Aalborg Universitet

AALBORG UNIVERSITY
DENMARK

False Data Injection Cyber-Attacks Detection for Multiple DC Microgrid Clusters

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

Published in:
Applied Energy

DOI (link to publication from Publisher):
10.1016/j.apenergy.2021.118425

Creative Commons License
CC BY 4.0

Publication date:
2022

Document Version
Publisher's PDF, also known as Version of record

Link to publication from Aalborg University

Citation for published version (APA):
Tan, S., Xie, P., Guerrero, J. M., & Vasquez, J. C. (2022). False Data Injection Cyber-Attacks Detection for Multiple DC Microgrid Clusters. *Applied Energy*, *310*, [118425]. https://doi.org/10.1016/j.apenergy.2021.118425

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

Take down policy
If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

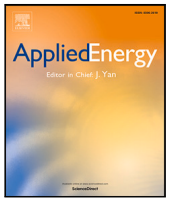
Downloaded from vbn.aau.dk on: November 19, 2022

Applied Energy 310 (2022) 118425

Contents lists available at ScienceDirect

Applied Energy

journal homepage: www.elsevier.com/locate/apenergy



False Data Injection Cyber-Attacks Detection for Multiple DC Microgrid Clusters

Sen Tan *, Peilin Xie, Josep M. Guerrero, Juan C. Vasquez

Center for Research on Microgrids (CROM), AAU Energy, Aalborg University, Aalborg, 9220, Denmark

ARTICLE INFO

Keywords:
Cyber-attacks
DC microgrids
Robust detection

ABSTRACT

DC microgrids are considered as the next generation of power systems because of the possibility of connecting various renewable energy sources to different types of loads based on distributed networks. However, due to the strong reliance on communication networks, DC microgrids are vulnerable to intentional cyber-attacks. Therefore, in this paper, a robust cyber-attack detection scheme is proposed for DC microgrid systems. Utilizing the parity-based method, a multi-objective optimization problem is formulated to achieve robust detection against electrical parameter perturbations and unknown disturbances. An analytical solution is then provided using the singular value decomposition approach. With the disturbance decoupling scheme, the presented detection strategy can monitor the system with only local knowledge of the DC microgrid. The proposed method is easy to design and with less computation complexity. The performances of the provided scheme are validated by simulation tests and experimental results.

1. Introduction

DC microgrids (MGs), known as next-generation power systems, have received significant attention in recent years because of their ability to transmit power from renewable energy sources and energy storage devices to various loads with greater efficiency and reliability than the AC grid. As a distributed power supply, the DC MG can be operated independently or connected to the utility grid. Such applications can be found in power generations [1], smart houses [2], transportation systems [3], etc.

Due to the rapid developments of the Industry 4.0 paradigm, information technology-based solutions have been widely used in industrial processes. The revolutionary changes have seen the emergence of cyber–physical systems where large amounts of data are exchanged between multiple devices in real time [4]. Accordingly, the framework of DC MG tends to be more distributed, intelligent and tightly integrated with the network. However, due to the strong reliance on the communication technologies, DC MGs are more vulnerable to security threats [5] and have a higher risk of being compromised by malicious attackers.

In general, the functionality of a potential microgrid controller relies heavily on the reliability of the data received by the measurement devices or sensors. For example, if the sensors or communication links are compromised by an attacker, the controllers may receive faulty data and therefore make inappropriate control decisions [6], leading to the undesirable power-sharing [7], frequency oscillating [8] and stability issues [9]. As a result, renewable energy generating units may not be able to produce the maximum amount of available power from nature or meet the appropriate power sharing between microgrids, and energy storage devices may not be able to provide the required amount of power or operate with optimal economic dispatch [10]. More seriously, attackers may be able to disrupt the system without adequate security protection in terms of hardware or software policies, leading to significant social losses. Examples include the nuclear facility struck by Stuxnet malware [11], power outage event [12,13] and nuclear plant blackout accident [14]. Considering the huge impact of attacks on microgrid systems, it is vital to provide an effective detection scheme to counter cyber attacks.

1.1. State of the art

Taking the cyber-security issues into consideration, the design and analysis of attack detection methods for microgrids can be deployed at both the cyber-layer and the physical layer [15]. Third-party detection methods, also known as data authentication, watermarking and key management methods, are typical defense mechanisms implemented in the cyber-layer. External messages are generated normally through various protocols or low-cost hardware, that can provide characteristics for security signals. Data without relevant characteristics is considered as a malicious attack. However, the disadvantage of this approach is

* Corresponding author.
E-mail addresses: sta@energy.aau.dk (S. Tan), pxi@energy.aau.dk (P. Xie), joz@energy.aau.dk (J.M. Guerrero), juq@energy.aau.dk (J.C. Vasquez).

https://doi.org/10.1016/j.apenergy.2021.118425
Received 1 September 2021; Received in revised form 26 October 2021; Accepted 30 October 2021
Available online 29 January 2022
0306-2619/© 2022 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Table 1
Summary of attack detection approaches.

Detection	Methodologies	Principles and limitations
Signal-based detection	Anomaly detection	1. Monitoring the real-time measurements 2. Do not investigate the relations of system model
Model-based detection	State estimation	1. Estimate the system state 2. Cannot detect intelligent attacks
	Observer-based detection	1. Compare the residual with a fix or adaptive threshold 2. Uneasy to design
	Statistical method	1. Capture the statistical behaviors of measurements 2. Cannot detect intelligent attacks
Data-based detection	Machine learning	1. Compare the system with a model build by historical data 2. Face a heavy computation burden to train a system model
Distributed attack detection	Model decomposition method	1. Portion the system into several subsystems 2. Undesirable in large-scale system
	Perturbation Decoupling	1. Eliminate the effect of disturbance to the residuals 2. Cannot achieve robust detection against modeling uncertainties

that it introduces an additional computational burden and can incur delayed performance, as external information needs to be encoded and decoded before and after data communication [5]. Therefore, there is a trade-off between communication security and computational efficiency.

Research into the attack detection in physical layer of microgrid can be divided into three categories, namely signal-based detection, model-based detection and data-based detection methods [16]. Table 1 lists the summary of common attack detection approaches employed in physical layer. The signal-based attack detection method implemented in microgrids is achieved by monitoring the signals in the communication links in real-time [17]. For example, the attack detection was achieved by checking the data transmission frequency in [18]. If the frequency of certain links is not consistent with the defined transmission frequency, these links are detected as being compromised. Furthermore, a signal temporal logic detection has been proposed in [19], where the voltages and currents of DC microgrids are monitored for comparison with pre-defined operational bounds. Moreover, the attack detection in [20,21] was performed by a consensus check between the local and neighboring measurements. An anomaly detection has been developed based on the use of software-defined networking [22]. If abnormal behavior is detected in a local generation unit, it will be considered under attack and isolated from the system. However, the disadvantage of this approach is that it does not sufficiently investigate the relationship between the control signal and the measurement, which is a useful tool for achieving reliable detection.

