An Analytical Parameter-Free Cyberattack Detection Method for Grid-Connected Converters

Alireza Jabbarnejad, Sadegh Vaez-Zadeh, and Mohammad Sadegh Eslahi

***Abstract*—The control unit, a critical component of power electronic converter-based systems, interfaces with monitoring and measurement units via data communication links, a configuration that increases the risk of system penetration. Such vulnerabilities could compromise the security of the communication links between control units and physical components, like sensors, by allowing data manipulation. This article introduces an analytical-based approach to detect such cyberattacks, designing data integrity attack scenarios that emulate the actual grid events. It conducts a mathematical analysis of the control system behavior during actual events and cyberattacks, extracting essential features for attack detection. An extended state observer is developed to estimate active and reactive power, mitigating noise effects, and eliminating parameter dependency in feature calculation. Unlike model-based methods, the proposed approach is devoid of convergence issues and parameter dependence. It also surpasses data-driven methods by eliminating the need for preprocessing and model training. The effectiveness of this novel method in detecting cyberattacks is demonstrated through simulation and experimental studies.**

***Index Terms*—Cyberattack, data driven, direct power control, grid-connection, microgrids, power converters, renewable energy.**

I. Introduction

MODERN power systems are affected by developing grid-connected converter-based distributed energy resources such as wind turbines and photovoltaic (PV) plants [1], [2]. Solid-state three-phase grid-connected converters (GCC) are the controllable interface for exchanging the active and reactive power between the grid and the renewable sources [2], [3]. In such systems, applying information communication technologies in the GCC systems provides considerable opportunities for control and optimization [4], [5]. Nevertheless, the risk of malicious intrusions increases under the conditions [4], [5]. Such threats including cyberattacks, may cause system shutdown, cascaded failure, damage to consumer loads, and endangered energy market operation [4], [5], [6].

Manuscript received 20 November 2023; revised 17 March 2024 and 31 May 2024; accepted 1 July 2024. Date of publication 22 July 2024; date of current version 7 October 2024. This work was supported by the Iran National Science Foundation under Project 940013. Recommended for publication by Associate Editor Q. Shafiee. *(Corresponding author: Sadegh Vaez-Zadeh.)*

Alireza Jabbarnejad and Mohammad Sadegh Eslahi are with the School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Tehran 14395-515, Iran (e-mail: jabbarnejad.a@ut.ac.ir; mseslahi@ut.ac.ir).

Sadegh Vaez-Zadeh is with the Advanced Motion Systems Research Laboratory, School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Tehran 14395-515, Iran (e-mail: vaezs@ut.ac.ir).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TPEL.2024.3430542.

Digital Object Identifier 10.1109/TPEL.2024.3430542

False data-injection attacks (FDIAs) can be perpetrated by various mechanisms, including the injection of auxiliary signals, altering the measurements reported by sensors, compromising actuators, and manipulating communication links between controllers [6], [7]. As a result, the attackers can penetrate the control system including calculation, estimation, predictions, and economic dispatch [7]. The security of GCCs is a considerable issue because any anomaly or FDIA may cause an incorrect decision by the system control. It can affect the power exchange through the converters, resulting in a range from economic loss to system instability [6], [7], [8]. Therefore, it is essential to diagnose erroneous data sent to GCC to prevent any adverse effects on the grid [6], [7].

In order to detect FDIAs, many methods are introduced, which can be categorized into model-based and data-driven methods [7]. A distributed watermark is proposed against FDIA on economic droop control for renewable energy-based microgrids [9]. The method avoids any central process to facilitate the diagnosis. However, it needs a dynamic system model to recognize the watermarked signal properly. Weighted less square-based detection is introduced to identify FDIA [10]. The method enjoys low complexity and computation burden. Nevertheless, the estimation is not accurate under the method. A detection approach including a Luenberger observer and extended Kalman filter is proposed for FDIA [11]. It enjoys good estimation accuracy and is suitable for nonlinear systems. However, the method does not guarantee convergence and has the gain tuning challenge. An unknown input observer-based FDIA detection method is proposed [12]. The method is accurate and has a good detection rate. However, it has some disadvantageous such as high time complexity. The model-based methods need the system parameters information, which can be affected by ambient and operation conditions.

Besides the model-based method, data-driven methods are proposed. The machine learning-based detection methods are considered as the subset of data-driven methods [4]. They can be categorized into supervised learning, e.g., naive bayes classifier [13], unsupervised learning, e.g., K-means clustering [14], and semisupervised learning, e.g., physics-informed spline learning [15]. They do not need any mathematical model of a physical system and completely depend on historical data of the system under test. However, the first one needs a data set with a label and training process. In addition, the second one only performs classification tasks and utilizes unlabeled data, which causes more sensitivity to outliers, noise, or missing values. Moreover, the third one uses both labeled and unlabeled data. Although they need a training process, can alleviate the sensitivity problems.

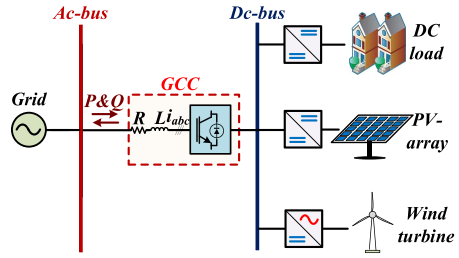

Fig. 1. Typical power converter-based grid.

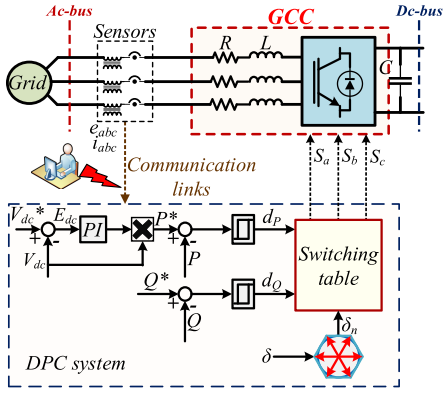

Fig. 2. System and cyberattack model.

A detection method based on two different kinds of popular supervised data-driven methods, e.g., support vector machine, and long short-term memory is proposed for PV farms [16]. It can detect the FDIA of the grid voltage sensors. However, it needs labeled data, preprocessing, data patterning, and model training for attack detection. A diagnosis method using the game theory as a subset of data-driven methods is proposed for GCCs [17]. This method detects some of the most common types of attacks on GCCs. However, it requires data and high computation for training. In addition, a resilient method is introduced for the GCCs under cyberattacks and grid voltage faults [18]. The method guarantees the stability of the vector control of GCCs under symmetrical fault conditions and the grid voltage FDIA. Nevertheless, it cannot distinguish FDIA from voltage faults.

This article proposes an analytical-based, parameter-free approach for detecting cyberattacks GCCs. It investigates the GCC vulnerability to FDIA and develops three main attack scenarios and two instances of more sophisticated ones to encompass a variety of FDIA types. Through mathematical analysis, the behavior of direct power control (DPC) [19] is examined under the conditions of both cyberattacks and actual grid events, such as load fluctuations and voltage sags/swells. This analysis determines distinctive features that clearly distinguish between the DPC response to actual grid events and its behavior under cyberattacks. Based on these insights, the article proposes a novel detection methodology, leveraging the unique characteristics identified for cyberattack detection in GCCs. The main contributions of this article are as follows.

1) It mathematically justifies the differences between the DPC performance under actual events and cyberattacks to extract the required features for cyberattack detection.
2) It designs a model-free extended state observer (ESO) to suppress the noise effect in the calculation of the feature.
3) It proposes a parameter-free detection method without any convergence problem to overcome the drawbacks of model-based methods.
4) The proposed analytical-based detection method avoids any preprocessing and model training to overcome the problems of data-driven methods.

II. Cyberattack in Grid Connected Converter System

A. System Model and False Data Injection Vulnerability

Fig. 1 presents a typical power converter-based grid. Sustainable energy resources, such as solar PV and wind turbine plants in addition to dc-loads, are connected to a dc-bus. The GCC should control the exchanged active and reactive power between the buses according to grid code requirements [2]. This article focuses on GCC-based modern power systems. These GCCs encompass digital communication systems, for remote monitoring and control [5], [7]. In the systems, sensors play a vital role by measuring various parameters especially voltage and current [5], [7]. The transmission of digitally encoded sensor data is crucial for real-time grid management and control [5], [7], [21]. Regardless of the specific transmission method used, this data traverses various networks and devices, such as routers, and is vulnerable to unauthorized access and manipulation by attackers [5], [7]. Malicious actors could exploit these network junctures to intercept and alter the data, causing a potential risk to the operations and safety of GCCs [15], [16], [17], [18]. For instance, in Man-in-the-Middle attacks, attackers could intercept and modify the sensor data, such as reducing voltage readings to simulate voltage sag conditions [21]. Similarly, by network compromise, attackers might access the network to manipulate data in transit, threatening system integrity [22]. These vulnerabilities in data transmission expose power systems, particularly GCCs, to the threat of FDIA, thus jeopardizing GCC operation and security [15], [16], [17], [18].

B. Control System and Its Vulnerable Points

The GCC and its control system are shown in Fig. 2, where the GCC mathematical model can be obtained as [19], [20]

$$\bar{e} = R\bar{i} + Ld\bar{i}/dt + \bar{v} \tag{1}$$

where $\tilde{P}\bar{e}$, $\bar{v}$, and $\bar{i}$ are the grid voltage vector, the output GCC voltage vector, and the grid current vector, respectively. In addition, R and L are the equivalent input resistance and inductance. The DPC method is applied to the converter [19]. The dc-link voltage $V_{\rm dc}$ can be calculated as [19]

$$V_{\rm dc} = P/I_{\rm dc} \tag{2}$$

where P and $I_{\rm dc}$ are the grid active power and the dc-link current. In this method, the PI controller of $V_{\rm dc}$ generates the active power reference, P^*, based on (3) as follows [19]:

$$(V_{\rm dc}^* - V_{\rm dc})(K_p + K_i/s)V_{\rm dc} = P^* \tag{3}$$

where the superscript "$*$" is used to denote the reference signal. Moreover, K_p and K_i are the PI controller gains. The active and reactive power is calculated in the stationary reference frame ($\alpha\beta$) as [19], [20]

$$P = 1.5(e_\alpha i_\alpha + e_\beta i_\beta) \tag{4}$$

$$Q = 1.5(e_\beta i_\alpha - e_\alpha i_\beta). \tag{5}$$

These signals are compared to their references, and the resulting errors enter the hysteresis controllers. Then, a proper voltage vector is selected based on the hysteresis flags (d_P and d_Q) and the grid voltage sector position (δ_n). Finally, it is applied to the converter by determining the switching states (S_a, S_b, and S_c). In addition, the Fourier series of the phase current is illustrated as

$$i(t) = I_1 \sin(\omega t + \phi_1) + \sum_{j=2}^{\infty} I_j \sin(j\omega t + \phi_j) \tag{6}$$

where I_1 is the amplitude of the fundamental frequency component, I_j are the amplitudes of the jth harmonic frequencies, and ϕ_1, ϕ_n are the phase angles. The grid current total harmonic distortion (THD) is calculated as [1], [27]

$$\begin{aligned} \mathrm{THD}_i &= \sqrt{\sum_{j=2}^{\infty} (I_{j,\mathrm{rms}})^2}/I_{1,\mathrm{rms}} = \sqrt{\sum_{j=2}^{\infty} (I_j)^2}/I_1 \\ &= \sqrt{\frac{\tilde{P}^2 + \tilde{Q}^2}{\bar{P}^2 + \bar{Q}^2}} \end{aligned} \tag{7}$$

where the superscribe "-" and "$\sim$" denote the dc and ac components, respectively.

