An Event-Driven Resilient Control Strategy for DC Microgrids

Sahoo, Subham; Dragicevic, Tomislav; Blaabjerg, Frede

Published in:
I E E E Transactions on Power Electronics

DOI (link to publication from Publisher):
10.1109/TPEL.2020.2995584

Publication date:
2020

Document Version
Accepted author manuscript, peer reviewed version

An Event-Driven Resilient Control Strategy for DC Microgrids

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

***Abstract*—Though recent advancements in DC microgrids are largely based on distributed control strategies to enhance reliability, their susceptibility to cyber attacks still remains a challenging issue. Additionally in converter-dominated DC microgrids, mitigation of cyber attacks upon detection in a timely manner is the need of the hour to prevent the system from immediate shutdown. Since most of the existing research is primarily focused on detection of cyber attacks in DC microgrids without giving prior attention to comprehensive steps of mitigation, this paper classifies cyber attacks as *events* and introduces an event-driven cyber attack resilient strategy for DC microgrids, which immediately replaces the attacked signal with a *trusted* event-driven signal constructed using `True` transmitted measurements. This mechanism not only disengages the attack element from the control system, but also replaces it with an event-triggered estimated value to encompass normal consensus operation during both steady-state as well as transient conditions even in the presence of attacks. Finally, the event detection criteria and its sensitivity is theoretically verified and validated using simulation and experimental conditions in the presence of both stealth voltage and current attacks.**

***Index Terms*—DC microgrid, cyber attacks, distributed control, cyber-physical systems.**

I. Introduction

THE rapid development of DC microgrids can be ascribed to their high flexibility in integrating renewable energy sources, storage devices and modern electronic loads, in both grid-connected and autonomous modes of operation [1]. In this regard, distributed control structures have been trending for microgrids as they facilitate scalability, reliability and automation in contrast to the centralized controllers, which are highly vulnerable to single-point-of-failure [2]. Moreover, they ensure robust performance under cyber imperfections such as communication delays, link failures and data packet losses [3]. However, this coordination philosophy can not be designated to be fully *reliable* owing to the availability of information of only neighboring units. This increases the vulnerability of microgrids to illegitimate sensors and actuators tampering in the form of cyber attacks [4]. As microgrids are a key component of mission critical applications such as military bases, hospitals and industrial plants [5], it is crucial to ensure their security against adversial attacks.

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: sssa@et.aau.dk and fbl@et.aau.dk) *(Corresponding Author: Subham Sahoo)*

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)

To detect the presence of cyber attacks, bad-data detection tests are usually performed to identify residual element(s) between estimated and measured states [6]. These attacks can be classified differently into a primary superset with false data injection attacks (FDIAs) [7], denial of service (DoS) [8] and replay attacks as its elements [9]. These are some of the prominent attacks that has precipitated in real-time applications. More details on other critical intrusion approaches, which are the subsets of the conventional attacks, can be found in [11]. Further, these attacks can also be *coordinated*, where the attacker attains sufficient knowledge about the cyber-physical architecture to create attack vectors, which can easily bypass the abovementioned bad-data detection tests [12]. Such attacks are commonly termed as *stealth* attacks [13]. In other words, these attacks introduce zero dynamics in distributed control systems, which goes unnoticeable. The attacker can use this *discreet* behavior to collect more system information by penetrating into the control system at first, and then attack microgrids to cause instability later in unforeseeable ways. Hence, accuracy in detection and mitigation of stealth attacks in a timely manner in distributed DC microgrids remain a primary concern. Specifically in power electronics based systems, the mitigating action needs to be fast, otherwise the network can become unstable or even lead to shutdown.

Considerable efforts have been put recently in modeling and detection of stealth cyber attacks on various elements (sensors, communication links) in DC microgrids [14], [15]. Further studies on differentiating between sensor faults and cyber attacks is carried out in [16]. However, these papers are limited to detection without providing any comprehensive steps of countermeasures for normal system operation to remove the attack element(s). Additionally, the information received from the attacked unit(s) is discarded as an elementary approach to prevent the propagation of attack into the system [17]. As a result, the network connectivity is affected, which leads to disruption in the consensus theory. In [18], O. Beg et. al. have proposed an attack impact quantification technique and suppressed the impact of attack element using a deterministic number in the low-pass filter. However, the scalability of the mitigation approach is not largely discussed. Another well-defined mitigation approach is to employ an observer for each unit to operate with the estimated states using the pre-attack points upon detection of attack [19]. Even though these approaches are quite efficient, they have model-intensive requirements, where their performance is highly prone to model uncertainities. Moreover, the design of observer can be complex, while its real-time execution may require heavy computational resources. Additionally, an upper bound based

mitigation condition is also proposed in [20] where the mitigation strategy is selectively determined based on the total number of compromised units, termed as F-total, or the local compromised agents in the neighborhood of each unit, termed as F-local. Although it counteracts against attacks on sensors, actuators and communication links, it might affect the cyber graph connectivity by unneccesarily abandoning neighbor's information during a load change even when there is no attack. As a result, its operation becomes a point of serious concern for stealth attacks, which entails zero dynamics in distributed networks. Further in [21], a cooperative trust and confidence factor based resiliency algorithm is proposed for DC microgrids to mitigate the false data immediately by adaptively changing the communication weights. 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. Hence, since the abovementioned approaches are based on restrictive assumption on the information exchange in the cyber network, a self-healing mitigation strategy needs to be developed, which provides maximum resilience for the system to recover without losing the cyber network connectivity.

To address these issues, this paper proposes an event-driven cyber attack resilient strategy for DC microgrids for the first time, where only the presence of a cyber attack element in a given agent is classified as an *event*. As compared to the conventional event-triggered schemes [22]-[23], attack detection criterion are used as triggering mechanisms for the proposed countermeasures to operate immediately [24]-[25]. As already discussed in [14], [15], since stealth attacks involve compromised sensors, actuators and communication links, activation of these events is defined using the detection criteria for each unit. Further, the activation status of these events in the attacked agent is also transmitted to non-compromised neighbors to authenticate the transmitted measurements as `False`. Since the cyber and control layers are closely coupled, this action firstly ensures that the attacked measurement is discarded locally and in the neighboring agents. Secondly, as long as the events are activated in the attacked unit, an event-triggered signal is constructed using the measurement(s) of *trusted* neighbors (with authentication signal labeled as `True`). The signal reconstruction is done by using detection criteria as triggering mechanism to operate within prespecified thresholds. Unlike observers, the proposed mechanism doesn't involve any integration operation to remove the attack elements, thereby making it computationally viable. By doing so, it is ensured that the system continues to operate normally during both steady-state and transient conditions. Finally, different avenues of system operation are discussed in detail corresponding to the severity of stealth attacks on both voltage and current measurements in DC microgrids. To establish the convergence between the event-driven resilient signal and time-triggered signal(s), a theoretical analysis is also carried out to establish that the system could operate with $N-1$ event-driven resilient signals under worst-case attack scenarios. As opposed to the existing resilient schemes, the proposed strategy offers $N-1$ and full scale of resilience for stealth attacks on currents and voltages in a DC microgrid comprising of N converters, respectively. Furthermore, no model-intensive design requirements and flexibility to operate without disabling the compromised cyber links are additional advantages of the propsed approach, which showcases a new norm of resiliency of cooperative microgrids against cyber attacks.

The rest of the paper is organized as follows. Section II depicts a brief overview of the cyber-physical architecture of DC microgrids alongwith a basic overhaul of distributed secondary control objectives and performance of conventional event-triggered theory in the presence of stealth attacks. Next, a comprehensive resilience framework alongwith signal reconstruction via triggering criterion for stealth attacks is provided in Section III. Section IV provides a convergence analysis of the event-driven resilient signals with the periodic time-triggered authenticated measurements from the neighbors to study the feasibility of the proposed approach. Simulations along with experimental validation are presented in Section V and VI, respectively. A brief on the main features and advantages of the proposed approach is added to Section VII. Finally, Section VIII provides the concluding remarks and future scope of this work.

