Aalborg Universitet

Mitigating Concurrent False Data Injection Attacks in Cooperative DC Microgrids

Zhang, Jingqiu; Sahoo, Subham; Chih-Hsien Peng, Jimmy ; Blaabjerg, Frede

Published in:
I E E E Transactions on Power Electronics

DOI (link to publication from Publisher):
10.1109/TPEL.2021.3055215

Publication date:
2021

Document Version
Accepted author manuscript, peer reviewed version

Link to publication from Aalborg University

Citation for published version (APA):
Zhang, J., Sahoo, S., Chih-Hsien Peng, J., & Blaabjerg, F. (2021). Mitigating Concurrent False Data Injection Attacks in Cooperative DC Microgrids. *I E E E Transactions on Power Electronics*, *36*(8), 9637-9647. Article 9339923. https://doi.org/10.1109/TPEL.2021.3055215

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 -

Take down policy
If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from vbn.aau.dk on: December 06, 2025

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3055215, IEEE Transactions on Power Electronics

Mitigating Concurrent False Data Injection Attacks in Cooperative DC Microgrids

Jingqiu Zhang, *Student Member, IEEE* Subham Sahoo, *Member, IEEE*, Jimmy Chih-Hsien Peng, *Member, IEEE* and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*—Limited global information in DC microgrids with distributed cooperative control makes them vulnerable to cyber attacks, which can lead to their destabilization and shut down. Here, we discuss a novel false data injection attack (FDIA) model, termed as the concurrent attack, that can compromise local and communicated estimated voltages simultaneously. We formalize that such an attack could be disguised as a conventional FDIA on the estimated voltages transmitted in communication links (termed as the communication link attack), thereby masking the presence of the attack on local estimated voltages and rendering corresponding mitigation attempts ineffective. Secondly, we present an energy-based detection strategy based on the intrinsic mode functions obtained using the ensemble empirical mode decomposition method. Further, a differentiation criterion using the voltage correction terms generated from the voltage observer is employed to help distinguish between the concurrent attack and the communication link attack. An event-driven mitigation strategy is then used to replace the attacked signal with a reconstructed signal. Finally, the efficacy of the proposed resilient control scheme is demonstrated using both simulations and experimental results.**

***Index Terms*—DC microgrid, distributed control, cyber attack detection and mitigation.**

I. Introduction

DC microgrids are gaining attention due to the increasing integration of renewable energy resources, installation of energy storage devices, and utilization of DC loads [1], [2]. To date, DC microgrids have been adopted in data centers, residential households, and shipboard power systems [3]. Further, distributed control has been implemented to provide high adaptability and efficiency among DC microgrids [4]. However, the lack of a centralized controller makes it difficult to detect as well as mitigate cyber attacks. Specifically, in a sparse distributed communication graph, the malicious information resulting from cyber attacks easily propagate to the rest of the network, which also affect the operation of other nodes. Several types of cyber attacks recently have been reported in the literature, including false data injection attacks (FDIAs) [5], replay attacks [6], denial of service (DoS) attacks [7] and disinformation attack [8].

In [9], FDIAs have been reported to compromise current and voltage sensors of an agent as well as communication links between neighboring agents. Moreover, the constrained FDIAs may harass the consensus protocol, while the unconstrained FDIAs may destabilize the entire DC grid. One way to detect cyber attacks is to check if the cooperative synchronization law has been violated [10]. However, *stealthy attacks* may employ multiple coordinated attack vectors to intrude into multiple nodes such that the physical laws are unchanged. Such kind of attacks may result in possible uneconomical dispatch problem [11] or instability issues [12]. These attacks can be launched when an adversary has some information about the system in advance [12], [13].

Detection of cyber attacks in distributed DC microgrids can be classified into two categories: model-based and model-free methods. The former assumes that the network topology and attack vectors are known/bounded and are devised to identify these attacks. Model-based detection techniques basically originate from fault detection and isolation, and they are used in multi-agent systems [14]–[17]. In the context of distributed DC microgrids, the only available information to anticipate the presence of attack is either available locally or communicated by neighboring agents [18]. Leveraging this property, a cooperative vulnerability factor (CVF) based detection metric has been proposed to detect stealthy voltage attacks in [10]. However, attack vectors can often be unpredictable in nature, and developing a robust model-based detection with significant accuracy can be a challenging task.

In contrast, model-free method does not rely on prior knowledge of the system and the attack vectors. Detection is carried out by analyzing the output signals. For distributed DC microgrids, a signal temporal logic-based (STL) method has been used to detect FDIAs and DoS [19]. Such approach targets the unpredictable nature of attack vectors.

As it has been mentioned in [12], coordinated intelligent attacks can be launched by attackers who have expertise in the entire system. Such attacks could be a combination of several types of attacks initiating concurrently by an adversary. Although such attacks can be determined sequentially by existing detection methods, there will still be errors and delays as these methods are originally designed to detect one type of attack at a time. Such issues can be sufficient to destabilise the grid due to deferred or inadequate control actions.

Upon detection of FDIAs, mitigation is required to remove them from the control system to enhance the resiliency of microgrids. In [20], a trust-based controller is proposed to mitigate attacks by changing the consensus gains adaptively

Manuscript received August 28, 2020; revised December 2, 2020; accepted January 15, 2021. This work was supported by the Singapore Ministry of Education Academic Research Fund Tier-1 grant R-263-000-D10-114.

J. Zhang and J. C.-H. Peng are with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583. (e-mail: jingqiuzhang@u.nus.edu and jpeng@nus.edu.sg)

S. Sahoo and F. Blaabjerg are with the Department of Energy Technology, Aalborg University, Aalborg East, 9220, Denmark (e-mail: sssa@et.aau.dk and fbl@et.aau.dk)

0885-8993 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Aalborg Universitetsbibliotek. Downloaded on February 18,2021 at 07:41:14 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3055215, IEEE Transactions on Power Electronics

between agents. However, it requires that at least half of the neighboring converters are trustworthy. Further, replacing the compromised states with pre-attack values stored in the observers has been implemented in [21]. Alternatively, attacked agents can be isolated such that FDIAs do not propagate to the rest of the network [22]. Nevertheless, such approach results in loss of graph connectivity and disruption in the consensus protocol. Hence, this mandates a self-healing resilient methodology such that the entire system can recover from any cyber attack without any compromise in cyber graph connectivity.

To address these issues, this paper addresses the presence of FDIAs in the local and communicated estimated voltage within distributed DC microgrids. This is a new form of intelligent attack, and it is referred as concurrent attack. The research contributions of this paper are summarized below:

1) A concurrent attack is designed to mask itself as a communication link attack, misleading the operators from taking appropriate actions. Such an attack can pose challenges to be promptly resolved by model-based detection.
2) A novel non-parametric detection based on an ensemble empirical mode decomposition (EEMD) is therefore proposed. The presence of FDIAs is identified from the energy relationship of neighboring agents, which operates on the decomposed intrinsic mode functions (IMFs) of the EEMD method.
3) A differentiation criterion is further used to classify the type of attack after detection, i.e., whether the attack is a concurrent attack or a communication link attack, based on the voltage correction terms generated by the voltage observer in the secondary controllers.
4) Finally, an event-driven mitigation approach is proposed, which reconstructs a trustworthy signal using the authenticated inputs from the proposed detection strategy. According to the classification of the attacked quantity, the reconstructed trustworthy signal replaces the attacked signal and eliminates all the risks associated with the attack.

The layout of this paper is as follows. Section II presents the distributed consensus-based cooperative law, and analyzes the system responses under the concurrent attack. In Section III, the proposed detection, attack classification, and mitigation methods are formulated. Section IV outlines the simulation results, while the experimental results are shown in Section V. Finally, conclusions are drawn in Section VI.