The load changes and grid voltage fluctuations, such as sags and swells, are common grid events [2], [17], detected by voltage and current sensors, as illustrated in Fig. 2. These sensor signals are crucial for GCC control systems and are transmitted through communication links, which are identified as potential security vulnerabilities [5], [15], [16], [17], [18], [19]. Attackers can manipulate grid voltage and current sensor data through several methods, including spoofing wireless signals [23], compromising network nodes [24], and injecting malicious codes [25]. They can use fake transmitters to spoof wireless signals, leading sensors, or receivers (such as base stations or gateways) to accept altered measurements [23]. By hacking into network infrastructure components like routers and firewalls, they can modify data packets, misleading downstream processing units (control centers) about the grid's actual conditions [24]. Injecting malicious code into computational devices allows for the unauthorized alteration or leakage of sensor measurements [25]. In each scenario, the manipulation of sensor data—often through the application of a constant multiplier to the original—threatens the integrity of grid monitoring and control systems [5], [15], [16].

C. Cyberattack Model and Proposed Scenarios

The measured voltage and current signals from the sensors can be considered as W. Fundamentally, the FDIA model, which alters the measured signals can be expressed as [5], [16], [21]

$$W(t) = \kappa W_0(t - t_d) + \upsilon W_F(t) \tag{8}$$

where $W(t)$ is the compromised signal, W_0 is the original signal, W_F is the signal that can be a function or independent of W_0, υ and κ are considered as coefficients that may be constrained by the physical properties of the system or the sensors, and t_d is the intrinsic communication system delay and/or caused by attackers. This equation can be rewritten as follows, by considering $W_F(t) = \delta W_0(t)$, based on the principles of data integrity attack as a kind of FDIA [5], [21]

$$W(t) = W_0(t)[\kappa + \upsilon\delta] \tag{9}$$

where the attackers can alter the measurement data of the grid voltage and current sensors ($E(t)$ and $I(t)$) as follows by setting appropriate κ, υ, and δ, to design different attacks:

$$E(t) = \begin{cases} E_0(t)[\kappa_E + \upsilon_E \delta_E] & \text{if } t \geq T_{\text{attack}} \\ E_0(t) & \text{if } t < T_{\text{attack}} \end{cases} \tag{10}$$

$$I(t) = \begin{cases} I_0(t)[\kappa_I + \upsilon_I \delta_I] & \text{if } t \geq T_{\text{attack}} \\ I_0(t) & \text{if } t < T_{\text{attack}} \end{cases} \tag{11}$$

where T_{attack} is the time at which the attack starts. During the preattack phase ($t < T_{\text{attack}}$), sensor readings remain unaltered, while in postattack ($t \geq T_{\text{attack}}$), the data is manipulated according to the attack parameters. A main goal here is to design some attack scenarios to cover FDIAs, including data integrity attacks [5], [21], emulating the grid condition [15], [16], [17], [18], and load-altering attacks [2], [26]. In the second one, attackers could manipulate data to emulate grid conditions like voltage sags/swells. Such attacks can have a broad impact, potentially leading to inappropriate activation of protection devices, destabilizing the grid, or causing physical damage to equipments. The third one consists of cyber manipulation of sensor data that affects the perceived load, which causes a load damage, an incorrect load balancing, or an inappropriate activation of protection systems. To cover these attacks, the following scenarios are considered.

1) *Cyberattak on Voltage Signal (CVS) [18]:* Based on (10), attackers can design these attack scenarios by setting κ_E, υ_E, and δ_E in which the grid voltages increase or decrease to indicate a reduction or increase in grid voltage value.
2) *Cyberattak on Current Signal (CCS) [5]:* Based on (11), attackers can design these attack scenarios by setting κ_I, υ_I, and δ_I in which the grid currents increase or decrease to indicate a reduction or increase in the grid current value.
3) *Cyberattak on Voltage and Current Signal (CVCS) [15], [17]:* A simultaneous alteration of both voltage and current signals based on (10) and (11) can create a more complex and believable scenario for imitating voltage sag/swell conditions. Additionally, CVS under actual voltage sag/swell conditions and CCS during dynamic load [26] changes as the fourth and fifth scenarios are considered for a more comprehensive performance evaluation. The first three scenarios exemplify DIA, whereas the third and fourth scenarios are also indicative of emulating grid conditions. The second and fifth scenarios align with

load-altering attacks due to their impact on perceived load. Subsequent sections will analyze the control system behavior in response to these scenarios.

III. Analysis of DPC Behavior Under Grid Voltage Disturbances and Corresponding Cyberattacks

In all analytical studies discussed in this article, it is assumed that the system operates under normal conditions initially, where variables are presented with no superscript. However, the superscript "′" is used to denote variables that are influenced by abnormal grid conditions, such as actual grid events and cyberattacks. Besides, "k" represents a changing coefficient.

A. Grid Voltage Sag/Swell

The grid voltages drop under symmetrical voltage sag and are presented as

$$e'_{abc} = ke_{abc} \rightarrow e'_{\alpha\beta} = ke_{\alpha\beta} \tag{12}$$

where $0 < k < 1$. The behavior of the DPC under these conditions is investigated in the following steps.

1) Power Control Reaction: The active and reactive powers decrease in response to voltage changes, based on (4) and (5)

$$P' = 1.5((ke_\alpha)i_\alpha + (ke_\beta)i_\beta) = kP \tag{13}$$

$$Q' = 1.5((ke_\beta)i_\alpha - (ke_\alpha)i_\beta) = kQ. \tag{14}$$

According to DPC principles, the internal power control loops compensate for the reduction in power by increasing the grid currents, as their power reference remains unchanged

$$i'_{\alpha\beta} = i_{\alpha\beta}/k \rightarrow i'_{abc} = i_{abc}/k. \tag{15}$$

2) Variations of V_{dc}: $V_{\rm dc}$ declines simultaneously, according to (2), until active power reaches its reference

$$V_{\rm dc}{}' = P'/I_{\rm dc} = kP/I_{\rm dc}. \tag{16}$$

3) ΔP and ΔQ Analysis: The variations of active and reactive power (ΔP and ΔQ) corresponding to the converter voltage vectors are obtained based on (1), (4), and (5) [19], [20], [28]

$$\frac{\Delta P}{\Delta t} = \frac{3e^2}{2L} - \frac{eV_{\rm dc}}{L}\cos\vartheta - \frac{R}{L}P - \omega Q \tag{17}$$

$$\frac{\Delta Q}{\Delta t} = -\frac{eV_{\rm dc}}{L}\sin\vartheta - \frac{R}{L}Q + \omega P \tag{18}$$

$$\vartheta = \omega t - \pi(n-1)/3 \tag{19}$$

where ω and e are the grid angular speed and voltage magnitude. In addition, $\mathrm{n} = \{1, 2, 3, \ldots, 6\}$ is the number of active voltage vectors. The sinusoidal terms in (17) and (18) are zero for null voltage vectors. The $R\bar{i}$ term in (1) is considered negligible [19], [20], [28]. Thus, omitting this term when recalculating (17) leads to eliminating the third term on the right-hand side of this equation. This simplification allows us to logically assert the inequality:

$$3e^2/2L - eV_{\rm dc}\cos\vartheta/L - \omega Q >> -RP/L \tag{20}$$

which is justifiable as, upon the exclusion of the $R\bar{i}$ term, the remaining terms in (17) are dominant. The ΔQ corresponding to null voltage vectors is expressed based on (18) as

$$\left.\frac{\Delta Q}{\Delta t}\right|_{V_{0,7}} = -\frac{R}{L}Q + \omega P. \tag{21}$$

Applying the vectors results in a constant reactive power [19], [27]. Hence, the following can be deduced from (18):

$$-eV_{\rm dc}\sin\vartheta/L >> -RQ/L + \omega P. \tag{22}$$

Consequently, based on (17), (18), (20), and (22), both ΔP and ΔQ are reduced by falling e, and controlling $V_{\rm dc}$, P, and Q

$$\begin{cases} \Delta P' < \Delta P \\ \Delta Q' < \Delta Q \end{cases}. \tag{23}$$

4) Current THD Analysis: The active and reactive power variations can be obtained based on (4) and (5) as

$$\frac{\Delta P}{\Delta t} = \frac{3}{2}\left(i_\alpha\frac{\Delta e_\alpha}{\Delta t} + e_\alpha\frac{\Delta i_\alpha}{\Delta t} + i_\beta\frac{\Delta e_\beta}{\Delta t} + e_\beta\frac{\Delta i_\beta}{\Delta t}\right) \tag{24}$$

$$\frac{\Delta Q}{\Delta t} = \frac{3}{2}\left(i_\alpha\frac{\Delta e_\beta}{\Delta t} + e_\beta\frac{\Delta i_\alpha}{\Delta t} - i_\beta\frac{\Delta e_\alpha}{\Delta t} - e_\alpha\frac{\Delta i_\beta}{\Delta t}\right). \tag{25}$$

By assumption of sinusoidal e_α and e_β as

$$e_\alpha = e\sin(\omega t) \tag{26}$$

$$e_\beta = -e\cos(\omega t) \tag{27}$$

where the variations of e_α and e_β can be expressed as

$$\Delta e_\alpha/\Delta t = e\omega\cos(\omega t) = -\omega e_\beta \tag{28}$$

$$\Delta e_\beta/\Delta t = e\omega\sin(\omega t) = \omega e_\alpha. \tag{29}$$

Substituting (26) and (27) in (22) and (23), yields

$$\frac{\Delta i_\alpha}{\Delta t} = \frac{2e_\alpha}{3e^2}\left(\frac{\Delta P}{\Delta t} + \omega Q\right) + \frac{2e_\beta}{3e^2}\left(\frac{\Delta Q}{\Delta t} - \omega P\right) \tag{30}$$

$$\frac{\Delta i_\beta}{\Delta t} = \frac{2e_\beta}{3e^2}\left(\frac{\Delta P}{\Delta t} + \omega Q\right) - \frac{2e_\alpha}{3e^2}\left(\frac{\Delta Q}{\Delta t} - \omega P\right). \tag{31}$$

By ignoring $R\bar{i}$ term in (1) and recalculating (17) and (18) and substituting the equations in (30) and (31), the variations of i_a and i_6 are provided as

$$\frac{\Delta i_\alpha}{\Delta t} = \frac{e_\alpha}{L} - \frac{V_{\rm dc}}{1.5L}\sin\left(\frac{\pi}{3}(n-1)\right) \tag{32}$$

$$\frac{\Delta i_\beta}{\Delta t} = \frac{e_\beta}{L} + \frac{V_{\rm dc}}{1.5L}\cos\left(\frac{\pi}{3}(n-1)\right). \tag{33}$$

Thus, by falling the grid voltages under voltage sag conditions

$$\begin{cases} \Delta i_\alpha{}' < \Delta i_\alpha \\ \Delta i_\beta{}' < \Delta i_\beta \end{cases}. \tag{34}$$

Fig. 3 illustrates the grid current of phase-a during instances of voltage sag. A comparative analysis reveals that, under voltage sag conditions, the grid current shows fewer variations (fluctuations) than under normal conditions, which results in a waveform that more closely approximates a pure sinusoid, thus leading to a reduction in THD. In addition, the amplitudes of the fundamental harmonic currents are subject to an increase during voltage sags.

