False Data Injection Attack Detection for DC Microgrids Using Partial Load Measurements

Ali Elrayyah, Member IEEE,Yilamz Sozer, Fellow IEEE

***Abstract*—In this paper, a method is proposed to detect False Data Injection Attack (FDIA) in decentralized DC Microgrids based on partial load measurements. The proposed attack detection scheme is capable of identifying the presence of attacks on the local current/voltage sensors of the converter units through state estimation based on load flow analysis and tracking the error between the estimated and sensor-sent values for converters' voltage and currents. The method can detect and/or identify FDIA within the microgrid merely through measurements from the load smart meters. Detailed simulation work has been conducted to showcase the effectiveness of the proposed attack detection method.**

***Index Terms*—Article submission, IEEE, IEEEtran, journal, LaTeX, paper, template, typesetting.**

I. INTRODUCTION

CONVERTER dominated standalone nature of DC microgrids yields several inherent advantages which include efficient integration of renewable energy sources, reliable and economic operation, and simpler control structures [1], [2]. To establish robust control and seamless operation of the DCMG entities, increased penetration of software-based controllers for DCMG converters and networked communication structures has become inevitable. As a result, DCMG systems have also been evolving as complex cyber-physical systems with the dynamic interaction between cyber and physical hardware layers.

Distributed control mechanism for cyber-physical DCMG operation has become an attractive choice of action due to its scalability, robustness, and economic nature of operation because of the transmission of a lesser amount of data traffic among the neighboring converter units [2]. However, the control and coordination of converter units in DCMG under a distributed control approach is challenged in the event of any sensor measurement imperfections, tampering, and compromise of the sparse communication link. Additionally, since the distributed control structures function via the propagation of participating converter units' voltage and current information over the sparse communication link, any external intrusion in the transmitted information and in the link itself will affect the operation of neighboring nodes. The external intrusion eventually leads the overall system towards destabilization, deviated performance due to violation of the control law, and ultimately untimely shutdown of the total system [3]. These incidents of external communication link tampering and intentional alteration of the sensor/actuator data to degrade the DCMG system performance are termed cyber-attacks. The cyber-physical characteristics and the deliberate deployment of distributed control schemes within the DCMG system in recent days have made these systems vulnerable to cyber threats/attacks. Model-based approaches that studied the detection of False Data Injection Attacks (FIDA) in [4] inherently assume the nature of attack vectors (bounded/unbounded/constant/time-varying) and the network topology of the DCMG under consideration. Some of the well-adapted model-based methods have been described in [5], [6]. Recently, artificial intelligence (AI) based reference tracking methods of FDIA detection schemes have been developed in DC microgrid systems in [7], [8]. However, these strategies pose additional challenges due to the requirement of an increased computational burden.

An estimation-based control protocol and concurrent FDIA attack mitigation rule have been proposed in [9] and [10], respectively. This paper proposes an FDIA attack detection strategy for DCMG systems using Load flow analysis (LFA) based estimator for converter voltage and current measurements, which are used to detect a mismatch between the actual converter output quantities and LFA-based estimated quantities. The proposed method is based on using partial load measurements to perform LFA, such that its signal communication requirement is reduced and its robustness against FDIA on load sent measurements is enhanced. With the application of this proposed detection principle, the secured DCMG operation in local mode will be ensured with a great enhancement in its operational reliability. The rest of the paper is organized as follows. Section II addresses the concept of the droop control mechanism in DC microgrid operation. Section III describes the approach to detecting FDIA based on partial load measurements. Section IV shows detailed small-signal modeling and simulation results, respectively. Section V concludes the paper with the performance analysis of the developed attack detection method and concluding remarks.

II. DECENTRALIZED DROOP CONTROL IN DC MICROGRIDS

The droop controller block of DC/DC converters operating in DCMG acquires the local converters' output current and the droop settings to generate the required converter output voltage reference for the voltage controller as seen from Fig. 1. The output voltage reference of the ith converter $v_{o,i}^*$ can be expressed as

$$v_{o,i}^* = V_{ref,i} - I_i R_{di}, i = 1, 2. \tag{1}$$

This paper was produced by the IEEE Publication Technology Group. They are in Piscataway, NJ.

