Cyberattack Detection for Converter-Based Distributed dc Microgrids

Observer-Based Approaches

Tan, Sen; Xie, Peilin; Guerrero, Josep M.; Vasquez, Juan C.; Han, Renke

Published in:
I E E E Industrial Electronics Magazine

DOI (link to publication from Publisher):
10.1109/MIE.2021.3059996

Publication date:
2022

Document Version
Accepted author manuscript, peer reviewed version

Cyberattack Detection for Converter-Based Distributed dc Microgrids

Observer-Based Approaches

SEN TAN, PEILIN XIE, JOSEP M. GUERRERO, JUAN C. VASQUEZ, AND RENKE HAN

Digital Object Identifier 10.1109/MIE.2021.3059996
Date of current version: 12 March 2021

DC microgrids are complex systems connecting various renewable energy sources to different types of loads based on distributed networks. However, the strong reliance on communication networks makes dc microgrids vulnerable to intentional cyberattacks. In this article, two typical types of observer-based approaches are presented to address the attack detection problem for distributed dc microgrid systems. The disturbance decoupling approach is utilized to eliminate the influence of unknown load conditions and the coupling effect between distributed generation units (DGUs) to the residuals. The proposed method is easy to design and has less computational complexity. The performance of the provided scheme is validated by a dSPACE-based dc microgrid platform.

An Introduction to Attack Detection

Microgrid Security

DC microgrids, referred to as the next-generation power systems, are receiving great attention from both industry and academia. Integrated with DGUs, energy storage systems, and a variety of loads, a dc microgrid functions as a localized power grid that can be operated independently or connected to utility grids. With the rapid development of technology in communication networks, the framework of dc microgrids tends to be more distributed,

1932-4529/21©2021IEEE

intelligent, and tightly integrated with networks. Applications of dc microgrids can be found in the Internet of Things, Industry 4.0, smart cities, and so on.

However, due to its strong dependence on networks, the dc microgrid is more vulnerable to security threats. Compared with a conventional power system, the microgrid network has a greater risk of being corrupted by malicious attackers as it incorporates millions of devices and users. Generally, the function of a potential controller heavily relies on the reliability of the measurement devices or sensors. The controller may generate faulty control signals when the measurements are corrupted by an attacker [1], which may cause undesired power sharing [2], frequency oscillation [3], voltage restoration [4], and stability issues [5]. As a consequence, the renewable generating units may not be able to extract the maximum available power from nature or achieve proper power sharing among microgrids, or the energy storage units may fail to provide the required amount of power or operate with the optimal economic dispatch [6]. More seriously, as illustrated in Figure 1, a malicious attacker can apply various kinds of attacks to the dc microgrid system, compromise the microgrid control, and lead to disruptive events in society.

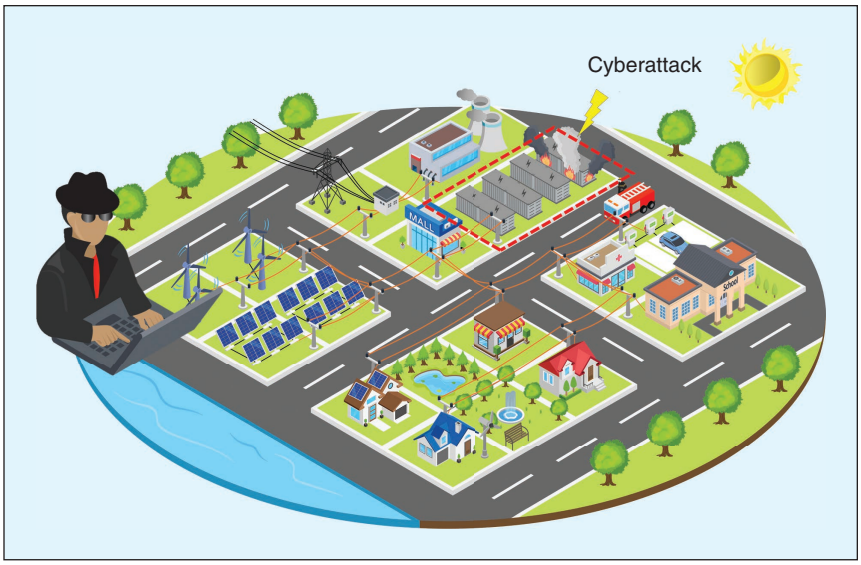

FIGURE 1 — Infrastructure destruction under cyberattacks.

Motivation

To ensure the safe and reliable operation of microgrids, the information security requirements of confidentiality, integrity, and availability [7] should be considered. Availability is the primary requirement of microgrids, ensuring reliable access to and use of information. Data integrity is the secondary—but increasingly critical—requirement that prevents unauthorized users from modifying the information. Confidentiality serves as the third important requirement to preserve restrictions on information access.

Currently, dc microgrids are generally designed with technologies that can protect against potential component failures as well as communication delays and data dropouts during operations [8]. However, attack detection differs from fault detection. Fault detection mainly focuses on potential known events and can be studied case by case, whereas attack detection deals with malicious attacks, the patterns of which are unknown to the designer. Due to the development of various intelligent attacks, traditional technologies behave in a very limited way to secure the microgrid system. Therefore, it is important to reexamine the existing techniques for attack detection of dc microgrids.

Related Work

Due to the great impact of attacks on microgrid systems, it is essential to provide effective countermeasures against cyberattacks, which can be designed both in the cyber and physical layer [9]. The typical defense mechanism deployed in the cyber layer is data authentication, realized by secure communication protocol design [10]. Data authentication, also known as watermarking or encryption methods, relies on the external message that can provide characterizations to the secure signals [11]. The data without the related characterizations are deemed as malicious attacks.

From the perspective of the physical layer, attack detection combined with resilience operations is the key method to eliminate the effect of attacks [12]. Attack detection can trigger an alarm in the presence of cyberattacks. The resilience of microgrids—defined as the capability to prepare for, respond to, and recover from attacks—can provide the microgrids with autonomous characteristics to achieve system restoration. Such methods can include 1) improving the topology or hardware redundancy, 2) reinforcing the infrastructure of microgrids, and 3) adopting a secure control function that is able to prevent the system from destruction under cyberattacks [13].

Taking cybersecurity issues into consideration, the design and analysis of attack detection schemes for a microgrid in the physical layer have been recognized as being more and more attractive in literature both for the linear [14]–[29], [31] and nonlinear system [32]. Figure 2 presents a summary of the various attack detection methods. Generally speaking, previos studies on attack detection can be classified into two categories, i.e., model-based [14]–[29], [31] and data-based schemes [33]–[40]. For the model-based scheme, a general analytical approach for attack detection problems is the use of the state estimation method by analyzing the microgrid model and measurements [14]–[18]. However, this method may fail when detecting some intelligent attacks, such as when the attacker holds some knowledge of the current

Structures	Methodologies	Principles	Limitations
Centralized	State Estimation [14]–[18]	Estimate the System States	Cannot Detect Intelligent Attacks
	Statistics [19], [20], [25], [26]	Monitor the Statistics of Measurements	Cannot Detect Intelligent Attacks
	Observer [21]–[24]	Monitor the System by Residual Signals	Difficult to Design
	Statistics and Observer [27]–[29]	Monitor the Statistics of Measurements or Residual Signals	Difficult to Design
	Data Based [33]–[40]	Compare the System With a Model Build by Historical Data	Heavy Training Burden
Distributed	Model Decomposition [43], [44]	Portion the System into Several Subsystems	Undesirable in Large-Scale System
	Disturbance Decoupling [45]	Eliminate the Effect of Disturbance to the Residuals	Difficult to Design

FIGURE 2 — A summary of attack detection approaches.

configuration of the microgrid, thus making the attack signal consistent with the detection mechanism [14], [26].

