Projections of Cyberattacks on Stability of DC Microgrids

Modeling Principles and Solution

Leng, Minrui; Sahoo, Subham; Blaabjerg, Frede; Molinas, Marta

Published in:
I E E E Transactions on Power Electronics

DOI (link to publication from Publisher):
10.1109/TPEL.2022.3175237

Creative Commons License
CC BY 4.0

Publication date:
2022

Document Version
Accepted author manuscript, peer reviewed version

Projections of Cyber Attacks on Stability of DC Microgrids – Modeling Principles and Solution

Minrui Leng, Subham Sahoo, *Member, IEEE,* Frede Blaabjerg, *Fellow, IEEE* and Marta Molinas

***Abstract*—Microgrids relying on cooperative control are supported by communications, which are highly vulnerable to cyber-attacks. A significant amount of research is already carried out on the detection and mitigation of cyber attacks to secure the operation of DC microgrids. Although cyber attacks are fully capable of causing cascaded converter outages leading to full/partial system blackouts, disturbing the system stability can also be a viable target by the adversaries, which has been overlooked so far. Hence, this paper focuses on addressing the instability caused by *stealth* cyber attacks, which can easily bypass the well-defined observability tests. In addition, this paper also introduces a novel adaptive stabilization method to eliminate the unstable modes due to cyber attacks, which has been designed considering a previously defined cyber attack detection metric as an input. To investigate its feasibility, a detailed model of a stable DC microgrid is firstly developed. Then, considering *stealth* cyber attack as a non-linear element, the describing function-based method is used to investigate system stability under attack conditions. Finally, theoretical analysis, simulation and experimental results under various scenarios are presented to verify the effectiveness of the proposed stabilization scheme.**

***Index Terms*—Cyber attacks, microgrid, stealth attacks, stability, describing function.**

I. Introduction

DC microgrids have gained an increased attention owing to the ability to integrate renewable energy sources such as photovoltaic systems, fuel cells, and energy storage systems and the electronic loads [1]. To achieve reliable and efficient operation of DC microgrids, a lot of efforts are devoted to the control technologies to regulate the voltage and the output powers of DC power networks [2]-[3]. Among the hierarchical layers, the secondary and the tertiary control layers need communication to coordinate between sources accordingly. Based on the high vulnerability of centralized controller to a single-point-of-failure, distributed controllers have proven themselves to become a strong candidate by offering enhanced reliability, scalability and robustness for microgrids [4].

Apart from the flexibility offered by the communication networks, their omnipresence also expose the microgrids to a wider possibility of cyber attacks. Several cyber threats have been reported in the past. In 2019, hackers exploited firewall vulnerabilities to cause periodic *blind spots* for grid operators in western US causing around 10 hours of disruption [5]. One of the most discussed cyber attacks surfaced in Ukraine in 2015, when its capital city suffered with one of the largest blackout as three oblenergos (energy companies) were attacked using spear phishing emails by the adversaries. This later allowed them to gain illegitimate access into their IT networks [6]. Some of the recent threats can be seen in grid-tied PV inverter systems [8]-[9] and electric vehicles [10], where the attackers seized control of vital safety functions such as braking and steering in Jeep Cherokee and Tesla's model X [11]-[12]. There are many kinds of malicious attacks and infiltration techniques, including false data injection (FDI) attacks, denial of service (DoS) [13], replay attacks [14], man-in-the-middle (MITM) attacks [15], etc. Usually, these attacks can also be well-curated by the adversary, which can be defined as generalized FDIAs, commonly known as *stealth attacks* [16]. In general, stealth attacks can easily penetrate into networked systems without altering the system observability. These attacks can be specifically classified as *coordinated intelligent attacks* [17] that involves coordinated attack vectors in multiple nodes to nullify system dynamics. By compromising the confidentiality, integrity and availability of information, the adversaries can easily affect system operation, or can cause shut down of power electronic dominated grids.

Recently, many papers have investigated the impact of cyber attacks in multi-converter systems, including identification and removal of misbehaving agents [16]-[22]. Some stealth attack detection metrics, namely cooperative vulnerability factor (CVF) [16] and discordant element (DE) [18] are proposed to identify the presence of attack elements on voltage and current sensors in DC networks, respectively. In order for each distributed energy resource (DER) to detect any misbehavior on its neighboring DERs, a neighborhood monitoring based attack detection mechanism is also presented using a Kullback-Liebler divergence-based criterion [19]. Further, the authors in [20] adopt an aperiodic control strategy in which the switching frequency is randomized for encapsuling the detection mechanism to be hidden from the adversaries. IoT based digital twins are also equipped for the resiliency of interconnected microgrids to quickly detect and mitigate different kind of cyber attacks [21]. In [22], a resilient control protocol based on trust coefficient is presented to mitigate the adverse effects of cyber attacks. In [23]-[24], an event-driven signal reconstruction scheme is proposed to detect sophisticated categories of cyber attacks on DC microgrids.

This work is supported by Reliable Power Electronic-Based Power System (REPEPS) project at AAU Energy as a part of the Villum Investigator Program funded by VELUX Foundation.

M Leng is with the College of Electrical Engineering, Sichuan University, Chengdu, China. (e-mail: mrleng_pece@163.com)

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

M Molinas is with the Department of Engineering Cybernetics, Norwegian University of Science and Technology, Trondheim, Norway. (e-mail: marta.molinas@ntnu.no)

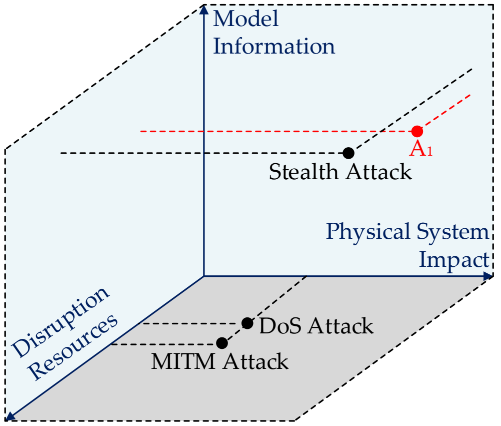


Fig. 1. A three-dimensional cyber-attack space highlighting qualitative positions of various prominent cyber attacks. Moreover, the highlighted point A_1 is the cyber attack under consideration in this paper.

As the ongoing research on cybersecurity in power electronics is primarily focused on detecting and mitigating the prominent cyber attacks, it is timely to assess these conditions on a qualitative basis using the available disruption resources with an adversary. In short, disruption resources are the necessary collateral that allow illegitimate access into the attack target. In networked microgrids, limited disruption resources may imply access to limited nodes. The problem formulation involving limited disruption resources can be explained clearly using the three-dimensional cyber attack space shown in Fig. 1. The cyber-attack space can be decomposed into two 2D planes with *model information* as the reference entity. From the attacker's point of view, a cyber attack designed using fair disruption resources and no model information will have a negligible impact on the physical network due to the existing cyber-secure arrangements. However considering the same situation with sufficient model information, the impact on physical system can be significant assuming that the attacker has enough resources to bypass the cyber-secure arrangements. By mapping the risk in three dimensions and comparing it with the ongoing research, the data integrity attacks in the abovementioned papers do not assume any limitation on the disruption resources for the adversary [25]. Whereas with enhancement of security infrastructure in modern power electronic systems, the disruption resources can be restricted. Under these circumstances, the adversary will have limited access despite having a reasonable amount of knowledge of both physical and cyber components. This situation has been reflected as A_1 in Fig. 1. One of the typical pursuits from the adversaries under this situation can be to force the microgrid to operate around boundary conditions, leading to instability. To the best of authors' knowledge, stability issues caused by cyber attacks being yet another serious concern, has been overlooked so far. In fact, causing instability can be a good tactical approach by the adversary to disturb the well-established stability certificates in microgrids, which have been formalized based on the physical manifestations [26].

In this regard, the stability boundaries of microgrids due to cyber-physical interactions are already investigated in [27]-[28]. However, these stability studies are only limited to cyber disturbances, such as, maximum communication delay, link failure and packet dropouts, etc. On the other hand, stability studies for resilient controllers in the presence of unbounded cyber attacks has already been carried out in [29]-[30]. However, design of resilient controllers in itself can be resource demanding in terms of computational complexity and system information. In contrast, the design of detect-and-isolate strategies [24] can be rather simple, scalable and does not require any system information. Hence, comprehensive ultimate bounded stability definitions for detect-and-isolate based cybersecurity strategies for microgrids need to be outlined. The instability phenomena caused by stealth cyber attacks is introduced briefly in our previous conference paper [31], where the stability analysis of an attacked microgrid is carried out by simple simulation results.

Considering increasing vulnerabilities to cyber attacks as a potential threat in the system, this paper envisions on assessing its projections on the stability of DC microgrids. Firstly, a small-signal model of DC microgrids under the presence of *stealth* cyber attack elements is designed. However as the modeling of cyber attacks can be indeterminate and unstipulated since it depends on adversary's behavior, we reverse-engineer the problem of stability of DC microgrid by exploiting the borderline conditions of the system due to *stealth* cyber attacks. Finally, a stabilization input is configured using a previously used cyber attack detection metric in [16], which makes it adaptive. Finally, treating cyber attack as a non-linear input in the linearized model of DC microgrid, the describing function method is used to certify the system stability based on different magnitude of *stealth* cyber attack elements allocated by the adversary across the system.

This paper is organized as follows. Section II depicts the preliminaries of cyber-physical DC microgrid with a clearly defined problem of projections of cyber attacks on the stability of microgrids. In Section III, the modeling and stability analysis of the attacked DC microgrid is carried out. After analyzing the root cause of the stability issue, the design of the proposed adaptive stabilization approach is explained in Section IV. The ruggedness of the proposed solution is tested under various cyber-physical disturbances in Section V and experimentally validated in Section VI. Finally, Section VII concludes the paper.

II. Cyber-Physical DC Microgrids

A. System Preliminaries

Fig. 2 shows a single-line diagram of networked dc microgrid with N *agents* consisting of renewable energy sources and DC/DC buck converters, which are connected by transmission lines to each other. Apart from the physical connection, these agents are linked by communication network to exchange information. The communication network receives and delivers data among agents, providing information for each controller. Each DC/DC converter is managed by inner voltage and current controllers, as shown in Fig. 2. On top, the secondary controller, comprising of an average voltage regulator and current regulator, is used to ensure global voltage regulation and proportionate load sharing by imposing voltage offsets from each layer, respectively.