Model-based detection schemes are alternative detection methods by utilizing the mathematical model of the system. The most common approach to achieve model-based attack detection is the implementation of state estimation [6,23]. Although such methods can detect basic attacks, they may fail when the false data is introduced in a coordinated manner that makes it appear to be consistent with the detection mechanism, thereby bypassing it [24]. To cope with this problem, observer-based detection approaches have been given full consideration by studying the dynamic model of the system [25,26]. Typically, a residual signal is carefully generated and compared to a fixed or adaptive threshold to determine if an attack is present. Moreover, statistical methods are widely used to detect attacks by monitoring the statistical behavior of the measurements. For example, the Kullback–Leibler distance was adopted in [24,27] to detect attacks by calculating the probability distributions of measurements. Furthermore, a χ^2 detector was developed in [28] for detecting attacks by checking the statistical behavior of estimation errors. The disadvantage of these methods, however, is that they may fail when tackling attacks with unchanged distribution and therefore deserve further research.

In addition, data-based detection methods are now accepted as a powerful tool for detecting attacks on smart grid systems [29]. These solutions typically rely on machine learning or statistical mechanisms to infer a model of the system from historical data and measurement signals. For example, a deep learning-based mechanism has been developed in [30] to recognize the behavior features of False Data Injection (FDI) attacks with historical measurements, the features of which can be employed to detect attacks. In addition, two machine learning-based techniques were proposed in [31] to detect the deviation in measurements. In [32], the artificial neural network and support vector machine were trained with 5 days data to predict cyber-attacks. Furthermore, the DC voltages and currents were estimated in [33] with a nonlinear auto-regressive exogenous model neural network. The cyber-attack can be then detected by checking the estimation errors. However, these data-based detection approaches usually face a heavy computational burden to train a fully connected network and therefore suffer from higher system costs [34].

Although significant progress has been made in the past decade in detecting attacks, these methods are not always practical due to the complexity induced by large-scale distributed DC MG systems. Moreover, traditional state estimation and observer-based methods may not achieve reliable state estimation due to the presence of unknown system disturbances (load variations, voltage oscillations, neighboring voltage variations, etc.) [35]. The design of attack detection for distributed DC MG systems should therefore lie in exploiting the relationships between the interconnected subsystems [16].

Recently, a set of distributed attack detection schemes have been proposed to deal with the coupling effects of the system in different ways through a model decomposition approach [36,37]. However, it requires a significant computational complexity in the decomposition process. Disturbance decoupling is an alternative method to deal with unknown disturbances in the attack detection for distributed DC microgrid, where the coupling effects are treated as external disturbances [38]. However, as the electrical parameters may fluctuate with the device temperature, the modeling uncertainties have introduced new challenges for the design of cyber-attack detection strategy. Although it is possible to represent the modeling errors as unknown disturbances with an approximate distribution matrix [39], it may lead to an increase in the number of disturbances and therefore makes the design of robust detection schemes for distributed DC MGs more challenging.

1.2. Objectives and contributions

The model-based attack detection approach depends strictly on the use of a mathematical model of the system. Therefore, the better

the model that represents the dynamics of the system, the better the detection performance. Although a number of attack detection methods have been developed in recent years, very little research has taken into account the modeling uncertainty when designing detection strategies. Due to the presence of parameter variations, traditional observer-based methods may fail to achieve reliable detection performance.

To the best of our knowledge, no research has been done to explain how to design and apply robust detection techniques for distributed DC microgrids. Robust cyber-attack detection is therefore still a worthwhile research topic. To address the above challenges, this paper proposes a parity-based cyber-attack detection scheme for a DC MG cluster. The main contributions of this work are listed as follows.

1.2.1. Attack detection framework for DC microgrids

A real-time cyber-attack detection framework capable of large scale implementation is provided in this paper in terms of residual generation and threshold calculation. The limitation of observer-based detection methods is discussed when considering modeling uncertainties of DC microgrids. The proposed attack detection method is able to monitor the system effectively even under unknown load and voltage change conditions.

1.2.2. Robust detection design

Different from existing detection approaches, the proposed residual generation enables reliable attack detection even in the presence of parameter variations. In addition, the sensitivity to attacks is improved by formulating a new multi-objective optimization problem. An analytical solution is also provided with singular value decomposition approach.

1.2.3. Suitable for multiple applications

Because the proposed attack detection method is based on the converter model, therefore, it can be applied both in the grid-feeding converters and grid-forming converters. In addition, considering that in a microgrid cluster, converters also play the role of energy interaction and conversion between individual microgrids. Therefore, the attack detection method proposed in this paper can also be applied in a multiple DC microgrid cluster.

1.3. Paper organization

The outline of this paper is given as follows. The research problem is presented in Section 2, which includes a description of the modeling and detection strategy for DC microgrids with cyber-attacks. In Section 3, the proposed detection framework is constructed, where a parity-based detection scheme is illustrated, taking into account the presence of unknown disturbances and modeling uncertainties. Experimental results are provided in Section 5, and concluding remarks are given in the last section.

2. Cyber–physical DC microgrids

This section explains the distributed control and proposed robust detection framework for a DC microgrid.

2.1. Electrical model of DC microgrids

Considering a microgrid composed of a renewable energy source (RES), a Buck converter and loads, the DC MG cluster can be obtained by interconnecting N microgird through power lines, as shown in Fig. 1.

Normally, for each microgird, a ZIP load is always assumed including a constant impedance load (Z), a constant current load (I) and a constant power load (P). While, as mentioned in [40], after linearization of the constant power load around the rated voltage point, the ZIP load can be represented by an equivalent impedance load R_{Li} and an equivalent current load I_{Li}. The structure of the local generation unit is also depicted in Fig. 1. Indeed, the linearization of constant power load does not influence the presented detector, because the proposed detection approach is robust to the unknown loads.

The dynamic of single microgrid i can be expressed as:

$$\begin{cases} V_i(k+1) = \left(1 - \dfrac{T_s}{\eta_c C_i R_{Li}}\right) V_i(k) + \dfrac{T_s}{\eta_c C_i} I_i(k) - \dfrac{T_s}{\eta_c C_i} I_{Li}(k) \\ \quad + \displaystyle\sum_{j \in N_i} T_s \left(\dfrac{V_j(k) - V_i(k)}{\eta_c C_i R_{ij}} \right) \\ I_i(k+1) = -\dfrac{T_s}{\eta_l L_i} V_i(k) + \left(1 - \dfrac{T_s R_i}{\eta_l L_i}\right) I_i(k) + \dfrac{T_s}{\eta_l L_i} V_{ti}(k) \end{cases} \tag{1}$$

where variables V_i, I_i are ith point of common coupling (PCC) bus voltage, filter current respectively; V_{ti} generated by the controller, is the voltage command of the converter; R_i, L_i and C_i are the resistance, inductance and capacitor of LC filter; η_c, η_l are unknown values, which refer to the degree of parameter variations of the capacitor and inductance; Moreover, V_j is the voltage at the PCC of each neighboring MGs, where $j \in \mathcal{N}_i$; The set $\mathcal{N}_i$ is neighbors of MG i; R_{ij} are the resistances of the power lines; T_s is the sample time of the system.

