Attack detection design for dc microgrid using eigenvalue assignment approach

Tan, Sen; Xie, Peilin; Guerrero, Josep M.; Vasquez, Juan C.; Li, Yunlu; Guo, Xifeng

Published in:
Energy Reports

DOI (link to publication from Publisher):
10.1016/j.egyr.2021.01.045

Publication date:
2021

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

Available online at www.sciencedirect.com
ScienceDirect
Energy Reports 7 (2021) 469–476
www.elsevier.com/locate/egyr

2020 The International Conference on Power Engineering (ICPE 2020), December 19–21, 2020, Guangzhou, China

Attack detection design for dc microgrid using eigenvalue assignment approach

Sen Tan[a,*], Peilin Xie[a], Josep M. Guerrero[a], Juan C. Vasquez[a], Yunlu Li[b], Xifeng Guo[c]

[a] *Aalborg University, Aalborg, 9220, Denmark*
[b] *Shenyang University of Technology, Shenyang, 110870, China*
[c] *Shenyang Jianzhu University, Shenyang, 110168, China*

Received 21 January 2021; accepted 24 January 2021

Abstract

DC microgrids (MGs) are complex systems connecting a number of renewable energy sources to different types of loads based on distributed networks. However, the strong reliance on communication networks makes DC MGs vulnerable to intentional cyber-attacks. In this paper, a distributed attack detection scheme is presented for the DC MG system by proposing an observer. The proposed detector is able to detect attacks with only local knowledge of the overall DC microgrid system. By eigenvalue assignment method, the designed residual is decoupled from both load and neighbor voltage changes. Furthermore, an optimization problem is provided to increase the attack detectability of the proposed observer. The presented method is easy to design with less computation complexity. The performances of the proposed scheme are validated by numerical simulations and experiments.

Peer-review under responsibility of the scientific committee of the International Conference on Power Engineering, ICPE, 2020.

Keywords: Attack detection; Cyber-attacks; Distributed DC microgrids; Observer; Residual

1. Introduction

Nowadays, with the growing penetration of renewable sources into modern electric systems, MGs have dominated the electrical grid in recent years [1–4]. They offer the possibility of transmitting renewable sources to different sorts of loads. Applications of DC MGs can be found in electrical vehicles and smart houses [5]. However, the strong dependence on communication networks may expose MGs to cyber-attacks [6]. For systems without enough security protection strategies, attacks may induce damage to power supplies and thus leads to significant societal losses [7].

* Corresponding author.
E-mail address: sta@et.aau.dk (S. Tan).

https://doi.org/10.1016/j.egyr.2021.01.045

Peer-review under responsibility of the scientific committee of the International Conference on Power Engineering, ICPE, 2020.

Taking the cyber-security issues into consideration, the design and analysis of attack detection schemes for microgrid have been recognized more and more attractive [8–14]. A general approach for detection problems is state estimation method analyzing the MG model and the measurements [8,9]. However, this method may fail when detecting some intelligent attacks. To overcome this limit, observer-based method is introduced to address the attack detection problems. Furthermore, χ^2 detector is another approach to detect random attacks by capturing the statistical behaviors of states [11]. However, it needs extra improvement in the case where the distribution of attack is unchanged. Moreover, deep learning approaches have also been introduced for detecting attacks [12,13] These solutions generally rely on machine learning mechanisms to infer a model for the system under inspection directly from data. However, it may introduce a heavy computational burden to train a fully connected network [14].

Although remarkable progress has been made in detecting attacks during the past decade, most of the studies mainly focus on centralized architectures. Indeed, those approaches are not sufficient to deal with attacks in distributed DC MG systems due to the physical interactions among distributed generation units (DGUs) of DC MG. Therefore, it is significant to develop an effective distributed attack detection approach for DC microgrid systems. Recently, a group of distributed attack detection schemes have been proposed in terms of different ways to deal with the coupling effect of the system [15–18]. In [15] and [16], a model decomposition method was provided to achieve a distributed attack detection based on the system Laplacian matrix. However, it requires a great computational complexity in the decomposition progress and thus is undesirable in the implementation of large scale systems. Furthermore, a discrete iteration method was proposed in [17] for a distributed power system. The limitation of this approach is the need to synchronize the time communication between neighboring units.

