Aalborg Universitet

AALBORG UNIVERSITY
DENMARK

Attack-resilient control for converter-based DC microgrids

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

Published in:
Global Energy Interconnection

DOI (link to publication from Publisher):
10.1016/j.gloei.2023.11.008

Creative Commons License
CC BY-NC-ND 4.0

Publication date:
2023

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

Link to publication from Aalborg University

Citation for published version (APA):
Tan, S., Vasquez, J. C., & Guerrero, J. M. (2023). Attack-resilient control for converter-based DC microgrids. *Global Energy Interconnection*, *6*(6), 751-757. https://doi.org/10.1016/j.gloei.2023.11.008

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: April 29, 2024

Global Energy Interconnection
Development and Cooperation Organization

ELSEVIER
Production And Hosting By Elsevier On Behalf Of KeAi
KeAi

Volume 6 Number 6 December 2023 (751-757)
DOI: 10.1016/j.gloei.2023.12.008

Global Energy Interconnection

Contents lists available at ScienceDirect
https: //www.sciencedirect.com/journal/global-energy-interconnection

Full-length article

Attack-resilient control for converter-based DC microgrids

Sen Tan[1], Juan C. Vasquez[1], Josep M. Guerrero[1]
1. Aalborg University, Fredrik Bajers Vej 7K, Aalborg, 9220, Denmark

Scan for more details

Abstract: In light of the growing integration of renewable energy sources in power systems, the adoption of DC microgrids has become increasingly popular, due to its simple structure, having no frequency, power factor concerns. However, the dependence of DC microgrids on cyber-networks also makes them susceptible to cyber-attacks. Potential cyber-attacks can disrupt power system facilities and result in significant economic and loss of life. To address this concern, this paper presents an attack-resilient control strategy for microgrids to ensure voltage regulation and power sharing with stable operation under cyber-attack on the actuators. This paper first formulates the cyber-security problem considering a distributed generation based microgrid using the converter model, after which an attack-resilient control is proposed to eliminate the actuator attack impact on the system. Steady state analysis and root locus validation illustrate the feasibility of the proposed method. The effectiveness of the proposed control scheme is demonstrated through simulation results.

Keywords: Cyber-attacks; DC microgrids; Resilient control

0 Introduction

It becomes increasingly prominent to use DC microgrids (MGs) in the power system landscape, driven by the widespread adoption of renewable energy sources (RESs), energy storage systems (ESSs), and DC loads [1]. Their significance is further amplified by advancements in information technology and control methods. DC microgrids offer inherent advantages such as scalability, reliability, and resiliency, making them a crucial component of modern power systems [2].

As microgrid systems become more prevalent, the increased connectivity and communication among distributed generation units, controllers, and sensors present a challenge in terms of cyber-security. The interconnections within the microgrid system make it susceptible to malicious cyber-attacks on communication links. This vulnerability to cyber-threats highlights the need for robust cybersecurity measures to ensure the integrity, confidentiality, and availability of the microgrid system and its components [3].

The control strategies implemented in microgrids heavily rely on accurate measurements obtained from sensors to effectively regulate voltage, control frequency, optimize power sharing, and manage economic dispatch [4]. However, the integrity and reliability of these measurements can be compromised by malicious cyber-attacks. The controller's capacity to guarantee the performance of the DC microgrid is compromised when the integrity of the sampled data is tampered with [5]. As a result, the overall operational efficiency and reliability of the system are significantly impacted [6]. Furthermore, a cyber-attack could potentially compromise the integrity of the microgrid system, enabling

Received: 7 June 2023/Received: 19 September 2023/Accepted: 20 October 2023/Published: 25 December 2023

✉ Sen Tan
sta@energy.aau.dk

Juan C. Vasquez
juq@energy.aau.dk

Josep M. Guerrero
joz@energy.aau.dk

2096-5117/© 2023 Global Energy Interconnection Development and Cooperation Organization. Production and hosting by Elsevier B.V. on behalf of KeAi Communications Co., Ltd. This is an open access article under the CC BY-NC-ND license (http: //creativecommons.org/licenses/by-nc-nd/4.0/).

unauthorized access to manipulate controller commands. This can lead to system malfunctions, physical damage, and result in significant economic and social losses [7]. Therefore, it is imperative to establish robust cybersecurity measures to protect microgrid systems from such cyber threats and ensure their reliable and secure operation [8].

