Cyber Secure-Oriented Communication Network Design for Microgrids

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

DOI
10.1109/PEDG61800.2024.10667366

Publication date
2024

Document Version
Final published version

Published in
Proceedings of the 2024 IEEE 15th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)

2024 IEEE 15th International Symposium on Power Electronics for Distributed Generation Systems (PEDG) | 979-8-3503-6100-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/PEDG61800.2024.10667366

Cyber Secure-oriented Communication Network Design for Microgrids

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

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

Pavol Bauer
Electrical Sustainable Energy
Delft University of Technology
Delft, The Netherlands
P.Bauer@tudelft.nl

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

***Abstract*—The communication network used in distributed secondary control (DSC) for microgrid power and voltage regulation is vulnerable to cyber-attacks. Unlike the predominantly resilient research on secondary control, which tends to employ passive defense strategies, this paper presents a proactive defense mechanism to design a resilient network for microgrid secure operation. This proposed method involves preparing the resilient scheme before attacks occur and facilitates timely resilience during an attack. First, novel metrics are introduced to effectively quantify the impact of various cyber attacks. Then, a multiobjective optimization method is applied to design the communication graph considering the quantified attacks, convergence, time-delay robustness, and communication cost. Simulations are performed on a microgrid consisting of 10 inverter units under different scenarios to validate the effectiveness of the proposed methodology.**

***Index Terms*—AC microgrid, adaptive virtual impedance, power sharing, distributed control.**

I. Introduction

MICROGRIDS (MG), which manage the power of the distributed generators (DGs), are developing toward cyber-physical systems (CPSs) [1]. To achieve synchronization, distributed secondary control (DSC) schemes have been investigated within a decentralized framework by information exchange [2]–[4], while the communication networks deployed can potentially expose MGs to cyber-attacks. Current research primarily focuses on three types of attacks [5], [6]: false-data injection attacks (FDIA), denial-of-service (DoS) attacks, and multiple deliberate attacks (MDA).

From the perspective of CPS security in MG systems, a resilience-enhanced controller equipped with a detector is a traditional way to mitigate cyber-attacks. The model-based detector in [7] serves to identify FDIA in power systems. Model-free approaches, such as AI-based algorithms, have also been proven to be prospective methods for cyber-attack detection.

Resilience enhancement can be summarised as: 1) corrupted link isolated; 2) consensus gain adaptively tuning; 3) counteract the attack effect; 4) reconstruction of the corrupted signal. Specifically, in [8]–[10], the corrupted information from neighbors is discarded by managing the connectivity of communication graphs. Besides, in [11], the adaptive law-based approach is presented to promote microgrid resilience by adaptively modifying the consensus gain among the related agents. In [12], After identifying the cyber attack. Then, the loss caused by estimated false signals is compensated by the proposed method to counteract the cyber attack's impact. Event-driven mitigation strategy replaces the attacked signal with a reconstructed signal [13]. The corrupted data is reconstructed from the healthy channel data.

However, with the abovementioned method, the MGs can still not provide enough resilience against attack. The resilience scheme is ineffective when faced with combination attack [14]. Another pending issue is that applied resilient schemes restrict the number of infected agencies [15], and the existing scheme works after the attack occurs.

This paper investigates secure communication networks for MGs, constituting a proactive approach to attack prevention.

The balance between convergence, time delay robustness, and communication cost in the multi-agent systems is explored in [16]. The DSC communication scheme can be considered an undirected graph within the microgrids' control layer [17], [18]. Considering MDA's effect, a novel optimal network optimization method is presented in [6]. However, its applicability may be limited in more malicious MDA scenarios. Furthermore, these network design methods overlook the adverse effects of FDIA, which can significantly disrupt power-sharing dynamics and voltage recovery processes.

