An Adaptive Cyber Security Scheme for AC Microgrids

Xiao, Junjie; Wang, Lu; Qin, Zian; Bauer, Pavol

DOI
10.1109/ECCE50734.2022.9948108

Publication date
2022

Document Version
Final published version

Published in
2022 IEEE Energy Conversion Congress and Exposition, ECCE 2022

An Adaptive Cyber Security Scheme for AC Micro-grids

Junjie Xiao
Electrical Sustainable Energy
TU Delft
Delft, The Netherlands
J.Xiao-2@tudelft.nl

Lu Wang
Electrical Sustainable Energy
TU Delft
Delft, The Netherlands
L.Wang-11@tudelft.nl

Zian Qin
Electrical Sustainable Energy
TU Delft
Delft, The Netherlands
Z.Qin-2@tudelft.nl

Pavol Bauer
Electrical Sustainable Energy
TU Delft
Delft, The Netherlands
P.Bauer@tudelft.nl

***Abstract*—Distributed secondary control is deemed necessary to restore the state of AC micro-grids to set points. However, for its limited global information, the power electronic system is vulnerable to cyber-attacks that aim to desynchronize converters or even cause a shutdown of micro-grids by unnecessarily triggering the protection schemes. To this end, an adaptive communication weight update for the secondary control layer is proposed. It guarantees frequency synchronization and active power sharing despite the presence of these attacks. Moreover, it automatically dispatches optimal communication lines when all its neighboring data are corrupted to different levels. Finally, the efficacy of the proposed resilient control method is demonstrated using simulations.**

Keywords— distributed control; adaptive control; cyber-attack; AC micro-grid

I. INTRODUCTION

It is widely known that the conventional structure of the electric power system is exclusively dependent on fossil energy sources. However, the exponential evolution of the industrial world has resulted in a series of concerns such as environmental pollution and the energy crisis, which briefly forced the power system to be reformed[1]. Microgrid technology is a prospective response to these challenges and is highly adapted to the requirements of the industrial world by integrating emerging resources such as fuel cells, solar power units, and micro wind turbines[2].

Among the research subjects of AC microgrids, the inverter control strategy is the most extensively studied. Normally, a voltage-source inverter tends to employ droop control to keep its robustness and scalability. But it will cause a frequency offset and voltage amplitude deviation from the nominal value.

Distributed Secondary Control (DSC) is gaining popularity for AC micro-grids, with which the set point of a converter is calculated following the information of the neighboring converters to regulate the output voltage of local converters. Hence, the AC micro-grid is preserved from a single failure of centralized secondary control because it does not need a central controller [3]. However, limited global information makes it vulnerable to cyber attacks, which may affect control accuracy and even cause stability problems.

Among different kinds of cyber attacks, False Data Injection attacks (FDIAs) [4] and Denial-of-Service (DoS) attacks [5] are the two most widely discussed cyber-attacks. These attacks jeopardize the confidentiality, integrity, and availability of information in the microgrid, leading to disruption of control objectives, which deserve attention.

Moreover, a series of recent cyber attack security incidents have demonstrated that the existing technical means are not sufficient to defend against hackers' elaborate virus data[6]-[7].

In 2003, a serious case of cyber attack occurred in Ohio, USA, when the Slammer worm broke into the control system of the David-Besse nuclear power plant [8]. In 2015, the networks of energy companies in Kyiv, Ukraine, were illegally compromised, leading to widespread power outages[9]. In 2019, hackers breached a firewall built by grid operators in the western United States, leading to a ten-hour power outage. In 2019, hackers breached firewalls built by grid operators in the western United States. Even more, hackers attacked the security features of cars, such as braking and steering in the Jeep Cherokee and Tesla's Model X[11].

A review of the earlier efforts indicates that the responses to cyber attacks fall into three types of mechanisms [12]: a) to avoid directing cyber attacks onto the system, b) resilience: to endure the largest impacts of an attack and to operate as close to normality as possible, and c)attack detection and isolation: to recognize the target of the attack, to isolate the damaged subsystem, and to recover the normal pattern as efficiently as possible.