1 State of the art

To address the cyber-security challenges in DC microgrids, the development of attack detection and resilience enhancement techniques has emerged as a key solution. These techniques aim to detect and mitigate cyber-attacks to ensure the reliable and secure operation of microgrids. Attack detection strategies can be categorized as cyber-layer detection and physical layer detection [9].

A common approach in the cyber layer is the use of data authentication or key-management techniques that rely on external information to characterize secure signals and identify potential malicious attacks [10]. Various protocols or low-cost hardware can be employed to analyze the data and determine whether they exhibit the expected characteristics of secure signals. Any data that do not satisfy the relevant characteristics are considered suspicious and indicative of a possible attack. However, this approach has some limitations. The use of third-party detection methods introduces additional computational processing that can increase the complexity and overhead of the system. Furthermore, it may introduce latency during data communication, potentially affecting the real-time responsiveness of the MG system. These factors need to be carefully considered and balanced when implementing attack detection strategies in the cyber-layer of DC microgrids [11].

Cyber-attack detection in the physical layer of DC microgrids can be categorized into three primary methods: data-based detection, feature-based detection and model-based detection [12-14]. Despite notable advancements in cyber-attack detection within DC microgrids, it remains true that existing methods do not offer comprehensive countermeasures capable of effectively suppressing or eliminating the impact of such attacks. Detection alone is not sufficient to ensure the security and resilience of microgrid systems in the face of sophisticated cyber threats. Therefore, the development of effective countermeasures is crucial to mitigate the potential consequences of cyber-attacks.

Three commonly employed methods are widely utilized to mitigate the impact of cyber-attacks on microgrid systems. First, a simple way to prevent the spread of cyber-attacks into the system is to remove the connections to the corrupted units once an attack is detected [15-17]. However, by disconnecting the affected units, the consensus control mechanism may be disrupted, which can result in a degradation of power sharing among the remaining units. To address the disruption caused by isolating compromised units, various attack mitigation methods have been developed, focusing on secure state estimation and attack estimation approaches using Kalman filter [18] or observer [19]. These methods aim to reconstruct reliable signals to replace the untrustworthy ones transmitted through compromised communication links.

1.1 Objectives and contributions

Based on the above discussions, it can be summarized that the current prevalent methods to cope with cyber-attacks are either by removing the attacked units or by state reconstruction to correct the tampered data. Moreover, it is also a significant approach to address cyber-attacks from a controller design perspective, which allows the development of a self-healing elimination strategy to maximize the resilience of the system without losing the physical connection among DC microgrids.

To ensure the continuous operation of microgrids in the presence of cyberattacks, the adoption of resilient control strategies has become increasingly important. Resilient control involves the use of adaptive controllers that are specifically designed to achieve various control objectives, such as consensus among distributed components and system stability [20, 21]. These adaptive controllers have the unique ability to dynamically adjust their parameters and behaviors in response to evolving cyber threats. For example, in [22], a novel approach is introduced, utilizing an adaptive controller and a distributed observer to maintain the tracking error within a boundary. Furthermore, ref [23] presents a strategy for distributed resilient control that involves the integration of a virtual microgrid model, enhancing the robust frequency synchronization within the microgrid.

Therefore, this paper introduces a new resilient control approach aimed at ensuring dependable control of DC microgrids in the face of actuator attacks.

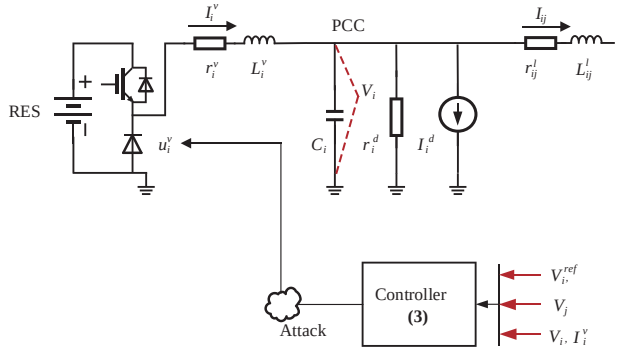
1.2 Paper organization

The outline of the paper is as follows. In Section 2, the electrical model of a DC microgrid are described. In section 3, the proposed resilient control is constructed for DC microgrids, followed by the illustration of steady-state analysis. The simulation results are provided in Section 4, and the conclusions are presented in the final section.