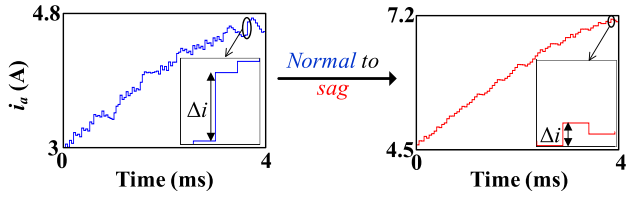

Fig. 3. Current waveform under normal and voltage sag conditions.

Therefore, the grid phase current can be expressed under voltage sag conditions as

$$i'(t) = \eta I_1 \sin(\omega t + \phi'_1) + \sum_{j=2}^{\infty} \rho_j I_j \sin(j\omega t + \phi'_j). \quad (35)$$

The current THD can be calculated based on (7) and (32)

$$\text{THD}_{i'} = \sqrt{\sum_{j=2}^{\infty} (\rho_j I_{j,\text{rms}})^2}/\eta I_{1,\text{rms}}$$

$$= \sqrt{\sum_{j=2}^{\infty} (\rho_j I_j)^2}/\eta I_1 = \sqrt{\frac{\tilde{P}'^2 + \tilde{Q}'^2}{\bar{P}'^2 + \bar{Q}'^2}} \quad (36)$$

where, η and ρ_j are determined to reflect the changes in the amplitude of the fundamental and harmonic frequency components. During voltage sag η exceeds 1 ($\eta > 1$), indicating an increase in the amplitude of the fundamental component. In addition, ρ_j falls between 0 and 1 ($0 < \rho_j < 1$), which corresponds to a decrease in the harmonic content. Consequently, the combined effect of $\eta > 1$ and $0 < \rho_j < 1$ leads to a reduction in the overall THD. On the other hand, based on (23), the ac components of the active and reactive powers decrease under voltage sag conditions. In other words, $\tilde{P}$ and $\tilde{Q}$ are greater than $\tilde{P}'$ and $\tilde{Q}'$, respectively. However, DPC aims to maintain constant active and reactive power despite the voltage drop. As a result, $\bar{P} = \bar{P}'$ and $\bar{Q} = \bar{Q}'$. Consequently, by comparing (7) with (36), the current THD is reduced during voltage sag conditions

$$\text{THD}_{i'} < \text{THD}_i. \quad (37)$$

The above studies can be repeated for voltage swell conditions by considering $k > 1$. Fig. 4(a) shows the mathematical analysis discussed previously for both grid voltage sag and swell conditions. This analysis is general and does not depend on the rate of change of the coefficient k. The influence of varying is further explored in Figs. 5(a) and 6(a), which present the simulation results of DPC performance during the transition from normal to voltage sag conditions, with both step and ramp voltage changes. The system parameters are listed in [20]. The waveforms, depicted from top to bottom, represent P, Q, V_{dc}, grid current magnitude (i), and grid voltage magnitude (e), respectively. According to Fig. 5(a), the grid voltage drops to 40% at $t = 0.1$ s. In addition, the reference signals are illustrated by a black dashed line. Before $t = 0.1$ s, the system operates under normal conditions where the grid current THD is 2.65%. In addition, the variations of active and reactive power decrease. Moreover, the current THD falls to 1.8%, a reduction from the baseline under normal conditions. According to Fig. 6(a), at $t =$

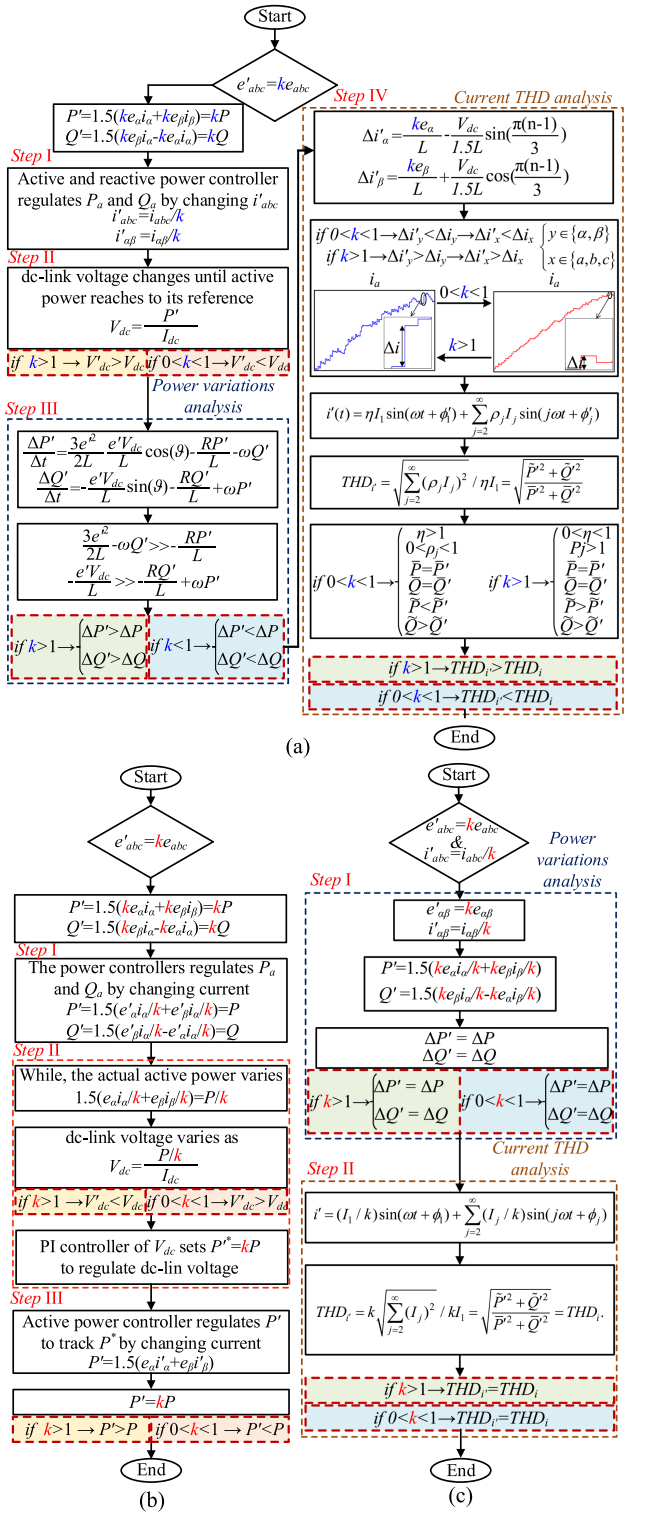

Fig. 4. Mathematical analysis for: (a) voltage sag/swell, (b) CVS, and (c) cyberattak on voltage and current signal (CVCS).

0.2 s, the grid voltages increase at a rate of about 7 V/s, which leads to an increase in active power according to (13). Then, this power declines by its controller through a reduction in the grid currents. The variations in both active and reactive power increase proportionally with the grid voltages, according to (17),

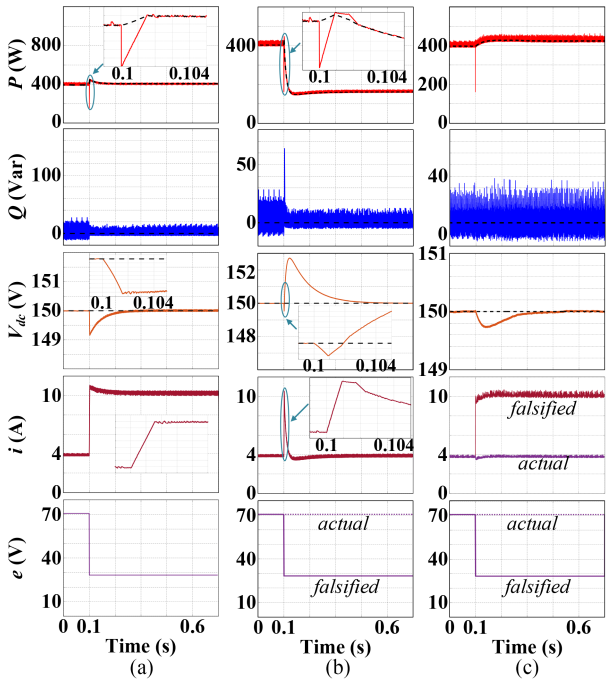

Fig. 5. Simulation results of DPC with step variations under: (a) grid voltage sag, (b) CVS, and (c) CVCS.

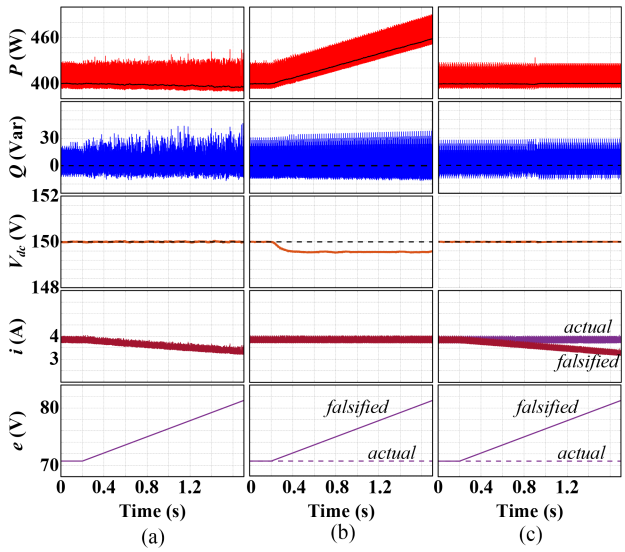

Fig. 6. Simulation results of DPC with ramp variations under: (a) grid voltage sag, (b) CVS, and (c) CVCS.

(18), (20), and (22). Similarly, the variations in grid currents also rise in response to increasing grid voltages, which is justified in (32) and (33). Consequently, it leads to an increase in THD, as formulated in (35) and (36).

B. Cyberattack on Information of Grid Voltage Sensors

Under this attack, the attackers alter the voltage sensor data to make it seem like the grid voltages have decreased or increased, as shown in (12). The following steps analyze how the DPC behaves when the voltages are reduced ($0<k<1$).

