2023 IEEE International Conference on Power Electronics, Smart Grid, and Renewable Energy (PESGRE) | 979-8-3503-1057-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/PESGRE58662.2023.10404728

An FDI Resilient Dynamic Average Distributed Control for DC Microgrids

Phani Swecha Tadepalli*, *Student Member, IEEE,* Deepak Pullaguram, *Member, IEEE*
M. N. Alam, *Member, IEEE.*

***Abstract*—The distributed control DC microgrids with integrated communication technologies form cyber-physical systems. Cyber-physical DC microgrids rely on peer-to-peer (P2P) communication to regulate average voltage and share proportional power. These P2P communications have greater exposure and increase the possibility of cyber intrusions. This paper aims to develop a cyber-resilient dynamic average consensus control for an autonomous DC microgrid. The proposed dynamic average resilient controller is designed to accurately track the DC microgrid network average voltage despite false data injections (FDI) attacks and also restores average voltage to nominal value while ensuring proportional current sharing. The proposed approach eliminates the need for full network connectivity and without any restrictions on the number of agents attacked. The convergence studies are carried out using input-to-state stability analysis. Further, the simulation results validate the proposed controllers efficacy against actuator and communication layer FDI attacks.**

***Index Terms*—Cyber-Physical Systems, Cyber-attacks, Distributed control, DC Microgrids, Dynamic-average consensus Consensus, False data injection, Resilience.**

I. Introduction

THE emerging DC distributed generators (DG) (like solar, fuel cells) and storage units require fewer conversion stages and suit modern loads, which makes DC microgrids more advantageous at distribution levels [1]. In the microgrid, each DG is expected to share the load changes proportionally. Virtual resistance-based droop control is extensively adopted for improving per-unit current sharing among all DG in the DC microgrids. The virtual resistance and differing line resistances in the network may lead to poor voltage regulation and may not guarantee proportional current sharing. To achieve better voltage regulation and provide improved current sharing, a secondary controller is used in the DC microgrids [2]. These secondary control methods are mostly communication-based and implemented using either centralized or distributed control. The distributed control algorithms can be more robust and adaptable than centralized systems, as they can continue functioning even if one or more DGs fail and require less communication bandwidth [3].

The distributed controllers are designed to coordinate among different agents using peer-to-peer communication to achieve the microgrid objectives: *i)* average voltage regulation, *ii)* proportional current sharing. But this distributed communication also increases the exposure and vulnerabilities to cyber attacks in the DC microgrid [4]. FDI is considered one of the most challenging types of cyberattacks to detect compared to other forms of cyberattacks. In an FDI attack, intruder adds malicious data to actual data to disrupt the system objectives. FDI can occur in different forms, one can devise an FDI to either destabilize the microgrid [5] or to create deception, which deviates operation points without compromising regulation [6]. The main objective of this paper is to design a distributed dynamic averaging control that provides resiliency against FDI attacks on DC microgrids while satisfying the control objectives.

In the literature, many strategies have been proposed for detecting and mitigating attacks, which are mainly classified as model-based and data-driven. The state-of-art literature on these techniques are detailed in [7]. In model-based detection, Observer-based methods [8], [9] are largely adopted. The design complexity of such methods depends on the model's size and may fail under parameter uncertainties. In [10], model- free distributed sliding observer is proposed, which involves the transmission of additional distributed terms, and steady-state chattering may be observed due to the sliding surface. Data-based techniques like Artificial neural networks [11] and reinforcement learning [12] use historical data to detect anomalies in the output. The availability of a high-quality training data set decides the performance of these methods. These detection and mitigation are usually more of an after-event approach, but it is always better to have design-for-security approaches. Thus, many researchers are exploring resilient techniques to offer such a comprehensive solution. [13], uses an event-driven signal constructed from actual measurements to replace attack signals to ensure normal operation during stealth FDI attacks. A trust-based strategy is proposed in [14] to hinder the propagation of the attack to the rest network by reducing the communication weight of the attacked DG. This has limitations on the number of DGs compromised. Multi-layer resiliency in DC microgrid is addressed in [15] using authentication signal for all neighboring agents. These methods may not always guarantee the accurate tracking of average voltage during the attack.

In this paper, an FDI resilient control approach for DC microgrids is developed, to ensure accurate average voltage regulation and sharing proportional power during FDI attacks on both actuator and communication channel. The main contributions of this paper are:

- The proposed control technique effectively estimates and restores the average voltage to nominal value while en-

Phani Swecha Tadepalli and M. N. Alam, are with the Department of Electrical Engineering, National Institute of Technology Warangal, Telangana, India 506004 *Email*: swechagsit@gmail.com, mnalam@nitw.ac.in.