To overcome this limit, observer-based methods are promising alternatives to address attack detection problems [21]–[24]. Normally, a carefully designed residual is compared with a fixed or time-varying threshold to determine if there is an attack [16]. Furthermore, statistical methods, e.g., the χ^2 detector, are another dimension to detect random attacks by capturing the statistical behaviors of states [19], [20], [25]–[29]. However, these methods need improvement in cases where the distribution of an attack is unchanged [25], [31]. Moreover, data-based approaches have also been introduced for detecting attacks in smart grid systems [33]–[37].

These solutions generally rely on machine learning or statistical mechanisms from historical data and online measured signals to infer a model for the system under inspection. In other words, the monitored system is treated as a black box. Different data-based techniques, e.g., deep learning methods, can then be employed to recognize the behavior features of attacks and thus achieve attack detection. However, these methods usually face a heavy computational burden to train a fully connected network [38], [39].

Although remarkable progress has been made in detecting attacks during the past decade, most of the studies focus on centralized architectures. Indeed, these approaches are becoming increasingly unpractical to deal with attacks as a result of the complexity induced by large-scale distributed dc microgrid systems. Furthermore, traditional state estimation and observer-based methods may not achieve a reliable state estimation due to the existence of unknown system disturbances (e.g., load change, voltage oscillation, neighbor voltage change, and so on) [41]. The interactions between DGUs of dc microgrids could also result in a coupling effect, which also poses a challenge to the design of attack detection algorithms. Therefore, the design of attack detection for distributed dc microgrid systems should lie in exploiting the relationships among interconnected subsystems [42].

Recently, a group of distributed attack detection schemes has been proposed in terms of different ways to deal with the coupling effect of the system [16], [43]–[45]. The model decomposition method can achieve a distributed attack detection by decomposing the system into several subsystems based on the system's Laplacian matrix [43], [44]. However, it requires great computational complexity in the decomposition progress and thus is undesirable in the implementation of large-scale systems. Besides, disturbance decoupling methods play a key role in distributed attack detection approaches, where the coupling effects among neighboring units are usually seen as external disturbances. These approaches are commonly implemented with observers [45].

Besides the aforementioned methods, in which much attention is paid to investigating the relations between control signals and measurements by the appropriate model, signal-based attack detection approaches are alternative methods that have been implemented in microgrid systems. Intrusion detection is one typical detection approach that monitors the signals in communication lines in real time [46], [47]. The individual agent is deemed to be attacked and will be isolated from the system after an abnormal behavior is detected. Generally, these can be divided into anomaly detection [46] and invariant-based detection approaches [47].

Anomaly detection approaches are developed by exploring the variable-related metrics that may be violated by the abnormal agent. The advantage of anomaly detection methods is that they do not rely on predefined thresholds. However, the implementation of these methods may lead to increased operating costs and degraded system performances [48].

Invariants-based detection is an alternative approach to evaluating system security. Invariants are microgrid properties that do not change over time, such as the bound of the voltage and current of each converter. However, historical data are always needed in the detection approach; therefore, this method also suffers from higher system costs. Specifically, the consensus

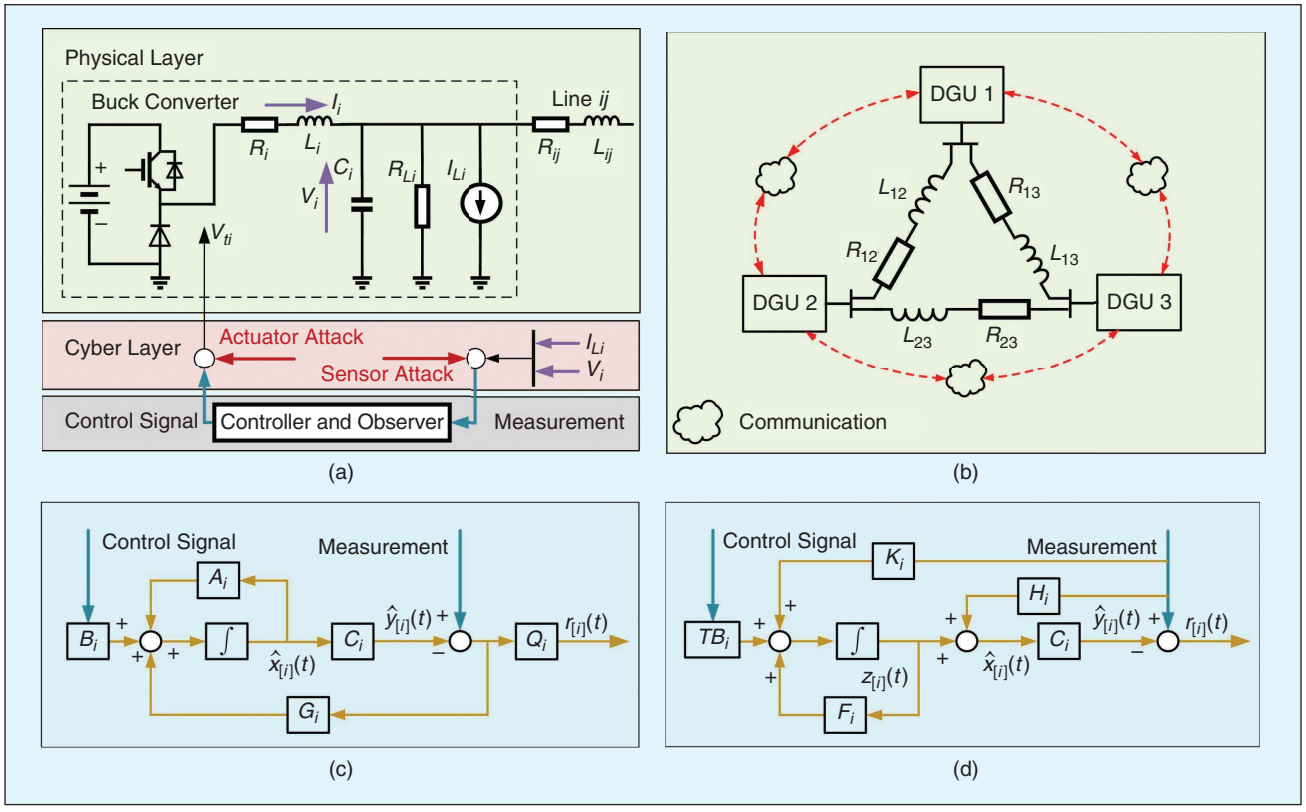

FIGURE 3 — The microgrid system structure and proposed detection approach. (a) The DGU i control system, (b) dc microgrid topology, (c) LLO, and (d) UIO.

check method is a reliable monitoring approach that can be adopted in the detection of a microgrid system, where a metric is calculated by the local and neighboring states [49]. The system is usually designed with a proper consensus protocol. If the distributed voltages, currents, or powers are detected to be not following the consensus theory, then an attack is assumed.

