
Proceedings Paper:
Tan, S. orcid.org/0000-0002-3492-2391, Xie, P. orcid.org/0000-0002-6147-7342, Guan, Y. orcid.org/0000-0002-1968-1542 et al. (3 more authors) (2024) A resilient control framework for enhancing cyber-security in microgrids. In: Nørregaard Jørgensen, B., Ma, Z.G., Wijaya, F.D., Irnawan, R. and Sarjiya, S., (eds.) Energy Informatics. Energy Informatics.Academy Conference 2024 (EI.A 2024), 23-25 Oct 2024, Bali, Indonesia. Lecture Notes in Computer Science, 15272 . Springer Nature Switzerland , pp. 372-378. ISBN 9783031747403

https://doi.org/10.1007/978-3-031-74741-0_24

A Resilient Control Framework for Enhancing Cyber-Security in Microgrids

Sen Tan[1][0000−0002−3492−2391], Peilin Xie[1][0000−0002−6147−7342], Yajuan Guan[1][0000−0002−1968−1542], Juan C. Vasquez[1][0000−0001−6332−385X], Josep M. Guerrero[1,2][0000−0002−6063−959X], and Xin Zhang[3][0000−0001−5236−4592]

[1] Energy Department, Aalborg University, Aalborg 9220, Denmark
[2] Department of Electronic Engineering, Universitat Politecnica de Catalunya, Barcelona 08034, Spain
[3] Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield S102TN, United Kingdom

Abstract. Microgrid security has become a critical concern due to the increasing reliance on communication technologies and a rising incidence of cyber-threats. While various attack detection and resilient control mechanisms have been developed to fortify microgrid defenses, most research still focuses on simplistic attack scenarios, often ignoring the complex interactions between multiple distributed generators within microgrids. To bridge this gap, this paper proposes a resilient secure control framework capable of addressing cyber-threats across multiple locations within a microgrid. The framework integrates state observations, robust control strategies, and time-varying graph theory to construct a robust defense mechanism. Simulation results are presented to validate the practicality and effectiveness of this approach, confirming its potential to enhance security for future microgrid against cyber-attacks.

Keywords: Cyber-security · Microgrid · Secure framework.

1 Introduction

Microgrids are increasingly recognized as pivotal in ensuring resilient and sustainable energy services to communities, particularly for critical infrastructure such as hospitals, residential areas, and emergency services. These infrastructures heavily rely on consistent and reliable power, especially critical in the context of natural disasters. Recent years have witnessed a substantial influx of research focused on cyber-security within microgrids, prompted by the growing threat of cyber-physical attacks [1]. Such cyber-attacks have the potential to disrupt not only microgrid operations but also broader macrogrid services, thereby impacting the resilience and sustainability of entire communities, which can result in significant energy disruptions, financial losses, and damage to infrastructure [2].

To address security challenges in microgrids, sophisticated attack detection and resilient control techniques have been developed [3]. These systems first detect potential cyber-threats by monitoring for abnormal behavior within the

grid. Upon detecting a cyber-threat, an alarm notifies operators, and resilient control methods are activated to either compensate for or isolate the affected components [4].

The detection of cyber-attacks in microgrids can be categorized based on their reliance on microgrid parameters and models into three primary methods: signal-based, model-based, and data-based. Signal-based detection methods analyze the features of transmitted data to identify anomalies [5]. Model-based detection makes use of microgrid models to analyze input-output behaviors, utilizing techniques like state estimation and observers [6]. Finally, data-based detection focuses on recognizing patterns and making predictions using a variety of learning-based methods [7]. The primary objective of resilient control in microgrids is to guarantee stable operation even in the presence of cyber-attacks using adaptive control, robust optimizations, virtual microgrid model (auxiliary variables) and etc. For example, a switching control is developed in [8], where the controller gains are adaptive to the combined error of grid voltage and current. To minimize the damage from attacks and prevent load shedding, a robust optimization approach is formulated in [9] to facilitate autonomous battery management during an ongoing cyber-attack. Furthermore, a virtual microgrid model is introduced in [10] to ensure the frequencies synchronization and restoration of distributed generations.