In general, it is practically impossible to stop every potential attack threat on the microgrid. So, detection, isolation, and a resilient framework are indispensable. For intrusion viruses, first, detect and distinguish different kinds of attacks, then the resilient scheme should be employed to make the system more robust. A severely infected unit should be immediately isolated to save the whole system.

Therefore, to cope with the demands of data privacy and the stability of microgrid performance, the response of distributed control strategies to cyber attacks deserves additional investigation[13].

Different cyber-attack detection methods could be broadly classified into two types. First, model-based like Kalman filter-based detector proposed in [14] to estimate the system state of a microgrid. Nevertheless, such approaches suffer from a reliance upon the correctness of the systematic model, which makes them

2022 IEEE Energy Conversion Congress and Exposition (ECCE) | 978-1-7281-9387-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ECCE50734.2022.9948108

elusive in practical implementations because of their inevitable mismatch with complicated real-world power electronic systems. Model-free approaches like artificial intelligence-based algorithms [15] have been proven to be a prospective method for cyber-attack detection as well. These detection techniques are elaborately studied in [16].

To cope with the above challenges of microgrid operation, resilient microgrids against malicious attacks are the main research priority of this paper. In General, applied resilient schemes restrict the number of the infected agency. In [17], if more than half of the units are attacked by FDIA, the defense mechanism will not work. The resilient scheme to mitigate cyber attacks proposed in [18] ensures that the grid system remains operational when N-1 units receive a corrupt signal with FDIA (in a system with N converters). For DoS attacks, a resilient sampling mechanism is applied in the secondary control layer to get data updates from neighbors[19].

However, to the best of the authors' knowledge, the development of a resilient DSC, which guarantees the resilience of FDIA and DoS at the same time is still an open question. To resist cyber-attacks in power electronic-based systems, this paper proposes a defense mechanism, which selects the optimal communication route and dampens the impact of cyber-attacks by modulating the communication.

In this paper, we mainly contribute to (1) defining two common classes of cyber attacks (FDIA and DoS) and giving physical expressions for each. (2) analyzing how different cyber attacks affect the secondary control and how it adversely impacts the output of the microgrid. (3) To solve the above problems, an adaptive control scheme is proposed in this paper. (4) The correctness of the theoretical analysis is verified by Matlab simulation.

This paper is organized as follows. Section II describes the microgrid framework, characterizes the sparse communication system involved in this paper, and introduces the distributed secondary controller. Section III presents the model of cyber attacks and the adaptive framework proposed in this paper to cope with cyber attacks. Section IV verifies the direct impact of cyber attacks on the performance of the microgrid as well as verifies the suppression effect of the proposed strategy on cyber attacks. The conclusions are given in Section V.

II. Stand Cooperative Secondary Control Strategy of Microgrid

To achieve voltage synchrony and active power sharing in AC micro-grids, a hierarchical control strategy consisting of a primary droop control and a cooperative secondary control is adopted. The typical micro-grid and its control program are shown in Fig. 1, where N energy storage units are connected through DC/DC and DC/AC converters and form a cyber-physical system. A sparse communication network connecting different agencies propagates reference information to share the state of each inverter unit, where the major goals of the controller are voltage regulation and proportional power-sharing, while the object of the communication control is to realize the optimal operation. The output voltage of each node is regulated by the primary control layer. The equalizing current leads to a voltage frequency error, compensated by the distributed secondary control.

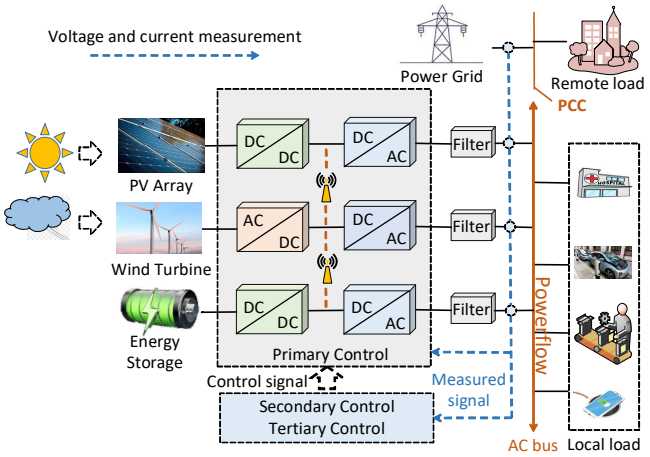


Fig. 1. A typical micro-grid system

A. Sparse Communication Network

Our research object is a microgrid system with N inverters connected in parallel, operating in islanded operation mode involved in regulating the frequency and amplitude of the voltage to maintain the power balance [8].