Manuscript received April 19, 2021; revised August 16, 2021.

979-8-3315-8138-1

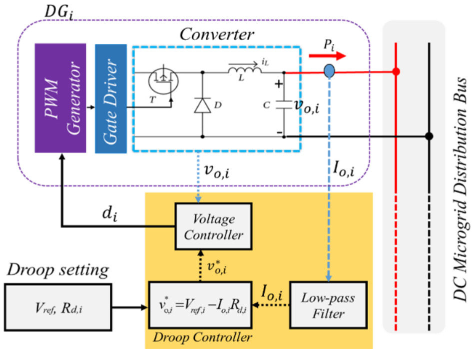

Fig. 1. Converter control diagram of a decentralized controller-based DCMG.

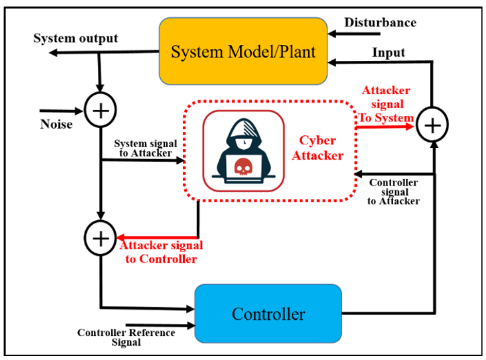

Fig. 2. Simplified block diagram showing the presence of an FDIA attack in the DCMG system model/plant.

where $V_{ref,i}$ is the desired output voltage global set point in each converter, I_i is the output current of the i^{th} converter, and R_{di} is the virtual resistance/droop coefficient. The converter's outputs have approximately the same voltage, ideal conditions, the relationship in **??** applies

$$\begin{aligned} v_{o,i}^* &= v_{o,j}^* \\ I_i R_{di} &= I_j R_{dj} \rightarrow \frac{I_i}{I_j} = \frac{R_{dj}}{R_{di}} \end{aligned} \tag{2}$$

Generally, DCMG converters can be exposed to FDIA where exogenous signals modify the sensors' measurements locally or when being transported over communication networks. A simplified block diagram of the FDIA model is shown in Fig. 2 below. Suppose a DC microgrid with a decentralized control structure under consideration has N DC/DC converter units. Then, an FDIA in sensor of the i^{th} $i = 1, 2, 3, \cdots N_s$ of the microgrid can be modeled as:

$$x_i^{FDIA} = x_i^{act} + x_i^{inj} \tag{3}$$

where, x_i^{act} is the sensor measurement on the i^{th} converter unit which can be either of the voltage or current sensor and x_i^{inj} represents the attack vector, which, depending on the attacker, can be a DC offset, unbounded ramp signal, sinusoidally varying signal or randomly changing signal. FDIA on the voltage sensor affects the accuracy of the converter voltage controller, while FDIA on the current sensor impacts the droop relationship. Assume there are FDIA on the voltage and current sensors of the i^{th} converter, 2 becomes 2 applies

$$\begin{aligned} I_i R_{di} + i_i^{inj} R_{di} + v_i^{inj} &= I_j R_{dj} \\ \frac{I_i}{I_j} = \frac{R_{dj}}{R_{di}} &- \frac{i_i^{inj} R_{di} + v_i^{inj}}{I_j R_{di}} \end{aligned} \tag{4}$$

Having nonzero i_i^{inj} and v_i^{inj} not only impacts current sharing accuracy among converters but also leads to poor voltage regulation at the converter outputs.

