2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Resilient Control of DC Microgrids Against FDI Attacks on Communication Links

Qifen Liu and Hongwei Zhang

Abstract— **The intrusion of cyber attacks on communication network in microgrids will deteriorate the control performance. And it is even more difficult to effectively extract unknown attacks to obtain correct transmitted information for a direct current (DC) microgrid. In this paper, a resilient controller is designed to mitigate the adverse effects of false data injection (FDI) attacks, where the DC microgrids could restore their control objectives, including current sharing and voltage regulation. Furthermore, the restriction on the number of healthy neighbors is relaxed in this proposed control scheme compared with related researches on mitigating FDI attacks on communication links. The effectiveness of this resilient controller is illustrated by numerical examples.**

I. Introduction

In order to cope with global energy crisis and climate warming, renewable energy sources such as photovoltaics and wind energy, whose outputs tend to exhibit direct current (DC) characteristics, are widely applied to microgrids. These energy sources can be compatible with DC loads, which greatly saves the hardware cost of microgrids and improves their power quality. Therefore, research on DC microgrids has rapidly progressed in recent years [1].

In general, there exist multiple distributed power sources in microgrids. For the stable operation of DC microgrids, it is necessary to coordinate these sources to guarantee voltage stability and reasonably allocate the contribution of each source [2]. To achieve the above two objectives, a hierarchical cooperative control structure has been proposed for DC microgrids, which includes primary control, secondary control and tertiary control [3], [4]. Tertiary control optimizes the power flow between microgrids and their main networks. Primary control is adopted to realize voltage stability as a local control method, in which droop mechanism is commonly implemented. However, power line impedances reduce the accuracy of power distribution among power sources, which resorts to secondary control to compensate for the loss.

Distributed secondary control becomes a candidate with general approval because it avoids the single-point failures inherent in centralized control schemes [5]. In [6], [7], a distributed cooperative algorithm is designed to achieve current sharing and voltage balance in DC microgrids. Its average voltage of buses is estimated via distributed observers and adjusted to reach the reference voltage. In [8], [9], a second-order distributed controller is proposed for current sharing and voltage regulation in DC microgrids, whose voltage regulation is independent of measured bus voltages. It must be emphasized that the satisfactory performance of these distributed controllers heavily relies on the integrity of communication networks. Therefore, the potential provocation originating from cyber-attacks will destroy the performance of secondary controllers, and cannot be ignored when exploring control protocols in microgrids.

False data injection (FDI) attack, one of the most common types of cyber-attack, deliberately tampers with the transmitted data via invading communication networks, so as to undermine the desired control objectives in microgrids. Therefore, distributed microgrids urgently need to counter-attack against cyber-attacks. In [10], an FDI attack detection strategy based on discordant element is utilized for secondary control in DC microgrids. However, this work only investigates a detection method, without providing a mitigation technique against FDI attacks upon detection. A cooperative controller for mitigating constant FDI attacks is provided via dynamically adjusting communication weights in alternating current (AC) microgrids, which represent agents' approval to the information their received [11]. Subsequently, this approach is verified by simulation examples that it is also suitable for DC microgrids under FDI attacks [12]. Nevertheless, the above two mitigation works are conducted on the premise that at least half of neighbors are healthy. That is, once more than half of neighbors are attacked, this mitigation technique will be invalid. To relax this restriction, a resilient controller is proposed to mitigate the adverse effects of FDI attacks via introducing an adaptive compensational term [13]. However, this compensational term can only deal with attacks on local control input channel of each converter, and is invalid when subjected to attacks on communication links.

It is particularly noticed that a limit on the health of neighbors is imposed in the existing researches on communication link attacks in DC microgrids. Considering the above-mentioned statements, in this paper, we aim to provide a resilient controller, as a complement to existing detection techniques, to protect the DC microgrids against constant FDI attacks, especially for attacks on communication links.

The rest of this paper is organized as follows. Section II presents notations, and preliminaries on communication

This paper was supported by the Shenzhen Science and Technology Program under project JCYJ20220818102416036, and by the Guangdong Basic and Applied Basic Research Foundation under project 2023A1515011981.