In Fig. 2, an undirected cyber graph is considered, where each node represents an agent, also denoted as $\mathbf{x} = \{x_1, x_2, \ldots, x_N\}$ and are linked by edges via an associated adjacency matrix, $\mathbf{A}_{\text{G}} = [a_{ij}] \in R^{N\times N}$, where the communication weight a_{ij} (from node j to node i) is modeled using the specified law: $a_{ij} > 0$, if (ψ_i, ψ_j) $\in$ $\mathbf{E}$, where $\mathbf{E}$ is an edge connecting two nodes, with ψ_i and ψ_j being the local and neighboring node, respectively. It should be noted that if there is no cyber link between psi_i and ψ_j, then a_{ij} = 0. Any given agent at ψ_i node share current and voltage information with neighbors $N_i = \{j \mid (\psi_j, \psi_i) \in \mathbf{E}\}$. The matrix representing incoming information can be given as, $\mathbf{D}_{\text{in}} = \texttt{diag}\{d_i^{in}\}$, where $d_i^{in} = \sum_{j\in N_i} a_{ij}$. Similarly, the matrix representing outcoming information can be given as, $\mathbf{D}_{\text{out}} = \texttt{diag}\{d_i^{out}\}$, where $d_i^{out} = \sum_{i\in N_j} a_{ji}$. Assembling the sending and receiving end information into a single matrix, we obtain the Laplacian matrix $\mathbf{L}$ = $[l_{ij}]$, where l_{ij} are its elements designed using, $\mathbf{L}$ = $\mathbf{D}_{\text{in}}$−$\mathbf{A}_{\text{G}}$.

The objective of cooperative control is to regulate the global average voltage and realize load current sharing proportionally. In order to achieve this, the local and neighboring information are used by the secondary voltage and current regulators to adjust the local reference voltage v_i^* for each converter. This reference is generated using two voltage correction terms, which are responsible for average voltage regulation and proportionate load sharing, respectively and can be given by:

$$\begin{aligned}\Delta V_{1i}(t) = K_P^{H_1}&(V_{\text{dcref}} - \bar{V}_i(t)) \\ &+ K_I^{H_1}\int(V_{\text{dcref}} - \bar{V}_i(t))dt\end{aligned} \tag{1}$$

$$\Delta V_{2i}(t) = K_P^{H_2}\delta_i(t) + K_I^{H_2}\int \delta_i(t)dt \tag{2}$$

where, $\bar{V}_i$ is the estimated average voltage at i^{th} agent; V_{dcref} is the nominal voltage; δ_i is the current mismatch error for i^{th} agent between the local per-unit and neighbors' per-unit output current. The voltage observer and current regulator blocks in Fig. 2 can be mathematically represented as:

$$\bar{V}_i(t) = V_{dc_i}(t) + \int \sum_{j\in N_i} a_{ij}(\bar{V}_j(t-\tau) - \bar{V}_i(t-\tau))dt \tag{3}$$

$$\delta_i(t) = \sum_{j\in N_i} ca_{ij}\left(\frac{I_{dc_j}(t-\tau)}{I_{dc_j}^{max}} - \frac{I_{dc_i}(t-\tau)}{I_{dc_i}^{max}}\right) \tag{4}$$

where, τ represents the communication delay between i^{th} & j^{th} agent and c is the coupling gain. Moreover, I_{dc_i} and I_{dc_j}, $I_{dc_i}^{max}$ and $I_{dc_j}^{max}$ are the measured and maximum output currents for i^{th} agent and j^{th} agent, respectively.

As a result, the local reference voltage V_i^* for i^{th} agent considering the two voltage correction terms in (1)-(2) can be denoted by:

$$V_i^*(t) = V_{\text{dcref}} + \Delta V_{1i}(t) + \Delta V_{2i}(t). \tag{5}$$

Using the distributed consensus algorithm for a well-connected cyber graph in microgrid, the system objectives for DC microgrids using (1)-(5) shall converge to:

$$\lim_{k\to\infty} \bar{V}_i(t) = V_{\text{dcref}}, \quad \lim_{k\to\infty} \delta_i(t) = 0 \quad \forall i \in N \tag{6}$$

B. Modeling and Detection of Stealth Attacks

Considering the possibility of false data injection attacks via many channels such as sensors, communication links, etc. [18] to disrupt the system objectives in (6), we extend our former studies on cyber attacks on voltages in (3), which can be modeled using:

$$\mathbf{u}_a(t) = \mathbf{L}\bar{\mathbf{V}}(t) + \kappa\mathbf{W}\mathbf{X}_a \tag{7}$$

where, $\mathbf{u}_a$, $\bar{\mathbf{V}}$ denote the vector representation of the attacked control input in (3) and the average voltage, respectively. κ is a binary variable, which denotes the presence of cyber attack element by 1, or otherwise. Moreover, $\mathbf{X}_a = [\lambda_i], \forall i \in N$, is a matrix with the false data λ_i for i^{th} agent. It is worth notifying that the system is not under attack, when $\mathbf{X}_a$ = 0. Basically, the second term in (7) represents the distribution of attack elements in DC microgrid, where the attacker may inject any positive valued λ_i into any agent. In simple terms, these elements can either be injected into either the measured values/sensors or the inputs/communicated values. Further, $\mathbf{W}$ = $[w_{ij}]$ denotes a row-stochastic matrix with its elements, given by:

$$w_{ij} = \begin{cases} \frac{1}{N_i+1}, j \in N_i \\ 1 - \sum_{j\in N_i} w_{ij}, j = i \\ 0, j \notin N_i, j \neq i \end{cases} \tag{8}$$

Remark I: *Based on the nature of the row-stochastic matrix* $\mathbf{W}$ *in (8), the cyber attack model in (7) automatically becomes stealth, as* $\mathbf{W}\mathbf{X}_a$ = 0.

However, it should be noted that the stealth cyber attacks modeled using Remark I will only adhere to (7), if and only if $\mathbf{X}_a$ is bounded, such that the following holds true:

$$\mathbf{V}_{\text{dc}_{\text{min}}} < \mathbf{V}_{\text{dc}} < \mathbf{V}_{\text{dc}_{\text{max}}} \tag{9}$$

where, $\mathbf{V}_{\text{dc}_{\text{min}}}$ and $\mathbf{V}_{\text{dc}_{\text{max}}}$ denote the vector representation of minimum and maximum threshold for output voltages, respectively. To detect the presence of these cyber attack elements in the system, a cooperative vulnerability factor (CVF) C_i based attack detection metric for i^{th} agent has already been proposed in [16], which can be mathematically represented as:

$$\begin{aligned} C_i = h_i & \underbrace{\left[\sum_{j\in N_i} a_{ij}(\Delta V_{1j}(t-\tau) - \Delta V_{1i}(t))\right]}_{O_1} \\ & \underbrace{\left[\sum_{j\in N_i} a_{ij}(\Delta V_{1j}(t-\tau) + \Delta V_{1i}(t))\right]}_{O_2} \end{aligned} \tag{10}$$

where, h_i is a positive constant; ΔV_{1i} and ΔV_{1j} are the voltage correction term from voltage observer (as shown in

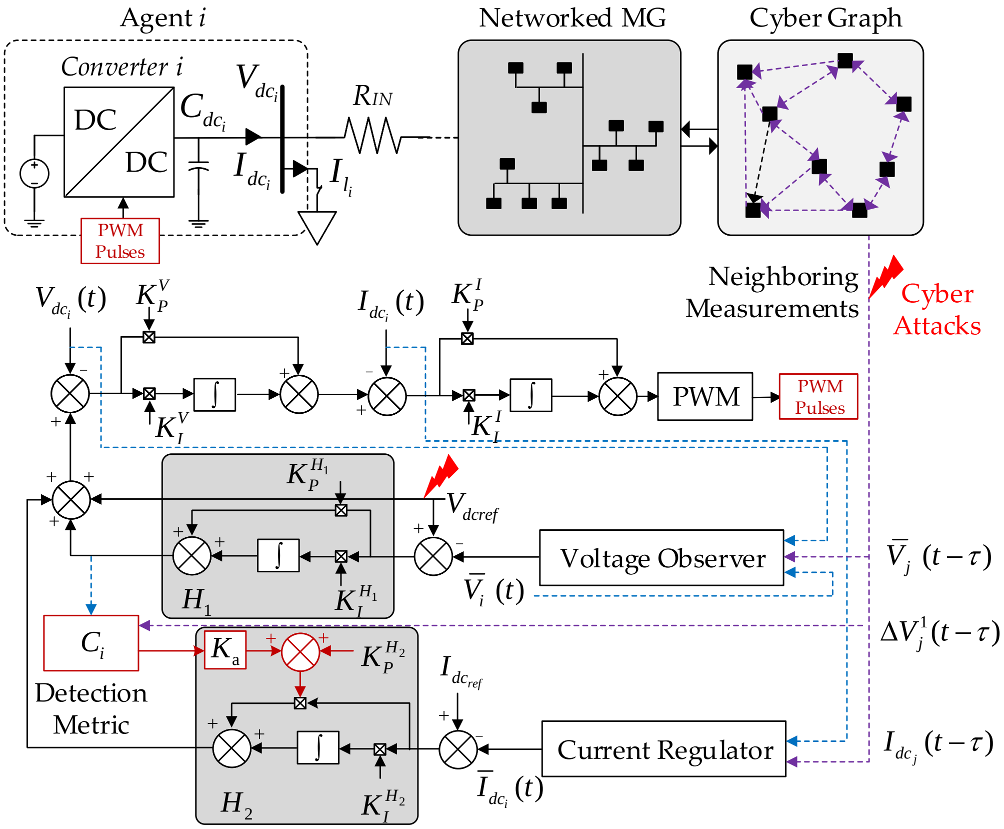


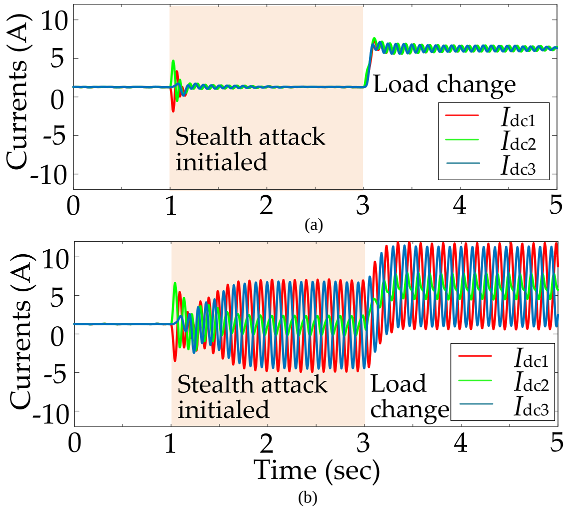
Fig. 2. Cyber-physical DC microgrid with N agents (in the networked MG) with the single line structure of i^{th} agent. Moreover, a cooperative cyber graph is also used to assist the secondary controllers achieve distributed synchronization. Further, a cooperative vulnerability factor (CVF) C_i based detection metric is also highlighted in red [16], which ensures detection of stealth voltage attack elements in DC microgrid.

