Cyber Resilient Communication Network Design for Secondary Control of Microgrids

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

DOI
10.1109/TII.2025.3558327

Publication date
2025

Document Version
Final published version

Published in
IEEE Transactions on Industrial Informatics

Citation (APA)
Xiao, J., Wang, L., Shafiee, Q., Bauer, P., & Qin, Z. (2025). Cyber Resilient Communication Network Design for Secondary Control of Microgrids. *IEEE Transactions on Industrial Informatics*, *21*(8), 6071-6080. https://doi.org/10.1109/TII.2025.3558327

Cyber Resilient Communication Network Design for Secondary Control of Microgrids

Junjie Xiao, *Graduate Student Member, IEEE*, Lu Wang, *Member, IEEE*, Qobad Shafiee, *Senior Member, IEEE*, Pavol Bauer, *Senior Member, IEEE*, and Zian Qin, *Senior Member, IEEE*

***Abstract*—Distributed secondary control achieves voltage restoration and power sharing through communication among adjacent units but exposes the microgrid to potential cyber-attacks. Traditional mitigation strategies modify the secondary controller after the attack, addressing the issue only postoccurrence. Furthermore, in microgrid planning, the structure of the communication network significantly influences the resilience to attacks, but it remains to be explored. This article presents a proactive defense mechanism by designing a resilient communication network. The proposed method quantifies the impact of attacks and develops a multiobjective optimization algorithm to design the network, considering quantified attacks, convergence, time-delay robustness, and communication costs. The method is validated through OPAL-RT simulations of an islanded microgrid with ten converters.**

***Index Terms*—Communication network, cyber security, distributed secondary control (DSC), multiobjective optimization.**

I. Introduction

MICROGRIDS (MGs) commonly adopt the P-f and Q-V droop control laws in the primary layer [1]. In the secondary layer, the distributed secondary control (DSC) method is used to enhance power sharing and achieve voltage restoration [2], regardless of the initial configuration caused by variations in the properties of distributed generators (DGs).

In practice, communication networks used for DSC are subject to constraints. For example, communication delays are expected to adversely affect system performance [3], [4]. Furthermore, cyber-attacks on communication channels can be more precarious. It may lead to bus voltage deviations and power sharing inaccuracies, ultimately jeopardizing the stability of the system. Three types of attacks are primarily focused: false-data injection attacks (FDIA) [5], denial-of-service (DoS) attacks [6], and multiple deliberate attacks (MDA) [7]. FDIA aims to manipulate transmitted information to disrupt system operation by injecting false data alongside actual transmitted data. DoS attacks can impair specific communication channels, rendering neighboring data inaccessible and, consequently, disrupting the connectivity of the communication system topology. With preknowledge of the communication topology, MDA targets crucial agents [7], posing a higher risk to the integrity of the system. Such MDA may subject targeted inverters to sustained and aggressive assaults, potentially resulting in unplanned DG plug-out.

Current research for attack defense is mainly passive, developing resilience-enhanced controllers equipped with an attack detector in the secondary control layer. For example, a model-based detector proposed in [8] identifies FDIA for attack detection. However, malicious attacks with deep information can impede state estimation [9], [10]. Model-free methods using AI-based algorithms [11] are used to detect attacks. Nevertheless, such methods require extra computing. Moreover, complex detections can lead to delayed responses [12].

The typically adopted resilient schemes for DSC against cyber-attacks can be summarized as follows: 1) isolation of corrupted links, 2) adaptive tuning of consensus gains, 3) counteraction of attack effects, and 4) reconstruction of corrupted signals. Specifically, in [6], [13], and [14], corrupted information from neighboring nodes is discarded by managing the connectivity of the communication network, thereby mitigating the effect of cyber-attacks. Furthermore, in [15] and [16], an adaptive law-based method is introduced to enhance the resilience of the distributed system by dynamically adjusting the consensus gain across the associated agents based on the evaluation of attack strength. In addition, cyber-attack mitigation strategies, once an attack is identified, involve counteracting the losses caused by estimated false signals [17], [18], [19]. An event-driven mitigation strategy has been proposed, which replaces attacked signals with reconstructed signals from healthy channels [20], [21]. While reconstructing corrupted data from healthy channel sources is beneficial [22], its effectiveness is significantly reduced when multiple channels are compromised.

Despite these efforts, current strategies cannot provide MGs sufficient resilience against attacks. For example, the deficiency becomes apparent when the prevailing detection methods struggle to ensure system recovery under severe conditions [12]. Moreover, the resilience scheme proves inadequate when faced

Received 14 December 2024; revised 7 March 2025; accepted 29 March 2025. Date of publication 28 April 2025; date of current version 9 July 2025. This work was supported by Chips Joint Undertaking under Grant 101139790 and its members, including the top-up funding by Germany, Italy, Slovakia, Spain and The Netherlands. Paper no. TII-24-6721. *(Corresponding author: Zian Qin.)*

The authors are with the DC System, Energy Conversion, and Storage Group, Faculty of Electrical Engineering, Mathematics, and Computer Science, Delft University of Technology, 2628 Delft, The Netherlands (e-mail: J.Xiao-2@tudelft.nl; L.Wang-11@tudelft.nl; q.shafiee@tudelft.nl; P.Bauer@tudelft.nl; z.qin-2@tudelft.nl).

Digital Object Identifier 10.1109/TII.2025.3558327

TABLE I
COMPARISON OF THE METHODS FOR ENHANCING MG CYBER SECURITY

Type	Defence	Method	Reference	Description	DoS	FDIA	MDA
Passive	detection	model based	[8]	model inaccuracy	\	\	\
		data driven	[10] and [11]	computational burden	\	\	\
	resilience	isolate corrupted	[6], [13], and [14]	degrade connectivity	\	\	\
		adaptive gain	[15] and [16]	hybrid attack ineffective	\	\	\
		counteract attack	[17], [18], and [19]	time consuming	\	\	\
		reconstruct signal	[20], [21], and [22]	limit infected sets	\	\	\
Proactive	resilience	optimal network design	[26] and [27]	converge, delay, cost	×	×	×
			[7]	prone to severe MDA	✓	×	✓✗
	resilience	optimal network design	this article	resilience oriented design	✓	✓	✓

with combined attacks [23], [24]. Furthermore, commonly existing approaches are limited by their tendency to restrict the number of affected entities [16], [25].

One critical point is that with the abovementioned resilient scheme, modifications to the secondary control only ensure passive resilience, activated after an attack has occurred and been detected. In addition, the different communication structures have been proven to affect secondary control performance significantly [6], [26], [27]. In the multiagents field, communication network optimization, which considers the tradeoff between convergence, time-delay robustness, and communication cost, has been explored in [26].