2.2. Description of system model

Consider a DC microgrid with an attack on the communication line between the converter and controller. The discrete model of MG i can be described in state space as:

$$\begin{cases} x_i(k+1) = A_{t[i]} x_i(k) + B_{t[i]}[u_i(k) + a_{1i}(k)] + E_{t[i]} d_i(k) \\ y_i(k) = C_{t[i]} x_i(k) + a_{2i}(k) \end{cases} \tag{2}$$

where $x_{[i]}(k) = [V_i(k), I_i(k)]^T \in \mathbb{R}^n$ is system state; $u_{[i]}(k) = [V_{ti}(k)] \in \mathbb{R}^u$ is the control input; $y_{[i]}(k) \in \mathbb{R}^m$ is the system measurement; $d_{[i]}(k) = \sum_{j \in \mathcal{N}_i} V_i(k)/R_{Li} + I_{Li}(k) - (V_j(k) - V_i(k))/R_{ij} \in \mathbb{R}^d$ accounts for the unknown disturbance, which is the combination of load conditions and coupling effect (neighboring voltage); $a_{1i}(k) \in \mathbb{R}^u$ and $a_{2i}(k) \in \mathbb{R}^m$ are the actuator attack and sensor attack, respectively. The false data injection attack is considered in this paper. If there is no attack on the system, then $a_{1i}(k), a_{2i}(k) = 0$, otherwise they can be arbitrary values. $\{A_{t[i]}, B_{t[i]}, C_{t[i]}, E_{t[i]}\}$ are proper system matrices which are not known precisely due to the modeling uncertainties and the subscript t denotes variations. These matrices have nominal value denoted as $\{A_i, B_i, C_i, E_i\}$, which can be defined when $\eta_c = \eta_l = 1$ as:

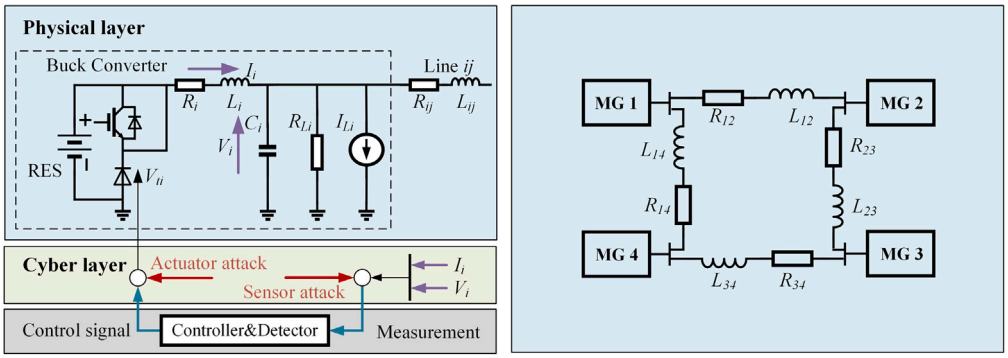
$$A_i = \begin{bmatrix} 1 & \dfrac{T_s}{C_i} \\ -\dfrac{T_s}{L_i} & 1 - \dfrac{R_i T_s}{L_i} \end{bmatrix}, \quad B_i = \begin{bmatrix} 0 \\ \dfrac{T_s}{L_i} \end{bmatrix}, \quad C_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_i = \begin{bmatrix} -\dfrac{T_s}{C_i} \\ 0 \end{bmatrix}, \tag{3}$$

2.3. Limitations of traditional observer-based approach

This section discusses the main reason why the traditional observer-based detection approach fails to achieve a reliable detection performance in the presence of modeling uncertainties. Commonly, the principle of the observer-based detection approach is first to construct a residual which is only sensitive to cyber-attacks by making use of the information from measurements and control input. Then the system can be monitored by comparing the real-time residual signals with a predefined threshold. Without considering the modeling errors, the residual responses of observer-based detection approach for DC microgrid system can be formulated as:

$$r_i(k) = G_{ra} a_i(k) + G_{rd} d_i(k) + G_{ru} u_i(k) + G_{ry} y_i(k) \tag{4}$$

where $r(k) \in \mathbb{R}^r$ is the residual; $G_{r\times}$, determined by the structure of observer, are the transfer functions from each input to the residual. To



(a) MG i control system (b) System topology

Fig. 1. DC microgrid control system.

reduce the impact of these inputs, especially the disturbances, on the observer, the residual should be designed to be decoupled from these inputs, which requires:

$$G_{rd} = G_{ru} = G_{ry} = 0 \tag{5}$$

With the designed observer satisfying the requirement (5), the residual will be only affected by the attack signals. Therefore, attack detection can be achieved. Specifically, the transfer function of the observer from disturbances to the residuals can be expressed as:

$$G_{rd} = GE_i \tag{6}$$

where $G \in \mathbb{R}^{r\times m}$ is a nonzero matrix determined by the observer. To make sure the requirement (6) is solvable, the matrix E_i should be full column rank, which asks the number of independent disturbances should be less than the number of system measurements. This condition can be fulfilled without difficulty by e.g. Luenberger-like observer [41] or unknown input observer [42], when there is a limited number of disturbances in the system. However, because the modeling uncertainties are an additive disturbance on the system, there will be an increase in the number of disturbances, which makes it difficult or even impossible to satisfy the requirement (5). Therefore, the traditional observer-based detection approach may fail to achieve a robust cyber-attack detection for the DC microgrids when considering the modeling uncertainties.

2.4. Detector architecture

As discussed above, the limitation of robust cyber-attack detection against model uncertainties is the lack of measurements. Considering the fact that it will increase the cost of the system and sometimes is unfeasible to increase the number of measurements/sensors, the traditional observer-based detection approach may not be implemented in real applications.

Taking this issue into consideration, the parity-based detection approach is proposed in this paper to achieve a robust detection for DC microgrids against both unknown disturbances and modeling uncertainties. The structure of the DC microgrid cluster under consideration and the proposed detection approach are shown in Figs. 1 and 2. Each MG is equipped with a local controller and detector, where the controller is designed to meet the general objectives, i.e. current sharing and voltage regulation. The detector is adopted to monitor the system by exploiting the relation between input and measurements, and can trigger an alarm in the presence of cyber-attacks.

