Stabilization of DC Microgrids Under Cyber Attacks

Optimal Design and Sensitivity Analysis

Leng, Minrui; Sahoo, Subham; Blaabjerg, Frede

Published in:
I E E E Transactions on Smart Grid

DOI (link to publication from Publisher):
10.1109/TSG.2023.3278094

Publication date:
2024

Document Version
Accepted author manuscript, peer reviewed version

Stabilization of DC Microgrids Under Cyber Attacks – Optimal Design and Sensitivity Analysis

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

***Abstract*—Due to increased efforts on digitizing the modern power electronic systems and microgrids, their operational reliability and stability are prone to the risk of cyber attacks. In this paper, we inspect the overlooked stability issues caused by cyber-attacks, and present an overall design insight for stabilization of microgrids under cyber attacks. Firstly, we shed light on the optimal design policy and sensitivity aspects of the solution for microgrids under cyber-attacks. These results are based on a describing function-based modeling method to map the stability region. Secondly, the sensitivity impact due to system parameter variations and stabilization gains on stability is theoretically investigated. In addition, the range of sensitivity of parameter variations with respect to cyber attacks are calculated. Based on different design requirements, optimal values are theoretically obtained and then tested on microgrids having different parameters in a simulation environment, which justifies the ruggedness of the proposed design approach. We provide a generalized philosophy, which can be easily extended to the overall design, stability and parameter sensitivity of cyber-physical energy systems.**

***Index Terms*—Cyber-attacks, microgrids, stability, optimal design, sensitivity analysis.**

I. Introduction

DISTRIBUTED controllers have emerged as a reliable prospect for networked control of microgrids because of high reliability and scalability within a fairly economic communication infrastructure [1]. Distributed controllers equip neighboring information exchange between local controllers to achieve a global control objective [2], which can be regarded as a good compromise between centralized and decentralized control. In DC microgrids, secondary controllers can achieve average voltage regulation, energy balancing and proportional load sharing by updating the voltage references for the primary controllers. Then, the droop control is used in primary controller to regulate the output voltage for each converter.

In distributed controllers, communication channel is essential for exchange of information, which makes them vulnerable to cyber attacks by third-party adversaries. Several reports of cyber-attacks on power grids, PV farms, data centers, electric vehicles [3]-[6] are recorded. There are many kinds of cyber-attacks, including false data injection attacks (FDIA), denial of service (DoS) [7], replay attacks [8], etc. These attacks are capable of compromising the confidentiality, integrity, and availability of information in energy systems, which may result in disrupting the control objectives [9] and possibly shutdown, which mandates essential conduct.

Current research on cybersecurity primarily focus on the evaluation of cyber attack effect, detection and mitigation strategies have been well discussed. The detection problem can be summarized by identifying a change in sets of inferred candidate invariants. Detection theories for detecting FDIAs on the current sensors, communication networks in the control architecture, as well as sensors and communication channels have been developed in [10]-[11]. Although many work provide promising choices in improving the resiliency of power grids against cyber attacks from an ultimate perspective of grid outage and partial/full blackouts, its impact on destabilizing the system as an intermediate stage is completely ignored. Instilling instability can be another viable arrangement by the adversary, which challenges the traditional stability principles in power electronic systems. This can be caused either by triggering instability via cyber attacks either in the cyber/physical layer or both simultaneously.

In connection with this, [12]-[13] reveal the stability issues caused by cyber disturbances, paying more attention on instability due to communication delays and cyber network topologies. Moreover, the steady-state analysis and stochastic small-signal stability related to cyber-physical dynamics of DC microgrid under cyber attacks are given in [14] and [15]. In [16], the presence of unknown nonlinear constant power loads is determined and a distributed nonlinear adaptive observer is proposed to address the security and stability issues. However, these studies fail to quantify the impact of cyber attack on the system stability. Recently, the instability phenomena caused by stealth cyber attacks is introduced briefly in [17]. Further in [18], an abstract modeling principle of the impact of cyber attacks on stability of microgrids is provided alongside a solution to address the instability issues. In our previous studies [19]-[20], we demonstrate that our proposed event-driven detection and mitigation strategy allows best reported resiliency of $N-1$, given that $N-1$ converters are attacked in a system with N converters. In [18], it is revealed that the oscillations caused by cyber attacks will not only affect the reliability of operation, but will also forbid the operation and decision of the abovementioned event-driven cybersecurity strategies. This can be explained owing to the lack of a formidable design approach in the selection of control quantities h_i and l_i as well as their impact on the effectiveness of detection being unclear. In addition, the design of the pinning gain and coupling gain are not well addressed in

This work is partly supported by Nordic Energy Research programme via Next-uGrid project n. 117766, partly by Reliable Power Electronics Based Power Systems (REPEPS) funded by the Villum Foundation, Denmark, and partly by the Youth Fund of Sichuan Province under Grant 23NSFSC3809.

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)*

presence of cyber attacks. Carrying over our previous work on design of a stabilization method of DC microgrid under cyber attacks [18], the selection of an optimal stabilization gain is critical for the dynamic performance of the system. As a result, the optimal design of parameters of an attacked system albeit the uncertainty in the type and magnitude of cyber attacks with a primary focus on the system performance is still an open research question. This study is significant as all the stability and design principles are manifested based on physical disturbances, but is worthy of extension into disturbances from the cyber layer.

To fill this gap, this paper provides an optimal design framework for power electronic systems for the first time in the realm of power electronics and extends the modeling prophecies to decipher sensitivity analysis of different system parameters with respect to multi-valued cyber attacks. We expand on our modeling principles and cyber-physical stability analysis in [18] to provide a formal relationship of system response with respect to different values of cyber attacks. The said relationship is achieved using a stabilizing gain in [18]. Considering DC microgrids as the test system in this paper, a describing function-based method is firstly applied to derive the stable region, wherein the effects of parameter variations and stabilization gains on stability are investigated.

II. Stability Arrangement for Microgrids Against Cyber Attacks

A. System Description

Fig. 1 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. 1. 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. 1, 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, $\mathbf{A}_{\mathrm{G}} = [a_{ij}] \in R^{N\times N}$, where the communication weight a_{ij} (from node j to node i) is modeled using the specified law: $a_{ij} > 0$, if $(\psi_i, \psi_j) \in \mathbf{E}$, 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 ψ_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, $\mathbf{D}_{\text{in}} = \mathtt{diag}\{d_i^{in}\}$, where $d_i^{in} = \sum_{j\in N_i} a_{ij}$. Similarly, the matrix representing outcoming information can be given as, $\mathbf{D}_{\text{out}} = \mathtt{diag}\{d_i^{out}\}$, 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, $\mathbf{L} = \mathbf{D}_{\text{in}} - \mathbf{A}_{\mathrm{G}}$.

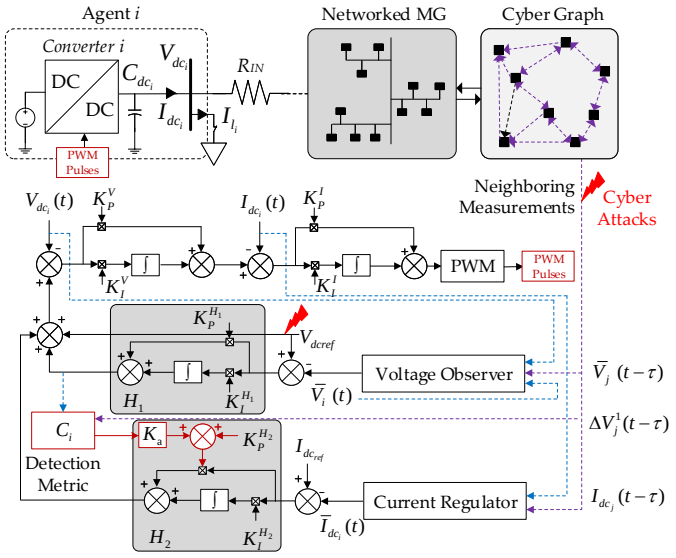

Fig. 1. Cyber-physical DC microgrid with N agents – a stabilization scheme proposed in [18] is equipped to mitigate unstable instances due to cyber attacks.