These considerations and the effects of cyber-attacks are also crucial in MGs, where they influence network design for DSC [6], [27]. For instance, the impact of DoS attacks on communication networks is thoroughly investigated in [6], highlighting their potential to degrade system performance. Moreover, to account for the effect of MDA, an optimal network optimization method is proposed in [7], ensuring both time-delay robustness and convergence while addressing potential cyber threats. However, its applicability is limited when facing more sophisticated and malicious MDA scenarios, which is one of the aims to address in this article. In addition, these network design strategies often overlook the disruptive impact of FDIAs [7], [26], [27], which can severely compromise MG consensus and stability. Motivated by these challenges, this work proposes a communication network that proactively enhances resilience against DoS, FDIA, and MDA.

As summarized in Table I, the literature highlights a notable research gap: they predominantly focus on secondary controller modifications against attacks, while communication network design, which can offer extra resilience, has not been adequately studied. Consequently, this article involves designing the communication network to enhance privacy and resilience, allowing MGs to be less affected by cyber-attacks. The main contributions are summarized in the following.

1) A communication network topology is designed using a multiobjective optimization approach, considering convergence behavior, robustness to delays, communication costs, and resilience against DoS, FDIA, and MDA.
2) Unlike the passive defense schemes in [6], [8], [10], [11], [13], [14], [15], [16], [17], [18], [19], [20], [21], and [22], the proposed method takes a proactive approach, enabling faster recovery and enhanced privacy in the presence of cyber threats.

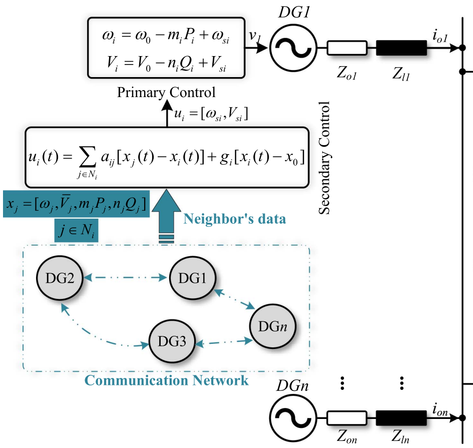
$\omega_i = \omega_0 - m_i P_i + \omega_{si}$
$V_i = V_0 - n_i Q_i + V_{si}$
v_1
DG1
Z_{o1}
Z_{l1}
i_{o1}
Primary Control
$u_i = [\omega_{si}, V_{si}]$
$u_i(t) = \sum_{j\in N_i} a_{ij}[x_j(t) - x_i(t)] + g_i[x_i(t) - x_0]$
Secondary Control
$x_j = [\omega_j, \bar{V}_j, m_j P_j, n_j Q_j]$
$j \in N_i$
Neighbor's data
Load1
Load2
DG2
DG1
DG3
DGn
Communication Network
DGn
Z_{on}
Z_{ln}
i_{on}

Fig. 1. Configuration of the AC MG with DSC.

3) Compared to the existing communication graph design methods in [7], [26], and [27], our approach not only optimizes the network for performance but also explicitly accounts for resilience against FDIA and MDA attacks, ensuring improved security.

II. DISTRIBUTED SECONDARY CONTROL

In islanded MGs, as shown in Fig. 1, the secondary control is utilized to coordinate interconnected converters, ensuring both voltage restoration and power sharing. The employed communication network facilitates information propagation, ensuring efficient and coordinated performance. Here, Z_{oi} represents the output impedance of DGi, while Z_{li} corresponds to the feeder impedance, and v_1 is the output of the droop controller.

A. Preliminaries on Graph Theory

In this study, we examine a networked MG consisting of n DGs, where each unit exchanges information with its neighboring units through a communication network for control. The communication structure can be represented mathematically by an adjacency matrix, $A = [a_{ij}]_{n\times n}$. The communication weight $a_{ij} = 1$ if the ith unit and the jth unit are in regular communication; otherwise, $a_{ij} = 0$.

The communication network is $\hat{G}$ can be modeled by an undirected graph $\hat{G}$, so, $a_{ij} = a_{ji}$. It can also be denoted by d_i, where $d_i = \sum_{j=1}^{n} a_{ij}$. $D = \text{diag}\{d_1, \ldots, d_n\}$ represents the degree matrix in the undirected graph. In addition, the Laplacian matrix of $\hat{G}$ satisfies the relationship $L = D - A$, and its eigenvalue determines the global dynamic performance.

B. Design of DSC

The main goals of MGs in islanded are denoted as follows:

$$\lim_{t\to\infty} \omega_i(t) = \omega_0; \quad \lim_{t\to\infty} m_i P_i(t) = \lim_{t\to\infty} m_j P_j(t) \quad (1)$$

$$\lim_{t\to\infty} V_i(t) = V_0; \quad \lim_{t\to\infty} n_i Q_i(t) = \lim_{t\to\infty} n_j Q_j(t) \quad (2)$$

where m_i and n_i represent the droop factors. ω_i and V_i converge to their nominal values ω_0 and V_0 respectively. The active power (P_i) and reactive power (Q_i) are expected to be proportionally shared, and the voltage and frequency are restored to their nominal values in the steady state.

The control objective in (1) and (2) can be reached by modifying the droop control with the secondary control compensation term ω_{si} and V_{si}

$$\omega_i = \omega_0 - m_i P_i + \omega_{si}; \quad V_i = V_0 - n_i Q_i + V_{si}. \quad (3)$$

With the DSC [3], DGs propagate information through the prescribed communication network $\hat{G}$, as follows:

$$u_i(t) = \sum_{j\in N_i} a_{ij}[x_j(t) - x_i(t)] + g_i[x_0 - x_i(t)] \quad (4)$$

where $u_i(t)$ represents ω_{si} and V_{si}, N_i is the set of the ith DG's neighbor, x_i is the local unit's state, ω_i, $\bar{V}_i$, $m_i P_i$, and $n_i Q_i$, and $\bar{V}_i$ denotes the estimated global average voltage. For frequency and voltage control, the virtual leader is employed, $g_i = 1$, implying the DGs' state approaches the reference value x_0. Conversely, active power and reactive power sharing controllers, $g_i = 0$. Notably, we propose to recover the global average voltage $\bar{V}_i$ to a nominal value rather than each DG's voltage V_i [27], which can be obtained by the dynamic average algorithm, shown as follows. With this philosophy, the output voltages of all DGs lie within an acceptable range

$$\bar{V}_i = V_i(t) + \int \sum_{j\in N_i} a_{ij}(\bar{V}_j - \bar{V}_i)dt. \quad (5)$$

III. Communication Network Design

Fig. 1 illustrates an n-DG ac MG with secondary control, where the voltage and power control performance depends on information exchanged with neighboring units. This performance is highly influenced by the design of the communication network, which is the focus of this article.

This section presents six optimization criteria for designing an optimal communication network: convergence performance, resistance to communication delays, communication costs, and the negative impacts of three types of cyber-attacks.

A. Convergence Performance

1) For active power and reactive power sharing: The network can be modeled as an undirected graph, where $g_i = 0$. With this consensus law, the sum of the output of all units is invariant. The state x can be decomposed as

$$x = \alpha 1 + \xi \quad (6)$$

where $\alpha 1 = \text{Ave}(x)$ is an invariant quantity [26], $\alpha 1 = \sum_i^n x_i(0)/n$. The disagreement vector ξ satisfies $\sum_i^n \xi_i = 0$, and its dynamics is given by $\dot{\xi} = -L\xi$.