II. Concurrent Attack Modeling in DC Microgrids

A. Cyber-Physical Preliminaries

Consider the physical network of a DC microgrid comprising of N interconnected DC/DC converters, also known as *agents* in the cyber layer, is managed by a cyber-physical control framework. Referring to Fig. 1, the output voltage of each converter is regulated by a primary droop control. By imposing virtual impedance on each converter, the droop control can achieve load sharing. The droop control method for the k^{th} agent in a DC microgrid is expressed as:

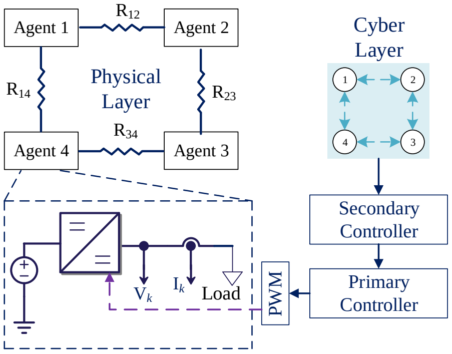

Fig. 1. Layout of a DC microgrid consisting of N = 4 distributed agents.

$$v_k = V_{ref} - r_k I_k \tag{1}$$

where v_k and V_{ref} denote the output voltage and the global voltage reference of the system, respectively. r_k is the droop coefficient (i.e. the virtual impedance) and I_k is the measured output current of the converter. The droop coefficient can be designed using $r_k = \Delta v_k / I_k^{max}$, where Δv is the allowable voltage deviation and I_k^{max} is the maximum output current of k^{th} converter, respectively.

However, the droop control method suffers from the current sharing accuracy and the DC voltage deviation problem [23]. In order to solve the two limitations resulted from the droop control, a distributed secondary controller is used to compensate this error for each converter.

Here, a digraph is used to model the interaction among agents in the cyber layer. The digraph is formulated by a set of nodes, connecting through a set of edges. The k^{th} node sends $x_k = [\bar{V}_k, I_k^{pu}]$ and receives information from its connected neighboring nodes (as depicted in Fig. 2). This is done using a pre-defined adjacency matrix $\mathbf{A} = [a_{kj}] \in R^{N \times N}$, such that average voltage regulation and proportional current sharing can be achieved. Note that $\bar{V}_j$ and I_j^{pu} represent the estimated voltage and the output current (in per unit) from one of the neighbors of the k^{th} agent, respectively. The communication weights a_{kj} are designed to represent the transfer of information between agents, and they are given by:

$$a_{kj} = \begin{cases} > 0, & \text{if } (x_k, x_j) \in \mathbf{E} \\ 0, & \text{else} \end{cases} \tag{2}$$

where $\mathbf{E}$ is an edge connecting two nodes. Whereas, x_k and x_j are the information from the local and neighboring nodes, respectively. Applying the consensus-based law, the secondary control input for the k^{th} agent can be obtained as:

$$\mathbf{u}_k = \sum_{j \in N_k} a_{kj} \underbrace{(x_j - x_k)}_{\mathbf{e}_{jk}} \tag{3}$$

where, $\mathbf{u}_k = \left[u_k^V, u_k^I\right]$ and $\mathbf{e}_{jk} = \left[e_{jk}^V, e_{jk}^I\right]$ corresponds to the two elements in x_k, while N_k is the set of neighbors of the k^{th} agent. In addition, the in-degree matrix $\mathbf{Z}^{\text{in}} = \text{diag}\left\{d_k^{\text{in}}\right\}$ is a diagonal matrix with $d_k^{\text{in}} = \sum_{j \in N_k} a_{kj}$. Similarly, the out-degree matrix can be expressed as $\mathbf{Z}^{\text{out}} = \text{diag}\left\{d_k^{\text{out}}\right\}$ with

0885-8993 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Aalborg Universitetsbibliotek. Downloaded on February 18,2021 at 07:41:14 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3055215, IEEE Transactions on Power Electronics

$d_k^{\text{out}} = \sum_{k \in N_j} a_{jk}$. Subsequently, the Laplacian matrix of the graph is defined as $\mathbf{L} = \mathbf{Z}^{\text{in}} - \mathbf{A}$, in which the sum of elements in each row is zero. Here, the Laplacian matrix determines the global dynamics, and is balanced if the in-degree matrix equals to the out-degree matix, i.e., $\mathbf{Z}^{\text{in}} = \mathbf{Z}^{\text{out}}$, as noted in [24].

Meanwhile, a secondary control is employed to reset the voltage reference for each connected microgrid within the network. Specifically, the distributed cooperative secondary controller is considered to work alongside the primary droop controller. Two voltage correction terms are generated from the secondary control to manage the local voltage set point in the k^{th} agent. They can be expressed as:

$$\Delta V_k^1 = H_1(s)\left(V_{ref} - u_k^V\right) \tag{4}$$

$$\Delta V_k^2 = -H_2(s) u_k^I \tag{5}$$

where $H_1(s)$, $H_2(s)$ are PI controllers for the outputs of voltage observer and current regulator, respectively. Therefore, the local voltage set point for each microgrid can be calculated by:

$$v_k^{ref} = V_{ref} + \Delta V_k^1 + \Delta V_k^2 - r_k I_k \tag{6}$$

Using (1)-(6), the global voltage regulation and the proportional current sharing can then be realized.

***Remark I**: The agents in distributed cooperative DC microgrids will achieve convergence based on the dynamic-consensus law using $\dot{\mathbf{x}} = -\mathbf{L}\mathbf{x}$ for a balanced Laplacian matrix $\mathbf{L}$ such that $\lim_{t \to \infty} x_k(t) = c$, $\forall k \in N$, where c is the steady-state value and N is the number of agents.*

Accordingly, the estimated voltage for each agent should converge to:

$$\lim_{t \to \infty} \bar{V}_k(t) = V_{ref} \tag{7}$$

where the estimated voltage of the k^{th} agent (i.e., $\bar{V}_k(t)$) is updated using:

$$\bar{V}_k(t) = V_k(t) + \int_0^t \sum_{j \in N_k} a_{kj}\left(\bar{V}_j(\tau) - \bar{V}_k(\tau)\right) \mathrm{d}\tau \tag{8}$$

with V_k being the measured output voltage of the k^{th} agent (as indicated in Fig. 1).

B. Modeling of Concurrent Attack

A concurrent attack is defined as compromising the local estimated voltages (termed as *local control input attacks*) and the estimated voltages received from neighboring agents (termed as *communication link attacks*) simultaneously within the distributed secondary controllers.

The attack on the estimated voltage received from the neighboring agent can be modeled using:

$$\bar{V}_{j,con}(t) = \bar{V}_j(t) + \alpha C_{con} \tag{9}$$

where $\bar{V}_j(t)$ is the estimated voltage transmitted from the neighbor of the k^{th} agent, and C_{con} denotes the magnitude of the false data injection attack on the estimated voltage in the communication link. The term α indicates a binary variable with $\alpha = 1$ representing the presence of the attack or 0, otherwise. At the same time, a ramp attack can be imposed on the local estimated voltage in the secondary control in the k^{th} agent. As a result, the consensus protocol in the voltage observer of the k^{th} agent will be updated by:

$$\begin{aligned} \bar{V}_{k,con}(t) &= V_k(t) + \alpha \cdot r \cdot t \\ &+ \textstyle\int_0^t [\sum_{j \in N_k} a_{kj}\left(\left(\bar{V}_j(\tau) - \bar{V}_k(\tau)\right) + \alpha C_{con}\right)] \mathrm{d}\tau \end{aligned} \tag{10}$$

where r is the gradient of the ramp attack and $\bar{V}_{k,con}(t)$ is the estimated voltage of k^{th} agent under a concurrent attack.

Here, the presence of the concurrent attack will cause the consensus protocol to diverge from the global reference value V_{ref}, which is described in (7).

C. Masking as a Communication Link Attack

Firstly, suppose an adversary only attacks the estimated voltage in the communication link.