1) Power Control Reaction: When the voltages decrease, the active and reactive power also decrease, as shown by (13) and (14). However, their references remain unchanged. Thus, the power controllers compensate for these errors by increasing the grid currents, as given by (15).

2) V_{dc} Control Reaction: The dc-link voltage increases as the actual active power supplying the dc-link (P_{actual}) exceeds the calculated active power, a discrepancy stemming from erroneous data reported by the voltage sensors

$$P_{\text{actual}} = 1.5(e_\alpha(i_\alpha/k) + e_\beta(i_\beta/k)) = P/k \tag{38}$$

$$V_{\text{dc}}{}' = (P/k)/I_{\text{dc}} > V_{\text{dc}}. \tag{39}$$

Therefore, based on (3), the PI controller of the dc-link voltage decreases the active power reference to regulate V_{dc} at the command value as

$$P^{*\prime} = kP^*. \tag{40}$$

3) Active Power Control Reaction: The grid current declines to reduce the active power to track the new reference as

$$i'_{\alpha\beta} = ki_{\alpha\beta} \rightarrow i'_{abc} = ki_{abc} \tag{41}$$

$$P' = 1.5(e_\alpha i_\alpha{}' + e_\beta i_\beta{}') = kP < P. \tag{42}$$

This attack may cause system protection and control to malfunction. Therefore, it should be detected quickly and cleared to avoid system disruption. A similar analysis can be performed when the attackers increase the voltage sensor data. Fig. 4(b) details these mathematical considerations for CVS, which remain invariant to the rate of change in k. For validation, Figs. 5(b) and 6(b) present the system performance under CVS conditions with step and ramp changes. According to Fig. 5(b), at $t = 0.1$ s, attackers alter the voltage sensor readings to simulate a 60% decrease. It leads to a corresponding fall in P and a rise in V_{dc}, justified in the prior analysis. Fig. 6(b) illustrates the simulation results where, after $t = 0.2$ s, the attackers tamper with voltage sensor data, causing an increment at 7 V/s. The actual power decreases compared to normal conditions, resulting in a lowered dc-link voltage, as detailed in (38) and (39), with $k > 1$. Consequently, the voltage controller elevates $P^{*\prime}$ based on (40) to regulate the voltage, while the active power controller adjusts the grid currents to align with the new setpoint. As a result, the active power ascends based on (42).

C. Cyberattack on Data of Grid Voltage and Current Sensors

The attackers attempt to imitate voltage sag/swell conditions in these attacks by changing voltage and current sensor data simultaneously. These attacks are mathematically analyzed by considering the following manipulation:

$$\begin{cases} e'_{abc} = ke_{abc} \rightarrow e'_{\alpha\beta} = ke_{\alpha\beta} \rightarrow \Delta e'_{\alpha\beta} = k\Delta e_{\alpha\beta} \\ i'_{abc} = i_{abc}/k \rightarrow i'_{\alpha\beta} = i_{\alpha\beta}/k \rightarrow \Delta i'_{\alpha\beta} = \Delta i_{\alpha\beta}/k \end{cases} \tag{43}$$

where $0<k<1$ and $k > 1$ are considered for imitating the voltage sag and swell conditions, respectively. The behavior of the DPC under these conditions is investigated in the following steps.

1) ΔP and ΔQ Analysis: Under the conditions, the active and reactive power can be expressed based on (43) as

$$P' = 1.5(ke_\alpha i_\alpha/k + ke_\beta i_\beta/k) = P \tag{44}$$

$$Q' = 1.5(ke_\beta i_\alpha/k - ke_\alpha i_\beta/k) = Q. \tag{45}$$

As a result, the powers vary under CVCS, similar to voltage sag/swell conditions. The power variations can be calculated as

$$\Delta P' = 1.5({i_\alpha}'\Delta {e_\alpha}' + {e_\alpha}'\Delta {i_\alpha}' + {i_\beta}'\Delta {e_\beta}' + {e_\beta}'\Delta {i_\beta}') \tag{46}$$

$$\Delta Q = 1.5({i_\alpha}'\Delta {e_\beta}' + {e_\beta}'\Delta {i_\alpha}' - {i_\beta}'\Delta {e_\alpha}' - {e_\alpha}'\Delta {i_\beta}'). \tag{47}$$

Substituting (43) into (46) and (47), yields

$$\begin{cases} \Delta P' = \Delta P \\ \Delta Q' = \Delta Q \end{cases}. \tag{48}$$

Consequently, in contrast to the voltage sag and swell conditions, the variations of the active and reactive power remain constant under CVCS.

2) Current THD Analysis: The Fourier series of the grid currents are expressed based on (43) under this attack

$$i' = (I_1/k)\sin(\omega t + \phi_1) + \sum_{j=2}^{\infty}(I_j/k)\sin(j\omega t + \phi_j). \tag{49}$$

The THD of the grid currents can be obtained as

$$\begin{aligned} \mathrm{THD}_i &= \sqrt{\sum\nolimits_{j=2}^{\infty}\left(I_{j,\mathrm{rms}}/k\right)^2}/\left(I_{1,\mathrm{rms}}/k\right) \\ &= k\sqrt{\sum\nolimits_{j=2}^{\infty}\left(I_j\right)^2/kI_1} = \sqrt{\frac{\tilde{P}'^2 + \tilde{Q}'^2}{\bar{P}'2 + \bar{Q}'^2}} = \mathrm{THD}_i. \end{aligned} \tag{50}$$

Based on (44)–(48), $\tilde{P}' = \tilde{P}, \tilde{Q}' = \tilde{Q}, \bar{P} = \bar{P}'$, and $\bar{Q} = \bar{Q}'$. Thus, the grid current THD remains constant under CVCS in contrast to voltage sag/swell conditions. The attackers aim to mislead the control and protection system into registering false voltage sag/swell conditions. As a result, these attacks should be diagnosed before the system malfunctions. The above analysis is presented in full detail in Fig. 4(c). This presentation is generalized and independent of the k variations rate. Figs. 5(c) and 6(c) illustrate the DPC simulation results under step and ramp changes to verify the analysis. Based on Fig. 5(c), after $t = 0.1$ s, the grid voltages drop to 40% and the currents increase by 40%. It is seen that in contrast to the voltage sag conditions, the power ripples remain about constant compared to the normal conditions, which is justified in (48). In addition, the grid current THD remains constant based on (49) and (50) with $k = 0.4$. Fig. 6(c) presents the simulation results, where the attackers falsify the information of the grid current and voltage sensors. After $t = 0.2$ s, they increase and decrease the voltage and current sensors data at a rate of about 7 V/s and 0.38 A/s to imitate the voltage swell conditions, as shown in Fig. 6(a). Although the active and reactive power ripples increase under voltage swell conditions, the ripples are about constant under CVCS. In addition, the THD of the grid current remains constant based on (49) and (50) by considering time-variant k.

IV. Analysis of DPC Behavior Under Load Changing and Corresponding Cyberattacks

A. Load Changing

In this section, the load-changing conditions are mathematically investigated. The DPC performance under increasing load conditions is studied in the following steps.

1) V_{dc} Control Reaction: The dc-link voltage decreases by increasing the load current based on (2)

$${V_{\mathrm{dc}}}' = P'/kI_{\mathrm{dc}} < V_{\mathrm{dc}}. \tag{51}$$

Thus, the PI controller of V_{dc} increases the active power reference based on (3), as shown in (40), to regulate the voltage.

2) Active Power Control Reaction: The inner active power control loop tracks the reference by increasing the grid current

$$P' = 1.5(e_\alpha(ki_\alpha) + e_\beta(ki_\beta)) = kP. \tag{52}$$

3) ΔP and ΔQ Analysis: The active and reactive power variations are calculated based on (17). (18), (20), and (22) as

$$\frac{\Delta P'}{\Delta t} \approx \frac{3e^2}{2L} - \frac{eV_{\mathrm{dc}}}{L}\cos\vartheta - \omega Q \approx \frac{\Delta P}{\Delta t} \tag{53}$$

$$\frac{\Delta Q'}{\Delta t} \approx -\frac{eV_{\mathrm{dc}}}{L}\sin\vartheta \approx \frac{\Delta Q}{\Delta t}. \tag{54}$$

Thus, these variations are approximately constant by changing the load. The above studies can be repeated for the decreasing load conditions by considering $0<k<1$. Fig. 7(a) represents this mathematical analysis, which is general and independent of the load-changing rate. Fig. 8(a) and (c) shows the results of the DPC under load step and ramp changes to justify the studies. According to Fig. 8(a), the load current increases by 50% at $t = 0.1$ s. It is seen that ΔP and ΔQ are approximately constant despite the surge in active power. This observation is substantiated by the relationships defined in (53) and (54). According to Fig. 8(c), at $t = 0.2$ s, the load varies, which leads to an increase in V_{dc}, as also presented by (51), with $0<k<1$. In response, the PI controller regulates V_{dc} by diminishing P^*, based on (52). Subsequently, the active power controller follows the command by decreasing the grid currents. Concurrently, the variations in both active and reactive power remain relatively constant, as explicated by (53) and (54).

B. Cyberattack on Information of Grid Current Sensors

The attacker can imitate the load-changing conditions by manipulating the information of the current sensors, which is mathematically investigated in this section. The following steps investigate how the DPC operates when the currents increase by attackers ($k > 1$)

$${i'}_{abc} = ki_{abc} \rightarrow {i'}_{\alpha\beta} = ki_{\alpha\beta} \rightarrow \Delta {i'}_{\alpha\beta} = k\Delta i_{\alpha\beta}. \tag{55}$$

1) Power Control Reaction: When attackers increase grid currents, this results in a proportional rise in both active and reactive power, as derived from (4) and (5) using (55). The controller, aiming to maintain power balance, reduces P and Q by lowering the grid current, as their references remain unchanged

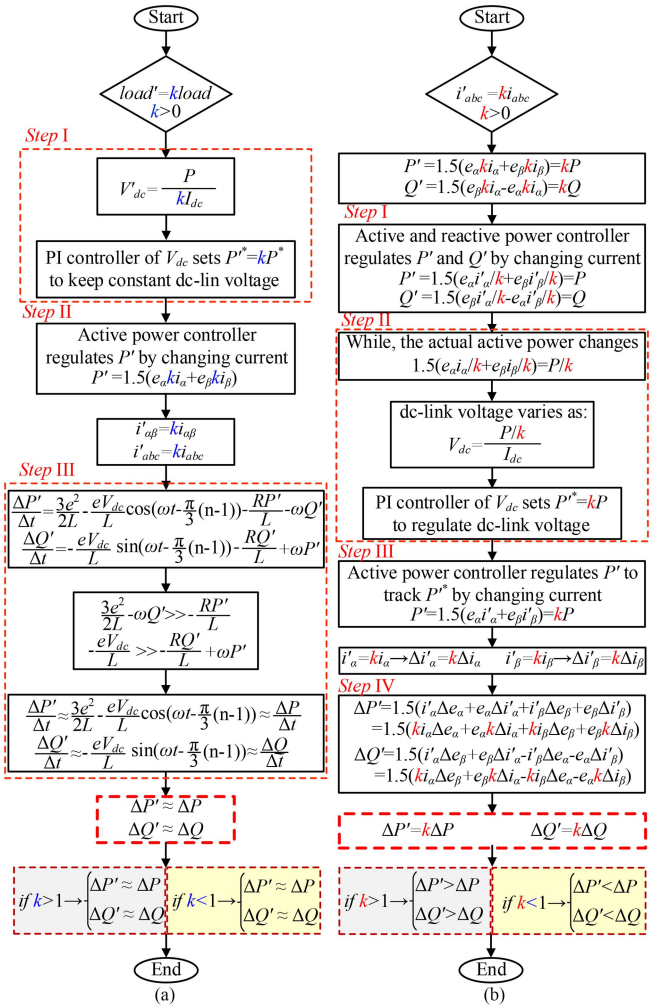

Fig. 7. Mathematical analysis for (a) load changes and (b) CCS.