The solution to the disagreement is given by

$$\xi \leq \xi(0)\exp(-\kappa t) \quad (7)$$

where $\kappa = \lambda_2(L)$ is the second smallest eigenvalue, defined as the algebraic connectivity of the graph [26]. A well-known observation from the Fiedler eigenvalue is that for dense graphs, $\lambda_2(L)$ is relatively large. In contrast, for sparse graphs, $\lambda_2(L)$ is relatively small in $\hat{G}$.

2) For frequency and voltage controllers: Here, the global voltage restoration error is defined as $e(t) = x(t) - x_0$. Combining with (3) and (4), the error dynamics can be described as $\dot{e}(t) = -(L+G)e(t)$, and $G = \text{diag}(g_1, \ldots, g_N)$ is the pinning matrix in which $g_i = 1$. By injecting reference values into designated nodes, the interconnected nature of the underlying network ensures that the remaining nodes converge toward the reference state.

The Lyapunov function is selected as $V(t) = e(t)^T e(t)/2$, showing its deviation, and its dynamics as

$$\begin{aligned}\dot{V}(t) &= \frac{d}{dt}\left[\frac{1}{2}e(t)^T e(t)\right] = e(t)^T \dot{e}(t) \\ &= -e(t)^T(L+G)e(t) \leqslant -\lambda_{\min}(L+G)e(t)^T e(t) \\ &\leqslant -2\lambda_{\min}(L+G)V(t) \end{aligned} \quad (8)$$

where $2\lambda_{\min}(L+G)$ represents the corresponding convergence rate [13]. Since the minimum eigenvalue $(L+G)$ is positive-definite and inevitable, the disagreement e would eventually converge to zero, which means x_i will ultimately converge to x_0. Therefore, the control objective is reached.

In this scenario, a higher convergence rate indicates that pinned DGs communicate more effectively with unpinned units. Therefore, selecting pinning nodes usually aims to maximize the minimum eigenvalue of the Laplacian matrix $(L+G)$ to increase the convergence rate. However, as noted in [28], this upper bound is constrained by the second smallest eigenvalue of L, denoted as $\lambda_2(L)$. Given these considerations, we fix the number of pinning nodes while ensuring convergence to a reference state. Consequently, the primary focus for improving convergence performance lies in the design of the Laplacian matrix L. Therefore, we establish $F_1(\hat{G}) = -\lambda_2(L)$ as the cost function representing the convergence rate.

B. Robustness to Communication Delay

Incorporating a communication network introduces time delays in MGs' control [29]. Such delays can potentially delay the convergence of system states and degrade the system's dynamic performance, even resulting in instability.

To gain further insight into the relation between robustness to delay and connection, we ignore the pinning node since few nodes are selected for pinning control [30]. The dynamic of the consensus protocol in (4) with time delay is described in [7], [26], and [27], also shown as follows:

$$\dot{x}_i(t) = u_i = \sum_{j\in N_i} a_{ij}[x_j(t-\tau_{ij}) - x_i(t-\tau_{ij})] \tag{9}$$

where τ_{ij} is the delay of the communication. The Laplace transform of both sides of (9) is denoted as

$$sX_i(s) - x_i(0) = \sum_{j\in N_i} a_{ij}e^{-\tau_{ij}s}(X_j(s) - X_i(s)). \tag{10}$$

The Laplace transform of the above formula is

$$X(s) = (sI + e^{-\tau_{ij}s}L)^{-1}x(0). \tag{11}$$

From Gregorian theorem, we know that $\lambda_{\max}(L) \leq 2d_{\max}(\hat{G})$, where $d_{\max}(\hat{G})$ is the maximum degree of the nodes of $\hat{G}$, and $\lambda_{\max}(L)$ is the greatest eigenvalue of L. Therefore, a sufficient condition for network convergence is shown in (12). When the following condition is met, (9) can realize global asymptotic stability with time-delay τ_{ij} [30], and the state of x_i converges to the average value

$$\tau_{ij} \in [0, \tau^*], \tau^* \leq \frac{\pi}{2\lambda_{\max}(L)} \tag{12}$$

where τ^* is the maximum tolerable communication delay. The upper bound of the time delay in the network is inversely proportional to the largest eigenvalue of the Laplacian matrix. Since the proof of this bound has already been established in [26] as part of the graph theory validation, we omit it here for brevity. Accordingly, networks with nodes with relatively large degrees cannot tolerate high communication time delays. Based on this, we set the cost function as: $F_2(\hat{G}) = 4d_{\max}(\hat{G})/\pi$.

C. Communication Cost

A crucial consideration in distributed multiagent systems involves minimizing communication cost, denoted as C, which is the total count of edges within the graph $\hat{G}$, represented as

$$C = \sum_{i=1}^{n} d_i/2. \tag{13}$$

In general, more edges mean higher communication costs. Based on the network, the optimal objective is to minimize the required edges, denoted as $F_3(\hat{G}) = \sum_{i=1}^{n} d_i/2$.

D. Invulnerability Design of Communication Network

The proposed DSC framework heavily depends on exchanging parameters x_i among DGs, thereby rendering the MGs susceptible to cyber-attacks.

1) Model of the Cyber-Attacks: The cyber-attacks can be modeled as [5], [6], [7]

$$x_{a,j} = K_j[x_j + \eta_j\varepsilon(t)] \tag{14}$$

where $x_{a,j}$ represents the corrupted frequency, and x_j denotes the original signal from the jth agent. Both η_j and K_j are binary variables. When $\eta_j = 0$ and $K_j = 0$, the system is subjected to a DoS attack. $\eta_j = 0$ and $K_j = 1$ indicate that the MG system operates under normal conditions. $\eta_j = 1$ and $K_j = 0$ denote that the system faces both a DoS attack and an FDIA. $\eta_j = 1$ and $K_j = 1$ denote that the presence of an FDIA is indicated, characterized by the malicious element $\varepsilon(t)$. Furthermore, when subjected to MDA, DGs are forced to drop out, resulting in disconnection.

2) Metric of DoS Attack Effect: Based on the above discussions, the DoS attack metric $F_4(\hat{G})$ is defined as in [6]. According to this reference, an increase in algebraic connectivity reduces the impact of DoS attacks. This relationship is expressed as follows:

$$F_4(\hat{G}) = 1/[1 + \lambda_2(L)]. \tag{15}$$

When a DoS attack occurs, the information propagation is interrupted, resulting in a low convergence rate. Notably, with a more extensive convergence connectivity of the original network, the system features a minor effect of the DoS attack. For connected systems, the attack metric negatively correlates with the algebraic connectivity $\lambda_2(L)$.