Fig. 2) in i^{th} and j^{th} agent, respectively. Using the law of consensusability to be followed uniformly for each control layer, it has been validated theoretically in [32] that the control outputs from the secondary control layer not in consensus suggest the presence of cyber attacks in the input signals of these control layers. Using (10) as the basis of cyber attack identification, the following principle is used to certify the presence of cyber attack element in i^{th} agent, if:

$$C_i = \begin{cases} > 0, & \textbf{if } \kappa = 1 \\ \quad 0, & \textbf{else} \end{cases} \tag{11}$$

However, the constraint in (9) may not be available as an information with the adversary. In this case, an instinctive course of action from the adversary could be to inject unbounded cyber attack elements. This will trigger instability and needs to specific attention. On the other hand, it will not only affect the decision making process of the available cybersecurity technologies, but will also put forth questions on the existing stability definitions in a networked system.

To provide a clear understanding, a case study is carried out in a DC microgrid with N = 3 agents in Fig. 3 to demonstrate how unbounded attacks can be responsible for instability. In Fig. 3(a), it can be seen that when a stealth cyber attack is conducted on agent I and III at t = 1 s with its magnitude λ being 15 V, the currents are anyway being proportionately shared. However in Fig. 3(b), when a stealth attack with the magnitude λ increased to 28 V, the microgrid becomes unstable with sustained oscillations. These oscillations will not only affect their reliability of operation, but will also forbid any possible mitigation approaches, which has been illustrated in Fig. 4, where the oscillating detection trajectory of C_3 around the zero point unconditionally proceeding to the mitigation stage. Hence, an adversary with limited resources,



(a)

(b)

Fig. 3. Performance of DC microgrid with N = 3 agents under stealth attacks with a magnitude λ of: (a) 15 V; (b) 28 V when applied to agent I and III at the same time.

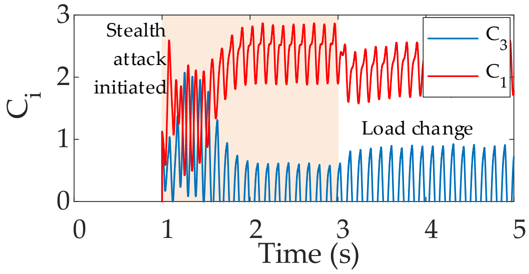


Fig. 4. Performance of cooperative vulnerability factor (CVF) based detection metric for the stealth attack in Fig. 3(b) – the oscillating behavior of C_3 will forbid the mitigation to take place as it goes below zero almost periodically.

system information and minimal effort can curate a cyber attack A_1 in Fig. 1, which has the same system impact and potential to disarm the existing cybersecurity technologies for microgrids.

Apart from the well-known security risks, instability problem arising from the cybersecurity perspective carries an elementary significance for future research. If the origin behind oscillations in DC microgrid can not be speculated, the established stability certificates in microgrids needs re-investigation. Hence, this paper provides a generalized approach for the first time to investigate the projection of cyber attacks on stability of DC microgrids. Firstly, we explain the modeling of stealth attacks and its inclusion principles into the small-signal model of a DC microgrid. Secondly using the cyber attack element as a non-linear input, we extend the describing function (DF) method to understand the origins of instability. Finally, we propose the adaptive stabilization scheme using the positive-definite detection metric in (11) to mitigate the unstable state caused by cyber attacks. This has been discussed in detail in the next section.

III. Modeling and Stability Analysis of Attacked DC Microgrid

A. Modeling of Attacked DC Microgrid

A detailed model of a DC microgrid under stealth cyber attacks needs to be established. The FDI attacks are usually introduced into the control systems using many well-defined intrusion approaches. As theoretically validated and concluded in [16], injecting a balanced set of zero sum attacks into different voltage references will not affect the steady-state performance of the microgrid. However, the mechanism behind the cause of instability due to unbounded stealth attack is unclear because of the lack of modeling generalization.

For a step change in the the false data $\mathbf{X}_a$ in (7), $\mathbf{u}_a$ can be regarded as a discontinuous variable related to time. As a result, this attack will introduce a set of non-linear input vectors into DC microgrid, thereby making it difficult to use the conventional small-signal stability analysis. Moreover, in a networked DC microgrid, cyber attack detection using (7) is an essential part, which corresponds to different non-zero values for various magnitudes of cyber attack elements. In this paper, an estimate of the nature of the cyber attack has been reverse engineered using the magnitude of C_i for mitigating the instability effectively. Hence, the model of detection part is also taken into consideration here. Hence, it is clear that the model of networked DC microgrid can be segregated into two parts, one being non-linear, which typically includes only the cyber attack input; and the other being linear.

In order to distinguish the positive and negative false data, the detection factor in (10) is re-written as:

$$f_i = h_i \sum_{j \in N_i} a_{ij}(\Delta V_{1j}(t-\tau) - \Delta V_{1i}(t)) \tag{12}$$

And the criterion for the detection of the attacked nodes can be given as:

$$f_i = \begin{cases} \neq 0, & \textbf{if } \kappa = 1 \\ 0, & \textbf{else} \end{cases} \tag{13}$$

By exploiting the distributed synchronization law [18] under stealth cyber attacks, $\mathbf{L}\bar{\mathbf{V}} = 0$. Using (13), we can employ the `sign` function to represent a balanced set of zero sum attacks, which is given by:

$$\mathbf{u^a} = \lambda[\mathrm{sgn}(f_1), \mathrm{sgn}(f_2), \ldots, \mathrm{sgn}(f_N)]^{\mathrm{T}} \tag{14}$$

where, $\mathbf{u^a} \in R^{N\times 1}$ denotes the input attack vectors and $\mathbf{F} = [(f_1), (f_2), \ldots, (f_N)]^{\mathrm{T}}$ denotes the vectors of simplified detection factors.

Before attaining the global model of the attacked DC microgrid, the expressions of the linear part are analyzed. In secondary controller, upon injection of stealth attacks, the average voltage estimated values will be affected, and can be represented as

$$\bar{\mathbf{V}}^{\mathbf{a}}(\mathbf{t}) = \bar{\mathbf{V}}(\mathbf{t}) + \mathbf{u^a} \tag{15}$$

where $\bar{\mathbf{V}}(\mathbf{t}) = [\bar{V}_1, \bar{V}_2, \ldots, \bar{V}_N]^{\mathrm{T}}$.

Then, the two voltage correction terms in (1) and (2) can be expressed as:

$$\mathbf{\Delta V_1(t)} = \mathbf{K_P^{H_1}}(\mathrm{V}_{\mathrm{dcref}}.\mathbf{1} - \bar{\mathbf{v}}^{\mathbf{a}}(\mathbf{t}) + \mathbf{K_I^{H_1}}\mathbf{\Sigma} \tag{16}$$

$$\mathbf{\Delta V_2(t)} = \mathbf{K_P^{H_2}}\boldsymbol{\delta} + \mathbf{K_I^{H_2}}\mathbf{\Delta} \tag{17}$$

where $\mathbf{\Delta V_1(t)} = [\Delta V_{11}, \Delta V_{12}, \ldots, \Delta V_{1N}]^{\mathrm{T}}$, $\mathbf{\Delta V_2} = [\Delta V_{21}, \Delta V_{22}, \ldots, \Delta V_{2N}]^{\mathrm{T}}$; $\mathbf{1}$ is a unit column matrix; $\boldsymbol{\delta} = [\delta_1, \delta_2, \ldots, \delta_N]^{\mathrm{T}}$; $\dot{\mathbf{\Sigma}} = (\mathrm{V}_{\mathrm{dcref}}.\mathbf{1} - \bar{\mathbf{v}}^{\mathbf{a}}) = [\Sigma_1, \Sigma_2, \ldots, \Sigma_N]^{\mathrm{T}}$; $\dot{\mathbf{\Delta}} = \delta = [\Delta_1, \Delta_2, \ldots, \Delta_N]^{\mathrm{T}}$. Further, $\mathbf{K_P^{H_1}} = diag\{K_P^{H_1}\}$ and $\mathbf{K_I^{H_1}} = diag\{K_I^{H_1}\}$ are the proportional and integral gains for the voltage controller matrices $\mathbf{H_{PI}^v}$ in secondary control layer; $\mathbf{K_P^{H_2}} = diag\{K_P^{H_2}\}$ and $\mathbf{K_I^{H_2}} = diag\{K_I^{H_2}\}$ are the proportional and integral gains for the current regulator $\mathbf{H_{PI}^i}$ in the secondary control layer.