II. Preliminaries of Stealth Attacks in Cooperative DC Microgrids

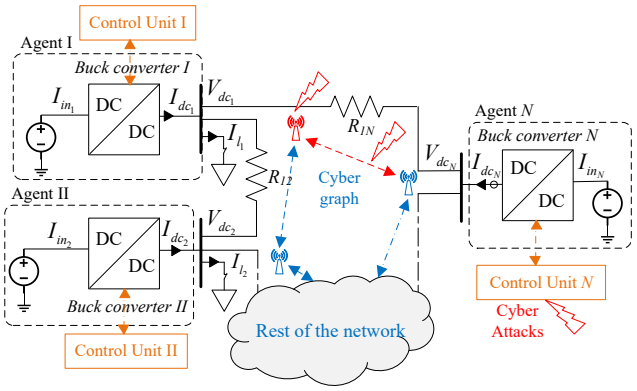

Fig. 1. Generic cyber-physical model of DC microgrid with N agents: Blue arrows represent the cyber layer and black lines represent the physical circuit. Further, red lines represent the attacked component(s) in the cyber-physical DC microgrid.

A. Preliminaries of Conventional Cooperative Control in DC Microgrids

An exemplary autonomous DC microgrid considered in this work is shown in Fig. 1. N DC sources connected via DC/DC buck converters of equal power rating are interconnected to each other via tie-lines forming the physical layer of the microgrid. Each converter is operated in voltage controlled mode. Cooperative secondary controllers are employed to improve current sharing performance and voltage regulation of these sources [26]. These controllers are made possible using

a distributed communication layer, which shares information only between the neighboring units. Each unit, represented as an *agent* in the cyber layer, sends and receives $x_j = \{\bar{V}_{dc_j}, I^{pu}_{dc_j}\}$ from the neighboring agent(s) to achieve secondary control objectives namely, average voltage regulation and proportionate current sharing, where $\bar{V}_{dc_j}$ and $I^{pu}_{dc_j}$ denote the average voltage estimate and per unit output current of the neighboring agents, respectively.

Each agent is represented via a node and a communication digraph is represented via edges. They constitute an adjacency matrix $\mathbf{A} = [a_{ij}] \in R^{N\times N}$, where the communication weights are given by: $a_{ij} > 0$, if $(\psi_i, \psi_j) \epsilon \mathbf{E}$, where $\mathbf{E}$ is an edge connecting two nodes, with ψ_i and ψ_j being the local and neighboring node, respectively. Otherwise, $a_{ij} = 0$. Further, the incoming cyber information matrix can be denoted by $\mathbf{Z}_{in} = \sum_{i\in N} a_{ij}$. Hence, if $\mathbf{A}$ 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:

$$u_i(t) = \sum_{j\epsilon M_i} \underbrace{a_{ij}(x_j(t) - x_i(t))}_{e_i(t)} \tag{1}$$

where $u_i = \{u_i^V, u_i^I\}$, $e_i = \{e_i^V, e_i^I\}$ respectively as per the elements in x and M_i is the set of neighbors of i^{th} agent.

Remark I: *As per the synchronization law [27], all the agents participating in distributed control will achieve consensus using* $\dot{\mathbf{x}} = -\mathbf{Lx}$ *for a well-spanned Laplacian matrix* $\mathbf{L}$ *such that* $\lim_{t\to\infty} x_i(t) = c, \ \forall \ i \in N$, *where* c *is the steady-state reference and* N *is the number of agents.*

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:

$$\textbf{Sublayer I: } \Delta V_{1_i} = H_1(s)(V_{dc_{ref}} - \bar{V}_{dc_i}) \tag{2}$$

$$\textbf{Sublayer II: } \Delta V_{2_i} = H_2(s)(I_{dc_{ref}} - u_i^I) \tag{3}$$

where $\bar{V}_{dc_i} = V_{dc_i} + \int_0^\tau \sum_{i\in M_i}(u_i^V d\tau)$, while $H_1(s)$, $H_2(s)$ are PI controllers. Further, $V_{dc_{ref}}$ & $I_{dc_{ref}}$ are the global reference voltage and current quantities for all the agents, respectively. It should be noted that $I_{dc_{ref}} = 0$ for proportionate current sharing between the agents. The correction terms obtained in (2)-(3) are finally added to the global reference voltage to achieve local voltage references for i^{th} agent using:

$$V^i_{dc_{ref}} = V_{dc_{ref}} + \Delta V_{1_i} + \Delta V_{2_i}. \tag{4}$$

Using (4) as the local voltage reference for i^{th} agent, the abovementioned secondary objectives are achieved.

Using the distributed consensus algorithm for a well connected cyber graph in a DC microgrid, the system objectives for DC microgrids using (1)-(4) shall converge to:

$$\lim_{t\to\infty} v_i(t) = V_{dc_{ref}}, \ \lim_{t\to\infty} u_i^I(t) = 0 \ \ \forall i \ \epsilon \ N \tag{5}$$

where $v_i(t) = V_{dc_i}(t) + \int_{j \ \epsilon \ M_i} u_i^V(t)$ with V_{dc_i} denoting the measured output voltage of i^{th} agent.

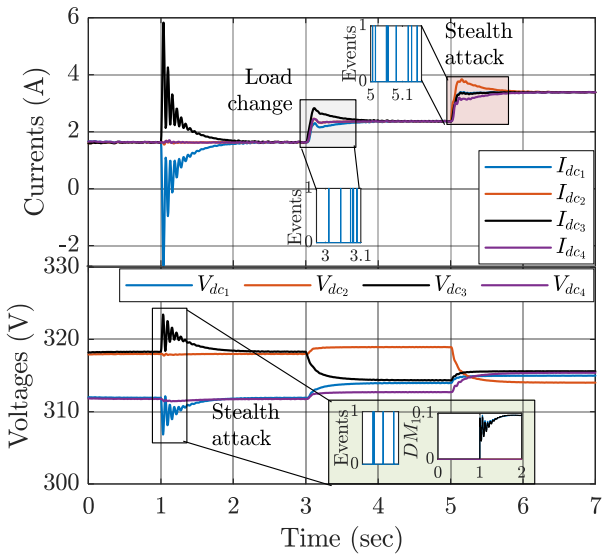

Fig. 2. Stealth attacks in DC microgrid with N = 4 agents on average voltage control inputs [14] of unit I and III at t = 1 sec and, current sensor and outgoing communication link [15] of unit II at t = 1 sec with attack II around t = 5 sec – Conventional event-triggered philosophy [22] can not discriminate between a load change and stealth attack since the objectives in (5) are met satisfactorily.

TABLE I
STEALTH ATTACKS IN DC MICROGRIDS IN [14] AND [15]

Affected Counterparts	Modeling
Voltage [14]	$\mathbf{W}x^V_{attack} = 0$
Current [15]	$\mathbf{W}x^I_{attack} = 0$

B. Modeling of Stealth Attacks in DC Microgrids

As shown in Fig. 1, cyber attackers may inject unknown exogeneous signals in many ways such as, injection of false data into the controllers, sensors, communication links, etc. to disrupt the system objectives in (5). These attacks can be conducted in a coordinated manner to deceive the system operator in the presence of any such attack elements using the following modified inputs in (1), given by:

$$\mathbf{u}^a(t) = \mathbf{Lx}(t) + \mathbf{W}\mathbf{x}_{attack} \tag{6}$$

where $\mathbf{u}^a, \mathbf{x}$ and $\mathbf{x}_{attack}$ denote the vector representation of the attacked control input $u_i^a = \{u_i^{Va}, u_i^{Ia}\}$, the states and the attack elements $x_{attack_i} = [x^V_{attack_i}, x^I_{attack_i}]^T$, respectively. Further, $\mathbf{W} = [w_{ij}]$ denotes a row-stochastic matrix with its elements given by:

$$w_{ij} = \begin{cases} \frac{1}{M_i+1}, \ j \in M_i \\ 1 - \sum_{j\epsilon M_i} w_{ij}, \ j = i \\ 0, j \notin M_i, j \neq i \end{cases} \tag{7}$$

It should be further noted that $\mathbf{x}_{attack}$ is bounded, such that the protection measures for the DC/DC converter do not operate as soon as the following holds true:

$$\mathbf{V}_{dc_{min}} < \mathbf{V}_{dc} < \mathbf{V}_{dc_{max}} \tag{8}$$

$$\mathbf{I}_{dc_{min}} < \mathbf{I}_{dc} < \mathbf{I}_{dc_{max}} \tag{9}$$

where $\mathbf{I}_{dc_{min}}$, $\mathbf{I}_{dc_{max}}$, $\mathbf{V}_{dc_{min}}$ and $\mathbf{V}_{dc_{max}}$ denote the vector representation of minimum and maximum threshold for output current, minimum and maximum threshold for output voltages.