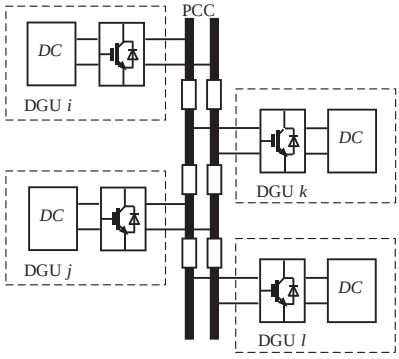
2 DC Microgrid

2.1 Microgrid modelling

The microgrid considered in this paper is composed of multiple distributed generation units (DGU). Fig. 1 illustrates the connection of each generation unit at the point of common coupling (PCC). A constant impedance load and constant current load is considered at each PCC bus.



(a) Electrical scheme of a single DGU



(b) Connections of the DGU

Fig. 1 Electrical scheme of an MG

The model of converter i can be represented in Eq. (1):

$$\begin{cases} C_i\dot{V}_i = I_i^v + -\dfrac{V_i}{r_i^d} - I_i^d - \sum \beta_{ij} I_{ij} \\ L_i^v \dot{I}_i^v = u_i^v - V_i - r_i^v I_i^v \\ L_{ij}^l \dot{I}_{ij} = -r_{ij}^l I_{ij} + \beta_{ij}(V_i - V_j) \end{cases} \tag{1}$$

where V_i is the i-th PCC bus voltage. For the grid forming converter, I_i^v and u_i^v are the filter current and control input; r_i^v and L_i^v represent the resistance and inductance of the converter. C_i denotes PCC bus capacitor. Moreover, I_{ij} is the line current flowing between converter i and j; r_{ij}^l and L_{ij}^l are the line resistance and inductance. β is the incidence matrix of DC MG graph, whose elements β_{ij} shows the direction of the line current I_{ij}. $\beta_{ij} = 1$ or $\beta_{ij} = -1$ when the line current flows from or into MG i; otherwise, $\beta_{ij} = 0$.

2.2 Resilient control problem

The attack on the microgrid will have a pronounced impact on the voltage and current tracking dynamics. According to [24], the consensus tracking errors with attacks on microgrid can be described as:

$$\dot{e}(t) = (L + G)e(t) + F(t) \tag{2}$$

where $e(t)$ is the state errors, L is Laplacian matrix; G denotes the secondary controller parameters; $F(t)$ is the impact of attacks. It can be seen that the consensus can no longer be achieved in the existence of attacks.

3 Attack Resilient Control for DC Microgrid

To eliminate the impact of cyber-attacks on the performances of system, the attack resilient control is formulated in this section.

3.1 Resilient control

The resilient control protocols are proposed to enable voltage regulation and power sharing in the presence of actuator attacks shown as:

$$\begin{aligned} u_i^v = {} & m_{1,i}V_i + m_{2,i}\sum_{j\in\mathcal{N}_i}(V_j - V_i) \\ & + \int m_{3,i}(V_i^{ref} - V_i) + m_{4,i}\sum_{j\in\mathcal{N}_i}(V_j - V_i) \end{aligned} \tag{3}$$

where $m_{1,i},\cdots,m_{4,i}$ denote the controller coefficients; u_i^v is the controller output that represents the voltage reference command; V_i^{ref} are the voltage and current reference. Fig. 2 depicts the structure of the proposed control scheme.

The dynamics of a cyber-physical DC microgrid under actuator attack can be described by combining the model (1) and the proposed controller (2) as:

$$\begin{cases} [C]\dot{\mathbf{V}} = \mathbf{I}^v - [r^d]^{-1}\mathbf{V} - \mathbf{I}^d - \beta\mathbf{I}_l \\ [L^v]\dot{\mathbf{I}}^v = ([m_1] - \mathbf{I}_n)\mathbf{V} - [r^v]\mathbf{I}^v + \mathbf{z}^v - [m_2]\mathcal{L}\mathbf{V} + \mathbf{F}^v \\ \dot{\mathbf{z}}^v = [m_3]\mathbf{V}^{ref} - [m_3]\mathbf{V} - [m_4]\mathcal{L}\mathbf{V} \end{cases} \tag{4}$$