Under such circumstances, the false data injection attack to the communication link is defined as:

$$\bar{V}_{j,com}(t) = \bar{V}_j(t) + \alpha C_{com} \tag{11}$$

where C_{com} denotes the magnitude of false data injection attack on the communication link. The corresponding consensus protocol in the voltage observer of the k^{th} agent can be updated as:

$$\bar{V}_{k,com}(t) = V_k(t) + \int_0^t [\sum_{j \in N_k} a_{kj}((\bar{V}_j(\tau) - \bar{V}_k(\tau)) + \alpha C_{com})] \mathrm{d}\tau \tag{12}$$

where $\bar{V}_{k,com}(t)$ is the estimated voltage of the k^{th} agent under a communication link attack. This is similar to the expression in (10), indicating that there are conditions when a concurrent attack can be masked as an attack on the communication link only. Note that an FDIA on the local estimated voltage only will cause the consensus law to converge to a final-state that is different from the global reference described in (7). Therefore, it is not possible to mask a concurrent attack as a local control input attack.

Consider a system consisting of $N = 3$ agents with a ring cyber graph. The response of the system with respect to a communication link attack and a concurrent attack is illustrated in Fig. 3. Both attacks are launched at $t = 1$ s, and resolved at $t = 1.5$ s. During this period, the system responses are the same. Although it is clear that an attack has occurred based on (7), it is impossible to differentiate its type from the estimated voltage by each agent. Specifically, the attack on the local estimated voltage at Agent 2 is now hidden. Given such a situation, the network operator will treat the concurrent attack as a communication link attack, and proceed with corrective actions such as disconnecting the link, which is a simple and straightforward way to eliminate the attack. The expected response will be to return to a steady state condition, as illustrated in Fig. 3(a). However, in the case of a concurrent attack shown in Fig. 3(b), the problem persists and further disrupts the consensus law of operation.

Furthermore, incorrectly identifying the concurrent attack as a communication link attack will incur delays, which may be sufficient to compromise the integrity of the entire network.

0885-8993 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Aalborg Universitetsbibliotek. Downloaded on February 18,2021 at 07:41:14 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3055215, IEEE Transactions on Power Electronics

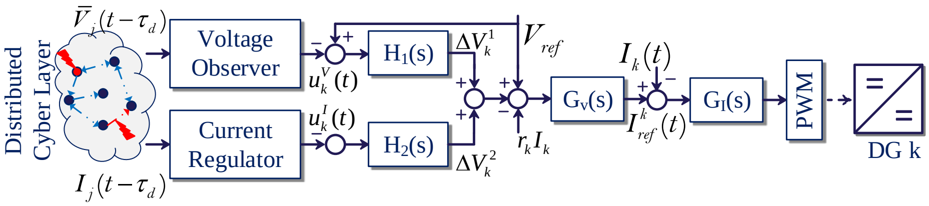

Fig. 2. The cyber-physical control framework used in the distributed DC microgrid. Inputs of the secondary control for converter k are the estimated voltage and current values (per unit) sent from its neighboring agents.

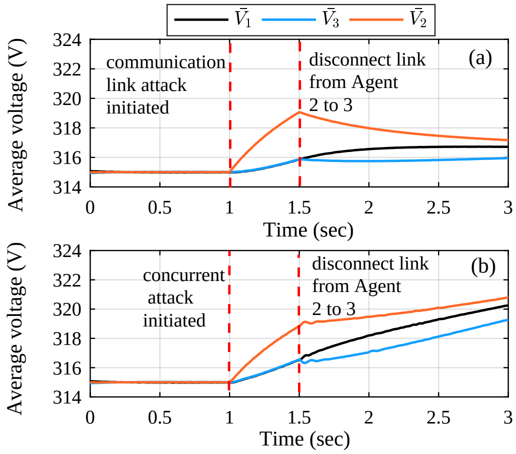

Fig. 3. System responses of: (a) an FDIA on the communication link between Agent 2 and 3, and (b) a concurrent attack consisting of an FDIA on the communication link between Agent 2 and 3 as well as a ramp attack on the local estimated voltage of Agent 2. $C_{com} = 12$ for the communication link attack in (a), while $C_{con} = 8$ for the FDIA in (b) along with a ramp attack of $r = 8$ on the estimated voltage.

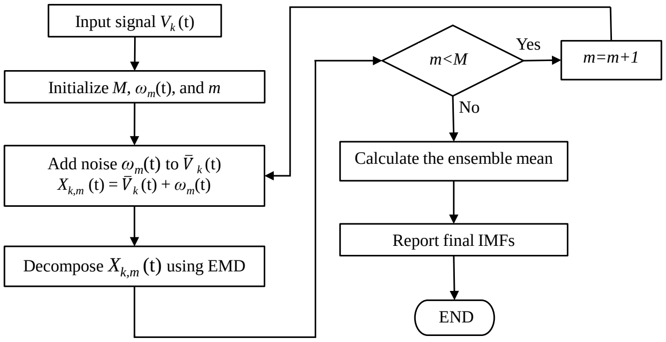
Input signal V_k(t)
Initialize M, ω_m(t), and m
Add noise ω_m(t) to $\bar{V}_k$(t)
$X_{k,m}$ (t) = $\bar{V}_k$(t) + ω_m(t)
Decompose $X_{k,m}$ (t) using EMD
m<M
Yes
m=m+1
No
Calculate the ensemble mean
Report final IMFs
END

Fig. 4. Summary of EEMD for decomposing an input signal into a set of IMFs.

Since the creativity of an adversary can be unbounded, the resilience of a network is threatened under the presence of such attacks. This requires the design of a new solution for detection and mitigation of these attacks.

Problem statement: If there exist C_{con}, r, and C_{com} satisfying the following condition:

$$\sum_{j\in N_k} a_{kj}(|C_{com}| - |C_{con}|) = |r| \tag{13}$$

then, the distributed consensus algorithm in (10) and (12) shall result in the same iterations. In other words, the system responses in terms of the estimated voltages under the concurrent attack can be manipulated to be the same as the communication link attack. Note that C_{con}, r, and C_{com} are all positive or all negative.

Proof: To obtain the same estimated voltages, the RHS of (10) equals to that of (12) such that:

$$\begin{aligned} &V_k(t) + \alpha rt + \textstyle\int_0^t [\sum_{j\in N_k} a_{kj}\big((\bar{V}_j(\tau) - \bar{V}_k(\tau)) + \alpha C_{con})]\mathrm{d}\tau \\ &= V_k(t) + \textstyle\int_0^t [\sum_{j\in N_k} a_{kj}\big((\bar{V}_j(\tau) - \bar{V}_k(\tau)) + \alpha C_{com})]\mathrm{d}\tau \end{aligned} \tag{14}$$

Eqn. (14) can simply be reduced into:

$$\int_0^t \sum_{j\in N_k} a_{kj}(\alpha C_{com} - \alpha C_{con})\mathrm{d}\tau = \alpha rt \tag{15}$$

resulting in:

$$\sum_{j\in N_k} a_{kj} \cdot \alpha(C_{com} - C_{con})t = \alpha rt \tag{16}$$

This proves that the consensus protocol iterations under a concurrent attack or a communication link attack are the same as long as these attacks are designed as per (13). ■

Remark II*: It can be concluded that the consensus law in (7) is violated under a concurrent attack or a communication link attack. Consequently, the consensus protocol no longer converges to the global reference value, which can be given by:*

$$\lim_{t\to\infty} \bar{V}_k(t) \neq V_{ref}. \tag{17}$$

Since the system responses of both the concurrent and communication link attacks are the same, (17) can no longer serve as an effective criterion to differentiate them. Therefore, we require a strategy that not only detects the presence of an attack, but also identifies the type of attack.

III. Proposed Resilient Control Scheme

A. EEMD-based Attack Detection

The mitigation strategy begins with a detection stage based on EEMD proposed in [25], [26]. This approach is model-free, and meets the need to address the unpredictable nature of attacks. In this context, EEMD decomposes the estimated voltage of the agents ($\bar{V}_k(t)$) into a set of intrinsic mode functions (IMFs), each containing a different mode of dynamic signature.