Deepak Pullaguram, is with the Department of Electrical Engineering, Indian Institute of Technology Kharagpur, West Bengal, India 721302. *Email*: drpullaguram@ee.iitkgp.ac.in.

suring proportional power sharing despite of FDI attacks on DC microgrid.
- The designed resilient distributed controller is system-independent, so individual DG has plug-and-play capabilities.
- The proposed method is resilient towards all bounded FDI attacks irrespective of the number of DGs attacked simultaneously.

The subsequent sections of the paper are arranged as follows: In Section II, the cyber and physical aspects of the DC microgrid and problem formulation are detailed. Section III, discusses the proposed resilient strategy against FDI attacks in the DC microgrid. Section IV provides simulation case studies using MATLAB/SIMULINK. Section V provides the conclusion of the paper.

II. Cyber Physical System Modelling

The DC microgrid forms a CPS by integrating physical components (energy generation, power converter, storage, and distribution network) with digital control systems and communication networks. This integration of cyber and physical elements creates a dynamic and interconnected system that can respond to real-time changes in energy demands and other disturbances.

A. Physical Layer

The physical layer of a DC microgrid comprises n DG units interconnected through m distribution lines and feeding multiple distributed loads.

Each DG unit consists of DC voltage source, identifying a dispatchable source such as a fuel cell or renewable sources with storage units having DC output, and a boost converter connected to the point of Common Coupling (PCC) and a local DC load as shown in Fig. 1(a). By applying Kirchhoff's laws, the averaged dynamic model of i^{th} DG boost converter is obtained as,

$$DG_i \begin{cases} L_{fi}\dot{i}_{fi} = v_{dci} - R_{fi}i_{fi} - (1-d_i)v_i, \\ C_{fi}\dot{v}_i = i_{fi}(1-d_i) + i_{ij} - i_{Li}, \end{cases} \tag{1}$$

where, L_{fi}, R_{fi}, and C_{fi} are the boosting inductor, resistance, and filter capacitor of the DC-DC converter of DG_i, respectively. v_{dci}, i_{fi}, d_i, indicates input dc voltage, filter current, and duty cycle of converter i, respectively. v_i is PCC voltage of DG_i, i_{ij} representing current in the distribution line between DG_i and DG_j. The dynamics of the distribution line between DG_i and DG_j are modelled as:

$$\text{Line}_{ij} \begin{cases} L_{ij}\dot{i}_{ij} = v_j - v_i - R_{ij}i_{ij}. \end{cases} \tag{2}$$

Here, R_{ij}, L_{ij} indicates resistance and inductance of the line between DG_i and DG_j. For the distribution lines, $R_{ij} >> L_{ij}$, this implies to $\dot{i}_{ij}$=$-\dot{i}_{ji}$=0 and (2) is modified as

$$i_{ij} = -i_{ji} = (v_j - v_i)/R_{ij}, \tag{3}$$

Now, replacing variable i_{ij} in (1) with (3) results in quasi-stationary line (QSL) approximated model of (1):

$$DG_i \begin{cases} L_{fi}\dot{i}_{fi} = v_{dci} - R_{fi}i_{fi} - (1-d_i)v_i, \\ C_{fi}\dot{v}_i = i_{fi}(1-d_i) + (v_j/R_{ij} - v_i/R_{ij}) - i_{Li}, \end{cases} \tag{4}$$

B. Control layer

In DC microgrid, the controller is designed to ensure proportional load sharing between DGs and maintain the average voltage at PCC. These objectives are achieved by implementing cooperative distributed hierarchical control algorithms [16]. In this, primary and secondary control provides the voltage set point (v^*) to a well-tuned local cascaded voltage and current controller. The voltage set point (v_i^*) of i^{th} DG is given by,

$$v_i^* = v_{nom} - R_{di}i_i + \delta v_i + \delta i_i, \tag{5}$$

where, v_{nom} is nominal voltage of microgrid, R_{di} is the virtual droop impedance, and i_i, is the output current of DG_i. δv_i and δi_i are correction terms of voltage and current mismatch from secondary control. The local inner current and outer voltage controls are implemented using PI controllers [17], whose dynamics are,

$$\dot{\phi}_{vi} = v_i^* - v_i; i_{fi}^* = k_{pv}(v_i^* - v_i) + k_{iv}, \phi_{vi} \tag{6}$$

$$\dot{\phi}_{ci} = i_{fi}^* - i_{fi}; d_i = k_{pc}(i_{f_i}^* - i_{fi}) + k_{ic}, \phi_{ci} \tag{7}$$

where ϕ_{vi} and ϕ_{ci} are the states associated with voltage and current controller, respectively. k_{pv}, k_{iv} and k_{pc}, k_{ic} are the proportional and integral gains of the voltage and current controller, respectively.

