Resilient Operation of Heterogeneous Sources in Cooperative DC Microgrids

Sahoo, Subham; Dragicevic, Tomislav; Blaabjerg, Frede

Published in:
IEEE Transactions on Power Electronics

Link to article, DOI:
10.1109/TPEL.2020.2991055

Publication date:
2020

Document Version
Peer reviewed version

Citation (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Resilient Operation of Heterogeneous Sources in Cooperative DC Microgrids

Subham Sahoo, Member, IEEE, Tomislav Dragičević, Senior Member, IEEE and Frede Blaabjerg, Fellow, IEEE

Abstract—As distributed control layer makes DC microgrids vulnerable towards cyber attacks, the identification and mitigation of attacked agent(s) becomes even more challenging with heterogeneity between each source based on factors, such as capacity, reliability and generation cost. This letter proposes a novel resilient methodology, which involves detection using adaptive discord element (ADE) and immediate mitigation via an event-driven approach. The proposed approach successfully mitigates cyber attacks under experimental conditions.

Index Terms—DC microgrid, cyber attacks, cooperative control, heterogeneous sources, resilient controller.

I. INTRODUCTION

DISTRIBUTED energy management system (EMS) in DC microgrids offers a flexible and economic alternative to centralized approach [1]. It provides resiliency from single-point-of-failure, plug-and-play capability, and a reduced cost of communication infrastructure [2]. As shown in Fig. 1, the measurements from grid-forming converters (commonly termed as agents in this letter) are transmitted between each other to achieve consensus by accommodating average voltage regulation and power sharing, respectively. The intermittent nature of renewable energy sources, which are usually operated in grid-following mode to extract maximum power, bring asymmetry in the current sharing profiles of grid-forming converters. Moreover, different characteristics of each source and operation principle of the corresponding converters leads to the principle of heterogeneity in DC microgrids. Based on some of the prominent aspects of heterogeneity overviewed in Table I for DC microgrids [1], [3]-[4], energy management schemes often introduce an adaptive droop to be applied on local current measurements, which leads to disproportionate current sharing profile.

However, these measurements can be corrupted by injecting malicious data into the cyber-physical components of the microgrid [6]. Many attack detection models have been proposed to detect such attacks for proportionate current sharing [7]-[10]. However, detection of these attacks becomes more challenging with disproportionate current sharing profile. On the other hand, mitigation of these attacks is still not adequately discussed in the abovementioned papers. To the best of authors’ knowledge, the only notable contribution in this area is the trust and confidence factor based resilient control in cooperative DC microgrids [11]. However, the online calculation of these factors, which involves additional layers of integration and division operations, assigns high computational burden. Moreover to provide attack-resilient operation, it requires a minimum of half of the neighboring converters to be trustworthy, thereby limiting its resilience capability for worst-case attacks.

To remove the attack elements in cooperative DC microgrids, this letter proposes an adaptive discord element (ADE) for each agent. Extending the presence of attacks as a binary mechanism using ADE, an event-driven mitigation strategy is proposed to reconstruct and replace the attacked signal with a trustworthy signal. As opposed to [11], this

This work was supported by THE VELUX FOUNDATIONS under the VILLUM Investigator Grant – REPEPS (Award Ref. No.: 00016591).
S. Sahoo and F. Blaabjerg are with the Department of Energy Technology, Aalborg University, Aalborg East, 9220, Denmark (e-mail: sss@et.aau.dk and fbl@et.aau.dk).
T. Dragičević is with the Center of Electric Power and Energy, Technical University of Denmark, 2800 Kgs. Lyngby, Denmark (e-mail: tomdr@elektro.dtu.dk)

Fig. 1. Generic cyber-physical model of DC microgrid with $N$ grid-forming heterogeneous agents: Blue and green arrows represent the cyber link and measurements/control signals, respectively. Further, red bolts represent the attacked layers.

