and M. M. Polycarpou, "Identification of sensor replay attacks and physical faults for cyber-physical systems," *IEEE Control Syst. Lett.*, vol. 6, pp. 1178–1183, 2022.
[41] D. Li, N. Gebraeel, and K. Paynabar, "Detection and differentiation of replay attack and equipment faults in SCADA systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 18, no. 4, pp. 1626–1639, Oct. 2021.
[42] B. Canaan, B. Colicchio, and D. O. Abdeslam, "Experimental HIl implementation of RNN for detecting cyber physical attacks in AC microgrids," in *Proc. Int. Symp. Power Electron., Electr. Drives, Autom. Motion (SPEEDAM)*, Jun. 2022, pp. 958–963.
[43] U. Prasad, A. Jagan, S. R. Mohanty, and S. P. Singh, "Remedial control scheme of PV systems against cyber-attack in AC microgrid," in *Proc. IEEE Int. Conf. Power Electron., Drives Energy Syst. (PEDES)*, Dec. 2022, pp. 1–6.
[44] N. Vafamand, M. M. Arefi, M. H. Asemani, M. Javadi, F. Wang, and J. P. S. Catalão, "Dual extended Kalman filter reconstruction of actuator and sensor faults in DC microgrids with constant power loads," in *Proc. IEEE Ind. Appl. Soc. Annu. Meeting (IAS)*, Oct. 2021, pp. 1–6.

MD. ABU TAHER (Graduate Student Member, IEEE) received the bachelor's degree in electrical and electronics engineering from the Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Florida International University, Miami, FL, USA. He is a highly experienced professional in the field of power system engineering, with over ten years of industry expertise. He is also a Research Assistant with the Energy, Power, Sustainability, and intelligence (EPSi) Laboratory. His research focuses on microgrid voltage and frequency regulation, accurate real and reactive power sharing among multiple renewable energy sources (RES), and microgrid cybersecurity with various mitigation methods. With his expertise in microgrid systems, he specializes in developing advanced control strategies to regulate voltage and frequency within microgrids. He also focuses on achieving accurate power sharing among different RES to enhance system stability and efficiency. Furthermore, he actively researches and implements cybersecurity measures to ensure the robustness and resilience of microgrid networks against potential threats.

MOHD TARIQ (Senior Member, IEEE) received the bachelor's degree in electrical engineering from AMU, Aligarh, the master's degree in machine drives and power electronics from IIT Kharagpur, and the Ph.D. degree in electrical engineering from Nanyang Technological University (NTU), Singapore.

He is currently a Faculty Member/Postdoctoral Associate with Florida International University, working on high penetration renewable systems, grid resiliency, large-scale data analysis, artificial intelligence, electric vehicles, and cybersecurity. He is also an Assistant Professor (on-leave) with AMU, where he directed various international and national sponsored research projects worth approximately 18 million INR and led a team of multiple researchers in the domain of power converters, energy storage devices and their optimal control for electrified transportation, and renewable energy application. He has authored more than 225 research papers in international journals/conferences, including many articles in IEEE TRANSACTIONS/journals. He is also an inventor of more than 25 patents granted/published by the patent offices of USA, Australia, U.K., Europe, India, and China. He is an Associate Editor of IEEE ACCESS, an Editorial Board Member of *Scientific Reports* and *Nature*, and a guest editor of various other journals.

MILAD BEHNAMFAR (Graduate Student Member, IEEE) received the B.S. degree in electrical engineering from the University of Kurdistan, in 2016, and the M.S. degree in power electronics and electric machines from Shahid Beheshti University, in 2018. He is currently pursuing the Ph.D. degree with Florida International University. He is also a Research Assistant with the Energy, Power, Sustainability, and intelligence (EPSi) Laboratory. His main research interests include wireless power transfer for the application of electric vehicle charging and high-frequency converters. He is a Regular Reviewer of IEEE ACCESS and other IEEE conferences.

ARIF I. SARWAT (Senior Member, IEEE) is currently an Eminent Scholar Chaired Professor with the Department of Electrical and Computer Engineering, and the Director of the FPL-FIU Solar Research Facility, Florida International University, Miami, FL, USA. He is also the Principal Investigator of the State-of-the-Art Grid-Connected 3MW/9 MWH AI-Based Renewable Microgrid Project funded by FPL. He has authored or coauthored more than 200 peer-reviewed articles and multiple patents. His research interests include smart grids, electric vehicles, high penetration renewable systems, storage, and battery management systems, grid resiliency, large-scale data analysis, artificial intelligence, advanced metering infrastructure, smart city infrastructure, and cybersecurity. He has multiple funded projects, funded by the National Science Foundation, industry, and the Department of Energy. He is the author or coauthor of a publication that won the Best Paper Award at the Resilience Week, in 2017, and a technical article that won both the Best Paper Award, in 2016, and the Most Cited Paper Award, in 2018, from Springer's *Journal of Modern Power Systems and Clean Energy*. He was a recipient of the Faculty Award for Excellence in Research, Creative Activities, in 2016; the College of Engineering and Computing Worlds Ahead Performance, in 2016; and the FIU TOP Scholar Award, in 2015 and 2019. Since 2012, he has been the Chair of the IEEE Miami Section VT and Communication. He is an Associate Editor of the *ACM Computing Surveys*.