$(P^{*'}=P$ and $Q^{*'}=Q)$

$$i'_{\alpha\beta}=i_{\alpha\beta}/k\rightarrow\begin{cases}P'=1.5(e_\alpha i_\alpha'+ke_\beta i_\beta')=P\\ Q'=1.5(e_\beta i_\alpha'-ke_\alpha i_\beta')=Q\end{cases}. \quad (56)$$

2) V_{dc} Control Reaction: The dc-link voltage decreases at this time because the actual power decreases, where

$$P_{\text{actual}}=P/k<P\rightarrow V_{\text{dc}}'=(P/k)/I_{\text{dc}}<V_{\text{dc}}. \quad (57)$$

Thus, the PI controller sets $P^{*'}=kP$ based on (3) to regulate V_{dc}.

3) Active Power Control Reaction: The active power control system increases the grid current to achieve a higher active power level and aligns it with its reference.

4) ΔP and ΔQ Analysis: The active and reactive power variations based on (24), (25), (55) are

$$\Delta P'=1.5(ki_\alpha\Delta e_\alpha+e_\alpha k\Delta i_\alpha+ki_\beta\Delta e_\beta+e_\beta k\Delta i_\beta)=k\Delta P \quad (58)$$

$$\Delta Q'=1.5(ki_\alpha\Delta e_\beta+e_\beta k\Delta i_\alpha-ki_\beta\Delta e_\alpha-e_\alpha k\Delta i_\beta)=k\Delta Q. \quad (59)$$

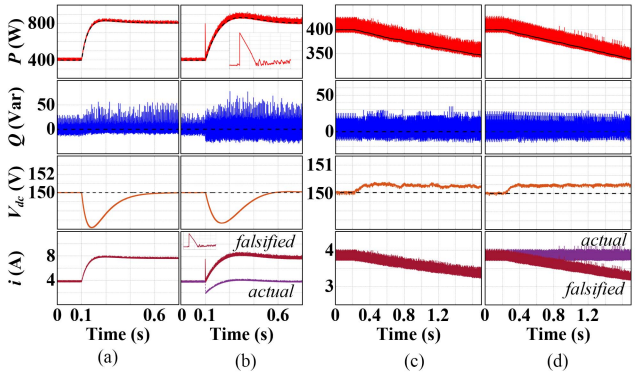

Fig. 8. Simulation results of DPC under: (a) load changes with step variations, (b) CCS with step variations, (c) load changes with ramp variations, and (d) CCS with ramp variations.

Consequently, in contrast to (53) and (54) reveal that $\Delta P'=\Delta P$ and $\Delta Q'=\Delta Q$ under load changes, $\Delta P'<\Delta P$ and $\Delta Q'<\Delta Q$ under CCS. The attacks may cause a false control system operation and damage the loads. Therefore, they should be detected quickly and removed. A similar analysis can be performed when the attackers decrease the current sensor data ($0<k<1$). Fig. 7(b) provides an in-depth presentation of this analysis. The model presented is general, with its validity not compromised by variations in the rate of k.

Fig. 8(b) shows the simulation results under CCS, where the attackers increase the sensor data at $t=0.1$ s by 50%. It is seen that this increase is directly correlated with a 50% rise in both ΔP and ΔQ, attributable to the corresponding amplification of grid current components and their variations. This outcome is consistent with the findings of (58) and (59). The simulation results of DPC under CCS with ramp-changing current are presented in Fig. 8(d). As seen at $t=0.2$ s, the attackers decrease the grid currents at a rate of 0.38 A/s to imitate load changing. It is seen that the active power reference is reduced through the PI controller of V_{dc} to regulate the voltage. Consequently, the power controller adjusts the grid currents to align with this new reference. During this period, both active and reactive power variations diminish due to the decrease in grid current components, a finding corroborated by (58) and (59).

V. Proposed Cybersecurity System

A. Features Extraction

The performance of GCC under DPC for various grid actual events and related cyberattacks is investigated by analytical studies in Sections III and IV. The studies provide a valuable opportunity to extract the required features for detecting cyberattacks. It is mathematically substantiated, as illustrated in Figs. 4 and 7, that the DPC response to genuine grid events diverges from its behavior under cyberattacks. For better clarity and comparison, these differences are accentuated in the figures with matching color coding. For instance, Fig. 7 demonstrates that ΔP and ΔQ signals serve as indicators that can distinguish between actual load changes and CCS. These signals are depicted in

TABLE I
PERFORMANCE OF DPC UNDER CYBERATTACKS AND THE REAL EVENTS

			Nominal Conditions				
			ΔP	ΔQ	THD	P	V_{dc}
Voltage sag		ΔP	<				
		ΔQ		<			
		THD			<		
		P				=	
		V_{dc}					<
CVCS	$e\downarrow$ & $i\uparrow$	ΔP	=				
		ΔQ		=			
		THD			=		
CVS	$e\downarrow$	P				<	
		V_{dc}					>
Voltage swell		ΔP	>				
		ΔQ		>			
		THD			>		
		P				=	
		V_{dc}					>
CVCS	$e\uparrow$ & $i\downarrow$	ΔP	=				
		ΔQ		=			
		THD			=		
CVS	$e\uparrow$	P				>	
		V_{dc}					<
Load $\uparrow$		ΔP	≈				
		ΔQ		≈			
CCS	$i\uparrow$	ΔP	>				
		ΔQ		>			
Load $\downarrow$		ΔP	≈				
		ΔQ		≈			
CCS	$i\downarrow$	ΔP	<				
		ΔQ		<			

gray and yellow, respectively. Under normal conditions of load variation, these signals remain relatively constant. In contrast, they increase/decrease corresponding to increases/decreases in grid currents during a CCS. These features are documented in Table I with consistent color markings. Drawing from the disparities revealed in Fig. 4, the extracted features have been listed for grid voltage sag/swell, CVS, and CVCS in Table I, using the same color scheme for ease of reference. These features are critical in distinguishing DPC behavior amidst actual events versus cyberattacks.

B. Proposed Logic

The improved DPC method, consisting of a cyber security system and a control system, is presented in Fig. 9. The system is proposed based on Table I and executes a proposed logic for detecting cyberattacks, which is shown overall in Fig. 10(a). As seen, the logic calculates the required features under normal conditions. If grid voltage and current variations occur, it calculates the same features under abnormal conditions. Then, it compares features between normal and abnormal conditions to detect cyberattacks. It finally corrects the sensor data after attack identification. This logic executes for every voltage change of more than 10% because these variations are considered voltage sag/swell in standard IEEE 1547 [2]. This logic also executes for every current change of more than 10%, which is considered a threshold. Fig. 10(a) is elaborated in Fig. 10(b) to show the

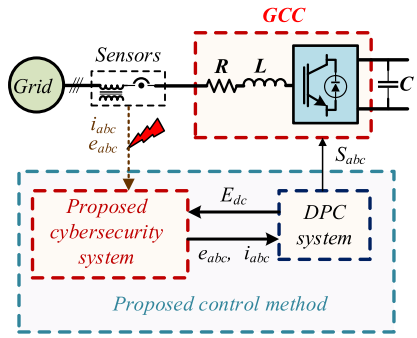

Fig. 9. Proposed control system.

proposed logic in detail. According to Fig. 9, the logic receives the grid voltage and current signals (e_{abc} and i_{abc}), and the dc-link voltage error $E_{\rm dc}$. Then, the proposed logic calculates the required features based on Table I for normal conditions using the received signals as follows. The active and reactive power is obtained based on (3) and (4), which are utilized in the designed ESO presented in the following section to provide the estimated active power samples (P_e) and variations of active and reactive power (ΔP_e and ΔQ_e) to suppress the noise effect and overcome the parameter dependency. The standard deviations of P and Q ($\sigma_{\Delta P}$ and $\sigma_{\Delta Q}$) are obtained based on the power samples for one period (T = 1/f) of the grid voltage [27], [29]. In addition, the current THD (THD_i) is also calculated during this time interval [1], [27], [29]. Next, the average active power is calculated for the 10 last samples of P_e to reduce the noise sampling.

The proposed logic should be capable of detecting grid voltage sag/swell from cyberattacks in a time interval of 1T to 5T in distributed generation systems [30], [31], [32]. To distinguish voltage sag/swell from CVS, it is proposed to execute the following calculations during the first period after the grid voltage variations. The dc-link voltage error (E) summation is calculated during this interval. Also, the average active power (P') is obtained for the 10 last interval samples. If $P' < P$ and $E > 0$, a CVS has occurred. Otherwise, a voltage sag may happen. Also, a CVS has occurred if $P' > P$ and $E < 0$. Else, a voltage swell had maybe happened. Then, the proposed system corrects the voltage signal information when CVS occurs. For doing so, the voltage sensor correction coefficient μ_e is calculated based on (42). Then, the sensor information is corrected using (60), after 5T to ensure that active power reaches its reference

$$\mu_e = e'/e = P'/P. \tag{60}$$

To detect the CVCS, it is proposed here to calculate the current THD ($\text{THD}_{i'}$) and the standard variations of active and reactive power ($\sigma_{\Delta P'}$ and $\sigma_{\Delta Q'}$) from 2T to 5T after grid voltage variations. If $\sigma_{\Delta P'} \geq \sigma_{\Delta P}$ and $\sigma'_{\Delta Q} \geq \sigma_{\Delta Q}$ and $\text{THD}_{i'} = \text{THD}_i$ a CVCS happened. Otherwise, a voltage sag happened. Also, if $\sigma_{\Delta P'} \leq \sigma_{\Delta P}$ and $\sigma_{\Delta Q'} \leq \sigma_{\Delta Q}$ and $\text{THD}_{i'} = \text{THD}_i$ CVCS happened. Else, a voltage swell occurred. Then, the proposed