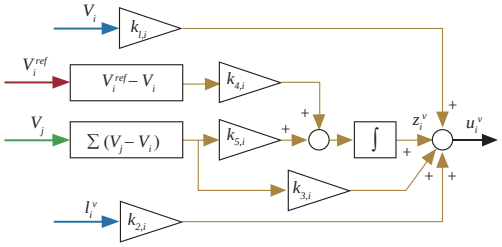


Fig. 2 Structure of proposed resilient controller

where $\mathbf{V} = [V_1, V_2, \cdots, V_n]^T$ and $\mathbf{I}^v = [I_1^v, I_2^v, \cdots, I_n^v]^T$ are the

PCC bus voltage and filter current of the DC, respectively, $\mathbf{I}^d$ is the current load, $\mathbf{I}^l$ is the line current, $\mathbf{F}^v$ is the actuator attack vector, and $\mathbf{z}^v$ is the controller state.

3.2 Steady-state analysis

Given the MG (1), the equilibrium point $\overline{x}$ in (4) without actuator attacks can be described as by making state variables equal to zero:

$$\overline{x} = \left[\overline{\mathbf{V}}^T, [\overline{\mathbf{I}}^v]^T, [\overline{\mathbf{z}}^v]^T, [\overline{\mathbf{I}}^l]^T\right]^T \tag{5}$$

where

$$\overline{\mathbf{V}} = (\mathbf{I}_n + [m_3]^{-1}[m_4]\mathcal{L})\mathbf{V}^{ref} \tag{6a}$$

$$\overline{\mathbf{I}}^v = [r^d]^{-1}\overline{\mathbf{V}} + \beta[r^l]^{-1}\beta^T\overline{\mathbf{V}} + \mathbf{I}^d \tag{6b}$$

$$\overline{\mathbf{I}}^l = [r^l]^{-1}\beta^T\overline{\mathbf{V}}^{ref} \tag{6c}$$

$$\overline{\mathbf{z}}^v = -([m_1] - \mathbf{I}_n)\overline{\mathbf{V}} + [r^v]\overline{\mathbf{I}}^v + [k4]\mathcal{L}\overline{\mathbf{V}} \tag{6d}$$

The error system dynamic of DC MG can therefore be obtained by combining (4), (5) and (6) as:

$$\dot{\tilde{x}}(t) = \mathbf{A}\tilde{x}(t) + \mathbf{B}f(t) \tag{7}$$

where $f(t) = \mathbf{F}^v$ are the actuator attacks, $\tilde{x}(t) = x(t) - \overline{x}$ is the error vector. The matrices $\mathbf{A}$, $\mathbf{B}$ are given in the Appendix.

The solution to error can be obtained as:

$$\tilde{x}(t) = e^{\mathbf{A}t}\tilde{x}(0) + \int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}f(t)\mathrm{d}\tau \tag{8}$$

Furthermore, the steady state of the error system can be derived as follows:

$$\begin{aligned}\lim_{t\to\infty}\tilde{x}(t) &= \int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}f(t)\mathrm{d}\tau \\ &\leqslant \int_0^t e^{\mathbf{A}(t-\tau)}\mathbf{B}\Gamma\mathrm{d}\tau = -\mathbf{A}^{-1}\mathbf{B}\Gamma\end{aligned} \tag{9}$$

where Γ is the boundary of the actuator attacks.

Next, by combining with matrix (14), we obtain

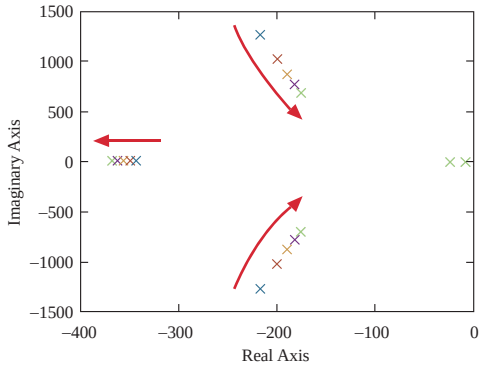
$$\mathbf{A}^{-1}\mathbf{B} = \begin{bmatrix}\mathbf{0} & \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0}\end{bmatrix}^T \tag{10}$$

where $\mathbf{I}$ is unit matrix.