Qifen Liu is with the Key Laboratory of Magnetic Suspension Technology and Maglev Vehicle, Ministry of Education, School of Electrical Engineering, Southwest Jiaotong University, Chengdu, Sichuan, 611756, P.R. China (Email: qfliu@my.swjtu.edu.cn).

Hongwei Zhang is with the School of Mechanical Engineering and Automation, Harbin Institute of Technology, Shenzhen, Guangdong 518055, P.R. China, and also with the Guangdong Provincial Key Laboratory of Intelligent Morphing Mechanisms and Adaptive Robotics, Shenzhen, Guangdong 518055, P.R. China (Email: hwzhang@hit.edu.cn).

All correspondence should be addressed to Hongwei Zhang.

network and electrical network of DC microgrids. In Section III, a cooperative control scheme for DC microgrids is introduced first, and then its corresponding resilient controller is designed to handle FDI attacks, along with the stability analysis. Section IV provides simulation examples to illustrate the performance of proposed resilient controller. Section V concludes this paper.

II. Preliminaries

A. Notations

A positive definite (positive semidefinite) matrix A is denoted by $A > 0$ ($A \geq 0$). A diagonal matrix B with b_i being the ith diagonal entry is denoted as $B = diag(b_1, b_2, \cdots, b_n)$. The $n \times 1$ column vector of ones is denoted as $\underline{1}_n$. The inverse of an invertible matrix C is denoted as C^{-1}. The identity matrix is E.

B. Communication network of DC microgrids

In order to realize the distributed cooperative control in DC microgrids, it is necessary to build a communication network among their secondary controllers for information exchange. A communication network could be modeled as a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{v_1, v_2, \cdots, v_n\}$ denotes the node set, and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ denotes the edge set. In DC microgrids, distributed generators (DGs) and their communication links could be considered as nodes and edges of a graph $\mathcal{G}$, respectively.

A communication graph $\mathcal{G}$ could be characterized by its adjacency matrix $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{n \times n}$, where a_{ij} is a weight of (v_j, v_i), $a_{ij} > 0$ if $(v_j, v_i) \in \mathcal{E}$ and $a_{ij} = 0$ if $(v_j, v_i) \notin \mathcal{E}$. A graph $\mathcal{G}$ is undirected if $\mathcal{A}^\top = \mathcal{A}$. The Laplacian matrix $\mathcal{L} = [l_{ij}] \in \mathbb{R}^{n \times n}$ of a graph $\mathcal{G}$ is defined as $l_{ii} = \sum_{j=1, j \neq i}^{n} a_{ij}$ and $l_{ij} = -a_{ij}$ if $i \neq j$. For an undirected graph $\mathcal{G}$, $\mathcal{L}^\top = \mathcal{L}$, $\underline{1}_n^\top \mathcal{L} = 0$ and $\mathcal{L}\underline{1}_n = 0$. An undirected graph $\mathcal{G}$ is connected, if there exists a path between any two nodes.

Assumption 1: The communication graph of DC microgrids is undirected and connected.

C. Electrical network of DC microgrids

In DC microgrids, as shown in Fig.1, each distributed energy source is connected to a DC bus by a converter and a series LC filter [8]. This integrated package is called a distributed generation unit (DGU). Consider a DC microgrid consisting of n DGUs, n local loads and m power lines, where these n DGUs are interconnected via m resistive-inductive power lines.

The dynamic characteristics of DGU i can be expressed as follows, upon applying the Kirchoff's Current Law (KCL) and Kirchoff's Voltage Law (KVL).

$$\begin{cases} L_{ti}\dot{I}_{ti} = -V_i + v_i^* \\ C_{ti}\dot{V}_i = I_{ti} - \sum_{j \in \varepsilon_i} I_j - I_{Li} \\ L_j\dot{I}_j = (V_i - V_j) - R_j I_j \end{cases}, \tag{1}$$

where L_{ti} and C_{ti} are the inductance and capacitance of LC filter i; L_j and R_j are the inductance and resistance of power line j; I_{ti} and v_i^* are the output current and local voltage setpoint of converter i; V_i is the bus voltage of node i; I_{Li} is the current drawn by local load i; I_j is the current of power line j; and ε_i is the set of power lines which are physically connected with DGU i.