The secondary controller is designed to restore the voltage deviation caused by droop and ensure load sharing using correction terms δv_i and δi_i in (5). These are realized by PI controllers, whose inputs are obtained from the resilient distributed controller detailed in the subsequent section. The dynamics of the secondary controllers are given by

$$\dot{\varphi}_{vi} = v_{nom} - \bar{v}_i; \delta v_i = k_{pvs}(v_{nom} - \bar{v}_i) + k_{ivs}\varphi_{vi} \tag{8}$$

$$\dot{\varphi}_{ci} = \bar{i}_i - i_i; \delta i_i = k_{pcs}(\bar{i}_i - i_i) + k_{ics}\varphi_{ci}, \tag{9}$$

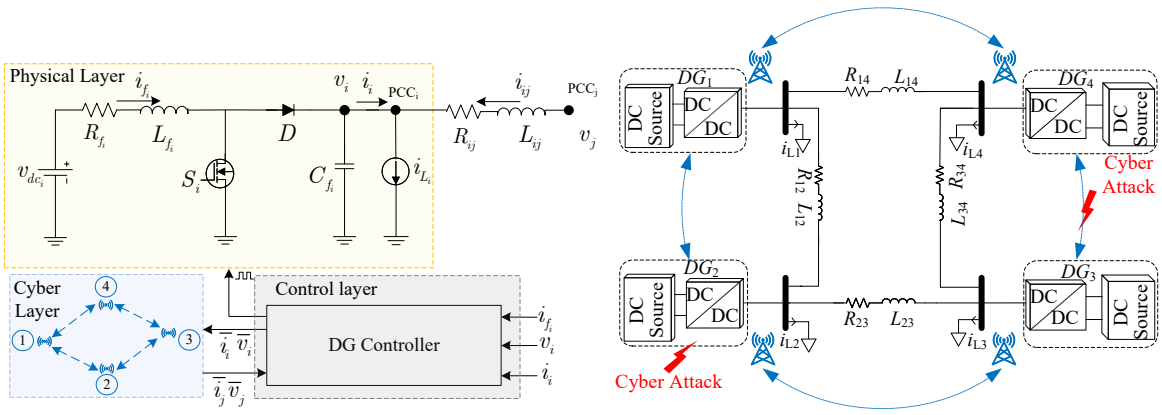
where $\bar{v}_i$ and $\bar{i}_i$, are average voltage and current estimation obtained from the resilient distributed controller. k_{pvs}, k_{ivs} and k_{pcs}, k_{ics} are the proportional and integral gains of the secondary voltage and current correction controllers, respectively. From (4)-(9), the complete state space representation of a DG, can be formulated as,

$$\dot{x}_{DG} = Ax_{DG} + B_1u_{DG} + B_2\bar{u}_{DG}. \tag{10}$$

Here, $x_{DG} = [i_f \ v \ \phi_v \ \phi_c \ \varphi_v \ \varphi_c]^T$ $u_{DG} = [v_{dc} \ i]^T$, and $\bar{u}_{DG} = [\bar{v} \ \bar{i}]^T$. The $\bar{u}_{DG}$, is obtained from the distributed control and is realized using the cyber graph.

C. Cyber Layer

In distributed control, each converter exchanges local variables, $\bar{u} = [\bar{v}, \bar{i}]$, with their neighbors via a communication network, as shown in Fig. 1(a). The cyber communication network of a DC microgrid can be modeled using graph theory. Based on the data flow direction, the graph $G(\mathcal{V}, \mathcal{E}, A_a)$ can be either directed or undirected. The converters are considered as a set of nodes $\mathcal{V} = (1, 2, ...n)$, and communication links between them are depicted by set of edges $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$. The adjacency matrix is indicated by $A_a = [a_{ij}] \in \mathbb{R}^{n\times n}$. $(i, j) \in \mathcal{E}$ are called adjacents and the entire neighboring set



(a) Schematic of a i^{th} DG unit with control and cyber layer

(b) DC microgrid test system with 4 DG

Fig. 1: Schematic of a microgrid test system indicating DG units, physical network, cyber communication network and control unit

of DG_i is represented as $\mathcal{N}_i = j|(i,j) \in \mathcal{E}$. If there is data exchange between DG_i and DG_j, then $a_{ij} = 1$, otherwise $a_{ij} = 0$. The Laplacian matrix $L = D - A_a$, analyzes the distributed graph dynamics. $D = diag\{\sum_{j\in\mathcal{N}_i} a_{ij}\}$ is a degree matrix. The eigenvalues of the L matrix determine the condition for convergence and stability of the system and it mandates that graph G must be a spanning tree for achieving consensus.