The objective of cooperative control is to regulate the global average voltage and realize load current sharing proportionally. In order to achieve this, a voltage 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:

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

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

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 (in (4)) for i^{th} agent between the local per-unit and neighbors' per-unit output current. The output from voltage observer and current regulator in Fig. 1 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 given by:

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

For a well-connected cyber graph in a DC microgrid, according to the cooperative-based consensus algorithm, the global control objectives can be given by:

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

B. Solution for Instability in DC Microgrids Caused by Cyber Attacks [18]

For a well-planned set of balanced attacks injected into multiple sensors or links, (6) will still be satisfied. This aspect has already been theoretically validated in [18]. The balanced attacks can be modeled by:

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

where, $\mathbf{u}_a$, $\bar{\mathbf{V}}$ denote the vector representation of the attacked control input 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. More details about **W** matrix can be obtained from [18]. Ref. [21] provides a cooperative vulnerability factor C_i to detect the attacked voltage sensors, which can be represented as:

$$C_i = h_i \left[\sum_{j\in N_i} a_{ij}(\Delta V_{1j}(t-\tau) - \Delta V_{1i}(t)) \right] \left[\sum_{j\in N_i} a_{ij}(\Delta V_{1j}(t-\tau) + \Delta V_{1i}(t)) \right] \tag{8}$$

where, h_i is a positive constant. As shown in Fig. 1, the detection criterion can be given by:

$$C_i = \begin{cases} > 0, & \textbf{if } \kappa = 1 \\ 0, & \textbf{else} \end{cases} \tag{9}$$

The attacked voltage sensors can be distinguished by (9). It is worth notifying that with different values of attacks, C_i is different, which means that a large value of attack indicates larger C_i and vice-versa. As a result, C_i can be regarded as an adaptive variable according to different value of attacks. In order to reduce the effects of smart attacks on the stability, an adaptive solution is presented, as shown in Fig. 1.

As it can be seen in Fig. 1, C_i is introduced in the secondary controller and is used to modify the proportional coefficient in sublayer II, thereby changing the voltage correction term only during attacks. Hence, a novel adaptive gain mechanism is proposed in [18], which exploits the positive-definiteness of the cooperative vulnerability factor C_i in (8) during attacks. As a result, when a stealthy group of cyber attack elements of any magnitude in (7) is injected into DC microgrid, the adaptive proportional gain of the current regulator damps out the unstable modes, given by:

$$\mathbf{K_P^{H_2}} = \mathbf{K_{P_{in}}^{H_2}} + \mathbf{K_a F} \tag{10}$$

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. As a result, a feedforward input from (9) is introduced as an adaptive term to solve stability issues in microgrids arising from cyber attacks.

III. Optimal Design under Cyber Attacks

A. Stable Regions

Based on the cyber graph model, the converter model, the controller and the transmission line model, the small-signal model for the DC microgrid including the adaptive terms from (10) is expressed below:

$$\begin{cases} \dot{\hat{\mathbf{V}}}(\mathbf{t}) = \dot{\mathbf{V}}_{\mathbf{dc}}(\mathbf{t}) - \mathbf{L}\hat{\mathbf{V}}(\mathbf{t}-\boldsymbol{\tau}) + \dot{\hat{\mathbf{u}}}^{\mathbf{a}} \\ \hat{\boldsymbol{\delta}}(\mathbf{t}) = -\mathbf{L}\dfrac{\hat{\mathbf{I}}(\mathbf{t}-\boldsymbol{\tau})}{\mathbf{I_{rated}}} \\ \boldsymbol{\Delta}\dot{\hat{\mathbf{V}}}_{\mathbf{1}}(\mathbf{t}) = -\mathbf{K_p^{H_1}}\dot{\hat{\mathbf{V}}}_{\mathbf{dc}}(\mathbf{t}) - \mathbf{K_I^{H_1}}\hat{\dot{\mathbf{V}}}(\mathbf{t}) \\ + \mathbf{K_P^{H_1}}\mathbf{L}\hat{\dot{\mathbf{V}}}(\mathbf{t}-\boldsymbol{\tau}) \\ \boldsymbol{\Delta}\dot{\hat{\mathbf{V}}}_{\mathbf{2}}(\mathbf{t}) = -\mathbf{K_P^{H_2}}\mathbf{L}\dot{\hat{\mathbf{I}}}(\mathbf{t}-\boldsymbol{\tau}) - \mathbf{K_I^{H_2}}\mathbf{L}\hat{\mathbf{I}}(\mathbf{t}-\boldsymbol{\tau}) \\ \hat{\mathbf{V}}^*(\mathbf{t}) = \boldsymbol{\Delta}\hat{\mathbf{V}}_{\mathbf{1}}(\mathbf{t}) + \boldsymbol{\Delta}\hat{\mathbf{V}}_{\mathbf{2}}(\mathbf{t}) \\ \dot{\hat{\mathbf{I}}}(\mathbf{t}) = \dfrac{\hat{\mathbf{V}}_{\mathbf{in}}(\mathbf{t})}{\mathbf{L_f}} - \dfrac{\hat{\mathbf{V}}_{\mathbf{dc}}(\mathbf{t})}{\mathbf{L_f}} + \dfrac{\mathbf{V_{dc}}\hat{\mathbf{d}}(\mathbf{t})}{\mathbf{L_f}} \\ + \dfrac{\mathbf{D_{on}}\hat{\mathbf{V}}_{\mathbf{dc}}(\mathbf{t})}{\mathbf{L_f}} \\ \dot{\hat{\mathbf{V}}}_{\mathbf{dc}}(\mathbf{t}) = \dfrac{\hat{\mathbf{I}}(\mathbf{t})}{\mathbf{C_f}} - \dfrac{\mathbf{D_{on}}\mathbf{I}(\mathbf{t})}{\mathbf{C_f}} - \dfrac{\mathbf{I}\hat{\mathbf{d}}(\mathbf{t})}{\mathbf{C_f}} - \dfrac{\hat{\mathbf{I}}_{\mathbf{load}}(\mathbf{t})}{\mathbf{C_f}} \\ \hat{\mathbf{V}}_{\mathbf{br}}(\mathbf{t}) = \mathbf{M}\hat{\mathbf{V}}_{\mathbf{dc}}(\mathbf{t}) \\ \dot{\hat{\mathbf{I}}}_{\mathbf{br}}(\mathbf{t}) = \dfrac{\hat{\mathbf{V}}_{\mathbf{br}}(\mathbf{t})}{\mathbf{L_{br}}} - \dfrac{\mathbf{R_{br}}\hat{\mathbf{I}}_{\mathbf{br}}(\mathbf{t})}{\mathbf{L_{br}}} \\ \hat{\mathbf{d}}(\mathbf{t}) = \dfrac{\mathbf{K_P^I}(\hat{\mathbf{I}}_{\mathbf{inref}}(\mathbf{t}) - \hat{\mathbf{I}}(\mathbf{t})) + \mathbf{K_I^I}\hat{\boldsymbol{\Xi}}(\mathbf{t})}{\mathbf{T_s F_m}} \\ \dot{\hat{\boldsymbol{\Xi}}} = \hat{\mathbf{I}}_{\mathbf{inref}}(\mathbf{t}) - \hat{\mathbf{I}}(\mathbf{t}) \end{cases} \tag{11}$$

where, $\{\mathbf{H_{PI}^v}, \mathbf{H_{PI}^i}\}$, $\{\mathbf{H_{PIV}}, \mathbf{H_{PII}}\}$ 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.