Noticed that mostly the measurement I_j is utilized by the local controller to achieve the power-sharing. While the detector can monitor the system only using the model information and variables appearing in (2) without any information from the neighboring states. Therefore, it can be implemented in a large scale DC microgrid. The design of the controller is omitted as it goes beyond the scope of this article. The detailed design process of the proposed detector is explained in Section 3.

3. Attack detection design

This section describes the design process for a detection method for DC microgrids. The structure of the proposed detection scheme is shown in Fig. 2. For each MG, the proposed detector is composed of residual generation $r_i(k)$ based on parity relations and a proper threshold $\bar{r}_i(k)$. If $r_i(k) > \bar{r}_i(k)$, then an attack is assumed. It will be shown that the proposed attack detection is robust to both unknown disturbances and parameter variations. The subscript ([i]) is omitted for brevity, because it does not influence the discussion of detection design.

3.1. Parity relation of DC microgrid

As pointed, it is not reliable to design an attack detection that is robust against both the unknown disturbances and parameter variations because of the lack of enough measurements. To achieve a perfect robust detection design, the parity relations of the DC MG are studied where the historical measurements of past s steps are kept.

The parity relation of the DC MG system (2) under consideration can be constructed by collecting a collection of data with a window length of s. The simplified parity relation can be obtained as:

$$Y(k) = H_t U(k) + W_t x(k-s) + L_t D(k) + M_{1t} A_1(k) + M_{2t} A_2(k) \tag{7}$$

where $Y(k)$, $U(k)$, $D(k)$, $A_1(k)$ and $A_2(k)$ are a batch of data of $y(k)$, $u(k)$, $d(k)$, $a_1(k)$ and $a_2(k)$. The detailed definition of (7) and H_t, W_t, L_t, M_{1t}, M_{2t} are defined in Appendix. To detect the cyber-attacks, the residual is designed as:

$$r(k) = v^T [Y(k) - HU(k)] \tag{8}$$

where $v^T \in \mathbb{R}^{r\times(s+1)m}$ is the residual generating vector needed to be designed.

As noticed from (8) that the proposed detection scheme can monitor the system with only local measurements and the control input of each MG. The attack detection scheme can be implemented by comparing the residuals with a threshold value. If the residual is above the threshold, an attack is assumed to exist.

3.2. Robust detection design

This section shows how the robust detection of DC microgrid can be achieved based on the parity relation provided in (7). Eq. (8) shows the computational form of the residual as a function of control input and MG measurements. Substituting (7) into (8) yields:

$$\begin{aligned} r(k) = \; & v^T [W_t x(k-s) + (H_t - H)U(k) + L_t D(k) \\ & + M_{1t} A_1(k) + M_{2t} A_2(k)] \\ = \; & v^T Z_t X(k) + v^T M_t A(k) \end{aligned} \tag{9}$$

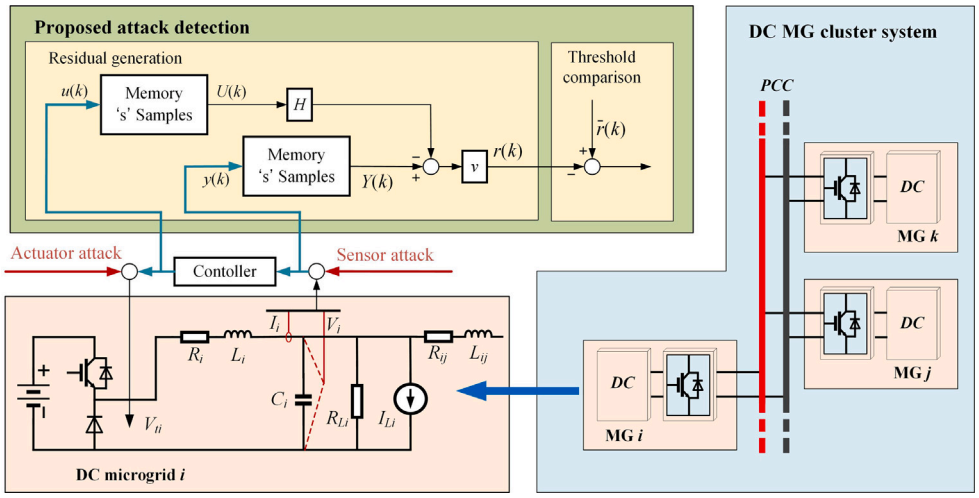


Fig. 2. Proposed parity-based attack detection approach.

where

$$Z_t = \begin{bmatrix} W_t & (H_t - H) & L_t \end{bmatrix} \in \mathbb{R}^{(s+1)m\times[n+(s+1)(u+d)]}$$
$$M_t = \begin{bmatrix} M_{1t} & M_{2t} \end{bmatrix} \in \mathbb{R}^{(s+1)m\times(s+1)(u+m)} \tag{10}$$
$$X(k) = \begin{bmatrix} x(k-s) \\ U(k) \\ D(k) \end{bmatrix} A(k) = \begin{bmatrix} A_1(k) \\ A_2(k) \end{bmatrix}$$

To make the residual only sensitive to cyber-attacks, the residual signal $r(k)$ should be zero when there is no attack and non-zero when there is an attack, which requires:

$$v^T Z_t = 0 \tag{11a}$$
$$v^T M_t \neq 0 \tag{11b}$$

Indeed, the vector v which satisfies requirement (11) can only guarantee the robustness against unknown disturbances, not the parameter variations. There is still a need for a robust detection design against modeling uncertainties.

Before devising a robust detection strategy, it is first assumed that the parameter variations are bounded, i.e., $L - \Delta L \leq L_t \leq L + \Delta L$, $C - \Delta C \leq C_t \leq C + \Delta C$. This is reasonable from a practical perspective because the maximum variations of LC filters are usually around $\pm 10\%$ of their nominal value. Therefore, the parameter variations can be contained within a pre-defined bound. To achieve a realistic design, the matrices set $\{A_t, B_t, C_t, E_t\}$ are extended to a finite set of possibilities, i.e., $\{A_p, B_p, C_p, E_p\}(p = 1, 2, \ldots, P)$ within their bounds. A number of representative parameter values can be chosen to reflect a particular set of parameters. Based on this idea, a corresponding set of matrices Z_p and M_p can be obtained. The design of the detection method therefore becomes a search for a satisfying residual generation vector v satisfying:

$$v^T Z_p = 0; \qquad p = 1, 2, \ldots, P \tag{12a}$$
$$v^T M_p \neq 0; \qquad p = 1, 2, \ldots, P \tag{12b}$$

The above requirements can be rewritten as:

$$v^T Z = 0; \tag{13a}$$
$$v^T M \neq 0; \tag{13b}$$

where

$$Z = [Z_1, Z_2, \ldots, Z_P] \in \mathbb{R}^{(s+1)m\times(s+1)(2u+d)P}$$
$$M = [M_1, M_2, \ldots, M_P] \in \mathbb{R}^{(s+1)m\times(s+1)(u+m)P} \tag{14}$$

It can be obtained that the solution (13a) exists under the condition that.

$$rank(Z) \leq (s+1)m - 1 \tag{15}$$

In fact, this condition cannot be satisfied in general and it is challenging to find an ideal solution provided by a multi-matrix set P, especially in the case of highly variable parameters. In order to implement a robust detection method for this case, the following multi-objective optimization problem is formulated:

$$\min J_1 = \min \left\{ \sum_{p=1}^{P} \|v^T Z_p\| \right\} \tag{16a}$$
$$\max J_2 = \max \left\{ \sum_{p=1}^{P} \|v^T M_p\| \right\} \tag{16b}$$

It is then practical to find the optimal solution to (16), which can be used to generate robust residuals that are insensitive to both unknown disturbances and parameter variations.