D. Problem Statement

In a DC microgrid consisting of n DG units, each DG unit is modeled in the form of (10), and its control input is obtained from the dynamic average consensus algorithm given by:

$$\dot{\bar{x}}_i(t) = \dot{x}_i(t) + u_i(t) \tag{11}$$

where $\bar{x}_i \in \{\bar{v}_i, \bar{i}_i\} \in \mathbb{R}^n$, u_i is the state and control input of i^{th} DG at cyber-layer and $x_i = \{v_i, i_i\} \in \mathbb{R}^n$ is the exogenous input from the physical system. Here, the control protocol u_i shall be designed to fulfill the objectives,

$$\lim_{t\to\infty} (\bar{x}_i(t) - \bar{x}_j(t)) = 0, i, j \in \mathcal{V}, \tag{12}$$

$$\lim_{t\to\infty} \bar{x}_i(t) = x_{avg} = \frac{1}{n}\sum_{k=1}^{n} x_k \tag{13}$$

Further, the communication links at the cyber layer are exposed and may be prone to cyber-attacks, disrupting system operation. Especially the FDI attacks are more tricky to handle as they may destabilize the entire system while remaining undetected if constructed in a stealthy manner. The FDI attacks can be targeted at the actuator and/or the communication channels of i^{th} DG and can be formulated as,

$$\tilde{u}_i = u_i + \eta_i \delta_{u_i}, \text{actuator attack} \tag{14}$$

$$\tilde{\bar{x}}_{ij} = \bar{x}_{ij} + \eta_{ij}\delta_{\bar{x}_{ij}}, \text{communication attack} \tag{15}$$

where, $\tilde{u}_i$ indicates corrupted control input of i^{th} agent with bounded false data δ_{u_i}, $\tilde{\bar{x}}_{ij}$ represents corrupted data received at DG_i from DG_j. $\eta, \eta_{ij} \in 0, 1$ is the activation function, which is 1 in case of attack and 0 otherwise.

This paper proposes a control law, denoted as u_i in (11) , that is both distributed and resilient. The objective is to ensure that the state variable, $\bar{x}_i(t)$, satisfies (12) and (13), even in the presence of cyber-attacks.

III. Proposed False-Data Injection Resilient Consensus Protocol

This section proposes the detailed design dynamic average consensus protocol to withstand FDI attacks in DC microgrid systems. Each agent tracks the average of a time-varying exogenous input signal x_i of i^{th} DG using the following consensus protocol [18]:

$$\begin{aligned}\dot{\bar{x}}_i &= \alpha(x_i - \bar{x}_i) + \sum_{j\in\mathcal{N}_i} \beta\left(\alpha(\bar{x}_j - \bar{x}_i) - (\sigma_{x_j} - \sigma_{x_i})\right) + \dot{x}_i \\ \dot{\sigma}_i &= \alpha(x_i - \sigma_i) + \sum_{j\in\mathcal{N}_i} \beta(\alpha(\sigma_j - \sigma_i) + (\bar{x}_j - \bar{x}_i)) + \dot{x}_i\end{aligned} \tag{16}$$

Here, $x_i(t)$ and σ_i are time-varying reference and state of i^{th} DG, α and β are positive gains that are obatined using the eigenvalues of L. Considering bounded FDI attack $(d(t), d^{'}(t))$, (16) can be reformulated in vector form as,

$$\begin{aligned}\dot{\bar{x}} &= \alpha(x - \bar{x}) - \alpha\beta L\bar{x} + \beta L\sigma + \dot{x} + d(t) \\ \dot{\sigma} &= \alpha(x - \sigma) - \alpha\beta L\sigma - \beta L\bar{x} + \dot{x} + d'(t)\end{aligned} \tag{17}$$

In order to demonstrate that (16) achieves dynamic average consensus, two error vectors are defined,

$$e_{\bar{x}} = \bar{x} - \frac{1}{n}1_n 1_n^\top x; \quad e_\sigma = \sigma - \frac{1}{n}1_n 1_n^\top x. \tag{18}$$

From the property of L, we have $Le_{\bar{x}} = L\bar{x}$ and $Le_\sigma = L\sigma$. Differentiating (18), one can obtain,

$$\begin{aligned}\dot{e}_{\bar{x}} &= -(\alpha I_n + \alpha\beta L)e_{\bar{x}} + \beta L e_\sigma + \Pi_n(\alpha x + \dot{x}), \\ \dot{e}_\sigma &= -(\alpha I_n + \alpha\beta L)e_\sigma - \beta L e_{\bar{x}} + \Pi_n(\alpha x + \dot{x}).\end{aligned} \tag{19}$$