From the literature mentioned above, two noticeable research gaps can be found: 1) The existing works for attacks are mostly passive defense, and the resilient communication network design for proactive against cyber attack has not been thoroughly investigated. Therefore, there is still a need to develop a secure commutation graph for DSC in MGs. The main contributions are summarized as follows:

1) Based on the consensus-based protocol, a multi-objective optimization criterion is first presented for the network selection, considering the convergence performance, network-relevant time delays, communication costs, DoS, FDIA, and MDA. An optimal network is selected to meet the practical application requirements by obtaining the Pareto frontier of the multi-objective model.

2) Compared to the existing research, the FDIA and MDA quantified for communication graph design are first investigated, enhancing resilience against cyber attacks.

II. Communication-based cooperative secondary control strategy microgrid

In an islanded MG, as shown in Fig.1, using different loads makes it necessary to regulate the active and reactive power properly. This paper uses communication-based distributed secondary control to coordinate the involved converters.

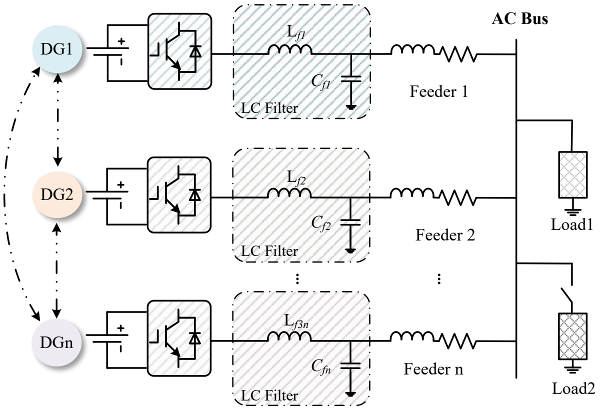

Fig. 1: The microgrid structure with coordinated control consisting of n converters.

A. Droop Law based-Primary Control

Droop control is the most widely used primary control strategy for islanded AC microgrids. Here, we mainly investigate the output angular frequency ω_i, filter voltage amplitude V_i, inverter output active power P_i, and reactive power Q_i.

Droop control philosophy ensures equal active power-sharing. The P-ω and Q-V droop control mechanism can be written as (4):

$$\omega_i = \omega_0 + m_i P_i, V_i = V_0 + n_i Q_i. \tag{1}$$

where the m_i and n_i are droop coefficients. ω_0 and V_0 are the nominal frequency and voltage set points, respectively. Notably, the active and reactive power should be proportionally shared in the steady state according to its maximum capacity, while the voltage and frequency are restored to the nominal value. The control objective for the microgrid can be represented as follows:

$$\lim_{i\to\infty} \omega_i(t) = \omega_0, \lim_{i\to\infty} m_i P_i(t) = \lim_{i\to\infty} m_j P_j(t) \tag{2}$$

$$\lim_{i\to\infty} V_i(t) = V_0, \lim_{i\to\infty} n_i Q_i(t) = \lim_{i\to\infty} n_j Q_j(t) \tag{3}$$

III. Distributed Secondary Control

A. Preliminaries on Graph Theory

Here, we investigate an islanded AC microgrid consisting of n DGs. The communication between these DGs is modeled by an undirected graph $\hat{G}$. Mathematically, the graph can be characterized by an adjacency matrix $A = [a_{ij}]_{n\times n}$. If there is regular communication between DGi and DGj,$a_{ij} = 1$, or else, $a_{ij} = 0$. As $\hat{G}$ is regarded as an undirected graph, $a_{ij} = a_{ji}$, and it can be denoted by d_i, where $d_i = \sum_{j=1}^{n} a_{ij}$. $D = diag\{D_1, \cdots, d_n\}$ represents the degree matrix in the undirected graph. In addition, the Laplacian matrix of G satisfies the relationship $L = D - A$.

B. Design of Coordinated Secondary Control

The secondary control layer modifies the droop law by:

$$\omega_i = \omega_0 + m_i P_i + \omega_{si}, V_i = V_0 + n_i Q_i + V_{si}. \tag{4}$$

where ω_{si} and V_{si} denotes the secondary control compensation term. The secondary lay compensation is given by:

$$u_i(t) = \sum_{x_j \in N_i} a_{ij}[x_j(t) - x_i(t)] + g_i[x_i(t) - x_0] \tag{5}$$

where x_i represents the the local unit's state, ω_i, $\bar{V}_i$, $m_i P_i$,$n_i Q_i$. $\bar{V}_i$ denotes the estimated global average voltage [18], which can be obtained by the dynamic average algorithm: $\bar{V}_i = V_i(t) + C_E \int \sum_{j\in N_i} a_{ij}(\bar{V}_j - \bar{V}_i)dt$.