Furthermore, the duty cycle $\mathbf{d(t)}$ can be obtained by:

$$\mathbf{d(t)} = \frac{\mathbf{K_P^I}(\mathbf{I_{inref}(t)} - \mathbf{I_L(t)}) + \mathbf{K_I^I}\mathbf{\Xi(t)}}{\mathbf{T_s F_m}} \tag{18}$$

where, $\dot{\mathbf{\Xi}}(\mathbf{t}) = \mathbf{I_{inref}(t)} - \mathbf{i_L(t)}$ and $\mathbf{I_{inref}(t)} = \mathbf{K_P^V}(\mathbf{V^*(t)}$ - $\mathbf{V}_{dc}(t)) + \mathbf{K}_I^V \int(\mathbf{V}^*(t) - \mathbf{V}_{dc}(t))dt$; $\mathbf{V^*(t)}$ and $\mathbf{I_L(t)}$ denote the column vectors of the local voltage references in (5) and inductor currents, respectively. $\mathbf{K_P^V}$ and $\mathbf{K_I^V}$ are diagonal matrices with PI controller gains to compensate the local voltage error while $\mathbf{K_P^I}$ and $\mathbf{K_I^I}$ are diagonal matrices with PI controller gains to compensate the local current error. $\mathbf{F_m}$

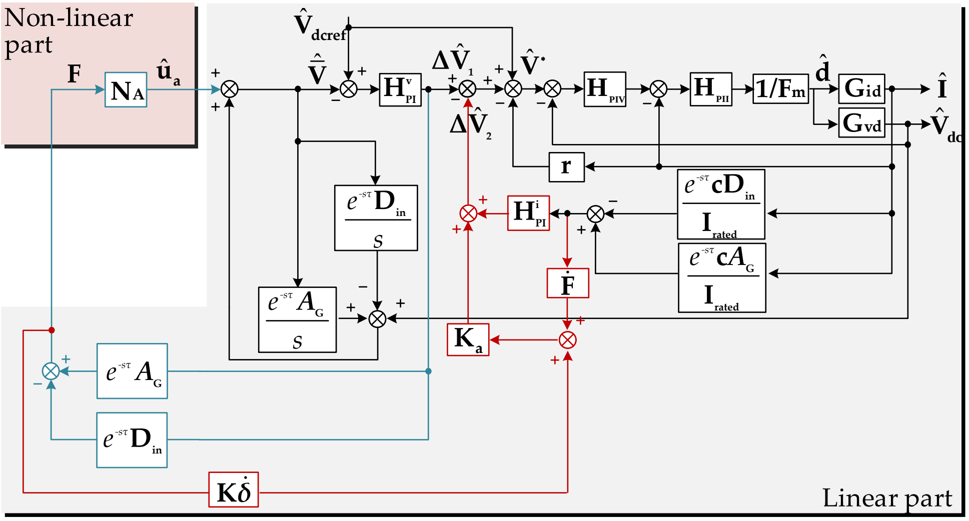


Fig. 5. Small-signal diagram of the attacked dc microgrid under steatlh cyber attack – the non-linear part includes cyber attack modeled as an undeterministic disturbance.

is the diagonal matrix of modulator gains; $\mathbf{T_s}$ is the diagonal matrix of switching periods for N converters.

Further, the representation for DC/DC buck converters as well as transmission lines can be given by:

$$\begin{cases} \mathbf{\dot{I}_L(t) = \frac{V_{in}(t)}{L_f} - (1 - d(t))\frac{V_{dc}(t)}{L_f}} \\ \mathbf{\dot{V}_{dc}(t) = (1 - d(t))\frac{I_L(t)}{C_f} - \frac{I_{load}(t)}{C_f}} \\ \mathbf{+M^T I_{br}(t)} \\ \mathbf{\dot{I}_{br}(t) = \frac{V_{br}(t)}{L_b} - \frac{I_{br}(t)R_b}{L_b}} \\ \mathbf{\dot{V}_{br}(t) = MV_{dc}(t)} \end{cases} \tag{19}$$

where, $\mathbf{V_{in}(t)}$ and $\mathbf{I_{load}}$ denote the column vector of input voltages and load currents from each agent; $\mathbf{V_{br}(t)}$ and $\mathbf{I_{br}(t)}$ are the column vectors of node voltages across each agent and transmission line currents between the agents; $\mathbf{L_f}$ and $\mathbf{C_f}$ are the diagonal matrices of filter inductors and capacitors for agents; $\mathbf{L_b}$ and $\mathbf{R_b}$ are the the diagonal matrices of transmission line inductance and resistance respectively. Finally, the physical graph connectivity matrix $\mathbf{M} = \{m_{ij}\}$ is an incidence matrix, where m_{ij} = 1, if line current leaves DG; m_{ij} = -1 if the line current enters DG; and 0, otherwise.

Finally, (16)-(19) are perturbed and separated into steady state and small signal equations. Neglecting the higher order terms in the small-signal equations, the model of linearized part for the DC microgrid with N agents is given by:

$$\begin{cases} \mathbf{\dot{\hat{\hat{V}}}(t) = \dot{\hat{V}}_{dc}(t) - L\hat{V}(t - \boldsymbol{\tau}) + \dot{\hat{u}}^a} \\ \mathbf{\hat{\boldsymbol{\delta}}(t) = -L\frac{\hat{I}(t-\boldsymbol{\tau})}{I_{rated}}} \\ \mathbf{\Delta\dot{\hat{V}}_1(t) = -K_p^{H_1}\dot{\hat{V}}_{dc}(t) - K_I^{H_1}\hat{\hat{V}}(t)} \\ +\mathbf{K}_P^{H_1}\mathbf{L}\hat{\hat{\mathbf{V}}}(t - \boldsymbol{\tau}) \\ \mathbf{\Delta\dot{\hat{V}}_2(t) = -K_P^{H_2}L\dot{\hat{I}}(t - \boldsymbol{\tau}) - K_I^{H_2}L\hat{I}(t - \boldsymbol{\tau})} \\ \mathbf{\hat{V}^*(t) = \Delta\hat{V}_1(t) + \Delta\hat{V}_2(t)} \\ \mathbf{\dot{\hat{I}}(t) = \frac{\hat{V}_{in}(t)}{L_f} - \frac{\hat{V}_{dc}(t)}{L_f} + \frac{V_{dc}\hat{d}(t)}{L_f}} \\ + \frac{\mathbf{D}_{on}\hat{\mathbf{V}}_{dc}(t)}{\mathbf{L}_f} \\ \mathbf{\dot{\hat{V}}_{dc}(t) = \frac{\hat{I}(t)}{C_f} - \frac{D_{on}I(t)}{C_f} - \frac{I\hat{d}(t)}{C_f} - \frac{\hat{I}_{load}(t)}{C_f}} \\ \mathbf{\hat{V}_{br}(t) = M\hat{V}_{dc}(t)} \\ \mathbf{\dot{\hat{I}}_{br}(t) = \frac{\hat{V}_{br}(t)}{L_{br}} - \frac{R_{br}\hat{I}_{br}(t)}{L_{br}}} \\ \mathbf{\hat{d}(t) = \frac{K_P^I(\hat{I}_{inref}(t) - \hat{I}(t)) + K_I^I\hat{\Xi}(t)}{T_sF_m}} \\ \mathbf{\dot{\hat{\Xi}} = \hat{I}_{inref}(t) - \hat{I}(t)} \end{cases} \tag{20}$$

The complete model of DC microgrid in (20) can then be translated to the s-domain. In the small-signal diagram shown in Fig. 11, $\{\mathbf{H^v_{PI}}, \mathbf{H^i_{PI}}\}$, $\{\mathbf{H_{PIV}}, \mathbf{H_{PII}}\}$ are transfer functions of the average voltage regulator, proportionate current sharing, inner voltage and current loop PI compensators for different agents in diagonal matrix form, respectively. On the other hand, $\mathbf{G_{id}}$ and $\mathbf{G_{vd}}$ represent the plant transfer function of inductors and capacitors for different agents in diagonal matrix form, respectively.

B. Stability Analysis of Attacked DC Microgrid

As it can be seen in Fig. 11, the global model of attacked DC microgrid includes a non-linear and a linear part. As a result, the small-signal stability analysis is not feasible anymore. Hence, the describing function (DF) method [33] is adopted in this paper to investigate the stability of microgrid under the presence of cyber attacks. This method is one of the most effective tools present in the literature, which linearize the non-linear system for average variables using the equivalent gain theory [34]. It is an efficient frequency domain tool to study the stability of discontinuous non-linear elements. The basic philosophy involves obtaining an output with the first harmonic component when the nonlinear function is conjoined with a sinusoidal input $x = A\sin(\omega t)$. We consider the first harmonic component of the output of the non-linear element based on the following hypothesis:

1) The non-linear part is odd-symmetric.

2) The linear part is low-pass.

which holds true for the considered case study in Fig. 5. Denoting the approximate transfer function of the non-linear part as N_{A}, the whole system can be roughly transformed into a linear system in the frequency domain with a variable gain amplifier N_{A}, as shown in Fig. 6.

Therefore, the system with a non-linear input can be approximately transformed into a linear system in the frequency domain with a variable gain amplifier N_{A} [33]. By checking the relationships between $-1/N_{\mathrm{A}}$ and the linear part $G(s)$ as shown in Fig. 7, the stability of the system can be adjudged.

We exploit the model of stealth cyber attacks in (14) as `sign` functions to extend our analysis. According to the definition, the DF of the `sign` function can be given by:

$$N_{\mathrm{A}} = \frac{4}{\pi A} \tag{21}$$

Moreover, according to the small signal diagram shown in Fig. 11, the transfer function of the linear part can be deduced, which can be given by:

$$\mathbf{G} = \frac{(e^{-s\tau}\boldsymbol{A}_{\mathbf{G}}\boldsymbol{\lambda} - e^{-s\tau}\mathbf{D_{in}}\boldsymbol{\lambda})\mathbf{H_{PI}^{v}}\mathbf{G_1}}{(\mathbf{1}+\boldsymbol{\Theta}-\boldsymbol{\Omega})\,\mathbf{G_1}+\mathbf{H_{PIV}}\mathbf{H_{PII}}\mathbf{G_{vd}}\mathbf{G_K}\mathbf{H_{PI}^{v}}} \tag{22}$$

where, $\mathbf{G_1} = \mathbf{F_m} + \mathbf{H_{PII}}\mathbf{G_{id}} + \mathbf{H_{PIV}}\mathbf{H_{PII}}\mathbf{G_{vd}} + \mathbf{H_{PIV}}\mathbf{H_{PII}}\mathbf{G_{id}}\mathbf{r} + \mathbf{H_{PIV}}\mathbf{H_{PII}}(\frac{\mathbf{c}\boldsymbol{A}_{\mathbf{G}}e^{-s\tau}}{\mathbf{I_{rated}}} - \frac{\mathbf{c}\mathbf{D_{in}}e^{-s\tau}}{\mathbf{I_{rated}}})\mathbf{G_{id}}\mathbf{H_{PI}^{i}}$ and $\mathbf{K} = 2(\boldsymbol{A}_{\mathbf{G}}e^{-s\tau} + \mathbf{D_{in}}e^{-s\tau})$, $\mathbf{G_K} = (\mathbf{1} - \mathbf{K}\mathbf{K_a})$. Moreover, $\boldsymbol{\Omega} = \frac{e^{-s\tau}\boldsymbol{A}_{\mathbf{G}}}{s}$ and $\boldsymbol{\Theta} = \frac{e^{-s\tau}\mathbf{D_{in}}}{s}$.