Here Π_n=$I_n - \frac{1}{n}1_n 1_n^\top \dot{x}$. Further, (19) is written as,

$$\dot{\varrho} = E\varrho + \Gamma(\alpha x, \dot{x}), \tag{20}$$

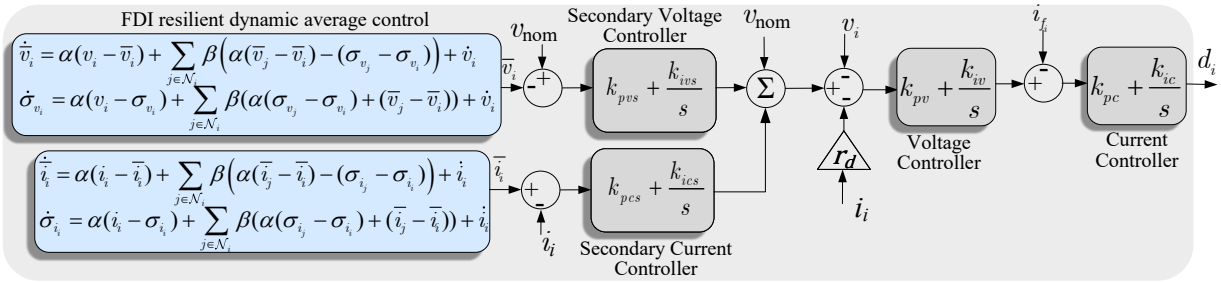


Fig. 2: FDI Resilient distributed dynamic average control strategy for DC microgrid system

where, $\varrho = [e_{\bar{x}}^\top,\ e_\sigma^\top]^\top$, $\Gamma(\alpha x, \dot{x}) = [1,\ 1]^\top \otimes \Pi_n(\alpha x + \dot{x})$, and $E = \begin{bmatrix} -(\alpha I_n + \alpha\beta L) & \beta L \\ -\beta L & -(\alpha I_n + \alpha\beta L) \end{bmatrix}$.
To prove the stability of (20), first, the system with $x(t) = 0$ is considered, then,

$$\dot{\varrho} = E\varrho \tag{21}$$

Applying transformation on

$$\varrho = \mathcal{T}R\bar{\varrho}, \mathcal{T} = \begin{bmatrix} iI_n & -iI_n \\ I_n & I_n \end{bmatrix}, R = blockdiag(\mathbf{V}, \mathbf{V}). \tag{22}$$

Here, $\bar{\varrho} = [\hat{\varrho}_1, \tilde{\varrho}_1, \tilde{\varrho}_2 ..... \tilde{\varrho}_{n-1}, \hat{\varrho}_2, \tilde{\varrho}_n, ... \tilde{\varrho}_(2n-2)]^T$,$\mathbf{V}$ is a matrix of left eigen vectors of L. Upon differentiating, (22), is obtained as

$$\dot{\bar{\varrho}} = \Lambda\bar{\varrho}; \Lambda = \begin{bmatrix} -\alpha I_n + \alpha\beta\mathbf{J} + i\beta\mathbf{J} & 0 \\ 0 & -\alpha I_n + \alpha\beta\mathbf{J} - i\beta\mathbf{J} \end{bmatrix} \tag{23}$$

Here, $\mathbf{J} = blockdiag(0, \tilde{\mathbf{J}})$ represents Jordan normal form of $-L$, $(i.e., -L = \mathbf{V}\mathbf{J}\mathbf{V}^{-1})$ and $\lambda_i(\mathbf{J}) = \lambda_i(L) \forall i \in \mathcal{V}$.
Hence, the eigenvalue of E is:

$$\lambda_i(E) = -\alpha - \alpha\beta\delta_i + i\beta\delta_i \forall i \in \mathcal{V}. \tag{24}$$

where δ_i is the i^{th} eigenvalue of L and $\delta_i > 0 \forall i = 2, ..n$, This ensures system stability if $\alpha > 0$ and $\beta > 0$.
Next, considering the system (20) with $x(t) \neq 0$, factoring out dynamics associated to zero eigen value of L:

$$\dot{\hat{\varrho}} = \Upsilon\hat{\varrho}, \quad \Upsilon = \text{diag}(-\alpha, -\alpha), \tag{25a}$$

$$\dot{\tilde{\varrho}} = \tilde{\Lambda}\tilde{\varrho} + \tilde{\Gamma}(\alpha x, \dot{x}). \tag{25b}$$

where,$\hat{\varrho} = [\hat{\varrho}_1, \hat{\varrho}_2]^T$, $\tilde{\varrho} = [\tilde{\varrho}_1, ... \tilde{\varrho}_{2n-2}]^T$, $\tilde{\Gamma}(\alpha x, \dot{x}) = [\tilde{\Gamma}_1, ..., \tilde{\Gamma}_{2n-2}]$ and $\tilde{\Lambda}$=blockdiag $(-\alpha I_{n-1} + \alpha\beta\tilde{\mathbf{J}} + i\beta\tilde{\mathbf{J}}$, $-\alpha I_{n-1} + \alpha\beta\tilde{\mathbf{J}} - i\beta\tilde{\mathbf{J}})$=$P + \beta Q$, where Q=blockdiag($i\tilde{\mathbf{J}}$,-$i\tilde{\mathbf{J}}$), P=blockdiag($\alpha I_{n-1} + \alpha\beta\tilde{\mathbf{J}}$, $-\alpha I_{n-1} + \alpha\beta\tilde{\mathbf{J}}$).