Remark II: Using the lemma of consensus in [27] despite of any initial conditions of $x(0)$, it can be concluded that the solution achieved for:

$$\lim_{t\to\infty} v_i^a(t) = V_{dc_{ref}},\ \lim_{t\to\infty} u_i^{Ia}(t) = 0 \quad \forall i \in N \tag{10}$$

with $v_i^a = V_{dc_i}(t) + \int_{j\epsilon M_i} u_i^{Va}(t)$, is feasible and stable. As a result, these attacks are termed as *stealth* attacks owing to identical convergence properties as in (5) even under the presence of attack elements. Hence, detection and mitigation of stealth attacks in a distributed network is an important aspect to prevent the system from further instability or shutdown. A brief overview of the modeling of these attacks in DC microgrids is provided in Table I.

Recently, event-triggered algorithms have been devised for DC microgrids to reduce the communication burden by estimating the desired states locally without use of communication [22]-[23]. However in the presence of external disturbances (categorized as *events*), the gradient projection algorithm used in [22] ensures that each control input remain within the bound by triggering the communication layer. However, stealth cyber attacks can not be detected using the abovementioned event-triggered algorithms since it exhibits zero dynamics without affecting the system states. This has been theoretically verified in the next subsection.

C. Undetectability of Stealth Attacks to Event-Triggered Algorithms [22]

Considering a theoretical state-space model under nominal operating conditions of the entire plant involving both converter and control dynamics in the presence of attacks, the estimated states can be obtained as:

$$\dot{\hat{\mathbf{x}}} = \mathbf{A}\hat{\mathbf{x}} + \mathbf{B}\mathbf{u}^a \tag{11}$$

$$= \mathbf{A}\hat{\mathbf{x}} + \mathbf{B}[\hat{\mathbf{u}} + \mathbf{W}\mathbf{x}_{attack}] \tag{12}$$

where $\hat{\circ}$ denote the estimated projections of the concerned variables. More details regarding the projection of these variables can be referred from [22]. It should be noted that the initial conditions of (11) are acquired using the measured states and inputs. Using the difference between (11) and the actual states, an event-triggered error e_{ev_i} in i^{th} agent ascertains any disturbance from the steady-state operation by activating the communication channels, only when the binary variable ρ_i is triggered using:

$$\rho_i = \begin{cases} 1, \textbf{if } e_{ev_i}(t)(= \hat{x}_i(t) - x_i(t)) \geq \Upsilon \\ 0, \textbf{else} \end{cases} \tag{13}$$

where Υ is an activation threshold. To align the control scheme effectively, a full state feedback is employed to update the inputs with respect to the states using:

$$\hat{\mathbf{u}} = -\mathbf{K}\hat{\mathbf{x}} \tag{14}$$

where $\mathbf{K}$ is the feedback matrix. Substituting (14) in (12), we obtain the actual state-space model without external disturbances since the term $\mathbf{W}\mathbf{x}_{attack}$ exhibits zero dynamics for the modeled attack in (6), as per Remark II. Hence, it can be concluded that stealth attacks can not be detected using event-triggered control mechanisms.

To provide a clear understanding, a case study is carried out in a DC microgrid with N = 4 agents in Fig. 2 to demonstrate that stealth attacks can not be detected using the event-triggered control mechanism for DC microgrids proposed in [22]. Firstly, a balanced set of attack elements {-15, 0, 15, 0} V are injected into the voltage control inputs in Fig. 2 as per the attack model in [14]. After the attack is initiated, it can be seen that the average voltage estimates return back to the global voltage reference of 315 V. At t = 3 sec, an increase in load is introduced to highlight identical dynamics and convergence, which makes it difficult to distinguish between physical disturbances and stealth attack. Further, a stealth attack of 4 A is conducted on the current sensor and outgoing communication links in unit II at t = 5 sec. However, it can be seen in Fig. 2 that the resulting control input made using the attacked sensors and other relevant quantities converge back to zero for stealth attacks. As a result, the event-triggering mechanism which gets activated in both the cases (at t = 1 & 3 sec) does not provide a direct manifestation into the differentation between stealth attacks and other disturbances. By maintaining this discretion, the attacker can launch a critical attack by increasing the magnitude of the injected attack elements, which activates the protective measures and consequently leading to shutdown. As a consequence, this case study necessitates the mitigation of stealth attacks using an authentic resilient mechanism, such that aforementioned risks can be prevented easily.

III. Proposed Event-Driven Resilient Control Strategy

In this section, the detection philosophy alongwith the proposed countermeasures to operate normally during both steady-state and transient conditions in the presence of stealth attacks is discussed in detail.

A. Detection

The detection strategies for both the stealth attacks in Table I, have been provided in Table II. More details on its formulation can be referred from [14] and [15]. Upon detection of attack elements, it is vital to remove these attacks as such unbounded signals in the control system may quickly trigger (8)-(9), ultimately leading to system shutdown. It should be noted that the aforementioned detection criteria will perform satisfactorily, even under the presence of *uncoordinated* attacks. By definition, *uncoordinated* attacks can be defined as a set of attack elements, which do not follow synchronization theory in $\mathbf{W}\mathbf{x}_{attack} \neq 0$. As a consequence, it follows from (6) to conclude that $\mathbf{L}^T\mathbf{u}^a \neq 0$ for *uncoordinated* attacks.

Remark III: Using (13), it can be formalized that the set of detection criterion $DM^i = \{DM_1^i, DM_2^i\}$ in Table II can be defined as *events*, when they start operating outside the detection threshold $\Upsilon = \{\Upsilon_1, \Upsilon_2\}$, respectively.

It is worth notifying that the detection thresholds are infinitesimal values, which are designed to disregard measurement noise to ensure accurate detection. As the detection

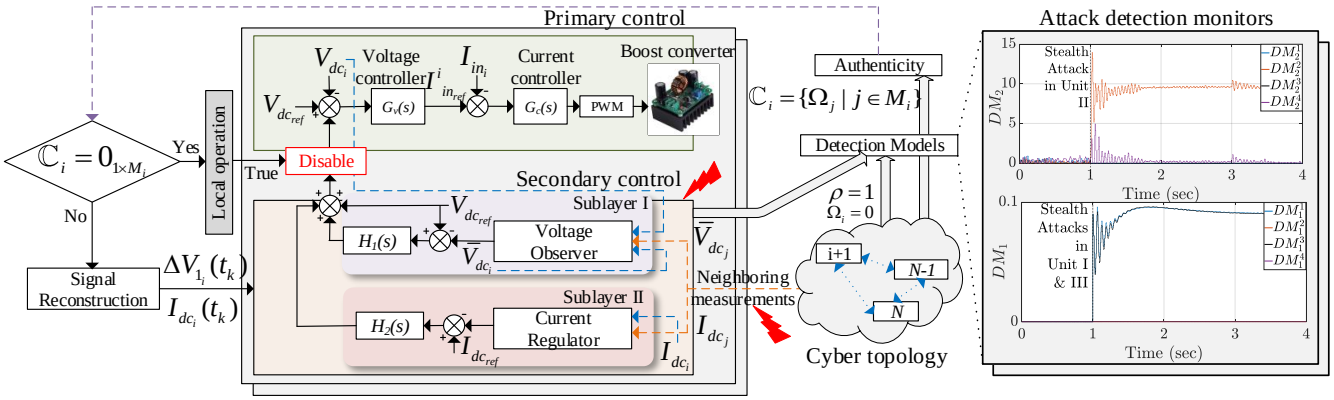

Fig. 3. Proposed event-driven resilient control strategy to mitigate stealth attacks [14], [15] in DC microgrids with N agents.

TABLE II
DETECTION CRITERIA FOR STEALTH ATTACKS IN TABLE I

Stealth Attack	Detection Criteria for i^{th} Agent	Terminology
Voltage [14]	$h_i{}^1[\sum_{j\epsilon M_i} a_{ij}(\Delta V_{1_j} - \Delta V_{1_i})]$ $[\sum_{j\epsilon M_i} a_{ij}(\Delta V_{1_j} + \Delta V_{1_i})] > \Upsilon_1$	DM_1^i
Current [15]	$c_i[\sum_{j\epsilon M_i} a_{ij}(I^j_{in_{ref}} - I^i_{in_{ref}})]$ $[\sum_{j\epsilon M_i} a_{ij}(I^j_{in_{ref}} + I^i_{in_{ref}})] > \Upsilon_2$ [2]	DM_2^i

[1] h_i is a positive quantity used for i^{th} agent.
[2] c_i, $I^i_{in_{ref}}$ denote a positive quantity and the input current reference for i^{th} agent.