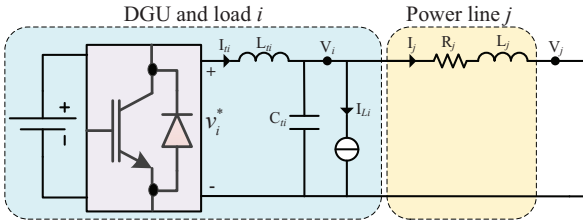

Fig. 1. An electrical network of DC microgrid.

Considering an electrical topology with n DGUs and m power lines, in which each power line is assigned to a unique index $e \in \{1, 2, \cdots, m\}$ and an arbitrary direction, the incidence matrix [14] $\mathcal{B} = [b_{ie}] \in \mathbb{R}^{n \times m}$ is defined as

$$b_{ie} = \begin{cases} +1, & if\ the\ edge\ e\ is\ (v_i, v_j)\ for\ some\ j \\ -1, & if\ the\ edge\ e\ is\ (v_j, v_i)\ for\ some\ j \\ 0, & otherwise \end{cases}.$$

We can rewrite (1) in a compact form:

$$\begin{cases} L_t\dot{I}_t = -V + V^* \\ C_t\dot{V} = I_t + \mathcal{B}I - I_L \\ L\dot{I} = -\mathcal{B}^\top V - RI \end{cases}, \tag{2}$$

where $L_t = diag(L_{t1}, L_{t2}, \cdots, L_{tn})$, $C_t = diag(C_{t1}, C_{t2}, \cdots, C_{tn})$, $L = diag(L_1, L_2, \cdots, L_m)$, $R = diag(R_1, R_2, \cdots, R_m)$, $I_t = [I_{t1}, I_{t2}, \cdots, I_{tn}]^\top$, $V^* = [v_1^*, v_2^*, \cdots, v_n^*]^\top$, $V = [V_1, V_2, \cdots, V_n]^\top$, $I_L = [I_{L1}, I_{L2}, \cdots, I_{Ln}]^\top$ and $I = [I_1, I_2, \cdots, I_m]^\top$.

III. Resilient control in DC microgrids

A. Problem formulation

For normal operation in DC microgrids, it is necessary to guarantee reasonable current distribution among power sources and suitable bus voltage. In this paper, we aim to regulate the current and bus voltage to satisfy the following two objectives in DC microgrids:

- Output currents are in proportion to the rated currents of corresponding converters [6], [8], [13], i.e.,

$$\lim_{t \to \infty} \frac{I_{ti}(t)}{I_i^{rat}} = \lim_{t \to \infty} \frac{I_{tj}(t)}{I_j^{rat}},$$

  $\forall i, j \in \{1, 2, \cdots, n\}$, where I_i^{rat} is the rated current of the ith converter.
- The average voltage across the DC microgrid is regulated to a specific reference voltage [6], [10], [13], i.e.,

$$\lim_{t \to \infty} \frac{1}{n} \sum_{i=1}^{n} V_i(t) = v_{ref},$$

  where v_{ref} is the global reference voltage.