An undirected cyber graph of the communication network is considered to show how the involved converters share information with their neighbors. For every object converter i of the microgrid, the communication graph with its all neighbors j can be written as a digraph via edges and links via communication adjacency matrix $A=(a_{ij})_{N\times N}$ (states are sent to agent i from agent j).

The communication weight will be $a_{ij}=1$ when there are lines of communication between the i-th unit and the j-th unit, otherwise, $a_{ij}=0$. The degree of vertex ς_i is given as $D=diag(d_1,...d_N)$ is the corresponding degree matrix, where $d_i=\sum_{j=1}^{N}a_{ij}$. Further, the Laplacian matrix **L** is defined as L=D-A.

With the sparse communication network outlined above, distributed generation units can communicate with each other to propagate their information.

B. Primary droop control

For Voltage Source Inverter(VSI), droop control is the dominant control method for the primary control of islanded AC microgrids. Droop control philosophy ensures all inverter output frequency and voltage amplitude will converge to the same value, equal active power-sharing and reactive power-sharing through a negative feedback mechanism. The active Power-Frequency (P-ω) and reactive Power–Voltage amplitude(Q-V) droop control mechanism can be represent as (1):

$$\omega_i=\omega_{ni}+m_{Pi}(P_{iref}-P_i) \quad (1)$$

$$V_i=V_{ni}+n_{Qi}(Q_{iref}-Q_i) \quad (2)$$

where ω_i, V_i, are the output angular frequency and voltage amplitude of inverter i, respectively. P_i and Q_i are the measured

active power and reactive power, respectively. n_{Qi} and m_{Pi} are the corresponding droop coefficient of the power control loop which are given according to the power-sharing ratio. ω_{ni} and V_{ni} are the frequency and voltage set-points, respectively, which are defined by the secondary control layer.

From(1) and (2), it can be demonstrated that the control goal of power equalization can be realized as long as power reference and droop coefficient are set reasonably. However, the droop control method suffers from the frequency and voltage amplitude deviation. Therefore, the secondary control strategy is employed to restore the frequency and voltage amplitude by adjusting angular frequency, and voltage amplitude setting set points ω_{ni} and V_{ni}. Herein, we only consider the modeling of the secondary frequency control and cyber-attacks model in the frequency data exchanging process in this paper, the details are outlined in Section III. It should be noted that this procedure can also be extended to the active control loop and secondary voltage control loop.

C. Distributed secondary control

Differentiating the P–ω droop characteristic in (1) yields

$$\dot{\omega}_i = \dot{\omega}_{ni} - m_{Pi}\dot{P}_i \tag{3}$$

$$\omega_{ni} = \int v_i dt \tag{4}$$

where v_i is the auxiliary control input to adjust the secondary control set-point. The expression of v_i is derived from (5)

$$\begin{aligned} v_i &= -c_{fi}(\vartheta_{\omega 1} + \vartheta_{\omega 2} + \vartheta_P) \\ \vartheta_{\omega 1} &= \sum_{j\in N_i} a_{ij}(\omega_i - \omega_{ij}) \\ \vartheta_{\omega 2} &= g_i(\omega_i - \omega_{ref}) \\ \vartheta_P &= \sum_{j\in N_i} a_{ij}(m_{Pi}P_i - m_{Pij}P_{ij}) \end{aligned} \tag{5}$$

where loop gain $c_{fi} > 0, g_i > 0$, a_{ij} is the communication coefficient. ω_{ref} is the nominal frequency which is predefined. $\vartheta_{\omega 1}$ is employed to keep frequency synchronized among different agencies. $\vartheta_{\omega 2}$ is used to promise frequency coverage to ω_{ref} at last. With ϑ_P, the active power during the whole process of microgrid operation is evenly shared by all converters. In this paper, we investigate a microgrid system that includes N converters. The control diagram of each converter is shown in Fig. 2. It should be noticed that this paper focus on frequency set-point ω_{ni} .voltage set-point V_{ni} comes from voltage reactive power control loop which is not presented in this paper.