Remark II: *The customization from the traditional Nyquist analysis is based on substituting the closed-loop stable reference s = –1 + j0 with –1/N_A. Using this concept, the modified Nyquist criteria using the Cauchy's principle can be depicted as follows:*

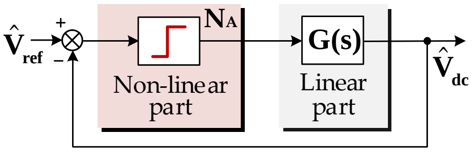
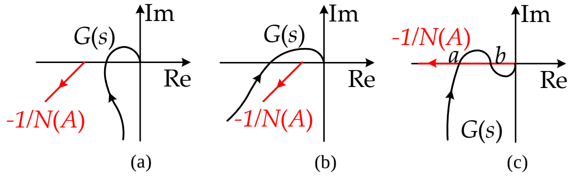

$\hat{\mathbf{V}}_{\mathbf{ref}}$
+
–
$\mathbf{N_A}$
Non-linear part
G(s)
Linear part
$\hat{\mathbf{V}}_{\mathbf{dc}}$

Fig. 6. Equivalent control diagram of Fig. 5 using the DF method.



(a) (b) (c)

Fig. 7. Stability certificates of the describing function – Relative position of $-1/N_{\mathrm{A}}$ and $G(s)$: (a) stable, (b) unstable, (c) critically stable.

1) If –1/N_A is not encircled by the contour of $G(s)$, the system is stable (as shown in Fig. 7(a)).

2) If –1/N_A is encircled by the contour of $G(s)$, the system is unstable (as shown in Fig. 7(b)).

3) For the system to be critically stable, –1/N_A should intersect with $G(s)$ such that the oscillation amplitude A_{osc} and frequency ω_{osc} is given by (as shown in Fig. 7(c)):

$$N_{A_{osc}} = 1/G_r(\omega_{osc}) \tag{23}$$

$$G_i(\omega_{osc}) = 0 \tag{24}$$

where, $G(j\omega) = G_r(\omega) + jG_i(\omega)$.

Using (21)-(22), the stability boundaries of the system were investigated for various magnitude of cyber attacks in (7), which triggered instability caused due to the proportional gain in $\mathbf{H_{PI}^{i}}$. One of the fundamental causes behind this instability could be ascribed to the interactions between converters arising due to lower attenuation properties from the controller when the voltage references are abruptly changed. Hence, the overall damping of the system is affected. This has been validated in Fig. 9(a) for a DC microgrid with N = 3 agents, where the stability margin improves as $\mathbf{K_P^{H_2}}$ is increased under the presence of cyber attacks. With a smaller value of $\mathbf{K_P^{H_2}}$ = 1, the intersected region is also small in Fig. 9(a) whereas with a relatively larger value of $\mathbf{K_P^{H_2}}$, it can be seen that $-1/N_{\mathrm{A}}$ & G(s) have no intersection. Further, $-1/N_{\mathrm{A}}$ is not surrounded by G(s), which indicates that the instability caused by cyber attacks is eliminated. As a result, this problem outlines the need of an adaptive feedforward input, where the adaptive behavior needs to be enforced, only if the cyber attacks are present. Hence, it becomes the basis of the design of the proposed stabilization approach, which is discussed in the next section.

IV. Proposed Adaptive Stabilization Approach

In this section, we will discuss about the design of the proposed stabilization approach. As outlined in the previous section, the origin of instability ascends from an improper design of the proportional gain of the current regulator $\mathbf{K_P^{H_2}}$. As a result, the system damping is affected. This provides a favorable condition to vary $\mathbf{K_P^{H_2}}$ in the secondary layer during cyber attacks. Hence, a novel adaptive gain mechanism is proposed in this paper, which exploits the positive-definiteness of the cooperative vulnerability factor C_i in (11) during attacks. As a result, when a stealthy group of cyber attack elements of any magnitude is injected into DC microgrid, the adaptive proportional gain of the current regulator will be given by:

$$\mathbf{K_P^{H_2}} = \mathbf{K_{P_{in}}^{H_2}} + \mathbf{K_a F} \tag{25}$$

where, $\mathbf{K_a}$ is a positive gain and $\mathbf{K_{P_{in}}^{H_2}}$ is the previously set value of the proportional gain in the current regulator. Moreover, $\mathbf{F}$ is directly proportional to the magnitude of cyber attack elements, which has already been established in [16]. As a result, a feedforward input from the cyber attack detection metric is introduced as an adaptive term in (25) to solve stability issues in microgrids arising from cyber attacks. Upon substituting (25) in (20), the current regulator output can be re-written as:

$$\boldsymbol{\Delta}\dot{\hat{\mathbf{V}}}_{\mathbf{2}}(\mathbf{t}) = (-\mathbf{L}\mathbf{K_{P_{in}}^{H_2}} - \mathbf{L}\mathbf{K_a}\dot{\mathbf{F}})\dot{\hat{\mathbf{I}}}(\mathbf{t}-\boldsymbol{\tau}) \tag{26}$$

Using (26), the system stability will now be investigated under different operating conditions. As the communicated signals into i^{th} agent in (26) will always be received with a time delay τ, the stability of the networked DC microgrid will be affected when this delay exceeds a certain value. This has been studied in Fig. 9(b), where the system performance is evaluated for different values of communication delay τ. It can be seen that with the introduction of communication delay, the system goes into an unstable condition using Remark II as τ is increased. This is quite evident as there is no intersection between the linear trajectory and the non-linear setpoint, which indicates that the system grows unstable with increasing τ.

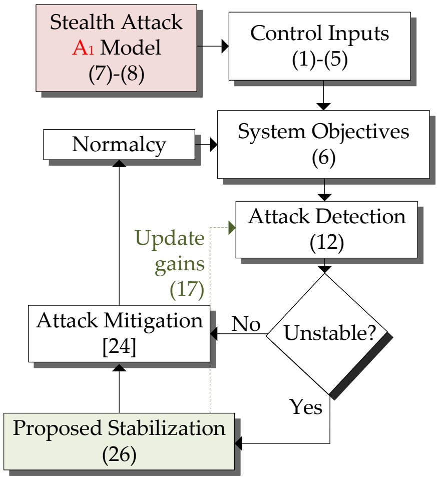


Fig. 8. Flowchart depicting the adaptive stabilization mechanism under the presence of cyber attacks A_1 in Fig. 1 – this mechanism ensures that the equipped cybersecurity technologies [24], [29] operate impartially.

The stability framework outlined in Remark II will now be used to investigate the system stability under stealth cyber attacks for different operating conditions in DC microgrids. A clear description of the step-by-step design procedure of the proposed countermeasure has been provided in the flowchart in Fig. 8. Before subjecting to the describing function method based analysis, the bode plot of linear part of the system is firstly studied in Fig. 9(c). In Fig. 9(c), the peak value of $K_\text{a} = 1$ is larger than the peak value of $K_\text{a} = 3$, which means that the overshoot will be larger when $K_\text{a} = 1$. Moreover, the bandwidth of using $K_\text{a} = 1$ is larger than that of using $K_\text{a} = 3$, which adjudges that the transient performance for $K_\text{a} = 1$ is better. Therefore, a design trade-off of K_a has to be instinctively comprehended between the overshoot in voltages and converter's transient performance during cyber attacks.

In Fig. 10(a), it can be seen that $-1/N_\text{A}$ is intersected by $G(s)$, which indicates that the system is unstable. With the decrease in load, it can be seen that the intersection region becomes larger, thereby making the system more unstable. This confirms our assertion on low system damping contributing to this instability. Furthermore, it is observed from Fig. 10(b) that with λ = 25, the considered DC microgrid almost becomes unstable upon examining the relationship between $-1/N_\text{A}$ and $G(s)$ in Remark II. With the increase in the value of λ, the intersection region becomes even larger, leading to further instability. Hence, it can be concluded that an attacked DC microgrid is highly vulnerable to instability under low loading levels and large values of stealth cyber attacks. In Fig. 10(c), the impact of communication delay on microgrid stability during cyber attacks is investigated, while the proposed stabilization approach is active. With different values of τ and the proposed stabilization approach active with $\mathbf{K_a}$ = 2, the Nyquist diagrams in Fig. 10(c) suggest that the system is always stable, since there is no intersection between the linear part and nonlinear part.

After conducting numerous simulations, it can be seen in Fig. 11(a) that when the global voltage reference is varied from 45 V to 315 V with D = 0.3, the difference among the values of λ, which make the system unstable is quite small. In Fig. 11(b), it can be concluded that when the stabilization gain K_a is very small, i. e., 0.1, the provided stabilization function can not fully eliminate the instability caused by a large valued λ. In addition, the stability region of λ-K_a for dc microgrid in Fig. 11(c) with more converters will be narrower than others, which means it will take larger value of K_a to destabilize a microgrid with more converters. Fig. 11(d) indicates that with smaller $\mathbf{K_P^{H_1}}$ in voltage observer, the microgrid with the proposed stabilization method is more likely to be stable against the stealth attacks. Hence, K_a needs to be selected appropriately considering the abovementioned factors to ensure adaptive stabilization for any given λ.

V. Simulation Results

The proposed stabilization approach is tested on cyber-physical DC microgrid, as shown in Fig. 2 with N = 3 converters for a global reference of 315 V. Each agent of equal power capacity (10 kW each) comprising of a DC source and DC/DC buck converter operate to regulate the output voltage to a local reference value of V_i^* at their respective buses. First, its performance is gauged under stealth attacks for different values of $\mathbf{K_a}$. Then, its performance is validated under large and random communication delay between the converters, which explicitly affects the stability of microgrids. The simulated plant and control parameters are provided in the Appendix.