To cope with the above challenges, an attack detection scheme for distributed DC microgrids is proposed. The main contributions are as follows: First, a real-time cyber-attack detection strategy is provided using Luenberger-Like observer (LLO). The proposed detection scheme can achieve a reliable attack detection with only local knowledge of the system. Second, the presented attack detection scheme is robust against the unknown load changes and coupling effect from neighboring units. Third, the sensitivity to attacks is improved by an optimal design of free parameters.

2. Problem formulation

2.1. Electrical model of DC microgrids

Fig. 1 shows the electrical structure of a distributed generation unit composed of a Buck converter, connecting different DC voltage sources to a variety of loads. A DC MG can be obtained by interconnecting N distributed generation units interconnected through power lines. Therefore, the corresponding model of DGU i is given by:

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

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

2.2. System model

Consider a DGU with an attack on the communication line between measurements and controllers. The model of DGU i can be described in state space as:

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

where $x_{[i]}(t) = [V_i, I_i]^T \in \mathbb{R}^n$ is 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; $d_{[i]}(t) = \sum_{j\in N_i}(V_j - V_i)/R_{ij} - (V_i/R_{Li} + I_{Li}) \in \mathbb{R}^d$ is the unknown disturbance, which is

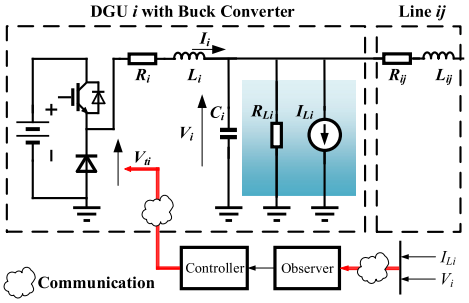

Fig. 1. Electrical structure of DGU i.

the combination of coupling effect (neighbor voltage) and load conditions; $a_{[i]}(t) \in \mathbb{R}^a$ is the attack signal. The matrices of (2) are defined as:

$$A_i = \begin{bmatrix} 0 & \frac{1}{C_i} \\ -\frac{1}{L_i} & -\frac{R_i}{L_i} \end{bmatrix}, B_i = \begin{bmatrix} 0 \\ \frac{1}{L_i} \end{bmatrix}, E_i = \begin{bmatrix} -\frac{1}{C_i} & 0 \\ 0 & 0 \end{bmatrix}, C_i = R_{1i} = R_{2i} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

2.3. Observer model

In order to detect the cyber-attacks, a Luenberger-like observer shown in Fig. 2 is adopted to monitor the system states. For system (2), the observer of DGU i under consideration is described by:

$$\begin{cases} \dot{\hat{x}}_{[i]}(t) = A_i \hat{x}_{[i]}(t) + B_i u_{[i]}(t) + K_i(y_{[i]}(t) - \hat{y}_{[i]}(t)) \\ \hat{y}_{[i]}(t) = C_i \hat{x}_{[i]}(t) \\ r_{[i]}(t) = Q_i[y_{[i]}(t) - \hat{y}_{[i]}(t)] \end{cases} \tag{3}$$

where $\hat{x}_{[i]}(t)$ is the estimated state; $r_{[i]}(t) \in \mathbb{R}^p$ is the residual, $p = m - rank(C_i E_i)$; K_i and Q_i are matrices to be designed. The Laplace transformed residual response to attacks and disturbances can be obtained from (3) as:

$$r_{[i]}(s) = G_{ra[i]}(s) a_{[i]}(s) + G_{rd[i]}(s) d_{[i]}(s) \tag{4}$$

where

$$\begin{cases} G_{ra[i]} = Q_i R_{2i} + Q_i C_i (sI - A_i + K_i C_i)^{-1}(R_{1i} - K_i R_{2i}) \\ G_{rd[i]} = Q_i C_i (sI - A_i + K_i C_i)^{-1} E_i \end{cases} \tag{5}$$

As noticed from (3) that the proposed observer can monitor the system with only local measurements of each DGU.