<p>| Aspects of Heterogeneity in DC Microgrids |
|-------------------------------------------------|------------------------------------------------|</p>
<table>
<thead>
<tr>
<th>Heterogeneity</th>
<th>Design of adaptive droop $\Delta R_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity oriented [1]</td>
<td>$H_2(s)\exp\left(\sum_{j\in N_i} \left(\text{SoC}_j(t) - \text{SoC}_i(t)\right) - 1\right)$</td>
</tr>
<tr>
<td>Reliability oriented [3]</td>
<td>$D^i$</td>
</tr>
<tr>
<td>Cost oriented [4]-[5]</td>
<td>$H_3(s)\left[\sum_{j\in N_i} (\lambda_j(t) - \lambda_i(t))\right]^2$</td>
</tr>
</tbody>
</table>

1 $H_2(s)$ is a PI controller, $\text{SoC}_j$ & $\text{SoC}_i$ are the state of charge of batteries in $i^{th}$ and $j^{th}$ agent, $N_i$ is the set of neighbors of $i^{th}$ agent.
2 $D^i$ and $D^j$ denotes the total damage and component damage (for each component $k$ in $i^{th}$ converter, respectively).
3 $H_3(s)$ is a PI controller, $\lambda_j$ & $\lambda_i$ are the incremental costs of generation of $i^{th}$ and $j^{th}$ agent, respectively.
strategy can provide resilience even using a single trustworthy neighboring information. The proposed resilient strategy is tested for the attacks discussed in [9] to validate its robustness in a distributed DC microgrid.

II. DESIGN OF RESILIENT CONTROL STRATEGY

In the system shown in Fig. 1 comprising of $N$ agents, each communication digraph is represented via edges to constitute an adjacency matrix $A = [a_{ij}] \in \mathbb{R}^{N \times N}$, where the communication weights are given by: $a_{ij} > 0$, if $(\psi_i, \psi_j) \in \mathcal{E}$, where $\mathcal{E}$ is an edge connecting two nodes, with $\psi_i$ and $\psi_j$ being the local and neighboring node respectively. Otherwise, $a_{ij} = 0$. Further, the incoming cyber information matrix can be denoted by $\mathbf{Z}_{in} = \sum_{i \in \mathcal{N}} a_{ij}$. Hence, if $A$ and $\mathbf{Z}_{in}$ match each other, the Laplacian matrix $\mathbf{L}$ is balanced, where $\mathbf{L} = \mathbf{Z}_{in} - \mathbf{A}$.

Using the preliminaries of the communication graph, the local control input of the cooperative secondary controller can be written as:

$$u_i(t) = \xi \sum_{j \in M_i} a_{ij} (x_j(t) - x_i(t))$$ \hspace{1cm} (1)

where $u_i = \{u_i^V, u_i^I\}$, $e_i = \{e_i^V, e_i^I\}$ corresponding to the elements in $x_j = \{\hat{V}_j, R_i I_j\}$, $\xi$ is the convergence variable and $M_i$ is the set of neighbors of $i^{th}$ agent. Further, $\hat{V}_j$, $R_i$ and $I_j$ denote the average voltage estimate, dynamic droop and output current of the neighboring agents, respectively. The design of dynamic droop for $i^{th}$ agent is carried out using:

$$R_i = R_i^0 + \Delta R_i$$ \hspace{1cm} (2)

where, $R_i^0 = \Delta V_i/I_{i, \text{max}}$ is a fixed droop quantity with $\Delta V_i$ denoting an allowable voltage deviation of 5% and $I_{i, \text{max}}$ denoting the maximum output current for $i^{th}$ converter. On the other hand, the adaptive droop for $i^{th}$ agent, $\Delta R_i$ can be designed based on the aspect of heterogeneity, as explained in Table I. It is worth noting that the update for capacity and reliability oriented adaptive droop gain is carried out in shorter (in ms) and fairly longer (monthly) time-scale, respectively.

Using (1), the control inputs to achieve average voltage regulation and proportionate current sharing can be obtained from secondary sublayer I and II respectively by using the following voltage correction terms for $i^{th}$ agent:

Sublayer I: $\Delta V_1 = H_1(s)(V_{ref} - \hat{V}_i)$ \hspace{1cm} (3)

Sublayer II: $\Delta V_2 = H_2(s)u_i^I$ \hspace{1cm} (4)

where $\hat{V}_i = V_i + \int_0^t \sum_{i \in M_i} a_{ij}(u_{ij}^I - d_r)$, while $H_1(s)$, $H_2(s)$ are PI controllers. Further, $V_{ref}$ is the global reference voltage quantity for all the agents. The correction terms obtained in (3)-(4) are finally added to the global reference voltage to achieve local voltage references for $i^{th}$ agent using:

$$V_{ref}^i = V_{ref} + \Delta V_1 + \Delta V_2.$$ \hspace{1cm} (5)

Using (5) as the local voltage reference for $i^{th}$ agent, the control objectives for distributed EMSs [1]-[2] in DC microgrids are achieved, which can be summarized as:

$$\lim_{t \to \infty} \hat{V}_i(t) = V_{ref}^i, \lim_{t \to \infty} u_{ref}^I(t) = 0 \forall i \in \mathcal{N}$$ \hspace{1cm} (6)