As it can be seen from Fig. 2, the overall model of the DC microgrid with the proposed stabilization method includes a non-linear part and a linear part. Henceforth, a describing function (DF) [22] based stability method is adopted to investigate the stability of the system.

Denoting the approximate transfer function of the nonlinear 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. 3. Using (9), we can employ the `sign` function to represent a balanced set of zero sum attacks, which is given by:

$$\mathbf{u^a} = \lambda[\mathrm{sgn}(f_1), \mathrm{sgn}(f_2), \ldots, \mathrm{sgn}(f_N)]^{\mathrm{T}} \tag{12}$$

where, $\mathbf{u^a} \in R^{N\times 1}$ denotes the input attack vectors. According to the definition, the DF of the `sign` function can be calculated as:

$$N_{\mathrm{A}} = \frac{4}{\pi A} \tag{13}$$

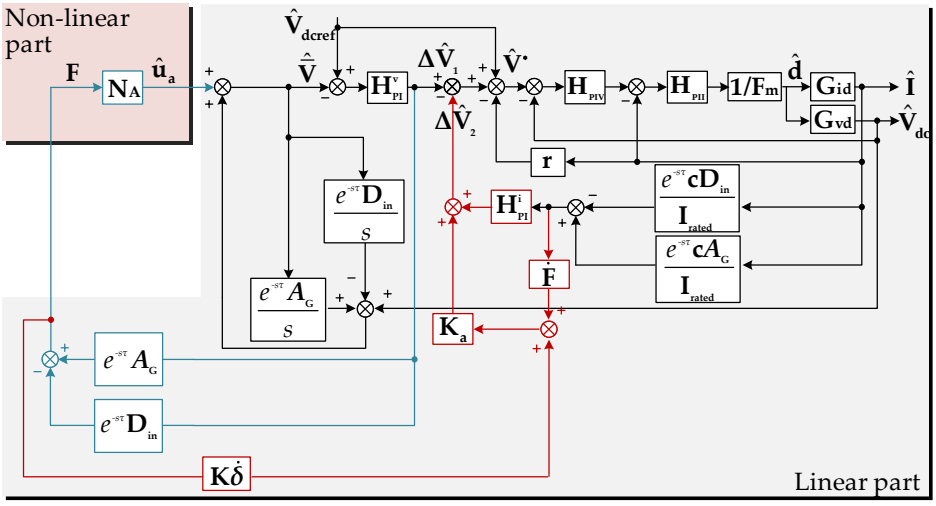

Fig. 2. Small-signal diagram of the attacked DC microgrid in Fig. 1 under steatlh cyber attack – the non-linear part includes cyber attack modeled as an non-deterministic disturbance.

Moreover, according to the small signal diagram shown in Fig. 2 for a system of N = 6 agents, the transfer function of the linear part can be deduced and given by:

$$\mathbf{G} = \frac{(e^{-s\tau}\boldsymbol{A_G}\boldsymbol{\lambda} - e^{-s\tau}\mathbf{D_{in}}\boldsymbol{\lambda})\mathbf{H_{PI}^{v}}\mathbf{G_1}}{(\mathbf{1}+\boldsymbol{\Theta}-\boldsymbol{\Omega})\,\mathbf{G_1} + \mathbf{H_{PIV}}\mathbf{H_{PII}}\mathbf{G_{vd}}\mathbf{G_K}\mathbf{H_{PI}^{v}}} \tag{14}$$

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

The stability region for the system can be given by:

$$\begin{cases} \mathbf{G_{Im}} = \mathbf{0}, \\ \mathbf{G_{Re}} = -\frac{\mathbf{1}}{\mathbf{N_A}} \end{cases} \tag{15}$$

where, $\mathbf{G_{Im}}$ and $\mathbf{G_{Re}}$ are the imaginary part and the real part of $\mathbf{G}$ in (14), respectively.

Using (15), the relationship between λ and $\mathrm{K_a}$ for different voltage/current regulator characteristics, parameters for DC/DC converters and loads are investigated, with the stability regions shown in Fig. 4-5. Fig. 4 indicates that with smaller $\mathbf{K_P^{H_1}}$ and larger $\mathbf{K_I^{H_1}}$ for voltage observer in the secondary layer, the considered system in Fig. 1 with the proposed stabilization method is more likely to be stable against the stealth attacks. While for the current regulator, the stable region of λ - $\mathrm{K_a}$ with larger $\mathbf{K_P^{H_2}}$ and smaller $\mathbf{K_I^{H_2}}$ will be wider. Furthermore, it can be seen from Fig. 5(a) that the stabilization method can be applied for DC/DC buck converter and boost converter, while it will take larger λ to destabilize a buck converter than for a boost converter. Consequently,

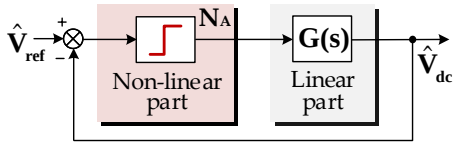

Fig. 3. Equivalent control diagram of Fig. 2 using the DF method.

the stability region of λ - $\mathrm{K_a}$ for buck converter is wider. Fig. 5(b) indicates that with the decrease of the load, DC microgrids are more vulnerable to instability due to stealth cyber-attack, requiring larger $\mathrm{K_a}$ to make the system stable. Moreover, the stability regions related to λ and $\mathrm{K_a}$ with the change of the global voltage reference is shown in Fig. 5(c). It can be seen that when the global voltage reference increases, the value of λ, which disturbs the system stability will decrease, indicating that the stability margin of the system operating with a larger global voltage reference is reduced. However, with the introduction of the stabilizing gain $\mathrm{K_a}$, the stability region will be widened. Moreover, the system trends to be stable with smaller output voltage, larger input voltage and larger line resistance. In conclusion, the stability of DC microgrid under stealth attacks are affected by different factors, which creates a multi-dimension design challenge.

B. Multi-Objective Design

According to the previous analysis, the selection of parameters is very important to ensure the whole performance of the microgrid. The purpose of this subsection is to shed light on the optimal design of the solution for microgrids under cyber-attacks. A sequential multi-objective design method is proposed here, in order to obtain an optimal stabilization gain in view of the desired steady-state and transient properties. Steady-state convergence given by voltage regulation, current sharing and transient properties given by settling time and overshoot, are the indices that need to be minimized through a design process, as shown in the flowchart in Fig. 6. The design framework is summarized below:

Step 1: Determine the stability regions, as per (15). Then, define the stable range (α_1, α_2) with different system parameters.