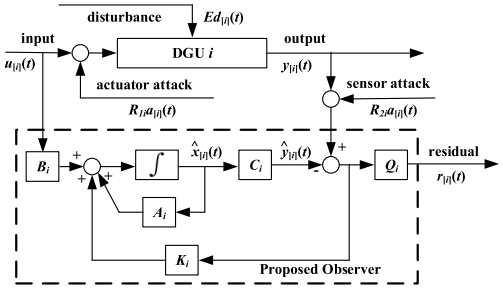

Fig. 2. Proposed observer.

3. Proposed attack detection scheme

It can be seen from (4) that, due to the existence of exogenous disturbances, the residual is not zero in the absence of attack. The unknown load conditions and coupling effects are the sources of false and missed alarms.

3.1. Observer design

In order to make residual signals only sensitive to attacks and decoupled from disturbances, it is necessary to null the transfer function from disturbances to residual, which means:

$$G_{rd[i]} = 0 \tag{6}$$

Therefore, the designing problem is to find the proper matrices K_i and Q_i such that (6) is satisfied and $A_i - K_i C_i$ is stable. Inspired by left eigenvalue assignment approach [19], the sufficient conditions for satisfying the disturbance decoupling requirement are:

Requirement 1. $Q_i C_i E_i = 0$.

Requirement 2. All rows of the matrix $H_i = Q_i C_i$ are p left eigenvectors of $A_i - K_i C_i$ corresponding to any eigenvalues. Considering the DC MG system (2), a solution for Requirement 1 is given by:

$$Q_i = I - C_i E_i [(C_i E_i)^T (C_i E_i)]^{-1} (C_i E_i)^T \tag{7}$$

In order to satisfy Requirement 2, the matrix K_i can be designed by decomposing as follows:

$$K_i = L_i^{-1} W_i = \begin{bmatrix} w_{i1}^T C_i (A_i - \lambda_{i1} I_n)^{-1} \\ \vdots \\ w_{in}^T C_i (A_i - \lambda_{in} I_n)^{-1} \end{bmatrix}^{-1} \begin{bmatrix} w_{i1} \\ \vdots \\ w_{in} \end{bmatrix} \tag{8}$$

where $W_i \in \mathbb{R}^{n \times m}$, $L_i \in \mathbb{R}^{n \times n}$ satisfying H_i be the first p rows of matrix L_i.

Thanks to (8), the design of matrix K_i turns into the design of eigenvalues $\lambda_i = \{\lambda_{ij} | \lambda_{ij} < 0, j = 1, 2, \ldots, n\}$ and W_i, whose elements can be arbitrarily chosen from any real values.

3.2. Optimization of free eigenvalues and parameters

The design problem of matrix K_i only places restriction on the choice of first p eigenvalues of observer. Therefore, there is extra design freedom that the remaining $(n - p)$ eigenvalues can be chosen to increase attack detectability.

Generally, the steady-state residual is the most important factor for detecting attacks, which can be selected as the evaluation index of attack detectability. Combining (4), (5) and (8), the design problem is expressed as:

$$\begin{aligned} \mathcal{O}: \quad & \max_{\lambda_i, W_i} \quad \| Q_i R_{2i} + Q_i C_i (K_i C_i - A_i)^{-1} (R_{1i} - K_i R_{2i}) \| \\ & s.t. \quad \begin{cases} L_{i(p)} = H_i \\ \lambda_{ij} < 0 \end{cases} \end{aligned} \tag{9}$$

where $L_{i(p)}$ denotes the first p rows of matrix L_i. The solution to problem (9) allows for the observer of distributed DC microgrid, which can be solved by any suitable numerical search methods.

4. Applications and results

Simulation and experimental results are given to verify the effectiveness and robustness of the proposed detection scheme. The topology of DC MG tested in this paper is shown in Fig. 3. The nominal voltage for the DC MG is 48 V. The parameters of each DGU and the MG system are listed in Table 1.

The control function is designed based on the standard hierarchical structure in [20]. In the following, the performance capabilities of proposed distributed detection are demonstrated through two cases. In the first case, constant injection attacks are launched to the measurements and control outputs on the corresponding communication links. In the second case, loads and neighbor voltage of a DGU are changed before launching an attack.