A flowchart summarizing the decomposition operation is shown in Fig. 4. Note that white noise $w_m(t)$ is added to the collected data $\bar{V}_k(t)$ to avoid mode-mixing among IMFs. Therefore, a decomposition signal can be modeled as:

$$X_{k,m}(t) = \bar{V}_k(t) + w_m(t) \tag{18}$$

0885-8993 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Aalborg Universitetsbibliotek. Downloaded on February 18,2021 at 07:41:14 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3055215, IEEE Transactions on Power Electronics

After decomposing the above voltage signal, the features corresponding to false data injection attacks are extracted and examined as follows. First, the energy of each individual IMF can be calculated using:

$$E_m = \sum_{p=1}^{n} |I_{mp}|^2 \tag{19}$$

where I_m is the obtained IMF and n denotes the size of the dataset used for the energy summation. The total energy for the k^{th} agent can then be calculated using:

$$E_k = \rho \sum_{m=1}^{M} E_m \tag{20}$$

where M is the number of obtained IMFs from the average voltage of k^{th} agent. ρ is a positive scaling factor.
Further, the energy ratio of the k^{th} agent (i.e., S_k) is defined to describe the relative energy level between the k^{th} agent and its neighboring agents:

$$S_k = \max(E_k/E_j), \forall j \in N_k \tag{21}$$

It is used to identify the abnormal increase of energy in an agent. Note that the energy ratio S is a set with a size of N.

Definition 1: *The authentication of an agent is labelled as $\mathbb{T}$ if the energy of the agent is greater than its neighboring agents, which can alternatively be written as:*

$$\Psi_k = \begin{cases} \mathbb{T}, & \text{if } \|S_k\| \geq e \\ \mathbb{F}, & \text{else} \end{cases} \tag{22}$$

where e is a threshold. The value of e can be found by selecting the maximum element of the set S under steady-state operations.

In this context, a detection index Θ_k using Boolean algebra is defined to determine whether an agent is attacked by FDIAs or not, i.e., 1 indicates the presence of attack, and 0, otherwise:

$$\Theta_k = \begin{cases} 1, & \text{if } \Psi_k \cap \Psi_j = \mathbb{T} \ \& \ max(E_k/E_j, E_j/E_k) < e \\ 0, & \text{else} \end{cases} \tag{23}$$

Remark III: *The detection index can be applied to the different types of false data injection attacks considered in this paper, i.e., communication link attack, local control input attack, and concurrent attack. Note that the assessment is based on the relative relationship of S_k and S_j rather than their exact values, which vary based on the system configuration.*

The proposed detection can be demonstrated using the system outlined in Fig. 1. Here, the network is subjected to (a) no attack conditions, (b) a concurrent attack between Agents 2 and 3 with $C_{con} = 5.5$ V and a ramp attack of $r = 3$ to the estimated voltage at Agent 2, and (c) a communication link attack between Agents 2 and 3 with $C_{com} = 7$ V.

In this example, the threshold e is found to be 4 from the set of $S = (2.615, 0.382, 3.997, 0.874)$. However, the energy of each agent under the concurrent attack is $E_1 = 2.939$, $E_2 = 5467$, $E_2 = 4525$, $E_4 = 3.063$, from which the set of S can be obtained as $S = (0.960, 1860, 1477, 1.042)$. Whereas, the energy of each agent under the communication link attack is $E_1 = 0.504$, $E_2 = 4692$, $E_2 = 5256$, $E_4 = 1.180$, which gives the corresponding $S = (0.427, 9309, 4454, 2.341)$. As it can be observed, the energy ratios S_2 and S_3 are significantly higher than the threshold under FDIAs. Therefore, Agents 2 and 3 are identified to encounter FDIAs according to the rules from (22) and (23).

Although the proposed EEMD-based detection is able to identify the presence of FDIAs, it cannot distinguish between concurrent attacks and communication link attacks. To differentiate these attacks, voltage correction terms from (4) will be used, as explained in the following section.

B. Differentiating Concurrent Attacks and Communication Link Attacks

For a concurrent attack, the estimated voltage of the attacked k^{th} agent can be denoted by (10). Subsequently, the estimated voltage of the attacked neighboring agent can be updated by:

$$\begin{aligned} \bar{V}_{j,con}(t) = V_j(t) \\ + \textstyle\int_0^t [\sum_{k \in N_j} a_{jk}\big(\big(\bar{V}_k(\tau) - \bar{V}_j(\tau)\big) + \alpha C_{con}\big)]\mathrm{d}\tau \end{aligned} \tag{24}$$

The corresponding voltage correction terms of these two agents can be calculated from (4). The difference between them can be used as a differentiation criterion and its value is given by:

$$DoVC = |H_1(s)\,(\alpha \cdot r \cdot t)\,| \tag{25}$$

Theoretically, the value of the proposed differentiation criterion $DoVC$ in (25) is not zero as long as there exists a concurrent attack, i.e., $\alpha \neq 0$. Moreover, its value depends on the magnitude of the local control input attack (i.e., the gradient of the ramp attack on the k^{th} agent) and time.

However, in the case of a communication link attack, the estimated voltage of the attacked neighboring agent can be obtained as:

$$\begin{aligned} \bar{V}_{j,com}(t) = V_j(t) \\ + \textstyle\int_0^t [\sum_{k \in N_j} a_{jk}\big(\big(\bar{V}_k(\tau) - \bar{V}_j(\tau)\big) + \alpha C_{com}\big)]\mathrm{d}\tau \end{aligned} \tag{26}$$

Substituting (12) and (26) into (4), the value of $DoVC$ is ideally zero as the injected false data exists in both the local agent and its neighboring agent. Note that $DoVC$ will also be zero when there is no attack on the system.

To sum up, the value of $DoVC$ can be used as a criterion to differentiate the two kinds of FDIAs, i.e.,

$$DoVC = \begin{cases} < \varepsilon & \textit{, communication link attack} \\ > \varepsilon & \textit{, concurrent attack} \end{cases} \tag{27}$$

where ε is a threshold. It can be determined by analyzing the data when the system is operating under steady-state conditions. Note that $DoVC$ of a concurrent attack is significantly larger than $DoVC$ of a communication link attack.

Returning to the case study in Section III-A, the EEMD-based detection identifies FDIAs existing in Agent 2 and 3 but it is unable to differentiate the type of attack. This can now be resolved by integrating the proposed $DoVC$ criterion with EEMD-based detection. Here, the value of $DoVC$ under steady-state operations for the considered system is found to be in the range of 0.5×10^{-4} to 1.5×10^{-4}. Hence, ε is set to the latter value. For the attack performed in Section-III-A (b), the value of $DoVC$ is 1.5×10^{-3}, which is greater than threshold ε. Therefore, it is identified as a concurrent attack.

0885-8993 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Aalborg Universitetsbibliotek. Downloaded on February 18,2021 at 07:41:14 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3055215, IEEE Transactions on Power Electronics

```
Algorithm 1: Detection and classification method of FDIAs
  Input: Average voltages of agents in the DC microgrid
  Output: Attack type
  Run EEMD algorithm to get the decomposition results;
  Calculate the energy of each agent using (19) and (20);
  Get the energy ratio of each agent using (21);
  while $|S_k| \geq e$ do
      check (23);
      if $\Theta = 1$ then
          if $DoVC > \varepsilon$ then
              The attack is a concurrent attack;
          else
              The attack is a communication link attack;
          end
      else
          check (23);
      end
  end
```

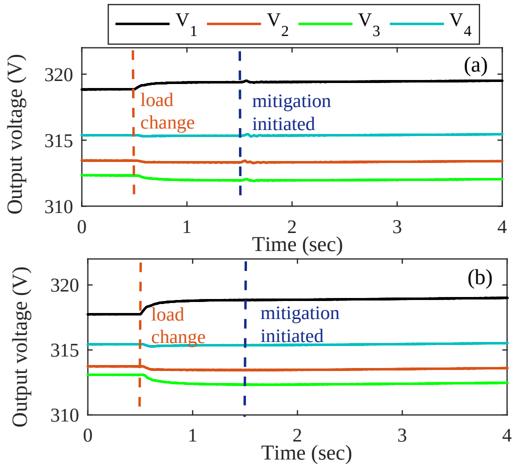

Fig. 5. Output voltages of the agents when subjected to load changes and attacks. (a) concurrent attack, and (b) communication link attack.