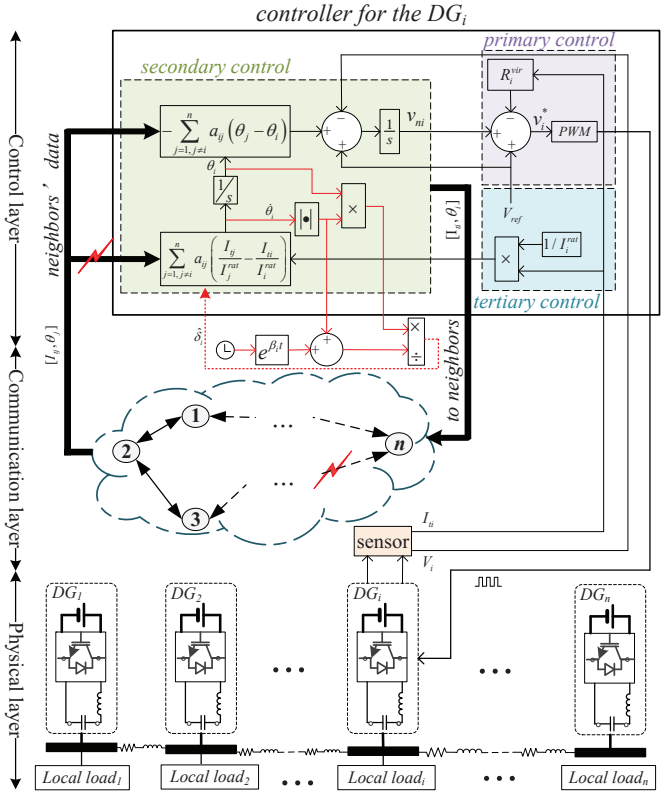

Fig. 2. A general DC microgrid. (The red line in control layer is resilient modules we provided, and the dashed red line means this DG is under cyber attacks.)

Figure 2 illustrates the physical, communication, and control layers in a general DC microgrid. The physical layer is an electrical network composed of n DGUs and m power lines. The communication layer undertakes information transfer among these n DGUs. And the control layer is responsible for realizing the above two objectives in DC microgrids.

For the integrity of control structure, primary control and secondary controls are incorporated into this paper. Like most works [6], [13], we employ the droop mechanism as a local control mechanism for voltage stabilization acting on local information with a virtual resistance R_i^{vir} to alter voltage setpoint v_i^* of converter i, and v_i^* is given as:

$$v_i^* = v_{ref} + v_{ni} - R_i^{vir} I_{ti}, \tag{3}$$

where v_{ni} is selected by secondary control to compensate for primary control, and its derivative could be obtained by the output u_i of a cooperative secondary law at DGU i, i.e.,

$$\dot{v}_{ni} = u_i. \tag{4}$$

In order to realize the above two objectives (current sharing and voltage regulation), u_i is derived through the following second-order distributed control protocol, which is based on the output current information with respect to its neighboring converters [8], [9].

$$\begin{cases} u_i = -\sum\limits_{j=1,j\neq i}^{n} a_{ij}\left(\theta_j - \theta_i\right) + g_i(v_{ref} - V_i) \\ \dot{\theta}_i = \sum\limits_{j=1,j\neq i}^{n} a_{ij}\left(\frac{I_{tj}}{I_j^{rat}} - \frac{I_{ti}}{I_i^{rat}}\right) \end{cases}, \tag{5}$$

where θ_i is an auxiliary variable, and a positive g_i means the DGU i can access to the reference voltage v_{ref}. Obviously, the neighboring information required in control protocol (5) always has to rely on a communication network $\mathcal{G}$. However, cyber attacks have long been stalking the transmitted message over communication networks. Once the intrusion of cyber attacks is not intervened in time, it will bring invalidation scenarios to these cooperative controllers.

In the presence of unknown FDI attacks injected to a communication link, the corrupted measurements of I_{tj} received by the ith converter can be expressed as

$$\hat{I}_{tj} = I_{tj} + \sigma_j, \tag{6}$$

where σ_j denotes the injections launched by the communication link attackers. When a communication network $\mathcal{G}$ is healthy, $\sigma_j = 0$. In practical scenarios, the attackers may have limited budgets to inject into microgrids [15]. Therefore, it is reasonable to assume that σ_j is bounded $\forall j \in \{1, 2, \cdots, n\}$. We further suppose Assumption 2 holds.

Assumption 2: The attack signal is assumed to be constant [11], [12].