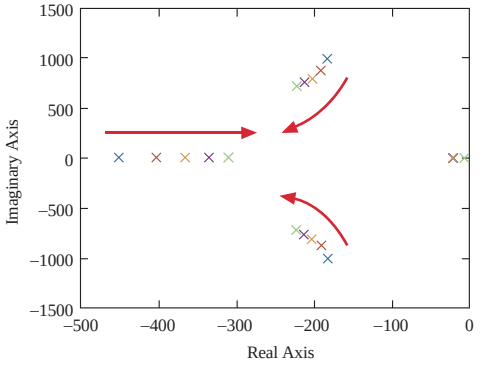
From (8) and (9), it is evident that the steady-state errors of the voltage and current state variables of the system are maintained at zero. This implies that the system can achieve voltage and current tracking performance at steady state regardless of the presence of actuator attacks.

3.3 Robustness against modeling errors

To assess the controller's robustness in the face of parameter uncertainty, the pole locations of the system are analyzed with variations in the capacitance, resistance, and inductance parameters of the converters. The controller parameters remain unchanged throughout the analysis. The results, depicted in Fig. 3, provide insights into the stability and performance of the system under parameter variations.



(a) Pole locus with C ranging from 1 to 3 mF



(b) Pole locus with L^v ranging from 1 to 3 mH

Fig. 3 Pole locus of the system

Table 1 DC MG parameters

Modules	Parameters	Values
DC MG	Sampling frequency	10 kHz
	Control frequency	10 kHz
LC filter	Bus capacitance	2.2 mF
	Inductance	1.8 mH

The stability analysis of the system with varying system parameters while keeping the controller coefficients constant reveals that the system remains stable. This observation highlights the robustness of the controller in the face of modeling uncertainties.

4 Performance Validation

Simulation tests were conducted to demonstrate the theoretical analysis and evaluate the performance of the proposed controller. The test model consists of four grid forming converters and four grid feeding converters with a meshed electrical topology, as depicted in Fig. 4. The power ratio for the four grid feeding converters rated capacity is $I_1^r : I_2^r : I_3^r : I_4^r = 2:3:3:2$. Table 1 provides the

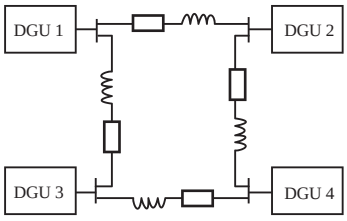


Fig. 4 DC MG circuit scheme

parameters for the microgrid (MG) and converters used in the simulation. The control parameters for the converters are determined as follows:

$$m_1 = -0.5,\ m_2 = 1,\ m_3 = 10,\ m_4 = 0.1 \tag{11}$$

4.1 Voltage/current tracking test under ramp-type attacks

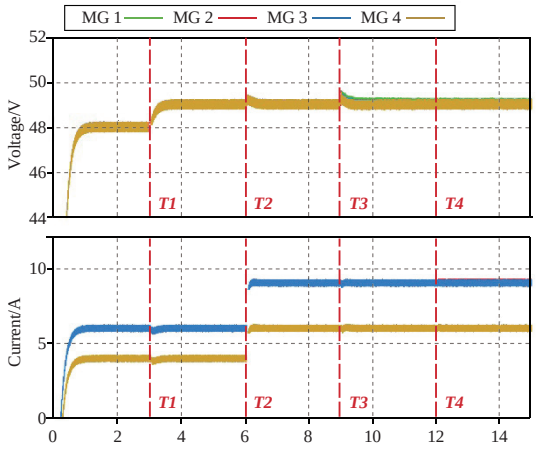
The study conducted in this case showcases the voltage and current tracking performance of the proposed controller and its resilience against ramp-type cyber-attacks. To demonstrate the advantages of the proposed controller, a comparison of results is performed across different control strategies. Fig. 5 displays the voltage and current dynamics in the presence of ramp-type attacks.

Initially, the four DGUs are interconnected and functioning as a microgrid. At time *T1*, the voltage reference values increase to 49 V, and at time *T2*, the current reference values for DGU 1 and DGU 4 change from 4 A to 6 A, while for DGU 2 and DGU 3, the current reference values change from 6 A to 9 A. The figures demonstrate that the voltages and currents of the microgrid quickly converge to the new reference values after the changes were made.