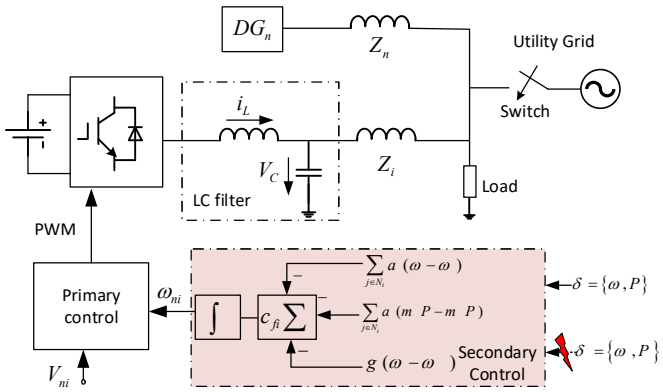


Fig. 2. The control diagram of an AC microgrid with distributed secondary control strategy consisting of N converters

With the proposed distributed secondary control algorithm, the micro-grid in islanding mode can recover the frequency and share the active power proportionally among the converters. The control objective for the active power control loop can be represented as:

$$\lim_{t\to\infty} \omega_i(t) = \omega_{ref}, \forall i \in \{1,2,...,N\} \tag{6}$$

$$\lim_{t\to\infty} m_{Pi}P_i(t) = \lim_{t\to\infty} m_{Pij}P_{ij}(t), \forall i, j \{1,2,...,N\} \tag{7}$$

III. Cyber Attacks and Defense Mechanism

As we discussed before, distributed secondary control can keep synchronizing voltage. However, The malicious can destabilize the AC microgrids depending on the attack intensity.

In this section, we first introduce FDIA and DoS attacks and then model these two typical attacks. Next, formulate the secondary resilience synchronization problem for island AC micro-grids in the presence of FDIA and DoS attacks.

A. Modeling the cyber attacks

The proposed distributed control framework is given by (5) relies heavily on exchanging $\delta_{ij} = \{\omega_{ij}, P_{ij}\}$ among different converters which makes the cyber-physical system may be attacked by hackers.

Typical cyber-attacks including the potential FDIA can be modeled as injected with false data. And DoS attacks can be modeled as failing to get the information of the neighboring converters. The attack on the estimated frequency received from the neighboring agent can be modeled with (8).

$$\omega_{a,ij} = \kappa_{ij}(\omega_{ij} + \eta_{ij}\varphi_{ij}) \tag{8}$$

where $\omega_{a,ij}$ denote the state information measured by local agent i. ω_{ij} represent the real angular frequency sent to the ith agent, φ_{ij} is the false data that inject to the communication line. η_{ij} and κ_{ij} are both binary variables. Specifically, $\eta_{ij} = 1, \kappa_{ij} = 1$ denoting the presence of FDIA with the malicious element φ_{ij}; while $\eta_{ij} = 1, \kappa_{ij} = 0$ representing the presence of a DoS attack and

FDIA at the same time; $\eta_{ij}=0,\kappa_{ij}=1$ Suggesting the microgrid system works in the normal state without any cyber-attack; $\eta_{ij}=0,\kappa_{ij}=0$ indicating there is a DoS attack and no FDIA.