On the other hand, the value of $DoVC$ is 0.5×10^{-4} for the attack performed in Section-III-A (c). Using (27), the attack in Section-III-A (c) is determined as a communication link attack.

The proposed detection method to determine concurrent attacks is summarized in Algorithm 1.

C. Event-Driven Mitigation Strategy

After the detection stage, the mitigation strategy is implemented to recover from FDIAs. The compromised signal is replaced with an event-driven reconstructed signal using:

$$\Delta e^V_{jk}(t) = (1 - \Theta_k) e^V_{jk}(t) + \Theta_k e^V_{jk}(t_k)\,, \tag{28}$$

TABLE I
CALCULATED ENERGY WHEN SUBJECTED TO FDIAS

Load	Concurrent Attack				Communication Link Attack			
Change(Ω)	E_1	E_2	E_3	E_4	E_1	E_2	E_3	E_4
10	0.086	8553	9659	0.798	0.032	21116	25034	0.694
25	13	10217	9584	9.448	14	25168	27548	30
40	11	11895	6883	12	8.308	27450	25298	26
55	30	22164	11013	303	18	25334	23795	16
70	8.394	12938	4337	0.372	25	27249	21231	7.418
95	96	19191	5749	269	23	26915	11969	5.628

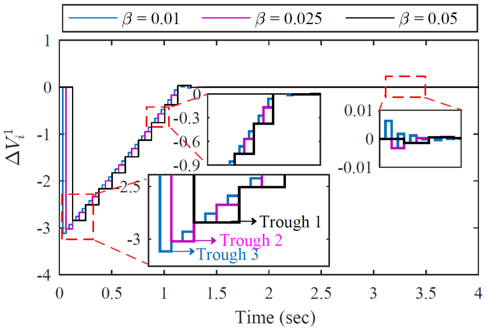

Fig. 6. Comparative analysis of the proposed mitigation strategy for different values of β in (29).

where t_k is the triggering instant with Θ_k in (23) denoting the authentication signal generated using the proposed attack detection strategy. It requires a trustworthy neighbor to be used as an input to the signal reconstruction stage. Basically, the philosophy of reconstructing a triggered signal is to hold the input signal in the absence of a trigger. It is worth notifying that a trigger is generated for the k^{th} agent when:

$$DoVC > (\varepsilon + \beta), \tag{29}$$

where β is a small positive value introduced to provide resiliency against noise in the measurements. Further if (29) is satisfied, the current set-point of the input signal is updated in the output using a `Sample and Hold` block. The input signal is $e^V_{jk}(t)$, which is communicated from a *trustworthy* agent. The reconstructed signal obtained in (28) is then substituted in (3) to attain resiliency against both the defined attacks. As soon as the objectives in (7) are met again, the authentication label is traversed back to *trustworthy* for the attacked agent. Prior to this step, the reconstructed signal is communicated to the neighboring agents. As a result, the proposed mitigation strategy eliminates the elementary step of disabling compromised communicated link(s). It is also worth notifying that regardless of any type of attack, the mitigation strategy can operate to restore the system immediately. For the purpose of brevity, further details on event-driven strategy can be referred from [27].

IV. SIMULATION RESULTS

Numerical studies have been conducted using the same network with $N = 4$ converters as depicted in Fig. 1. Each converter is treated as an *agent*, and is managed by a two-layer control framework to achieve the global reference voltage $V_{ref} = 315$ V at their respective buses. The control parameters of the test system are provided in Appendix. In this Section, the proposed resilient scheme is examined in the presence of concurrent attacks and communication link attacks, which cannot be differentiated by the distributed voltage observers. Scenarios such as load changes, faults, converter outages, and

0885-8993 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Aalborg Universitetsbibliotek. Downloaded on February 18,2021 at 07:41:14 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3055215, IEEE Transactions on Power Electronics

TABLE II
CALCULATED ENERGY WHEN SUBJECTED TO FAULTS

Fault Position	E_1 ($\times 10^6$)	E_2 ($\times 10^6$)	E_3 ($\times 10^6$)	E_4 ($\times 10^6$)
Agent 1	193.4	1.841	1.913	1.757
Agent 2	2.877	156.8	2.545	4.355
Agent 3	3.254	4.683	172.5	3.652
Agent 4	2.087	2.263	2.188	158.8

communication failures have also been simulated to assess the robustness of the proposed method.

A. Scenario I: Load Changes

The proposed method is examined in the presence of load changes and false data injection attacks (FDIAs). The initial load conditions are 96 Ω at Agent 1, 50 Ω at Agent 2, 52 Ω at Agent 3, and 56 Ω at Agent 4. A step change is triggered at Agent 1 at $t = 0.5$ s while the loads at other agents (i.e. Agent 2, 3 and 4) remain unchanged. The size of the step change ranges from 5 Ω to 95 Ω. Furthermore, the FDIAs are launched at Agents 2 and 3 at $t = 1.5$ s as shown in Fig. 5.

The settings of the concurrent attack are $C_{con} = 10$ and $r = 10$, while the communication link attack is $C_{com} = 15$.

The calculated E under different load conditions and attack scenarios are listed in Table I. In all scenarios, Agents 2 and 3 have a significantly larger E than those of the healthy agents, i.e. Agents 1 and 4. Let's consider the example when the system is subjected to a step change of 55 Ω and a concurrent attack. According to the definition in (22), Agents 2, 3 and 4 are labelled as $\mathbb{T}$. Furthermore, the proposed detection index Θ_k identifies Agents 2 and 3 as compromised agents based on (23). The type of attack can then be ascertained using the $DoVC$ differentiation criterion. In this case, $DoVC$ is found to be 3.8×10^{-3}, which is larger than the threshold ε (i.e., 1.5×10^{-4}). Using (27), such an FDIA is identified as a concurrent attack.

Moreover, the event-driven mitigation strategy defined in (28) has been initiated at $t = 1.55$ s. As a result, the output voltages are able to converge to the new steady-state values due to the load change as shown in Fig. 5.

In Fig. 6, the performance of the proposed event-driven mitigation strategy is tested for different values of β. It can be seen that with the increasing value of β, the resolution of the reconstructed signal becomes poorer. However, the dynamic performance is improved with an almost equal settling time but with varying troughs, as indicated in Fig. 6. However, a very low value of β will also be an important issue in a system with variable noise. Hence, the design of β needs to consider factors such as accuracy and dynamic response.

B. Scenario II: Faults

Next, the proposed method is evaluated when the system is subjected to a short-circuit fault at different agents. The purpose of this analysis is to evaluate the ability of the resilient control strategy in distinguishing a physical fault from a data attack. The loads connected to each agent are the same as those in Subsection IV-A. Its corresponding energy E at various fault locations are summarized in Table II. Overall, E of a short-circuited agent is significantly higher than that of other agents in the network. This can be regarded as the feature of a physical fault. Subsequently, the authentication in (22) will only label $\mathbb{T}$ for an agent which is subjected to faults.

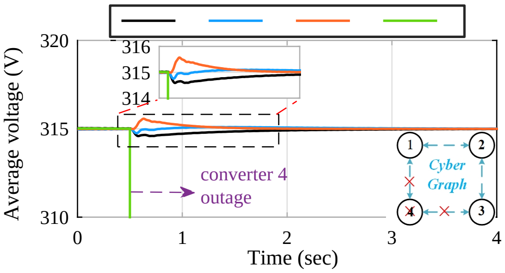

Fig. 7. Average voltages of the agents when Agent 4 is disconnected. The average voltage of Agent 4 (i.e., $\bar{V}_4$) drops to zero immediately after this outage.

However, the corresponding detection index Θ_k in (23) is zero, indicating there are no attacks.