IV. Communication Network design

In this section, to design an optimal communication network, we mainly establish six optimization indexes for the communication network design: convergence performance, robustness to communication delay, communication cost, and the three different kinds of adverse cyber attack effects.

A. Convergence rate, Time-delay Robustness and Cost

The secondary control can be considered as an undirected graph with balanced information flow, where g_i in (5) equals zero. This consensus law can decompose the state x as $x = \alpha 1 + \xi$. $\alpha 1 = Ave(x)$ is an invariant quantity [16], $\alpha 1 = \sum_i^n x_i(0)/n$, and $\xi \in \mathbb{R}^n$ satisfies $\sum_i^n \xi_i = 0$. We refer to ξ as the (group) disagreement vector of L, provided that $\hat{G}$ is connected.

With fixed topology, the error is given by:

$$\xi \leq \xi(0)exp(-\kappa t) \tag{6}$$

where $\kappa = \lambda_2(L)$, representing the second smallest eigenvalues, defined as the algebraic connectivity of the connected graph [16]. Therefore, we set $F_1(\hat{G}) = -\lambda_2(L)$ as the cost function to represent the converge speed.

Incorporating a communication network introduces time delays in MGs' control. This can potentially delay the convergence of system states and degrade the system's dynamic performance, even resulting in instability.

From the Geršgorin theorem, we know that $\lambda_{max}(L) \leq 2d_{max}(\hat{G})$. $d_{max}(\hat{G})$ is the maximum out-degree of the nodes of $\hat{G}$. Therefore, a sufficient condition for protocol convergence is shown in (7).

$$\tau_{ij} \in [0, \tau^*], \tau^* \leq \frac{\pi}{2\lambda_{max}(L)} \tag{7}$$

τ^* is the maximum communication time delay. Here we set the cost function as: $F_2(\hat{G}) = 4d_{max}(\hat{G})/\pi$.

A crucial consideration in distributed multiagent systems involves minimizing communication expenses. We define the communication cost or communication complexity, denoted as C, in relation to the total count of directed edges within the graph $\hat{G}$, as denoted by $F_3(\hat{G}) = C = \sum_{i=1}^{n} d_i/2$:

B. Invulnerability Design of Communication Network

As it was reported, cyber attacks can cause suboptimal control or even instability. DoS, FDIA, and MDA have been considered in this paper.

1) Metric of DoS attack effect: Based on the above-mentioned conclusions, we define the attack metric $F_4(\hat{G})$ as follows:

$$F_4(\hat{G}) = 1/[1 + \lambda_2(L)] \tag{8}$$

When the communication link suffers DoS attacks, with a smaller attack metric $F_4(\hat{G})$, the graph features a better convergence connectivity.

2) Metric of FDIA effect: FDIA on the information propagation channel from the neighbor can be modeled in $x_{a,j} = x_j + \varepsilon(t)$. Where $x_{a,j}$ denotes the transmitted information corrupted by the cyber attack. x_j represents the real frequency signal of the jth agent. ε_i is the malicious signal.