TABLE III
TRIGGERING CRITERIA FOR STEALTH ATTACKS IN TABLE I

Stealth Attack	Triggering Criteria for i^{th} Agent	Triggering Function
Voltage [14]	$\mathbf{L}\Delta\mathbf{V}_1^a \leq \Upsilon_1$ [1]	Ξ_1
Current [15]	$\mathbf{L}\Delta\mathbf{I}^a_{in_{ref}} \leq \Upsilon_1$ [2]	Ξ_2

[1] $\Delta\mathbf{V}_1^a$ denote vector representation of ΔV_{1_i} with attack elements.
[2] $\mathbf{I}^a_{in_{ref}}$ denote vector representation of $I^i_{in_{ref}}$ with attack elements.

criterion monitors (as shown in Fig. 3) reveal the compromised section in each agent, an authentication signal Ω_i is generated for the particular counterpart (voltage/current) in i^{th} agent. It should be noted that the nature of authentication signal is binary, such that:

$$\Omega_i = \begin{cases} 0(\mathtt{F}), & \textbf{if } DM^i \leq \Upsilon \\ 1(\mathtt{T}), & \textbf{else} \end{cases} \tag{15}$$

Further, as shown in Fig. 3, a set of authentication signals from the neighboring agents $\mathbb{C}_i = \{\Omega_j | j \in M_i\}$ are also communicated to i^{th} agent. To simplify the representation of authentication for any signal, $\circ^{\mathtt{T}}$ and $\circ^{\mathtt{F}}$ will be used to symbolize `True` and `False` for local/communicated measurements, respectively using (15).

B. Mitigation

As long as the event(s) hold true, the control variables used in designing DM^i are forced to follow the trajectories of non-compromised neighboring signals (with Ω_j labeled as `True`). As highlighted in Fig. 3, if the set of authentication signals in i^{th} agent $\mathbb{C}_i$ is not a zero vector in the presence of attack elements, event-driven resilient signals are reconstructed to mitigate stealth attacks in Table I by using:

$$\Delta V_{1_i}(t_k) = \Xi_1(\Delta V^{\mathtt{T}}_{1_j}(t)) \tag{16}$$

$$I_{dc_i}(t_k) = \Xi_2(I^{\mathtt{T}}_{dc_j}(t)) \tag{17}$$

where, $\circ(t_k)$ (with k as the triggering instant) denote the event-triggered samples of the respective signals generated when the triggering criterion in Table III is activated during stealth attacks. It is worth notifying that $\Xi(\circ)$ in (16)-(17) is a triggering function, which holds the input signal $\circ$ until the next instant of triggering. However, if $\mathbb{C}_i$ is a null vector, this implies that all the communicated measurements 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 highlighted in Fig. 3). Finally,

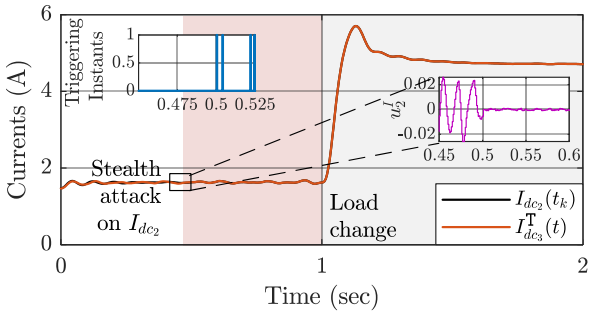

Fig. 4. Peformance of event-driven resilient mechanism for a stealth attack on $I_{dc_2}(t)$ at t = 0.5 sec (in the considered system in Fig. 1 with N = 4 agents) with the resilient signal reconstructed using $I^{\mathtt{T}}_{dc_3}(t)$.

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

$$\Delta V_{1_i}(t) = \Omega_1 \Delta V_{1_i}(t) + (1 - \Omega_i)\Delta V_{1_i}(t_k) \tag{18}$$

$$I_{dc_i}(t) = \Omega_i I_{dc_i}(t) + (1 - \Omega_i) I_{dc_i}(t_k) \tag{19}$$

Finally, the signals obtained in (18) and (19) are substituted into (4) and (1) respectively to realize the mitigation of

stealth attacks in DC microgrids. This philosophy exploits the basic theory of consensus law in (1) where all the participating elements are identical. Further, this philosophy not only mitigates the attacks but allows to operate normally under external disturbances such as load change, communication delay, etc. To prove its robustness in the presence of external disturbances, a case study is carried out for the considered system in Fig. 1 with N = 4 agents following a ring based cyber topology, where a stealth attack is injected into I_{dc_2} at t = 0.5 sec. As soon as the attack is launched, (19) is activated prior to detection of *events* in sublayer II of agent II in Fig. 3. Upon signal reconstruction of event-driven apriori using $I^{\tau}_{dc_3}$, it can be seen in Fig. 4 that the error convergence is held to zero owing to every triggering instants in Table III. Further, its performance aligns perfectly for external disturbances, such as load change at t = 1 sec, thereby obeying (5).

Theorem 1: Apart from mitigating attacks, the proposed event-driven resilient strategy is also robust to operate under both steady-state and dynamic conditions.

To provide a theoretical justification of its performance under any disturbances, a convergence analysis is carried out in the next section.

IV. Convergence Analysis of the Proposed Resilient Strategy

In this section, the convergence analysis of event-driven resilient signals with periodic time-triggered signals will be theoretically verified to establish its performance for worse attack scenarios when all the agents are compromised. It is worth notifying that the resilient approach involves triggering of ΔV_1^i (control input) for stealth voltage attacks and I_{dc_i} (state) for stealth current attacks. As a result, the state-input relationship limits detection capability of the proposed controller for full-scale attacks in the case of voltages and currents. Since control inputs can be redesigned using the states in (14), it is viable to guarantee full scale resiliency in case of stealth voltage attacks, however one *trustworthy* node will always be required to provide resilient operation for stealth current attacks. More details regarding full-scale resilient control systems can be referred from [28].

Considering the sampled measurements using the triggering criterion in Table III as:

$$\hat{\Lambda}_i(k) = \Lambda_i(t_k) \tag{20}$$

for $k \in [t_k, t_{k+1}]$ with $\Lambda_i = \{\Delta V_{1_i}, I_{dc_i}\}$. Define

$$z_i(t_k) = \hat{\Lambda}_i(t_k) - \frac{1}{M_i} \sum_{j \ \epsilon \ M_i} \Lambda_j^{\tau}(t) \ \forall i \in N \tag{21}$$

Let t_k^i, $\forall k$ = 1, 2,... denote the triggering instants in i^{th} agent and also broadcasted to the neighbors $j \in M_i$. Hence, the sampled control input is a piecewise constant function in which $\hat{u}_i(k) = u_i(t_k^{M_i})$ for $k \in [t_k^{M_i}, t_{k+1}^{M_i})$. Given an initial condition $\Lambda(0)$, the iteration from event-triggered algorithm for i^{th} agent will provide:

$$\Lambda_i(k+1) = \Lambda_i(k) + \gamma_i u_i(k) \tag{22}$$

where γ_i denotes the step length. Considering a Lyapunov candidate $V(\Lambda(k))$ = $f(\Lambda(k))$ - $f(\hat{\Lambda}(k))$ for the system in (22). Hence, it is trivial to derive from (21)-(22) that $\Delta V(\Lambda) = \Delta f(\Lambda)$. For all $k \geq 0$, we have

$$\Delta V \leq \sum_{i=1}^{N} \{\gamma_i u_i [\sum_{j \in M_i} (\Lambda_j - \hat{\Lambda}_j) - u_i] + \frac{N}{2} \gamma_i^2 u_i^2\} \tag{23}$$

Using Young's inequality $xy < \frac{x^2}{2\varepsilon}$ + $\frac{\varepsilon y^2}{2}$ with ε denoting an infinitesimal value, we get

$$\Delta V \leq \sum_{i=1}^{N} \{-\gamma_i (1 - \frac{\varepsilon_i}{2} - \frac{N}{2}\gamma_i) u_i^2 + \frac{\gamma_i}{2\varepsilon_i} [\sum_{j \epsilon M_i} (\Lambda_j - \hat{\Lambda}_i)]^2\}. \tag{24}$$