B. Proposed resilient control strategy

As is shown in Figure 3, to mitigate the attack, an adaptive control scheme for the AC microgrid is proposed as (9)-(12):

$$\lambda_{ij}=\kappa_{ij}\left\|\omega_i-\omega_{a,ij}\right\| \tag{9}$$

$$\Omega_{ij}=e^{-\lambda_{ij}} \tag{10}$$

$$\rho_{ji}=\Omega_{ji}\Big/(\Omega_{ji}+\ldots+\Omega_{Ni}) \tag{11}$$

$$\dot{a}_{ij}=\xi_{ij}\rho_{ij}(t)-\xi a_{ij} \tag{12}$$

where λ_{ij} is an auxiliary state of the controller of DG i, it is employed to distinguish if there is a cyber attack or not. If $\lambda_{ij}=0$, it is suggested that no cyber attack exists in the microgrid system. Ω_{ij} is used to reduce the impact of cyber attacks on the system, and the exponential function is adopted to decrease communication weights because it's more sensitive to attacks compared to other correlation functions. ρ_{ji} is obtained by a comparison term, and if all the information transmitted by the locally controlled neighbors is disturbed, (11) will choose to trust the less infected line. Combining (10) (11), it is possible to obtain that greater attack measurements will be given smaller communication weights, thus mitigating cyber-attacks affecting the decisions of the secondary control layer. whereas ξ_{ij} is added to prevent unwanted oscillations in the frequency response of DG units. $\xi_{ij}\in\mathbb{R}_+,\kappa_{ij}\in\mathbb{R}_+$ called resilience index, are the control parameters are added to enhance resilience against cyber-attacks, Using the term defined in (12), the communication weight inputs previously defined in (5) are updated with cyber-attacks.

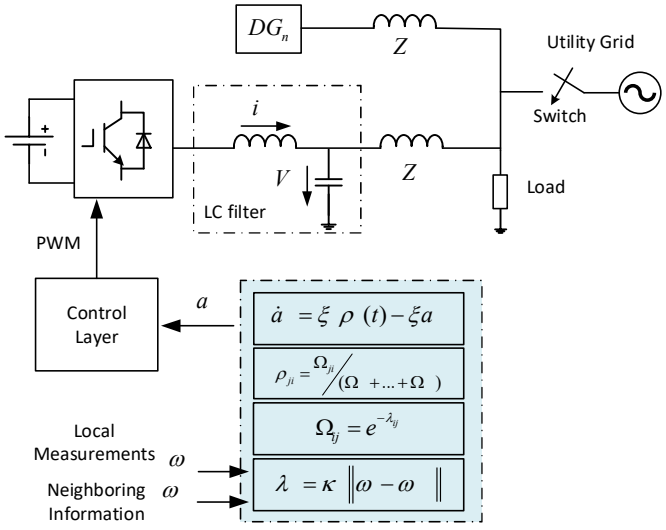


Figure 3 Proposed resilience scheme for cyber attacks

IV. RESULT

The proposed adaptive control strategy has been tested in a simulation of a distributed AC micro-grid with N = 3 (as shown in Figure 3) to validate the effectiveness. All the parameters are provided in Appendix. It can be seen in Figure 4 and Figure 5 that the Simulation time is 8s. The microgrid system starts up at 0s. The secondary control algorithm is enabled at t=1s, after which the frequency is restored to a nominal value and the power is proportionally shared. At 3s, FDIA and DoS attacks are imposed on the microgrid in separate experiments. The proposed adaptive defense mechanism is enabled at 4s. At 6s, the load changes from 6kW to 10kW.

Scenario I: Only one communication line is attacked (FDIA or DoS)

In this case, FDIA ($\varphi_{13}=6$) and DoS attack ($\kappa_{23}=0$) are imposed on the system at 3s separately in different experients. According to Figure 4(a) and Figure 4(c), because of the inserted data into the communication line, the secondary control setpoint will not reach the optimal value, in other words, the output frequency will not equal ω_{ref} . As we can see, the output frequency of the inverter parallel-connected will works under 50.05Hz, and the agents can't share the active power.

For the DoS attack situation, as we can see from Figure 4(b) and Figure 4(d), inverter 2 receives the frequency of inverter 3 is 0Hz. So, to synchronize frequency, inverter 2 will adjust its set point and then adjust its output voltage rapidly which leads to the frequency and active power suffering from an oscillation. After the defense mechanism is enabled at 4s, the adverse effect caused by the DoS attack is mitigated, and the system gradually recovers to a normal state.