Take the active power-frequency loop as an example. $\delta i = m_i P_i$. Considering FDIA, the neighbor's frequency ω_j can be changed to $\omega_j + \varepsilon$. With the FDIA, the global auxiliary control input is written as:

$$-[\dot{\omega} + \dot{\delta}] = (L + G)(\omega - \omega_0) + L\delta + B\varepsilon \tag{9}$$

where $B = diag\{b_1, \cdots, b_n\}$, b_i is the corresponding matrix of FDIA. In a power system, all the DGs' frequencies synchronize to the common microgrid frequency in the steady state. Therefore, one can obtain $L\omega = 0$. Setting the left side of (9) equal to zero, yields:

$$L\delta + G(\omega - \omega_0) + B\varepsilon = 0 \tag{10}$$

$b_i\varepsilon_i \neq 0$ means the neighbor selected DGs is under FDIA. In this case, (10) can be written as (11):

$$\begin{bmatrix} \sum\limits_{j=1}^{n} a_{1j} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \sum\limits_{j=1}^{n} a_{2j} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} \delta_1 \\ \delta_2 \\ \vdots \\ \sum\limits_{i=1}^{n} \delta_i \end{bmatrix} + \begin{bmatrix} g_1(\omega_1 - \omega_0) \\ g_2(\omega_2 - \omega_0) \\ \vdots \\ \sum\limits_{i=1}^{n} g_i(\omega_i - \omega_0) \end{bmatrix} + \begin{bmatrix} b_1\varepsilon_1 \\ b_2\varepsilon_2 \\ \vdots \\ \sum\limits_{i=1}^{n} b_i\varepsilon_i \end{bmatrix} = 0 \tag{11}$$

One can obtain the relationship between the attack element and frequency by solving the matrix of (11). As the frequency of each inverter is the same in the state, which in turn yields:

$$\omega_i = \omega_0 + \sum_{i=1}^{N} b_i\varepsilon_i / 1_N^T G 1_N, i \in N \tag{12}$$

The effect of FDIA on frequency performance is $\sum_{i=1}^{N} b_i\varepsilon_i/(1_N^T G 1_N)$. The frequency is independent of the communication matrix L. Attack elements and the reference node determine the frequency error.

In addition, frequency convergence has been known to synchronize to a common value, even under FDIA [8]. However, the dynamic frequency adjustment will cause phase differences, which may result in improperly shared output power. Therefore, one can establish an index to quantify the FDIA on power-sharing performance as $F_5(\hat{G})$.

$$\Lambda(i) = \{l(i,1), l(i,1) \cdots l(i,j)\}, j \in N \tag{13}$$

where $l_{i,j}$ denotes the length of links directed from the node j to node $i.\Lambda(i)$ represents a vector that is composed of the length of the communication path from every node in the graph to node i. $F_5(\hat{G}) = max\_Var\{\Lambda(i)\}, i \in N$. $F_5(\hat{G})$ denotes the propagation rate from one DG to the remaining per unit time. *Var*$\Lambda(i)$ denotes the variance of the vector, signifying the difference in time consumption for the error information transmitted from node i to other nodes. The *max* function selects the maximum variance to account for the worst-case scenario.

3) Metric of MDA effect: The MDA means the hacker launches an indiscriminate attack on each node. Once hackers access relevant information about the communication topology through special means, they will precisely strike some communication nodes selectively. Thus, when subjected to MDA in MGs, the attacked inverter is forced to be plugged out.

$F_6(\hat{G})$ denotes the survivability of the networked system when it is under deliberate attack.

$$F_6(\hat{G}) = \sum_{m=1}^{n} [n_m - rank(L_m)]/m^2 \tag{14}$$

where m represents how many DGs are disconnected from the microgrid due to the deliberate cyber attack.n_m represents how many DGs are in operational after m is attacked. L_m is the Laplacian matrix, when m units are out from the graph.

C. Communication Design

We formulate an optimization problem aimed at reconfiguring the network's topology. This formulation considers six key performance indices. Then, a multi-objective optimization method is developed with the objective of minimum cost function and maintaining cyber connectivity for n-DGs, therefore capturing the optimal network as shown in (15):

$$\begin{aligned} minF = (&\vartheta_1 \frac{F_1 - F_{1,min}}{F_{1,max} - F_{1,min}} + \vartheta_2 \frac{F_2 - F_{2,min}}{F_{2,max} - F_{2,min}} \\ &+ \vartheta_3 \frac{F_3 - F_{3,min}}{F_{3,max} - F_{3,min}} + \vartheta_4 \frac{F_4 - F_{4,min}}{F_{4,max} - F_{4,min}} \\ &+ \vartheta_5 \frac{F_5 - F_{5,min}}{F_{5,max} - F_{5,min}} + \vartheta_6 \frac{F_6 - F_{6,min}}{F_{6,max} - F_{6,min}}) \end{aligned} \tag{15}$$