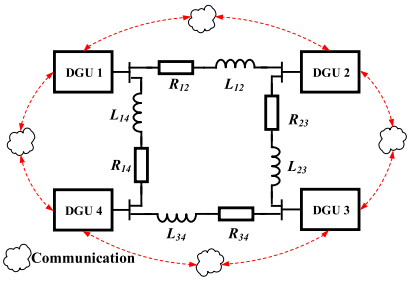

Fig. 3. Topology structure of DC microgrid.

Table 1. Electrical parameters.

Modules	Parameters	Symbol	Values
DC microgrid	DC bus voltage	V_d	150 V
	MG nominal voltage	V_i^*	48 V
	Switching frequency	f_{sw}	10 kHz
	Control period	T_s	10 ms
DC/DC converter	Inductor resistance	R_i	0.1 Ω
	Inductor inductance	L_i	1.8 mH
	DC bus capacitance	C_i	2.2 mF
	DC load	R_{Li}	4 Ω
Lines	Line resistance	R_{12}	0.05 Ω
	Line resistance	R_{14}	0.05 Ω
	Line resistance	R_{23}	0.03 Ω
	Line resistance	R_{24}	0.07 Ω

4.1. Sensitivity to attacks

Studies in this section illustrate the performance of the residual with attacks in different communication channels. In this case, three tests have been carried out, where the false data are injected into the voltage command, PCC bus voltage and filter current channels of DGU 1, respectively. In each test, the attacks are only injected into one specific channel. In order to show the sensitivity of residual to the attacks, the attack vectors are selected as 1% of the nominal values of corresponding channels. Assuming that the attacks are launched at 6 s, the bus voltages, output currents, residuals and corresponding thresholds under different attack conditions are presented in Figs. 4–6.

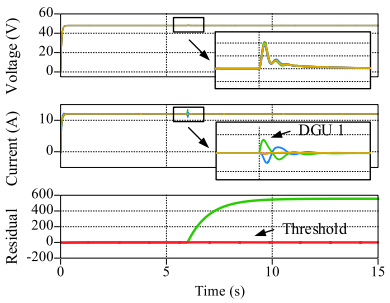

Fig. 4. Attack in command channel.

It can be seen that the cyber-attacks can either deteriorate system dynamics (Figs. 4 and 5) or make the system unstable (Fig. 6), depends on different channels the attacks are launched. The test results show that the attacks are promptly detected by the increased residuals. In addition, although the residual of the system under current channel attacks is smaller than ones under command and voltage channel attacks, it is still larger than the threshold signal, which verifies that the designed observer is sensitive to the attacks.

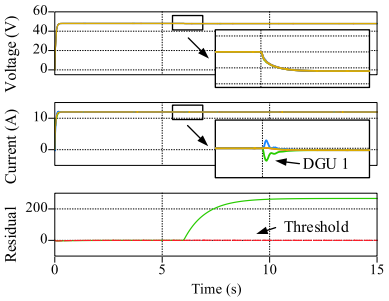

Fig. 5. Attack in voltage channel.

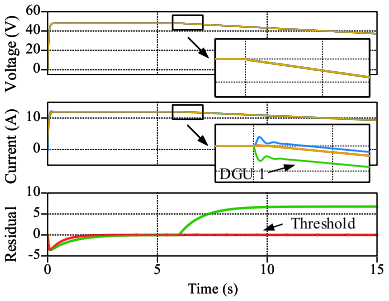

Fig. 6. Attack in current channel.

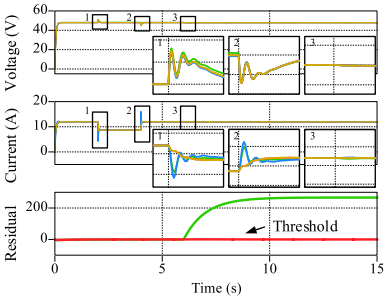

Fig. 7. Load changes.