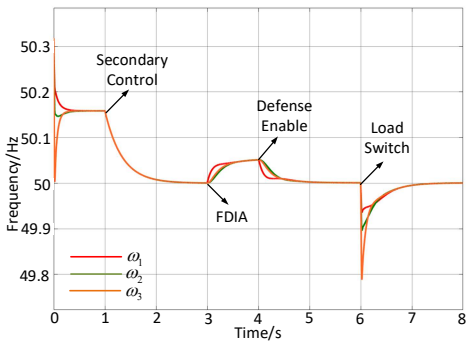
According to the proposed resilient scheme, when one communication line is attacked, the controller will choose other uninfected lines to acquire the real state of its neighbors. So we can conclude that the proposed adaptive method is effective for mitigating cyber-attack with one line attacked because the system is restored to the pre-attack set-point within 2s.

Scenario II: Attacked by a combination of FDIA and DoS

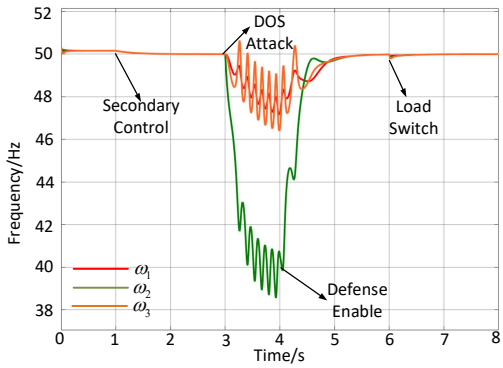
In this case, the combined attack or infused at t = 3s. From Fig. 5 (a) and Fig. 5 (b), it can be seen that when all communication lines of Inverter 1 suffer FDIA $\varphi_{13}=6,\varphi_{12}=1$, the controller chooses the communication line from inverter 2 to inverter 1 to continue exchanging information with its neighbors, as it is the less infected line.

From Fig. 5 (c) and Fig. 5 (d), it can be seen that inverter 3 to inverter 1 suffers FDIA $\varphi_{13}=1$, and from inverter 2 to inverter 1 suffers DoS which is modeled failing to get neighbor's data, furthermore, the impact of the DoS attack is greater than FDIA, so the controller will choose to favor trusting inverter 3.

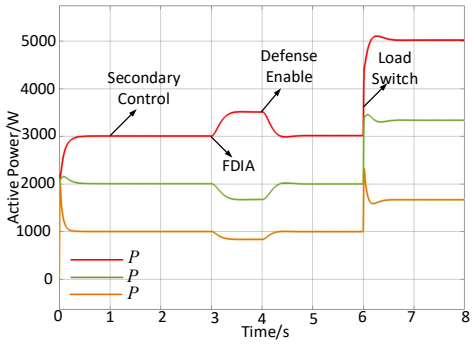
For serious cyber attack issues, when all communication lines are infected, the proposed adaptive method updates communication weight with the optimal operation and then disregards the light attacks. In this way, the microgrid will endure the smallest possible impact. Unavoidable, there are still active power and frequency deviations (about 200W for active power and 0.02Hz for frequency) because the optimal data exchanging way is also being attacked.