Step 2: Determine the optimal design of steady-state performance using (16) to minimize the voltage regulation and the current sharing error. Comparing g_1 with the steady state design performance, an optimal range of steady-state performance $(\beta_1, \beta_2) \in (\alpha_1, \alpha_2)$ can be obtained.

$$g_1 = W_1 \left(V_{refi} - \bar{v}_i\right)^2 + W_2 \delta_i^2 \tag{16}$$

Step 3: Determine the optimal design for transient performance using (17) to minimize the overshoot and tune to the desired setting time. In (17), the resonant peak of the magnitude M_r can represent the overshoot while the phase margin φ_m can indicate the setting time. Comparing g_2 with the transient design performance, an optimal stabilization gain for the considered system can be obtained.

$$g_2 = W_3 \left(\frac{M_r}{M_{max}}\right)^2 + W_4 \left(\frac{\varphi_m}{\pi}\right)^2 \tag{17}$$

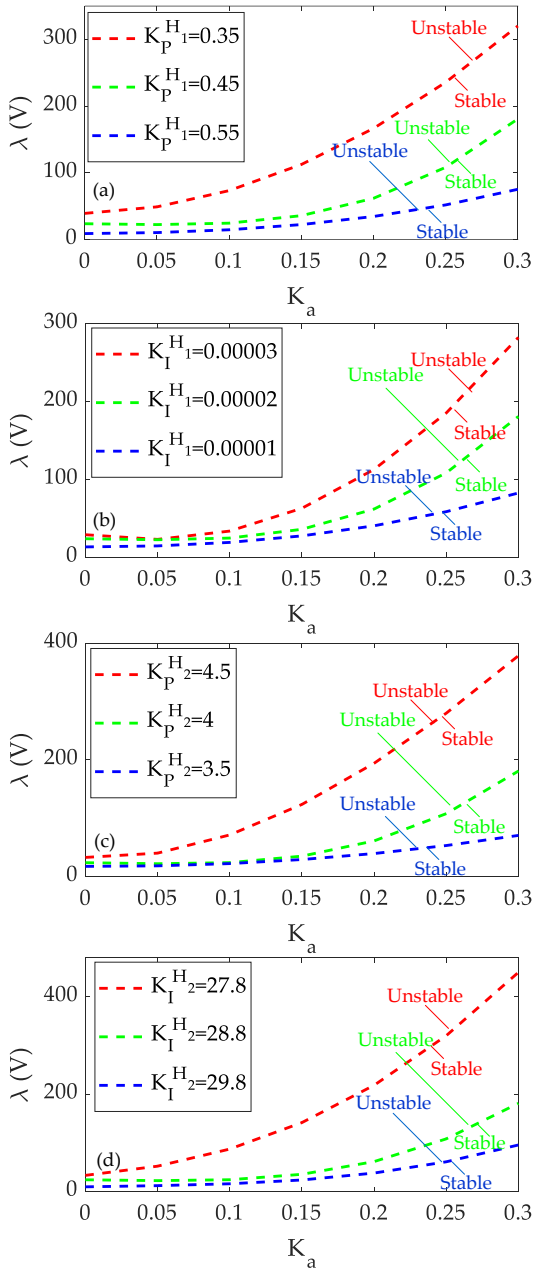

Fig. 4. Stability region: Relationship between λ – K_a with change of the voltage/current regulator characteristics: (a) voltage regulator proportional gain, (b) voltage regulator integral gain (c) current regulator proportional gain, (d) current regulator integral gain.

Since the unit and value of M_r and φ_m are totally different, it is necessary to make a normalization. In this paper, a maximum resonant peak of the magnitude M_{max} is introduced to normalize the overshoot while the setting time is normalized

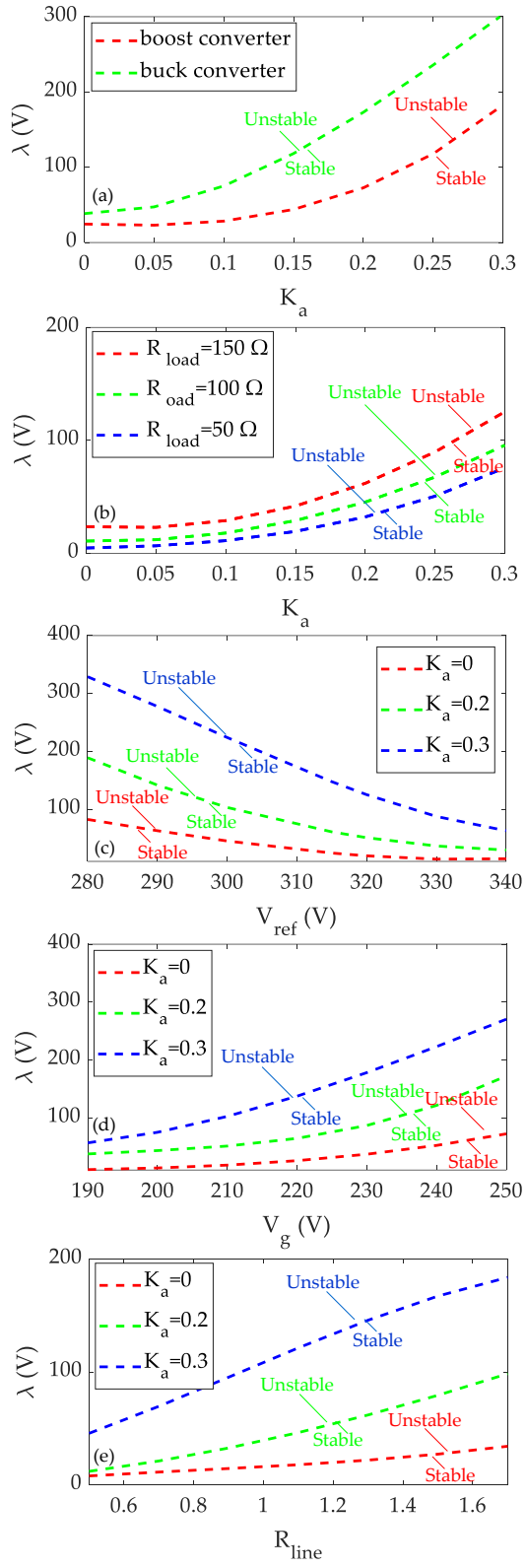

Fig. 5. Stability region for different cases: (a) converter types, (b) load values, (c) voltage references, (d) input voltages, and (e) line parameters.

by introducing π. It is worth notifying that M_{max} and π are deciphered based on the design requirements.

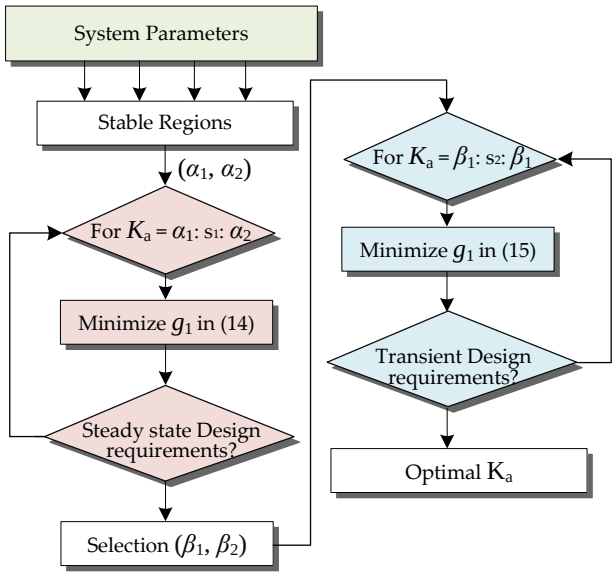

Fig. 6. Flow chart of the sequential multi-objective design method for DC microgrids considering FDI attacks at vulnerable points.

Define the design requirements as $D(\delta_v, \delta_i, t_s, \Delta i_p)$, where δ_v denotes the voltage regulation error, δ_i denotes the current sharing error, t_s describes the setting time and Δi_p indicates the overshoot of current in DC microgrid. By constraining the design requirements $D(\delta_v, \delta_i, t_s, \Delta i_p)$ as ($\delta_v \leq 0.05$ V, $\delta_i \leq 0.01$ A, $t_s \leq 0.3$ s, $\Delta i_p \leq 2$ A), K_a can be optimized by the sequential multi-objective design method. According to the flow chart of the proposed method, the optimal K_a is found out to be 5.2. In order to analyze the steady state and transient performance with the variation of K_a, time-domain and frequency-domain results are presented, as shown in Fig. 7 and Fig. 8. It can be seen that the voltage regulation and current sharing error is quite small, when K_a is larger than 0.3. With the increase of K_a, the overshoot decreases with the increase in setting time. The resonant peak and phase margin shares similar trends with that of overshoot and setting time, respectively when K_a changes. It should be noted that the stabilization gain K_a is optimized for DC microgrids in this paper, however the framework can be generalised for optimization of other system parameters.