Contributions

We mainly consider model-based detection in this article due to the lower computational burden and system costs compared with data-based and signal-based detection methods. To the best of our knowledge, there is little research working on distributed attack detection for the dc microgrid system. Although observer-based methods provide a promising trend in attack detection applications, there have been no studies explaining how to apply these technologies to distributed dc microgrids. To address the aforementioned challenges, an observer-based detection scheme against cyberattacks for distributed dc microgrid systems is proposed in this article. The main contributions of this work are listed here.

Attack Detection Framework for a Distributed dc Microgrid System

First, a real-time cyberattack detection framework is proposed for a distributed dc microgrid with only local information of the entire system. Therefore, it is easy for scalable implementation. Second, by a disturbance decoupling method, the presented attack detection schemes are robust against unknown load conditions and coupling effects among DGUs.

Observer-Based Detection Approaches

A comprehensive design progress of Luenberger-like observer (LLO)-based and unknown input observer (UIO)-based attack detection strategies are provided. The detection strategies are complete in terms of observer design and threshold computation. Different from the existing methods, the observers are designed in the sense of residual generation. Furthermore, the sensitivity to an attack is increased by the optimal design of the observer and time-various threshold. The pros and cons of LLO and UIO are also given.

Problem Formulation: System and Attack Model

Electrical Model of dc Microgrids

Considering a DGU composed of a dc voltage source, a buck converter, and various loads, the dc microgrid can be obtained by interconnecting N DGUs through power lines. Figure 3(a) and (b) depict the electrical structure of a DGU and dc microgrid system.

In particular, as mentioned in [30], a load that includes a constant impedance load Z, a constant current load I, and a constant power load P (i.e., a ZIP load) can be represented by one equivalent impedance load, R_{Li}, and one equivalent current load, I_{Li}. Moreover, with quasi stationary line approximation, the interconnection of power lines can be assumed to be purely resistive. Therefore, the corresponding model of DGU i can be expressed as

$$\begin{cases} \dfrac{dV_i}{dt} = \dfrac{1}{C_i} I_i - \dfrac{1}{C_i}\left(\dfrac{V_i}{R_{Li}} + I_{Li}\right) \\ \qquad + \displaystyle\sum_{j\in N_i}\left(\dfrac{V_j - V_i}{C_i R_{ij}}\right) \\ \dfrac{dI_i}{dt} = -\dfrac{1}{L_i} V_i - \dfrac{R_i}{L_i} I_i + \dfrac{1}{L_i} V_{ti} \end{cases}, \quad (1)$$

where variables V_i and I_i are the ith point of common coupling (PCC) bus voltage and filter current, respectively; V_{ti} is the voltage command of the converter; R_i and L_i are the electrical parameters; and C_i is the capacitor at the PCC bus. Moreover, V_j is the voltage at the PCC of each neighboring DGU, $j \in N_i$, and R_{ij} is the resistance of the power lines.

Description of the System Model

We consider a DGU with an attack on the communication line between the converter and controller. The model of DGU i can be described in state space as

$$\begin{cases} \dot{x}_{[i]}(t) = A_i x_{[i]}(t) + B_i[u_{[i]}(t) \\ \qquad + a_{1[i]}(t)] + E_i d_{[i]}(t), \\ y_{[i]}(t) = C_i[x_{[i]}(t) + a_{2[i]}(t)] \end{cases} \quad (2)$$

where $x_{[i]}(t) = [V_i, I_{Li}]^T \in \mathbb{R}^n$ is the system state; $u_{[i]}(t) = [V_{ti}] \in \mathbb{R}^u$ is the control input; $y_{[i]}(t) \in \mathbb{R}^m$ is the system measurement; $d_{[i]}(t) = \Sigma_{j\in N_i}(V_j - V_i/R_{ij}) - ((V_i/R_{Li}) + I_{Li}) \in \mathbb{R}^d$ is the unknown disturbance, which is the combination of the coupling effect (neighbor voltage) and load conditions; and $a_{1[i]}(t) \in \mathbb{R}^u$ and $a_{2[i]}(t) \in \mathbb{R}^m$ are the actuator and sensor attack, respectively. If there is no attack on the system, then $a_{1[i]}(t), a_{2[i]}(t) = 0$; otherwise, they can be arbitrary values. A_i, B_i, C_i, and E_i are proper system matrices.

Observer Model

To detect the cyberattacks, the two typical observers (LLO and UIO) depicted in Figure 3(c) and (d) are implemented in each converter to monitor the system performance. For system (2), the LLO and UIO of the DGU i under consideration can be described by (3), in the box at the bottom of the page, where $\hat{x}_{[L,U][i]}(t) \in \mathbb{R}^n, r_{L[i]}(t) \in \mathbb{R}^p$ and $r_{U[i]}(t) \in \mathbb{R}^n$ are the estimated states and residual signals of LLO and UIO, where $p = m - rank(C_i E_i)$; and G_i, Q_i, F_i, T_i, K_i, and H_i are the observer matrices to be designed. As noticed from (3), the proposed observer can monitor the system with only local measurements of each DGU. The attack detection scheme can be achieved by comparing the residuals with a threshold. If the residuals exceed the threshold, an attack is assumed.

Observer Design and Analysis for Attack Detection

The generation of residuals is the most important task in observer-based attack detection techniques. To develop a reliable detection scheme, the following three criteria are usually adopted in the design of observers.

1) *Stability criterion*: the eigenvalues of observers (3) are located in the left half plane.
2) *Robustness criterion*: the effect of disturbances on residuals should be minimized.
3) *Sensitivity criterion*: the effect of attacks on residuals should be maximized.

For brevity, the subscript i is omitted in this section as this does not affect the discussion of observer design. Instead, the subscripts L and U are adopted to indicate the values related to LLO and UIO, respectively.

Disturbance Decoupling

The robustness criterion attempts to reduce the effect of disturbance on the monitor scheme. For LLO and UIO, the Laplace-transformed residual responses are obtained from (3) as

$$\begin{cases} r_L(s) = G_{ra[L]}(s)a(s) + G_{rd[L]}(s)d(s) \\ r_U(s) = G_{ra[U]}(s)a(s) + G_{rd[U]}(s)d(s) \\ \qquad + G_{ru[U]}(s)u(s) + G_{rz[U]}(s)z(s), \\ \qquad + G_{ry[U]}(s)y(s) \end{cases} \quad (4)$$

where $G_{r\times}$ are the transfer functions from each input to the residuals.

It can be seen from (4) that, due to the existence of exogenous disturbances, the residual is not zero in the absence of an attack. The unknown load conditions and coupling effects are the sources of false and missed alarms. To make residual signals sensitive to attacks only, it is necessary to null the transfer function from those inputs to residuals, which requests that

$$\begin{aligned} G_{rd[L]}(s) = G_{rd[U]}(s) = G_{ru[U]}(s) \\ = G_{rz[U]}(s) = G_{ry[U]}(s) = 0. \end{aligned} \quad (5)$$

Therefore, the design problem is to find the proper observer matrices to meet the requirement (5). A general necessary condition for the observers is that the maximum number of disturbances cannot be larger than the number of the independent measurements, which is satisfied in the presented dc microgrid model (2). The design problem for attack detection for the presented distributed dc microgrid is solved by the left eigenvalue assignment approach for LLO and the direct design approach for UIO in this article. The proof of existence is omitted as it goes beyond the scope of this article.

