# Signal Temporal Logic-based Attack Detection in DC Microgrids

Omar Ali Beg, *Member, IEEE,* Luan Nguyen, *Student Member, IEEE,* Taylor T. Johnson, *Member, IEEE,* and Ali Davoudi, *Senior Member, IEEE*

***Abstract*—Emerging converter-dominated DC microgrids employ distributed cooperative control strategies and communication network. Since there is no central entity to monitor and assess the global cyber scenario, microgrids employing distributed control are prone to cyber attacks. This work presents signal temporal logic (STL) detection of two major types of cyber attacks, namely false-data injection attacks (FDIA) and denial-of-service (DoS) attacks. Such cyber attacks can compromise voltage regulation and load sharing in DC microgrids. STL is a formalism to monitor the output voltages and currents of DC microgrids against the defined specifications, such as operational bounds, over time. Besides detection, the proposed approach also quantifies the attack impact. Moreover, it can be effectively employed for a complex DC microgrid without prior knowledge of its dynamics. This detection technique is successfully demonstrated using a physical microgrid setup or in a hardware-in-the-loop environment, where various attacks are formalized, detected, and quantified.**

***Index Terms*—DC microgrid, denial-of-service attack, distributed control, false-data injection attack, signal-temporal logic.**

## I. Introduction

DC microgrids have emerged as an alternative to their AC counterparts offering more efficiency, reliability, and compatibility with DC-native renewable resources (e.g., photovoltaics), storage units (e.g., batteries), and loads (e.g., vehicle charging stations, lighting, and electronic loads) [1]. Owing to complex interactions between the physical layer (composed of converters, loads, and power distribution network) and the cyber layer (software-based controllers and communication network), such microgrids have transformed into cyber-physical systems. Distributed multi-agent control of DC microgrids has appeared as a scalable and secure alternative to the legacy central control architecture that had required a complex and fully-connected communication network and had exposed a single point-of-failure [2]–[4].

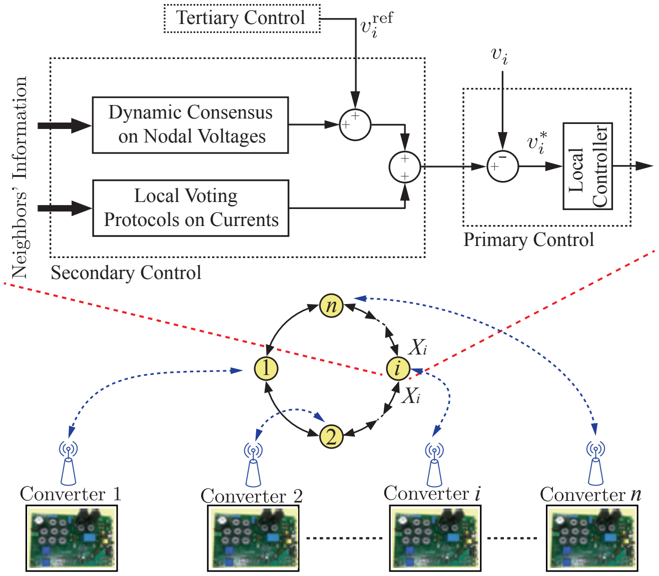


Fig. 1. Overview of the distributed cooperative control scheme in a DC microgrid showing the physical converters, data sharing among converters, and the controller block diagram for the $i$th converter.

The control hierarchy for microgrids has three layers: primary, secondary, and tertiary [5]. In this work, the secondary control is based on distributed cooperative control scheme [2], [6], shown in Fig. Fig. 1, such that the control signal for a given converter depends on the information it exchanges with other converters neighboring it on the communication graph. For example, the vector $X_i$ in Fig. 1 represents the information transferred by the $i^{th}$ converter to $(i+1)^{th}$ and $(i-1)^{th}$ neighbor converters. This ensures that all the converters reach consensus on quantities of interest. This secondary control scheme achieves two objectives: proportional load sharing among DC-DC converters, depending upon their respective power ratings, and global voltage regulation over the distribution bus. These objectives are acheived by assigning a proper voltage set point, $v_i^*$, to the local controller for each individual converter. This is implemented through augmenting the local voltage, $v_i$, with current and voltage regulator modules as shown in Fig. 1. The current regulator shares the overall load among converters depending upon their power ratings such that no single converter is overloaded. The voltage regulator requires that the average voltage across the entire DC microgrid is adjusted to the global voltage reference, $v_i^{ref}$, set forth at the tertiary control.

This distributed cooperative control framework is vulnerable to cyber attacks, as it relies on local sensing of current/-

Work of Omar A. Beg and Ali Davoudi was supported by the Department of Defense under grant number W91NF-16-1-0534, the National Science Foundation (NSF) under Grant ECCS-1405173, Office of Naval Research (ONR) under Grant N00014-17-1-2239, and Defense University Research Instrumentation Program under Grant N00014-16-1-3180. Work of Taylor T. Johnson and Luan Nguyen was supported by NSF under grant numbers CNS 1464311 and SHF 1527398, the Air Force Research Laboratory through contract numbers FA8750-15-1-0105, and FA8650-12-3-7255 via subcontract number WBSC 7255 SOI VU 0001, and the Air Force Office of Scientific Research under contract numbers FA9550-15-1-0258 and FA9550-16-1-0246.

Omar A. Beg, Luan Nguyen, and A. Davoudi are with the University of Texas, Arlington, TX 76019, USA (e-mail: omar.beg@mavs.uta.edu; luanvnguyen@mavs.uta.edu; davoudi@uta.edu).

Taylor T. Johnson is with Vanderbilt University, Nashville, TN 37240, USA (e-mail: taylor.johnson@vanderbilt.edu).

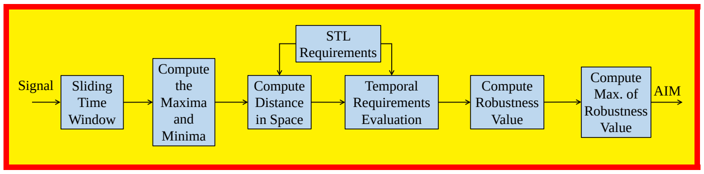

Signal
Sliding Time Window
Compute the Maxima and Minima
STL Requirements
Compute Distance in Space
Temporal Requirements Evaluation
Compute Robustness Value
Compute Max. of Robustness Value
AIM

Fig. 2. STL-based attack detection provides the robustness value that quantifies the extent by which a given signal violates/meets a given STL requirement. The maximum of the robustness value over the trace gives us the impact measure.

voltage variables and a communication network to exchange local variables, and there is no central entity to monitor the overall cyber scenario. Indepedent of a network setting used, there still could be vulnerability to cyber attacks, e.g., via remote access points meant for maintenance purposes [7], computerized communication protocols [8], measured data being exchanged among different nodes [9], and sensors' measurements [10]. The attacker could exploit such vulnerabilities, hack into the communication network, and initiate false-data injection attacks (FDIA), jamming, or denial-of-service (DoS) attacks. While the vulnerability of the legacy power systems with respect to various cyber attack scenarios has recently been studied, e.g., DoS attacks [11], FDIA [12], random attacks [10], and jamming attacks [13], extending such frameworks to power electronic-intensive DC microgrids is not a trivial task.

Two main types of cyber attacks, i.e., FDIA and DoS, are considered here. The adversary may initiate an FDIA by spoofing a signal, either in the sensors or the communication network [14]. DoS is directed against the communication network, and either floods it with data packets, or compromises specific devices to disrupt the data transfer [15]. FDIA detection in power systems broadly employs state estimation techniques [12], [16]–[18]. DoS attack is comparatively easier to deploy and has serious implications [15], with recent remedies in the literature [11], [19]. Such detection techniques merely indicate the presence of an attack, but do not quantify their impacts for a more comprehensive image of the prevailing threats. Moreover, most techniques require a detailed knowledge of the system under consideration. Finally, to the best of the authors' knowledge, detection of FDIA and DoS attacks is to be systematically studied in the context of converter-dominated DC microgrids.