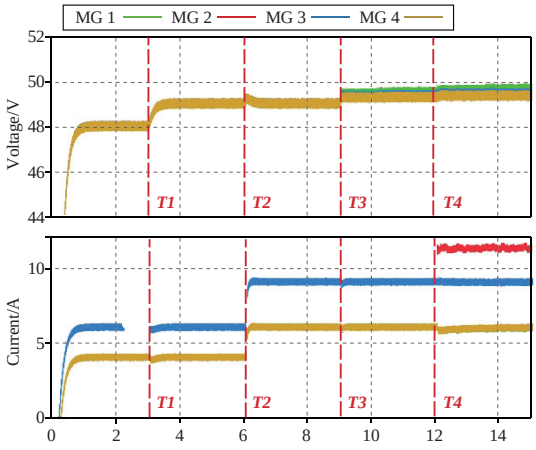
Furthermore, ramp-type cyber-attacks were initiated at *T3* on grid forming converter 1 of DGU 1 and at time *T4* on the grid feeding converter of DGU 3. Fig. 5(a) demonstrates that the system achieved accurate voltage and current tracking at a steady state. In contrast, Fig. 5(b) shows the dynamic responses of grid voltages and currents using conventional control methods, revealing oscillations and significant tracking errors at steady state. These results indicate the resilience of the proposed controller against attack signals, confirming its effectiveness in maintaining stable and accurate operation of the system.

4.2 Voltage/current tracking test under sine-type attacks

The study conducted in this case showcases the voltage and current tracking performance of the proposed controller and its resilience against sine-type cyber-attacks. Similarly, the simulation results are compared under different control strategies. Fig. 6 shows the voltage and current dynamics in



(a) With the proposed resilient controller



(b) With the traditional controller

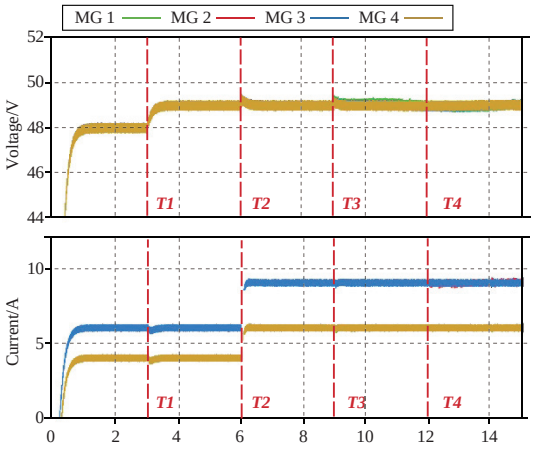
Fig. 5 Voltage and current dynamics under ramp-type attacks

the presence of sine-type cyber-attacks.

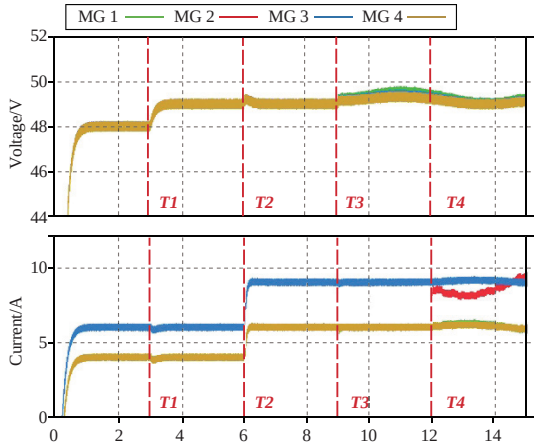
As the same as the cases in previous study, the converters are interconnected in the beginning. At *T1*, the voltage reference values are raised to 49 V, and at *T2*, the current reference values for DGU 1 and DGU 4 are adjusted from 4 A to 6 A, while for DGU 2 and DGU 3, the current reference values are changed from 6 A to 9 A. The obtained results show the rapid convergence of voltages and currents to the reference values.

At *T3*, a sine-type cyber-attack was launched on the grid forming converter 1 of DGU 1, while at time *T4*, a similar attack is carried out on the grid feeding converter of DGU 3. These attacks introduce gradually changing disturbances to the system, characterized by varying values.