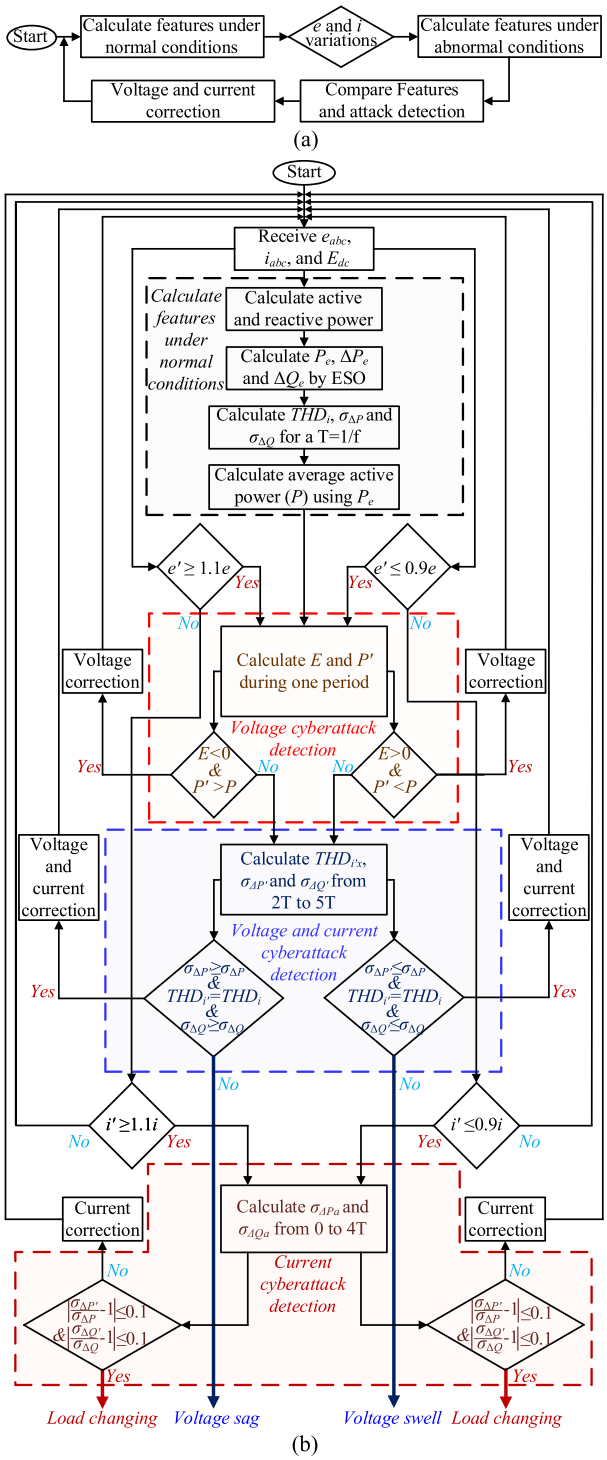

Fig. 10. Proposed logic detection: (a) overall view and (b) in detail.

system corrects the voltage and current signal information by calculation of correction coefficients when CVCS occurs.

To detect load changes from CCS, after current variations, it is proposed to calculate $\sigma_{\Delta P'}$ and $\sigma_{\Delta Q'}$ from 0 to 4T to suppress the noise and reach the system to steady-state conditions. If ($\sigma_{\Delta P'} \geq 1.1\sigma_{\Delta P} \,\|\, \sigma_{\Delta P'} \leq 0.9\sigma_{\Delta P}$) and ($\sigma_{\Delta Q'} \geq 1.1\sigma_{\Delta Q} \,\|\, \sigma_{\Delta Q'} \leq 0.9\sigma_{\Delta Q}$) a current cyberattack occurred, and the proposed system should correct the current sensor data. Otherwise, an increasing load change occurred. The correction coefficient in this case can be obtained based on (58)

$$\mu_i = i'/i = \sigma_{\Delta P'}/\sigma_{\Delta P}. \tag{61}$$

The proposed detection system enjoys the following advantages.

1) Compared to learning-based methods, the proposed method does not require preprocessing and model training due to using features extracted based on analytical studies.
2) It can detect various cyberattacks such as step and ramp variations because the extracted features are independent of the changing rate of voltage and current.
3) The method is parameter-free and does not too much sensitive to sampling noise. It is achieved because the method employs an ESO for real-time feature estimation.
4) It enjoys generalizability since anomaly detection is performed through self-comparison.

The method identifies anomalies by contrasting current system metrics with historical or expected data, pinpointing discrepancies that may indicate cyberattacks. Also, the criteria, which include ΔP, ΔQ, $V_{\rm dc}$, and THD, are chosen judiciously because they remain unaffected by changes in the test system. The aforementioned advantages emphasize the generalizability of the proposed method.

C. Design of Extended State Observer

The proposed method is sensitive to sampling noise effect due to the utilization of ΔP and ΔQ. Thus, an ESO is designed in this section for the estimation of P and Q and their variations to suppress the effect and avoid any parameter dependency. The space state equations for the reactive power can be obtained based on (18)

$$\begin{cases} \dot{Q} = \Delta Q \\ \dot{\Delta Q} = \mathrm{N} \\ y = Q \end{cases} \tag{62}$$

where Q and ΔQ are the selected space state variables. In addition, y is the output of the system. Moreover, N is the time derivative of ΔQ and includes the reactive power dynamic and system disturbances like sampling noise. The equations of the proposed ESO are obtained based on the observer principles

$$\begin{cases} \dot{Q}_e = \Delta Q_e + \lambda_1 (Q - Q_e) \\ \dot{\Delta Q}_e = \lambda_2 (Q - Q_e) \end{cases} \tag{63}$$

where Q and ΔQ are estimated by Q_e and ΔQ_e. Besides, λ_1 and λ_2 are the gains of the designed ESO. Next, (63) can be discretized as

$$\begin{aligned} Q_e[k] &= T_s \lambda_1 Q[k-1] + (1 - T_s \lambda_1) Q_e[k-1] \\ &\quad + T_s \Delta Q_e[k-1] \end{aligned} \tag{64}$$

$$\Delta Q_e[k] = T_s \lambda_2 Q[k-1] - T_s \lambda_2 Q_e[k-1] + \Delta Q_e[k-1] \tag{65}$$

where T_s is the sampling period. In order to select λ_1 and λ_2, the error equations are generated based on (62) and (63) as

$$\begin{cases} \dot{e}_Q = \dot{Q} - \dot{Q}_e = -\lambda_1(Q - Q_e) + \Delta Q - \Delta Q_e \\ \quad = -\lambda_1 e_Q + e_{\Delta Q} \\ \dot{e}_{\Delta Q} = \Delta\dot{Q} - \Delta\dot{Q}_e = -\alpha_2(Q - Q_e) + \mathrm{N} = -\alpha_1 e_Q + \mathrm{N} \end{cases}. \tag{66}$$

If all roots of the characteristic equation of (66), $s^2 + \lambda_1 s + \lambda_2$, are located in the left half-plane, the proposed ESO is bounded-input–bounded-output stable. The equation can be rearranged as $(s + \xi)^2$ by considering that its roots are placed at ξ. To obtain impressive noise suppression as well as a quick reactive power response, ξ is selected as 600 rad/s. Finally, λ_1 and λ_2 are provided based on ξ as

$$\begin{cases} \lambda_1 = 2\xi \\ \lambda_2 = \xi^2 \end{cases}. \tag{67}$$

As a result, Q_e and ΔQ_e accurately follow Q and ΔQ by well-tuning coefficients λ_1 and λ_2. The same procedure can be repeated for designing an ESO for active power.

VI. Performance Evaluation

In this section, simulation studies are performed for the proposed cybersecurity system of the DPC method shown in Fig. 2 under various cyberattack scenarios. The results are presented to confirm the effectiveness of the proposed system. The system parameters are listed in [20]. Fig. 11 presents the simulation results of the proposed cybersecurity system under various CVS including step and ramp changing. At $t = 0.1$ s, the attackers decrease the grid voltage signals by 20% intently, according to Fig 11(a). It is seen that the proposed system detects the attack and corrects the signals. Also, the attackers increase the signals by 20% and decrease them by 40% at $t = 0.5$ s and $t = 0.9$ s, respectively. It is seen that the proposed system diagnoses the attacks successfully after 20 ms and corrects them. Moreover, the attackers increase and decrease the grid voltages with ramp variations at $t = 0.1$ s and $t = 2$, as presented in Fig. 11(b). As seen, the proposed system can detect and remove these invasions.

The simulation results of the proposed system under five different CVCS scenarios including step and ramp changes are shown in Fig. 12. According to Fig. 12(a), the attackers manipulate the grid voltage and current signals at 0.1 s, 0.5 s, and 0.9 s to emulate the voltage sag and swell conditions. The voltage and current signals decrease and increase by about 30% and 50% for the first and third ones. In addition, they increase and decrease by about 20% in the second one. It is seen that the attacks are detected and removed by the proposed system quickly. The results of the system under CVCS with ramp variations are presented in Fig. 12(b), where the attackers manipulate the sensors data at $t = 0.1$ s and $t = 0.7$ s. The proposed system can also diagnose these invasions and remove them.

Fig. 13 presents the simulation results of the proposed cybersecurity system under several CCS scenarios, where the attackers try to imitate the load change conditions. According to Fig. 13(a), the current signals increase intentionally by 30%

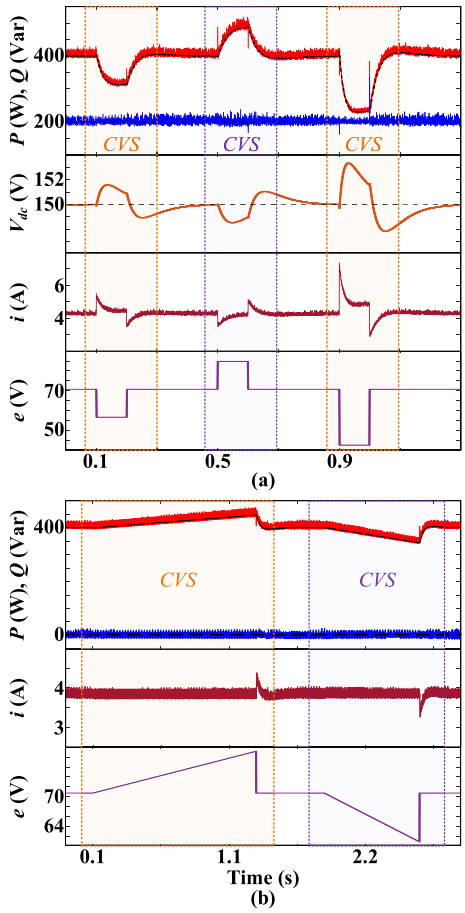

Fig. 11. Simulation results of the proposed detection system under CVS for: (a) step variations and (b) ramp variations.

and 70% at 0.1 s and 0.9 s, respectively. Also, they decrease the signals by 50% at 0.5 s. As seen, the proposed system diagnoses the attacks and corrects the current signals after 80 ms in each case. Moreover, the invaders change the current sensors data to imitate the ramp load change, as shown in Fig. 13(b). They decrease and increase the data at $t = 0.1$ s and $t = 1$ s. However, the proposed system detects these attacks and clears them quickly.