3) Metric of FDIA Effect: We first reframe the f/V recover to a pinning synchronization problem. This approach allows a few DG to access predefined reference values while all other units synchronize via communication. The FDIA can be equivalently considered a modification of these reference values, as the attack elements in the neighbor can be mathematically written at the change of the reference value. Hence, its effect depends on the number of pinning nodes. Subsequently, we transform the P/Q sharing problem into an undirected graph consensus problem, where each DG adjusts its power outputs based on the outputs of its neighbors. Here, the influence of the FDIA on power sharing is mainly shaped by the differences in f/V propagation rates throughout the network.

Herein, the P-f is considered as an example for verification, and DSC is written as

$$\dot{\omega}_{si} = \sum_{j\in N_i} a_{ij}(\omega_j - \omega_i) + g_i(\omega_0 - \omega_i) + \sum_{j\in N_i} a_{ij}(\delta_j - \delta_i) \tag{16}$$

where $\delta_i = m_iP_i$ is the power sharing coefficient. Based on (3) and (16), when FDIA occurs, the global dynamics of DSC is expressed as

$$-[\dot{\omega} + \dot{\delta}] = (L+G)(\omega - \omega_0) + L\delta + B\varepsilon \tag{17}$$

where $B = \text{diag}\{b_1, \ldots, b_n\}$ is the matrix associated with the FDIA. Based on [13] and [15], under an FDIA, voltage and frequency experience deviations, but it reach an equilibrium point. Consequently, the frequency and power sharing ratio is a constant, and they satisfy $\omega + \dot{\delta} = 0$. At steady state, all DGs' frequencies align with the same, leading to

$$L(\omega + \omega_0) = 0. \tag{18}$$

Setting the left-hand side of (17) equal to 0, and considering (18)

$$L\delta + G(\omega - \omega_0) + B\varepsilon = 0. \tag{19}$$

Without any limitation, it is assumed that if $g_i = 1$, the unit has access to the reference. $b_i\varepsilon_i \neq 0$ means that the ith-DG's neighbor is under FDIA. Therefore, another expression of (19) is re-expressed as

$$\begin{bmatrix} \sum_{j=1}^{n} a_{1j} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \sum_{j=1}^{n} a_{2j} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & \sum_{j=1}^{n} a_{nj} \end{bmatrix} \begin{bmatrix} \delta_1 \\ \delta_2 \\ \vdots \\ \delta_n \end{bmatrix} + \begin{bmatrix} g_1(\omega_1 - \omega_0) \\ g_2(\omega_2 - \omega_0) \\ \vdots \\ g_n(\omega_n - \omega_0) \end{bmatrix} + \begin{bmatrix} b_1\varepsilon_1 \\ b_2\varepsilon_2 \\ \vdots \\ b_n\varepsilon_n \end{bmatrix} = 0. \tag{20}$$

To make a determinant transformation on (20), add the elements of the first $(n-1)$ rows to the elements of the nth row to obtain

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

By solving (21), we can determine the relationship between the attack and the frequency. All DGs within the MG operate at the same frequency in a steady state, which leads to

$$\omega_i = \omega_0 + \sum_{i=1}^{N} b_i\varepsilon_i / 1_N^T G 1_N \tag{22}$$

when no cyber-attacks exist, ω_i will gradually reach to a value close to ω_0. When FDIA exists, the DG's frequency is falsified by FDIA, given by $\sum_{i=1}^{N} b_i\varepsilon_i/(1_N^T G 1_N)$. As noted, the FDIA's effect on frequency is independent of the communication matrix L. Instead, the attack elements and the leader node determine the frequency convergence error.

In addition, DG's active power can be written as

$$P_i \approx V_i V_p \int (\omega_i - \omega_p)/Z_{li} \tag{23}$$

where V_p and ω_p denote the point of common coupling (PCC) voltage and frequency. It has been proved that all DG frequencies converge to the same value, even if FDIA occurs [13].

However, as shown in (23), the dynamic frequency change can lead to phase variation, potentially disrupting power sharing. Building on this, the following index can be defined to quantify the impact of FDIA on power:

$$\Lambda(i) = \{l(i,1), l(i,2) \ldots l(i,j)\}, j \in N_i \tag{24}$$

where $\Lambda(i)$ is a vector containing the lengths of the communication paths from all neighbors node i, and $l_{i,j}$ represents the length of the link from node j to node i

$$F_5(\hat{G}) = \max\_\mathrm{Var}\{\Lambda(i)\}, i \in N. \tag{25}$$

$F_5(\hat{G})$ represents the global propagation rate from one DG to the others per unit of time. The term $\mathrm{Var}\Lambda(i)$ refers to the vector variance, which reflects the variation in the time it takes for error information to be transmitted from unit i to all other units. This variance plays a crucial role in power sharing, as it leads to abnormal power fluctuations, as previously discussed. The max function is used to select the highest variance, for the worst-case scenario.

4) Metric of MDA Effect: MDA is an attack that the hacker attacks each unit indiscriminately to make it drop out. Once hackers obtain information about the communication topology through unique means, they selectively attack some communication units. Therefore, the attacked DG is forced to be disconnected, and the attacked communication unit loses effect, unable to receive and send system interaction information [7].

Under MDA, the remaining DGs should strive to maintain power sharing performance to the greatest extent possible. In this context, there should be as few independent units as possible, ensuring the continuity of power sharing capabilities among the operational inverters. The metric $F_6(\hat{G})$ is used to quantify the survivability of the MG under MDA

$$F_6(\hat{G}) = \sum_{m=1}^{n} [n_m - \mathrm{rank}(L_m)]/m^2 \tag{26}$$

where m denotes the DG numbers that are disconnected caused by MDA. $n_m = n - m$ is the remaining DGs still operational after the attack. L_m is the Laplacian matrix of the graph, accounting for the removal of m units from the system. The attack metric is nearly inversely proportional to $\mathrm{rank}(L_m)$ for a given MDA. Lower $\mathrm{rank}(L_m)$ represents more isolated units and denotes higher attack metrics. The worst case is that the attack metric reaches the upper limit m when $\mathrm{rank}(L_m) = 0$. At this time, no available DGs exist in cyber topology.