Design Freedoms

The design problem of requirement (5) restricts only the choice of the parts of observer matrices. Indeed, there is extra design freedom (e.g., the eigenvalues of the observer) that can be used to improve the sensitivity criterion. Generally, the positions of eigenvalues greatly affect the performance of the observer. However, they are commonly determined by arbitrary values, which may not be the optimal solution. In this article, the attack detectability is improved by an optimization problem, where the norm of the transfer function from the attacks to residuals is selected as the evaluation index. For the dc microgrid (2), the observer design problem is expressed as

$$\begin{cases} \dot{\hat{x}}_{L[i]}(t) = A_i \hat{x}_{L[i]}(t) + B_i u_{[i]}(t) \\ \qquad + G_i[y_{[i]}(t) - \hat{y}_{L[i]}(t)] \\ \hat{y}_{L[i]}(t) = C_i \hat{x}_{L[i]}(t) \\ r_{L[i]}(t) = Q_i[y_{[i]}(t) - \hat{y}_{L[i]}(t)] \end{cases} \quad \begin{cases} \dot{\hat{z}}_{[i]}(t) = F_i z_{[i]}(t) + T_i B_i u_{[i]}(t) \\ \qquad + K_i y_{[i]}(t) \\ \hat{x}_{U[i]}(t) = z_{[i]}(t) + H_i y_{[i]}(t) \\ r_{U[i]}(t) = y_{[i]}(t) - C_i \hat{x}_{U[i]}(t) \end{cases}, \quad (3)$$

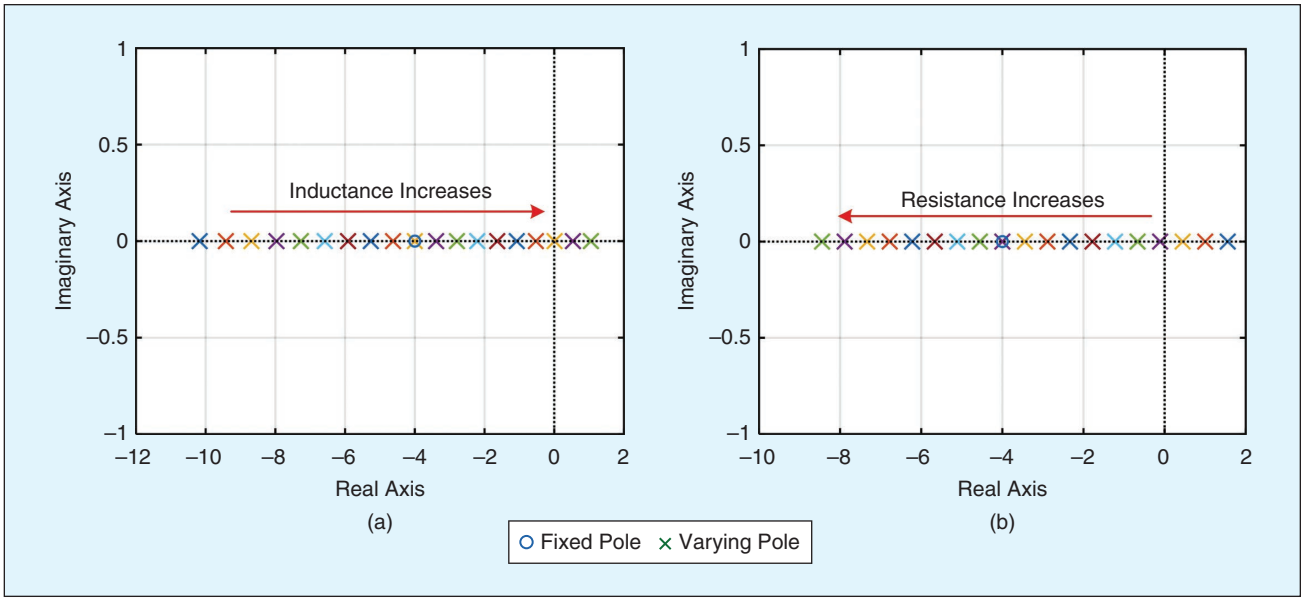

FIGURE 4 — The pole loci of the observer under filter parameter changes for (a) inductance changes and (b) resistance changes.

$$O:\ \max_{G,Q,K,H}\ \left\|G_{ra[L](s)}\right\|_{\infty},\left\|G_{ra[U](s)}\right\|_{\infty}$$
$$\text{s.t.}\quad G_{rd[L]}=G_{rd[U]}(s)=G_{ru[U]}(s)=G_{rz[U]}(s)=G_{ry[U]}(s)=0 \tag{6}$$

where the related functions are given as

$$\begin{cases} G_{ra[L]}(s)=QC+QC(sI-A+GC)^{-1}\times(B-GC) \\ G_{ra[U]}(s)=C(sI-A+HCA+K_1C)^{-1}\times[(I-HC)B-K_1C-HCs] \end{cases},$$

where $K_1=K-FH$. Notice that the matrix G, Q and K_1, H determine the observer eigenvalues as well as the magnitude of residuals. It is evident that the closer the eigenvalues are to the imaginary axis, the faster the system responds. Additionally, the higher the $|Q|,|H|$ or the farther the eigenvalues are to the imaginary axis, the higher the residual magnitude.

Residual Evaluation Criterion

The final step for designing the attack detection scheme is to determine the threshold. To detect the cyberattack more quickly and avoid false alarms, an adaptive threshold is constructed based on DGU dynamics. Given the presented observer (3), the state estimation error $e(t)=x(t)-\hat{x}(t)$ and residual can be written as the following dynamics after disturbance decoupling:

$$\begin{cases} \dot{e}_L(t)=(A-GC)e_L(t)+Ed(t)+Ba_1(t)-GCa_2(t) \\ r_L(t)=QCe_L(t)+QCa_2(t) \end{cases}$$
$$\begin{cases} \dot{e}_U(t)=(A-HCA-K_1C)e_LU(t)+(I-HC)Ba_1(t)-K_1Ca_2(t)-HC\dot{a}_2(t) \\ r_U(t)=Ce_U(t) \end{cases}. \tag{7}$$

The solution to the residual in the absence of attack can be obtained as

$$\begin{cases} r_L(t)=QCe^{(A-GC)t}|e_L(0)| \\ r_U(t)=Ce^{(A-HCA-K_1C)t}|e_U(0)| \end{cases}, \tag{8}$$

where $|e_{[L,U]}(0)|$ is the initial estimation error. Therefore, the threshold value $\bar{r}(t)$ can be selected as

$$\begin{cases} \bar{r}_L(t)=QC\Lambda e^{\bar{\lambda}t}|\bar{e}_L(0)|+\rho_L \\ \bar{r}_U(t)=C\Lambda e^{\bar{\lambda}t}|\bar{e}_U(0)|+\rho_U \end{cases}, \tag{9}$$

where $|\bar{e}_{[L,U]}(0)|>|e_{[L,U]}(0)|$ and $0\geq\bar{\lambda}\geq\lambda_{[L,U]}$ hold, Λ is a diagonal matrix whose elements should be greater than 1, $\lambda_{[L,U]}$ are the eigenvalues of the observers, and $\rho_{[L,U]}\geq 0$ are proper bound values that can be determined by multiple experimental tests.