This work presents a *signal-temporal logic* (STL) based cyber-attack detection technique for DC microgrids that also provides such a quantitative measure, called *attack impact measure* (AIM). STL is defined over the valuation of a given signal [20], [21]. Using this formalism, one can evaluate output voltage or load currents of the DC microgrid, and ascertain how closely they meet given requirements, i.e., whether the DC microgrid output remains bounded over time, and the extent to which it violates the bounds. Since the technique requires only the output signals of the DC microgrid, it is model-free, and can be used for complex DC microgrids. A flow diagram of the STL-based detection technique is shown in Fig. 2. For a given signal, the maxima and minima are computed over a sliding time window, which is followed by computing the distance in space and evaluating the temporal requirements for a given STL formula. In the later stages, the *robustness value* for the signal is computed that quantifies the extent by which the signal violates/meets the STL requirement. In the last step, the AIM value is achieved by computing the maximum of the robustness value.

This work is then extended to FDIA mitigation analysis using *hyperproperties* [22]. A hyperproperty is evaluated over two given traces in contrast to the STL formalism that verifies a signal for a given requirement. A *trace* is defined as a set of two or more signals. We extend the idea of hyperproperties to DC microgrids, formally define the relationships among multiple traces, and analyze candidate mitigation strategies. In summary, the main contributions of this paper are as follows.

1. An STL-based technique is customized to DC microgrids that not only detects FDIA and DoS attacks but also quantifies their impact.
2. We extend the idea of hyperproperties to DC microgrids to help identify the best candidate mitigation strategy to thwart a cyber attack.
3. We demonstrate that such a technique can also detect and quantify the impact of anomalies such as short-circuit faults.
4. Validation and verification of STL-based technique on cyber-physical microgrid hardware and hardware-in-the-loop (HIL) systems are achieved.

The remainder of this paper is organized as follows: STL with formal syntax and semantics is discussed in the context of cyber-physical DC microgrids in Section II. The STL-based detection technique is presented in Section III. In Section IV, various types of cyber attacks, namely, constrained FDIA, unconstrained FDIA, and DoS attacks, are implemented, detected, and quantified. Section V concludes the paper.

## II. Signal Temporal Logic

This work detects cyber attacks in DC microgrids by verifying given STL requirements. A *requirement* is a formally defined specification for the acceptable microgrid outputs in response to the inputs. Requirements can be classified into the *safety* requirements, asserting that nothing bad ever happens, and *liveness* requirements, asserting that something good eventually happens [23]. The terms *eventually* and *ever* relate to the time (hence, the temporal aspect of STL). Attack detection relates to the safety requirement as it requires monitoring of the microgrid over time. The next step would require appropriate mitigation actions and monitoring remedial effects, which relates to the liveness requirements. A practical approach is to formalize these safety and liveness requirements in the form of STL, and monitor the behavior (i.e., output voltage and current signals) of DC microgrids, over time, in comparison with these requirements.

The underlying STL concepts are illustrated using an example of a single hysteresis-controlled Buck converter with its output voltage shown in Fig. 3. The switching action depends on a hysteresis band that is formed by an upper boundary, $v_{ref} + \delta$, and a lower boundary, $v_{ref} - \delta$, where $v_{ref}$ is the desired output voltage, and $\delta$ is the tolerance level. Let $\mathbb{R}_{\geq 0} = \{a \in \mathbb{R} \mid a \geq 0\}$ be the set of non-negative real numbers, where $\mathbb{R}$ is the set of real numbers. The real-valued output voltage and current measured over time are considered as *signals*, whereas a collection of various signals forms a *trace*, e.g., if $v_{out}(t)$ and $i_{out}(t)$ are two signals measured over $t \in \mathbb{R}_{\geq 0}$, then $\theta(t) = \{v_{out}(t), i_{out}(t)\}$ is the corresponding trace. For simplicity, we omit $t$ in parenthesis throughout this paper. Intuitively, $\theta$ defines the *behavior* of the system over time. STL formulas are based on the predicates defined for signals, such that a *signal predicate* $\phi$ is a set of constraints over real-valued signals. It is written as $\phi = y(\theta(t)) \bowtie \eta$, where $y$ is a real-valued function over $\theta$, $\bowtie \in \{>, \geq, =, <, \leq\}$, and $\eta \in \mathbb{R}$. As an example, $v_{out} < 65\ V$ is a predicate for the output voltage of the hysteresis-controlled Buck converter in Fig. 3. Temporal operators form the pertinent components in STL formulas that include *always*, *eventually*, and *until*, denoted as $\mathcal{G}, \mathcal{F}$, and $\mathcal{U}$, respectively:

1. Always: This operator requires that a given requirement $\phi$ has to be true for *every* signal valuation. For example, let $\phi_1 : \mathcal{G}\ v_{out} < 65\ V$ (i.e., it is always the case that $v_{out} < 65\ V$), and it is evident that $\phi_1$ is satisfied in Fig. 3 for the output voltage.
2. Eventually: This operator requires a given requirement $\phi$ to be true for *some* signal valuation. Let $\phi_2 : v_{out} = 63.4\ V$, and it is evident that $\mathcal{F}\phi_2$ is satisfied in Fig. 3 at about $0.005\ s$.
3. Until: This operator takes two requirements (e.g., $\phi_3$ and $\phi_4$) as arguments. This operator requires that $\phi_3$ is satisfied in every valuation in the signal *until* a valuation is encountered that satisfies $\phi_4$.

STL can be defined in terms of its *syntax* and *semantics*. Syntax describes the structure of syntactically-correct formulas for the logic, while semantics describe the meaning of the formulas and the rules to evaluate them. The syntax of STL is defined as

$$\varphi := \top \mid \phi \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1\ \mathcal{U}_\tau\ \varphi_2\ , \tag{1}$$

where $\top$ denotes Boolean constant *true*, and $\neg$ and $\wedge$ are the Boolean negation and conjunction operations, respectively. $\mathcal{U}$ is the *until* temporal operator, and $\tau$ is an interval over $\mathbb{R}_{\geq 0}$. For a given signal $\sigma$, the STL syntax defined in (1) is explicitly explained as:

1. If $\phi$ is a predicate over $\sigma$, then $\phi$ is an STL formula. In the example of Fig. 3, the STL formula $\phi_v$ for the output voltage $v_{out}$ could be written as $\phi_v = \mathcal{G}\ v_{out} < 70\ V$.
2. A given STL formula $\varphi$ could be evaluated as true or false. Considering the example stated above, $\phi_v$ is true.
3. If $\varphi$ is an STL formula, so is $\neg\varphi$. For example, if $\varphi_v = \mathcal{G}\ v_{out} < 70\ V$, then the negation of $\varphi_v$ could be formally written as $\neg(\mathcal{G}\ v_{out} < 70\ V)$, which is also an STL formula as per definition in (1).
4. If $\varphi_1$ and $\varphi_2$ are STL formulas, so are $\varphi_1 \wedge \varphi_2$ and $\varphi_1\ \mathcal{U}_\tau\ \varphi_2$. Consider, for example, the output voltage $v_{out}$ and current $i_{out}$ in a DC-DC converter, such that we could write the STL formulas as $\varphi_v = \mathcal{G}\ v_{out} < 70\ V$ and $\varphi_i = \mathcal{G}\ i_{out} < 5.5\ A$. The conjunction of $\varphi_v$ and $\varphi_i$ (i.e., $\varphi_v \wedge \varphi_i$) is also an STL formula as per definition in (1).

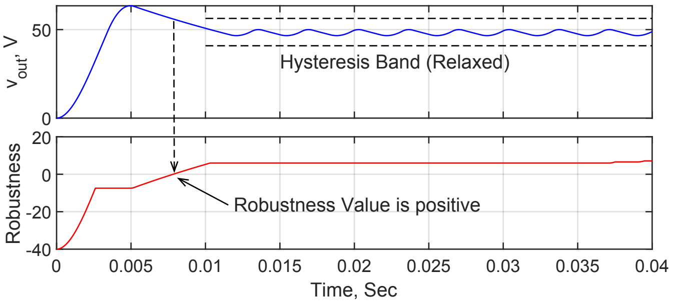


Fig. 3. Output voltage of a hysteresis-controlled buck converter (Top Plot) with its corresponding robustness value (Bottom Plot). $\phi_{Buck}$ evaluates to true and attains a positive value as soon as $V_{out}$ enters the relaxed hysteresis band (shown in dotted lines) at about $0.0078\ s$ and stays within the band.