E. Optimal Communication Network Design

In this section, an optimal network is designed, with the aim of configuring the network. A multiobjective optimization method is proposed, incorporating the developed indices in the previous section. The cost function for n DGs is defined as

$$\begin{aligned} &\min F(\hat{G}_i) \\ &= \Bigg(\vartheta_1 \frac{F_1(\hat{G}_i) - F_{1,\min}}{F_{1,\max} - F_{1,\min}} + \vartheta_2 \frac{F_2(\hat{G}_i) - F_{2,\min}}{F_{2,\max} - F_{2,\min}} \\ &\quad + \vartheta_3 \frac{F_3(\hat{G}_i) - F_{3,\min}}{F_{3,\max} - F_{3,\min}} + \vartheta_4 \frac{F_4(\hat{G}_i) - F_{4,\min}}{F_{4,\max} - F_{4,\min}} \\ &\quad + \vartheta_5 \frac{F_5(\hat{G}_i) - F_{5,\min}}{F_{5,\max} - F_{5,\min}} + \vartheta_6 \frac{F_6(\hat{G}_i) - F_{6,\min}}{F_{6,\max} - F_{6,\min}}\Bigg) \end{aligned} \tag{27}$$

where F_1–F_6 are different objective functions for specific performance criteria, such as convergence, delays bound, and cost, along with indexes for DoS, FDIA, and MDA. We have taken all these six indexes into consideration. Therefore, it is not designed for a specific attack. The variables ϑ_1–ϑ_6 are the weights associated with these functions. The values $F_{i,\min}$ and $F_{i,\max}$ represent the minimum and maximum outcomes of the corresponding objective function among the given candidates,

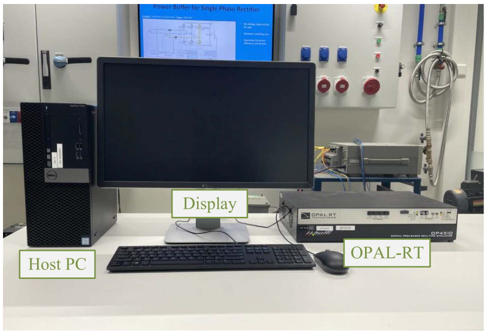

Fig. 2. Verification setup.

as shown in Fig. 3, where $F_1(\hat{G}_1)$–$F_1(\hat{G}_8)$ are evaluated. For instance, $F_{1,\min}$ is the smallest value among all candidate networks. Clearly, $F_{1,\min} = F_1(\hat{G}_1)$ and $F_{1,\max} = F_1(\hat{G}_8)$, since $\hat{G}_1$ is the sparsest network with the slowest response speed, whereas $\hat{G}_8$ is the densest network, achieving the fastest response. Notably, we normalized each objective function to minimize the impact of magnitude differences between objectives. Since this article assumes equal importance for the involved indices, assigning equal weights is reasonable. Moreover, the weight design can be adapted based on the specific requirements of the grid operator.

The comprehensive procedure for optimal network design includes the selection of the feasible communication network, determining Pareto bounds for multiobjective optimization, and selecting the optimal topology. The determination of Pareto frontiers for different DG configurations is performed as follows.

1) *Map all possible networks:* For each MG system size, the possible range of possible networks must be determined. Essentially, a sequential series of $1 \sim n$ DG units can form $(n-1)n/2$ networks.
2) *Selection of feasible networks:* Considering that these interconnected networks typically yield some homogeneous counterparts with identical eigenvalues and algebraic connectivity, further investigation is required based on the network unit degree. Importantly, the feasible network should have an even degree due to the requirements for plug-and-play operation, thus limiting the candidate networks to $n-2$ types.
3) *Optimal network selection:* Scanning the candidate DG set for operational MG case and searching the related Pareto optimal networks according to the involved quantification indices. In particular, the emphases corresponding to different evaluation functions may lead to various optimal networks.

IV. Verification

The proposed network design for DSC is validated through OPAL-RT simulations, with the verification setup depicted in Fig. 2. The test MG consists of ten converters in a radial configuration, as shown in Fig. 1, and can be scaled to accommodate other topologies and larger MGs. The basic parameters are as follows: $V_0 = 190$ V, $\omega_0 = 314$ rad/s, and $m_1 = n_1 = 1/400$. The other droop coefficients are configured to ensure the active and reactive power sharing ratios follow DG1 : DG2 : DG3 : DG4 : DG5 : DG6 : DG7 : DG8 : DG9 : DG10 $= 1 : 1.5 : 2 : 2.5 : 3 : 3.5 : 4 : 4.5 : 5 : 5.5$. The *LC* filter parameters are the same for all DGs, with capacitance $C_f = 12$ μF, inductance $L_f = 2.2$ mH, and feeder impedance $Z_f = 2.2$ mH. The proposed method is a graph-theory-based secondary control approach that relies on communication rather than an explicit system model, making it inherently model-free. Notably, different MG structures, such as radial, ring, and meshed grids, exhibit different dynamic performances, primarily due to differences in equivalent line impedance. However, our approach mitigates this issue by leveraging communication to ensure the control objectives are met, regardless of grid structure.

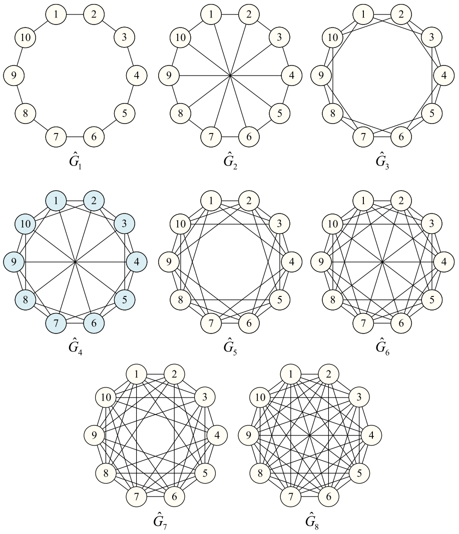

Fig. 3. Optimal communication network candidates.

For a grid with ten DGs, the number of edges in the network ranges from 9 to 45. In addition, various network configurations can be generated for the same set of DGs. However, as more units and edges are added, the optimization process becomes increasingly complex due to the exponential growth in possible configurations. The weighting factor of the cost function in (27) is set as $\vartheta_1 = \vartheta_2 = \vartheta_3 = \vartheta_4 = \vartheta_5 = \vartheta_6 = 1/6$ for verification.

In MGs, plug-and-play capabilities require an evenly distributed degree among units to ensure uniform communication links and minimize the impact of a DG shutdown. The uniform degree is thus essential for feasible network configurations. Therefore, the optimal network is identified by prioritizing symmetry, as analyzed for $\hat{G}_1$–$\hat{G}_8$ in Fig. 3.

The index values corresponding to $\hat{G}_1$–$\hat{G}_8$ are presented in Table II. Notably, the index value of the cost function for $\hat{G}_4$ is the smallest among the alternatives. Consequently, the communication network associated with $\hat{G}_4$ is taken as optimal, which is with 25 edges, and the unit degrees of each DG are 5.

1) Optimal Communication Network Validation

To showcase the dynamic of the optimized communication topology, we evaluate $\hat{G}_4$ under typical communication delays, load changes, and plug-and-play operations.