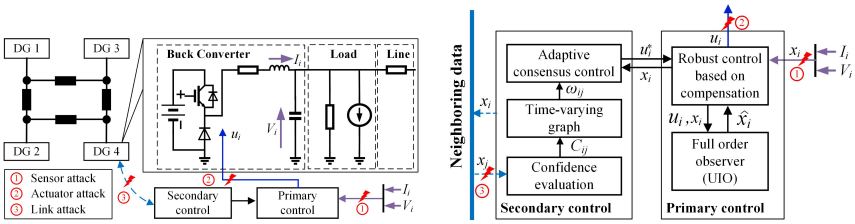
However, current research on microgrid security exhibits two main gaps. Firstly, the studies primarily focus on scenarios where cyber-attacks target individual local distributed generations (DGs), often overlooking the need for coordination among various generation sources within the microgrid. Secondly, existing studies typically concentrate on attacks at a single location, disregarding the potential for attacks at multiple points within the microgrid. Consequently, strategies developed to counteract attacks at one specific location may prove ineffective in different scenarios. To address these shortcomings, this paper proposes a resilient secure control framework for microgrids, specifically designed to manage cyber-attacks across all potential locations within the grid.

2 Cyber-physical DC Microgrid and Attacks

2.1 Microgrid Dymanics

The microgrid is conceptualized as a network comprising multiple DGs interconnected with each other. A distributed control system, consisting of secondary and primary control layers, is adopted to facilitate power sharing and voltage regulation across the network. Fig. 1(a) illustrates the control diagram and the structure of the microgrid, with the model described as below:

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



(a) Microgrid structure. (b) Proposed secure control.

Fig. 1: Proposed resilient control framework for microgrids.

where I_i and V_i represent the filter current and voltage, respectively; The electrical parameters of the LC filter are denoted by R_i, L_i and C_i; V_{ti} represents the control input of i-th converter; Additionally, V_j denotes the voltage at the point of common coupling (PCC) of each neighboring DGs, where $j \in \mathcal{N}_i$ with $\mathcal{N}_i$ representing the set of neighbors of DG i; The resistance of the DC power line is represented by R_{ij}.

2.2 State-space Model

The dynamics of microgrid can then be further described by state-space model as follows:

$$\begin{cases} \dot{x}_i(t) = A_i x_i(t) + B_i(u_i(t) + a_{i,a}(t)) + E_i d_i(t) \\ y_i(t) = C_i x_i(t) + a_{i,s}(t) \end{cases} \tag{2}$$

where $x_i(t) = [V_i, I_i]^T \in \mathbb{R}^2$ and $y_i(t) \in \mathbb{R}^2$ denote the system state variables and output, receptively; $u_i(t) = V_{ti} = f(y_i(t), x_j(t)) \in \mathbb{R}^1$ is the distributed controller of DG i. $d_i(t) = \sum_{j \in N_i}(\frac{V_j - V_i}{R_{ij}}) - (\frac{V_i}{R_{Li}} + I_{Li}) \in \mathbb{R}^1$ represents the unknown disturbances affecting DG i; $a_{i,s}(t) \in \mathbb{R}^2$ and $a_{i,a}(t) \in \mathbb{R}^1$ are the cyber-attack on the sensors and actuators, receptively. Furthermore, the neighboring information could also be tampered with resulting in $x_j(t) = \bar{x}_j(t) + a_{i,c}(t)$, where $\bar{x}_j(t)$ is the real value of neighboring states, $a_{i,c}(t) \in \mathbb{R}^2$ represents the link attacks. The corresponding matrices are represented by $A_i = [0, \frac{1}{C_i}; -\frac{1}{L_i}, -\frac{R_i}{L_i}]$, $B_i = [0; \frac{1}{L_i}]$, $C_i = I_n$ and $E_i = [-\frac{1}{C_i}; 0]$, where I_n is the identity matrix.

Observed from Fig. 1(a), the microgrid is vulnerable to cyber-attacks that can target the data flowing through sensors, actuators, and communication links between neighboring units. This susceptibility leads to three primary types of cyber-threats: sensor attacks, where data captured by sensors is tampered with or falsified; actuator attacks, where the commands to actuators are intercepted or modified; and link attacks, where the communication links between different units are disrupted or corrupted.

3 Proposed Secure Control Framework

To address the vulnerabilities associated with sensor, actuator, and link attacks, a resilient secure control framework is proposed, integrating state observations,

robust control mechanisms, and time-varying graph theory, as depicted in Fig. 1(b). The microgrid operates under the assumption that an effective attack detection system is incorporated within the control system. Typically, distributed control methods are employed for hourly or day-to-day operations. However, upon detection of any abnormal behavior indicative of a cyber-attack, the control system transitions to the proposed secure control to ensure the uninterrupted and stable operation, effectively mitigating the potential disruptions caused by cyber-threats.

3.1 State Observations against Sensor Attacks

Different from the traditional state estimation used in power systems, the state observations of microgrids require correctly observing state variables among a limited number of erroneous measurements. Given the presence of unknown disturbances (load variations, voltage perturbation, etc), accurate state observation may only be achieved through the use of a full-order observer capable of handling these disturbances. To estimate the microgrid states $x_i(t) = [I_i, V_i]$, an unknown input observer (UIO) is adopted. When a suspicious signal is detected on sensors, the observed states $\hat{x}_i(t)$ derived from the UIO will be utilized as a substitute to feed the controller.