In the first scenario, the performance of DC microgrids is tested in Fig. 12 under the presence of stealth cyber

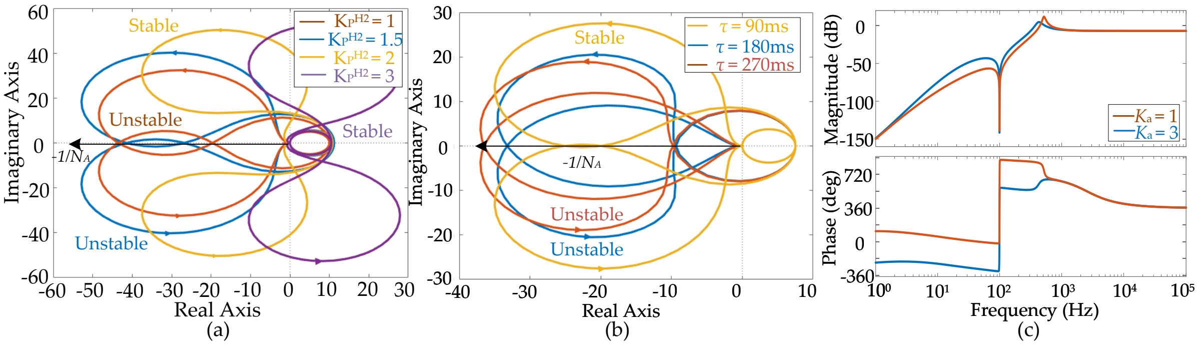


Fig. 9. Stability certificates of DC microgrid under different operating conditions – (a) For increasing $\mathbf{K_P^{H_2}}$, the Nyquist plot suggests that the system traverses from critically damped to overdamped condition, (b) the system goes into an unstable condition as the max. communication delay in the network goes beyond 180 ms, (c) the bode plot highlights the dynamic performance trade-off for different values of K_a.

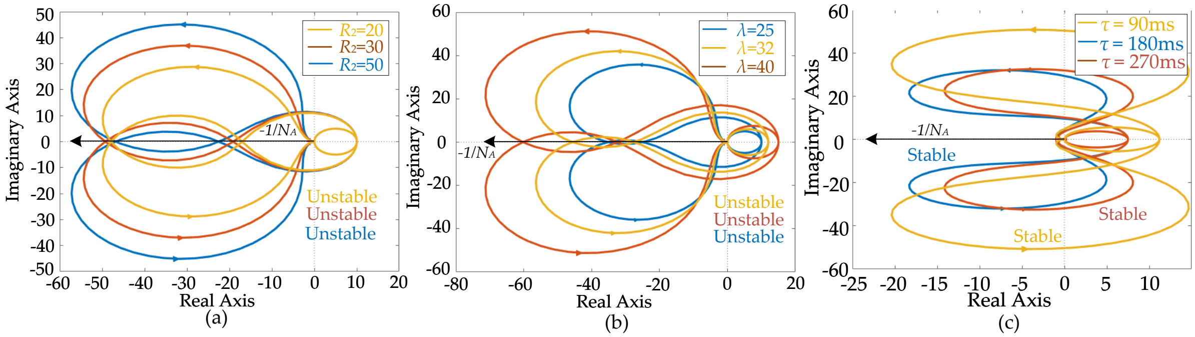


Fig. 10. Stability validation of DC microgrids employed with the proposed adaptive stabilization approach under (a) different loading conditions, (b) under different magnitude of cyber attack elements, and (c) different values of communication delay τ.

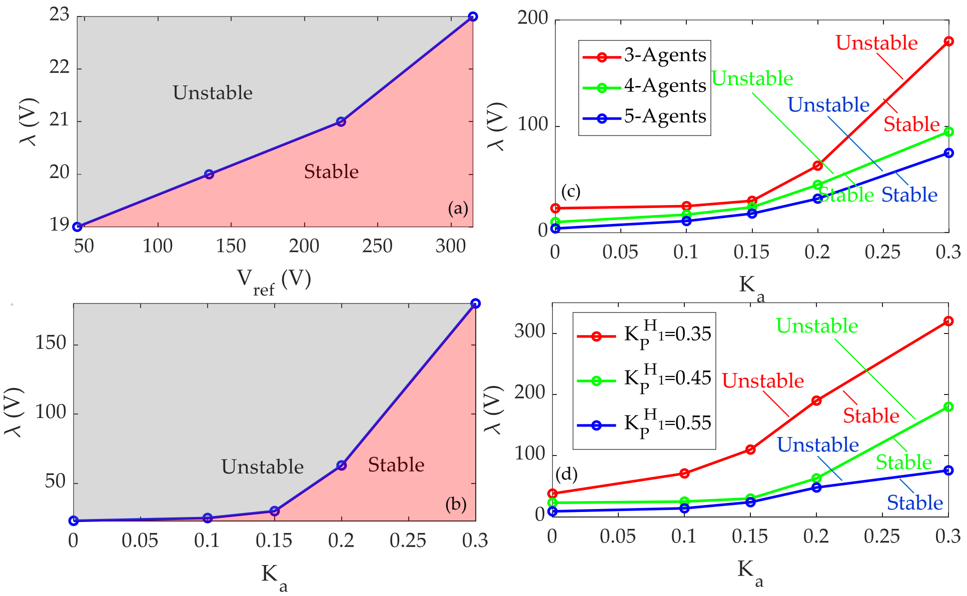


Fig. 11. Stability boundaries of the relationship between the attack element λ and system parameters, such as (a) global voltage reference V$_{ref}$, (b) adaptive stabilization gain K$_a$. The stability boundaries to verify the relationship between K$_a$ with respect to different values of λ in a system with different: (c) number of agents, (d) proportional gains in the compensator of the voltage observer in Fig. 2.

attack (with a magnitude of λ = 32 V in converter I and III) with and without the proposed stabilization approach. In Fig. 12(a), once the stealth attack is initiated at t = 2 sec, the microgrid immediately becomes unstable with oscillating currents from each source. It should be noted that the proposed stabilization approach is absent in Fig. 12(a). However, when it is introduced in Fig. 12(b)-(c), it can be seen that the stabilization update $\mathbf{K_a F}$ for the attacked converters vary for

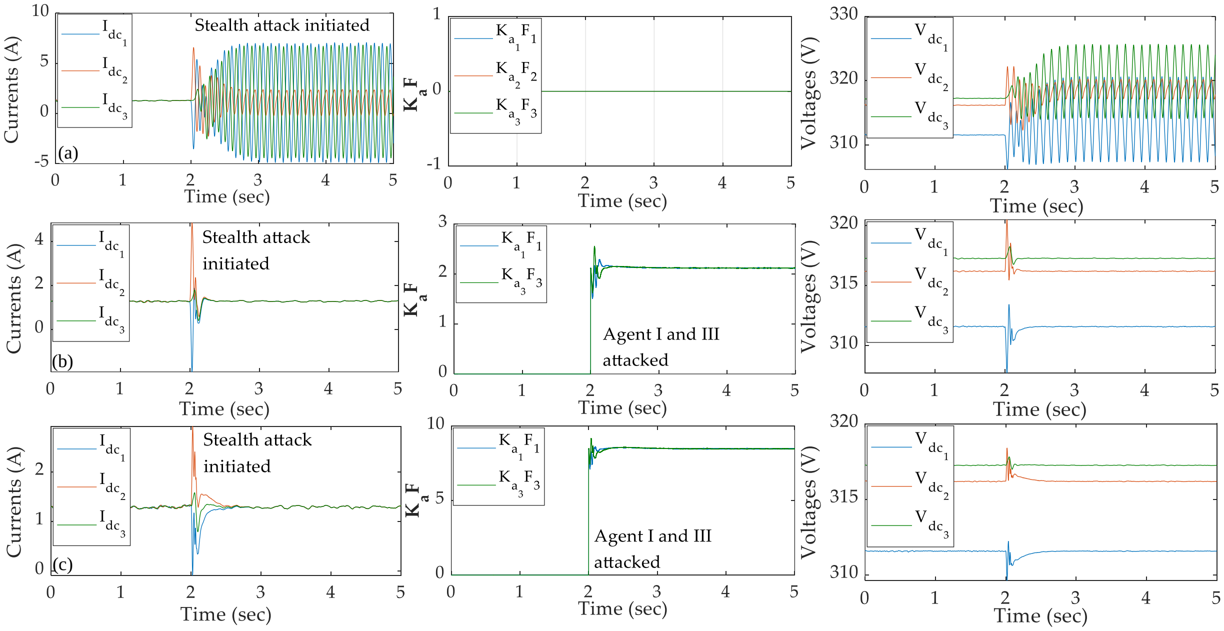


Fig. 12. Performance of DC microgrid comprising N = 3 agents with stealth cyber attack (λ = 32 V) simultaneously initiated on converter I and III at t = 2 sec, when: (a) $\mathbf{K_a}$ = 0, (b) $\mathbf{K_a}$ = 5, (c) $\mathbf{K_a}$ = 15.

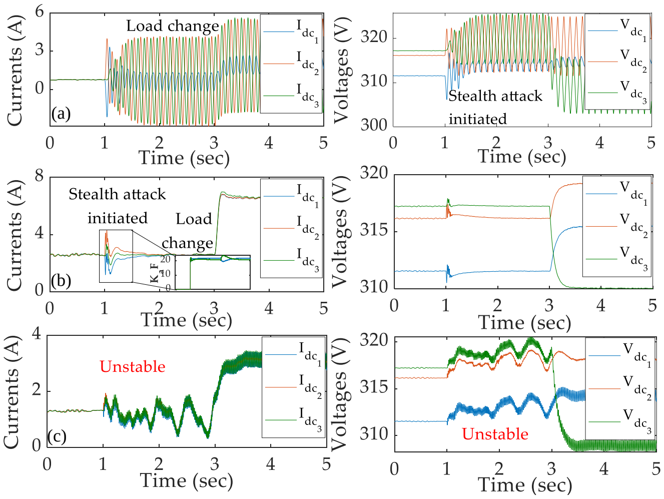


Fig. 13. Performance of DC microgrid comprising N = 3 agents with stealth cyber attack (λ = 40 V) simultaneously initiated at t = 1 sec under a maximum communication delay τ_{max} of 150 ms, when: (a) $\mathbf{K_a}$ = 0, (b) $\mathbf{K_a}$ = 15, (c) $\mathbf{K_a}$ = 45 – higher gain of $\mathbf{K_a}$ renders the system unstable, which could be governed using the time-delay analysis.

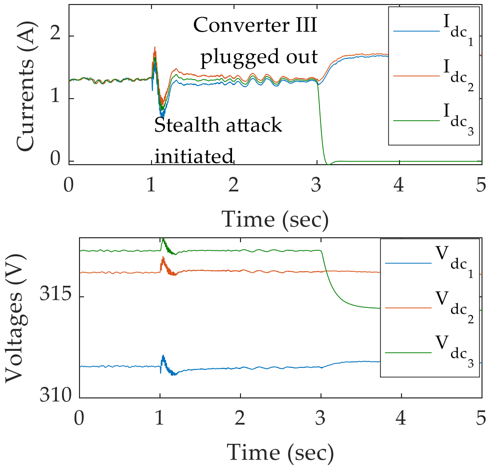


Fig. 14. Performance of DC microgrid when converter III is plugged out at t = 3 sec under the presence of stealth attacks with $\mathbf{K_a}$ assigned to 10 – the proposed adaptive stabilization approach is able to manage large-signal disturbances.

the same attack magnitude, owing to different stabilization gains $\mathbf{K_a}$. Furthermore, the adaptive behavior of this update can be ascribed to the cyber attack detection metric $\mathbf{F}$, which varies proportionately in relation with λ. It can be seen that as $\mathbf{K_a}$ increases, the dynamic response with reduced overshoots. Although the settling time increases with increasing $\mathbf{K_a}$, it can not be a governing factor since secondary control layer typically demands steady-state error convergence in order of few seconds.