The results presented in Fig. 6(a) highlight the precise voltage and current tracking performance by the system at steady states. In contrast, Fig. 6(b) depicts the dynamic responses of grid voltages and currents when conventional control methods were employed, revealing oscillations and



(a) With the proposed resilient controller



(b) With the traditional controller

Fig. 6 Voltage and current dynamics under sine-type attacks

tracking errors at steady state. Therefore, it is evidence to validate the robustness and effectiveness of the proposed controller in mitigating the impact of attack signals and ensuring stable and accurate operation of the system.

5 Conclusion

In this research, the vulnerability of DC microgrid systems to cyber-attacks is addressed. To mitigate the impact of cyber-attacks and ensure reliable operation of the system, a resilient control scheme is proposed. A steady-state analysis confirms the effectiveness of the control method in achieving voltage control and power sharing in the presence of cyber-attacks. Moreover, the robustness against modeling uncertainties is also demonstrated. Simulation results validate the performance of the proposed resilient control scheme under various cyber-attack scenarios, highlighting its ability to ensure secure operation of DC microgrid systems.

Acknowledgements

This work was supported by VILLUM FONDEN, Denmark under the VILLUM Investigator Grant (No. 25920): Center for Research on Microgrids (CROM).

Declaration of Competing Interests

The authors have no conflicts of interest to declare.

Appendix

Matrices **A** and **B** are expressed as

$$\mathbf{A}=\begin{bmatrix} -[C]^{-1}[r^d]^{-1} & [C]^{-1} & \mathbf{0} & -[C]^{-1}\beta \\ [L^v]^{-1}([m_1]-\mathbf{I}_n-[m_2]\mathcal{L}) & -[L^v]^{-1}[r^v] & [L^v]^{-1} & \mathbf{0} \\ -[m_3]-[m_4]\mathcal{L} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ [L^l]^{-1}\beta^T & \mathbf{0} & \mathbf{0} & -[L^l]^{-1}[r^l] \end{bmatrix}$$

$$\mathbf{B}=\begin{bmatrix} \mathbf{0} & [L^v]^{-1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}^T \tag{12}$$

References

[1] Yan N, Ma G, Li X, et al. (2023) Low-carbon economic dispatch method for integrated energy system considering seasonal carbon flow dynamic balance. IEEE Transactions on Sustainable Energy, 14(1): 576-586

[2] Chub A, Vinnikov D, Liivik E, et al. (2018) Multiphase quasi-Z-source DC-DC converters for residential distributed generation systems. IEEE Transactions on Industrial Electronics, 65(10): 8361-8371

[3] Tan S, Wu Y, Xie P, et al. (2020) New challenges in the design of microgrid system. IEEE Electrification Magazine, 8(4): 98-106

[4] Tan S, Xie P, Guerrero J M, et al. (2022) Cyberattack detection for converter-based distributed DC microgrids: Observer-based approaches. IEEE Industrial Electronics Magazine, 16(3): 67-77

[5] Saha S, Roy T K, Mahmud M, et al. (2018) Sensor fault and cyber-attack resilient operation of DC microgrids. International Journal of Electrical Power & Energy Systems, 99: 540-554

[6] Zhao J, Mili L, Wang M (2018) A generalized false data injection attacks against power system nonlinear state estimator and countermeasures. IEEE Transactions on Power Systems, 33(5): 4868-4877

[7] Danzi P, Stefanovic C, Meng L, et al. (2016) On the impact of wireless jamming on the distributed secondary microgrid control. 2016 IEEE Globecom Workshop, 1-6

[8] Tan S, Guerrero J M, Xie P, et al. (2020) Brief survey on attack detection methods for cyber-physical systems. IEEE Systems Journal, 14(4): 5329-5339