Since there are M_i terms in $\sum_{j \epsilon M_i} (\Lambda_j - \hat{\Lambda}_i)$, and further using the sum of squares inequality, we get

$$[\sum_{j \epsilon M_i} (\Lambda_j - \hat{\Lambda}_i)]^2 \leq |N_i| \sum_{j \epsilon M_i} (\Lambda_j - \hat{\Lambda}_i)^2. \tag{25}$$

Substituting (25) in (24), we get

$$\Delta V \leq \sum_{i=1}^{N} [-\gamma_i (1 - \frac{\varepsilon_i}{2} - \frac{N}{2}\gamma_i) z_1^2 + \frac{\gamma_i |M_i|}{2\varepsilon_i} \sum_{j \epsilon M_i} (\Lambda_j - \hat{\Lambda}_i)^2]. \tag{26}$$

Re-arranging the last term of (26), we get:

$$\Delta V \leq \sum_{i=1}^{N} [-\gamma_i (1 - \frac{\varepsilon_i}{2} - \frac{N}{2}\gamma_i) u_1^2 + \sum_{j=1}^{N} (\Lambda_j - \hat{\Lambda}_i)^2 \sum_{i \in N} \frac{\Gamma_i |M_i|}{2\varepsilon_i}. \tag{27}$$

Since the attack detection event instants in i^{th} agent are determined by

$$u_i^2(k) = \rho_i \hat{u}_i^2(k) \tag{28}$$

$$(\Lambda_j(k) - \hat{\Lambda}_i(k))^2 \leq \frac{\sum_{i \in N} \frac{\rho_i \gamma_i}{M_i} (1 - \frac{\varepsilon_i}{2} - \frac{N}{2}\gamma_i) \hat{u}_i^2}{\sum_{i \in N} \frac{\gamma_i M_i}{2\varepsilon_i}}, \tag{29}$$

adding and subtracting $\sum_{i=1}^{N} \rho_i \gamma_i (1 - \frac{\varepsilon_i}{2} - \frac{N}{2}\gamma_i) \hat{u}_i^2$, we obtain

$$\begin{aligned} \Delta V \leq & -\sum_{i=1}^{N} \gamma_i (1 - \frac{N}{2} - \frac{\varepsilon_i}{2}) (u_i^2 - \rho_i \hat{u}_i^2) \\ & + \sum_{i=1}^{N} [(\Lambda_j - \hat{\Lambda}_i)^2 \sum_{i \in N_j} \frac{\gamma_i |M_i|}{2\varepsilon_i} (1 - \frac{\varepsilon_i}{2} - \frac{N}{2}\gamma_i) \hat{u}_i^2] \end{aligned} \tag{30}$$

Theorem 2: $\Delta V(\Lambda) \leq 0$ is guaranteed for all k using (28)-(30) for any $i \in N$ and $j \in M_i$. The only scenario where ΔV = 0 can happen is when

$$\begin{aligned} u_i = \hat{u}_i = 0 \ \forall i \in N \\ \Lambda_i = \hat{\Lambda}_i = 0 \ \forall j \in M_i. \end{aligned} \tag{31}$$

Theorem 3: Using (31), it has been proved that $\hat{\Lambda}_i(k)$ is asymptotically stable and converges to the periodic time-triggered signals.

V. Simulation Results

The proposed event-driven resilient control strategy is tested on cyber-physical DC microgrid, as shown in Fig. 1 with N= 4 agents for a global reference of 315 V. Each agent of equal power capacities comprising of a DC source and DC/DC buck converter, operate to maintain an output voltage for a local reference $V^i_{dc_{ref}}$ at their respective buses. Firstly, a sensitivity analysis to study the performance of the proposed strategy for different detection thresholds Υ is studied alongwith a study on variation of settling time of the attacked signals. Next, its performance validation for multiple stealth attacks under scenarios such as plugging out of converters, communication delay is carried out to verify the robustness of the event-driven signal reconstrunction based attack mitigation strategy. Moreover, it has been thoroughly verified in case studies that only attacks qualify as *events* to accommodate the resilience of DC microgrids. The simulated plant and control parameters are provided in Appendix.

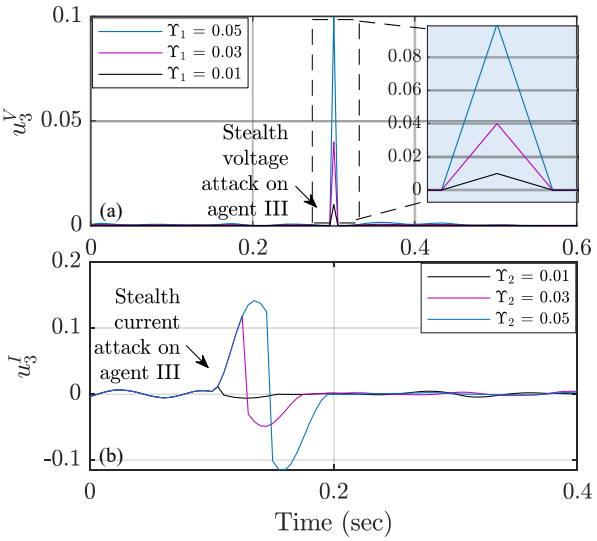

Fig. 5. Sensitivity analysis of the proposed event-driven attack resilient mechanism in the considered system under the presence of stealth: (a) voltage, and (b) current attack on agent III for different values of Υ_1 and Υ_2 respectively.

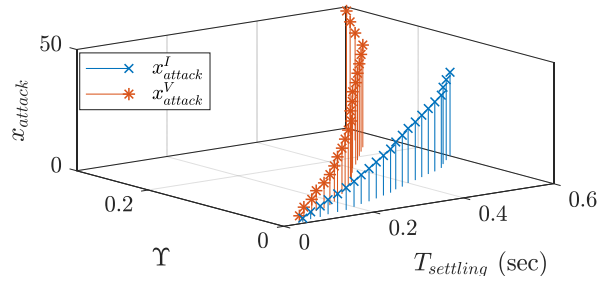

Fig. 6. Variation of settling time $T_{settling}$ of the control input signals u^a in the considered system for different magnitude of attack elements x_{attack} and respective triggering thresholds Υ.

A sensitivity analysis is carried out for the considered system to inspect the detection capability of the proposed strategy in Fig. 5 for different values of Υ. A stealth voltage attack is performed at t = 0.3 sec on agent III, as shown in Fig. 5(a). As soon as the attack is launched, it can be seen that with increase in the value of Υ_1, the transient peak and the settling time to the optimal setpoint keeps increasing. A similar performance can be observed for stealth current attack for different values of Υ_2 in Fig. 5(b). Moreover, to provide resiliency against input and acquisition noise, Υ can be adjudged as small as possible, yet sufficiently larger than the measurement noise to avoid unnecessary triggering. Hence,

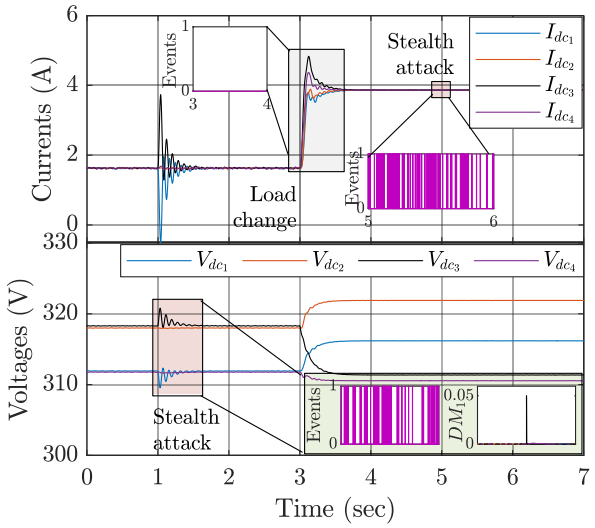

Fig. 7. Performance of the proposed event-driven attack resilient controller in the presence of stealth voltage and current attacks in Fig. 2 – It only detects attacks as *events* and mitigates it using the triggering criteria immediately.