Generally, the distributed algorithm (5) fails to achieve the control objectives in DC microgrids when DGU i receives a fake neighboring message, such as $\hat{I}_{tj}$. Of course, we do not have the ability to effectively extract unknown attacks to obtain correct neighboring information I_{tj} for an operating DC microgrid. Based on the above facts, we aim to provide a resilient controller in this paper to mitigate the adverse effects of FDI attacks defined in (6) and do not impose a limit on the health of neighbors.

B. Resilient control protocol

In this section, we aim to offset the fatal flaws in cooperative secondary controller (5) from FDI attacks as much as possible by constructing a variable to approximate the amount of attacks pumped into node i. Hence, on the basis of secondary control law (5), a resilient controller is designed via introducing an adaptive compensational term to mitigate FDI attacks as follow:

$$\begin{cases} u_i = -\sum\limits_{j=1,j\neq i}^{n} a_{ij}\left(\theta_j - \theta_i\right) + g_i(v_{ref} - V_i) \\ \dot{\theta}_i = \sum\limits_{j=1,j\neq i}^{n} a_{ij}\left(\frac{\hat{I}_{tj}}{I_j^{rat}} - \frac{I_{ti}}{I_i^{rat}}\right) - \gamma_i\hat{\delta}_i \\ \dot{\hat{\delta}}_i = \dfrac{\alpha_i\theta_i\dot{\theta}_i\mathrm{sgn}\dot{\theta}_i}{\dot{\theta}_i\mathrm{sgn}\dot{\theta}_i + e^{-\beta_i t}} \end{cases} \tag{7}$$

where $\hat{\delta}_i$ is a compensational term to estimate the communication attack signal δ_i, and $\delta_i \triangleq \sum\limits_{j\in\mathcal{N}_i} \sigma_j$ is the injection sum of all communication link attacks on DGU i ($\mathcal{N}_i$ is the neighbors set of node i); α_i and β_i are both positive

constants; the constant γ_i is a sign of whether node i is under attack. If all communication links of node i are healthy, $\gamma_i = 0$, otherwise $\gamma_i = 1$.

Remark 1: There are plentiful research outputs on cyber attack detection in microgrids [10]–[12], [16], which could target specific variables under cyber attacks. It is explicit that these detection techniques are sufficient to determine γ_i, because it only depends on whether the node i is attacked, and does not need to further clarify the specific variables being attacked. In addition, arbitrary delays could be tolerated between node i being aware of cyber attacks and the intervention of a compensation signal $\tilde{\delta}_i$ in (7), which leaves sufficient operating time for practical systems.

C. Stability analysis

Applying the primary and secondary control protocol (3)-(5) to DC microgrids (1), the dynamics of closed-loop system can be written in a compact form:

$$\begin{cases} L_t\dot{I}_t = -V + V_{ref} + V_n - R^{vir}I_t \\ C_t\dot{V} = I_t + \mathcal{B}I - I_L \\ L\dot{I} = -\mathcal{B}^\top V - RI \\ \dot{V}_n = \mathcal{L}\Theta + G(V_{ref} - V) \\ \dot{\Theta} = -\mathcal{L}(I^{rat})^{-1}I_t \end{cases}, \tag{8}$$

where $V_{ref} \triangleq v_{ref}\underline{1}_n$, $V_n \triangleq [v_{n1}, v_{n2}, \cdots, v_{nn}]^\top$, $R^{vir} \triangleq diag(R_1^{vir}, R_2^{vir}, \cdots, R_n^{vir})$, $\mathcal{L} \in \mathbb{R}^{n\times n}$ is the Laplacian matrix associated with communication network $\mathcal{G}$ in DC microgrids, $\Theta \triangleq [\theta_1, \theta_2, \cdots, \theta_n]^\top$, $G \triangleq diag(g_1, g_2, \cdots, g_n)$, and $I^{rat} \triangleq diag(I_1^{rat}, I_2^{rat}, \cdots, I_n^{rat})$.

Theorem 1: Suppose Assumption 1 holds. The closed-loop system (8) is stable; and exact current sharing and voltage regulation for DC microgrids can be achieved.
The proof is omitted due to space limitation.