where F_1-F_6 represent different objective functions, corresponding to convergence performance, robustness to time delays, and cost-effectiveness, metrics of DoS, FDIA, and MDA, respectively. ϑ_1-ϑ_6 are the weights corresponding to $F_1(\hat{G})$-$F_6(\hat{G})$. $F_{i,min}$ and $F_{i,max}$ are the $minimum$ and $maximum$ values of the corresponding functions of candidate topologies, which can be obtained by solving the corresponding single-objective optimization problem.

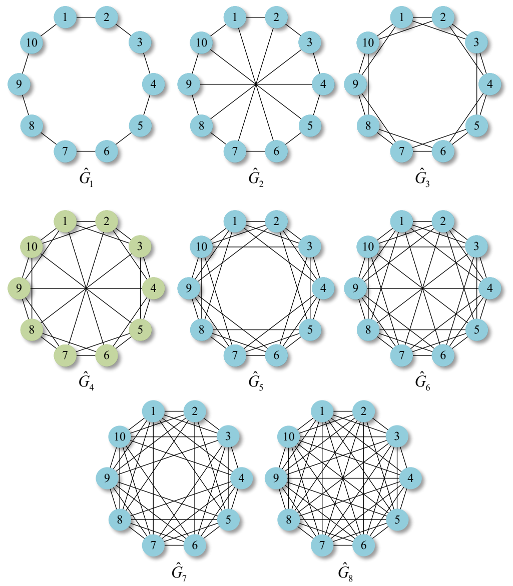

Fig. 2: The candidate optimal communication network.

V. Simulink Results

The efficiency of the proposed optimal design algorithm for distributed secondary control is evaluated using a real-time simulator, OPAL-RT. The experimental setup is illustrated in Figure 1. Specifically, the study focuses on a test microgrid (MG) configuration consisting of 10 DGs with various power ratings, all connected to a shared voltage bus. Notably, the output active power and reactive power sharing ratio are set as $DG1 : DG2 : DG3 : DG4 : DG5 : DG6 : DG7 : DG8 : DG9 : DG10 = 1 : 1.5 : 2 : 2.5 : 3 : 3.5 : 4 : 4.5 : 5 : 5.5$. As we enable the secondary control, the active and reactive power can be facilitated proportionally shared, and frequency and global voltage amplitude can be restored to reference.

TABLE I: Optimal design under different graph

Graph	F_1	F_2	F_3	F_4	F_5	F_6	F
$\hat{G}_1$	-0.38	2.55	10	0.72	1.94	2.00	0.667
$\hat{G}_2$	-1.38	3.82	15	0.42	0.61	1.47	0.410
$\hat{G}_3$	-1.76	5.09	20	0.36	0.50	1.25	0.389
$\hat{G}_4$	**-3.76**	**6.37**	**25**	**0.21**	**0.28**	**1.19**	**0.332**
$\hat{G}_5$	-4.38	7.64	30	0.19	0.25	1.10	0.345
$\hat{G}_6$	-6.38	8.91	35	0.14	0.19	1.08	0.335
$\hat{G}_7$	-8	10.19	40	0.11	0.11	1.06	0.338
$\hat{G}_8$	-10	11.46	45	0.09	0	1.04	0.333

The number of edges for the network with ten units should be between 9 and 45. As discussed above, it is essential to maximize the plug and operation for a microgrid, which requires the degree of nodes in this communication topology to be evenly distributed and all nodes to have the same degree. This can be the mandatory requirement for choosing a feasible network. Based on this, there are still different communication structures for giving communication links and ”degree evenly distributed,”. A more symmetrical communication graph can provide greater resilience to deliberate cyber-attacks, as shown in the comparative study. Based on this, the candidate optimal graph can be obtained as $\hat{G}_1 - \hat{G}_8$ in Fig.2.