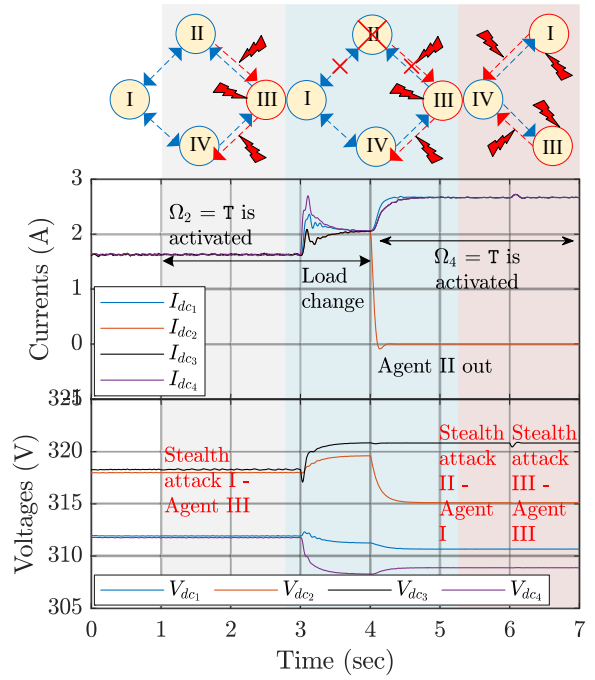

Fig. 8. Performance of the proposed event-driven attack resilient controller in the presence of stealth voltage and current attacks in multiple agents with agent II plugged out at t = 4 sec – resiliency is always achieved with authentication signal for agent III immediately switched from Ω_2 to Ω_4 when agent II is plugged out.

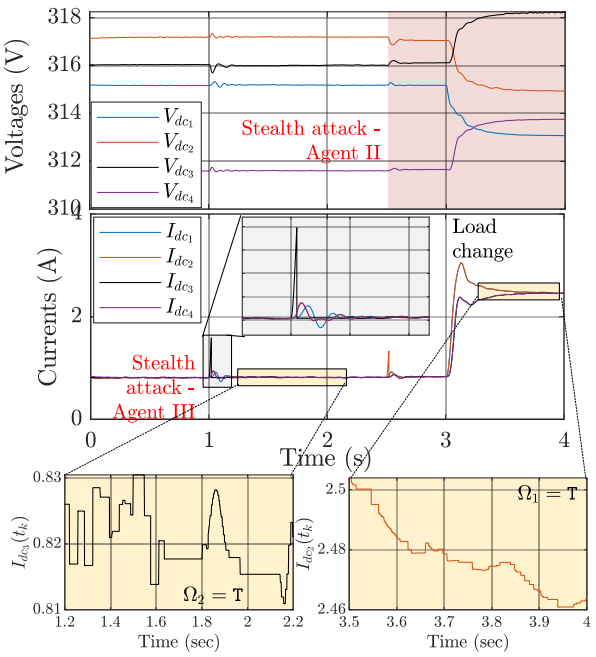

Fig. 9. Performance of the proposed event-driven attack resilient controller in the presence of multiple stealth current attacks on agent II and III at t = 1 and 2.5 sec under a maximum communication delay of 125 ms – the settling time increases due to delayed authentication updates from neighbors.

the design of Υ is a deterministic task for each system, which highly affects factors such as accuracy and dynamic response. To simplify this task, the variance of noise in the measurements for a given system can be used as a good indicator to decide the minimum value of Υ in advance.

To encompass the relationship between triggering thresholds for different magnitude of attack elements and its physical impact, a case study is carried out in Fig. 6 to variation of settling time $T_{settling}$ of the attacked control inputs. It can be seen that with increase in the magnitude of x_{attack} and Υ, $T_{settling}$ follows an increasing trend for both voltage and current attacks. It should be noted that the consideration of x_{attack} in Fig. 6 is limited to the respective upper and lower limits in (8)-(9). Moreover, better noise filtering capabilities of secondary sublayer II allows a lower value of Υ_2 as compared to Υ_1 to design the proposed event-driven resilient strategy.

Next, the performance of the event-driven resilient controller is compared to the case study for conventional event-triggering method (studied in Fig. 3) in Fig. 7. As it can be seen in Fig. 7, the stealth voltage attack is successfully determined as *event* at t = 1 sec, which triggers the signal reconstruction of $\Delta V_{1_1}(t_k)$ and $\Delta V_{1_3}(t_k)$, such that the triggered DM_1 remains within the detection threshold. However for an increase in load at t = 3 sec, the proposed controller do not detect any events; which justify its robustness to differentiate between physical disturbances and cyber attacks. Further at t = 5 sec, a stealth current attack is launched on agent II, which led to increase in current from each agent, as studied previously in Fig. 2. However, the proposed resilient controller ensures that the currents from each agents continue to operate at the same loading level as $I_{dc_2}(t_k)$ is reconstructed to follow consensus using the proposed mitigation strategy.

In the next case study, the performance of the proposed resilient controller is tested for instances when the authentication signal is switched from one agent to another. It can be seen in Fig. 8 that a stealth curent attack is conducted on agent III at t = 1 sec, which triggers the mitigation philosophy as $\mathbb{C}_3$ is not a null vector. This implies that all the neighbors of agent III are transmitting `True` measurements. It is worth notifying that the selection of authentication signal from the set $\mathbb{C}_i$ is not governed by any priority labels. Using this hypothesis, agent II signals with authenticity labeled as $\Omega_2 = \mathtt{T}$ is activated immediately for signal reconstruction of $I_{dc_3}(t_k)$. Following up to monitor its performance to regard consensus during external disturbances, it can be seen in Fig. 8 that the event-driven resilient signal $I_{dc_3}(t_k)$ still follows proportionate current sharing. However when agent II is plugged out at t = 4 sec, the outgoing communication links are disabled which restricts the transmission of signals to any of its neighbors. Consequently, agent III immediately switches from Ω_2 to Ω_4 for reconstruction of $I_{dc_3}(t_k)$ such that the remaining active agents share the load current equally. Moreover, when stealth current attack II and III of magnitude 6 and 24 A is launched on agent I and III at t = 5 and 6 sec respectively, it can be seen that the sharing accuracy and consensus between agents is unlatered despite the magnitude of attack.

In the final case study, the performance of the proposed resilient controller is tested for multiple stealth current attacks under a maximum network communication delay of 125 ms in Fig. 9. At first, when a stealth current attack is launched on agent III at t = 1 sec; the attacked signal causes a momentary increase with the transient being eliminated as the authentication signal $\Omega_2 = \mathtt{T}$ is reached after a delay of 125 ms to update the event-driven signal $I_{dc_3}(t_k)$ using (19). As this hypothesis is well-studied previously, the settling time intuitatively increases to 0.1 sec for a value of Υ_2 = 0.01. Further at t = 2.5 sec, a stealth current attack is launched on agent II which creates a momentary increase and settles down as the resilient update of $I_{dc_2}(t_k)$ is received after a delay of 125 ms using $\Omega_1 = \mathtt{T}$. The robustness of the proposed controller can be ensured via a load change at t = 3 sec, when the currents from each agent are proportionately shared. Further, the discretized values from every triggering instant is zoomed in to show the trajectory which they follow during steady-state and dynamic conditions. Hence, the proposed event-driven resilient scheme is not limited to mitigating attacks for steady-state operation of converter(s), but is also flexible to operate for dynamic conditions such as load changes.

VI. Experimental Results

The proposed detection strategy has been experimentally validated in a DC microgrid operating at a voltage reference $V_{dc_{ref}}$ of 48 V with N = 2 buck converters, as shown in Fig. 10. A single line diagram of the experimental setup is also shown in Fig. 11. Both the converters are tied radially to a programmable load (voltage-dependent mode). Each converter is controlled by dSPACE MicroLabBox DS1202 (target), with control commands from the ControlDesk from the PC (host).

Using the local and neighboring measurements, the proposed event-driven resilient strategy shown in Fig. 3 is modeled for every converter to mitigate the attacks and meet the control objectives in (5). The experimental testbed parameters are provided in Appendix.

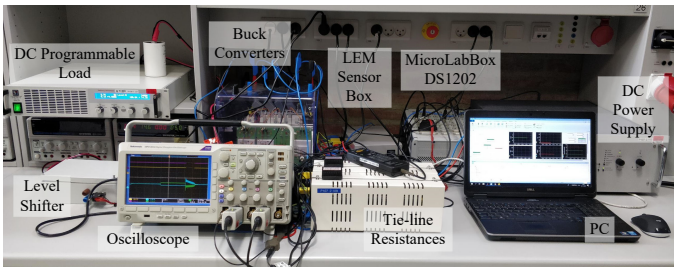

Fig. 10. Experimental setup of a cooperative DC microgrid comprising of N = 2 agents controlled by dSPACE MicroLabBox DS1202 supplying power to the programmable load.