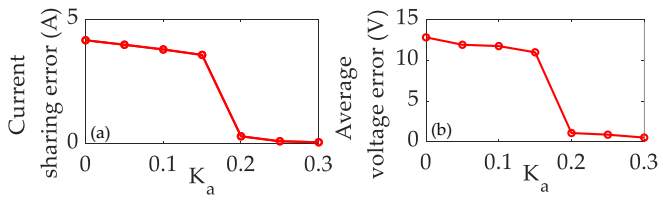

Fig. 7. Steady-state performance results on the impact of stabilization gain K_a on current sharing and average voltage regulation error.

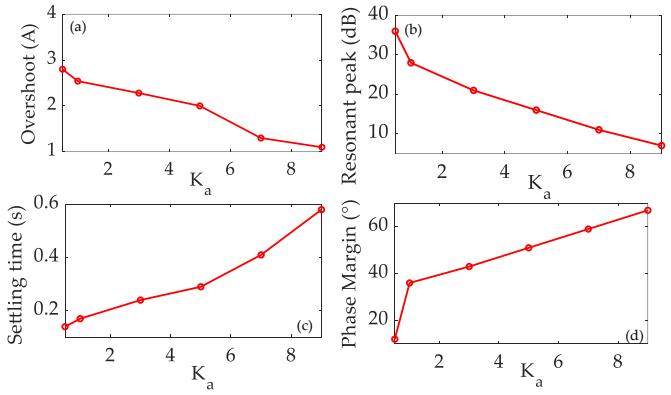

Fig. 8. Analytical results of transient performance on the impact of K_a on time-domain and frequency-domain metrics.

IV. Sensitivity Analysis under Cyber Attacks

A. Sensitivity Framework

A sensitivity analysis based on DF stability method is proposed to intuitively and quantitatively investigate the influence of the paramters in DC microgrid in Fig. 15 under cyber attacks. The DF-based stability method is described in [22], which is shown in Fig. 9(a). After that, the Nyquist plot of $G(s)$ is manifested into the frequency domain plot, as shown in Fig. 9(b). In Fig. 9(a), if the setpoint $-1/N_A$ is not encircled by the contour of $G(s)$, the system is stable otherwise it will be unstable or critically stable. The real part and the imaginary part of Curve 1 and Curve 2 shown in Fig. 9(a) can be equivalently manifested into Fig. 9(b). Curve 1 encircling the $-1/N_A$ can be converted as an equivalent condition in Fig. 9(b): in the frequency range where the real part $\mathtt{Re}_1$ is less than $-1/N_A$, the imaginary part $\mathtt{X}$ crosses the frequency axis once, and the crossed frequency is noted as f_0. While for Curve 2, since it does not encircle the $-1/N_A$, the real part $\mathtt{Re}_2$ is larger than $-1/N_A$ at the crossed frequency f_0. Hence, the stability criteria for Fig. 9(b) is that the imaginary part does not cross the frequency axis in the frequency range where the real part is less than $-1/N_A$, denoted as $\mathtt{X}(f_0) = 0$, $\mathtt{Re}(f_0) > -1/N_A$.

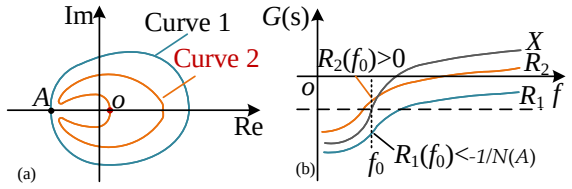

Fig. 9. Stability certificates in: (a) Nyquist plot, and (b) frequency domain plot of $G(s)$.

The sensitivity of the key transfer function $G(s)$ to the system parameters α can be described as:

$$\mathrm{Se}(\alpha) = \frac{\partial G_{Re}}{\partial \alpha} + j\frac{\partial G_{Im}}{\partial \alpha} \tag{18}$$

The absolute value of the sensitivity of the linear part transfer function $G(s)$ to any given parameter α represents how a change in that parameter affects the magnitude of $G(s)$. If the

sign of sensitivity is positive, it means that as the parameter increases or decreases, the linear part of $G(s)$ increases or decreases, and vice versa. The sensitivity calculation results can therefore be used to know which parameters of the system have a greater impact on the system stability, and to enhance the system stability by adjusting the corresponding parameter accordingly.

We illustrate the response of $G(s)$ in the frequency domain with respect to a change in the parameter α in Fig. 10. The solid line in Fig. 10 indicates that for the current value, $\mathrm{X}(f_0) = 0$, $\mathrm{Re}(f_0) < -1/N_A$, indicating that the system is unstable. From here, the system stability can be improved by adjusting the parameter accordingly. The ideal way is to increase the real part while its imaginary part decreases, which means that the frequency range of $\mathrm{Re}(f_0) < -1/N_A$ is reduced with the frequency of $\mathrm{X}(f_0) = 0$ moving towards the right, as shown by the dashed lines. The system amplitude margin increases as the intersection of the dashed lines and the real axis is shifted to the right.

A large absolute value of sensitivity indicates that the parameter has a large effect on the correlation function, so it is more efficient to preferentially adjust those parameters having a large absolute value of sensitivity.

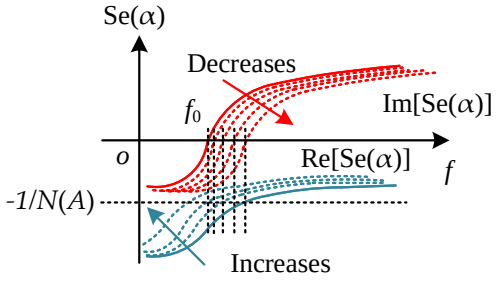

Fig. 10. Frequency domain plot of $G(s)$ with the change of system parameters – the stability margin increases with the increase of real-part and decrease of the imaginary part of the sensitivity function.

B. Sensitivity Analysis

The sensitivity analysis for different parameters is shown in Fig. 11-14, where the solid lines represent the real part and the dashed lines represent the imaginary part. In Fig. 11, with the increase of $\mathrm{K_a}$, the real part is decreased, whereas the imaginary part is increased. When $\mathrm{K_a}$ is larger than 0.2, there are no interactions between zero and the imaginary part, which indicates that the system operates in a stable manner. Conversely, when $\mathrm{K_a}$ is smaller than 0.2, there are interactions between zero and imaginary part. Moreover, at the frequency range of the imaginary part, the real part is smaller than zero, indicating that the system operates in an unstable manner.

In Fig. 12, the sensitivity analysis for the proportional gain $\mathbf{K_P^{H_2}}$ and integral gain $\mathbf{K_I^{H_2}}$ in current regulator is presented. With the increase of $\mathbf{K_P^{H_2}}$, the imaginary part is increasing, and the frequency region of interactions between zero and the imaginary part is decreased, whereas the real part is larger than zero, indicating that the DC microgrid is stable. As for $\mathbf{K_I^{H_2}}$, the considered DC microgrid is unstable when $\mathbf{K_P^{H_2}}$ is smaller than 30 because the real part is smaller than zero. Based on the stability boundaries, the system stability is hereby improved by either increasing $\mathbf{K_P^{H_2}}$ or decreasing $\mathbf{K_I^{H_2}}$. However, the proportional gain and integral gain in the voltage regulator has the opposite stability trends with that of the current regulator, as shown in Fig. 13. Moreover, the sensitivity of load is shown in Fig. 14, where the real part and the imaginary part are increased with an increase in R_{load}. Especially when the overall load R_{load} is smaller than 50 Ω, DC microgrid is prone to instability under cyber attacks due to the very small real part at the frequency region of interaction between the imaginary part and the zero.