STL formulas have each temporal operator indexed by $\tau$. We assume $\tau = [0, +\infty)$ if it is not specified for a given temporal operator. STL requiremetns are formally defined in terms of STL formulas. A signal $\sigma$ *satisfies* the STL requirement $\phi$ (i.e., $\sigma \models \phi$), if $\phi$ evaluates to *true* when $\sigma$ meets the conditions defined in $\phi$. For example, the signal $v_{out}$ satisfies the STL formula $\varphi = \mathcal{G}_{[0,0.04)}(v_{out} > 0 \wedge v_{out} < 65)$ in Fig. 3. There always exists a time instant $0 \leq t < 0.04$, where $v_{out}$ is greater than 0 and less than $65\ V$, signifying that $v_{out} \models \varphi$. One could evaluate this STL formula to be true or false that merely provides a *Yes* or *No* answer for the satisfaction of the formula. This, however, should be augmented with some quantitative information to ascertain the degree to which signal $\sigma$ satisfies an STL formula, e.g., if one can distinguish whether a given signal $\sigma = c + \gamma$ or $\sigma >> c$, where $c$ is the desired value of the signal and $\gamma$ is some small number. This is captured through the *quantitative semantics* of STL that provides the *robustness degree* for the satisfaction of STL formulas [20], [21]. It explicitly provides a measure to ascertain whether $\sigma$ violates the STL formula by far ($\sigma >> c$) or very marginally ($\sigma = c + \gamma$), i.e., how far a signal deviates from its desired value.

Given $\chi$, a real-valued function of a formula $\varphi$, a trace $\theta$, and a time $t$, the quantitative semantics $\chi(\varphi, \theta, t)$ is defined as:

$$\begin{cases} \chi(\theta(t) \geq 0, \theta, t) = y(\theta(t)) \\ \qquad \chi(\neg\varphi, \theta, t) = -\chi(\varphi, \theta, t), \\ \chi(\varphi_1 \wedge \varphi_2, \theta, t) = \min(\chi(\varphi_1, \theta, t), \chi(\varphi_2, \theta, t)), \\ \chi(\varphi_1 \mathcal{U}_\tau \varphi_2, \theta, t) = \sup\limits_{t_1 \in t+\tau} \min(\chi(\varphi_2, \theta, t_1) \\ \qquad\qquad \inf\limits_{t_2 \in [t, t_1]} \chi(\varphi_1, \theta, t_2)). \end{cases} \tag{2}$$

Unlike Boolean outcomes, i.e., *Yes* or *No*, such quantitative semantics provide a real value representing the quantitative measure to satisfaction or violation of an STL formula $\varphi$.

The STL requirements may be formally defined and monitored based on the relaxed hysteresis switching boundaries in Fig. 3, i.e., $v_{ref} + \delta$ and $v_{ref} - \delta$. In plain language, *the output voltage* $v_{out}$ *should eventually reach the relaxed hysteresis band and always remain there until* $0.04\ s$. This

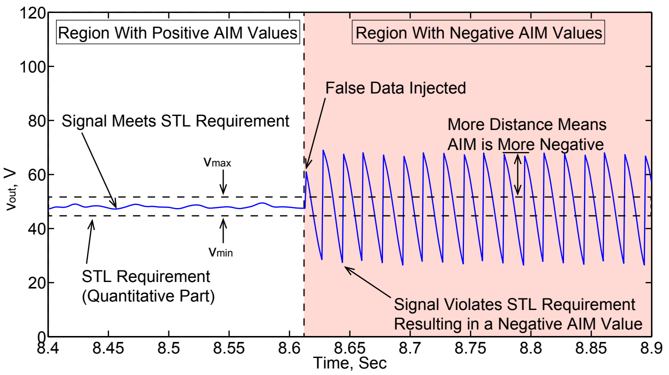


Fig. 4. Effects of FDIA on the measured output voltage signal of a DC microgrid. The proposed STL monitoring technique not only detects an attack, but also provides an impact measure to ascertain its severity.

STL requirement can be formally defined as

$$\phi_{Buck} = \mathcal{F}_{[0,\ 0.04]}\big[\mathcal{G}_{[0,\ 0.04]}\ (v_{out} \leq v_{ref} + \delta) \wedge \\ \mathcal{G}_{[0,\ 0.04]}\ (v_{out} \geq v_{ref} - \delta)\big]. \quad (3)$$

In this example, $v_{ref} = 48\ V$ and $\delta = 8\ V$. Here, the Breach tool [21] is used to evaluate the STL requirement $\phi_{Buck}$ defined in (3). The time plot for $v_{out}$ of the hysteresis-controlled Buck converter along with the corresponding robustness value of the STL requirement, $\phi_{Buck}$, are shown in Fig. 3. Initially, the robustness value is negative with a large value, indicating the extent by which it violates the given STL requirement. However, the robustness value becomes positive as soon as $v_{out}$ enters the relaxed hysteresis band.

STL requirements for DC microgrids are formalized as a singleton formula based on their output signals, i.e., output current, $i_{out}$, and output voltage, $v_{out}$. For the $j^{th}$ DC-DC converter, an STL requirement $\phi_j$ can be formulated as

$$\phi_j = \mathcal{G}_{[t_s,\infty]}\ \big[(i_{min} \leq i_{out} \leq i_{max}) \wedge \\ (v_{min} \leq v_{out} \leq v_{max})\big], \quad (4)$$

where $i_{min}$, $i_{max}$, $v_{min}$, and $v_{max}$ are the safe operating bounds for $i_{out}$ and $v_{out}$, respectively, and $t_s$ is the settling time. STL-based attack detection does not require the microgrid model information, it only requires the measured signals.

## III. STL-based Cyber Attack Detection

### A. Detection Mechanism

In the context of attack detection, the AIM value for a given signal is based on the robustness degree that provides the extent by which the signal violates the STL requirement. In the illustrative example of Fig. 4, the output voltage from the DC microgrid is passed through the STL monitoring process that evaluates it against a predefined formal requirement. The quantitative part of such a requirement is depicted by the upper and lower voltage levels (i.e., $v_{max}$ and $v_{min}$, respectively, shown by the dotted lines in Fig. 4). This results in a positive AIM value as long as the signal meets the STL requirement (i.e., remains within the dotted lines). Any violation of STL requirements results in a negative AIM value indicating the presence of a cyber attack. The magnitude of AIM indicates the robustness of the DC microgrid against a cyber attack if positive, and severity of the cyber attack if negative. In other words, *attack impact measure* (AIM) is the maximum robustness value $max\{|\chi(\varphi,\theta,t)|\}$ for a given STL formula $\varphi$ evaluated over a trace $\theta(t) = \{i_{out}(t), v_{out}(t)\}$ for a given DC-DC converter in the microgrid.

This work employs the Breach tool [21] to compute the robustness degree (based on the quantitative semantics in (1)) of a trace for a given STL formula, such that the signals are described as a finite sequence of time-stamped points. Let $\zeta$ be the robustness signal, and $d\zeta(t_i)$ denote its derivative at time $t$. A signal is then represented by its sequence $(t_i, \zeta(t_i), d\zeta(t_i))$ for all $i < n_\zeta$, where $n_\zeta$ is a natural number. Such a finite sequence of points is considered as piece-wise linear via interpolation in the Breach tool. The minima and maxima of those points are computed over a sliding time-window through an optimal streaming algorithm. Moreover, this tool accommodates the temporal aspects by employing Boolean, eventually, always, and until operators [21].

For example, in the case of Boolean operators, the robustness value computation for an STL requirement $\neg\varphi$ is obvious, with a known robustness value corresponding to $\varphi$. If the sequence $(t_i, \zeta(t_i), d\zeta(t_i))$ for all $i < n_\sigma$ is the robustness signal corresponding to $\chi(\varphi,\theta,t_i)$, then the sequence $(t_i, -\zeta(t_i), -d\zeta(t_i))$ corresponds to $\chi(\neg\varphi,\theta,t_i)$. To describe the conjunction operator, let $\zeta$ and $\zeta'$ be the robustness signals of $\varphi$ and $\phi$, respectively. The conjunction operation then involves computing the sequence of points as both the robustness signals, $\zeta$ and $\zeta'$, intersect.