3.3. Optimal robust detection design via singular value decomposition approach

This section provides the analytical solution to the optimal robust detection design problem (16) based on a two-stage procedure, where the solution to (16a) is determined first before the searching of the solution to (16b). Before providing an illustration of the design process, the following lemma is provided.

Lemma 1 ([39]). *Let the singular value decomposition of Z be:*

$$Z = \Gamma_Z [diag\{\sigma_1, \sigma_2, \ldots, \sigma_z\}, \ldots, 0] \Phi_Z^T \tag{17}$$

where Γ_Z and Φ_Z are called left and right singular matrices of Z; $\sigma_1 \leq \sigma_2 \leq \cdots \leq \sigma_z$ are singular values of Z. Then, the vector v which minimized J_1 lies in a subspace spanned by matrix $\Gamma_{Z(l)}$. Similarly, the vector v which maximizes J_1 lies in a subspace spanned by matrix $\Gamma_{Z(-l)}$. The matrix $\Gamma_{Z(l)}$ and $\Gamma_{Z(-l)}$ are the first and last l column of matrix Γ_Z.

By Lemma 1, the optimal solution for minimizing J_1 lies in the subspace that is spanned by $\Gamma_{Z_p(l)}$, therefore, the typical solution can be written as:

$$v = \Gamma_{Z_p(l)} v_1 \tag{18}$$

Table 2
Performance indices.

Window length	l	J_1	J_2
$s=0$	$l=1$	1	1
	$l=2$	2	2
$s=1$	$l=1$	0.04×10^{-3}	1.0
	$l=2$	1.30×10^{-3}	2.0
	$l=3$	25.7×10^{-3}	3.0
$s=2$	$l=1$	0.01×10^{-3}	1.0
	$l=2$	0.12×10^{-3}	2.0
	$l=3$	1.00×10^{-3}	3.0
	$l=4$	2.00×10^{-3}	4.0
$s=3$	$l=1$	0.01×10^{-3}	1.0
	$l=2$	0.03×10^{-3}	2.0
	$l=3$	0.29×10^{-3}	3.0
	$l=4$	1.00×10^{-3}	4.0

Table 3
Electrical parameters.

Modules	Parameters	Values
DC microgrid	MG nominal voltage	48 V
	Switching frequency	10 kHz
	Control frequency	10 kHz
DC/DC converter	Inductor resistance	0.1 Ω
	Inductor inductance	1.8 mH
	DC bus capacitance	2.2 mF

where $v_1 \in \mathbb{R}^l$ is an arbitrary nonzero vector. Substitute v_1 into J_2, the problem (16b) becomes:

$$\max J_2 = \max\left\{\sum_{p=1}^{P}\|v_1^T \Gamma_{Z_p(l)}^T M_p\|\right\} \tag{19}$$

Accordingly, the v_1 that maximizes J_2 can be found in the space spanned by the matrix $\Gamma_{\bar{M}(-l)}$ where $\bar{M} = \Gamma_{Z_p(l)}^T M_p$, which finished the robust detection design.

Notice that it is undesirable to solve the problem (16a) and (16b) simultaneously or perform the two-stage design procedure reversely because it is crucial to eliminate the influence of disturbances on the residual than to improve the sensitivity to attacks, which requires a priority of requirement (11a) than (11b).

Furthermore, the performance indices J_1 and J_2 are dependent on the choice of step s and constant l. Table 2 lists the performance indices for different l values and design procedures based on the DC microgrid parameters shown in Table 3. As seen from Table 2 that the robust detection cannot be achieved given only real-time measurements ($s = 0$), because the J_1 and J_2 are always the same. It can also be found that the more the window length, the smaller the J_1, the more robust the detection system is. However, the computational effort of the system also increases. Therefore, there is a tradeoff between the robustness of detection performance and the computational burden of the system.

In addition, the constant l determines the extent of the matrix approximation. Table 2 shows that both the performance indices J_1 and J_2 rise with the increase of l. Considering the fact that the desirable solution to the problem (16) is to minimize J_1 on one hand and maximize J_2 on the other hand, therefore, there is also a tradeoff in the choice of l.

3.4. Threshold calculation

As illustrated, the system's detector can trigger an alarm when the residual is greater than a potential threshold. In order to complete the design of the DC MGs for attack detection, the thresholds need to be appropriately designed. The generation of the threshold can be achieved by considering the residual dynamics (9) in the no-attack condition, denoted as:

$$r(k) = v^T Z_t X(k) \tag{20}$$

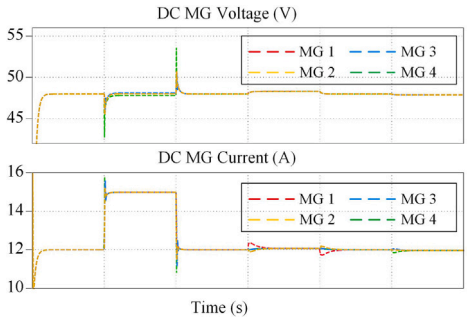


Fig. 3. Microgrid system response.

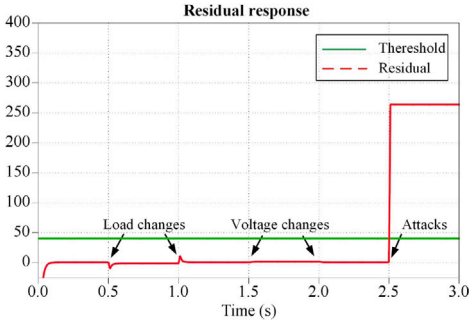


Fig. 4. Residual response.

Therefore, the threshold value $\bar{r}(k)$ can be determined by:

$$\bar{r}(k) = v^T \bar{Z}_t \bar{X}(k) \tag{21}$$

where $\bar{Z}_t$ and $\bar{X}(k)$ are the upper boundaries of Z_t and $X(k)$. Because the Z_t and $X(k)$ are formulated by the electrical parameters and measurements, it is possible to find their boundaries.