However, the objectives in (6) can be misconstrued in the presence of cyber attacks on current measurements in $i^{th}$ agent using:

Sensor attack: $I_{i, \text{ref}}^f = I_i(t) + \kappa I_i^a$ \hspace{1cm} (7)

Cyber link attack: $I_{i, \text{ref}}^f = I_i(t) + \kappa I_i^a$ \hspace{1cm} (8)

where $\kappa = 1$ denotes the presence of an attack element $I_i^a$ in $i^{th}$ agent, or 0 otherwise. Hence, this letter concerns the mitigation of the most sophisticated attack, namely deception attacks, where $I_i^a = L I_i^a = 0$. Since the attack elements in deception attacks follow the cooperative synchronization theory, it leads to a feasible and stable solution. Further details about these attacks and their impact in DC microgrids with homogeneous sources can be found in [9].

To detect the presence of attack elements, we consider the average state-space voltage dynamics of each grid-forming DC/DC converter in vector form upon multiplication of $\mathbf{R}$ on both sides, given by:

$$\dot{\mathbf{V}} = \mathbf{RC}^{-1}(\mathbf{T}_i^{\text{in}} - \mathbf{I}^f)$$ \hspace{1cm} (9)

where $\mathbf{T}_i = 1 - \mathbf{T}$. Further, $\mathbf{T}^{\text{in}}, \mathbf{T}, \mathbf{R}, \mathbf{C}$ and $\mathbf{I}^f$ denote the diagonal matrices of the input current $I_{in}$, duty ratio $T$, dynamic droop $R_i$, DC link capacitance $C_i$ and the attacked output current measurement $I_{i, ref}^f$ respectively, for $N$ agents.

Considering the error into the voltage controller to be zero under steady-state conditions such that

$$\lim_{t \to \infty} V_i(t) = V_{ref}^i.$$ \hspace{1cm} (10)

Substituting (5) into (10) and multiplying $\mathbf{L}^T$ on both sides, we get steady-state solution of reference tracking as:

$$\mathbf{L}^T \Delta \mathbf{V}_i + \mathbf{L}^T \mathbf{H}_2 e^{\kappa I_i^a} + V_{ref}^i \mathbf{I} = \mathbf{L}^T \mathbf{V}$$ \hspace{1cm} (11)

where $e^{\kappa I_i^a}$ denotes a diagonal matrix of the error quantity $e_{ij}$ in (1) including the attacked signal $I_{i, ref}^f(t)$ ($\kappa = 1$). $\Delta \mathbf{V}_i$ denotes the diagonal matrix of $\Delta \mathbf{V}_i$ in (3) with $\mathbf{H}_2$ denoted as diagonal matrix of PI controller in (4). Moreover, $\mathbf{I}$ denote an identity matrix with a dimension of $N \times N$. 

![Fig. 2. Proposed resilient strategy in $i^{th}$ agent to mitigate deception attacks in DC microgrid with heterogeneous sources–red bolts depict cyber attack.](image-url)
Remarks

Realized in [8]-[9]

– $FD > \beta$

Realized in [8]-[9]

other hand, cyber attacks on agent II irrespective of their nature. On the current measurements, leaving the average voltage estimates $\Delta V_1 = 0$ holds true [7].

Using Remark I to eliminate $L^T \Delta V_1$ in (11) and differentiating (11) w.r.t. time upon multiplication of $R$ on both sides, we get:

$$L^T R K^H e^{1a} + L^T R K^H e^{1a} - L^T R \dot{V} = 0. \tag{12}$$

As already explained in [9], $L^T e^{1a} = 0$ and $L^T C^{-1} I^f = 0$ will hold true for deception attacks. Using these equalities after substituting (9) in (12), we obtain:

$$L^T R K^D e^{1a} - L^T R C^{-1} T \dot{I}^{in} = 0. \tag{13}$$

Remark II: Due to the injected attack signal, the first term of (13) will be asymmetric, not obeying the consensus theory. For (13) to hold true, this property will be reflected in the second term of (13), which becomes the basis of detection for deception attacks in cooperative DC microgrids with heterogeneous sources.