Upon analyzing Fig. 11-14, the sensitivity of $\mathrm{K_a}$, $\mathbf{K_P^{H_2}}$ and $\mathbf{K_I^{H_2}}$ are larger than others which indicates that these parameters have a higher impact on the stability of the considered system than $\mathbf{K_P^{H_1}}$, $\mathbf{K_I^{H_1}}$ and R_{load}. According to the sensitivity analysis, it is more efficient to improve the system stability by increasing $\mathrm{K_a}$, $\mathbf{K_P^{H_2}}$ as well as by decreasing $\mathbf{K_I^{H_2}}$.

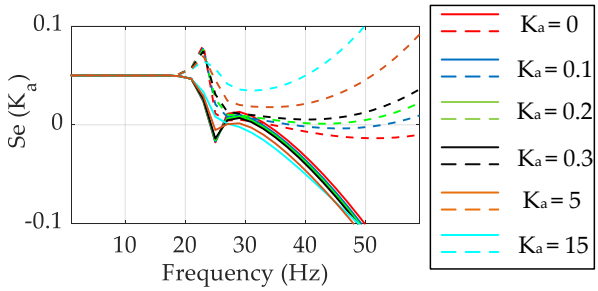

Fig. 11. Sensitivity analysis for $G(s)$ (Fig. 15) to the stabilization gain $\mathrm{K_a}$ – the solid lines represent the real part whereas the dashed lines represent the imaginary part.

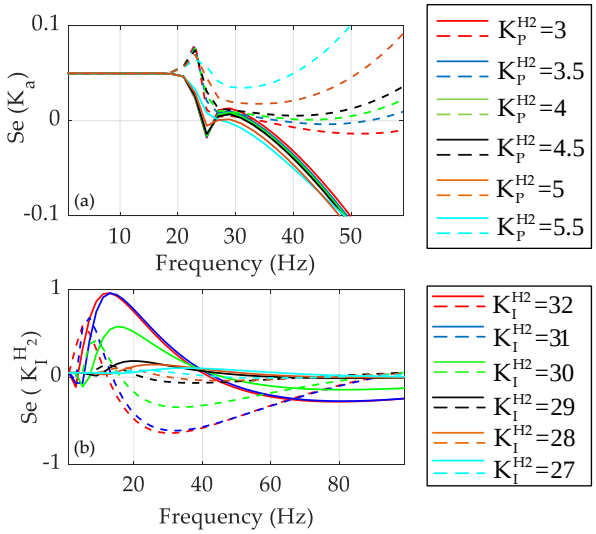

Fig. 12. Sensitivity analysis for $G(s)$ (Fig. 15) to the PI controller gains across voltage observer: (a) $\mathrm{K_P^{H_2}}$, and (b) $\mathrm{K_I^{H_2}}$.

V. Results and Discussions

The simulated system is shown in Fig. 15 with the controller for each converter being presented in Fig. 1. We analyze the

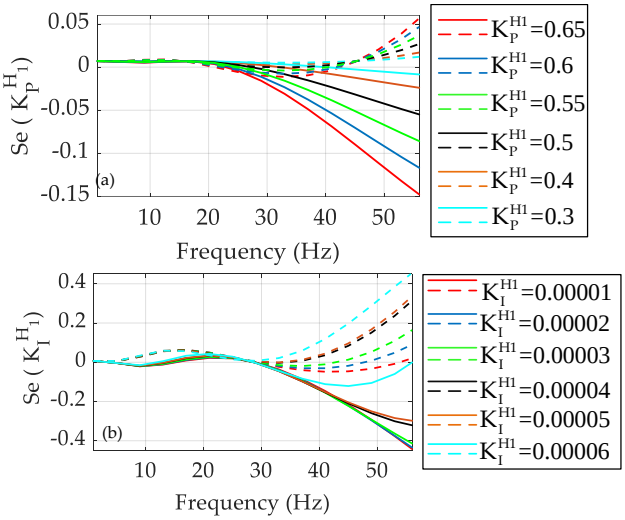

Fig. 13. Sensitivity analysis for $G(s)$ (Fig. 15) to the PI controller gains across current regulator: (a) $K_P^{H_1}$, and (b) $K_I^{H_1}$.

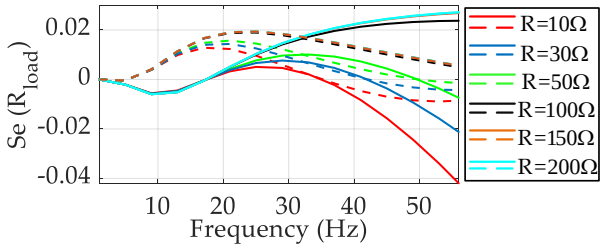

Fig. 14. Sensitivity analysis for $G(s)$ (Fig. 15) to R_{load}.

impact and sensitivity analysis of different system parameters on the stability of DC microgrid under cyber attack(s). Although our previous solution proposed in [18] can be used to eliminate the oscillations, it is equally crucial to formulate a design philosophy of an optimal stabilization gain K_a, which can be accommodated into any system with considerable parameter variations. Simulations have been carried out to test the effectiveness of the multi-objective design of K_a. Different cases with variation parameters are presented and the simulation results are concluded in Table I. To verify the optimal K_a for different cases, both the simulation results using optimal K_a and parameters closed to optimal K_a are also shown in Fig. 16–19.

In Table I, for each case, the optimal K_a is obtained as per the optimal design method in Fig. 7. Formal design specifications have been provided for each case. In Case I & II, constraining the design requirements $D\,(\delta_v, \delta_i, t_s, \Delta i_p)$ as ($\delta_v \leq 0.05$ V, $\delta_i \leq 0.01$ A, $t_s \leq 0.3$ s, $\Delta i_p \leq 2$ A), we obtain an optimal K_a of 5.2 and 3.3 with different system parameters, respectively. It is worth notifying that the only difference between Case I & II is the value of $\mathbf{K_I^{H_2}}$ and R_{load}. Furthermore, in Case III & IV, upon changing the design requirements as ($\delta_v \leq 0.05$ V, $\delta_i \leq 0.01$ A, $t_s \leq 0.35$ s, $\Delta i_p \leq 1$ A), we obtain the optimal K_a to be 6.5 and 4.5 with different system parameters, respectively. It is worth notifying that the differences between Case III & IV is that the former

TABLE I
DIFFERENT CASES WITH VARIOUS PARAMETERS

		Case I	Case II	Case III	Case IV
Parameters	$K_P^{H_1}$	0.5	0.3	0.4	0.5
	$K_I^{H_1}$	0.00001	0.00005	0.00002	0.00005
	$K_P^{H_2}$	1	1	1	1
	$K_I^{H_2}$	68	65	65	65
	V_g	220 V	220 V	220 V	190 V
	V_o	315 V	315 V	340 V	315V
	R_{load}	60 Ω	24 Ω	38 Ω	30 Ω
	λ	±20	±20	±20	±20
Optimal K_a		5.2	3.3	6.5	4.5
Design requirements		*D* (0.05 V, 0.01 A, 0.3 s, 2 A)		*D* (0.05 V, 0.01 A, 0.35 s, 1 A)	
D (δ_v, δ_i, t_s, Δi_p)	δ_v	0.02 V	0.009 V	0.011 V	0.006 V
	δ_i	0.005 A	0.007 A	0.005 A	0.008 A
	t_s	0.29 s	0.289 s	0.34 s	0.342 s
	Δi_p	1.95 A	1.93 A	0.94 A	0.96 A

operates with a different output voltage reference, whereas the latter operates with a different input voltage. The corresponding measured steady-state and transient performance metrics are also shown in Table I.