4. Performance validation

The proposed parity-based attack detection strategy is tested on a cyber–physical DC microgrid cluster with MGs, as shown in Fig. 1(b). The parameters of each MG and the system are listed in Table 3. First, a sensitivity analysis is provided to investigate the robust detection performance of the proposed strategy against unknown disturbances. Next, the robustness to parameter variations is addressed. Finally, performance validation for each scenario is performed on a dSPACE-based microgrid platform to validate the robustness of the proposed detection strategy. In addition, in order to show the sensitivity of the proposed method, the injected attack signals are selected as only 1% of the nominal values, which are much smaller than the attacks being 12%, 20%, and 22% of their nominal values in [17,20,28] respectively.

4.1. Robustness to unknown disturbances

In this context, the study verifies the robustness of the proposed detection method to load variation conditions and to neighboring voltage variation conditions. In this case, the DC load increases and decreases at 0.5 and 1 s respectively, and the neighboring voltage increases and decreases by 0.5 V at 1.5 and 2 s. A false data injection attack with a value of 0.5 V is launched on the local voltage sensor at 2.5 s. The bus voltage, output current, residuals and corresponding thresholds for converter 1 are shown in Figs. 3 and 4.

As shown, there is an oscillation in the voltage dynamics and a 3 A change in the output current after a shift of load, while the residual dynamics stay at zero. Furthermore, it can be observed that the current fluctuates after a neighboring voltage change, while the

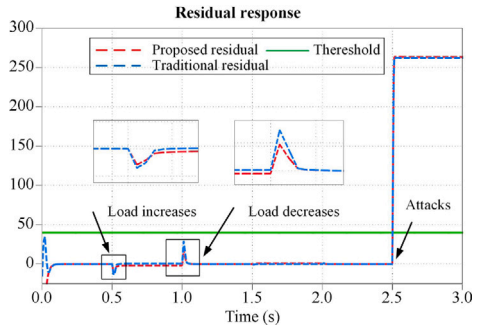


Fig. 5. Detection performance comparison.

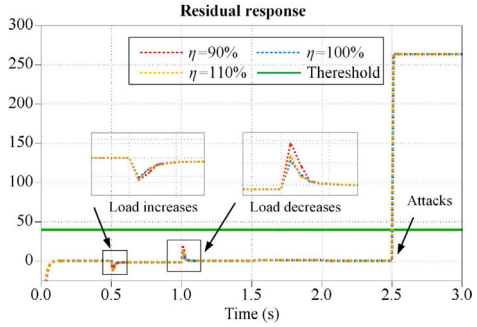


Fig. 6. Detection performance under different parameter variations.

residuals remain constant. However, the residuals increase directly after an attack is injected into the system. It is worth noting that although the oscillations in the voltage and current dynamics caused by the load and neighboring voltage changes are larger than those following a cyber-attack, the residuals are only sensitive to the attack. Therefore, it can be concluded that the detection scheme is decoupled from the unknown disturbance.

4.2. Robustness to parameter variations

In this context, the study verifies the robustness of the proposed detection method to parameter perturbations. Fig. 5 shows the comparison of residual response between the proposed detection approach and traditional approach under different scenarios when the LC parameters are selected as 90% of its nominal value. In the similar way, the load and neighboring voltages varied at 0.5 s, 1 s, 1.5 s and 2 s respectively, and a 0.5 V attack on the voltage sensor is launched at 2.5 s. It can be seen from Fig. 5 that, although the conventional method shows the same detection performance, there is a relatively large spike in the residual response after changing the load compared to the proposed detection method. This suggests that the proposed method has a small risk of false alarms even with varying parameters.

The residual response of the proposed detection approach is further shown in Fig. 6 when the LC filter parameters are selected from 90% to 110% of their nominal value. It can be seen that the response of the residuals at load and neighboring voltage change conditions show little oscillations and no change compared to the residuals after launching a cyber-attack. The test results verify that the parameter change conditions have little impact on the detection scheme.

4.3. Experimental results

Experimental results are given in order to verify the effectiveness of the proposed detection scheme. The control and monitoring scheme was implemented on a dSPACE-based microgrid platform consisting

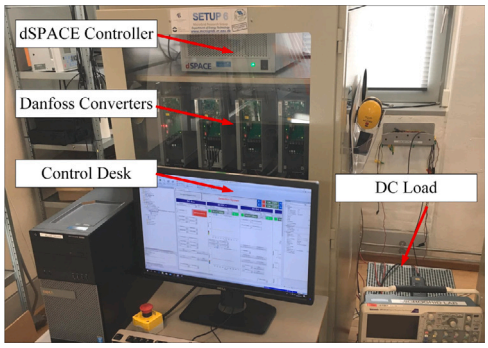


Fig. 7. Experimental setup.

mainly of a dSPACE controller, a DC power supply, four Danfoss converters and a DC load, as shown in Fig. 7. Fig. 8 shows the system response of the microgrid and the residual response of MG 1, when the LC parameter is chosen to a different value. In this case, the load was changed at 5 and 10 s respectively and a 0.5 V cyber-attack was launched on the voltage measurement at 15 s. It can be seen that the residuals remain constant under load variation and parameter change conditions. In addition, the residuals increase rapidly after the injection of attack. Similarly, Fig. 9 shows the microgrid response and residual response under neighboring voltage change conditions. It can be seen that although the effect of the attack on the system dynamics is comparatively smaller than the effect of the disturbance, the residuals increase rapidly. Therefore, it can be concluded that the proposed detection method is robust to load variations, neighboring voltage variations and parameter variation conditions.

5. Conclusion

Parity-based attack detection schemes have been proposed to address the problem of robust detection in DC microgrids. The proposed approach has four benefits: firstly, the proposed detection scheme is able to detect attacks with only local information from the MG system. Therefore, it is easy to be implemented on a large scale microgrid. Secondly, the residuals are decoupled from unknown load conditions and neighboring voltage variations with disturbance decoupling method. Thirdly, the detection is robust to perturbations in the electrical parameters of the DC MG. Fourthly, the proposed detection method can also be applied to the DC microgrid clusters. Simulation tests and experimental results illustrate the achievable performance of the proposed detection strategy.

CRediT authorship contribution statement

Sen Tan: Conceptualization, Methodology, Software, Investigation, Writing – original draft, Writing – review & editing. **Peilin Xie:** Software, Writing – review & editing. **Josep M. Guerrero:** Supervision, Project administration, Funding acquisition. **Juan C. Vasquez:** Supervision, Project administration, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by VILLUM FONDEN, Denmark under the VILLUM Investigator Grant (no. 25920): Center for Research on Microgrids (CROM), www.crom.et.aau.dk.