In the case of a typical temporal operator *eventually*, given the robustness signal $\zeta$ for STL requirement $\varphi$, and $\rho$ as the corresponding robustness signal for $\mathcal{F}\varphi$, by definition, $\rho(t_j) = max\{\sup\limits_{[t_j,t)} \zeta, \rho(t)\},\ \forall t_j < t$. For a timed eventually operator, the robustness degree for the time window, $t+\alpha$ to $t+\beta$, is given by

$$\sup_{t+[\alpha,\beta]} \zeta = max\{\zeta(t+\alpha), \zeta(t+\beta)\} \cup \\ \{\zeta(t_i) \mid t_i \in (\alpha,\beta]\}. \quad (5)$$

The computation of $\rho$ is thus reduced to finding the maximum of $\{\zeta(t_i) \mid t_i \in (\alpha,\beta]\}$, which is achieved by the running maximum algorithm [24] in Breach tool.

*until* operator involves two robustness signals, $\zeta$ and $\zeta'$, for $\varphi$ and $\phi$, respectively, such that their respective time sequences are $(t_i)\forall\ i \leq n_\zeta$ and $(t'_i)\forall\ i \leq n'_\zeta$. Let $\varepsilon$ be the robustness signal for $\varphi\,\mathcal{U}\,\phi$, then $\varepsilon(t) = \sup\limits_{\tau\in[t,+\infty)} min\{\zeta'(\tau), \inf\limits_{[t,\tau]} \zeta\}$. The Breach tool computes this signal as

$$\varepsilon(t_j) = max\{\varepsilon(t_j), min\{\inf_{[t_j,t)} \varepsilon(t)\}\}, \quad (6)$$

where $t_j < t$, and $\varepsilon(t_j) = \sup\limits_{\tau\in[t_j,t)} min\{\zeta'(\tau), \inf\limits_{[t_j,\tau]} \zeta\}$ [21].

### B. FDIA

In the distributed cooperative control scheme, the information is transmitted among the neighboring converters on a sparse communication graph. For example, the vector $X_i$

in Fig. 1 represents the information transmitted by the $i^{th}$ converter to $(i+1)^{th}$ and $(i-1)^{th}$ neighbor converters. In an FDIA, the adversary contaminates the original data/measurement vector with a vicious vector and disturbs the consensus among the converters as will be demonstrated in Section IV. Let $X_i = [x_1, x_2, \dots, x_k]$ be the vector containing $k$ variables for the $ith$ converter in a DC microgrid. This data/measurement vector could be contaminated if an FDIA vector with the same dimension is formulated and added to $X_i$. Let the FDIA vector for the $i^{th}$ converter be $\Lambda_i = [\lambda_1, \lambda_2, \dots, \lambda_k]$, then the compromised vector is given by $Z_i = X_i + \Lambda_i$.

For an effective FDIA vector formulation, the adversary must have knowledge of DC microgrid infrastructure (e.g., communication topology and distributed control scheme), and have physical access to the sensors and the communication network. In this paper, both *unconstrained* and *constrained* FDIAs are considered. In an unconstrained scenario, the intruder has knowledge and access to all the converters, sensors, and the entire communication network. Under a constrained scenario, the intruder has limited knowledge and access, hence affecting a limited number of converters. One or more elements of the FDIA vector $\Lambda$ are zero in case of a *constrained* FDIA, whereas all the elements are non-zero in case of an *unconstrained* FDIA.

### C. DoS

DoS is targeted against the communication infrastructure, partially or entirely paralyzing the data exchange among converters. The attacker may either drop all transmitted packets or flood the communication network to consume its resources [19]. This paper considers a DoS attack that totally paralyzes the communication between two converters, and is represented through the communication link failure. There are possibly two main distinguishing features between DoS attacks and short-circuit faults in DC microgrids, i.e., the physical impact (observable to measurements) and the nature of stimuli (observable through the operational status of device or a physical components).

*1) Physical Impact:* Short-circuit faults lead to a large current flow and a drop in distribution bus voltage, depending on the available DC sources and the grounding impedance [25]. The physical impact of a short circuit fault on DC microgrid is typically more severe as compared to a DoS attack, as shown in a case study in Section IV.

*2) Nature of Stimuli:* A short circuit has a physical stimuli, e.g, a line-to-line fault or a line-to-ground fault, whereas, a cyber attack has a cyber stimuli. In case of a DoS attack, the communication links of the DC microgrids are compromised. The AIM-based approach could further be augmented if more distinguishing signatures are available, such as the operational status of the communication links.

### D. Hyperproperties Formulation for Mitigation Analysis

Once an FDIA is detected, an appropriate mitigation strategy can augment the controller with a suppression mechanism. The effectiveness of such strategy could then be ascertained through hyperproperty formalism. Given a set of all the traces $\mathcal{T}$ and the relevant power set $\mathcal{P}$, the *hyperproperty* $\mathcal{H}$ is defined by the sets of allowed traces such that $\mathcal{H} \subset \mathcal{P}$. A *hyperproperty* requires two or more traces to be verified, in contrast to an STL requirement that is verified on an individual trace.

Intuitively, every property of a given system is a hyperproperty if the system is represented as an aggregation of the traces. This work presents hyperproperties that capture the relationships among multiple traces of DC microgrids in the attack mitigation context. The hyperproperty formalism is defined as

$$\mathcal{H} = \Theta \in \mathcal{P} \mid \exists\, \theta \in \Theta, \forall\, \theta' \in \Theta, (\theta, \theta') \models \phi, \tag{7}$$

where $\phi$ is any given property to be verified. $\theta = \sigma_u(t) \cup \sigma_f(t) \cup \sigma_y(t)$ such that $\sigma_u(t)$, $\sigma_f(t)$, and $\sigma_y(t)$ correspond to the controller action, false signal, and the output signal, respectively. The hyperproperty formalism is further extended to verify effectiveness of the FDIA suppression mechanism in terms of the *robust control invariance* property [26], [27]. Such a property requires that an appropriate control strategy exists for a given set of safe behaviors to keep the system in a safe set as it is subjected to an external disturbance [26]. This hyperproperty is formally defined as

$$\mathcal{H}_c = \exists\, \theta\, \forall\, \theta' \mathcal{G}_{[t_s,\infty]} |\sigma_u, \sigma'_u|_{sup} = 0 \implies v_{min} \leq v' \leq v_{max}, \tag{8}$$

where $t_s$ is the settling time, and $|\sigma_u, \sigma'_u|_{sup}$ is the supremum norm of two given control signals $\sigma_u$ and $\sigma'_u$, such that

$$|\sigma_u, \sigma'_u|_{sup} = sup_{t \in \mathbb{R}_{\geq 0}} \|\sigma_u(t) - \sigma'_u(t)\|. \tag{9}$$

The hyperproperty defined in (8) requires comparison of system behaviors under two different control strategies. In this paper, we consider three different mitigation strategies as candidates to be analyzed. The first strategy employs the distributed cooperative control without any FDIA mitigation, the second strategy augments the existing control scheme with an FDIA suppression mechanism with reduced performance, and the third strategy involves an improved FDIA suppression mechanism. To employ the STL framework for verification, the hyperproperty defined by (8) can be transformed to an STL requirement for the output voltage of a DC microgrid as

$$\begin{split}\phi_c = \forall\, v_f\ \mathcal{G}_{[t_s,\infty]}\big[(v_{min} \leq v_{mit1} \leq v_{max}) \vee (v_{min} \leq \\ v_{mit2} \leq v_{max}) \vee (v_{min} \leq v_{mit3} \leq v_{max})\big],\end{split} \tag{10}$$

where $v_{mit1}$, $v_{mit2}$, and $v_{mit3}$ are the output voltages for the effected converter of a DC microgrid under three different mitigation strategies, and $v_f$ is the false voltage signal. The STL requirement (10) is used in Section IV-D.