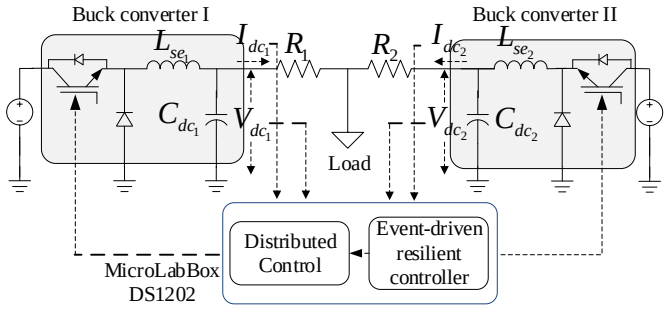

Fig. 11. Single line diagram of the experimental setup shown in Fig. 10.

In Fig. 12(a), stealth voltage attacks is launched by injecting attack elements of $\pm$ 8 V on both agents. As a result, the secondary sublayer I output is displaced by equal quantities thereby activating the mitigation criteria to trigger these outputs to zero. Even though both the agents are attacked, since the detection rule is local DM_1 goes positive, which will essentially trigger the respective mitigation criteria. As a result, it can be seen in Fig. 12(a) that as soon as the attack is launched, the currents and voltages return back to the pre-attack instant values following a transient. A zoomed picture is also highlighted to establish that consensus is achieved between the states. Further in Fig. 12(b), two stealth current attacks on agent I is carried out with $x^I_{attack_1}$ = 4 and 24 A (highlighted as event **A** and **B** respectively in Fig. 12) are launched. It can be seen in Fig. 12(b) that as soon as the attack is launched, the authentication signal from both agents is cross-verified as soon as the detection criteria suggests the presence of an attack. Since Ω_2 = `T` in this case, the reconstructed resilient signal $I_{dc_1}(t_k)$ is designed such that consensus holds true. Intuitively, the settling time and peak value of the transients prior to the attack in Fig. 12(b) increases with the magnitude of attack element. Finally in Fig. 12(c), when stealth current attack is launched on both the agents at the same time, since the detection philosophy is dependent on transmitted sensor measurements, the authentication signals from both converters will traverse to `F`. As a result, the

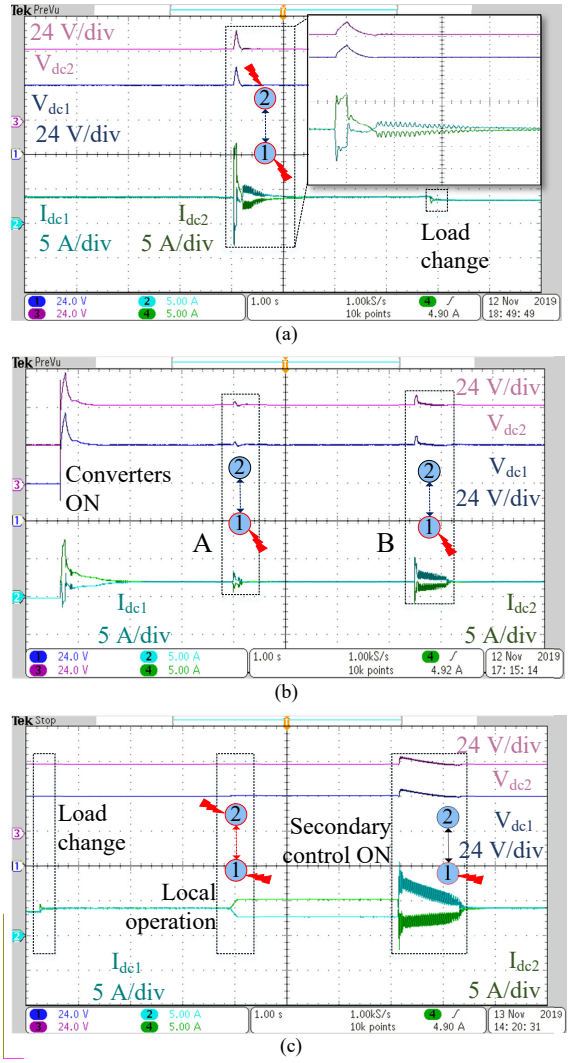

Fig. 12. Experimental validation of the proposed resilient controller for : (a) stealth voltage attack on all agents, (b) two stealth current attacks on agent I (During events **A** and **B**, $x^I_{attack_1}$ = 4 and 24 A is injected into agent I), (c) stealth current attacks on agent I and II simultaneously.

system immediately runs into local operation as described in Fig. 3. Finally, when the attack element in agent II is removed, it can be seen that the system returns back to the normal operating condition following consensus theory using the proposed event-driven mitigation strategy. Hence, this validates the effectiveness of the performance of proposed resilient controller to full scale attacks for voltages and $(N-1)$ scale attacks for currents (at least one *trusted* agent will always be required to broadcast `True` signals).

VII. Discussion

The core idea of the proposed resilience mechanism is to substitute the compromised signal with an event-driven resilient signal constructed using *trustworthy* measurements from neighbors. The robustness of its operation has been tested for many scenarios, which has been tabulated in Table IV.

In Table IV, it can be seen that the proposed event-driven resilient scheme is also robust to other anomlaies such as line-to-line faults and sensor faults, where the dynamic response are

TABLE IV
EFFECTIVENESS OF EVENT-DRIVEN RESILIENT STRATEGY

Disturbances	Performance
Load change/line outage	✓
Stealth attack on voltages & currents	✓
Attack under max. communication delay	✓
Sensor fault	$DM^i < \Upsilon$[1]
Converter outage under attack	✓
Line-to-line fault	$DM^i < \Upsilon$[2]

[1] A fault detection metric FD_I^i is proposed in [16] to differentiate between current sensor faults and cyber attacks.
[2] A line-to-line fault evaluation theory is proposed in [15] to differentiate between line faults and cyber attacks.

quite identical to cyber attacks. However, since the detection criteria DM^i doesn't exceed the detection threshold Υ for these disturbances, the event-driven mitigation process will not be activated. More details on detection of line-to-line and sensor faults and their differentiation with cyber attacks have been provided in [15] and [16], respectively. Finally, the main features of the proposed event-driven resilient scheme are:

1) It ensures $N-1$ and full scale of resilience for stealth attacks on currents and voltages, respectively.
2) It has no model-intensive requirements and scalable to N units.
3) It provides flexibility to maintain resilience against cyber attacks without disabling any cyber links.

VIII. CONCLUSIONS

This paper has presented an event-driven resilient control scheme to detect two categories of stealth attacks, i.e. on voltage and current measurements in cyber-physical DC microgrids. Since such attacks can impose risk on critical infrastructure, it is vital to remove these attacks in a timely manner in power electronics intensive systems. Adopting a new philosophy by emphasizing cyber attacks as *events*, this paper detects the attacks locally and transmit the authentication signal (Ω_i = T/F) of measurements to the neighboring measurements. As a result, the rest of the agents re-orient their operation and assist the attacked agent to reconstruct an event-driven signal using their autheticated measurements. Since the basic philosophy of consensus theory complies with *identical* arrangements, this concept has been exploited to design the proposed controller. Theoretical analysis and simulations under different instances are carried out to establish that the proposed controller is robust to many physical disturbances and provides a good manifestation to trigger only during cyber attacks. Moreover, the full-scale resiliency is widely discussed and the prophecies are validated in the experimental prototype. This strategy is also applicable for *uncoordinated* attacks and will be highly applicable for mission-critical application such as naval ships and electric aircrafts where security is a prime concern. As a future scope of work, this philosophy will be extended for heterogeneous system dynamics, wherein the system objectives will be different for grid-forming and grid-following applications of microgrids. Further studies will be conducted on the proposed scheme to extend the scope of resiliency against cyber attacks in AC microgrids. Moreover, further focus on exchange of authenticity signatures needs to be studied in detail with the possibility of a man-in-the-middle (MITM) attack.