It can also be obtained from (7) and (8) that the LLO cannot achieve a state estimation as the estimation errors are still coupled from the disturbances. In contrast, the UIO can achieve a state estimation function. However, the UIO usually asks for stronger existence conditions than the LLO.

Stability Analysis to Parameter Perturbations

Considering that the electrical parameters (*LC* filter inductance and resistance) may change during operations, the stability analysis of the proposed observer is provided quantitatively. According to the analysis presented, the poles of the observer can be freely designed as long as it meets the requirement (5). Figure 4 demonstrates an analysis of the dynamic behavior of the system with inductor parameter changes, including the pole loci, which contain a fixed and varying pole. Figure 4(a) illustrates the pole loci with the inductance increasing from 90 to 110% of nominal value. This shows that the poles on the real axis move toward the imaginary axis and even go to the right half plane (RHP), which leads to the system becoming unstable. Similarly, Figure 4(b) depicts the poles with inductor resistance changes from 90 to 110% of nominal value. As can be seen, the poles may be located in the RHP with a lower resistance value.

It can be concluded from the results that the system may become unstable with higher inductance and lower resistance values. As a consequence, a new constraint for the eigenvalues should be considered in the observer designing process (6), where the poles must lay in the left half plane

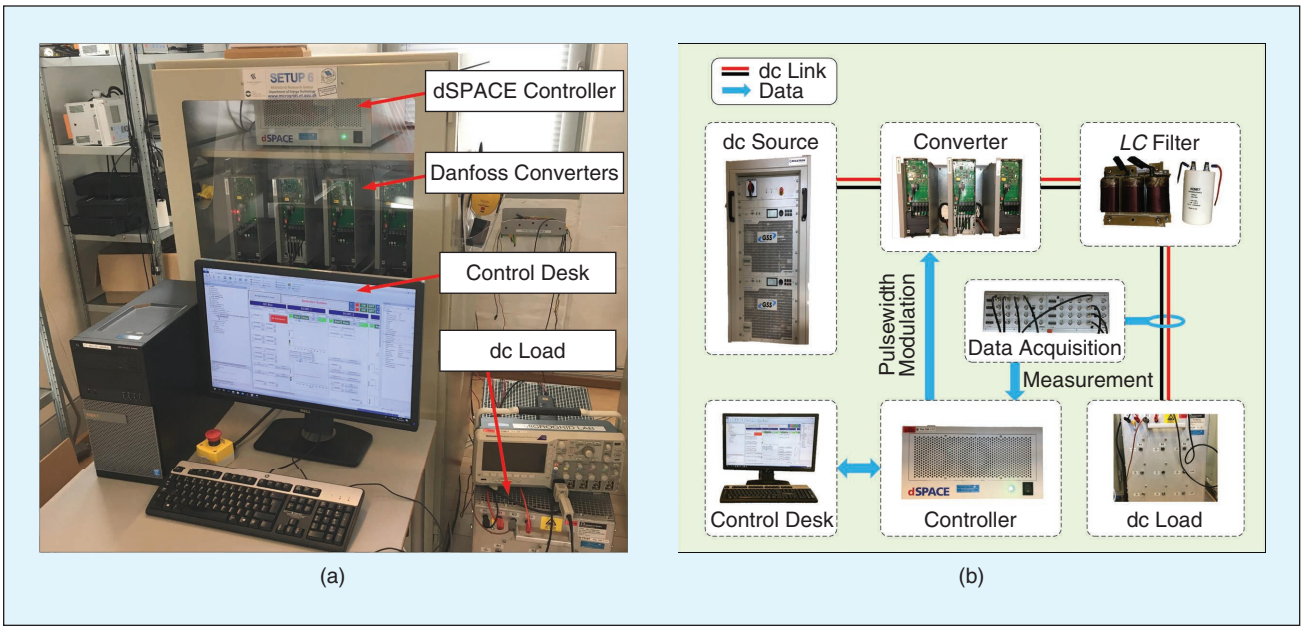

FIGURE 5 — The (a) experimental setup and (b) configuration.

Modules	Parameters	Values
dc Microgrid	Microgrid Nominal Voltage	50 V
	Switching Frequency	10 kHz
	Control Period	10 ms
dc/dc Converter	Inductor Resistance	0.1 Ω
	Inductor Inductance	1.8 mH
	dc Bus Capacitance	2.2 mF

FIGURE 6 — The electrical parameters.

given the maximum inductance value $\overline{L_i}$ and minimum resistance value $\underline{R_i}$ under consideration as

$$\lambda_{ij[\overline{L_i},\underline{R_i}]} < 0. \tag{10}$$

In addition, the system dynamics cannot be affected by the capacitor values provided by the proposed observer (3). Therefore, the pole loci under capacitance changes are omitted.

Performance Validation

Experimental results are given to verify the effectiveness of the proposed detection scheme. The control and monitor scheme is implemented in a dSPACE-based microgrid platform, which is mainly composed of a dSPACE controller, a dc source, three Danfoss converters, and a dc load, as presented in Figure 5. The setup is placed in the Center for Research for Microgrids facilities, Department of Energy Technology, Aalborg University (www.crom.et.aau.dk). The parameters of each DGU and the microgrid system are listed in Figure 6.

The control function is designed based on a standard hierarchical structure, where the primary controller is used to provide a stable output voltage, and the secondary controller is adopted to ensure power sharing. In the following, the performance capabilities of the proposed detection strategy are provided. Consider the dc microgrid with the topology in Figure 3(b), where an attacker gains access to the voltage measurements through attacks and is able to change the measurements. Notice that, although the voltage demand is 50 V, the actual voltages of the converters may shift to achieve the power-sharing function. As a result, the currents are the same among the distributed converters.

LLO

Scenario 1

Studies in this case verify the robustness against load change conditions of the presented LLO-based detection approach. In this scenario, the dc load decreases and increases at 5 and 10 s, respectively, and a constant voltage sensor attack of 0.4 V is launched on the system. The bus voltages, output currents, residuals, and corresponding thresholds of converter 1 are illustrated in Figure 7(a) and (b). As shown, there are few oscillations in voltage dynamics and 0.1-A changes in the output current after the shifting of loads, while the residual dynamic remains zero.