To prove that (20) is input-to-state stable (ISS), we prove ISS of its equivalent system (25a)-(25b). For any $\alpha > 0$, the system (25a) is asymptotically stable. As we know $\tilde{\Lambda}$, is Hurwitz, for $\alpha > 0$ and $\beta > 0$, the solution of (20) is,

$$\tilde{\varrho}(t) = exp(t\tilde{\Lambda})\tilde{\varrho}(0) + \int_0^t exp((t-\tau)\tilde{\Lambda})\tilde{\Gamma}(\alpha x, \dot{x})\, d\tau. \tag{26}$$

Using inequality $||exp(t(\bar{\Lambda}))|| \leq exp(\mu(\bar{\Lambda}(t)))$, the solution can be modified as:

$$||\tilde{\varrho}(t)|| \leq exp(\mu\tilde{\Lambda}t)\ ||\tilde{\varrho}(0)|| + \int_0^t exp(\mu\tilde{\Lambda}(t-\tau))\ ||\tilde{\Gamma}||\ d\tau \tag{27}$$

TABLE I: System parameters

Parameter	Value
L_i	$3mH$
C_i	$250\mu F$
Load resistance	$R_1 = R_2 = 20\Omega$, $R_3 = R_4 = 30\Omega$
Line resistance	$R_{12} = 0.6\Omega$ $R_{14} = 1\Omega$ $R_{34} = 3\Omega$ $R_{23} = 1.8\Omega$.
Line inductance	$L_{12} = 50\mu H$ $L_{14} = 60\mu H$ $L_{34} = 75\mu H$ $L_{23} = 65\mu H$
Device level control gains	Voltage controller: $K_{pv} = 3, k_{iv} = 10$; Current controller: $K_{pc} = 0.1, k_{ic} = 3.5$
Droop resistance	0.33Ω

where, $\mu(\tilde{\Lambda})$ is the measure of matrix, and from its property, $\mu(\tilde{\Lambda}) = \mu(P + \beta Q) \leq \mu(P) + \beta\mu(Q)$, this implies to,

$$||\tilde{\varrho}(t)|| \leq exp((-\kappa)t)\ ||\tilde{\varrho}(0)|| + 1/(\kappa) \sup_{0 \leq \tau \leq t} ||\tilde{\Gamma}(\alpha x, \dot{x})|| \ . \tag{28}$$

Here, $\kappa = \alpha + \alpha\beta\lambda_2(sym(L) - \beta\mu(Q))$, $\mu_2(\alpha\beta\tilde{\mathbf{J}}) = -\alpha\beta\lambda_2(sym(L))$, $sym(L) = \frac{1}{2}(L + L^\top)$ and $\lambda_2(sym(L)$ is second eigne value of $sym(L)$. The error corresponding to zero input response of (28) approaches zero exponentially if α and β are chosen such that $\alpha + \alpha\beta\lambda_2(sym(L)) > \beta\mu(Q)$. It can be observed from (28), that when $\alpha > \mu(Q)/\lambda_2(sym(L))$, and the error decreases to zero, as the value of β increases. Now, by premultiplying $\dot{e}_{\bar{x}}$ and $\dot{e}_\sigma$ in (19) by 1_n^T and using balanced property of graph G,

$$\sum_{i=1}^n \dot{e}_{x_i} = -\alpha \sum_{i=1}^n \dot{e}_{x_i}, \sum_{i=1}^n \dot{e}_{\sigma_i} = -\alpha \sum_{i=1}^n \dot{e}_{\sigma_i} \tag{29}$$

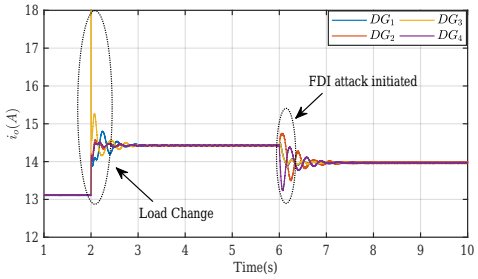
As a result, $x_{avg} = 1/n \sum_{i=1}^n x_i$ remains within the state trajectories $\bar{x}_i$ and $\sigma_i\ \forall i \in 1, 2..n$. This proves that dynamic average consensus (16), can dynamically track the average value of exogenous input.

IV. Results and Discussion

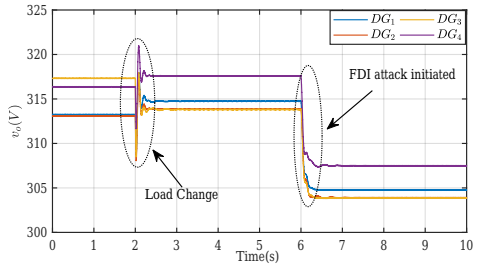
The proposed control strategy is tested on a DC microgrid with 4 DG sources and communication topology, as shown in Fig.1. Each DG has a rated capacity of $5kW$, and the nominal voltage is selected as $315V$. The Table. I details the line distribution network and system parameters used for simulation. The test system is simulated in MATLAB/SIMULINK platform under different operating conditions.