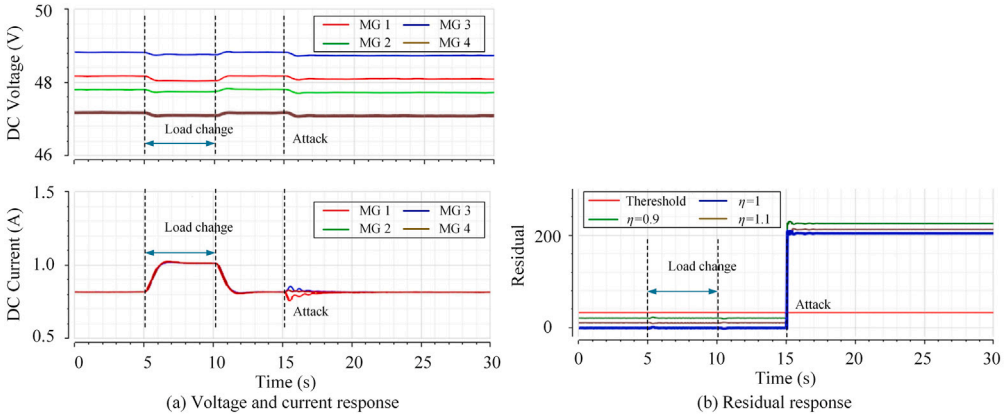


Fig. 8. Microgrid system response under load change conditions.

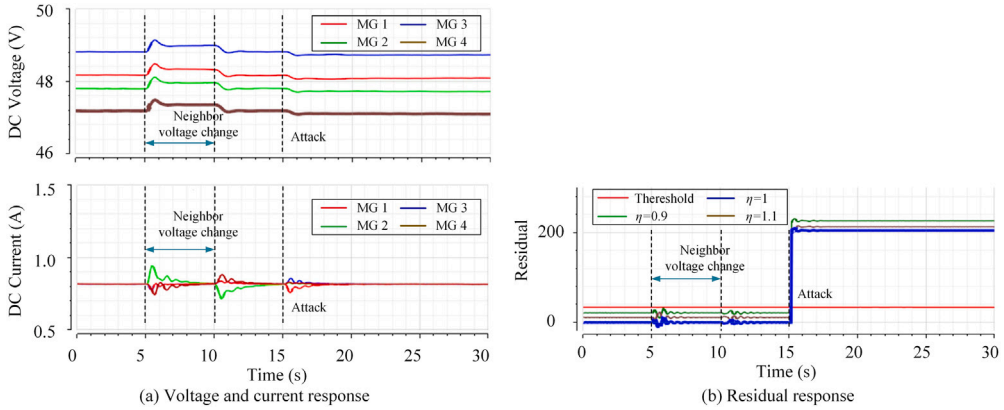


Fig. 9. Microgrid system response under neighbor voltage change conditions.

Appendix

The complex parity relation of the DC MG system (2) is constructed as:

$$\underbrace{\begin{bmatrix} y(k-s) \\ y(k-s+1) \\ \vdots \\ y(k) \end{bmatrix}}_{Y(k)} - H_t \underbrace{\begin{bmatrix} u(k-s) \\ u(k-s+1) \\ \vdots \\ u(k) \end{bmatrix}}_{U(k)} = W_t x(k-s)$$
$$+ L_t \underbrace{\begin{bmatrix} d(k-s) \\ d(k-s+1) \\ \vdots \\ d(k) \end{bmatrix}}_{D(k)} + M_{1t} \underbrace{\begin{bmatrix} a_1(k-s) \\ a_1(k-s+1) \\ \vdots \\ a_1(k) \end{bmatrix}}_{A_1(k)}$$
$$+ M_{2t} \underbrace{\begin{bmatrix} a_2(k-s) \\ a_2(k-s+1) \\ \vdots \\ a_2(k) \end{bmatrix}}_{A_2(k)} \tag{22}$$

where

$$H_t = \begin{bmatrix} 0_{m\times u} & 0_{m\times u} & \cdots & 0_{m\times u} \\ C_t B_t & 0_{m\times u} & \cdots & 0_{m\times u} \\ \vdots & \vdots & \ddots & \vdots \\ C_t A_t^{s-1} B_t & C_t A_t^{s-2} B_t & \cdots & 0_{m\times u} \end{bmatrix}_{(s+1)m\times(s+1)u}$$
$$L_t = \begin{bmatrix} 0_{m\times d} & 0_{m\times d} & \cdots & 0_{m\times d} \\ C_t E_t & 0_{m\times d} & \cdots & 0_{m\times d} \\ \vdots & \vdots & \ddots & \vdots \\ C_t A_t^{s-1} E_t & C_t A_t^{s-2} E_t & \cdots & 0_{m\times d} \end{bmatrix}_{(s+1)m\times(s+1)d}$$
$$W_t = \begin{bmatrix} C_t \\ C_t A_t \\ \vdots \\ C_t A_t^{s} \end{bmatrix}_{(s+1)m\times n}, M_{1t} = H_t \in \mathbb{R}^{(s+1)m\times(s+1)u}$$
$$M_{2t} = \begin{bmatrix} I_m & 0_m & \cdots & 0_m \\ 0_m & I_m & \cdots & 0_m \\ \vdots & \vdots & \ddots & \vdots \\ 0_m & 0_m & \cdots & I_m \end{bmatrix}_{(s+1)m\times(s+1)m} \tag{23}$$

References

[1] Lu S-y, Wang L, Lo T-M, Prokhorov AV. Integration of wind power and wave power generation systems using a DC microgrid. IEEE Trans Ind Appl 2014;51(4):2753–61.

[2] Chub A, Vinnikov D, Liivik E, Jalakas T. Multiphase quasi-z-source DC–DC converters for residential distributed generation systems. IEEE Trans Ind Electron 2018;65(10):8361–71.

[3] Mardani MM, Khooban MH, Masoudian A, Dragičević T. Model predictive control of DC–DC converters to mitigate the effects of pulsed power loads in naval DC microgrids. IEEE Trans Ind Electron 2018;66(7):5676–85.

[4] Villalonga A, Beruvides G, Castaño F, Haber R. Cloud-based industrial cyber-physical system for data-driven reasoning. a review and use case on an industry 4.0 pilot line. Statistics 2020;34:35.

[5] Tan S, Wu Y, Xie P, Guerrero JM, Vasquez JC, Abusorrah A. New challenges in the design of microgrid system. IEEE Electrif Mag 2020;8(4):98–106.

[6] Hug G, Giampapa JA. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans Smart Grid 2012;3(3):1362–70.

[7] Zhao J, Mili L, Wang M. A generalized false data injection attacks against power system nonlinear state estimator and countermeasures. IEEE Trans Power Syst 2018;33(5):4868–77.