Note that a short-circuit fault at one agent will physically disrupt the power flow in the microgrid. Such disruption will be felt among all agents.

C. Scenario III: Converter Outage and Communication Failure

The performance of the proposed method is examined when the considered system suffers from a converter outage. In this scenario, converter 4 (or Agent 4) is disconnected at $t = 0.5$ s. The estimated voltages of the agents are shown as Fig. 7. The energy of the remaining agents (i.e., Agents 1, 2, and 3) are found to be $E_1 = 614$, $E_2 = 2.436$, and $E_3 = 150$. Referring to *Definition 1*, the authentication of the remaining agents are $\mathbb{T}$, $\mathbb{F}$, and $\mathbb{T}$, respectively. Applying the detection index in (23), the resilient control strategy identifies that there are no attacks considering that none of the neighboring agents both have $\mathbb{T}$. On the other hand, the current sent by the agent of the converter outage will be zero. This enables the proposed method to distinguish the converter outage from cyber attacks.

Next, the cyber link between Agents 2 and 3 is disconnected to simulate a communication failure. As a result, the number of neighboring agents communicating with Agent 2 and Agent 3 has decreased. Note that the consensus protocol will still operate based on the remaining cyber graphs to achieve the global reference value of 315 V. On the other hand, the energy values of each agent under this communication outage are: $E_1 = 34.301 \times 10^4$, $E_2 = 9.812 \times 10^4$, $E_3 = 15.023 \times 10^4$, $E_4 = 8.6149 \times 10^4$. Subsequently, all agents are labelled as $\mathbb{F}$, indicating that there are no attacks within the microgrid.

V. DISCUSSIONS

In the EEMD method, the noise amplitude α and the ensemble number N_{um} are the two parameters that need to be stipulated. We have also carried out analysis on the effects of the two parameters on the proposed attack detection method. The simulation results are listed in Table III and Table IV. The

0885-8993 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Aalborg Universitetsbibliotek. Downloaded on February 18,2021 at 07:41:14 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3055215, IEEE Transactions on Power Electronics

TABLE III
CALCULATED ENERGY WHEN $\alpha = 0.19$

Parameter	Concurrent Attack				Communication Link Attack			
Settings	E_1	E_2	E_3	E_4	E_1	E_2	E_3	E_4
e_n=1%, N_{um} =400	19	4945	4255	8.562	12	5632	5698	13
e_n=2%, N_{um} =100	21	5599	4273	6.681	10	4960	7859	11
e_n=3%, N_{um} =45	19	7779	4441	7.423	8.006	7991	4330	28

[1] e_n is the difference of the targeted data and the summation of IMFs.

[2] N_{um} is the number of ensemble trials in the EEMD method.

TABLE IV
CALCULATED ENERGY WHEN $\alpha = 0.3$

Parameter	Concurrent Attack				Communication Link Attack			
Settings	E_1	E_2	E_3	E_4	E_1	E_2	E_3	E_4
e_n=1%, N_{um}=950	28	2716	1822	25	2.690	3489	4061	3.416
e_n=2%, N_{um} =240	28	2599	2015	29	4.286	3623	3175	3.842
e_n=3%, N_{um} =106	28	2432	2221	29	3.455	3629	3117	4.704

FDIAs are launched at t = 1.5 s at Agents 2 and 3. The settings for the concurrent attack are $C_{con} = 10$ and $r = 10$, while the communication link attack is $C_{com} = 15$. In all scenarios from Table III and Table IV, it can be observed that the energy of Agents 2 and 3 are much higher than Agents 1 and 4. This facilitates the successful attack detection using the proposed detection index Θ_k.

Therefore, we can conclude that the noise amplitude and the number of ensembles will not affect the effectiveness of the proposed attack detection method.

VI. EXPERIMENTAL RESULTS

In the previous section, we have demonstrated the effectiveness of the proposed resilient control scheme using simulation examples. In this section, we demonstrate that the proposed method could be implemented experimentally as well. For this, we consider a DC microgrid consisting of $N = 2$ converters. Each converter is connected with a programmable load as shown in Fig. 8. The global voltage reference of the DC microgrid is 48 V. The converters are controlled by dSPACE MicroLabBox DS1202 (target), while control commands are sent from a computing workstation (host). The communication network in experimental setup is realized using *SimEvents* elements (modeled inside the dSPACE platform) to emulate the cyber network characteristics in detail. This model requires inputs: event priority time, sequence, latency and number of servers corresponding to any communication medium, which can be acquired by OPNET Riverbed Modeler [28]. OPNET Modeler is used to design, model and analyze communication networks and their redundancies. More details on the SimEvents based communication network model can be referred from [29]. The parameters of the experimental setup are provided in Appendix.

In Fig. 9, a concurrent attack is launched in the system shown in Fig. 8. Regardless of the classification technique, the mitigation strategy is activated as long as the detection strategy suggests that false data injection attacks are present in the control system. After the detection index Θ_k is triggered, the proposed event-driven signal reconstruction process is carried out to replace the attacked signal with the reconstructed signal. As a result, it can be seen in Fig. 9 that the voltages of both converters follow a steady-state response even in the presence of an attack. Furthermore, the mitigation strategy is robust to the disturbance such as a load change at $t = 4.1$ s. A similar case study is carried out in Fig. 10 for a communication link attack on the link directed from agent 1 to 2. It can be seen that as soon as the detection strategy is activated to send the authentication labels, the mitigation strategy operates to achieve system recovery immediately. In this way, the system resiliency against the defined cyber attacks has been enhanced.

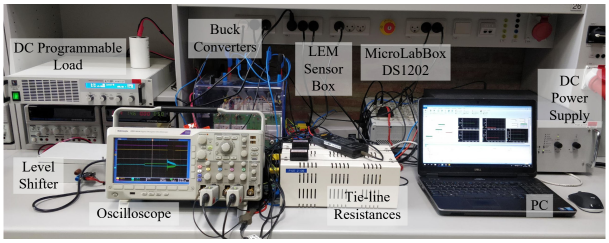

Fig. 8. Experimental setup of a DC microgrid consisting of $N = 2$ agents.

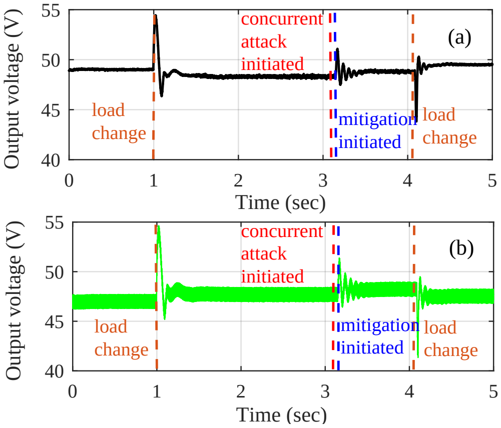

Fig. 9. Output voltages for the agents when subjected to load changes and a concurrent attack. (a) converter 1, and (b) converter 2.

Next, we examined the robustness of proposed resilient control strategy under communication delays. As studied in [30], distributed control is resilient to a limited maximum communication delay. This value varies for different communication mediums. As this paper employs a ring based cyber topology, two communication mediums, namely WLAN (IEEE 802-11 b/g) and wired (narrowband DS0) have been considered here to analyze the performance of the proposed attack identification strategy. Basically, the time delay performance is marginalized by the convergence properties of the Laplacian matrix, which could easily go into the RHP when the delay is more than the theoretical value of maximum delay τ_d, where eigenvalues are placed in the origin. Using the time-delay stability analysis (already carried out in [30]) for N = 2 converters in the experimental setup, it is established that the system remains stable even under a maximum communication delay of τ_d = 336 ms.

These communication mediums (with a ring based cyber graph) are simulated in the OPNET Riverbed Modeler to get the maximum latency and bit error rate, as outlined in Table V.