A. Microgrid Operation with Conventional Control under Actuator FDI Attack

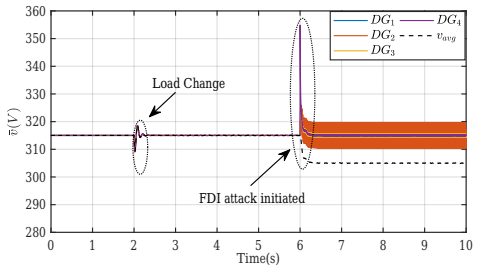
The DC microgrid operation with the conventional dynamic average consensus [16] under actuator FDI attacks is evaluated in this case study. Initially, the system is at a steady state, all DGs share load the total load of $16.5kW$ proportionally, as shown in Fig.3(a), while maintaining the average voltage at a nominal value. At $t = 2s$, a load of $1.5kW$ is increased at DG_3, and the controller responds to load change and esures the load variation is distributed among all DGs. At $t = 6s$, a bounded stealth FDI attack vector $\delta_{u_i} = [0 \quad 5sin(100\pi t) \quad 0 \quad 40]$ is injected into the actuator of DGs. This attack did not induce any steady state deviations on the average voltage estimate ($\bar{v}$) at individual DGs, as shown in Fig. 3(c) and it appears as a load change to the operator as seen in Fig.3(a). But the actual output voltages and the true average value of the actual voltages were largely deviated from the nominal values, which can be observed from Fig.3(b) and Fig.3(c), respectively. The results in Fig.3 demonstrate the deception caused due to FDI attacks. This attack is not easily detectable with traditional approaches and may endanger the operation of the microgrid.



(a) Output current of DGs



(b) Ouput voltages of DGs

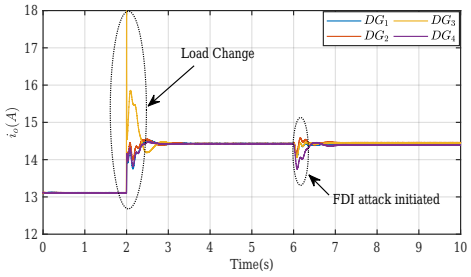


(c) Average voltage of DGs

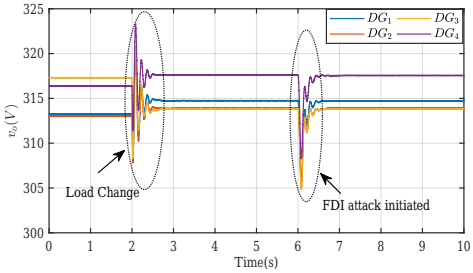
Fig. 3: DC microgrid operation with proposed consensus algorithm under link failure conditions

B. Microgrid Operation with Proposed Resilient Control under Actuator FDI Attack

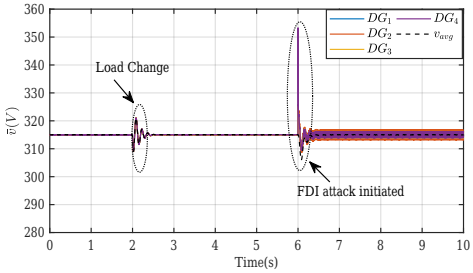
This case study examines the operation of a microgrid with proposed controller under load change conditions and evaluates the resiliency against actuator FDI attacks. Initially, the system is operating as in the previous case study. At $t = 2s$, the load at DG_3 has increased by $1.5kW$, which is proportionally distributed among the DGs and average voltage is regulated by the proposed controller, as shown in Fig. 4. A time-varying bounded attack vector δ_{u_i} similar to that of the previous case is injected into all DGs, at $t = 6s$. This attack has led to some transient voltage drop across all the DGs, as shown in Fig. 4(b). But in less than $1s$, the voltages and currents were restored to their pre-attack condition by



(a) Output current of DGs



(b) Ouput voltages of DGs



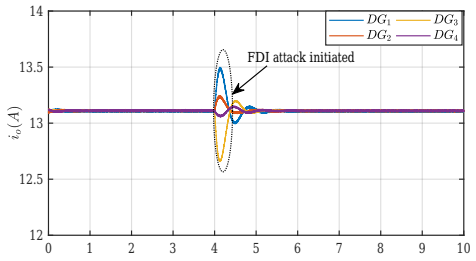
(c) Average voltage of DGs

Fig. 4: Performance of DC microgrid under actuator FDI attacks on all DGs

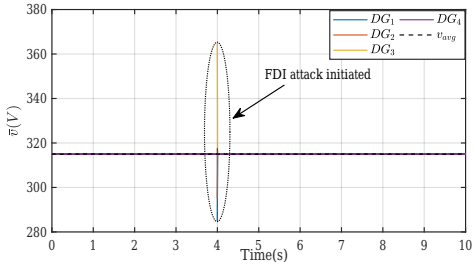
the resilient action of the proposed controller. Further, the average voltage estimated ($\bar{v}$) at all DGs perfectly tracked the true average voltage as shown in Fig. 4(c) and regulated at the nominal value, $V_{nom} = 315V$, unlike in the conventional controller (Fig. 3(c)).