## IV. Experimental Evaluation

### A. DC Microgrid Testbed

The topological structure of a DC microgrid testbed is shown in Fig. 5. This testbed is composed of four dSPACE DS 1202 MicroLabBoxes (MLBXs) [28] to implement controllers and the communication network, four Typhoon HIL 603 systems [29] to emulate power converters and the power distribution network, Netgear ProSAFE 24-port Ethernet Smart Switch

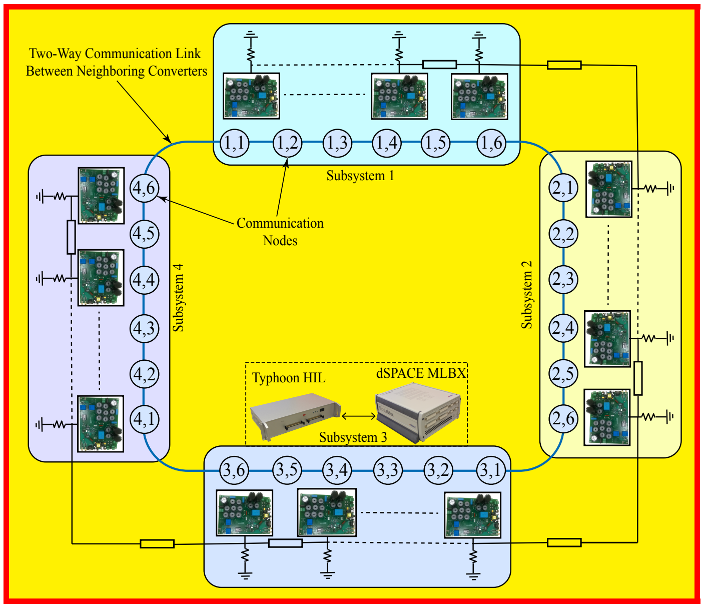


Fig. 5. The DC microgrid is composed of 24 DC-DC converters, clustered in four groups of six converters, their corresponding distributed controllers, and the communication network, implemented through four Typhoon HIL603 systems, four dSPACE MLBXs, and a LAN switch, respectively.

to enable communication among converters, and a desktop computer with Intel Xeon 3.6 $GHz$ processor, 64 $GB$ RAM, and Windows 7-64 bit operating system as a man-machine interface. The DC microgrid is divided into four *subsystems*. In each subsystem, a dSPACE MLBX and a Typhoon HIL system are interconnected through a sub-D connector and an interface board, such that six DC-DC Buck converters are emulated onto one Typhoon HIL system, and their respective distributed control scheme is implemented onto its corresponding dSPACE MLBX through C-code. Overall, 24 converters are emulated on four subsystems (6 converters in each subsystem). The communication topology among converters is shown in Fig. 5. In their enumeration, the first digit signifies the subsystem, and the second digit denotes the converter. For example, the encircled "$2,5$" denotes the communication node of the $5^{th}$ converter of the $2^{nd}$ subsystem, and $C_{2,5}$ denotes the respective converter. The converter parameters are $C = 2.2\ mF$, $L = 2.64\ mH$, $f_s = 60\ kHz$, $R_L = 10\ \Omega$, $v_{ref} = 48\ V$, and $v_{in} = 80\ V$. The STL requirements are defined by (4), where $i_{min} = 2.5\ A$, $i_{max} = 3.0\ A$, $v_{min} = 46\ V$, and $v_{max} = 49\ V$.

### B. FDIA

Sawtooth signals with 60Hz frequency, and 3.5 $A$ and 21 $V$ amplitudes are used as false data for currents and voltages variables, respectively.

*1) Unconstrained FDIA:* In the first case study, we initiate an unconstrained FDIA for all 24 converters around 10.1 $s$. The effects of unconstrained FDIA on six converters of subsystems 1 are shown in Fig. 6. The AIM values for all the 24 converters have been computed for the STL requirements defined by (4) and are found to be negative with large magnitudes. The absolute AIM values range from $|-17.4|$ to $|-20.81|$, and are plotted in Fig. 7. Such large AIM values signify that an unconstrained FDIA can severely distort the converters outputs.

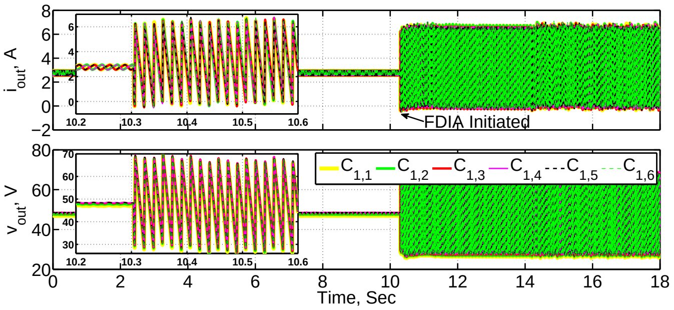


Fig. 6. Output current and voltage waveforms for six converters in subsystem 1 when an unconstrained FDIA targets converters' sensors.

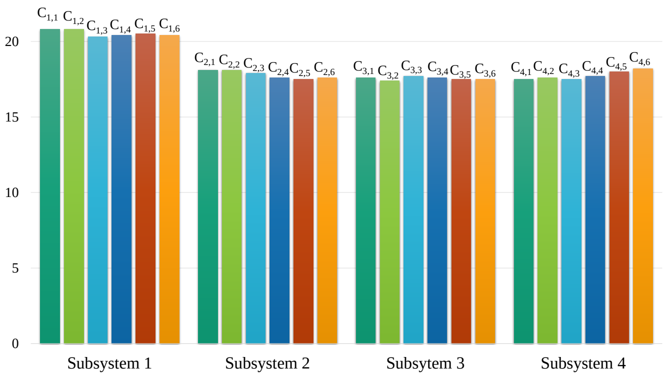


Fig. 7. Absolute AIM values are plotted when all the 24 converters (four subsystems with six converters in each) are subjected to an unconstrained FDIA.

*2) Constrained FDIA:* Converters 1, 3, and 6 of all the subsystems are targeted around 10.1 $s$. As an example, the effects on six converters of subsystems 1 are shown in Fig. 8. The computed absolute AIM values are shown in Fig. 9. As seen, the consensus process in all converters is disturbed due to trickling effects of the attack. The AIM values for converters 1, 3, and 6 of all the subsystems lie in the range between $-19.41$ to $-16.94$, whereas for all other converters, this values lies between $-0.294$ to $-0.186$. The magnitude of AIM values in Fig. 9 shows the impact of the constrained FDIA, where the attack severity is more on converters 1, 3, and 6 in all the subsystems. It is evident that one not only can pinpoint the affected converter, but can also ascertain the attack impact.

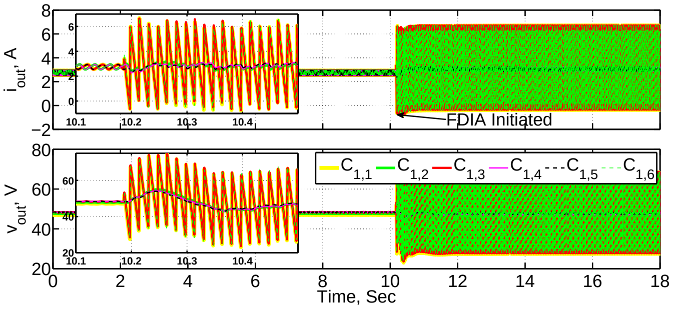


Fig. 8. Output current and voltage waveforms for converters in subsystem 1 when constrained FDIA targets only converters 1, 3, and 6.

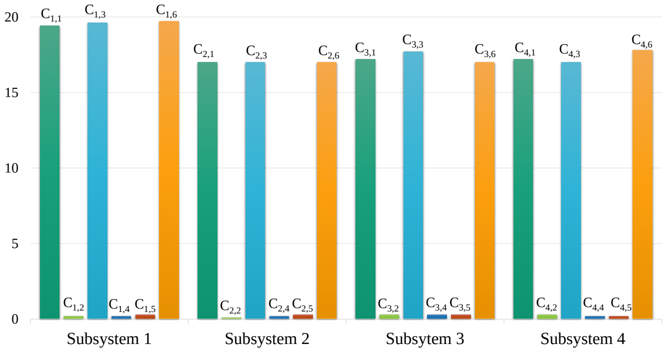


Fig. 9. The absolute AIM values are plotted when converters 1, 3, and 6 in each subsystem are subjected to a constrained FDIA.