We now validate the quantitative results of our proposed design framework to monitor the specifications for steady-state and transient performance in time-domain simulations. As it can be seen in Fig. 16, with the increase of K_a, the setting time will rise and the overshoot is reduced. When K_a = 5, K_a = 5.2, K_a = 5.4, the setting time is 0.285 s, 0.029 s and 0.315 s while the overshoot is 2.1 A, 1.95 A and 1.93 A, respectively. The design requirements are only satisfied with K_a = 5.2, which validates the ruggedness of the proposed multi-objective optimal design method. Similarly in Case II, when the system parameters are changed, i. e., PI controller gains for voltage regulator and current regulator, the stabilization gain K_a is optimized to meet the same design requirements, which is different from that of Case I. It can be seen in Fig. 17 that K_a = 3.3 comes out as the optimal value for Case II, by which both the steady-state performance and the transient performance of the attacked DC microgrid holds good.

Similarly, we test a new design specification D ($\delta_v \leq 0.05$ V, $\delta_i \leq 0.01$ A, $t_s \leq 0.35$ s, $\Delta i_p \leq 1$ A) in Case III & IV. Based on the design requirements, we obtain an optimal stabilization gain K_a of 6.5 and 4.5 for case III & IV, respectively. The choice of K_a is validated through time-domain simulations carried out in Fig. 18 and 19, respectively. It can also be seen that even a small change of K_a (within ± 5%) incurs a trade-off in its performance, where either the steady-state or transient performance metric is not met.

In conclusion, under different circumstances, the stabilization gain K_a should be considered carefully to ensure good dynamic performance of the attacked system. By using the proposed design method, an optimal stabilization gain K_a with minimum sensitivity and maximum robustness for stability under cyber attacks can be obtained. It should be further

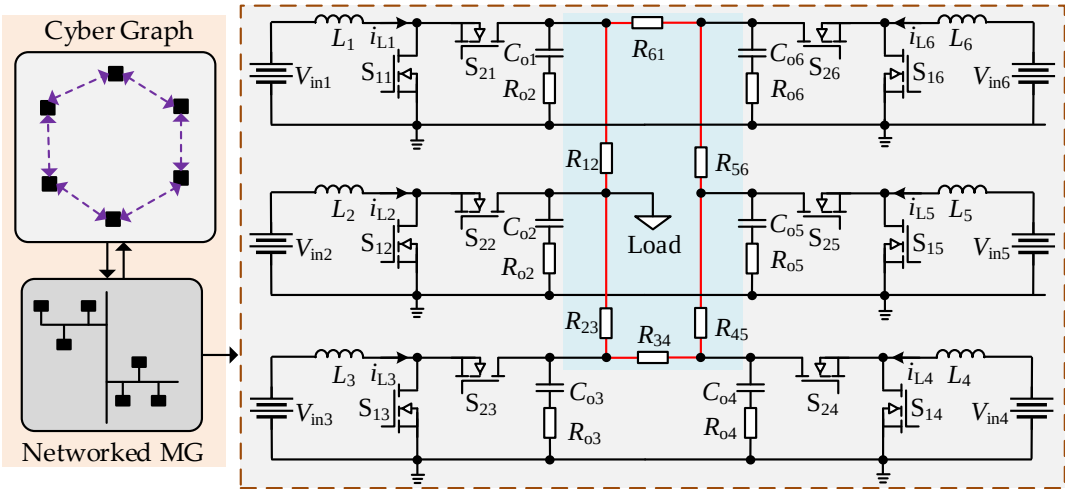

Fig. 15. Simulated system of a 6-bus networked cyber-physical DC microgrid with the converters (C#1-C#6) distributed via tie-lines between them – V_n and I_n represent the measured capacitor voltage and inductor current, respectively for agent n.

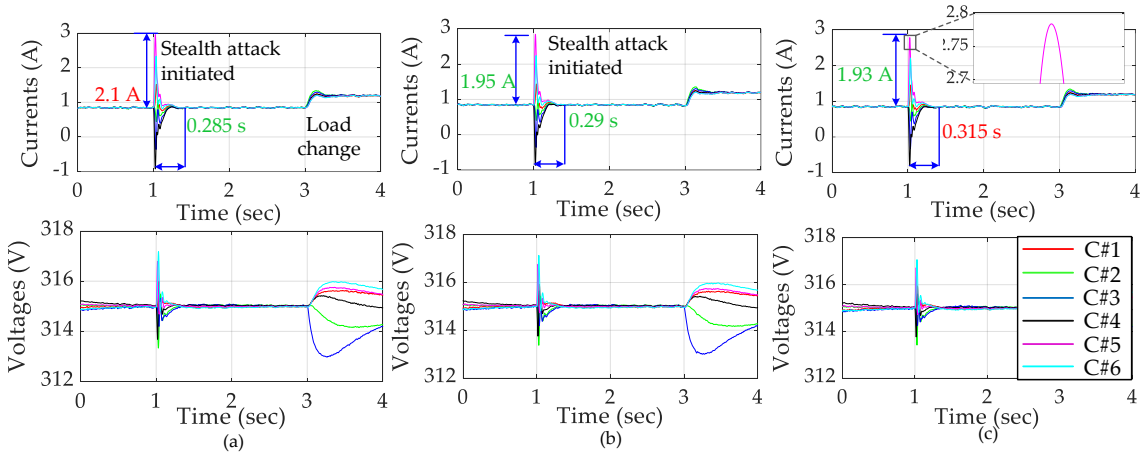

Fig. 16. Time-domain waveforms of Case I with design requirement D ($\delta_v \leq 0.05$ V, $\delta_i \leq 0.01$ A, $t_s \leq 0.3$ s, $\Delta i_p \leq 2$ A): (a) $K_a = 5$, (b) $K_a = 5.2$, (c) $K_a = 5.4$. As calculated in Table I for Case I, only $K_a = 5.2$ complies with the said requirements of the overshoot and settling time bounds.

noted that the proposed design method can be extended to any system with defined stability bounds.

VI. Conclusions

This paper proposes a novel design philosophy and sensitivity analysis by mapping the stability of DC microgrids under cyber attacks to the dependence of system parameters for different cyber attack values. Firstly, a describing function based stabilization method is designed using a cyber attack detection metric as an adaptive feedforward to enhance the damping under stealth cyber attacks. Then, the stability regions of the microgrid under cyber attacks are investigated. Considering them as inputs, an optimal design philosophy is proposed considering the steady-state stability and transient performance of microgrids for quantitative formulation of the stabilization gain for a given system. The sensitivity of the stability approach is carried out to analyze the parameter sensitivity with respect to system stability. Finally, different case studies are carried out to validate the optimal calculation of the stabilization gain for microgrids having varying design requirements. It turns out that the small stabilization coefficient will lead to faster transient performance but larger overshoot voltage while large stabilization coefficient will get the opposite results. Moreover, it also provides an empirical idea on the critical parameters from a cyber-physical perspective, which will affect the overall system stability. Based on this study, we argue that the proposed mechanism will broadcast new manifestations on stability and modeling of microgrids not just being limited to physical disturbances, but also needs more analysis from an uncertain input in the cyber layer. Moreover, the proposed design philosophy can also be applicable for system designers with different design requirements to model against the cyber-physical interactions and prevent their impact on the operation of microgrids.

Appendix

Simulation Parameters

It is to be noted that the line parameter R_{ij} is connected from the i^{th} converter (each of 10 kW) to the j^{th} converter.