Fig. 4 illustrates the performance of the DSC of the optimized communication network, showing the DGs' active power,

TABLE II
OPTIMAL COMMUNICATION NETWORK SELECTION

Graph	F_1	F_2	F_3	F_4	F_5	F_6	$F(\hat{G_i})$
$\hat{G}_1$	-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

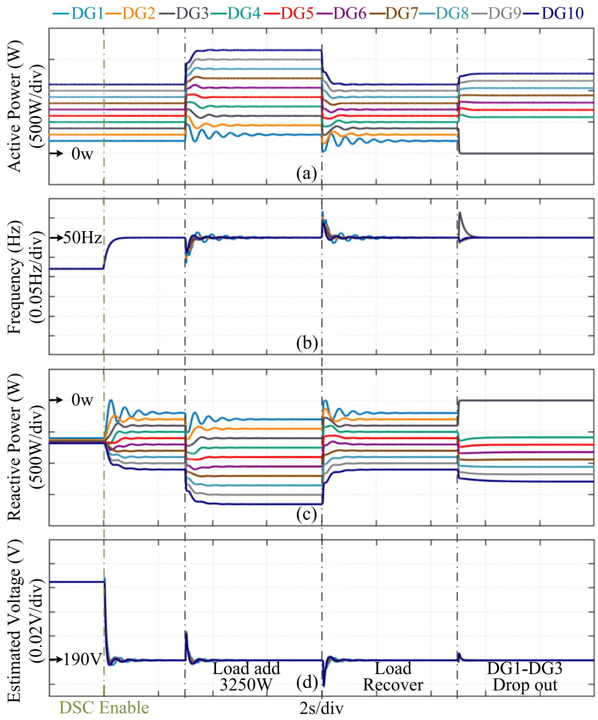

Fig. 4. Dynamics of optimal network $\hat{G}_4$ under 100-ms delay: (a) active power, (b) frequency, (c) reactive power, and (d) global average voltage.

frequency, reactive power, and global average voltage. A 100-ms delay, the typical upper bound [31], is simulated.

Initially, active power is synchronized since the frequency is a global variable. When DSC is activated at $t = 2$ s, reactive power is proportionally shared, and both frequency and voltage are restored. Load changes occur at $t = 5$ s and $t = 10$ s, and despite slight fluctuations due to communication delay, the MG reaches consensus, demonstrating convergence under delay. At $t = 15$ s, DG1–DG3 disconnect, while DG4–DG10 remain synchronized, showing the plug-and-play capability.

2) *Comparative Study I*

To validate the benefits of the proposed communication network, a comparison with [27] is conducted. In Fig. 5(a) from [27], a 14-edge network is presented. For a fair comparison, the proposed network is designed with the same number of edges, as shown in Fig. 5(b).

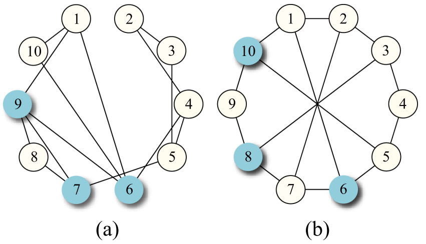

Fig. 5. Communication network of the MG with 14 edges. (a) Optimal network in [27]. (b) Proposed optimal network.

a) Comparison study against FDIA: The DSC dynamics under FDIA are investigated in this section. Fig. 6(a) and (b) illustrates the active power sharing coefficient (m_iP_i), frequency (f_i), reactive power sharing coefficient (n_iQ_i), and estimated global voltage ($\bar{V}_i$) for each network.

Following the established protocol, secondary control is activated at $t = 2$ s for both networks, ensuring both active and reactive power sharing. At this point, the system achieves balanced power distribution, with the active power sharing coefficients converging to $m_1P_1 = \cdots = m_{10}P_{10} = 0.5$ and the reactive power sharing coefficients stabilizing at $n_1Q_1 = \cdots = n_{10}Q_{10} = -0.5$. At $t = 10$ s, an FDIA is launched, specifically targeting the communication link between DG10 and DG1. The attack injects falsified measurement data, reporting an incorrect power value of 2200 W for both active and reactive power. As a result, the system is misled, leading to deviations in frequency and voltage. The frequency increases to 50.1 Hz, while the estimated global voltage rises to 190.1, indicating a significant disturbance in system stability. Under the network structure from [27], the impact of the FDIA is pronounced, causing substantial variations in power sharing coefficients across different DGs. Specifically, the active power sharing coefficients fluctuate significantly, ranging from $m_4P_4 = 0.2$ to $m_1P_1 = 0.95$, while the reactive power sharing coefficients deviate from $n_4Q_4 = -0.8$ to $n_1Q_1 = -0.05$, as illustrated in Fig. 6(a). These discrepancies highlight the vulnerability of this network configuration to FDIA, as the manipulated measurements lead to severe imbalances in power distribution. In contrast, the proposed network, as shown in Fig. 6(b), demonstrates a significantly improved resilience to the attack.

Although FDIA still impacts performance, the deviations in power sharing coefficients are effectively limited, keeping values much closer to the expected 0.5. This indicates that the proposed network mitigates the adverse effects of FDIA, preventing extreme imbalances in active and reactive power distribution. Despite the differences in FDIA impact on power sharing accuracy, it is important to note that the steady-state deviations in frequency and voltage remain nearly identical in both networks. This is attributed to the fact that both configurations utilize the same number of pinning DGs, which inherently determines the system's overall frequency and voltage deviation, as proved in (22).

b) Comparison study against MDA: Fig. 7(a) and (b) illustrates the dynamic performance of the networks shown in Fig. 5(a) and (b), respectively. Initially, DSC is activated at $t = 2$ s, ensuring synchronization of all DGs and stable power sharing

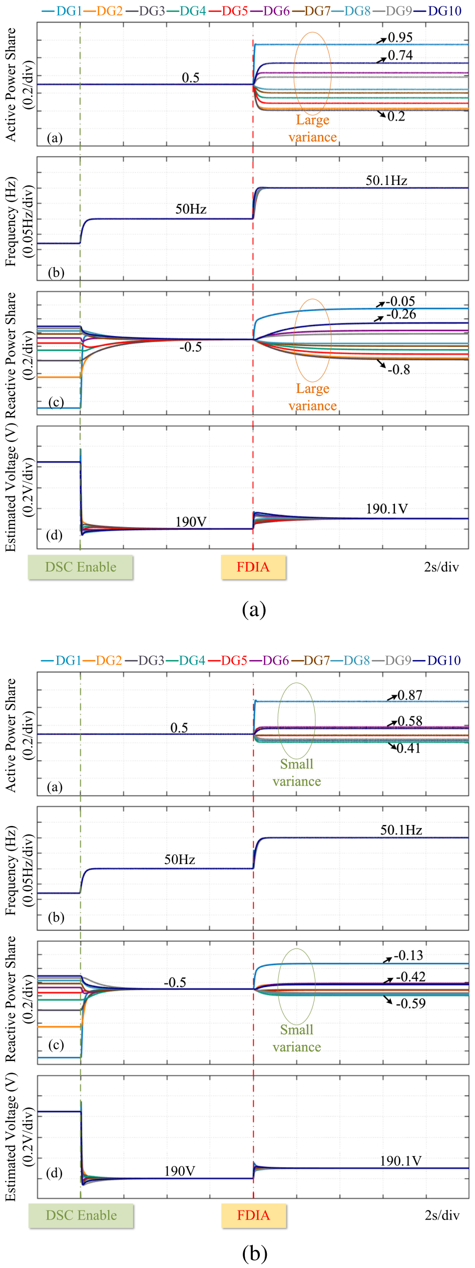

Fig. 6. Comparison to the design in [27] under FDIA. (a) Network performance in [27] under FDIA. (b) Proposed network performance under FDIA.