Fig. 14(a) shows the simulation results of the proposed method for CVS under voltage sag conditions. After $t = 0.5$, a 40% voltage sag event leads to a decrease in the active power, based on (13) with $k = 0.4$. To maintain a constant active power, the power controller increases the grid currents based on (15). During this event, attackers artificially escalate the grid voltage levels by 20% to counteract the voltage sag effects. It leads to an increase in active power based on (13), with $k = 1.2$. Consequently, the power controller reduces grid currents based on (15), causing a decline in the dc-link voltage. This decline is explained by (39), which correlates with (38), indicating that the actual active power supporting the dc-link is less than the calculated value due to the false data of the voltage sensors. In response, the PI controller of V_{dc}, according to (3), boosts the active power reference based on (40) to regulate the V_{dc}. Thus, the active

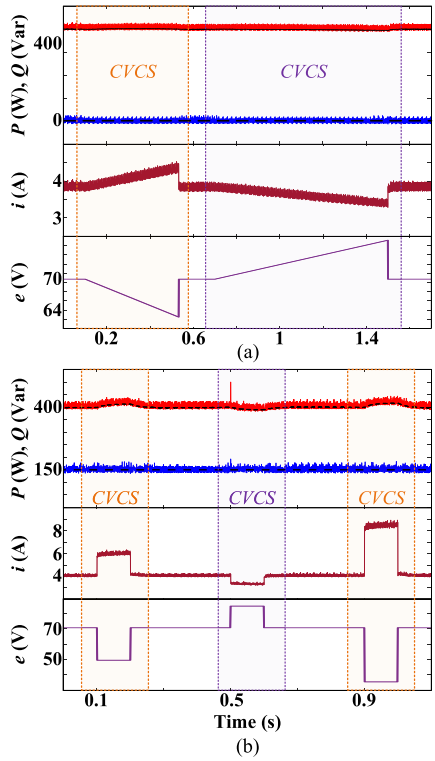

Fig. 12. Simulation results of the proposed detection system under CVCS for: (a) step variations and (b) ramp variations.

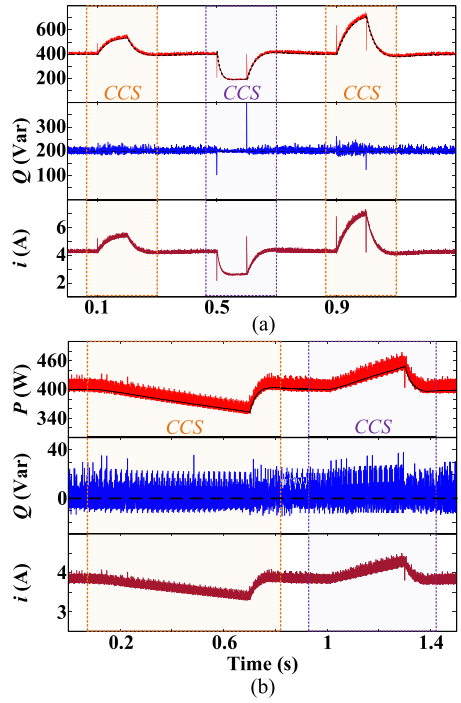

Fig. 13. Simulation results of the proposed detection system under CCS for: (a) step variations and (b) ramp variations.

power controller aligns with the command by increasing the grid currents. As the voltage fluctuates, the proposed detection system evaluates the active power and dc-link voltage against their values under normal operating conditions. The analysis, as illustrated in Fig. 14(a), reveals an increase in active power and a decrease in dc-link voltage under attack conditions compared to normal operation, as presented in Fig. 14(a), enabling the proposed method to identify the cyberattack. Upon the detection, the proposed system corrects the voltage signal information based on (60).

Fig. 14(b) presents the simulation results of the proposed method under CCS during dynamic load changes. After $t = 0.1$ s, the load increases by 100%, which results in a drop in $V_{\rm dc}$ based on (51) with $k = 2$. The PI controller for $V_{\rm dc}$ then adjusts the active power reference to regulate the voltage, based on (3). The internal active power control loop responds by boosting the grid current to follow the new reference. However, in this scenario, attackers intervene by reducing the current sensor data by 50%, aiming to artificially lower the perceived load demand. It leads to a reduction in both active and reactive powers, despite their reference values remaining unchanged. In response, the power controllers increase the powers by increasing the grid currents based on (56), with $k = 0.5$. Thus, the dc-link voltage rises due to the increased actual power, based on (57). As a result, the PI controller of $V_{\rm dc}$ decreases the active power reference, based on (3), to regulate the voltage. The active power controller then reduces the grid currents to align with the lower command, which diminishes the current variations based on (55), with $k = 0.5$. These adjustments lead to decreases in ΔP and ΔQ,

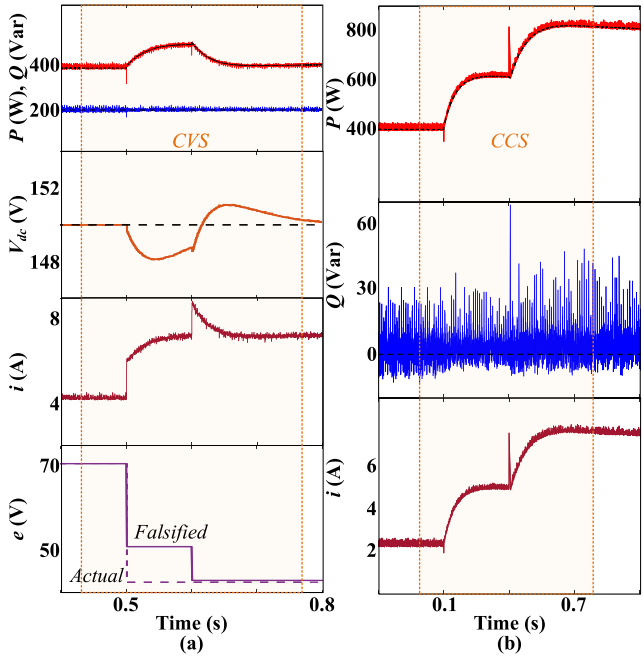

Fig. 14. Simulation results of the proposed detection system under: (a) CVS during voltage sag conditions and (b) CCs during load-changing.

as based on (58) and (59). These changes are also illustrated in Fig. 13(b). After current variations, the proposed system calculates the standard deviations of active and reactive power, comparing them against typical conditions. If the deviations in active and reactive powers exceed 10%, it flags a cyberattack. As a result, this attack is detected. After detection, a current sensor correction coefficient μ_i is derived from (61).

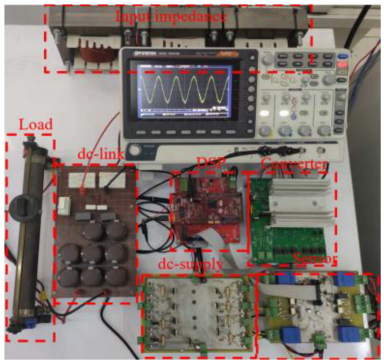

Fig. 15. Experimental setup.

TABLE II
SETUP COMPONENTS DESCRIPTIONS

Component	Description
DSP	TMS320F28377D
Converter	Three-phase two-level inverter based on an intelligent power module
Sensor	LEM current and shunt voltage sensors
Dc-link	3.76 mF capacitance
Dc-supply	Supplying the sensor and DSP boards
Input impedance	15 mH inductance and about a 0.2 Ω resistance
Load	Variable resistance

Experimental tests are carried out to validate the effectiveness of the proposed method. The experimental setup is shown in Fig. 15, where the specification of the setup components is illustrated in Table II. The other GCC parameters are the same as those listed in [20]. In addition, to carry out the cyberattack scenarios, the information of the grid voltage and current sensors are manipulated directly by changing the analog to digital converter (ADC) registers of the control code.

The experimental results of the proposed system under the CVCS, CVS, and CCS scenarios are shown in Fig. 16(a), (b), and (c), respectively. Fig. 16(a) shows the active power, reactive power, current magnitude, and voltage magnitude under the CVCS scenario. As shown in this figure, at first, the system performs under nominal conditions. Suddenly, the attackers manipulate the grid voltage and current signals to emulate the voltage sag conditions, where the grid voltage and current signals are decreased and increased by about 30%. It is seen that the attacks are detected and removed by the proposed system quickly. Fig. 16(b) shows the active power, reactive power, current magnitude, and voltage magnitude under the CVS scenario. Similar to the CVCS scenario, under the CVS scenario, as results shown in Fig. 16(b), the system performs under nominal conditions at first. The attackers manipulate the grid voltage by about 30%. It is seen that the attacks are detected and removed quickly by the proposed system. The active and reactive power of the system before, during, and after the CCS attack scenario is shown in Fig. 16(c).

The experimental results of the proposed detection system under the CVCS, CVS, and CCS scenarios for ramp variations are shown in Fig. 17(a), (b), and (c), respectively. Fig. 17(a)

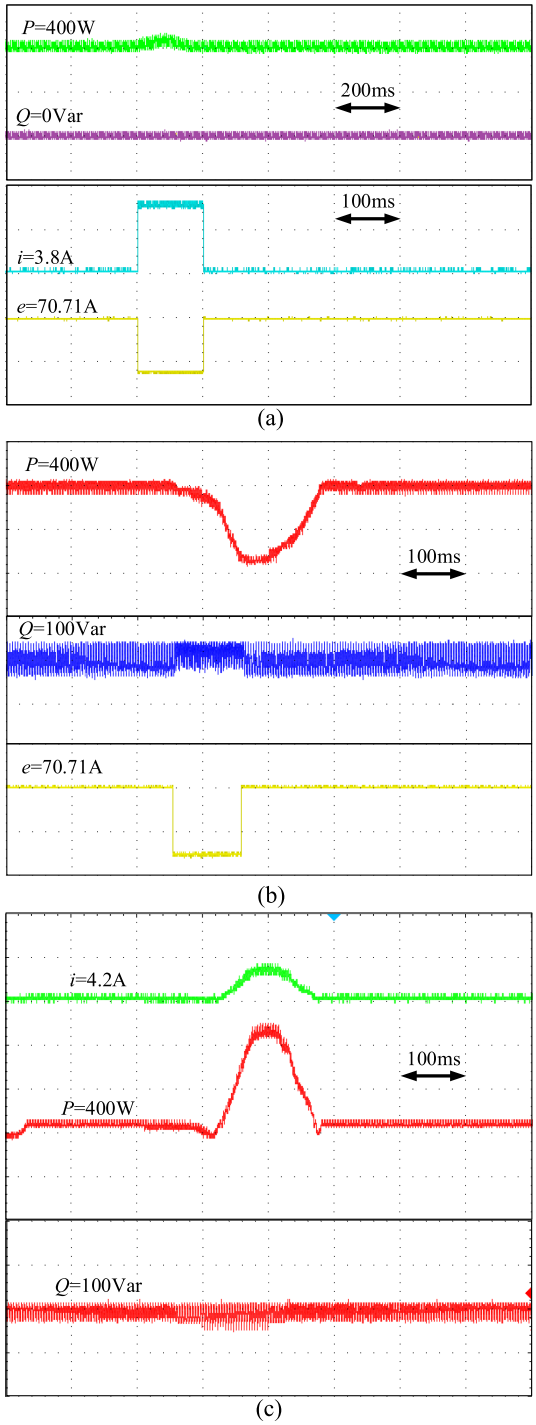

Fig. 16. Experimental results of the cyberattacks with step variations under the proposed method: (a) CVCS, (b) CVS, and (c) CCS.