In the second scenario, the performance of DC microgrids is tested in Fig. 13 under the presence of stealth cyber attacks and a communication delay of 150 ms. Since time delay in exchange of information between converters already affects the stability of microgrids, the presence of cyber attack may further trigger this problem and may cause instability even for a small delay. In fact, this aspect has been validated in Fig. 13(a) that even for a delay of 150 ms, stealth cyber attack (introduced as a step change) has made the system unstable by causing an oscillatory behavior. It is worth notifying that the time-delay stability of the same system guarantees stability upto a communication delay of 325 ms without cyber attacks [27]. However, when the proposed stabilization approach ($\mathbf{K_a}$ = 15) is activated in Fig. 13(b), it can be seen that the system operates normally with the current being shared proportionately and the voltages regulated as per the dynamic consensus principle. It is intuitive that with the increase in the stabilization gain $\mathbf{K_a}$, the dynamic response is improved. However in Fig. 13(c), it has been shown that high-frequency oscillations arise when the value of $\mathbf{K_a}$ is increased to 45. As a result, we can conclude that the design of the stabilization gain should always be limited within a defined value, which can be calculated using the time-delay stability analysis of (20). This aspect has not been discussed in this paper for the purpose of brevity.

In the third scenario, the plug-and-play capability of the DC microgrid with the proposed stabilization approach is tested. The idea behind doing so is to investigate its response for a large-signal disturbance. In Fig. 14, it can be seen that in addition to its stabilization properties under stealth cyber attacks, the proposed stabilization approach provides robust operation, when converter 3 is plugged out of the microgrid at t = 3 sec. As a consequence, the remaining converters share the load equally, as their output current rise immediately. Moreover, it doesn't affect the secondary voltage controller, as the average voltages are still regulated to the global reference of 315 V.

VI. Experimental Results

The proposed stabilization approach has been experimentally validated in a DC microgrid operating at a voltage reference V_{dcref} of 48 V with N = 2 buck converters, as shown in Fig. 15. A single line diagram of the experimental setup is also shown in Fig. 16. 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 stabilization approach shown in Fig. 2 is incorporated into both the distributed controllers to mitigate the stability and cyber-security concerns, simultaneously. The experimental testbed parameters are provided in Appendix.

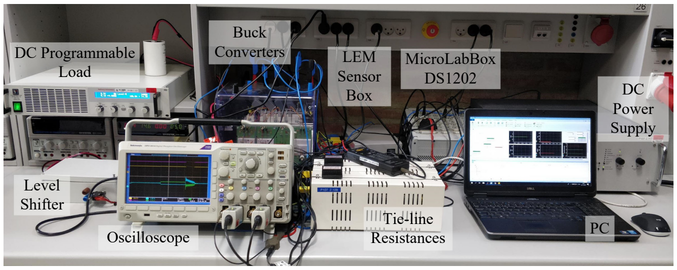


Fig. 15. Experimental setup of a cooperative DC microgrid comprising of N = 2 agents controlled by dSPACE MicroLabBox DS1202 supplying power to the programmable load.

Firstly, we investigate its performance on a simulation replica of the experimental setup in Fig. 15. It can be seen in Fig. 17 that when a stealth cyber attack (with a magnitude λ of 18 V) is injected simultaneously into both converters at t = 2 sec, oscillations occur. However, when the stabilization method is introduced at t = 3 sec, the instability is mitigated, which illustrates that the stabilization method is adapted in a wide range of power applications. In Fig. 18(a), the instability problem due to stealth cyber attack is firstly validated, where the output current start oscillating when the stealth cyber attack (with a magnitude λ of 18 V) is injected simultaneously into both converters. It is worth notifying that the proposed stabilization approach is not active in Fig. 18(a). Carrying on with the same stealth cyber attack scenario in Fig. 18(a) where the currents and voltages are oscillating, the stabilization update when activated in Fig. 18(b) not only mitigates the oscillations, but also provides good dynamic performance under physical disturbances later. This has been validated in Fig. 18(b) and (c), where the system operates normally even under load changes and presence of the cyber attack A_1. It is worth notifying that the adaptive feedforward update can be extended to mitigate unstable modes induced by any class of FDIAs, which has been theoretically validated in Section IV. As a result, it has been guaranteed that the proposed stabilization approach not only mitigates the instability caused by cyber intrusions, but also contributes to the previously defined cybersecurity framework of microgrids. From an implementation perspective, this mechanism can be introduced as a plug-and-play tool alleviating the commercialization in practical field applications.

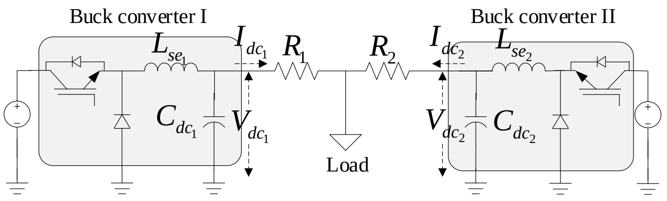


Fig. 16. Single line diagram of the experimental setup shown in Fig. 15.

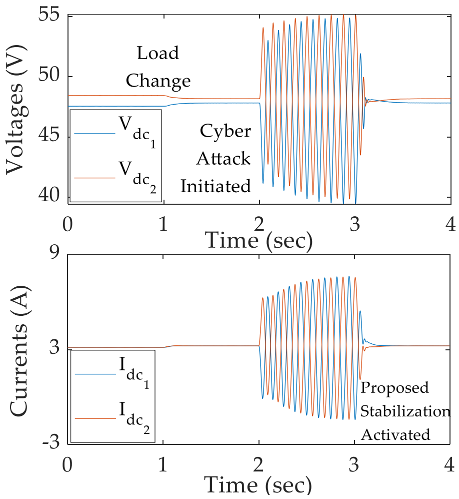


Fig. 17. Simulated replica of DC microgrid in Fig. 15 with stealth cyber attack (λ = 18 V) simultaneously initiated at t = 2 sec – the oscillation is mitigated as soon as the proposed stabilization approach is activated at t = 3 sec.

VII. Conclusions and Future Scope of Work

As cyber attacks affect the operation and stability of cyber-physical microgrids, it is increasingly important to assess the threat from a security as well as stability perspective,

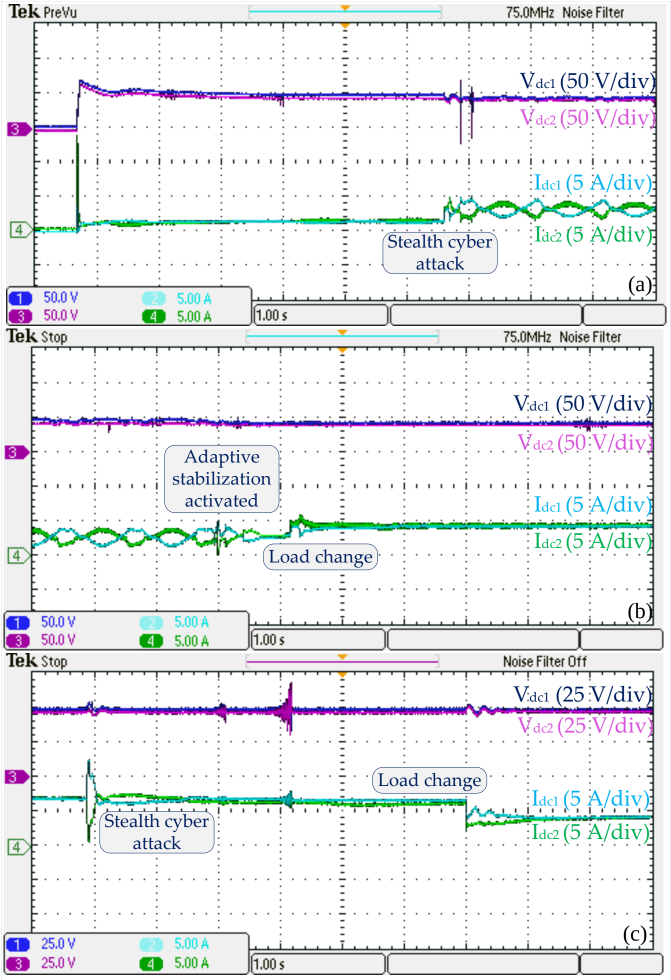


Fig. 18. Experimental results to showcase the operation of experimental prototype of DC microgrid in presence of stealth attacks: (a) Without any stabilization measures, (b) with the proposed adaptive stabilization method for a communication delay of 150 ms, and (c) load change.

simultaneously. Hence, this paper firstly analyzes the limited resources problem of cyber attacks, which has the potential of causing a big impact on the system. It has been identified that a carefully curated pair of cyber attack (without much disruption resources) can not only compromise the system security but can also make it unstable. This kind of instability clearly diverges from the established stability definitions and certificates for microgrids. To address this gap, this paper provides the modeling principles of such cyber attacks, which directly affects the system stability. It has been analyzed using the describing function method to reveal the cause of instability and then establish an adaptive stabilizing mechanism. Since cyber attacks highly contribute to this problem, the cyber attack detection metric is used to provide a stabilizing effect and adapting its behavior accordingly as per the magnitude of cyber attack. Alongside theoretical analysis, its rugged performance is tested in simulation and then validated in an experimental prototype. Since the pre-defined cyber attack detection metric is exploited directly in the adaptive feedforward update for mitigating stability and security issues, it can be readily introduced as a plug-and-play tool for commercialization purposes. Further focus will be provided on investigating the sensitivity analysis of the adaptive gain with respect to different system parameters, topologies and operating conditions. We further aim to investigate to model high resolution approaches to investigate instability due to DoS attacks.

Appendix

Simulation Parameters

The considered system consists of three converters rated equally for 10 kW. It is to be noted that the line parameter R_{ij} is connected from the i^{th} agent to the j^{th} agent. Moreover, the controller gains are identical for each converter.