3.2 Robust Control against Actuator Attacks

To combat actuator attacks, a robust controller capable of compensating for the impact of such attacks is employed, as detailed in [4]. The controller is designed to ensure the microgrid maintain accurate current sharing and voltage regulation, despite the presence of cyber-threats. Notably, the effectiveness of this controller allows the microgrid to perform reliably both under normal operating conditions and in scenarios where actuator attacks are occurring.

3.3 Time-varying Graph-based Control against Link Attacks

To address cyber-attacks on communication links between neighboring units within the microgrid, time-varying graph-based secondary control is adopted, as in Fig. 1(b). This approach begins with the design of a confidence score system that evaluates the reliability of data received from neighboring units $x_j(t)$ and quantifies their trustworthiness using a trust-based methodology. Subsequently, based on these confidence scores $C_{ij}(t)$, the weights $\omega_{ij}(t)$ in the consensus control are dynamically adjusted. Finally, the data deemed less reliable, as indicated by lower confidence scores, are assigned reduced influence in the consensus control. This strategic adjustment ensures that compromised data exert minimal impact on control decisions, effectively mitigating the effects of cyber-threats and preventing the propagation of attacks throughout the microgrid. Readers can refer to [11] for more details.

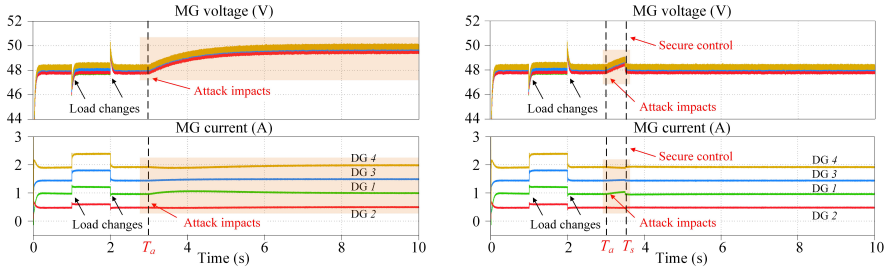
Table 1: Electrical setup parameters.

Modules	Parameters	Values
DC microgrid	Nominal voltage	48 V
	Control frequency	10 kHz
LC filter	Bus capacitance	2.2 mF
	Inductance	1.8 mH
	Resistance	0.2 Ω

4 Simulation Results

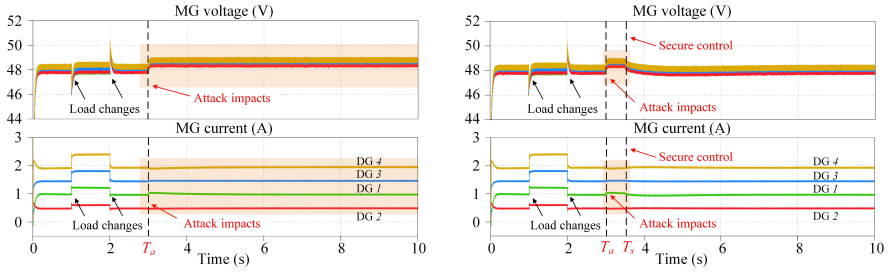
The effectiveness of the proposed security control method is verified by simulation results in PLECS, where the test model is comprised by four DGs with a ring topology, as shown in Fig. 1(a) and the parameters of tested microgrid is shown in Tab. 1. At the beginning, four DGs are interconnected to form a microgrid. To verify the robustness against unknown disturbances, the loads are changed at $1s$ and $2s$. Following this, a cyber-attack is imposed at $t = T_a$ on the voltage sensors, actuators, and link connections, respectively. Figs. 2 to 4 show the comparison of system dynamics under traditional control versus proposed secure control, where the security control is initiated at $t = T_s$ and the impact of the cyber-attacks on the microgrid is highlighted.