shows the active power, reactive power, current magnitude, and voltage magnitude under the CVCS scenario. It is seen that the attackers manipulate the grid voltage and current signals to emulate the voltage sag/swell conditions with ramp variations. It is seen that the attacks are detected and removed by the proposed system quickly. Fig. 17(b) shows the active power, reactive power, current magnitude, and voltage magnitude under the

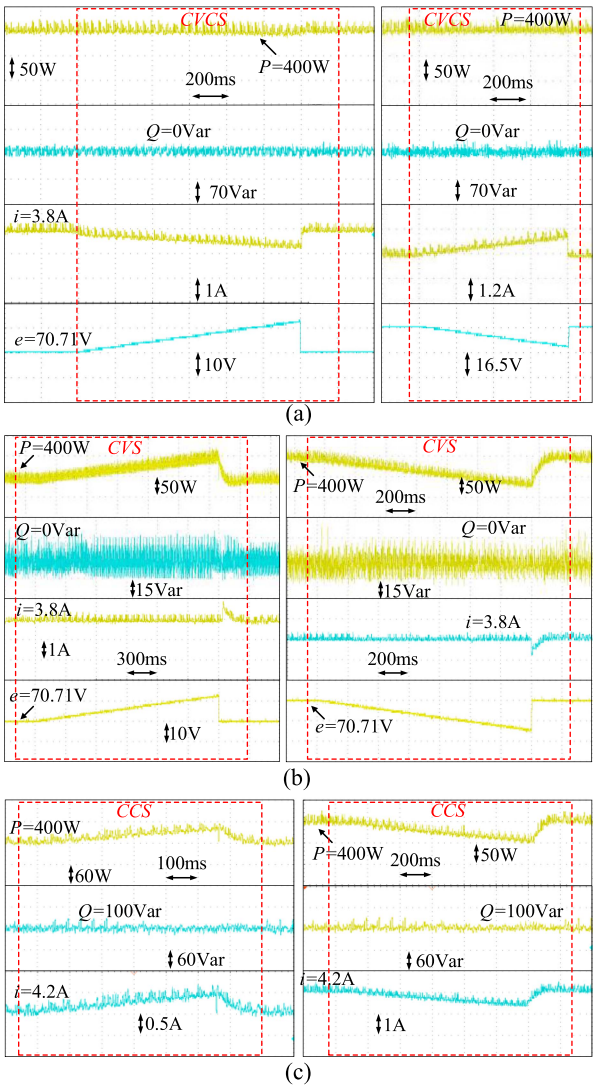

Fig. 17. Experimental results of the cyberattacks with ramp variations under the proposed method: (a) CVCS, (b) CVS, and (c) CCS.

CVS scenario. The attackers decrease and increase the voltage sensor data with ramp variations. As seen, the proposed detection system detects and clears the attacks quickly. The active power, reactive power, and current magnitude of the proposed system before, during, and after the CCS attack scenario are shown in Fig. 17(c). According to this figure, the attackers manipulate the information of the current sensors with ramp variations. However, the proposed system diagnoses and removes the attacks quickly.

VII. Conclusion

This article presents an analysis of the vulnerability of DPC in GCCs to cyberattacks. It studies DPC performance under various real-world scenarios, such as grid voltage sags/swells and load fluctuations. In addition, it considers the following cyberattack scenarios to cover various FDIA, including data integrity attacks, emulating the grid conditions, and load-altering attacks. These scenarios include attacks on current signals, voltage signals, concurrent attacks on both, an attack on voltage signals during voltage sags, and an attack on current signals during load variations. Cyber-attacks related to delay tactics will be investigated in future works. The article methodically investigates the performance of DPC under both actual events and cyberattack scenarios through a rigorous mathematical analysis. It identifies clear differences in DPC behavior under normal and compromised conditions, facilitating the extraction of crucial features for cyberattack detection. This analysis and feature extraction are performed within the stationary $\alpha\beta$ reference frame and independent of the variation rates of the grid currents and voltages. Subsequently, the article proposes a novel analytical-based, parameter-free detection method that utilizes the identified features. This method includes a designed extended state observer for computing active and reactive power samples, effectively mitigating parameter dependency and minimizing noise interference. This approach is adept at detecting a spectrum of cyberattacks, including step, and ramp variations. The method, like data-driven approaches, does not require system parameter information. However, unlike these methods, it also avoids using labeled data and training processes.

References

[1] M. S. Eslahi, S. Vaez-Zadeh, and J. Rodriguez, "Resiliency enhancement and power quality optimization of converter-based renewable energy microgrids," *IEEE Trans. Power Electron.*, vol. 38, no. 6, pp. 7785–7795, Jun. 2023.

[2] A. A. Alkahtani et al., "Power quality in microgrids including supra-harmonics: Issues, standards, and mitigations," *IEEE Access*, vol. 8, pp. 127104–127122, 2020.

[3] B. Mirafzal and A. Adib, "On grid-interactive smart inverters: Features and advancements," *IEEE Access*, vol. 8, pp. 160526–160536, 2020.

[4] D. Du et al., "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *J. Modern Power Syst. Clean Energy*, vol. 11, no. 3, pp. 727–743, May 2023.

[5] J. Ye et al., "A review of Cyber–physical security for photovoltaic systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 4, pp. 4879–4901, Aug. 2022.

[6] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—Challenges and vulnerabilities," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5326–5340, Oct. 2021.

[7] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy," *IEEE Access*, vol. 10, pp. 35846–35875, 2022.

[8] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1330–1339, May 2017.

[9] T. Huang, B. Wang, J. Ramos-Ruiz, P. Enjeti, P. R. Kumar, and L. Xie, "Detection of cyber attacks in renewable-rich microgrids using dynamic watermarking," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Aug. 2020, pp. 1–5.

[10] L. Sun et al., "Optimum placement of phasor measurement units in power systems," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 2, pp. 421–429, Feb. 2019.

[11] 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.

[12] A. Gallo, M. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3800–3815, Sep. 2020.

[13] M. Cui, J. Wang, and M. Yue, "Machine learning-based anomaly detection for load forecasting under cyber attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5724–5734, Sep. 2019.

[14] M. Zanetti, E. Jamhour, M. Pellenz, M. Penna, V. Zambenedetti, and I. Chueiri, "A tunable fraud detection system for advanced metering infrastructure using short-lived patterns," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 830–840, Jan. 2019.

[15] V. B. Kurukuru, M. A. Khan, and S. Sahoo, "Cybersecurity in power electronics using minimal data–a physics-informed spline learning approach," *IEEE Trans. Power Electron.*, vol. 37, no. 11, pp. 12938–12943, Nov. 2022.

[16] J. Zhang, Q. Li, J. Ye, and L. Guo, "Cyber-physical security framework for Photovoltaic Farms," in *Proc. IEEE CyberPELS*, Miami, FL, USA, 2020, pp. 1–7.

[17] M. A. Khan, V. S. Bharath Kurukuru, S. Sahoo, and F. Blaabjerg, "From physics to data oriented cyber attack profile emulation in grid connected PV systems," in *Proc. IEEE 22nd Workshop Control Model. Power Electron.*, 2021, pp. 1–8.

[18] X. Zha, Y. Liu, and M. Huang, "Resilient power converter: A grid-connected converter with disturbance/attack resiliency via multi-timescale current limiting scheme," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 11, no. 1, pp. 59–68, Mar. 2021.

[19] S. Yan, Y. Yang, S. Hui, and F. Blaabjerg, "A review on direct power control of pulsewidth modulation converters," *IEEE Trans. Power Electron.*, vol. 36, no. 10, pp. 11984–12007, Oct. 2021.

[20] A. Jabbarnejad, S. Vaez-Zadeh, and P. Jamallo, " Low-complexity model-free combined control of grid-connected converters under normal and abnormal grid conditions," *IEEE Trans. Energy Convers*, vol. 38, no. 4, pp. 2409–2419, Dec. 2023.

[21] R. D. Trevizan, J. Obert, V. De Angelis, T. A. Nguyen, V. S. Rao, and B. R. Chalamala, "Cyberphysical security of grid battery energy storage systems," *IEEE Access*, vol. 10, pp. 59675–59722, 2022.

[22] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst. Man Cybern. A Syst. Hum.*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[23] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," *Secur. Distrib., Grid, Mobile, Pervasive Comput.*, vol. 1, no. 367, 2007, Art. no. 6.

[24] H. Lin, Z. Yan, Y. Chen, and L. Zhang, "A survey on network security-related data collection technologies," *IEEE Access*, vol. 6, pp. 18345–18365, 2018.

[25] A. Shabtai, R. Moskovitch, Y. Elovici, and C. Glezer, "Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey," *Inf. Secur. Tech. Rep.*, vol. 14, no. 1, pp. 16–29, 2009.

[26] Z. Chu, S. Lakshminarayana, B. Chaudhuri, and F. Teng, "Mitigating load-altering attacks against power grids using cyber-resilient economic dispatch," *IEEE Trans. Smart Grid*, vol. 14, no. 4, pp. 3164–3175, Jul. 2023.

[27] L. Wang, C.-S. Lam, and M.-C. Wong, "Total harmonic distortion (THD) estimation technique based on power concept for smart power meters," in *Proc. IEEE PES Asia-Pacific Power Energy Eng. Conf.*, 2019, pp. 1–6.

[28] Y. Zhang, Z. Li, Y. Zhang, W. Xie, Z. Piao, and C. Hu, "Performance improvement of direct power control of PWM rectifier with simple calculation," *IEEE Trans. Power Electron.*, vol. 28, no. 7, pp. 3428–3437, Jul. 2013.

[29] A. Malik, A. Haque, V. B. Kurukuru, M. A. Khan, and F. Blaabjerg, "Overview of fault detection approaches for grid connected photovoltaic inverters. E-Prime - advances in Electrical engineering," *Electron. Energy*, vol. 2, 2022, Art. no. 100035.

[30] A. Ahmadi, E. Aghajari, and M. Zangeneh, "High-impedance fault detection in power distribution grid systems based on support vector machine approach," *Elect. Eng.*, vol. 104, no. 5, pp. 3659–3672, 2022.

[31] A. Jabbarnejad, S. Vaez-Zadeh, M. Khalilzadeh, and M. S. Eslahi, "Model-free predictive control for Grid-connected converters with flexibility in power regulation: A solution for unbalanced conditions," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 12, no. 2, pp. 2130–2140, Apr. 2024.

[32] A. Jabbarnejad, S. Vaez-Zadeh, and M. Jahanpour-Dehkordi, "Combined control of grid connected converters based on a flexible switching table for fast dynamic and reduced harmonics," *IEEE Trans. Energy Convers.*, vol. 35, no. 1, pp. 77–84, Mar. 2020.