Based on the obtained results from OPNET (for wired

0885-8993 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Aalborg Universitetsbibliotek. Downloaded on February 18,2021 at 07:41:14 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3055215, IEEE Transactions on Power Electronics

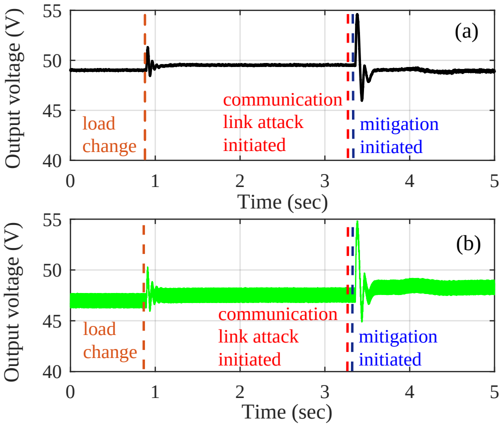

Fig. 10. Output voltages for the agents when subjected to load changes and a communication link attack. (a) converter 1, and (b) converter 2.

medium) and the time delay analysis, the maximum communication delay obtained under both conditions are almost same. Finally, the real-time performance in the presence of attacks has been tested in Fig. 11 under the latency values obtained in Table V. It can be seen in Fig. 11 that the proposed attack identification and mitigation strategy provides good resilience behavior to achieve the secondary control objectives of DC microgrids under a communication delay of 0.029 s and 0.327 s in the presence of concurrent attack. Note that any value above the theoretical margin of τ_d = 336 ms will anyway result in oscillatory instability in the microgrid regardless of the presence or absence of cyber-attacks. Hence, the proposed controller is limited to provide resiliency against cyber-attacks only within the time-delay stability margin of the defined system.

VII. Conclusion

This paper presents a novel false data injection attack, known as a concurrent attack, targeting both local estimated voltages and communication links simultaneously in DC microgrids governed by distributed cooperative control. The impact of this attack is investigated using the consensus theory. Since the system response to the concurrent attack can be manipulated to be identical to that of a communication link attack, the grid operator may incorrectly identify the type of attack. This may cause inadequate mitigation of the attacks. Therefore, a resilient control scheme is proposed. The scheme can detect the presences of false data injection attacks. Additionally, a classification criterion is proposed to differentiate between concurrent attacks and communication link attacks. Subsequently, an event-driven reconstructed signal replaces the attacked signal and mitigates the attack impact. The performance of the proposed resilient control scheme has been validated under load changes, faults, converter outages, and communication failures.

Appendix

Simulation Parameters

The simulated cooperative DC microgrid consists of four equal-rated source for 3 kW. The line resistance R_{ij} denotes the resistance from i^{th} agent to j^{th} agent. In addition, the gains for the controller in each agent are consistent.

Plant: $R_{12} = 1.3\Omega$, $R_{13} = 1.8\Omega$, $R_{23} = 1.2\Omega$, $R_{43} = 1.5\Omega$, $L_i = 3\text{mH}$, $C_{dci} = 250\mu\text{F}$

Controller: $V_{ref} = 315\text{V}$, $I_{ref} = 0$, $K_P^{H_1} = 3$, $K_I^{H_1} = 0.01$, $K_P^{H_2} = 4.5$, $K_I^{H_2} = 0.32$, $G_{VP} = 2.8$, $G_{VI} = 12.8$, $G_{CP} = 0.56$, $G_{CI} = 21.8$, $a_{ij} = 1$, $\rho = 1.0 \times 10^4$

TABLE V
Latency In Different Communication Mediums

Transmission Medium	Max. Latency (s)	Bit Error Rate (%)
WLAN (IEEE 802-11 b/g)	0.029	0.01
Wired (narrowband DS0)	0.327	0.02

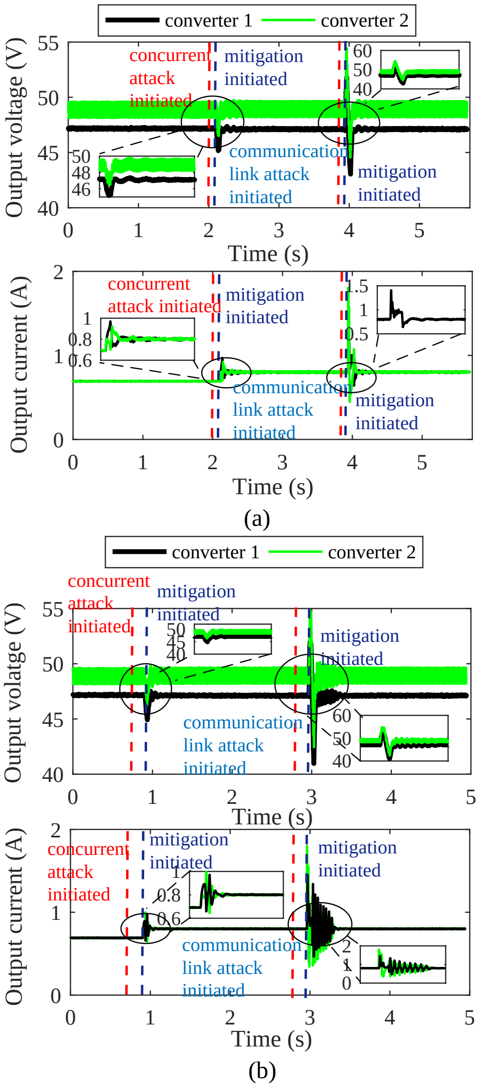

Fig. 11. Experimental results on performances of the proposed resilient control strategy under different communication delays: (a) with 0.029 s communication delay, and (b) with 0.327 s communication delay

Experimental Testbed 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.

0885-8993 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Aalborg Universitetsbibliotek. Downloaded on February 18,2021 at 07:41:14 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3055215, IEEE Transactions on Power Electronics

Plant: L_{se_i}= 3 mH, C_{dc_i}= 100 μF, R_1 = 0.8 Ω, R_2 = 1.4 Ω

Controller: $V_{dc_{ref}}$= 48 V, $I_{dc_{ref}}$ = 0, $K_P^{H_1}$ = 1.92, $K_I^{H_1}$ = 15, $K_P^{H_2}$ = 4.5, $K_I^{H_2}$ = 0.08, h = 1.8, f = 2.4, β = 0.025.

References

[1] J. J. Justo, F. Mwasilu, J. Lee, and J.-W. Jung, “AC-microgrids versus DC-microgrids with distributed energy resources: A review,” *Ren. Sustain. Energy Reviews*, vol. 24, pp. 387–405, Aug. 2013.

[2] T. Dragičević, 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.

[3] A. T. Elsayed, A. A. Mohamed, and O. A. Mohammed, “DC microgrids and distribution systems: An overview,” *Electric Power Systems Research*, vol. 119, pp. 407–417, Feb. 2015.

[4] S. Anand, B. G. Fernandes, and J. Guerrero, “Distributed control to ensure proportional load sharing and improve voltage regulation in low-voltage DC microgrids,” *IEEE Trans. Power Electron.*, vol. 28, no. 4, pp. 1900–1913, Apr. 2013.

[5] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Trans. Information and System Security*, vol. 14, no. 1, pp. 1–33, Jun. 2011.

[6] F. Pasqualetti, F. Dörfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” *IEEE Trans. Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[7] C. Cameron, C. Patsios, P. C. Taylor, and Z. Pourmirza, “Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes,” *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3010–3019, May 2019.

[8] G. Raman, B. AlShebli, M. Waniek, T. Rahwan, and J. C.-H. Peng, “How weaponizing disinformation can bring down a city’s power grid,” *PloS one*, vol. 15, no. 8, p. e0236517, 2020.

[9] O. A. Beg, T. 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.

[10] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, “A stealth cyber-attack detection strategy for DC microgrids,” *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[11] C. Zhao, J. He, P. Cheng, and J. Chen, “Analysis of consensus-based distributed economic dispatch under stealthy attacks,” *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 5107–5117, Jun. 2017.

[12] S. Sridhar, M. Govindarasu, and C.-C. Liu, “Risk analysis of coordinated cyber attacks on power grid,” in *Control and Optimization Methods for Electric Smart Grids*. Springer, 2012, pp. 275–294.