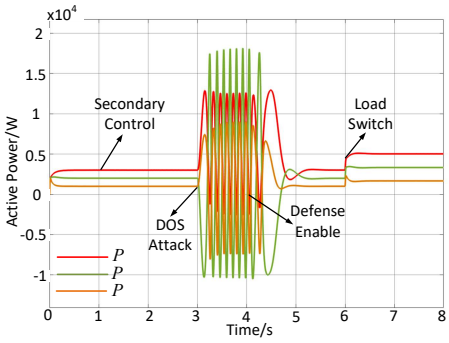
(a) Frequency performance under FDIA



(b) Frequency performance under DoS

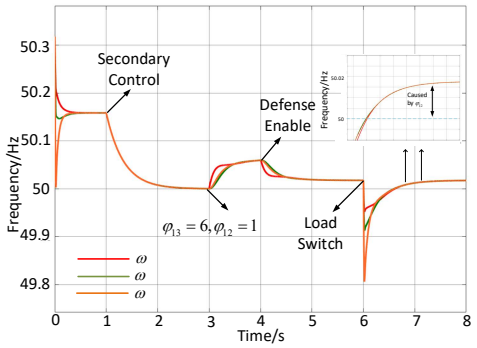


(c) Active power performance under FDIA

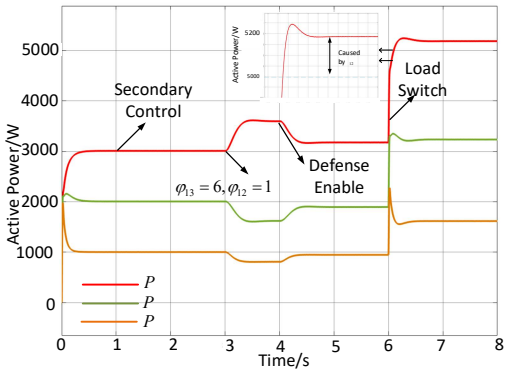


(d) Active power performance under DoS

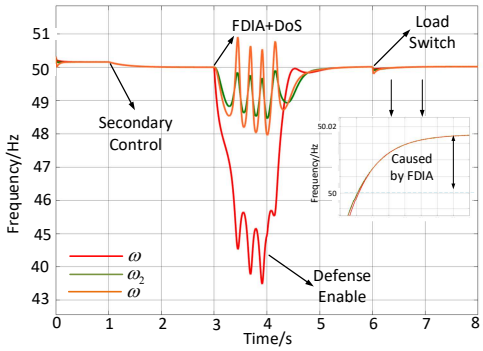
Figure 4 Performers of frequency and active power under FDIA and DoS



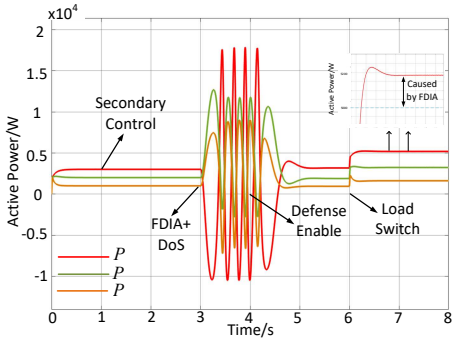
(a) Frequency performance under 2FDIA



(b) Active power performance under 2FDIA



(c) Frequency performance (FDIA+DoS)



(d) Active power performance (FDIA+DoS)

Figure 5 Performance of converter when all neighbors are under attacks

V. Conclusion

This paper presents a novel adaptive control scheme for both FDIA and DoS attacks in the secondary-frequency layer of AC micro-grids. The proposed control framework offers real-time adjustable communication weight, it guarantees frequency synchronization and active power-sharing. when data delivery is attacked, the adaptive scheme updates an optimal communication line to dampen the attack influence. Moreover, if all communication lines to its neighbors are attacked, the microgrid controller will choose a less infected line to propagate information among converters. The performance of the proposed secondary frequency control is evaluated under different combined attack case studies.

VI. Appendix

$$P_{1ref} = 6000, P_{2ref} = 4000, P_{3ref} = 2000, m_{P1} = 1/6000, m_{P2} = 1/4000,$$
$$m_{P3} = 1/2000, Z_N = 0.321 + 0.003j, \omega_{ref} = 314 rad/s, L_{filter} = 3mH,$$
$$C_V = 30\mu F, V_{ref} = 190V, \xi_{ij} = 0.01, \kappa_{ij} = 3.$$

References

[1] Wang Y, Wang Y, Huang Y, et al. Planning and operation method of the regional integrated energy system considering economy and environment[J]. Energy, 2019, 171: 731-750.

[2] Tuyen, Nguyen Duc, et al. "A Comprehensive Review of Cybersecurity in Inverter-based Smart Power System amid the Boom of Renewable Energy." IEEE Access (2022).