4.2. Robustness to disturbances

Studies in this section illustrate the robustness of proposed observer to the load and neighbor voltage change conditions. In this case, the load and neighbor voltage are changed respectively at 2 s and 4 s to alter the system operation point before launching the attacks. In each test, the attack vectors are injected to the PCC bus voltage channel, where 1% of the nominal values are selected. The time of starting the attacks is 6 s. Figs. 7 and 8 shows the bus voltages, output currents, residuals and corresponding thresholds for the second case.

As shown in Fig. 7, there are 3 V overshoots in voltage dynamics and 4 A changes in output current after the shifting of load at 2 s and 4 s, while the residual remains zero dynamic. In addition to that, although the changes to the voltage and current dynamics (0.12 V, 0.03 A) under attacks are smaller than that under load change conditions, the residual increases rapidly. Moreover, it can be seen from Fig. 8 that there is no false alarm when the voltage changes for 0.25 V after 2 s and 4 s. While, the residual increases after 6 s when there is a 0.03 V attack in the voltage measurement channel. Therefore, it can be concluded that the distributed observer is totally decoupled from the unknown disturbances.

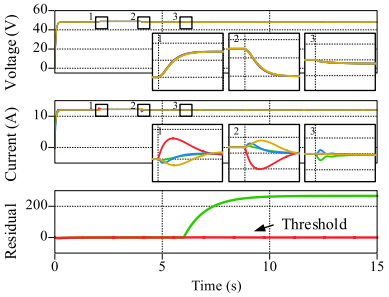

Fig. 8. Neighbor voltage changes.

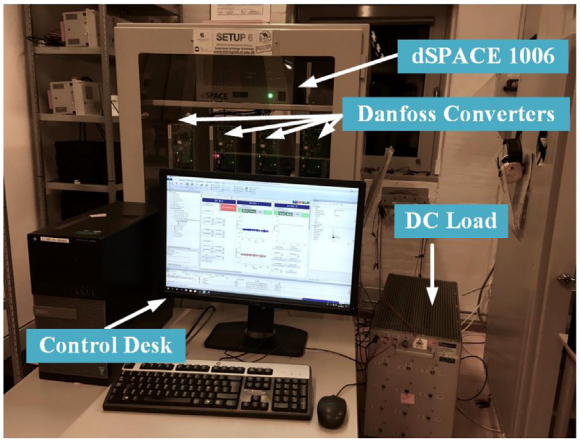

Fig. 9. Experimental results.

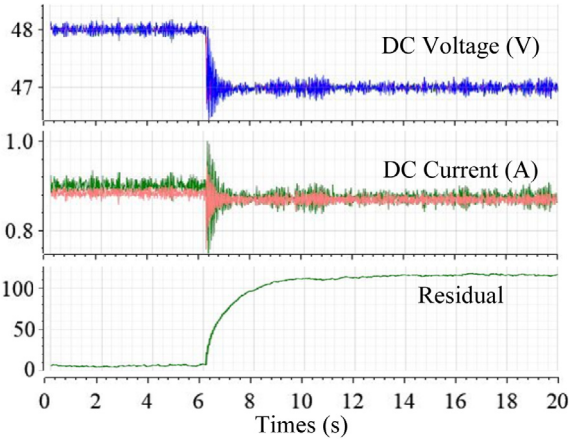

Fig. 10. Experimental results.

4.3. Experimental results

The proposed attack detection scheme is implemented and tested in an experimental DC MG setup operated in an islanded mode shown in Fig. 9. The topology of the setup is given in Fig. 3. The load is set as $R_{Li} = 57\ \Omega$. The experimental result shown in Fig. 10 is matching with the simulation in Fig. 5. It can be seen that the attack

is quickly detected by the residual. This illustrated that the proposed approach can successfully be used for attack detection in the distributed DC MG system.

5. Conclusion

A model-based attack detection scheme has been presented to detect cyber-attacks in the distributed DC microgrid system. The benefits of the proposed approach are threefold: first, the distributed observer is able to detect attacks with only local information of MG system. Second, with left eigenvalue assignment technology, the residual is decoupled from unknown load conditions and neighbor voltage changes. Third, the detectability is improved by an optimization-based designing process. Simulation and experimental tests are presented to illustrate the effectiveness and achievable performance of proposed scheme.

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.