III. FDIA Detection through Partial Load Measurements

Consider the radial DCMG in Fig. 3. The droop relationship of the i^{th} converter susceptible to FDIA can be expressed as

$$v_{o,i}^* = V_{ref,i} - i_{si} R_{di} + \delta_i \tag{5}$$

$$\delta_i = i_i^{inj} R_{di} + v_i^{inj}$$

where δ_i is a parameter produced due to FDIA. Usually, all converters have the same value for $V_{ref,i}$. Then, from Fig. 3, considering the converters' voltage in III along with the loads' currents and line impedance. Accordingly, the LFA of the system after rearranging the terms can yield the following equations:

$$\begin{aligned} &\alpha_{1,1} i_{s1} + \alpha_{1,2} i_{s2} = \beta_{1,1}\delta_1 + \beta_{1,2}\delta_2 + \gamma_{1,1} i_{L1} + \gamma_{1,2} i_{L2} \\ &\alpha_{2,1} i_{s1} + \alpha_{2,2} i_{s2} + \alpha_{2,3} i_{s3} = \\ &\qquad \beta_{2,1}\delta_1 + \beta_{2,2}\delta_2 + \beta_{3,1}\delta_3 + \gamma_{2,2} i_{L2} + \gamma_{2,3} i_{L3} \\ &\qquad \vdots \\ &\alpha_{N_S,N_S-1} i_{sN_s-1} + \alpha_{N_S,N_S} i_{sN_s} = \beta_{N_S,N_S-1}\delta_{N_R-1} \\ &\qquad + \beta_{N_S,N_S}\delta_{N_R} + \gamma_{N_S,N_S-1} i_{LN_R-1} + \gamma_{N_S,N_S} i_{LN_R} \end{aligned}$$

where

$$\begin{aligned} &\alpha_{1,1} = 1 + \frac{R_{d1}}{R_2 + R_3}, \alpha_{1,2} = \frac{-R_{d2}}{R_2 + R_3} \\ &\beta_{1,1} = \frac{1}{R_2 + R_3}, \beta_{1,2} = \frac{-1}{R_2 + R_3}, \\ &\gamma_{1,1} = 1, \gamma_{1,2} = \frac{R_3}{R_2 + R_3} \\ &\alpha_{2,1} = \frac{-R_{d1}}{R_2 + R_3}, \alpha_{2,2} = 1 + \frac{R_{d2}}{R_2 + R_3} + \frac{R_{d2}}{R_4 + R_5}, \\ &\alpha_{2,3} = \frac{-R_{d3}}{R_4 + R_5}, \beta_{2,1} = \frac{-1}{R_2 + R_3}, \\ &\beta_{2,2} = \frac{1}{R_2 + R_3} + \frac{1}{R_4 + R_5}, \beta_{2,3} = \frac{-1}{R_4 + R_5} \\ &\gamma_{2,1} = \frac{R_2}{R_2 + R_3}, \gamma_{2,3} \frac{R_5}{R_4 + R_5}, \\ &\alpha_{N_S,N_S-1} = \frac{-R_{d_{N_R-1}}}{R_{N_R-1} + R_{N_R}}, \\ &\alpha_{N_S,N_S} = 1 + \frac{-R_{d_{N_R}}}{R_{N_R-1} + R_{N_R}} \end{aligned}$$

979-8-3315-8138-1

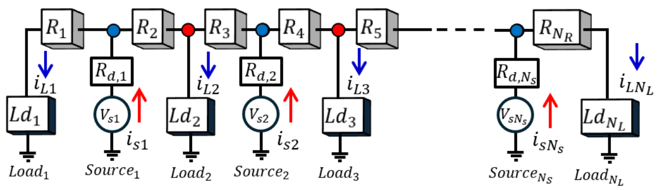

Fig. 3. Radial DCMG with N_S converters and N_L loads.

$$\beta_{N_S,N_S-1} = \frac{-1}{R_{N_R-1}+R_{N_R}},$$
$$\beta_{N_S,N_S} = \frac{1}{R_{N_R-1}+R_{N_R}}$$
$$\gamma_{N_S,N_S-1}\frac{-R_{N_R-1}}{R_{N_R-1}+R_{N_R}}, \gamma_{N_S,N_S} = 1$$