[3] Bidram A, Davoudi A, Lewis F L. A multiobjective distributed control framework for islanded AC microgrids[J]. IEEE Transactions on industrial informatics, 2014, 10(3): 1785-1798.

[4] Beg O A, Johnson T T, Davoudi A. Detection of false-data injection attacks in cyber-physical DC microgrids[J]. IEEE Transactions on industrial informatics, 2017, 13(5): 2693-2703.

[5] Liu S, Hu Z, Wang X, et al. Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks[J]. IEEE Transactions on Industrial Informatics, 2018, 15(7): 4066-4075.

[6] Shahidehpour M, Tinney F, Fu Y. Impact of security on power systems operation[J]. Proceedings of the IEEE, 2005, 93(11): 2013-2025.

[7] Hardy T L. Software and System Safety: Accidents[J]. Incidents, and Lessons Learned, 2012: 223.

[8] Hardy T L. Software and System Safety: Accidents[J]. Incidents, and Lessons Learned, 2012: 223.

[9] Liang G, Weller S R, Zhao J, et al. The 2015 ukraine blackout: Implications for false data injection attacks[J]. IEEE Transactions on Power Systems, 2016, 32(4): 3317-3318.

[10] Guo L, Ye J, Yang B. Cyberattack Detection for Electric Vehicles Using Physics-Guided Machine Learning[J]. IEEE Transactions on Transportation Electrification, 2020, 7(3): 2010-2022.

[11] Leng M, Sahoo S, Blaabjerg F, et al. Projections of Cyber Attacks on Stability of DC Microgrids-Modeling Principles and Solution[J]. IEEE Transactions on Power Electronics, 2022.

[12] Sánchez H S, Rotondo D, Escobet T, et al. Bibliographical review on cyber attacks from a control oriented perspective[J]. Annual Reviews in Control, 2019, 48: 103-128.

[13] Cecilia, Andreu, et al. "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 (2021): 2801-2814.

[14] Manandhar K, Cao X, Hu F, et al. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter[J]. IEEE transactions on control of network systems, 2014, 1(4): 370-379.

[15] Wan Y, Dragicevic T. Data-driven Cyber-attack Detection of Intelligent Attacks in Islanded DC Microgrids[J]. IEEE Transactions on Industrial Electronics, 2022.

[16] Musleh A S, Chen G, Dong Z Y. A survey on the detection algorithms for false data injection attacks in smart grids[J]. IEEE Transactions on Smart Grid, 2019, 11(3): 2218-2234.

[17] Abhinav S, Modares H, Lewis F L, et al. Synchrony in networked microgrids under attacks[J]. IEEE Transactions on Smart Grid, 2017, 9(6): 6731-6741.

[18] Sahoo S, Yang Y, Blaabjerg F. Resilient synchronization strategy for AC microgrids under cyber attacks[J]. IEEE Transactions on Power Electronics, 2020, 36(1): 73-77.

[19] Lian Z, Guo F, Wen C, et al. Distributed Resilient Optimal Current Sharing Control for an Islanded DC Microgrid Under DoS Attacks[J]. IEEE Transactions on Smart Grid, 2021.

[20] Guerrero J M, Vasquez J C, Matas J, et al. Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization[J]. IEEE Transactions on industrial electronics, 2010, 58(1): 158-172.

[21] Sadabadi M S, Sahoo S, Blaabjerg F. A Fully Resilient Cyber-Secure Synchronization Strategy for AC Microgrids[J]. IEEE Transactions on Power Electronics, 2021.

[22] Abhinav S, Modares H, Lewis F L, et al. Resilient cooperative control of DC microgrids[J]. IEEE Transactions on Smart Grid, 2018, 10(1): 1083-1085.

[23] Sahoo S, Dragičević T, Yang Y, et al. Adaptive Resilient Operation of Cooperative Grid-Forming Converters Under Cyber Attacks[C]//2020 IEEE CyberPELS (CyberPELS). IEEE, 2020: 1-5.

[24] Habibi M R, Sahoo S, Rivera S, et al. Decentralized coordinated cyber-attack detection and mitigation strategy in DC microgrids based on artificial neural networks[J]. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2021.