APPENDIX

Simulation Parameters

The considered system consists of four sources rated equally for 6 kW. It is to be noted that the line parameter R_{ij} is connected from i^{th} agent to j^{th} agent. Moreover, the controller gains are identical for each agent.
Plant: R_{12} = 1.8 Ω, R_{14} = 1.3 Ω, R_{23} = 2.3 Ω, R_{43} = 2.1 Ω
Converter: L_{se_i}= 3 mH, C_{dc_i}= 250 μF, $I_{dc_{min}}$ = 0 A, $I_{dc_{max}}$ = 18 A, $V_{dc_{min}}$ = 270 V, $V_{dc_{max}}$ = 360 V.
Controller: $V_{dc_{ref}}$= 315 V, $I_{dc_{ref}}$ = 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, V_{in} = 270 V, h = 1.2, c = 2.1, Υ_1 = 0.02, Υ_2 = 0.015.

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.
Plant: R_1 = 0.9 Ω, R_2 = 1.2 Ω
Converter: L_{se_i}= 3 mH, C_{dc_i}= 100 μF
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, g = 0.64, h = 1.5, c = 1.4, Υ_1 = 0.025, Υ_2 = 0.035.

REFERENCES

[1] T. Dragicevic, X. Lu, J.C. Vasquez, J.M. Guerrero, "DC microgrids–Part I: A review of control strategies and stabilization techniques", *IEEE Trans. on Power Elect.*, vol. 31, no. 7, pp. 4876-4891, 2016.
[2] M. Yazdanian and A. Mehrizi-Sani, "Distributed Control Techniques in Microgrids," *IEEE Trans. on Smart Grid*, vol. 5, no. 6, pp. 2901–2909, 2014.
[3] S. Sahoo and S. Mishra, "A Distributed Finite-Time Secondary Average Voltage Regulation and Current Sharing Controller for DC Microgrids", *IEEE Trans. on Smart Grid*, vol. 10, no. 1, pp. 282-292, Jan 2019.
[4] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, "Microgrid cyber security reference architecture," *Sandia Nat. Lab.(Hierarch. SNLNM), Albuquerque, NM, USA, Tech. Rep. SAND2013-5472*, 2013.
[5] T. Dragicevic, X. Lu, J.C. Vasquez, J.M. Guerrero, "DC microgrids–Part II: A review of power architectures, applications, and standardization issues", *IEEE Trans. on Power Elect.*, vol. 31, no. 5, pp. 3528-3549, 2016.
[6] S. Sahoo, T. Dragicevic and F. Blaabjerg, "Cyber Security in Control of Grid-Tied Power Electronic Converters–Challenges and Vulnerabilities", *IEEE Journ. Emerg. and Select. Topics Power Electron.*, 2019.
[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. on Inf. Syst. Security*, vol. 14, no. 1, p. 13, 2011.
[8] P. Danzi, M. Angjelichinoski, C. Stefanovic, T. Dragicevic, and P. Popovski, "Software-Defined Microgrid Control for Resilience Against Denial-of-Service Attacks" *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5258-5268, 2019.
[9] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. on Autom. Control*, vol. 58, no. 11, pp. 2715–2729, 2013.
[10] P. Danzi, C. Stefanovic, L. Meng, J.M. Guerrero, and P. Popovski, "On the impact of wireless jamming on the distributed secondary microgrid control", *2016 IEEE GlobeCom Workshop*, Washington DC, 2016.
[11] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630-1638, 2016.

[12] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid", *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847-855, 2013.
[13] K. Sun, I. Esnaola, S.M. Perlaza, and H.V. Poor, "Stealth Attacks on the Smart Grid" *arXiv preprint arXiv:1808.04184*, 2018.
[14] S. Sahoo, S. Mishra, J.C.H. Peng, and T. Dragicevic, "A Stealth Attack Detection Strategy for DC Microgrids", *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162-8174, 2019.
[15] S. Sahoo, J.C.H. Peng, A. Devakumar, S. Mishra, and T. Dragicevic, "On Detection of False Data in Cooperative DC Microgrids–A Discordant Element Approach", *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6562-6571, 2019.
[16] S. Sahoo, J. C. -H. Peng, S. Mishra, and T. Dragicevic, "Distributed Screening of Hijacking Attacks in DC Microgrids", *IEEE Trans. Power Electron.*, vol. 35, no. 7, pp. 7574-7582, 2019.
[17] S. Sundaram, and C.N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Automatic Contr.*, vol. 56, no. 7, pp. 1495-1508, 2011.
[18] O. 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, 2019.
[19] 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.
[20] S. Sundaram, and B. Gharesifard, "Consensus-based distributed optimization with malicious nodes," *In Proceedings of Conference on Communication, Control, and Computing (Allerton)*, pp. 244-249, 2015.
[21] 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.
[22] S. Sahoo and S. Mishra, "An Adaptive Event-Triggered Communication Based Distributed Secondary Control for DC Microgrids", *IEEE Trans. on Smart Grid*, vol. 9, no. 6, pp. 6674-6683, Nov. 2018.
[23] L.G. Moreira, L.B. Groff, J.M.G. da Silva, "Event-triggered state-feedback control for continuous-time plants subject to input saturation", *Journ. Control, Autom. and Electr. Sys.*, vol. 27, no. 5, pp. 473-484, Oct. 2016.
[24] S. Sahoo and J. C. -H. Peng, "A Localized Event Driven Resilient Mechanism for Cooperative Microgrid Against Data Integrity Attacks", *IEEE Trans. Cybern.*, 2020.
[25] S. Sahoo, T. Dragicevic and F. Blaabjerg, "Resilient Operation of Heterogeneous Sources in Cooperative DC Microgrids", *IEEE Trans. Power Electron.*, 2020.
[26] V. Nasirian, S. Moayedi, A Davoudi and F. L. Lewis, "Distributed Cooperative Control of DC Microgrids," *IEEE Trans. on Power Elect.*, vol. 30, no. 4, pp. 2288–2303, 2015.
[27] M. Zhu, and S. Martinez, "Discrete-time dynamic average consensus", *Automatica*, vol. 46, no. 2, pp. 322-329, 2010.
[28] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems." *IEEE Control Systems*, vol. 35, no. 1, pp. 110-127, 2015.

Subham Sahoo (S'16-M'18) 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 and as a postdoctoral researcher in the Department of Electrical and Computer Engineering in National University of Singapore in 2018-2019. He is currently working as a research fellow in the Department of Energy Technology, Aalborg University, Denmark.

He is a recipient of the Innovative Students Projects Award for Doctoral level by Indian National Academy of Engineering (INAE) for the year 2019. His current research interests include control and stability of microgrids, cyber security in power electronic systems.

Tomislav Dragičević (S'09-M'13-SM'17) received the M.Sc. and the industrial Ph.D. degrees in Electrical Engineering from the Faculty of Electrical Engineering, Zagreb, Croatia, in 2009 and 2013, respectively. From 2013 until 2016 he has been a Postdoctoral research associate at Aalborg University, Denmark. From 2016 until 2020, he was an Associate Professor at Aalborg University, Denmark. From 2020, he is a professor at the Technical University of Denmark.

He made a guest professor stay at Nottingham University, UK during spring/summer of 2018. His principal field of interest is design and control of microgrids, and application of advanced modeling and control concepts to power electronic systems. He has authored and co-authored more than 200 technical papers (more than 100 of them are published in international journals, mostly in IEEE), 8 book chapters and a book in the field.

He serves as Associate Editor in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, in IEEE TRANSACTIONS ON POWER ELECTRONICS, in IEEE Journal of Emerging and Selected Topics in Power Electronics and in IEEE Industrial Electronics Magazine. Dr. Dragičević is a recipient of the Končar prize for the best industrial PhD thesis in Croatia, and a Robert Mayer Energy Conservation award. He is a winner of Alexander van Humboldt fellowship for experienced researchers.

Frede Blaabjerg (S'86-M'88-SM'97-F'03) was with ABB-Scandia, Randers, Denmark, from 1987 to 1988. From 1988 to 1992, he got the PhD 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 Prize in 2019 and the IEEE Edison Medal in 2020. He was the Editor-in-Chief of the IEEE TRANSACTIONS ON POWER ELECTRONICS from 2006 to 2012. He has been 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 serves a President of IEEE Power Electronics Society. He is Vice-President of the Danish Academy of Technical Sciences too. He is nominated in 2014-2018 by Thomson Reuters to be between the most 250 cited researchers in Engineering in the world.