According to the cos function in 15, the Pareto frontiers value is shown in Tab.I. According to the cos function in 15, the Pareto frontiers value is shown in Tab.I.As the cost function of $\hat{G}_4$ is the smallest. Therefore, $\hat{G}_4$ is selected as the optimal communication network. Herein, $\vartheta_1 = \vartheta_2 = \vartheta_3 = \vartheta_4 = \vartheta_5 = \vartheta_6 = 1/6$ is used for optimization.

1) Optimal communication network validation: To demonstrate that the optimized communication topology has good dynamic performance, we test the $\hat{G}_4$ in Fig.2 under communication delay, load switch, and plug-and-play operation.

Fig.3 shows the performance of the optimal graph. The responses of the output active power, frequency, reactive power, and global of the involved inverters are displayed in Fig.3(a),(b),(c),(d) respectively. $100ms$ time delay is imposed in the system, which is reported to be the common delay in microgrids [19].

After the distributed secondary control is enabled at $2s$, the reactive power can be proportionally shared while the frequency and global voltage amplitude are recovered to its reference. Then, there is a load increase $(3250W)$ for active and reactive power at $5s$ and $10s$, respectively. The power, frequency, and voltage can converge. At $15s$, DG1, DG2, and DG3 drop out, while the remaining inverters (DG4-DG10) can keep synchronization with an acceptable fluctuation.

2) Comparative study I: In order to confirm the validity of the proposed network design methodology, we take the optimal communication network with 14 edges, proposed in [18] depicted in Fig. 4 as a comparison counterpart. we develop a 14-edged optimal network with the proposed method to make the comparison fairer.

This section provides a comprehensive investigation of the performance of communication networks when the system is under FDIA. Fig.4 and Fig.5 showcase the active power sharing coefficient (m_iP_i), frequency (f_i), reactive power sharing coefficient (n_iQ_i) and estimated global voltage $(\bar{V}_i)$. Secondary control is enabled at $2s$, and synchronization is gradually researched, where $m_1P_1 = m_2P_2 = \cdots = m_{10}P_{10} = 0.5$, $n_1Q_1 = n_2Q_2 = \cdots = n_{10}Q_{10} = -0.5$.

As shown in Fig.4, FDIA is launched at $10s$. The communication link from DG10 to DG1 is attacked, leading to a $2200W$ false data being inserted into the original data for both active and reactive power. With the FDIA, the frequency is driven to 50.02, while the global voltage is changed to 190.25. Moreover, the power can not be proportionally shared, and the sharing coefficient is largely distributed. However, as shown in Fig.5, the same FDIA will lead to a smaller distributed power-sharing coefficient. This means that the proposed optimal network can decrease the effect of FDIA.

3) Comparative study II: A capacitive study is conducted compared to the research in [6] to investigate the benefit of the proposed network against MDA. Fig.6 and Fig.7 indicate different networks when MDA challenges the system, which

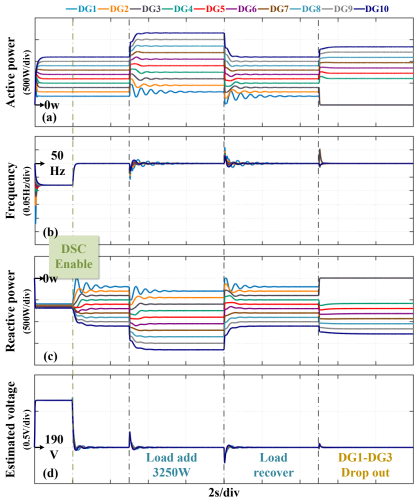

Fig. 3: Dynamics of optimal graph $\hat{G}_4$ under $100ms$ delay.