While encountering FDI attacks, the dynamics of resilient closed-loop system can be established in a compact form by applying resilient control protocol (3), (4) and (7) to DC microgrids (1):

$$\begin{cases} L_t\dot{I}_t = -V + V_{ref} + v_n - R^{vir}I_t \\ C_t\dot{V} = I_t + \mathcal{B}I - I_L \\ L\dot{I} = -\mathcal{B}^\top V - RI \\ \dot{v}_n = \mathcal{L}\Theta + G(V_{ref} - V) \\ \dot{\Theta} = -\mathcal{L}(I^{rat})^{-1}I_t + \gamma\delta - \gamma\dfrac{\alpha\Theta\dot{\Theta}\mathrm{sgn}\dot{\Theta}}{\dot{\Theta}\mathrm{sgn}\dot{\Theta} + e^{-\beta t}} \end{cases}, \tag{9}$$

where $\delta \triangleq= [\delta_1, \delta_2, \cdots, \delta_n]^\top$, $\alpha \triangleq diag(\alpha_1, \alpha_2, \cdots, \alpha_n)$, $\beta \triangleq diag(\beta_1, \beta_2, \cdots, \beta_n)$, and $\gamma \triangleq diag(\gamma_1, \gamma_2, \cdots, \gamma_n)$.

To analyze the convergence of resilient closed-loop system (9), we review the following stability definition.

Definition 1 [17]: $x(t) \in \mathbb{R}$ is uniformly ultimately bounded (UUB) with ultimate bound b if there exist constants $b > 0, c > 0$, independent of $t_0 \geq 0$, and for every $a \in (0, c)$, there exists $T = T(a, b) \geq 0$, independent of t_0, such that

$$\|x(t_0)\| \leq a \Rightarrow \|x(t)\| \leq b, \forall t \geq t_0 + T. \tag{10}$$

Theorem 2: Suppose Assumption 1 and Assumption 2 hold. The resilient closed-loop system (9) is stable and realizes bound current sharing and voltage regulation for DC microgrids against unknown constant attacks on communication links.
The proof is omitted due to space limitation.

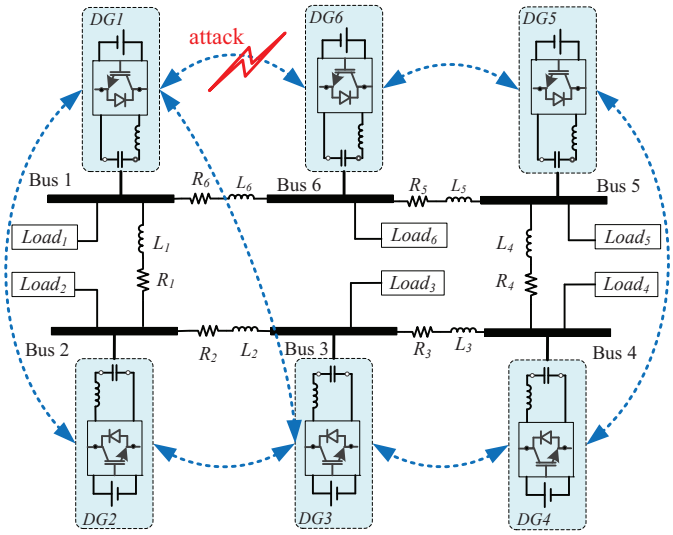

Fig. 3. A DC microgrid under attack. (Solid lines: electrical network; dashed lines: communication network)

IV. Simulation Examples

We consider a DC microgrid including six DGUs, as shown in Fig.3, whose communication network is described by the dashed lines, and the topology can be captured by the following adjacency matrix:

$$\mathcal{A} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

The parameters of resilient controller is selected as $\alpha = 20E$, $\beta = 0.1E$. Let the global reference voltage be $V_{ref} = 315\underline{1}_n$. Let the rated currents of DGUs be $I^{rat} = diag(3, 3, 3, 1, 1, 1)$, and the values of virtual resistances be $R^{vir} = diag(1, 1, 1, 3, 3, 3)$. The parameters of electrical network, including LC filters, power lines and local loads, are listed in Table I.