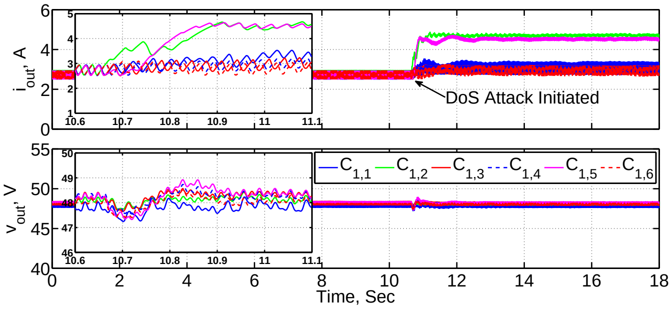


Fig. 10. Output current and voltage waveforms in subsystem 1 when DoS attack targets only converters 2 and 5.

### C. DoS Attack

The control scheme relies on information exchange (namely, values of the current and the local voltage estimates) among DC-DC converters neighboring on a communication network (represented by a sparse graph). If the process of information exchange is distorted, e.g., by a cyber attack on a communication link, the desired control objectives cannot be met. Herein, DoS attack is emulated through communication link failure. DoS attack disables all the communication links between converters 2 and 5, of all the subsystems, and their neighbors. For a given subsystem, converter 2 exchanges information with converters 1 and 3, whereas converter 5 exchanges information with converters 4 and 6 as shown in Fig. 5. The effects of DoS attack on subsystems 1, 2, 3, and 4 are shown in Fig. 10, Fig. 11, Fig. 12, and Fig. 13, respectively. Here, DoS attack is initiated at about 10 $s$ that effectively distorts the outputs of converters 2 and 5. The outputs of all other converters are slightly disturbed.

Let us consider converter 2 in subsystems 1 as an example in Fig. 5, wherein, the corresponding communication node is denoted as "$1, 2$". Since both incoming communication links to converter 2 are affected by a DoS attack, the input to the control module in converter 2 is affected, and the output of converter 2 is distorted. A similar argument applies to converter 5. The computed absolute AIM values are shown in Fig. 14. The impact of DoS attack appears to be more severe on converters 2 and 5 of all the subsystems, whereas that for all other converters is almost negligible.

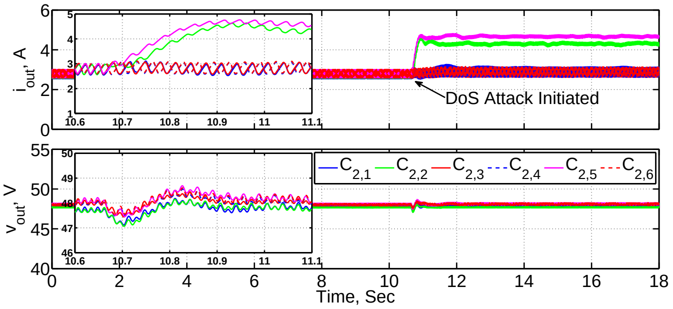


Fig. 11. Output current and voltage waveforms in subsystem 2 when DoS attack targets only converters 2 and 5.

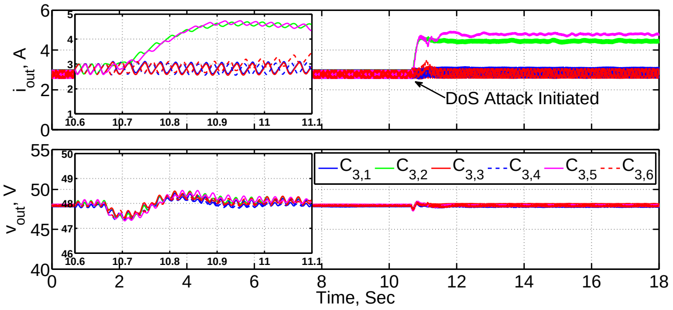


Fig. 12. Output current and voltage waveforms in subsystem 3 when DoS attack targets only converters 2 and 5.

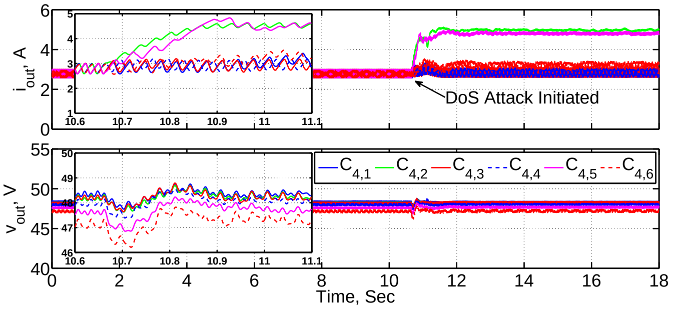


Fig. 13. Output current and voltage waveforms in subsystem 4 when DoS attack targets only converters 2 and 5.

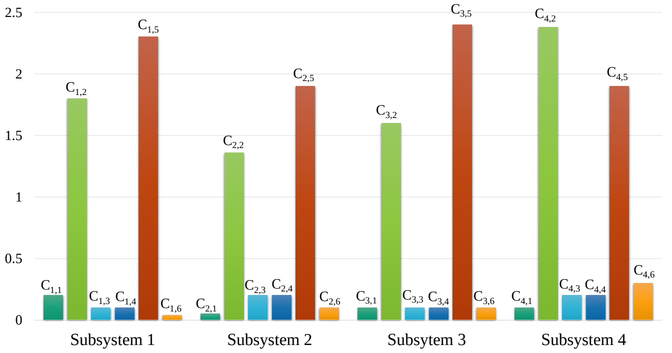


Fig. 14. The absolute AIM values under a DoS attack scenario.

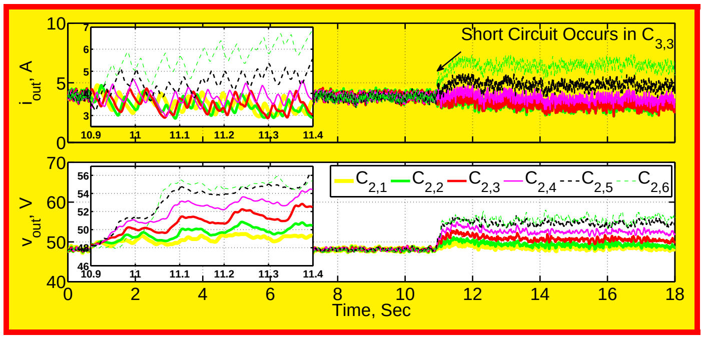


Fig. 15. Output current and voltage waveforms in subsystem 2 when short circuit fault occurs in converter 3 of subsystem 3.

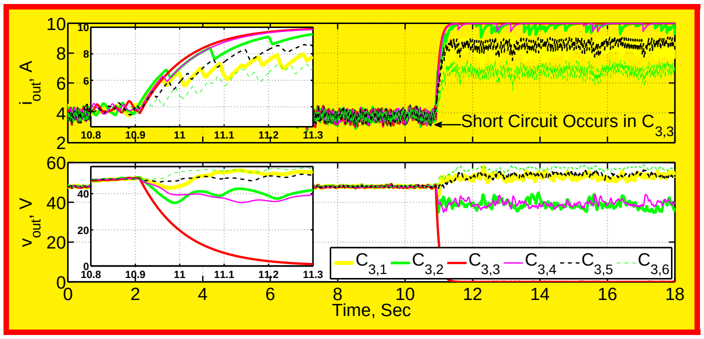


Fig. 16. Output current and voltage waveforms in subsystem 3 when short circuit fault occurs in converter 3 of subsystem 3.