[13] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, Y. Zhang, and C.-K. Wen, “Local cyber-physical attack for masking line outage and topology attack in smart grid,” *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4577–4588, Jul. 2019.

[14] A. Teixeira, H. Sandberg, and K. H. Johansson, “Networked control systems under cyber attacks with applications to power networks,” in *Proceedings of the 2010 American Control Conference*. IEEE, Jun. 2010, pp. 3690–3696.

[15] I. Shames, A. M. Teixeira, H. Sandberg, and K. H. Johansson, “Distributed fault detection for interconnected second-order systems,” *Automatica*, vol. 47, no. 12, pp. 2757–2764, Dec. 2011.

[16] F. Pasqualetti, F. Dörfler, and F. Bullo, “A divide-and-conquer approach to distributed attack identification,” in *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, Dec. 2015, pp. 5801–5807.

[17] M. Davoodi, N. Meskin, and K. Khorasani, “Simultaneous fault detection and consensus control design for a network of multi-agent systems,” *Automatica*, vol. 66, pp. 185–194, Apr. 2016.

[18] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, and G. Ferrari-Trecate, “Distributed cyber-attack detection in the secondary control of DC microgrids,” in *2018 European Control Conference (ECC)*. IEEE, 2018, pp. 344–349.

[19] 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.

[20] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, “Resilient cooperative control of DC microgrids,” *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 1083–1085, Jan. 2019.

[21] K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Detection of faults and attacks including false data injection attack in smart grid using Kalman filter,” *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[22] S. Sundaram and C. N. Hadjicostis, “Distributed function calculation via linear iterative strategies in the presence of malicious agents,” *IEEE Trans. Automatic Control*, vol. 56, no. 7, pp. 1495–1508, Jul. 2011.

[23] X. Lu, J. M. Guerrero, K. Sun, and J. C. Vasquez, “An improved droop control method for DC microgrids based on low bandwidth communication with DC bus voltage restoration and enhanced current sharing accuracy,” *IEEE Trans. Power Electron.*, vol. 29, no. 4, pp. 1800–1812, April. 2014.

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

[25] N. Huang, Z. Shen, S. Long, M. Wu, E. Shih, Q. Zheng, C. Tung, and H. Liu, “The empirical mode decomposition method and the hilbert spectrum for nonlinear and non-stationary time series analysis,” *Proceedings of the Royal Society of London, Series A. v454*, pp. 903–995, 1998.

[26] Z. Wu and N. E. Huang, “Ensemble empirical mode decomposition: a noise-assisted data analysis method,” *Advances in Adaptive Data Analysis*, vol. 1, no. 01, pp. 1–41, Jan. 2009.

[27] S. Sahoo, T. Dragicevic, and F. Blaabjerg, “An event-driven resilient control strategy for DC microgrids,” *IEEE Trans. Power Electron.*, 2020, DOI 10.1109/TPEL.2020.2995584.

[28] “Opnet modeler [online],” https://support.riverbed.com/content/support/software/opnet-model/modeler.html.

[29] R. Rana, S. Sahoo, S. Mishra, and J. C. Peng, “Performance validation of cooperative controllers in autonomous AC microgrids under communication delay,” in *2019 IEEE Power Energy Society General Meeting (PESGM)*, 2019, pp. 1–5.

[30] S. Sahoo, S. Mishra, S. Jha, and B. Singh, “A cooperative adaptive droop based energy management and optimal voltage regulation scheme for DC microgrids,” *IEEE Trans. Ind. Electron.*, vol. 67, no. 4, pp. 2894–2904, April. 2020.

Jingqiu Zhang (Student Member, IEEE) received the B.S. and M.S. degree in electrical engineering from Tianjin University, Tianjin, China in 2016 and 2019, respectively. He is currently working towards his Ph.D. degree in electrical and computer engineering at the National University of Singapore, Singapore. His current research interests include cyber security of power grids, distributed control and optimization in microgrids.

Subham Sahoo (Member, IEEE) received the B.Tech. & Ph.D. degree in Electrical and Electronics Engineering from VSS University of Technology, Burla, India and Electrical Engineering at Indian Institute of Technology, Delhi, New Delhi, India in 2014 & 2018, respectively. He has worked as a Visiting Student with the Department of Electrical and Electronics Engineering in Cardiff University, UK in 2017. Prior to completion of his PhD, he worked as a Research Fellow in the Department of Electrical and Computer Engineering in National University of Singapore. He is currently working as a postdoctoral researcher in the Department of Energy Technology, Aalborg University, Denmark. He is a recipient of the Indian National Academy of Engineering (INAE) Innovative Students Project Award for his PhD thesis across all the institutes in India for the year 2019. He has also won the IRD Student Start-up Award in the year 2017 to incorporate a company named SILOV SOLUTIONS PVT. LTD. commercialized and based on his contributions during his doctoral studies. He was also one of the outstanding reviewers for IEEE Transactions on Smart Grid in the year 2020. He currently serves as a secretary of IEEE Young Professionals Affinity Group, Denmark and Joint IAS/IES/PELS in Denmark section. His research interests are control and stability of microgrids, renewable energy integration, cyber-physical power electronic systems and cyber security in power electronic systems.

0885-8993 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Authorized licensed use limited to: Aalborg Universitetsbibliotek. Downloaded on February 18,2021 at 07:41:14 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2021.3055215, IEEE Transactions on Power Electronics

Jimmy Chih-Hsien Peng (Member, IEEE) received the B.E. and Ph.D. degrees in electrical and computer engineering from the University of Auckland, Auckland, New Zealand, in 2008 and 2012, respectively. He is currently an Assistant Professor in Electrical and Computer Engineering with the National University of Singapore, Singapore. Previously, he was with the Masdar Institute (now part of the Khalifa University), Abu Dhabi, United Arab Emirates. In 2013, he was appointed a Visiting Scientist with the Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA, USA, where he became a Visiting Assistant Professor in 2014. He is currently a member of the Electrical and Electronic Standards Committee, under the Singapore Standards Council. His research interests include power system stability, grid resilience, cyber security, microgrids, and high-performance computing.

Frede Blaabjerg (Fellow, IEEE) was with ABB-Scandia, Randers, Denmark, from 1987 to 1988. From 1988 to 1992, he got a Ph.D. degree in Electrical Engineering at Aalborg University in 1995. He became an Assistant Professor in 1992, an Associate Professor in 1996, and a Full Professor of power electronics and drives in 1998. From 2017 he became a Villum Investigator. He is honoris causa at University Politehnica Timisoara (UPT), Romania, and Tallinn Technical University (TTU) in Estonia. His current research interests include power electronics and its applications, such as in wind turbines, PV systems, reliability, harmonics, and adjustable speed drives. He has published more than 600 journal papers in the fields of power electronics and its applications. He is the co-author of four monographs and editor of ten books in power electronics and its applications. He has received 32 IEEE Prize Paper Awards, the IEEE PELS Distinguished Service Award in 2009, the EPE-PEMC Council Award in 2010, the IEEE William E. Newell Power Electronics Award 2014, the Villum Kann Rasmussen Research Award 2014, the Global Energy uPrize in 2019 and the 2020 IEEE Edison Medal. He was the Editor-in-Chief of the IEEE TRANSACTIONS ON POWER ELECTRONICS from 2006 to 2012. He has been a Distinguished Lecturer for the IEEE Power Electronics Society from 2005 to 2007 and for the IEEE Industry Applications Society from 2010 to 2011 as well as 2017 to 2018. In 2019-2020 he served a President of the IEEE Power Electronics Society. He is Vice-President of the Danish Academy of Technical Sciences too. He is nominated in 2014-2019 by Thomson Reuters to be between the most 250 cited researchers in Engineering in the world.

0885-8993 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Aalborg Universitetsbibliotek. Downloaded on February 18,2021 at 07:41:14 UTC from IEEE Xplore. Restrictions apply.