TABLE I
THE PARAMETERS OF ELECTRICAL NETWORK

LC filters (mH, μF)	power lines (Ω, μH)	loads (Ω)
$L_{t1} = 4,\ C_{t1} = 50$	$R_1 = 1.23,\ L_1 = 318$	300
$L_{t2} = 3,\ C_{t2} = 40$	$R_2 = 1.35,\ L_2 = 1800$	200
$L_{t3} = 5,\ C_{t3} = 60$	$R_3 = 1,\ L_3 = 800$	200
$L_{t4} = 2,\ C_{t4} = 40$	$R_4 = 1.5,\ L_4 = 1800$	300
$L_{t5} = 2,\ C_{t5} = 40$	$R_5 = 1,\ L_5 = 700$	200
$L_{t6} = 4,\ C_{t6} = 50$	$R_6 = 1.2,\ L_6 = 800$	400

The effectiveness of the proposed resilient control algorithm (7) is demonstrated by simulation examples in two

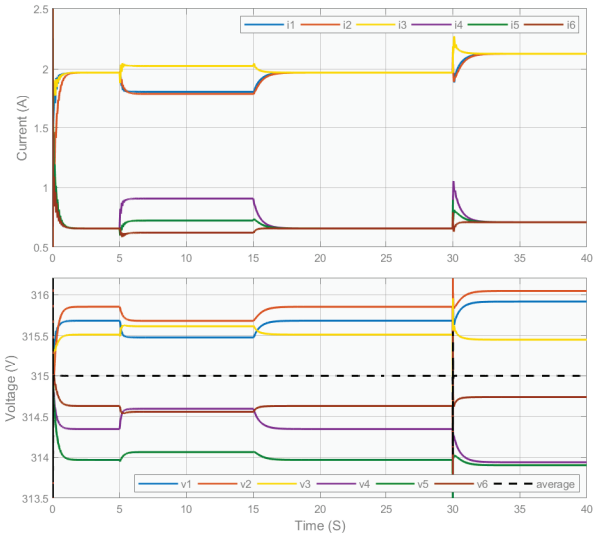

Fig. 4. The simulation results when attack on a communication link of DGU 4.

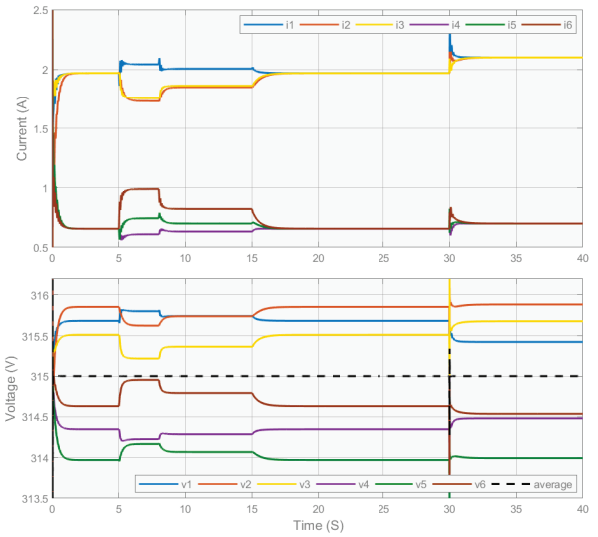

Fig. 5. The simulation results when attacks on all communication links of DGU 6.

scenarios when FDI attacks invade the communication links in DC microgrids.

Case I: one arbitrary communication link is attacked.

In this case, we assume that one communication link is attacked at some time, e.g. an attacked data $\hat{I}_{t3} = I_{t3} + 1.5$ is received by DGU 4 at $t = 5s$. Then, the proposed resilient algorithm (7) is activated at $t = 15s$. Such latency of ten seconds or longer interval provides sufficient operating time for practical microgrids. As shown in Fig.4, the output current that has been charged to be consistent is disrupted due to the disruption of FDI attack during $5s$ to $15s$. In other words, the control objective of current sharing cannot be realized. This inconsistent circumstance is gradually diminished after the proposed resilient controller (7) is activated, and its effectiveness towards plug-and-play operations is verified by paralleling a local load in DGU 4 at $30s$.