This verifies that the load change conditions have little effect on the detection scheme. The false data are injected into the voltage sensor of

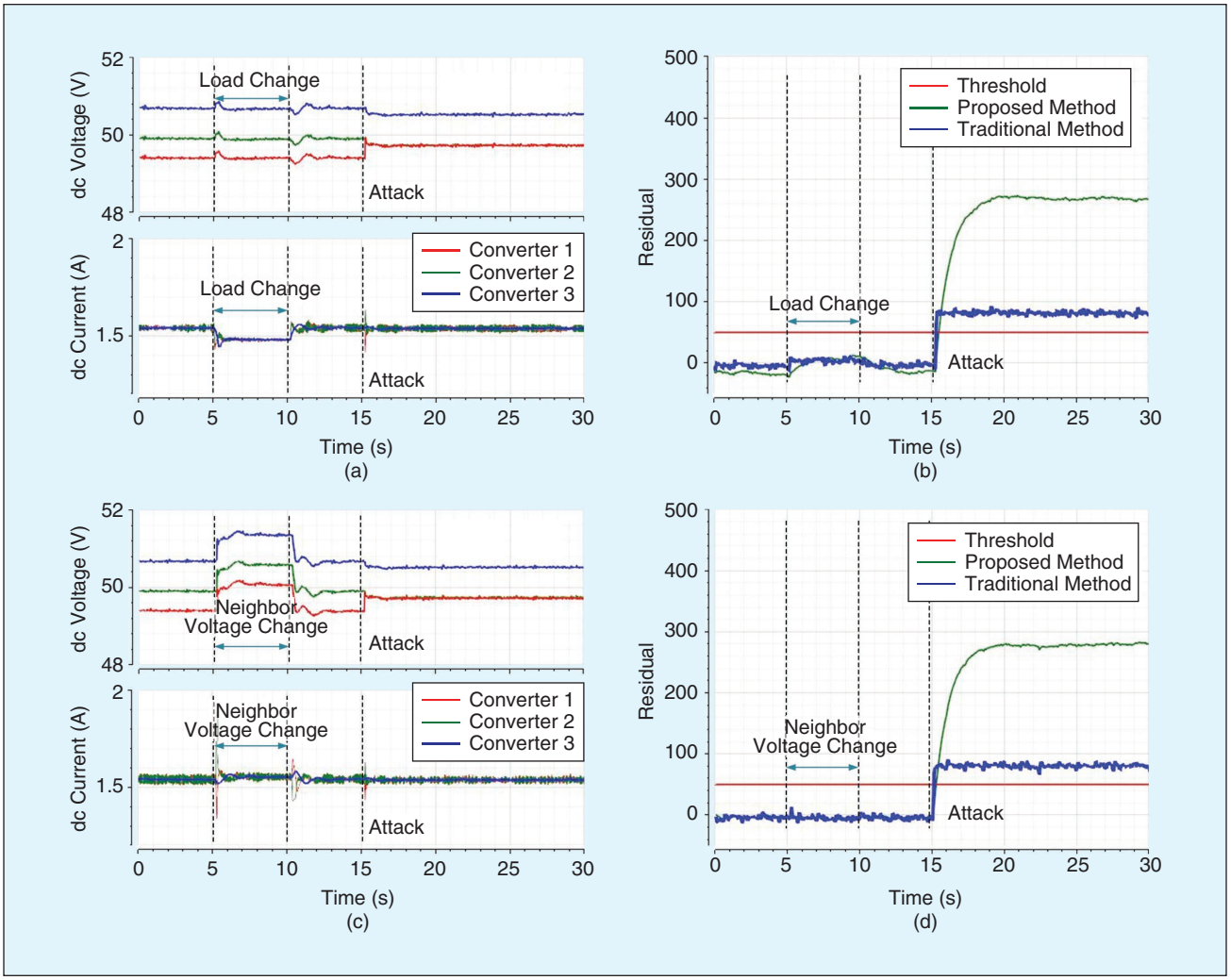

FIGURE 7 — The detection performance of LLO. (a) The microgrid voltage and current at load change conditions, (b) converter 1 residual at load change conditions, (c) microgrid voltage and current at voltage change conditions, and (d) converter 1 residual at voltage change conditions.

converter 1 at 15 s. Accordingly, the voltage measurement increases and thus leads to the decrease of neighboring voltages by 0.2 V. The residual also increases rapidly after cyberattacks, which verifies the effectiveness of the presented approach. In addition, as presented in Figure 7(b), the proposed detection approach is more sensitive to attacks compared with the traditional method provided by the larger residual signals.

Scenario 2

Studies in this scenario verify the robustness against the change of neighboring voltage conditions of the presented LLO. In this case, the neighboring voltage increases and decreases by 0.8 V at 5 and 10 s, respectively. Then a constant voltage sensor attack of 0.4 V is launched on the system at 15 s. The bus voltages, output currents, residuals, and corresponding thresholds of converter 1 are presented in Figure 7(c) and (d). It can be seen that there are oscillations in the current responses after neighboring voltage changes, while the residual remains unchanged. As seen in Figure 7(d), the residual increases directly after injecting a stealth attack into the system.

It is worth noticing that, although the oscillations of both voltage and current dynamics induced by the neighboring voltage changes are larger than that after cyberattacks, the residual only is sensitive to the attacks; this shows the reliability of the presented detection approach. Furthermore, one can also see that the magnitude of residuals with the proposed method is comparatively larger than with the conventional approach. Therefore, it can be concluded that the observer is completely decoupled from the unknown disturbances and more sensitive to the attacks.

UIO

Scenario 1

Similarly, in this case, the dc load is changed at 5 and 10 s, respectively, and a constant voltage sensor attack of 0.4 V is launched on the system. The corresponding measurements and thresholds of converter 1 are shown in Figure 8(a) and (b). As seen, the residual remains unchanged under load change conditions. Furthermore, the test results indicate that the attacks are promptly detected by the