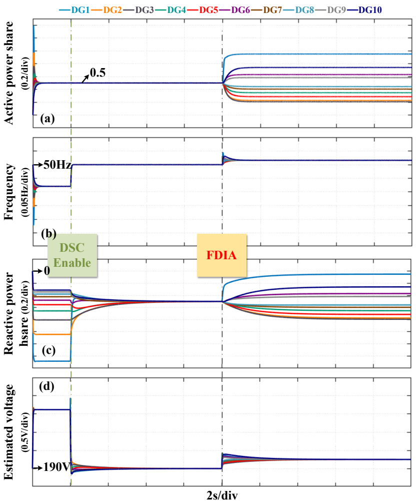

Fig. 4: Dynamics of the optimal graph in [18] with 14 edges under FDIA.

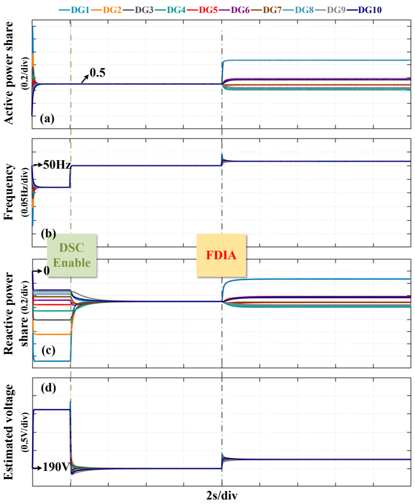

Fig. 5: Dynamics of the proposed optimal with 14 edges under FDIA.

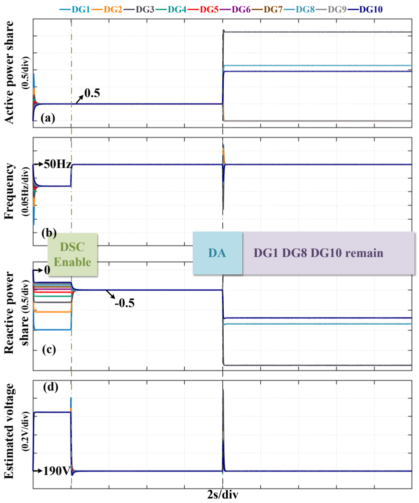

Fig. 6: Dynamics of the optimal graph in [6] with 30 edges under MDA.

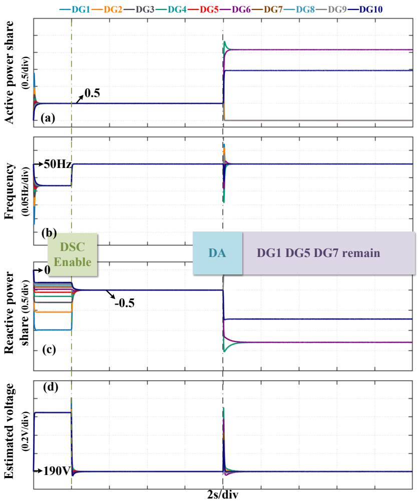

Fig. 7: Dynamics of the proposed graph with 30 edges under MDA.

will cause 7 DGs to disconnect the microgrid. The hacker attempted to destroy the synchronization of the optimal graph in [6].With preknowledge of the graph, the worst case with 7 is drop out, DG1, DG8, and DG10 remain in the microgrid. With this configuration, there are three isolated islands. However, with the worst MDA, DG1, DG5, and DG7 are kept for the optimal graph using the proposed method. There are only two isolated islands. The proposed optimal graph can support more convergence under the DA compared to the method in [6].

VI. Conclusion

This proposed approach entails the preparation of a resilient scheme prior to potential attacks, enabling prompt resilience during an attack occurrence. Initially, novel metrics are introduced to quantify the impact of denial of service, false data injection attacks, and multiple deliberate attacks effectively. Subsequently, a multiobjective optimization technique is employed to devise the communication graph, taking into account the quantified attacks, convergence, time-delay robustness, and communication cost. Simulations are conducted on a microgrid comprising 10 inverter units across various scenarios to validate the efficacy of the proposed methodology.

References

[1] X. Yu and Y. Xue, “Smart grids: A cyber–physical systems perspective,” *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058–1070, 2016.