### D. Short Circuit Fault Analysis

We present a comparison between a DoS attack and a short circuit fault using the proposed STL-based technique. Herein, a line-to-line short circuit fault is emulated in converter 3 of subsystems 3 (denoted by $C_{3,3}$) at about $10.92$ $s$. The severe effects of this anomaly are shown in Fig. 15, Fig. 16, and Fig. 17 for the converters of subsystems 2, 3, and 4, respectively. The line-to-line voltage of $C_{3,3}$ drops to zero, and its line current jumps to a higher value, severely effecting neighbor converters. The computed absolute AIM values are shown in Fig. 18. The absolute AIM value computed for $C_{3,3}$ (the effected converter) under this short circuit fault is $46$. Whereas, in the case of a DoS attack, the absolute AIM values in Fig. 14 for converters 2 and 5 for all four subsystems are in the range of $1-2.5$. The AIM values of converters effected by a DoS attack are much lesser as compared to the case of a short circuit fault. As discussed in Section III, this approach could be augmented with the operational status of communication links which are compromised under a DoS attack.

### E. Experimental Evaluation on a Prototype DC Microgrid

This technique is also verified using a prototype DC microgrid system with four DC-DC Buck converters with the communication topology as shown in Fig. 19. For this case study, $v_{ref}$ is set to 20 $V$ so as not to overheat the system during an FDIA. The converter component values are the same as used in previous studies The STL requirements are defined by (4), such that $i_{min} = 1.9$ $A$, $i_{max} = 2.1$ $A$, $v_{min} = 19$ $V$, and $v_{max} = 21$ $V$. An unconstrained FDIA is initiated at about $9.8$ $s$, keeping the physical testbed safety in mind. Sawtooth signals with 60Hz frequency, and 1 $A$ and 10 $V$ amplitudes, have been used as the false data for currents and voltages, respectively. The effects of an unconstrained FDIA on the prototype DC microgrid system are shown in Fig. 20.

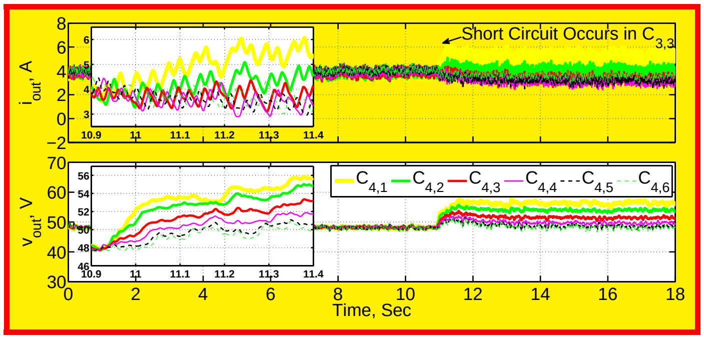


Fig. 17. Output current and voltage waveforms in subsystem 4 when short circuit fault occurs in converter 3 of subsystem 3.

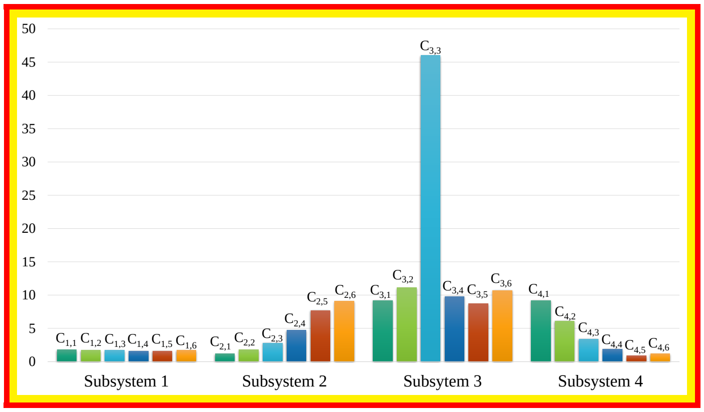


Fig. 18. The absolute AIM values under a short circuit fault scenario.

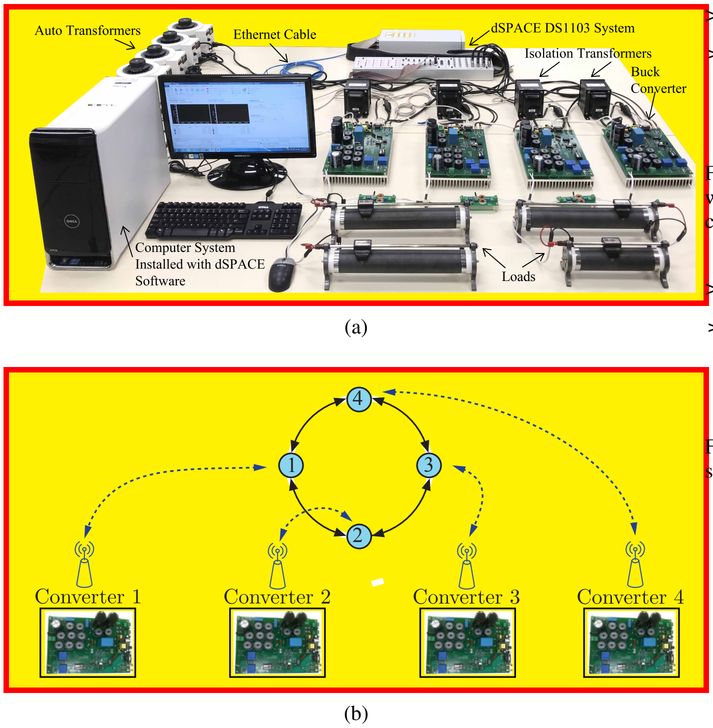
The corresponding AIM values are found to be $-9.4$, $-9.67$, $-9.29$, and $-9.97$ for converters 1, 2, 3, and 4, respectively. In the second case study, a constrained FDIA is initiated at about $9.5$ $s$ on converters 1 and 3. The effects of an unconstrained FDIA on the prototype DC microgrid system are shown in Fig. 21. The corresponding AIM values are $-9.262$, $-0.262$, $-9.265$, and $-0.256$ for converters 1, 2, 3, and 4, respectively. By comparison, it is evident that the attack severity is more on converters 1 and 3.

### F. Selection of the Best Candidate Mitigation Strategy

Since the proposed STL-based method can quantify the attack impact, it can be used as a measure of effectiveness to evaluate any mitigation strategy. For this case study, the FDIA is initiated on the voltage sensor of converter 3 in subsystem 1. We have considered three candidate mitigation strategies, and quantified the attack impact in each scenario, where the respective mitigation strategy was employed:

1. First, the conventional distributed cooperative controller is used in isolation, with no mitigation strategy. The results are shown in Fig. 22.
2. Then, a partial FDIA suppression mechanism [30], using a low-pass filter of the form

$$H(s) = \frac{1}{s+a}, \tag{11}$$



(a)

(b)

Fig. 19. Experimental DC Microgrid Setup. (a) The prototype DC microgrid with four DC-DC Buck converters, and the distributed cooperative controller implemented on a dSPACE DS 1103 system. (b) Communication topology for four converters.

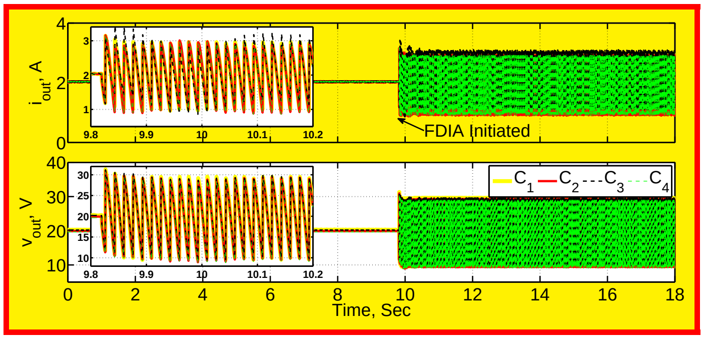


Fig. 20. Output current and voltage waveforms in the prototype microgrid, when an unconstrained FDIA targets the converters' sensors.

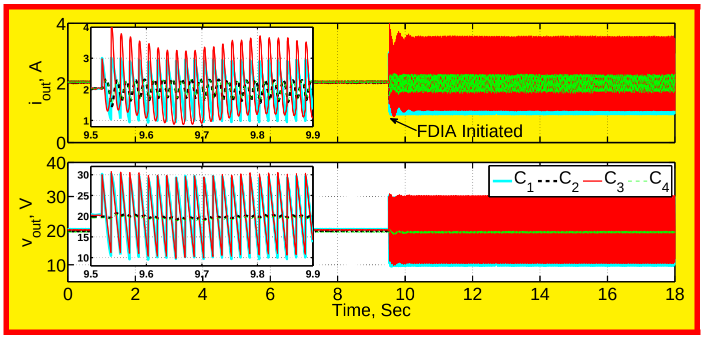


Fig. 21. Output current and voltage waveforms in the prototype microgrid, when a constrained FDIA targets the sensors of converters 1 and 3.