It can be observed from Fig. 2 that sensor attacks can deviate the grid voltages and impose small variations in the current dynamics, whereas the observer-based approach is able to compensate for the voltage deviation and bring the system back to its normal dynamics. It can be noticed from Fig. 3 that a steady state error in the grid voltages appears under the actuator attack and the robust control is capable of eliminating the error. Furthermore, as can be seen in Fig. 4, the grid voltages and currents diverge in the event of a link attack, because the local DG is given the erroneous measurements from the neighbors, which in turn generates faulty control commands. The time-varying graph-based control al-



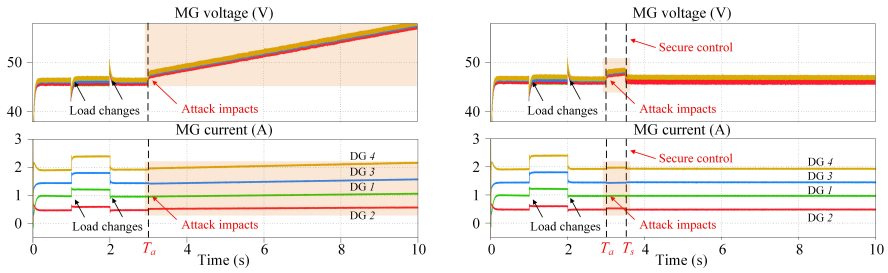
(a) With traditional control (b) With secure control

Fig. 2: Microgrid dynamics under sensor attacks.



(a) With traditional control (b) With secure control

Fig. 3: Microgrid dynamics under actuator attacks.



(a) With traditional control (b) With secure control

Fig. 4: Microgrid dynamics under link attacks.

lows for a quick removal of the compromised link connections, thus restoring the system to a normal state. To summarize, the proposed secure control is capable of addressing all potential cyber-attacks that may appear on microgrids.

5 Conclusions

The digitization of microgrids has improved operational efficiency while also making them more susceptible to cyber-attacks. However, current research tends to investigate attacks on a singular location only. For this reason, this paper aims to propose a secure control framework against multi-location cyber-attacks targeting microgrids, and provides a benchmark for enhancing security for future microgrids. The proposed resilient control eliminates the effects of sensor, actuator, and link attacks through state observation, robust control, and time-varying graph-based control, which can improve the microgrid security. Simulation results validate the feasibility of the proposed control framework under multiple scenarios.

Acknowledgements This work received support from VILLUM FONDEN through the VILLUM Investigator Grant (Grant No. 25920).

References

1. Tan, S., Guerrero, J.M., Xie, P., Han, R., Vasquez, J.C.: Brief survey on attack detection methods for cyber-physical systems. IEEE Systems Journal **14**(4), 5329–5339 (2020)
2. Zhang, W., Qian, T., Chen, X., Huang, K., Tang, W., Wu, Q.: Resilient economic control for distributed microgrids under false data injection attacks. IEEE Transactions on Smart Grid **12**(5), 4435–4446 (2021)
3. Tan, S., Wu, Y., Xie, P., Guerrero, J.M., Vasquez, J.C., Abusorrah, A.: New challenges in the design of microgrid system. IEEE Electrification Magazine **8**(4), 98–106 (2020)
4. Tan, S., Xie, P., Guerrero, J.M., Vasquez, J.C., Alcala, J.M., Carreño, J.E.M., Zapata, M.G.: Lyapunov-based resilient cooperative control for dc microgrid clusters against false data injection cyber-attacks. IEEE Transactions on Smart Grid (2023)
5. Tan, S., Xie, P., Guerrero, J.M., Vasquez, J.C., Han, R.: Cyberattack detection for converter-based distributed dc microgrids: Observer-based approaches. IEEE Industrial Electronics Magazine (2021)
6. Lu, J., Zhang, X., Hou, X., Wang, P.: Generalized extended state observer-based distributed attack-resilient control for dc microgrids. IEEE Transactions on Sustainable Energy **13**(3), 1469–1480 (2022)
7. Ismail, M., Shaaban, M.F., Naidu, M., Serpedin, E.: Deep learning detection of electricity theft cyber-attacks in renewable distributed generation. IEEE Transactions on Smart Grid **11**(4), 3428–3437 (2020)
8. Liu, X.K., Wen, C., Xu, Q., Wang, Y.W.: Resilient control and analysis for dc microgrid system under dos and impulsive fdi attacks. IEEE Transactions on Smart Grid **12**(5), 3742–3754 (2021)
9. Kushal, T.R.B., Lai, K., Illindala, M.S.: Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system. IEEE Transactions on Smart Grid **10**(5), 4741–4750 (2018)
10. Chen, Y., Qi, D., Dong, H., Li, C., Li, Z., Zhang, J.: A fdi attack-resilient distributed secondary control strategy for islanded microgrids. IEEE Transactions on Smart Grid **12**(3), 1929–1938 (2020)
11. Tan, S., Xie, P., Vasquez, J.C., Guerrero, J.M.: Consensus check in the detection of faulty and hijacking attacks for multiple converter-based microgrids. In: 2024 IEEE 10th International Power Electronics and Motion Control Conference (IPEMC2024-ECCE Asia). pp. 2360–2365. IEEE (2024)