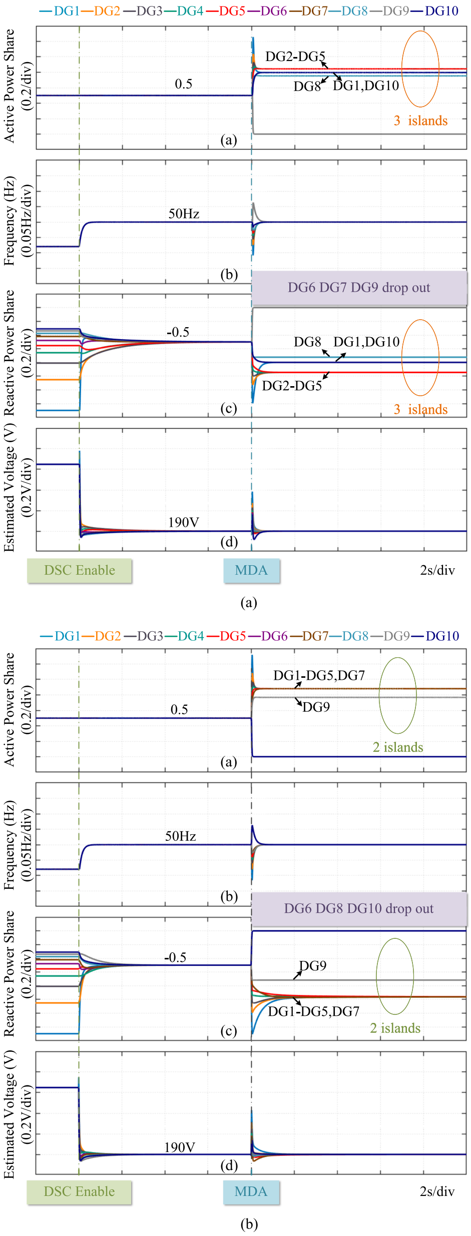

Fig. 7. Comparison to the design in [27] under MDA. (a) Network performance in [27] under MDA. (b) Proposed network performance under MDA.

among them. The system operates under normal conditions until $t = 10$ s, when an MDA occurs, leading to the disconnection of three DGs from the network. In the worst-case scenario, the network from [27] experiences severe fragmentation, resulting in the formation of three isolated islands: {8}, {1,10}, and {2,3,4,5}, when DG6, DG7, and DG9 drop out. The loss of these key nodes disrupts the connectivity between several DGs, significantly affecting power sharing and system stability. By contrast, in the proposed network, the impact of the same MDA is mitigated.

When DG6, DG8, and DG10 drop out, the system forms only two islands: {9} and {1,2,3,4,5,7}. This indicates that the proposed network maintains stronger connectivity among the remaining DGs, reducing the extent of fragmentation and preserving overall system integrity. This comparison demonstrates that the proposed network design enhances resilience against MDA by limiting the number of isolated islands and maintaining a more cohesive structure even under severe disturbances. This improved robustness is crucial for maintaining reliable operation in distributed control environments.

3) Comparative Study II

The network from [7], where each DG is connected to four others, is shown in Fig. 8(a) and compared to a 30-edge network

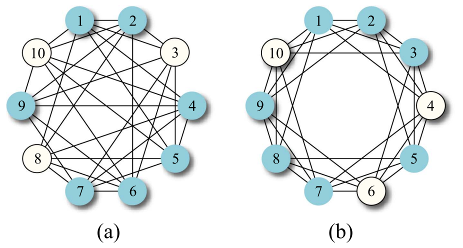

Fig. 8. Communication network of the MG with 30 edges. (a) Optimal network in [7]. (b) Proposed optimal network.

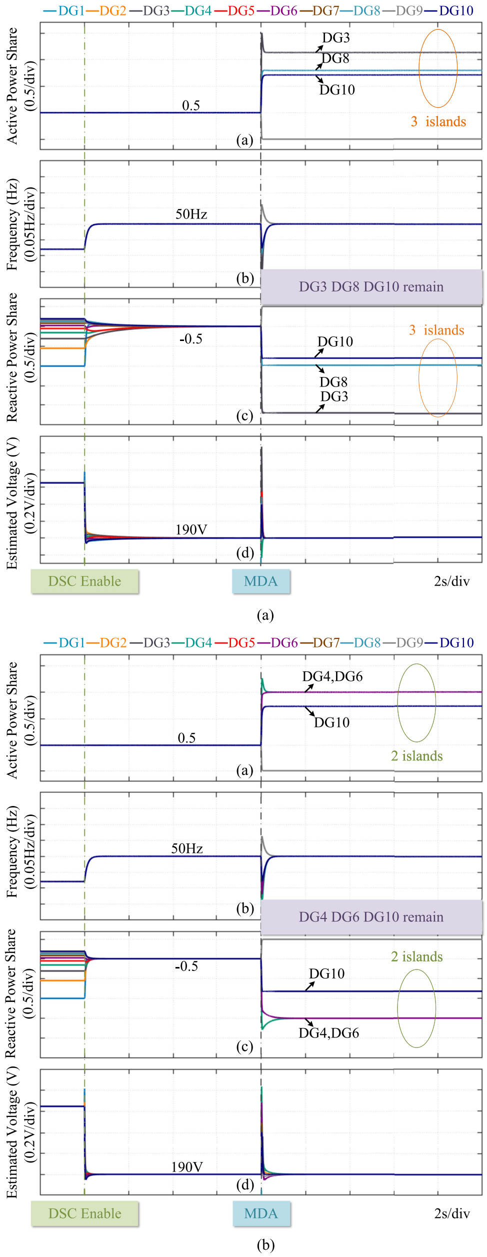

Fig. 9. Comparison to the designed network in [7] under MDA. (a) Network performance in [7] under MDA. (b) Proposed network performance under MDA.

optimized using the proposed method, as illustrated in Fig. 8(b). Their dynamic responses to deliberate attacks are analyzed and presented in Fig. 9(a) and (b), respectively.

The DSC is activated at $t = 2$ s, ensuring proportional power sharing among DGs and synchronization of both frequency and voltage. The system remains stable under normal operating conditions until $t = 10$ s, when an MDA is triggered, which has the capability to cause the dropout of anywhere from 1 to 10 DGs. To effectively illustrate the impact of such disturbances, the analysis focuses on a scenario with a 7-DG dropout, as it presents the most significant performance differences. Cases with 1–6 and 8–10 DG dropouts are omitted from the discussion since the observed differences between the network from [7] and the proposed method are minimal in those scenarios.

As shown in Fig. 9(a), under the network structure from [7], DG3, DG8, and DG10 remain operational after the MDA, leading to severe fragmentation, with the formation of three isolated islands: $\{3\}$, $\{8\}$, and $\{10\}$. This level of fragmentation significantly disrupts power sharing.