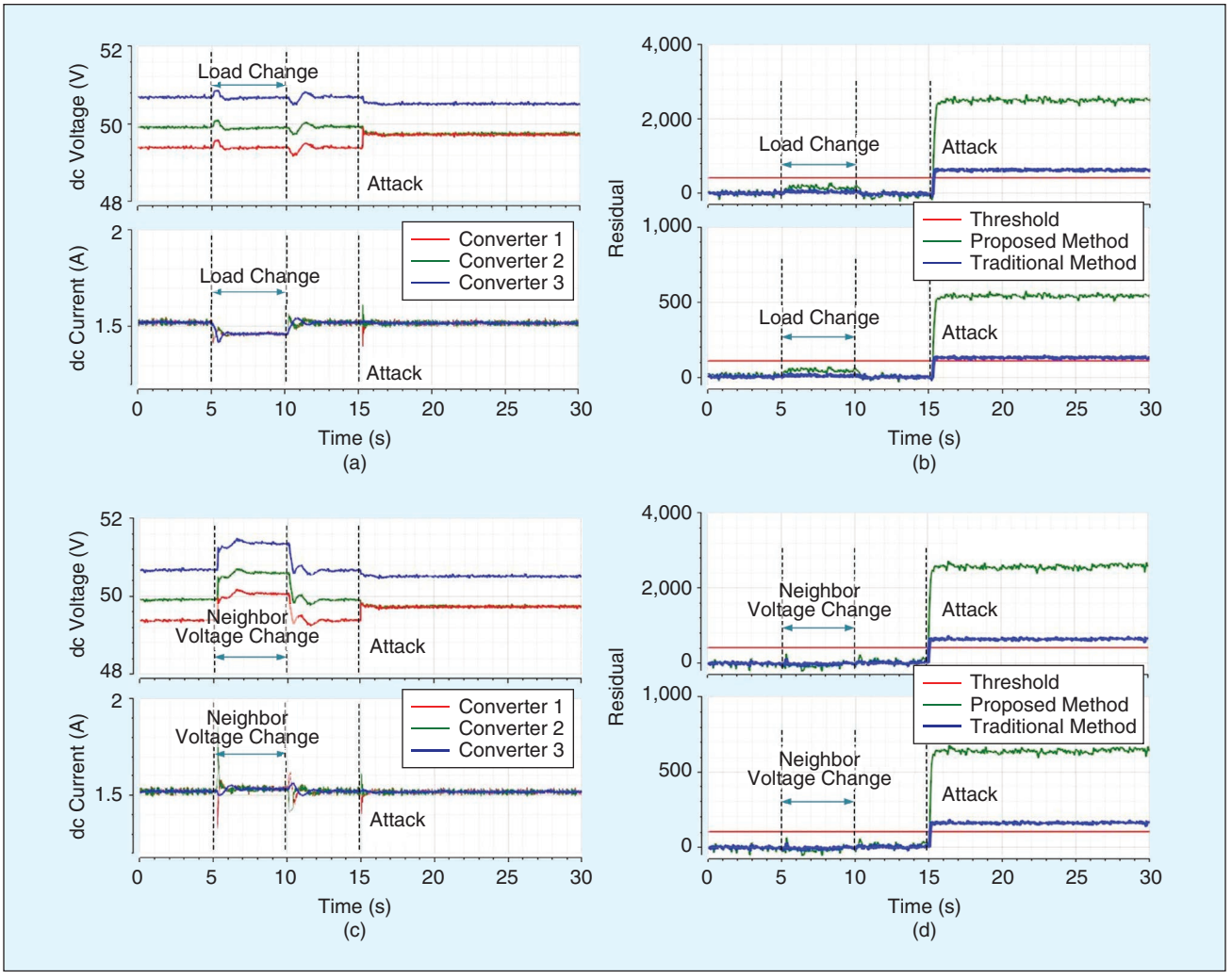

FIGURE 8 — The detection performance of UIO. (a) The microgrid voltage and current at load change conditions, (b) converter 1 residual at load change conditions, (c) microgrid voltage and current at voltage change conditions, and (d) converter 1 residual at voltage change conditions.

increased residuals after the injection of attacks, which illustrates the effectiveness of the designed observer.

Scenario 2

The test results in this scenario are presented in Figure 8(c) and (d). It can be seen that, although the effects of an attack on the system dynamics are relatively smaller, there is a rapid increase in the residual. Therefore, it can be concluded that the designed UIO is decoupled from the unknown disturbances. In addition, the larger residual of the proposed detection approach shows the improved sensitivity of the proposed approach.

Conclusion

Taking cybersecurity issues into account, an observer-based attack detection scheme has been presented in this article to address the attack detection problem for a distributed dc microgrid system. A comprehensive design procedure is provided using an LLO and a UIO. The benefits of the proposed approach are threefold. First, because the observer is able to detect attacks with only local information of the microgrid system, it can facilitate a scalable implementation. Second, with the disturbance decoupling method, the residual is decoupled from unknown load conditions and neighboring voltage changes. Third, the detectability of the observer is improved by extra design freedom, which makes the detection scheme more sensitive to cyberattacks. A time-varying threshold is designed based on the dynamics of the dc microgrid system. Experimental tests are presented to illustrate the effectiveness and achievable performance of the proposed scheme.

Acknowledgment

This work was supported by VILLUM FONDEN under the VILLUM Investigator Grant 25920: Center for Research on Microgrids (www.crom.et.aau.dk).

Biographies

Sen Tan (sta@et.aau.dk) earned his B.S. degree in automation and his M.S. degree in control engineering from Northeastern University, China, in 2014 and 2017, respectively. He is currently working toward his Ph.D. degree with the Department of Energy Technology, Aalborg University, Aalborg, 9220, Denmark. His research interests include distributed control in microgrids, fault detection, and motor drive technologies. He is a Student Member of IEEE.

Peilin Xie (pxi@et.aau.dk) earned her B.S. degree in electrical engineering from Beijing Jiaotong University, China, in 2015 and her M.S. degree in electrical engineering and automation from North China Electric Power University, China, in 2018. She is currently working toward her Ph.D. degree at the Department of Energy Technology, Aalborg University, Aalborg, 9220, Denmark. Her research interests include power management control for shipboard microgrids. She is a Student Member of IEEE.

Josep M. Guerrero (joz@et.aau.dk) earned his Ph.D. degree from the Technical University of Catalonia, Spain, in 2003. He is a full professor with the Department of Energy Technology, Aalborg University, Aalborg, 9220, Denmark, where he is the director of the Center for Research on Microgrids. His research interests include distributed energy-storage systems, hierarchical and cooperative control, energy management systems, smart metering, and the Internet of Things for ac/dc microgrid clusters. He was awarded the Institute for Scientific Information Highly Cited Researcher by Thomson Reuters. He is a Fellow of IEEE and a member of the IEEE Industrial Electronics Society.

Juan C. Vasquez (juq@et.aau.dk) earned his Ph.D. degree in automatic control, robotics, and computer vision from Barcelona Tech, Polytechnic University of Catalonia, Spain, in 2009. In 2019, he became a professor of the energy Internet and microgrids. He is the codirector of the Villum Center for Research on Microgrids, Aalborg University, Aalborg, 9220, Denmark. His current research interests include operation, control, and energy management in microgrids, the Internet of Things, and the energy Internet. He was awarded the Institute for Scientific Information Highly Cited Researcher by Thomson Reuters. He is a Senior Member of IEEE and a member of the IEEE Industrial Electronics Society.

Renke Han (renke.han@eng.ox.ac.uk) earned his Ph.D. degree in power electronics systems from Aalborg University, Denmark, in 2018. Since November 2018, he has been with the Power Electronics Group, University of Oxford, Oxford, OX1 3PJ, United Kingdom, as a postdoctoral researcher. His research interests include power electronics converter design, including printed circuit board design for power and control circuitries, magnetic elements design, embedded system development, and modeling, control, and stability analysis for microgrids. He was selected as one of six research representatives by the University of Oxford attending the Global Young Scientist Summit 2021. He is a Member of IEEE.

References

[1] S. Saha, T. Roy, M. Mahmud, M. Haque, and S. Islam, "Sensor fault and cyber attack resilient operation of DC microgrids," *Int. J. Electr. Power Energ. Syst.*, vol. 99, pp. 540–554, July 2018. doi: 10.1016/j.ijepes.2018.01.007.

[2] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, 2018. doi: 10.1109/TPWRS.2018.2794468.

[3] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked AC microgrids under unbounded cyber attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3785–3794, 2020. doi: 10.1109/TSG.2020.2984266.

[4] P. Danzi, C. Stefanovic, L. Meng, J. M. Guerrero, and P. Popovski, "On the impact of wireless jamming on the distributed secondary microgrid control," in *Proc. 2016 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6. doi: 10.1109/GLOCOMW.2016.7848980.

[5] S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4066–4075, 2018. doi: 10.1109/TII.2018.2885170.

[6] P. Xie et al., "Optimization-based power and energy management system in shipboard microgrid: A review," *IEEE Syst. J.*, early access, 2021. doi: 10.1109/JSYST.2020.3047673.

[7] "The smart grid interoperability panel–cyber security working group." Wikia. 2010. https://itlaw.wikia.org/wiki/Smart_Grid_Interoperability_Panel%E2%80%93Cyber_Security_Working_Group

[8] B. Arbab-Zavar, E. J. Palacios-Garcia, J. C. Vasquez, and J. M. Guerrero, "Smart inverters for microgrid applications: A review," *Energies*, vol. 12, no. 5, p. 840, 2019. doi: 10.3390/en12050840.