Since the proposed detection concept for heterogeneous sources (operating with an adaptive droop $\Delta R_i$) is basically inspired from [8]-[9], it is termed as adaptive discordant element (ADE) in this letter, can be mathematically represented for $i^{th}$ agent using Remark II as:

$$ADE_i = I_i \left[ \sum_{j \in M_i} a_{ij} (R_j I_j^{in} - R_i I_i^{in}) \right] + \sum_{j \in M_i} a_{ij} (R_j I_j^{in} + R_i I_i^{in}) \tag{14}$$

It is worth notifying that the proposed detection criteria is scalable to $N$ agents, which has been largely discussed in [8]-[9]. Since $ADE$ exceeds $\beta$ only in the presence of cyber attacks on current measurements, it guarantees robust and accurate detection performance under many scenarios including sensor and line-to-line faults, which has been detailed in Table II. Some of the scenarios in Table II have been simulated for $ADE$ in Fig. 3, where $ADE_2$ goes beyond $\beta (= 0.02)$ only for cyber attacks on agent II irrespective of their nature. On the other hand, $ADE_2$ stays within the detection band $\beta$ for load change and sensor faults. In fact, sensor faults are detected via a fault detection metric $FD_i^2 > \rho_{FD} (= 0.02)$ [8], thereby differentiating sensor faults with deception attack.

Even though discord element based detection strategy was proposed in [9], a timely mitigation technique to remove these attacks was still not discussed. As the robustness of the proposed attack detection strategy is guaranteed using Table II, this letter uses an event-driven signal reconstruction based mitigation strategy based on a follow-up signal from $ADE_i$ to provide resilience against such attacks. Upon detection of the presence of attack element in $i^{th}$ agent using (14), an authentication label $\Omega_i$ is generated for the current measurements in $i^{th}$ agent to alarm the presence of attack element to its neighbors. It should be noted that the nature of authentication label is binary, such that:

$$\Omega_i = \begin{cases} \{0\} & \text{if } ADE_i > \beta \\ \{1\} & \text{else} \end{cases} \tag{15}$$

where $\beta$ is a small value detection threshold to disregard measurement noise yet ensure accurate detection. To simplify the representation of authentication for any signal, $\circ^T$ and $\circ^R$ will be used to symbolize True and False for the communicated measurements, respectively using (15).

As long as (15) holds True, the control variables used in designing $ADE_i$ are forced to follow the trajectories of non-compromised neighboring signals (with $\Omega_j$ labeled as True). As highlighted in Fig. 2, if the set of authentication signals $\Theta_i$ for $i^{th}$ agent is not a zero vector in the presence of attack elements, event-driven resilient signals are reconstructed to mitigate deception attacks in system with heterogeneous sources using:

$$I_i(t_k) = \Xi(t_k) \left[ \frac{R_i I_i^j(t_k)}{R_i} \right] \tag{16}$$

where $o(t_k)$ (with $k$ as the triggering instant) denote the event-triggered samples of the output current in $i^{th}$ agent. It is worth notifying that $\Xi[o]$ in (16) is a triggering function, which holds the input signal $o$ until the next instant of triggering. These event-driven signals are generated when the triggering criterion ($LRI^{in} > \beta$) in Fig. 2 is activated in the attacked agent. However, if $\Theta_i$ is a null vector, this implies that all the remaining agents are compromised with attack elements and should be prevented from being used in $i^{th}$ agent. Hence, this leads to localized operation of $i^{th}$ agent (as shown in Fig. 2).

The resilient action is completed by substituting the event-driven resilient signals with the attacked signal based on the local authentication signal using:

$$I_i(t) = \Omega_i I_i^j(t) + (1 - \Omega_i) I_i(t_k) \tag{17}$$

![Fig. 3. Performance of ADE for various cyber attacks at $t = [1, 2] \ s$ and the fault detection metric $FD_1$ [8] for current sensor fault at $t = [2, 3] \ s$.](image-url)
Finally, the signal obtained in (17) is substituted into (1) to realize the mitigation of MITM attacks in DC microgrids. As soon as the reconstructed signal in (17) obeys (6), the authentication label transmitted to the neighbors is switched back to $T$. The proposed strategy not only mitigates the attacks but also allows to operate normally under external disturbances such as load change, communication delay, etc.

$$\text{V}_{ref} \text{ of 64 V with } N = 2 \text{ heterogeneous sources, as shown in Fig. 4(a). The entire physical layer along with flow of control signals is detailed in Fig. 4(b). Both the sources have been made to regulate the average voltage and share load current to regard the reliability of converters for enhancing the lifetime of components. Using the local and neighboring measurements, the proposed resilient strategy shown in Fig. 2 is modeled for every converter to mitigate the attacks and meet the control objectives in (6). The experimental testbed parameters along with the adaptive droop gains are provided in Appendix.}