C. Communication and actuator FDI attacks on all DGs

The microgrid operation under the combination of communication and actuator attacks is evaluated in this case study. To evaluate the performance of microgrid operation with multiple attacks, simultaneous attacks were performed on all DGs. At $t = 4s$, an attack vector of $\delta_i = [10 \ -50 \ 20 \ 30]$ is injected at all DG actuators, and the same is communicated with the neighboring agents. A significant transient is observed in average voltage and currents as shown in Fig.5, which are damped within $1s$ and reached to pre-attack conditions.



(a) Output current of DGs



(b) Average voltage of DGs

Fig. 5: Resilient DC microgrid: attack on the actuator and communication link

V. Conclusion

This paper presents a distributed control DC microgrid system that is resilient to FDI attacks. In the DC microgrid, the proposed secondary controller ensures for accurate tracking of the dynamic average voltage of the network, which is regulated at nominal value while ensuring proportional current sharing even during attacks. The proposed controller is independent of the attack or system model and makes DC microgrid resilient against any bounded attacks. Dynamic average voltage tracking convergence is proved using input-to-system stability analysis. Through various simulation studies under different attack scenarios and operating conditions, the resiliency of proposed controller is tested. It was observed from results that, even under the multiple attacks on all DGs, both at the actuator and in communication, the microgrid was resilient and could able to fulfill the desired control objectives.

Acknowledgment

This work is partly supported by the NITW-Hitachi Energy Smart Electric Grid Laboratory and by the Science & Engineering Research Board (SERB), Govt. of India, under the head of SRG/2020/002557

References

[1] N. Eghtedarpour and E. Farjah, "Power control and management in a hybrid ac/dc microgrid," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1494–1505, 2014.

[2] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical control of droop-controlled ac and dc microgrids—a general approach toward standardization," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 1, pp. 158–172, 2011.

[3] E. Espina, J. Llanos, C. Burgos-Mellado, R. Cárdenas-Dobson, M. Martínez-Gómez, and D. Sáez, "Distributed control strategies for microgrids: An overview," *IEEE Access*, vol. 8, pp. 193 412–193 448, 2020.

[4] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2693–2703, 2017.

[5] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragičević, "On detection of false data in cooperative dc microgrids—a discordant element approach," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, 2020.

[6] D. Shi, P. Lin, Y. Wang, C.-C. Chu, Y. Xu, and P. Wang, "Deception attack detection of isolated dc microgrids under consensus- based distributed voltage control architecture," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 1, pp. 155–167, 2021.

[7] P. S. Tadepalli and D. Pullaguram, "Distributed control microgrids: Cyber-attack models, impacts and remedial strategies," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 8, pp. 1008–1023, 2022.

[8] T. Wang, L. Liang, S. K. Gurumurthy, F. Ponci, A. Monti, Z. Yang, and R. W. De Doncker, "Model-based fault detection and isolation in dc microgrids using optimal observers," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5613–5630, 2021.

[9] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to dc microgrids," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3800–3815, 2020.

[10] 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.

[11] 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 Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 2, pp. 717–721, 2021.

[12] A. J. Abianeh, Y. Wan, F. Ferdowsi, N. Mijatovic, and T. Dragičević, "Vulnerability identification and remediation of fdi attacks in islanded dc microgrids using multiagent reinforcement learning," *IEEE Transactions on Power Electronics*, vol. 37, no. 6, pp. 6359–6370, 2022.

[13] S. Sahoo, T. Dragičević, and F. Blaabjerg, "An event-driven resilient control strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 35, no. 12, pp. 13 714–13 724, 2020.

[14] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, "Resilient cooperative control of dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 1083–1085, 2019.

[15] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Multilayer resilience paradigm against cyber attacks in dc microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 3, pp. 2522–2532, 2021.

[16] V. Nasirian, S. Moayedi, A. avoudi, and F. L. Lewis, "Distributed cooperative control of dc microgrids," *IEEE Transactions on Power Electronics*, vol. 30, no. 4, pp. 2288–2303, 2015.

[17] D. Pullaguram, S. Mishra, and N. Senroy, "Event-triggered communication based distributed control scheme for dc microgrid," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5583–5593, 2018.

[18] M. Iqbal, Z. Qu, and A. Gusrialdi, "Resilient dynamic average-consensus of multiagent systems," *IEEE Control Systems Letters*, vol. 6, pp. 3487–3492, 2022.