[9] S. Tan, Y. Wu, P. Xie, J. M. Guerrero, J. C. Vasquez, and A. Abusorrah, "New challenges in the design of microgrid systems: Communication networks, cyberattacks, and resilience," *IEEE Electrific. Mag.*, vol. 8, no. 4, pp. 98–106, 2020. doi: 10.1109/MELE.2020.3026496.

[10] Y. Mo et al., "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, 2011. doi: 10.1109/JPROC.2011.2161428.

[11] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1554–1569, 2019. doi: 10.1109/TSMC.2018.2884952.

[12] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Bie, "Microgrids for enhancing the power grid resilience in extreme conditions," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 589–597, 2016.

[13] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, "Networked microgrids for enhancing the power system resilience," *Proc. IEEE*, vol. 105, no. 7, pp. 1289–1310, 2017. doi: 10.1109/JPROC.2017.2685558.

[14] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. Syst. Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011. doi: 10.1145/1952982.1952995.

[15] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, 2014. doi: 10.1109/JSYST.2014.2323266.

[16] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, 2013. doi: 10.1109/TAC.2013.2266831.

[17] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014. doi: 10.1109/TSG.2013.2284438.

[18] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012. doi: 10.1109/TSG.2012.2195338.

[19] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, "Detection and mitigation of data manipulation attacks in AC microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2588–2603, 2019. doi: 10.1109/TSG.2019.2958014.

[20] B. P. Poudel, A. Mustafa, A. Bidram, and H. Modares, "Detection and mitigation of cyberthreats in the DC microgrid distributed control system," *Int. J. Electr. Power Energ. Syst.*, vol. 120, pp. 105,968, Sept. 2020. doi: 10.1016/j.ijepes.2020.105968.

[21] A. J. Gallo et al., "Distributed cyber-attack detection in the secondary control of DC microgrids," in *Proc. 2018 Euro. Control Conf. (ECC)*, pp. 344–349. doi: 10.23919/ECC.2018.8550549.

[22] W. Ao, Y. Song, and C. Wen, "Adaptive cyber-physical system attack detection and reconstruction with application to power systems," *IET Control Theory Appl.*, vol. 10, no. 12, pp. 1458–1468, 2016. doi: 10.1049/iet-cta.2015.1147.

[23] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 2008 28th Int. Conf. Distrib. Comput. Syst. Workshops*, pp. 495–500. doi: 10.1109/ICDCS.Workshops.2008.40.

[24] J. Yan, F. Guo, and C. Wen, "Attack detection and isolation for distributed load shedding algorithm in microgrid systems," *IEEE J. Emerg. Sel. Topics Ind. Electron.*, vol. 1, no. 1, pp. 102–110, 2020. doi: 10.1109/JESTIE.2020.3004744.

[25] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, 2014. doi: 10.1109/TCNS.2014.2357531.

[26] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015. doi: 10.1109/TSG.2015.2388545.

[27] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 4–13, 2016. doi: 10.1109/TCNS.2016.2570003.

[28] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Trans. Autom.*

Control, vol. 61, no. 9, pp. 2618–2624, 2015. doi: 10.1109/TAC.2015.2498708.

[29] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, 2014. doi: 10.1109/TCST.2013.2280899.

[30] R. Han, M. Tucci, A. Martinelli, J. M. Guerrero, and G. Ferrari-Trecate, "Stability analysis of primary plug-and-play and secondary leader-based controllers for DC microgrid clusters," *IEEE Trans. Power Syst.*, vol. 34, no. 3, pp. 1780–1800, 2018. doi: 10.1109/TPWRS.2018.2884876.

[31] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, 2015. doi: 10.1109/LSP.2015.2421935.

[32] L. Mili, M. Cheniae, N. Vichare, and P. J. Rousseeuw, "Robust state estimation based on projection statistics [of power systems]," *IEEE Trans. Power Syst.*, vol. 11, no. 2, pp. 1118–1127, 1996. doi: 10.1109/59.496203.

[33] W.-H. Chen, S.-H. Hsu, and H.-P. Shen, "Application of SVM and ANN for intrusion detection," *Comput. Oper. Res.*, vol. 32, no. 10, pp. 2617–2634, 2005. doi: 10.1016/j.cor.2004.03.019.

[34] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017. doi: 10.1109/TSG.2017.2703842.

[35] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, 2014. doi: 10.1109/JSYST.2014.2341597.

[36] K.-F. Abdollah, W. Su, and T. Jin, "A machine learning based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 650–658, Jan. 2021. doi: 10.1109/TII.2020.2964704.

[37] M. R. Habibi, H. R. Baghaee, T. Dragi˘cevi, F. Blaabjerg, "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE J. Emerg. Sel. Topics Power Electron.*, 2020. doi: 10.1109/JESTPE.2020.2968243.

[38] K. Hamedani, L. Liu, R. Atat, J. Wu, and Y. Yi, "Reservoir computing meets smart grids: Attack detection using delayed feedback networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 734–743, 2017. doi: 10.1109/TII.2017.2769106.

[39] K. Hamedani, L. Liu, S. Hu, J. Ashdown, J. Wu, and Y. Yi, "Detecting dynamic attacks in smart grids using reservoir computing: A spiking delayed feedback reservoir based approach," *IEEE Trans. Emerg. Topics Computat. Intell.*, vol. 4, no. 3, pp. 253–264, 2019. doi: 10.1109/TETCI.2019.2902845.

[40] B. M. Sanandaji, E. Bitar, K. Poolla, and T. L. Vincent, "An abrupt change detection heuristic with applications to cyber data attacks on power systems," in *Proc. 2014 American Control Conf.*, pp. 5056–5061. doi: 10.1109/ACC.2014.6859403.

[41] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, 2012. doi: 10.1109/MSP.2012.2185911.

[42] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, "Brief survey on attack detection methods for cyber-physical systems," *IEEE Syst. J.*, vol. 14, no. 4, pp. 5329–5339, 2020. doi: 10.1109/JSYST.2020.2991258.

[43] M. Davoodi, N. Meskin, and K. Khorasani, "Simultaneous fault detection and consensus control design for a network of multi-agent systems," *Automatica*, vol. 66, pp. 185–194, Apr. 2016. doi: 10.1016/j.automatica.2015.12.027.

[44] P. P. Menon and C. Edwards, "Robust fault estimation using relative information in linear multi-agent networks," *IEEE Trans. Autom. Control*, vol. 59, no. 2, pp. 477–482, 2013. doi: 10.1109/TAC.2013.2274689.

[45] I. Shames, A. M. Teixeira, H. Sandberg, and K. H. Johansson, "Distributed fault detection for interconnected second-order systems," *Automatica*, vol. 47, no. 12, pp. 2757–2764, 2011. doi: 10.1016/j.automatica.2011.09.011.

[46] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3690–3701, 2020. doi: 10.1109/TSG.2020.2979160.

[47] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731–6741, 2017. doi: 10.1109/TSG.2017.2721382.

[48] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "False data injection attacks on inverter-based microgrid in autonomous mode," in *Distributed Control Methods and Cyber Security Issues in Microgrids*. Elsevier, 2020, pp. 125–146.

[49] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, "Resilient cooperative control of DC microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 1083–1085, 2018. doi: 10.1109/TSG.2018.2872252.