Case II: more than half of communication links are attacked.

In this case, we consider the worst situation where all communication links of DGU i are attacked at some time so that it cannot receive any healthy neighboring information. For example, an attacked data $\hat{I}_{t5} = I_{t5} + 2$ is received by DGU 6 at $t = 5s$, and then it received another compromised data $\hat{I}_{t1} = I_{t1} - 1$ at $t = 8s$. The proposed resilient algorithm (7) is activated at $t = 15s$. As shown in Fig.5, the current sharing in this DC microgrid is no longer maintained because FDI attacks have destructed all communication links in DGU 6 so that it cannot receive any actual neighboring information. The adverse effects of FDI attacks is gradually mitigated after the proposed resilient controller (7) is activated. In addition, the effectiveness towards plug-and-play is also verified by paralleling a local load in DGU 1 at $30s$.

V. Conclusion

To handle the disruption of cyber attacks towards communication networks, a resilient cooperative controller is proposed in this paper to restore current sharing and voltage regulation in DC microgrids against unknown FDI attacks, especially for attacks on communication links, where the number of healthy neighbors does not need to be prescribed. This resilient controller is also a further complement to those researches that only provide attack detection techniques. Our future work will emphasize dynamic attacks. It also makes sense to explore simpler attack detection techniques, since our proposed resilient controller does not involve targeting a specific variable being attacked.

References

[1] T. Dragičević, X. Lu, J. C. Vasquez, and J. M. Guerrero, "DC microgrids-part I: A review of control strategies and stabilization techniques," *IEEE Transactions on Power Electronics*, vol. 31, no. 7, pp. 4876–4891, 2016.

[2] P. Karlsson and J. Svensson, "DC bus voltage control for a distributed power system," *IEEE transactions on Power Electronics*, vol. 18, no. 6, pp. 1405–1412, 2003.

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

[4] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1963–1976, 2012.

[5] A. Bidram, A. Davoudi, F. L. Lewis, and Z. Qu, "Secondary control of microgrids based on distributed cooperative control of multi-agent systems," *IET Generation, Transmission & Distribution*, vol. 7, no. 8, pp. 822–831, 2013.

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

[7] M. Tucci, L. Meng, J. M. Guerrero, and G. Ferrari-Trecate, "Stable current sharing and voltage balancing in DC microgrids: A consensus-based secondary control layer," *Automatica*, vol. 95, pp. 1–13, 2018.

[8] S. Trip, M. Cucuzzella, X. Cheng, and J. Scherpen, "Distributed averaging control for voltage regulation and current sharing in DC microgrids," *IEEE Control Systems Letters*, vol. 3, no. 1, pp. 174–179, 2019.

[9] P. Nahata, M. S. Turan, and G. Ferrari-Trecate, "Consensus-based current sharing and voltage balancing in DC microgrids with exponential loads," *IEEE Transactions on Control Systems Technology*, vol. 30, no. 4, pp. 1668–1680, 2021.

[10] 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.

[11] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6731–6741, 2018.

[12] 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.

[13] S. Zuo, T. Altun, F. L. Lewis, and A. Davoudi, "Distributed resilient secondary control of DC microgrids against unbounded attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3850–3859, 2020.

[14] F. Dörfler, J. W. Simpson-Porco, and F. Bullo, "Electrical networks and algebraic graph theory: Models, properties, and applications," *Proceedings of the IEEE*, vol. 106, no. 5, pp. 977–1005, 2018.

[15] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked AC microgrids under unbounded cyber attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3785–3794, 2020.

[16] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2019.

[17] H. K. Khalil, *Nonlinear Systems (Third edition)*. New Jersey: Patience Hall, 2002.