[9] Mo Y, Kim T H J, Brancik K, et al. (2011) Cyber-physical

security of a smart grid infrastructure. Proceedings of the IEEE, 100(1): 195-209
[10] Peng C, Sun H, Yang M, et al. (2019) A survey on security communication and control for smart grids under malicious cyber-attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(8): 1554-1569
[11] Tan S, Xie P, Guerrero J M, et al. (2022) False data injection cyber-attacks detection for multiple DC microgrid clusters. Applied Energy, 310: 118425
[12] Zhou Q, Shahidehpour M, Alabdulwahab A, et al. (2020) A cyber-attack resilient distributed control strategy in islanded microgrids. IEEE Transactions on Smart Grid, 11(5): 3690-3701
[13] Yan J, Guo F, Wen C (2020) Attack detection and isolation for distributed load shedding algorithm in microgrid systems. IEEE Journal of Emerging and Selected Topics in Industrial Electronics, 1(1): 102-110
[14] Abdollah K F, Su W, Jin T, et al. (2020) A machine learning based cyber-attack detection model for wireless sensor networks in microgrids. IEEE Transactions on Industrial Informatics, 17(1): 650-658
[15] Beg O A, Nguyen L V, Johnson T T, et al. (2018) Signal temporal logic-based attack detection in DC microgrids. IEEE Transactions on Smart Grid, 10(4): 3585-3595
[16] Beg O A, Johnson T T, Davoudi A (2017) Detection of false-data injection attacks in cyber-physical DC microgrids. IEEE Transactions on industrial informatics, 13(5): 2693-2703
[17] Abhinav S, Modares H, Lewis F L, et al. (2018) Resilient cooperative control of DC microgrids. IEEE Transactions on Smart Grid, 10(1): 1083-1085
[18] Rana M M, Li L, Su S (2017) Cyber-attack protection and control of microgrids. IEEE/CAA Journal of Automatica Sinica, 5(2): 602-609
[19] Cecilia A, Sahoo S, Dragicevic T, et al. (2021) On addressing the security and stability issues due to false data injection attacks in DC microgrids—an adaptive observer approach. IEEE Transactions on Power Electronics, 37(3): 2801-2814
[20] Liu X, Wen C, Xu Q, et al. (2021) Resilient control and analysis for DC microgrid system under DoS and impulsive FDI attacks. IEEE Transactions on Smart Grid, 12(5): 3742-3754
[21] Liu X, Wang S, Chi M, et al. (2024) Resilient secondary control and stability analysis for DC microgrids under mixed cyber-attacks. IEEE Transactions on Industrial Electronics, 71(2): 1938-1947
[22] Deng C, Wen C, Zou Y, et al. (2020) A hierarchical security control framework of nonlinear CPSs against DoS attacks with application to power sharing of AC microgrids. IEEE Transactions on Cybernetics, 52(6): 5255-5266
[23] Chen Y, Qi D, Dong H, et al. (2020) A FDI attack resilient distributed secondary control strategy for islanded microgrids. IEEE Transactions on Smart Grid, 12(3): 1929-1938
[24] Zhou Q, Shahidehpour M, Alabdulwahab A, et al. (2020) A cyber-attack resilient distributed control strategy in islanded microgrids. IEEE Transactions on Smart Grid, 11(5): 3690-3701

Biographies

Sen Tan received the B.S. degree in automation and the M.S. degree in control engineering, from Northeastern University, China, in 2014 and 2017, Ph.D. degree in energy technology from Aalborg University, Denmark, in 2022. He is currently working as Post Doc. with the Department of Energy Technology, Aalborg University, Denmark. His research interests include cyber-security, distributed control in microgrid and power management system.

Juan C. Vasquez (M'12-SM'14) received the B.S. in Electronics Engineering from the Autonomous University of Manizales, Manizales, Colombia and the Ph.D. in Automatic Control, Robotics, and Computer Vision from the Technical University of Catalonia, Barcelona, Spain in 2004 and 2009, respectively. Since 2019, he has been a full professor with the Department of Energy Technology, Aalborg University, Denmark. His current research interests include operation, advanced hierarchical and cooperative control, optimization and energy management applied to distributed generation in AC/DC microgrids, maritime microgrids, advanced metering infrastructure, and the integration of the Internet of things and cyber-physical systems into smart grids.

Josep M. Guerrero (S'01-M'12-SM'14 FM'15) received the B.S. in Telecommunications Engineering, the M.S. in Electronics Engineering, and the Ph.D. in Power Electronics from the Technical University of Catalonia, Barcelona, in 1997, 2000, and 2003, respectively. Since 2011, he has been a full professor with the Department of Energy Technology, Aalborg University, Denmark. His research interests is oriented toward different microgrid aspects, including power electronics, distributed energy storage systems, hierarchical and cooperative control, energy management systems, smart metering, and the Internet of things for AC/DC microgrid clusters and islanded minigrids. Recently, he particularly focuses on maritime microgrids for electrical ships, vessels, ferries, and seaports.

(Editor Yajun Zou)