Acknowledgment

This work was supported by VILLUM FONDEN, Center for Research on Microgrids, Aalborg University, Denmark, under the VILLUM Investigator Grant 25920.

References

[1] J.M. Guerrero, J.C. Vasquez, J. Matas, L.G. De Vicuña, M. Castilla, Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization, IEEE Trans Ind Electron 58 (2010) 158–172.
[2] G. Xiaoqiang, W. Baoze, J. Xiaoyu, et al., Common mode current suppression for FB10 threephase non-isolated PV grid-connected inverter, Trans China Electrotech Soc 30 (2015) 135–142.
[3] B. Wei, J.C. Vásquez, J.M. Guerrero, X. Guo, Control architecture for paralleled current-source-inverter (CSI) based uninterruptible power systems (UPS). In: 2016 IEEE 8th int. power electron. motion control conf. 2016. p. 151–6.
[4] B. Wei, A. Marzàbal, J. Perez, R. Pinyol, J.M. Guerrero, J.C. Vásquez, Overload and short-circuit protection strategy for voltage source inverter-based UPS, IEEE Trans Power Electron 34 (2019) 11371–11382.
[5] L. Meng, Q. Shafiee, G.F. Trecate, H. Karimi, D. Fulwani, X. Lu, J.M. Guerrero, Review on control of DC microgrids and multiple microgrid clusters, IEEE J Emerg Sel Top Power Electron 5 (2017) 928–948.
[6] S. Tan, Y. Wu, P. Xie, J.M. Guerrero, J.C. Vásquez, Abdullah Abusorrah, New challenges in the design of microgrid systems, IEEE Electr Mag 8 (2020) 98–106.
[7] S. Tan, J.M. Guerrero, P. Xie, R. Han, J.C. Vasquez, Brief survey on attack detection methods for cyber-physical systems, IEEE Syst J (2020).
[8] Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Trans Inf Syst Secur 14 (2011) 1–33.
[9] Y. Huang, J. Tang, Y. Cheng, H. Li, K.A. Campbell, Z. Han, Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis, IEEE Syst J 10 (2014) 532–543.
[10] F. Pasqualetti, F. Dörfler, F. Bullo, Attack detection and identification in cyber-physical systems, IEEE Trans Automat Control 58 (2013) 2715–2729.
[11] K. Manandhar, X. Cao, F. Hu, Y. Liu, Detection of faults and attacks including false data injection attack in smart grid using Kalman filter, IEEE Trans Control Netw Syst 1 (2014) 370–379.
[12] W.-H. Chen, S.-H. Hsu, H.-P. Shen, Application of SVM and ANN for intrusion detection, Comput Oper Res 32 (2005) 2617–2634.
[13] Y. He, G.J. Mendis, J. Wei, Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism, IEEE Trans Smart Grid 8 (2017) 2505–2516.
[14] K. Hamedani, L. Liu, R. Atat, J. Wu, Y. Yi, Reservoir computing meets smart grids: Attack detection using delayed feedback networks, IEEE Trans Ind Inf 14 (2017) 734–743.
[15] M. Davoodi, N. Meskin, K. Khorasani, Simultaneous fault detection and consensus control design for a network of multi-agent systems, Automatica 66 (2016) 185–194.
[16] P.P. Menon, C. Edwards, Robust fault estimation using relative information in linear multi-agent networks, IEEE Trans Automat Control 59 (2013) 477–482.
[17] F. Pasqualetti, F. Dörfler, F. Bullo, Attack detection and identification in cyber-physical systems–Part II: Centralized and distributed monitor design, 2012, ArXiv Prepr. ArXiv:1202.6049.
[18] I. Shames, A.M.H. Teixeira, H. Sandberg, K.H. Johansson, Distributed fault detection for interconnected second-order systems, Automatica 47 (2011) 2757–2764.
[19] J. Chen, R.J. Patton, Robust model-based fault diagnosis for dynamic systems, Springer Science & Business Media, 2012.
[20] R. Han, H. Wang, Z. Jin, L. Meng, J.M. Guerrero, Compromised controller design for current sharing and voltage regulation in DC microgrid, IEEE Trans Power Electron 34 (2018) 8045–8061.