In general, the x^{th} equation for this system has the form

$$\alpha_{x,x-1}i_{s(x-1)} + \alpha_{x,x}i_{s(x)} + \alpha_{x,x+1}i_{s(x+1)} = \beta_{x,x-1}\delta_{x-1} + \beta_{x,x}\delta_x + \beta_{x,x+1}\delta_{x+1} + \gamma_{x,x}i_{L(x)} + \gamma_{x,x+1}i_{L(x+1)}$$
$$\alpha_{1,0} = \alpha_{N_S,N_S+1} = \beta_{1,0} = \beta_{N_S,N_S+1} = 0$$

In a matrix format, the system equations can be formulated as

$$AI_S = B\Delta + \Gamma I_L \tag{6}$$

$$A = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & 0 & 0 & \cdots & 0 \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_{N_S,N_S-1} & \alpha_{N_S,N_S} \end{bmatrix}$$

$$B = \begin{bmatrix} \beta_{1,1} & \beta_{1,2} & 0 & 0 & \cdots & 0 \\ \beta_{2,1} & \beta_{2,2} & \beta_{2,3} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \beta_{N_S,N_S-1} & \beta_{N_S,N_S} \end{bmatrix}$$

$$\Gamma = \begin{bmatrix} \gamma_{1,1} & \gamma_{1,2} & 0 & 0 & \cdots & 0 \\ 0 & \gamma_{2,2} & \gamma_{2,3} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \gamma_{N_S,N_S-1} & \gamma_{N_S,N_S} \end{bmatrix}$$

$$I_S = \begin{bmatrix} i_{s1} \\ i_{s2} \\ \vdots \\ i_{sN_S} \end{bmatrix}, \Delta = \begin{bmatrix} \delta_1 \\ \delta_2 \\ \vdots \\ \delta_{N_S} \end{bmatrix}, I_L = \begin{bmatrix} i_{L1} \\ i_{L2} \\ \vdots \\ i_{LN_L} \end{bmatrix}$$

These are N_S equations in (6) which can be used to determine the of N_S unknowns. The variables in these equations are i_{sx} $x = 1, 2, ..., N_S$, i_{Ly} $y = 1, 2, ..., N_L$, and $\delta_x x = 1, 2, ..., N_S$. The FDIA detector receives measurements for $i_{sx}$from the sources and for i_{Ly} from the loads. In the ideal case, all source and load currents are sent to the FDIA detector such that it can estimate $\delta_x x = 1, 2, ..., N_S$. However, the method presented in this section shows that FDIA can be detected with fewer measurements.

The ability to detect FDIAs with fewer load measurements provides valuable support, especially for large networks. Assume the N_S converter measurements are available, but only the measurements of N_{L1} loads are available. Let the number of unavailable load current measurements $N_{L2} = N_L - N_{L1}$ be smaller than N_S. It is possible, in this case, to detect the presence of any FDIA in the system. If, besides that, the FDIA are in dispersed converters, the method can identify up to $N_S - N_{L2} - 1$ concurrent FDIAs.

Let the set of unmeasured loads be included in $\mathcal{L}_{\mathcal{U}}$, then the set $\mathcal{S}_{\mathcal{D}}$ for the converters whose FDIA can be identified satisfies the relationships in (7) for any value of x and y.

$$\left|\left[\Gamma^{\mathcal{L}_{\mathcal{U}}}|B^{\mathcal{S}_{\mathcal{D}}}\right]_{\{1,2,\cdots,N_S\}\backslash x}\right| \times \left|\left[\Gamma^{\mathcal{L}_{\mathcal{U}}}|B^{\mathcal{S}_{\mathcal{D}}}\right]_{\{1,2,\cdots,N_S\}\backslash y\neq x}\right| \neq 0 \tag{7}$$

$|[X]|$ is the determinant of X, $\{1, 2, \cdots, N_S\}\backslash z$ means the set of the rows from 1 to N_S except the z^{th} one, and $M^{\mathcal{S}}$ is the sub-matrix of M whose columns indexes are included in the set $\mathcal{S}$. In other words, $[\Gamma^{\mathcal{L}_{\mathcal{U}}}|B^{\mathcal{S}_{\mathcal{D}}}]_{\{1,2,\cdots,N_S\}\backslash x}$ is a matrix formed by augmented the columns of Γ includes in the set $\mathcal{L}_{\mathcal{U}}$ with the column of B included in the set $\mathcal{S}_{\mathcal{D}}$ in (6) after eliminating the x^{th} row from each of them.