In Fig. 5(a), before the deception attack is launched on agent II, agent II shares the load current in higher proportion as compared to agent I. This sharing proportion can be explained by severe ageing of component(s) in source I. When the attack is launched on agent II, it can be seen that the currents are being shared almost equally in the absence of the proposed resilient controller. As a result, reliability-oriented sharing between DC sources is clearly disregarded due to the attack. However, in the presence of the proposed resilient controller, $ADE_2$ is immediately activated when the deception attack is launched and adjusts the authentication label of signals from agent II to $F$. As per the proposed resilience mechanism, $F^2$ is immediately transmitted to reconstruct $I^2(t)$ as per (16). This action allows the system to return back to the normal operating condition (pre-attack loading level). Additionally, it can be seen in Fig. 5(b) that the dynamic performance varies for different values of the threshold $\beta$. Intuitively, the settling time increases as the value of $\beta$ increases from 0.02 to 0.05. This adjudges $\beta$ to be as small as possible for faster settling time, yet it has to be sufficiently larger than the measurement noise to avoid unnecessary triggering. Moreover, it can be clearly justified that the resilient mechanism performs satisfactorily for steady-state conditions as well as disturbances, such as load change. The action is so fast that it easily accommodates

III. EXPERIMENTAL RESULTS

The proposed detection strategy has been experimentally validated in a DC microgrid operating at a voltage reference

![Fig. 4](image)

**Fig. 4.** (a) Experimental setup of a cooperative DC microgrid comprising of $N = 2$ agents controlled by dSPACE MicroLabBox DS1202 supplying power to a programmable load, and (b) single line diagram of the experimental setup.

![Fig. 5](image)

**Fig. 5.** Performance of DC microgrid (shown in Fig. 4(b)) for a deception attack on agent II: (a) in the absence, and (b) in the presence of the proposed resilient strategy.

![Fig. 6](image)

**Fig. 6.** Performance of DC microgrid (shown in Fig. 4(b)) for deception attacks on agent I and II simultaneously: (a) in the absence, and (b) in the presence of the proposed resilient strategy.
an increase in load immediately following the deception attack.

Finally in Fig. 6(a), when a worst-case deception attack is launched on both agents, the current sharing proportion between the converters is reversed in the absence of resilient controller, which disregards the aspect of reliability of components in power electronic converters. This issue has been addressed by the proposed resilient controller in Fig. 6(b) where the sharing proportion between the converters is retained as per the pre-attack loading levels to regard reliability. Since the authentication pool $\Theta_i$ is $F$ for both agents, the signal reconstruction algorithm holds the pre-attack instant throughout the period. It is worth notifying that any load change under these circumstances will lead to local instability (disabled secondary controller, as shown in Fig. 2). Nevertheless when the attack element is removed from agent 1, it can be seen that the system returns back to the normal operating condition following a transient using the authenticated $I_{\tau_1}(t)$. Hence, this validates the effectiveness of the performance of proposed resilient controller to a maximum of $(N-1)$ scale attacks (at least one trusted agent will always be required in the system to broadcast true signals). This establishes that the proposed resilient mechanism can be easily scaled to many applications in DC based power electronic systems.

IV. CONCLUSION

A novel resilient control strategy is proposed to mitigate the most sophisticated form of cyber attacks in DC microgrids. As opposed to the existing work, this strategy is simple and can be readily applied to any distributed energy management schemes (EMSs) for DC microgrids comprising of heterogeneous sources. Additionally, this strategy can be easily scaled up to any number of units since only one trusted agent is required to reconstruct trustworthy signals, thereby removing the attack. This theory has been validated experimentally to show the robustness and ease of implementation for mission-critical applications such as naval ships and electric aircrafts, where reliability and security are of prime concern.

APPENDIX - EXPERIMENTAL PARAMETERS

The considered system consists of two sources with the converters rated equally for 600 W. It should be noted that the controller gains are consistent for each converter.

**Plant:** $L_{se} = 3 \, mH, \quad C_s = 100 \, \mu F, \quad r_1 = 0.8 \, \Omega, \quad r_2 = 1.4 \, \Omega$

**Controller:** $V_{ref} = 64 \, V, \quad K_p^{H_1} = 1.92, \quad K_i^{H_1} = 15, \quad K_p^{H_2} = 4.5, \quad K_i^{H_2} = 0.08, \quad l = 1.36, \quad \xi = 1.8, \quad \beta = 0.02, \quad R_0 = 0.5, \quad \Delta R_1 = 0.05, \quad \Delta R_2 = 0.4$

REFERENCES