[2] J. Xiao, L. Wang, Z. Qin, and P. Bauer, “An adaptive cyber security scheme for ac micro-grids,” in *2022 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2022, pp. 1–6.

[3] J. W. Simpson-Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero, and F. Bullo, “Secondary frequency and voltage control of islanded microgrids via distributed averaging,” *IEEE Transactions on Industrial Electronics*, vol. 62, no. 11, pp. 7025–7038, 2015.

[4] J. Xiao, L. Wang, Z. Qin, and P. Bauer, “An adaptive virtual impedance control for reactive power sharing in microgrids,” in *2023 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2023, pp. 584–589.

[5] ——, “A resilience enhanced secondary control for ac micro-grids,” *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 810–820, 2024.

[6] L. Sheng, G. Lou, W. Gu, S. Lu, S. Ding, and Z. Ye, “Optimal communication network design of microgrids considering cyber-attacks and time-delays,” *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 3774–3785, 2022.

[7] J. Xiao, L. Wang, Z. Qin, and P. Bauer, “Detection of cyber attack in smart grid: A comparative study,” in *2022 IEEE 20th International Power Electronics and Motion Control Conference (PEMC)*. IEEE, 2022, pp. 48–54.

[8] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, “A cyber-attack resilient distributed control strategy in islanded microgrids,” *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3690–3701, 2020.

[9] J. Xiao, L. Wang, P. Bauer, and Z. Qin, “Virtual impedance control for load sharing and bus voltage quality improvement in low voltage ac microgrid,” *IEEE Transactions on Smart Grid*, pp. 1–1, 2023.

[10] J. Xiao, L. Wang, Z. Qin, and P. Bauer, “Virtual impedance control for load sharing and bus voltage quality improvement,” in *2023 25th European Conference on Power Electronics and Applications (EPE’23 ECCE Europe)*, 2023, pp. 1–8.

[11] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, “Synchrony in networked microgrids under attacks,” *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6731–6741, 2017.

[12] Y. Jiang, Y. Yang, S.-C. Tan, and S. Y. Hui, “Distributed sliding mode observer-based secondary control for dc microgrids under cyber-attacks,” *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 1, pp. 144–154, 2021.

[13] J. Zhang, S. Sahoo, J. C.-H. Peng, and F. Blaabjerg, “Mitigating concurrent false data injection attacks in cooperative dc microgrids,” *IEEE Transactions on Power Electronics*, vol. 36, no. 8, pp. 9637–9647, 2021.

[14] J. Chen, L. Wang, L. Diao, H. Du, and Z. Liu, “Distributed auxiliary inverter of urban rail train—load sharing control strategy under complicated operation condition,” *IEEE Transactions on Power Electronics*, vol. 31, no. 3, pp. 2518–2529, 2015.

[15] L. Meng, X. Zhao, F. Tang, M. Savaghebi, T. Dragicevic, J. C. Vasquez, and J. M. Guerrero, “Distributed voltage unbalance compensation in islanded microgrids by using a dynamic consensus algorithm,” *IEEE Transactions on Power Electronics*, vol. 31, no. 1, pp. 827–838, 2015.

[16] R. Olfati-Saber and R. Murray, “Consensus problems in networks of agents with switching topology and time-delays,” *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1520–1533, 2004.

[17] W. Yao, Y. Wang, Y. Xu, and C. Deng, “Cyber-resilient control of an islanded microgrid under latency attacks and random dos attacks,” *IEEE Transactions on Industrial Informatics*, vol. 19, no. 4, pp. 5858–5869, 2023.

[18] G. Lou, W. Gu, J. Wang, W. Sheng, and L. Sun, “Optimal design for distributed secondary voltage control in islanded microgrids: Communication topology and controller,” *IEEE Transactions on Power Systems*, vol. 34, no. 2, pp. 968–981, 2019.

[19] C. Kalalas, L. Thrybom, and J. Alonso-Zarate, “Cellular communications for smart grid neighborhood area networks: A survey,” *IEEE Access*, vol. 4, pp. 1469–1493, 2016.