In above equations, a number of N_{L2} load currents are unknown, thus (6) can be used to determined these N_{L2} currents and since (6) can be used to determine N_S variables, additional $N_S - N_{L2}$ variables can also be determined and these can be from the FDIA parameters δ_x. Usually, there can be a few FDIAs in the DCMG, since finding security gaps in converters provided by different manufacturers can be challenging. Moreover, attaching several converters at the same time is associated with abnormal traffic in the communication network, which can easily be detected at the communication level. Thus, attackers usually target and carefully select a few resources for attack. Therefore, it is reasonable to assume most of the δ_x are 0, but a few of them can have a nonzero value.

Equation (7), indicates there are at least two selections for a $N_S - 1$ subset of the equations in (6) that yield a unique solution for the same elements in $\mathcal{L}_{\mathcal{U}}$ and $\mathcal{S}_{\mathcal{D}}$. Note that the δs not included $\mathcal{S}_{\mathcal{D}}$ are assumed to have zero values. The first selection is $\{1, 2, \cdots, N_S\}\backslash x$ and the second selection is $\{1, 2, \cdots, N_S\}\backslash y$, and the solution provided by these two selections can be identical or different. If the solutions provided by the two selections are identical, then the determined values for the elements in $\mathcal{L}_{\mathcal{U}}$ and $\mathcal{S}_{\mathcal{D}}$ are valid, but if the two solutions do not match, this indicates one or more FDIAs in the DCMG, but the considered selection for the elements in $\mathcal{S}_{\mathcal{D}}$ is invalid.

A special case of (7), is when the current measurements for the loads $1, 3, 5, \cdots, N_L$ are available and $\mathcal{L}_{\mathcal{U}}$ which corresponds to the elements $2, 4, 6, \cdots, N_L - 1$ is shown in (8). In this case, the FDIAs can be detected by algorithm 1.

$$\Gamma^{\mathcal{L}_{\mathcal{U}}} = \begin{bmatrix} \gamma_{2,1} & 0 & 0 & \cdots & 0 \\ \gamma_{2,2} & 0 & 0 & \cdots & 0 \\ 0 & \gamma_{4,3} & 0 & \cdots & 0 \\ 0 & \gamma_{4,4} & 0 & \cdots & 0 \\ & & & \vdots & \\ 0 & 0 & \cdots & 0 & \gamma_{N_L-1,N_L-1} \\ 0 & 0 & \cdots & 0 & \gamma_{N_L,N_L-1} \end{bmatrix} \tag{8}$$

979-8-3315-8138-1

Algorithm 1 FDIA Detection with Partial Load Measurements

A. Include the loads $2, 4, 6, ..N_L - 1$ in the set $\mathcal{L_U}$ and let N_{L2} be the number of elements in $\mathcal{L_U}$.

B. determine the current measurement of the loads not included in $\mathcal{L_U}$.

C. Assume there are FDIA in $N_V = N_S - N_{L2} - 1$ of the converters

D. For various combinations of selecting N_V out of the N_S converters

D.I. Include the selected converter in the set $\mathcal{S_D}$

D.II. Find values for x and y that satisfy (7).

D.III. Determine for the variables for the elements in $\mathcal{L_U}$ and $\mathcal{S_D}$ by solving.

$$\left[\frac{I_L^{\mathcal{L_U}}}{\Delta^{\mathcal{S_D}}}\right] = [\Gamma^{\mathcal{L_U}}|B^{\mathcal{S_D}}]^{-1}_{\{1,2,\cdots,N_S\}\backslash x}[Y]_{\{1,2,\cdots,N_S\}\backslash x}$$

D.IV. validate the results obtained in D.II by solving

$$\left[\frac{I_L^{\mathcal{L_U}}}{\Delta^{\mathcal{S_D}}}\right] = [\Gamma^{\mathcal{L_U}}|B^{\mathcal{S_D}}]^{-1}_{\{1,2,\cdots,N_S\}\backslash y}[Y]_{\{1,2,\cdots,N_S\}\backslash y}$$

D.V. If the results in D.III match those obtained in D.IV, then save the obtained solution as a potentially valid set of δs. Select another combination and go to D.I.