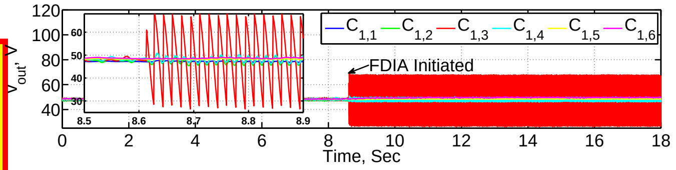


Fig. 22. Effects of an FDIA on cyber-physical DC microgrid are shown, when converter 3 of subsystem 1 is targeted. It is evident that distributed cooperative control scheme alone is suceptible to FDIA.

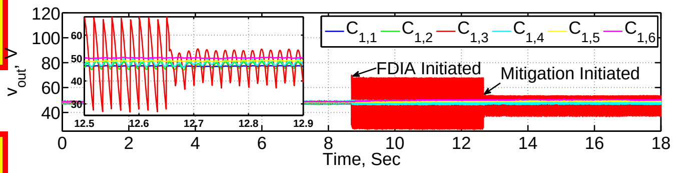


Fig. 23. Partial suppression mechanism is shown, when converter 3 of subsystem 1 is targeted.

is employed, where $a \in \mathbb{R}_{\geq 0}$. The value of $a$ is chosen such that the effects of FDIA are partially suppressed as shown in Fig. 23.

3. Finally, the performance of the FDIA suppression mechanism is improved by adjusting $a$ in (11). The resulting performance is shown in Fig. 24.

The traces produced by the three mitigation strategies are subjected to the STL-based analysis, and the AIM values computed are $-20.18$, $-9.42$, and $0.55$, respectively. Comparison of the AIM values provides a guideline on how to select the best mitigation strategy. Per its AIM value, and as expected, the third mitigation strategy is considered the best strategy.

## V. Conclusion

Cyber attacks, such as FDIA and DoS, can distort the operation of a power electronics-intensive DC microgrid by impairing the consensus protocols used in its distributed control paradigm. An STL-based cyber attack detection is presented that not only successfully locates and detects both FDIA and DoS attacks, but also provides the measure to determine the attack severity on the point of impact. This approach is independent of the system knowledge; therefore, it can conveniently be used for complex microgrids for anomaly/attack detection. The effectiveness of the proposed technique is demonstrated on a hardware-in-the-loop as well as a physical prototype microgrid testbeds.

## Acknowledgment

The authors would like to thank Typhoon and dSPACE technical support and engineering teams for their help with setting up their respective units.

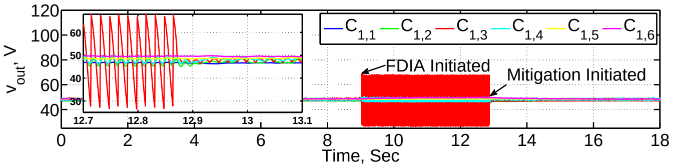


Fig. 24. The mitigation effects of the FDIA suppression mechanism are shown, when converter 3 of subsystem 1 is targeted.

## References

[1] T. Dragičević *et al.*, "Dc microgrids - part ii: A review of power architectures, applications, and standardization issues," *IEEE Trans. Power Electron.*, vol. 31, no. 5, pp. 3528–3549, May 2016.

[2] V. Nasirian *et al.*, "Distributed cooperative control of dc microgrids," *IEEE Trans. Power Electron.*, vol. 30, no. 4, pp. 2288–2303, Apr 2015.

[3] L. Meng *et al.*, "Modeling and sensitivity study of consensus algorithm-based distributed hierarchical control for dc microgrids," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1504–1515, May 2016.

[4] T. V. Vu *et al.*, "An alternative distributed control architecture for improvement in the transient response of dc microgrids," *IEEE Trans. Ind. Electron.*, vol. 64, no. 1, pp. 574–584, Jan 2017.

[5] T. Dragičević *et al.*, "Dc microgrids - part i: A review of control strategies and stabilization techniques," *IEEE Trans. Power Electron.*, vol. 31, no. 7, pp. 4876–4891, July 2016.

[6] Q. Shafiee *et al.*, "A multi-functional fully distributed control framework for ac microgrids," *IEEE Trans. Smart Grid*, 2017, doi:10.1109/TSG.2016.2628785.

[7] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58–66, Jan 2012.

[8] M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 436–447, April 2017.

[9] A. E. Shafie, D. Niyato, R. Hamila, and N. Al-Dhahir, "Impact of the wireless network's phy security and reliability on demand-side management cost in the smart grid," *IEEE Access*, vol. 5, pp. 5678–5689, May 2017.

[10] K. Manandhar *et al.*, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE Trans. Control Network Syst.*, vol. 1, no. 4, pp. 370–379, Dec 2014.

[11] M. Chlela *et al.*, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Trans. Smart Grid*, 2017, doi: 10.1109/TSG.2017.2667586.

[12] J. Zhao, G. Zhang, M. L. Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, July 2017.

[13] Z. Lu, W. Wang, and C. Wang, "Camouflage traffic: Minimizing message delay for smart grid applications under jamming," *IEEE Trans. Dependable Secure Computing*, vol. 12, no. 1, pp. 31–44, Jan 2015.

[14] G. Liang *et al.*, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, July 2017.

[15] H. Zhang *et al.*, "Dos attack energy management against remote state estimation," *IEEE Trans. Control Network Syst.*, 2017, doi: 10.1109/TCNS.2016.2614099.

[16] R. Moslemi, A. Mesbahi, and J. M. Velni, "A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids," *IEEE Trans. Smart Grid*, 2017, doi: 10.1109/TSG.2017.2675960.

[17] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, 2017, doi: 10.1109/TSG.2017.2703842.

[18] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, 2017, doi: 10.1109/TSG.2016.2596298.

[19] P. Yi *et al.*, "Puppet attack: A denial of service attack in advanced metering infrastructure network," *J. Network Comput. Applicat.*, vol. 59, pp. 325–332, May 2016.

[20] O. Maler and D. Nickovic, "Monitoring temporal properties of continuous signals," in *Proc. Formal Techniques Real-Time Fault -Tolerant Syst.*, 2004, pp. 152–166.

[21] A. Donzé, T. Ferrère, and O. Maler, "Efficient robust monitoring for stl," in *Proc. 25th Int. Conf. Comput. Aided Verification*, 2013, pp. 264–279.

[22] M. R. Clarkson and F. B. Schneider, "Hyperproperties," *Journal of Computer Security*, vol. 18, no. 6, pp. 1157–1210, Sep 2010.

[23] R. Alur, *Principles of cyber-physical systems*. Cambridge, MA: MIT Press, 2015.

[24] D. Lemire, "Streaming maximum-minimum filter using no more than three comparisons per element," *Computing Research Repository*, vol. abs/cs/0610046, pp. 1–12, Oct 2006.

[25] J. D. Park and J. Candelaria, "Fault detection and isolation in low-voltage dc-bus microgrid system," *IEEE Trans. Power Delivery*, vol. 28, no. 2, pp. 779–787, April 2013.

[26] L. Nguyen *et al.*, "Hyperproperties of real-valued signals," in *ACM-IEEE Int. Conf. Formal Methods Models for Syst. Design*, 2017, pp. 1–10.

[27] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, Nov 1999.

[28] *MicroLabBox Product Information*, dSPACE GmbH, Paderborn, Germany, 2017.

[29] *Typhoon HIL 603 Technical Manual*, Typhoon HIL, Inc., Somerville, MA, USA, 2017.

[30] F. C. Schweppe and D. B. Rom, "Power system static-state estimation, part i, ii, and iii," *IEEE Trans. Power App. Syst.*, vol. PAS-89, no. 1, pp. 120–135, Jan 1970.