In contrast, the proposed network, as shown in Fig. 9(b), exhibits improved resilience. After the MDA, DG4, DG6, and DG10 remain operational, forming only two islands: $\{4{,}6\}$ and $\{10\}$. This demonstrates a notable improvement in maintaining network connectivity, reducing the number of isolated components.

The results clearly highlight the superior resilience of the proposed network design, which maintains better synchronization and connectivity under MDA, reducing the impact of severe disturbances and ensuring more stable operation compared to the network from [7].

V. Conclusion

This article proposes an approach to optimize the communication network for DSC of MGs, focusing on enhancing resilience against attacks and minimizing the impact of attacks on power and voltage regulation. To achieve this, novel metrics are developed to assess the effects of false data injection, DoS, and MDA. Subsequently, a multiobjective optimization technique is employed to develop the communication network, considering the quantified attacks, convergence, time-delay robustness, and communication cost. Unlike real-time cyber-attack detection and counteraction, the proposed method can be used for MG planning, which is implemented during the development stage of the MG, preparing resilience before the attacks go to the secondary control layer. Consequently, the proactive design approach makes the MG less affected by these attacks. In the proposed scheme, cyber-attacks' dynamics and increasing complexity may need to be fully considered, which can be a focus of future research. One limitation is that the proposed optimal communication network is fixed after design; extending it to dynamic optimization could further enhance flexibility and resilience, which may be explored in future work.

References

[1] M. Kosari and S. H. Hosseinian, “Decentralized reactive power sharing and frequency restoration in islanded microgrid,” *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2901–2912, Jul. 2017.

[2] Y. Xu, H. Sun, W. Gu, Y. Xu, and Z. Li, “Optimal distributed control for secondary frequency and voltage regulation in an islanded microgrid,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 225–235, Jan. 2019.

[3] M. Chen, X. Xiao, and J. M. Guerrero, “Secondary restoration control of islanded microgrids with a decentralized event-triggered strategy,” *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3870–3880, Sep. 2018.

[4] J. Xiao, L. Wang, Y. Wan, P. Bauer, and Z. Qin, “Distributed model predictive control-based secondary control for power regulation in AC microgrids,” *IEEE Trans. Smart Grid*, vol. 15, no. 6, pp. 5298–5308, Nov. 2024.

[5] S. Yang, K.-W. Lao, Y. Chen, and H. Hui, “Resilient distributed control against false data injection attacks for demand response,” *IEEE Trans. Power Syst.*, vol. 39, no. 2, pp. 2837–2853, Mar. 2024.

[6] W. Yao, Y. Wang, Y. Xu, and C. Deng, “Cyber-resilient control of an islanded microgrid under latency attacks and random DoS attacks,” *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5858–5869, Apr. 2023.

[7] 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 Trans. Smart Grid*, vol. 13, no. 5, pp. 3774–3785, Sep. 2022.

[8] B. Li, R. Lu, G. Xiao, T. Li, and K.-K. R. Choo, “Detection of false data injection attacks on smart grids: A resilience-enhanced scheme,” *IEEE Trans. Power Syst.*, vol. 37, no. 4, pp. 2679–2692, Jul. 2022.

[9] M. H. Ranjbar, M. Kheradmandi, and A. Pirayesh, “Assigning operating reserves in power systems under imminent intelligent attack threat,” *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 2768–2777, Jul. 2019.

[10] A. S. Musleh, G. Chen, and Z. Y. Dong, “A survey on the detection algorithms for false data injection attacks in smart grids,” *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[11] Y. Wan and T. Dragičević, “Data-driven cyber-attack detection of intelligent attacks in islanded DC microgrids,” *IEEE Trans. Ind. Electron.*, vol. 70, no. 4, pp. 4293–4299, Apr. 2023.

[12] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, “Flexible division and unification control strategies for resilience enhancement in networked microgrids,” *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 474–486, Jan. 2020.

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

[14] 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 Trans. Smart Grid*, vol. 15, no. 3, pp. 2447–2458, May 2024.

[15] J. Xiao, L. Wang, Z. Qin, and P. Bauer, “A resilience enhanced secondary control for AC micro-grids,” *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 810–820, Jan. 2024.

[16] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, “Synchrony in networked microgrids under attacks,” *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6731–6741, Nov. 2018.

[17] 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 Trans. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 1, pp. 144–154, Mar. 2021.

[18] J. Duan and M.-Y. Chow, “A resilient consensus-based distributed energy management algorithm against data integrity attacks,” *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4729–4740, Sep. 2019.

[19] H. Wang, Z. Yan, M. Shahidehpour, X. Xu, and Q. Zhou, “Quantitative evaluations of uncertainties in multivariate operations of microgrids,” *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 2892–2903, Jul. 2020.

[20] S. Sahoo, T. Dragičević, and F. Blaabjerg, “An event-driven resilient control strategy for DC microgrids,” *IEEE Trans. Power Electron.*, vol. 35, no. 12, pp. 13714–13724, Dec. 2020.

[21] J. Zhang, S. Sahoo, J. C.-H. Peng, and F. Blaabjerg, “Mitigating concurrent false data injection attacks in cooperative DC microgrids,” *IEEE Trans. Power Electron.*, vol. 36, no. 8, pp. 9637–9647, Aug. 2021.

[22] J. Xiao, L. Wang, P. Bauer, and Z. Qin, “A consensus algorithm-based secondary control with low vulnerability in microgrids,” *IEEE Trans. Ind. Informat.*, vol. 21, no. 4, pp. 3196–3205, Apr. 2025.

[23] J. Liu, X. Lu, and J. Wang, “Resilience analysis of DC microgrids under denial of service threats,” *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3199–3208, Jul. 2019.

[24] J. Liu, Y. Du, S.-i. Yim, X. Lu, B. Chen, and F. Qiu, “Steady-state analysis of microgrid distributed control under denial of service attacks,” *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5311–5325, Oct. 2021.

[25] S. Sahoo, Y. Yang, and F. Blaabjerg, “Resilient synchronization strategy for AC microgrids under cyber attacks,” *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 73–77, Jan. 2021.

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

[27] 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 Trans. Power Syst.*, vol. 34, no. 2, pp. 968–981, Mar. 2019.

[28] S. Manaffam, M. Talebi, A. K. Jain, and A. Behal, “Intelligent pinning based cooperative secondary control of distributed generators for microgrid in islanding operation mode,” *IEEE Trans. Power Syst.*, vol. 33, no. 2, pp. 1364–1373, Mar. 2018.

[29] Y. Khayat et al., “On the secondary control architectures of AC microgrids: An overview,” *IEEE Trans. Power Electron*, vol. 35, no. 6, pp. 6482–6500, Jun. 2020.

[30] J. Lai, H. Zhou, X. Lu, X. Yu, and W. Hu, “Droop-based distributed cooperative control for microgrids with time-varying delays,” *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1775–1789, Jul. 2016.

[31] 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.