E. If only one valid solution is identified, then this represents the actual FDIA and it is successfully identified.

F. If several potential valid set are identified, N_V concurrent FDIAs are detected within these potential valid sets.

G. If none of the combinations in step D produces a valid set, then more than N_V concurrent FDIAs are detected.

The $[Y]_{\{1,2,\cdots,N_S\}\backslash z}$ in step **D** is a vector that includes all the element in Y except the z^{th} element. $Y = AI_S - \Gamma^{\mathcal{L_A}} I_L^{\mathcal{L_A}}$ where $\mathcal{L_A}$ is the loads with available measurement. In this approach through N_{L1} load measurements, up to $N_S - N_{L2} - 1$ concurrent FDIA can accurately be identified.

The condition in **F** occurs when the converters with FDIAs are not adequately dispersed within the DCMG. In this case, the matrix $[\Gamma^{\mathcal{L_U}}|B^{\mathcal{S_D}}]$ comprises two decoupled sub-matrices, where the sub-matrix associated with $\mathcal{S_D}$ in step D.III is identical to that in D.IV. Accordingly, these two steps produce the same results, which satisfy the condition in D.IV for some of the adjacent converters. In this case, N_V FDIAs within this subset of converters are detected, but cannot be identified. This indicates that the proposed approach can isolate the group of impacted converters by the FDIAs even when these converters are not optimally positioned in regard to the method's effectiveness. Section IV demonstrates this capability through a representative example.

In practical systems, it is unlikely to experience a large number of concurrent FDIAs on dispersed converters, especially when these converters are from different providers. Thus, the proposed approach in this section can be effective in identifying FDIAs with a reduced number of load measurements. This approach is not limited to the radial topology; it can rather be extended to address networks with different typologies where the same principle applies in all these cases.

TABLE I
SIMULATION PARAMETERS FOR THE FDIA DETECTION THROUGH PARTIAL MEASUREMENTS

Parameter	Value	Parameter	Value	Parameter	Value
V_{ref}	$48V$	R_{d1}-R_{d6}	0.1Ω	Ld_1	$5A$
Ld_2	$4A$	Ld_3	$10A$	Ld_4	$7A$
Ld_5	$2A$	Ld_6	$6.0A$	Ld_7	$8A$
R_1	0.5Ω	R_2	0.3Ω	R_3	0.2Ω
R_4	0.15Ω	R_5	0.1Ω	R_6	0.2Ω
R_7	0.2Ω	R_8	0.2Ω	R_9	0.4Ω
R_{10}	0.3Ω	R_{11}	0.3Ω	R_{12}	0.25Ω

TABLE II
FDIA DETECTION WITH PARTIAL MEASUREMENT (NO FDIAS)

	$\delta_1 = 0$	$\delta_2 = 0$	$\delta_3 = 0$	$\delta_4 = 0$	$\delta_5 = 0$	$\delta_6 = 0$
	1	2	3	4	5	6
1		0, 0	0, 0	0, 0	0, 0	0, 0
2	X		0, 0	0, 0	0, 0	0, 0
3	X	X		0, 0	0, 0	0, 0
4	X	X	X		0, 0	0, 0
5	X	X	X	X		0, 0

IV. SIMULATION RESULTS

In this simulation, a radial network similar to the one in Fig. 3 with 6 converters and 7 loads is considered with the parameters listed in Table I. In this case, the measurements of Loads $2, 4$, and 6 are unavailable. For this system $N_V = 2$ and accordingly up to 2 FDIAs can be detected.

Various FDIAs scenarios are then implemented in voltage sensors and the results are shown in Table II - VI In these tables, the imposed FDIAs are shown at the top of the table and the element in cell x, y is the value of (δ_x, δ_y) determined by the method in Section III. If this cell contains "-", this indicates a non-valid solution, while "X" is not considered, as this case is covered in the upper triangle of that table.