[8] Zuo S, Beg OA, Lewis FL, Davoudi A. Resilient networked AC microgrids under unbounded cyber attacks. IEEE Trans Smart Grid 2020;11(5):3785–94.

[9] Liu S, Hu Z, Wang X, Wu L. Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks. IEEE Trans Ind Inf 2018;15(7):4066–75.

[10] Tan S, Xie P, Guerrero JM, Vasquez JC, Han R. Cyberattack detection for converter-based distributed dc microgrids: Observer-based approaches. IEEE Ind Electron Mag 2021;2–12. http://dx.doi.org/10.1109/MIE.2021.3059996.

[11] Farwell JP, Rohozinski R. Stuxnet and the future of cyber war. Survival 2011;53(1):23–40.

[12] Conti JP. The day the samba stopped [power blackouts]. Eng Technol 2010;5(4):46–7.

[13] Case DU. Analysis of the cyber attack on the ukrainian power grid. Electr Inf Shar Anal Cent (E-ISAC) 2016;388.

[14] Lee C-H, Chen B-K, Chen N-M, Liu C-W. Lessons learned from the black-out accident at a nuclear power plant in Taiwan. IEEE Trans Power Deliv 2010;25(4):2726–33.

[15] Peng C, Sun H, Yang M, Wang Y. A survey on security communication and control for smart grids under malicious cyber attacks. IEEE Trans Syst Man Cybern: Syst 2019;49(8):1554–69. http://dx.doi.org/10.1109/TSMC.2018.2884952.

[16] Tan S, Guerrero JM, Xie P, Han R, Vasquez JC. Brief survey on attack detection methods for cyber-physical systems. IEEE Syst J 2020.

[17] Beg OA, Johnson TT, Davoudi A. Detection of false-data injection attacks in cyber-physical DC microgrids. IEEE Trans Ind Inf 2017;13(5):2693–703.

[18] Zhou Q, Shahidehpour M, Alabdulwahab A, Abusorrah A. A cyber-attack resilient distributed control strategy in islanded microgrids. IEEE Trans Smart Grid 2020.

[19] Beg OA, Nguyen LV, Johnson TT, Davoudi A. Signal temporal logic-based attack detection in DC microgrids. IEEE Trans Smart Grid 2018;10(4):3585–95.

[20] Lu L-Y, Liu HJ, Zhu H, Chu C-C. Intrusion detection in distributed frequency control of isolated microgrids. IEEE Trans Smart Grid 2019;10(6):6502–15.

[21] Abhinav S, Modares H, Lewis FL, Ferrese F, Davoudi A. Synchrony in networked microgrids under attacks. IEEE Trans Smart Grid 2017;9(6):6731–41.

[22] Jin D, Li Z, Hannon C, Chen C, Wang J, Shahidehpour M, et al. Toward a cyber resilient and secure microgrid using software-defined networking. IEEE Trans Smart Grid 2017;8(5):2494–504. http://dx.doi.org/10.1109/TSG.2017.2703911.

[23] Liu L, Esmalifalak M, Ding Q, Emesih VA, Han Z. Detecting false data injection attacks on power grid by sparse optimization. IEEE Trans Smart Grid 2014;5(2):612–21.

[24] Chaojun G, Jirutitijaroen P, Motani M. Detecting false data injection attacks in ac state estimation. IEEE Trans Smart Grid 2015;6(5):2476–83.

[25] Ao W, Song Y, Wen C. Adaptive cyber-physical system attack detection and reconstruction with application to power systems. IET Control Theory Appl 2016;10(12):1458–68.

[26] Yan J, Guo F, Wen C. Attack detection and isolation for distributed load shedding algorithm in microgrid systems. IEEE J Emerg Sel Top Ind Electron 2020;1(1):102–10. http://dx.doi.org/10.1109/JESTIE.2020.3004744.

[27] Mustafa A, Poudel B, Bidram A, Modares H. Detection and mitigation of data manipulation attacks in AC microgrids. IEEE Trans Smart Grid 2020;11(3):2588–603. http://dx.doi.org/10.1109/TSG.2019.2958014.

[28] Manandhar K, Cao X, Hu F, Liu Y. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans Control Netw Syst 2014;1(4):370–9.

[29] Abdollah K-F, Su W, Jin T. A machine learning based cyber attack detection model for wireless sensor networks in microgrids. IEEE Trans Ind Inf 2020.

[30] He Y, Mendis GJ, Wei J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. IEEE Trans Smart Grid 2017;8(5):2505–16.

[31] Esmalifalak M, Liu L, Nguyen N, Zheng R, Han Z. Detecting stealthy false data injection using machine learning in smart grid. IEEE Syst J 2014;11(3):1644–52.

[32] Chen W-H, Hsu S-H, Shen H-P. Application of SVM and ANN for intrusion detection. Comput Oper Res 2005;32(10):2617–34.

[33] Habibi MR, Baghaee HR, Dragičevi T, Blaabjerg F, et al. Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. IEEE J Emerg Sel Top Power Electron 2020.

[34] Hamedani K, Liu L, Atat R, Wu J, Yi Y. Reservoir computing meets smart grids: Attack detection using delayed feedback networks. IEEE Trans Ind Inf 2017;14(2):734–43.

[35] Cui S, Han Z, Kar S, Kim TT, Poor HV, Tajer A. Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions. IEEE Signal Process Mag 2012;29(5):106–15.

[36] Pasqualetti F, Dörfler F, Bullo F. Attack detection and identification in cyber-physical systems. IEEE Trans Automat Control 2013;58(11):2715–29.

[37] Davoodi M, Meskin N, Khorasani K. Simultaneous fault detection and consensus control design for a network of multi-agent systems. Automatica 2016;66:185–94.

[38] Tan S, Xie P, Guerrero JM, Vasquez JC, Li Y, Guo X. Attack detection design for dc microgrid using eigenvalue assignment approach. Energy Rep 2021;7:469–76.

[39] Chen J, Patton RJ. Robust model-based fault diagnosis for dynamic systems, Vol. 3. Springer Science & Business Media; 2012.

[40] Han R, Tucci M, Martinelli A, Guerrero JM, Ferrari-Trecate G. Stability analysis of primary plug-and-play and secondary leader-based controllers for DC microgrid clusters. IEEE Trans Power Syst 2018;34(3):1780–800.

[41] Dörfler F, Pasqualetti F, Bullo F. Distributed detection of cyber-physical attacks in power networks: A waveform relaxation approach. In: 2011 49th Annual allerton conference on communication, control, and computing. (Allerton), IEEE; 2011, p. 1486–91.

[42] Teixeira A, Sandberg H, Johansson KH. Networked control systems under cyber attacks with applications to power networks. In: Proceedings of the 2010 American control conference. IEEE; 2010, p. 3690–6.