Plant: R_{12} = 1.5 Ω, R_{23} = 1.2 Ω, R_{13} = 0.8 Ω

Converter: L_{se_i}= 3 mH, C_{dc_i}= 250 μF, $I_{dc_{min}}$ = 0 A, $I_{dc_{max}}$ = 28 A, $V_{dc_{min}}$ = 270 V, $V_{dc_{max}}$ = 360 V

Controller: V_{dcref}= 315 V, I_{dcref} = 0, K_P^v = 1.92, K_I^v = 15, K_P^i = 4.5, K_I^i = 0.08, $K_P^{H_1}$ = 0.00002, $K_I^{H_1}$ = 0.45, $K_P^{H_2}$ = 4, $K_I^{H_2}$ = 28.8, h_i = 2.5, K_a = 15.

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_{dcref}= 48 V, I_{dcref} = 0, K_P^v = 1.92, K_I^v = 15, K_P^i = 4.5, K_I^i = 0.08, $K_P^{H_1}$ = 0.0005, $K_I^{H_1}$ = 6.4, $K_P^{H_2}$ = 2.8, $K_I^{H_2}$ = 16, h_i = 0.8, K_a = 5.

References

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

[2] M. Yazdanian, and A. Mehrizi-Sani, "Distributed control techniques in microgrids," *IEEE Trans. Smart Grid.*, vol. 5, no. 6. pp. 2901–2909, Nov. 2014.

[3] S. Sahoo and S. Mishra, "A distributed finite-time secondary average voltage regulation and current sharing controller for DC microgrids," *IEEE Trans. Smart Grid.*, vol. 10, no. 1, pp. 282–292, Jan. 2019.

[4] T. Dragicevic, X. Lu, J. C. Vasquez, and J. M. Guerrero, "DC microgrids-part I: a review of control strategies and stabilization Techniques," *IEEE Trans. Power Electron.*, vol. 31, pp. 4876–4891, Jul. 2016.

[5] "Hackers hit US power utilities with a cyberattack," Available: https://www.wired.com/story/power-grid-cyberattack-security-news, Jul. 2019.

[6] Electricity Information Sharing and Analysis Center. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. [Online]. Available: https://ics.sans.org/media/E-ISAC-SANS-Ukraine-DUC-5.pdf.

[7] [Online] "Cyber-Physical Security Initiative by IEEE PELS", Available: https://ieee-pels.org/programs-projects/cyber-physical-security-initiative

[8] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," *IEEE Journ. Emerg. Sel. Topics Power Electron.*, 2019.

[9] M. Greidanus, S. Sahoo, S. Mazumder, F. Blaabjerg, "Novel control solutions for DoS attack delay mitigation in grid connected and standalone inverters", *2021 Intl. Symp. Power Electron. for Dist. Gen. Syst. (PEDG)*, pp. 1-5, 2021.

[10] L. Guo, J. Ye and B. Yang, "Cyber-Attack Detection for Electric Vehicles Using Physics-Guided Machine Learning," *IEEE Trans. Transport. Electr.*, 2020. DOI: 10.1109/TTE.2020.3044524.

[11] A. Greenburg, "Hackers remotely kill a Jeep on the highway - with me in it," Available: https://www.wired.com/2015/07/hackers-remotely-killjeep-highway/, Tech. Rep., Jul. 2015.

[12] "Cyber attacks in connected cars: what Tesla did differently to win," [Online]. Available: https://www.appknox.com/blog/cyber-attacksin-connected-cars, Tech. Rep., Sep. 2017.

[13] S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE Trans. Ind. Inform.*, vol. 15, no. 7, pp. 4066–4075, July 2019.

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

[15] J. Ye, et. al., "A review of cyber-physical security in photovoltaic systems," *Journ. Emerg. Sel. Topics Power Electron.*, 2021.

[16] 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, Aug. 2019.

[17] S. Sridhar, M. Govindarasu, and C. C. Liu, "Risk analysis of coordinated cyber attacks in the power grid," *Contr. & Optim. Methods for Electr. Smart Grid*, vol. 275-294, Springer, 2012.

[18] 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, Aug. 2020.

[19] A. Mustafa, B. Poudel, A. Bidram and H. Modares, "Detection and mitigation of data manipulation attacks in AC microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2588-2603, May 2020.

[20] Q. Zhou, M. Shahidehpour, A. Alabdulwahab and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3690-3701, Sept. 2020.

[21] A. Saad, S. Faddel, T. Youssef and O. A. Mohammed, "On the implementation of IoT-Based digital twin for networked microgrids resiliency against cyber attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5138-5150, Nov. 2020.

[22] 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, 2018.

[23] S. Sahoo, T. Dragičević and F. Blaabjerg, "Multilayer resilience paradigm against cyber attacks in dc microgrids," *IEEE Trans. Power Electron.*, vol. 36, no. 3, pp. 2522– 2532, Mar. 2021.

[24] S Sahoo, T. Dragičević and F. Blaabjerg, "An event-driven resilient control strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 35, no. 12, pp. 13714-13724, 2020.

[25] A. Teixeira, I. Shames, H. Sandberg, K. H. Johansson, "A secure control framework for resource-Limited adversaries," *Automat.*, vol. 51, pp. 135-148, 2015.

[26] M. Farrokhabadi, "Microgrid stability definitions, analysis, and examples" *IEEE Trans. Power Sys.*, vol. 35, no. 1, pp. 13-29, 2019.

[27] S. Sahoo and F. Blaabjerg, "A model-free predictive controller for networked microgrids with random communication delays," *2021 IEEE Applied Power Electron. Conf. and Expo. (APEC)*, 2021, pp. 2667-2672, doi: 10.1109/APEC42165.2021.9487438.

[28] Y. Li, P. Zhang and M. Yue, "Networked microgrid stability through distributed formal analysis", *Applied Energy*, vol. 228, pp. 279-288, 2018.

[29] M. S. Sadabadi, S. Sahoo, and F. Blaabjerg, "Stability oriented design of cyber attack resilient controllers for cooperative DC microgrids," *IEEE Trans. Power Electron.*, vol. 37, no. 2, pp. 1310-1321, 2021.

[30] A. Cecilia, S. Sahoo, T Dragicevic, R. Costa, F. blaabjerg, "On Addressing the Security and Stability Issues Due to False Data Injection Attacks in DC Microgrids — An Adaptive Observer Approach," *IEEE Trans. Power Electron.*, vol. 37, no. 3, pp. 2801-2814, 2022.

[31] M. Leng, S. Sahoo and F. Blaabjerg, "Stability investigation of DC microgrids under stealth cyber attacks," *2021 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2021, pp. 1427-1432.

[32] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "Resilient operation of heterogeneous sources in cooperative DC microgrids," *IEEE Trans. Power Electron.*, vol. 35, no. 12, pp. 12601-12605, 2020.

[33] V. Lanza, M. Bonnin, and M. Gilli, "On the application of the describing function technique to the bifurcation analysis of nonlinear systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 54, no. 4, pp. 343–347, 2007.

[34] E. Vidal, A. Poveda, and M. Ismail, "Describing functions and oscillators," *IEEE Circuits Devices Mag.*, vol. 17, no. 6, pp. 7–11, 2001.

Minrui Leng (S'18) received the B.S. degree in electronic and information engineering and Ph.D. degrees in electrical engineering from Southwest Jiaotong University, Chengdu, China, in 2014 and 2021, respectively. She is currently an assistant professor with the School of Electrical Engineering, Sichuan University.

Her research interests include small signal modelling and dynamical modeling of power converter, control techniques of power converter, stability of distributed power systems and model predictive control, cyber-attacks of dc microgids.

Subham Sahoo (S'16-M'18) received the B.Tech. Ph.D. degree in Electrical and Electronics Engineering from VSSUT, Burla, India and Electrical Engineering at Indian Institute of Technology, Delhi, New Delhi, India in 2014 2018, respectively. He is currently an Assistant Professor and a vice-leader for Reliability of Power Electronic Converters (ReliaPEC) research group in the Department of Energy, AAU, Denmark.

His research interests are control, optimization, cybersecurity and stability of power electronic dominated grids, physics-informed machine learning tools for power electronic systems.

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 a Ph.D. degree in Electrical Engineering at Aalborg University in 1995. He became an Assistant Professor in 1992, an Associate Professor in 1996, and a Full Professor of power electronics and drives in 1998. From 2017 he became a Villum Investigator. He is honoris causa at University Politehnica Timisoara (UPT), Romania, and Tallinn Technical University (TTU) in Estonia. His current research interests include power electronics and its applications, such as in wind turbines, PV systems, reliability, harmonics, and adjustable speed drives.

He has received 32 IEEE Prize Paper Awards, the IEEE PELS Distinguished Service Award in 2009, the EPE-PEMC Council Award in 2010, the IEEE William E. Newell Power Electronics Award 2014, the Villum Kann Rasmussen Research Award 2014, the Global Energy uPrize in 2019 and the 2020 IEEE Edison Medal. He was the Editor-in-Chief of the IEEE Transactions on Power Electronics from 2006 to 2012. He has been a Distinguished Lecturer for the IEEE Power Electronics Society from 2005 to 2007 and for the IEEE Industry Applications Society from 2010 to 2011 as well as 2017 to 2018. In 2019-2020 he served a President of the IEEE Power Electronics Society. He is Vice-President of the Danish Academy of Technical Sciences too. He is nominated in 2014-2019 by Thomson Reuters to be between the most 250 cited researchers in Engineering in the world.

Marta Molinas received the Doctor of Engineering degree from the Tokyo Institute of Technology, Tokyo, Japan, in 2000. She was a JSPS Fellow at AIST Tsukuba, Japan from 2008 to 2009. From 2008-2014 she has been professor at the Department of Electric Power Engineering at the Norwegian University of Science and Technology (NTNU) and since 2014 she is Professor at the Department of Engineering Cybernetics, NTNU. In the period 2013-2014 she has been visiting professor at Columbia University in New York and Bhutan Prime Minister Fellow for the Kingdom of Bhutan.

She is currently a JSPS Fellow at the International Institute of Integrative Sleep Medicine of Tsukuba University. Dr. Molinas is Editor of the IEEE Journal of Emerging and Selected Topics in Power Electronics, the IEEE Journal of Emerging and Selected Topics in Industrial Electronics, the IEEE Transactions on Energy Conversion, the Scientific Reports and Associate Editor of the IEEE Transactions on Power Electronics.