Table II shows the results for the no FDIA scenario in the system where the selections of any two converters produce

TABLE III
FDIA DETECTION WITH PARTIAL MEASUREMENT (CONVERTER 1)

	$\boldsymbol{\delta_1 = 1.0}$	$\delta_2 = 0$	$\delta_3 = 0$	$\delta_4 = 0$	$\delta_5 = 0$	$\delta_6 = 0$
	1	2	3	4	5	6
1		1.0, 0.0	1.0, 0.0	1.0, 0.0	1.0, 0.0	1.0, 0.0
2	X		-0.7, -0.3	-	-	-
3	X	X		-	-	-
4	X	X	X		-	-
5	X	X	X	X		-

TABLE IV
FDIA DETECTION WITH PARTIAL MEASUREMENTS (CONV. 1 AND 3)

	$\boldsymbol{\delta_1 = 1.0}$	$\delta_2 = 0$	$\boldsymbol{\delta_3 = 2.0}$	$\delta_4 = 0$	$\delta_5 = 0$	$\delta_6 = 0$
	1	2	3	4	5	6
1		-5.5, -4.5	1.0, 2.0	-	-	-
2	X		-0.69, 1.69	-	-	-
3	X	X		-	-	-
4	X	X	X		-	-
5	X	X	X	X		-

TABLE V
FDIA DETECTION WITH PARTIAL MEASUREMENTS (CONV. 1 AND 4)

	$\boldsymbol{\delta_1 = 1.0}$	$\delta_2 = 0$	$\delta_3 = 0$	$\boldsymbol{\delta_4 = 2.0}$	$\delta_5 = 0$	$\delta_6 = 0$
	1	2	3	4	5	6
1		-	-	1.0 , 2.0	-	-
2	X		-	-	-	-
3	X	X		-	-	-
4	X	X	X		-	-
5	X	X	X	X		-

TABLE VI
FDIA DETECTION WITH PARTIAL MEASUREMENTS (CONV. 1, 4 AND 5)

	$\boldsymbol{\delta_1 = 1.0}$	$\delta_2 = 0$	$\delta_3 = 0$	$\boldsymbol{\delta_4 = 2.0}$	$\boldsymbol{\delta_5 = 3.0}$	$\delta_6 = 0$
	1	2	3	4	5	6
1		-	-	-	-	-
2	X		-	-	-	-
3	X	X		-	-	-
4	X	X	X		-	-
5	X	X	X	X		-

a valid estimation $(0.0, 0.0)$, which represents an accurate estimation from the proposed method.

Table III shows the results for a single FDIA scenario in $converter_1$ with $\delta_1 = 1.0$. The algorithm considers all possible combinations of 2 concurrent FDIAs, and Table III shows that whenever $converter_1$ is considered, the algorithm produces a valid estimation. However, when the combination of $converter_2$ and $converter_3$ is considered, the algorithm produced a wrong estimation for FDIAs in these two converters. Note that this wrong estimation is obtained since the shape of $Y = AI_S - \Gamma^{\mathcal{L}_A} I_L^{\mathcal{L}A}$ shown in 9 has the first four rows decoupled from the last two. Then solving for i_{L2}, i_{L4}, δ_2 and δ_3 is limited in the first four rows of Y. Steps D.III and D.IV in algorithm 1, accordingly, use the same sub-matrix to solve for i_{L2}, i_{L4}, δ_2 and δ_3 which leads to identical solutions. However, in this scenario, a single FDIA $converter_1$ is identified since it produces the same result whenever this converter is considered in the set S_D.

$$\begin{bmatrix} \gamma_{2,1} & 0 & 0 & \beta_{1,2} & 0 \\ \gamma_{2,2} & 0 & 0 & \beta_{2,2} & \beta_{2,3} \\ 0 & \gamma_{4,3} & 0 & 0 & \beta_{3,3} \\ 0 & \gamma_{4,4} & 0 & 0 & \beta_{4,3} \\ 0 & 0 & \gamma_{6,5} & 0 & 0 \\ 0 & 0 & \gamma_{6,6} & 0 & 0 \end{bmatrix} \begin{bmatrix} i_{L2} \\ i_{L4} \\ i_{L6} \\ \delta_2 \\ \delta_3 \end{bmatrix} = Y \quad (9)$$

The third scenario considers FDIAs in $converter_1$ and $converter_3$. This scenario includes converters inadequately dispersed in the DCMG. The obtained results are shown in IV. Note that whenever two converters among $converter_1$, $converter_2$, and $converter_3$ are selected, a potentially valid solution is obtained; however, the obtained estimations do not match. Accordingly, the algorithm declares two or more FDIAs contained in the set of $converter_1$, $converter_2$, and $converter_3$.

The fourth scenario considers FDIAs in $converter_1$ and $converter_4$. This scenario represents a case of FDIAs in converters adequately dispersed in the network. Table V shows that a single valid solution is determined by the algorithm, and accordingly, the proposed method successfully identified the imposed FDIAs.

The last scenario considers three FDIAs in $converter_1$, $converter_4$ and $converter_5$. In this case, all combinations of converters produce a non-valid solution, which indicates a case of more than two FDIAs.

The results in this section show that the proposed method in Section III is effective in identifying, isolating, or detecting any number of concurrent FDIAs in DCMGs through partial load measurements.

V. CONCLUSION

This paper presented an FDIA attack detection algorithm on decentralized standalone DCMG systems using partial load measurements. The proposed algorithm adds an extra layer of resiliency in communication-based DCMG systems during an attack on the link or in applications. Detailed simulation results in MATLAB/Simulink environment and corresponding results have been provided under different FDIA attack scenarios to verify the effectiveness of the developed attack detection/identification scheme.

REFERENCES

[1] T. Dragicevi ˇ c, X. Lu, J. C. Vasquez, and J. M. Guerrero, “DC microgrids— ´Part I: A review of control strategies and stabilization techniques,” *IEEE Trans. Power Electron.*, vol. 31, no. 7, pp. 4876–4891, Jul. 2016.

[2] T. Dragicevi ˇ c, X. Lu, J. C. Vasquez, and J. M. Guerrero, “Dc microgrids— ´Part II: A review of power architectures, applications, and standardization issues,” *IEEE Trans. Power Electron.*, vol. 31, no. 5, pp. 3528–3549, May2016.

[3] S. Sahoo and S. Mishra, “A distributed finite-time secondary average voltage regulation and current sharing controller for DC microgrids,” *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 282–292, Jan. 2019.

[4] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dhong, “A review of false data injection attacks against modern power systems,” *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[5] O. A. Beg, T. Johnson, and A. Davoudi, “Detection of false-data injection attacks in cyber-physical dc microgrids,” *IEEE Trans. Ind. Inform.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[6] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, “Signal temporal logic-based attack detection in DC microgrids,” *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3585–3595, Jul. 2019.

[7] M. R. Habibi, H. R. Baghaee, T. Dragičević and F. Blaabjerg, “False Data Injection Cyber-Attacks Mitigation in Parallel DC/DC Converters Based on Artificial Neural Networks,” *IEEE Trans. on Circuits and Sys. II: Express Briefs*, vol. 68, no. 2, pp. 717-721, Feb. 2021.

[8] M. R. Habibi, S. Sahoo, S. Rivera, T. Dragičević and F. Blaabjerg, “Decentralized Coordinated Cyberattack Detection and Mitigation Strategy in DC Microgrids Based on Artificial Neural Networks,” *IEEE J. of Emerg. and Sel. Topics in Power Electron.*, vol. 9, no. 4, pp. 4629-4638, Aug. 2021.

[9] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[10] J. Zhang, S. Sahoo, J. C. -H. Peng and F. Blaabjerg, “Mitigating Concurrent False Data Injection Attacks in Cooperative DC Microgrids,” *IEEE Trans. on Power Electron.*, vol. 36, no. 8, pp. 9637-9647, Aug. 2021.

979-8-3315-8138-1