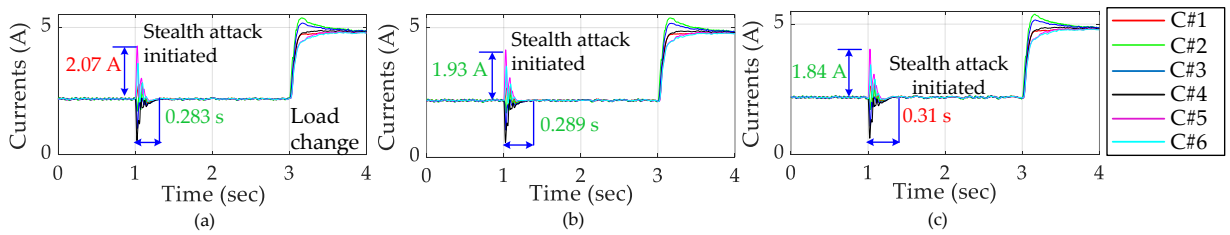

Fig. 17. Time-domain waveforms of Case II with design requirement D ($\delta_v \leq 0.05$ V, $\delta_i \leq 0.01$ A, $t_s \leq 0.3$ s, $\Delta i_p \leq 2$ A): (a) $K_a = 3.1$, (b) $K_a = 3.3$, (c) $K_a = 3.5$. As calculated in Table I for Case II, only $K_a = 3.3$ complies with the said requirements of the overshoot and settling time bounds.

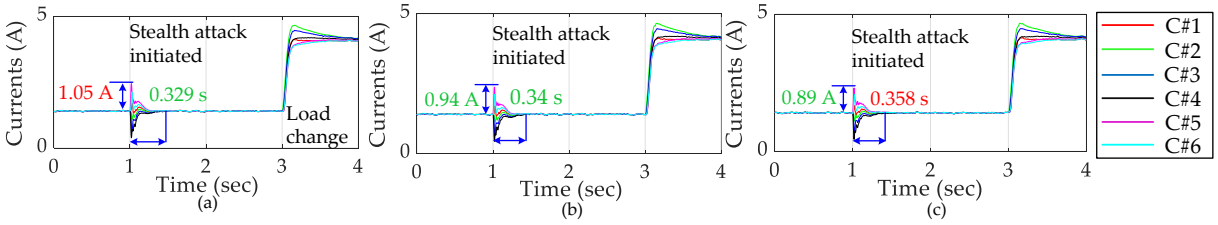

Fig. 18. Time-domain waveforms of Case III with design requirement D ($\delta_v \leq 0.05$ V, $\delta_i \leq 0.01$ A, $t_s \leq 0.35$ s, $\Delta i_p \leq 1$ A): (a) $K_a = 6.3$, (b) $K_a = 6.5$, (c) $K_a = 6.7$. As calculated in Table I for Case III, only $K_a = 3.3$ complies with the said requirements of the overshoot and settling time bounds.

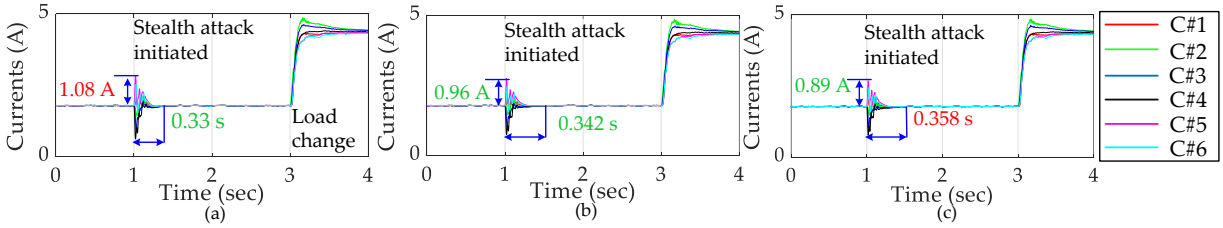

Fig. 19. Time-domain waveforms of Case IV with design requirement D ($\delta_v \leq 0.05$ V, $\delta_i \leq 0.01$ A, $t_s \leq 0.35$ s, $\Delta i_p \leq 1$ A): (a) $K_a = 4.3$, (b) $K_a = 4.5$, (c) $K_a = 4.7$. As calculated in Table I for Case IV, only $K_a = 3.3$ complies with the said requirements of the overshoot and settling time bounds.

Moreover, the controller gains are identical for each converter.
Plant: R_{12} = 1.5 Ω, R_{23} = 1.2 Ω, R_{34} = 0.8 Ω, R_{45} = 0.3 Ω, R_{56} = 0.5 Ω, R_{61} = 0.6 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: I_{dcref} = 0, K_P^v = 5, K_I^v = 100, K_P^i = 2.5, K_I^i = 0.05, h_i = 2.5.

REFERENCES

[1] 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.

[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] R. M. Lee, M. J. Assante, and T. Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid. Washington, DC, USA: E-ISAC, 2016.

[4] S. Sahoo, F. Blaabjerg, T. Dragicevic, "Cyber Security for Microgrids," *IET Digital Library*, 2022. DOI: 10.1049/PBPO196E

[5] J. Ye et al. "A Review of Cyber-Physical Security for Photovoltaic Systems," *IEEE Journ. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 4, pp. 4879-4901, 2022.

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

[7] 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. Smart Grid.*, vol. 15, no. 7, pp. 4066–4075, July 2019.

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

[9] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. on Power Syst.*, vol. 33, no. 5, pp. 4868–4877, 2018.

[10] S. Sahoo, J. C. 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.

[11] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Trans. Autom. Control.,* vol. 65, no. 9, pp. 3800–3815, Sep. 2020.

[12] 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).,* pp. 2667-2672, 2021.

[13] L. Sheng, G. Lou, W. Gu, S. Lu, S. Ding and Z. Ye. "Optimal communication network design of microgrids considering cyber-attacks and time-delays," *IEEE Trans. Smart Grid.,* doi: 10.1109/TSG.2022.3169343.

[14] J. Liu, Y. Du, S. -i. Yim, X. Lu, B. Chen and F. Qiu, "Steady-state analysis of microgrid distributed control under denial of service attacks," *IEEE Journ. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5311-5325, Oct. 2021.

[15] 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.

[16] 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.

[17] M. Leng, S. Sahoo and F. Blaabjerg, "Stability Investigation of DC Microgrids Under Stealth Cyber Attacks," *Proc. of IEEE ECCE*, 2021, pp. 1427-1432, doi: 10.1109/ECCE47101.2021.9595243.
[18] M. Leng, S. Sahoo, F. Blaabjerg and M. Molinas, "Projections of Cyber Attacks on Stability of DC Microgrids - Modeling Principles and Solution," *IEEE Trans. Power Electron.*, pp. 37, no. 10, pp. 11774-11786, 2022.
[19] 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, Dec. 2020.
[20] S. Sahoo, Y. Yang and F. Blaabjerg, "Resilient Synchronization Strategy for AC Microgrids Under Cyber Attacks," *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 73-77, Jan. 2021.
[21] 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.
[22] 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 (Student Member, IEEE) received the B.S. degree in electrical engineering and automation from Southwest Jiaotong University, Chengdu, China, in 2014, and the Ph.D. degree from the School of Electrical Engineering, Southwest Jiaotong University, in 2021. From 2019 to 2021, she was a visiting Ph.D. student with the Department of Energy Technology, Aalborg University, Aalborg, Denmark. She is currently an Assistant Professor with the College of Electrical Engineering, Sichuan University, Chengdu, China.

Her research interests include small-signal modeling and dynamical modeling of power converters, control techniques of power converters, stability of distributed power systems and model predictive control, and cyberattacks of dc microgids.

Subham Sahoo (Senior Member, IEEE) 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 in the Department of Energy, Aalborg University (AAU), Denmark, where he is also the vice-leader of the research group on Reliability of Power Electronic Converters (ReliaPEC) in AAU Energy.

He is a recipient of the Indian National Academy of Engineering (INAE) Innovative Students Project Award for the best PhD thesis across all the institutes in India for the year 2019. He is selected into EU-US National Academy of Engineering (NAE) Frontier of Engineering (FOE) Class of 2021. He was also a distinguished reviewer for IEEE Transactions on Smart Grid in 2020. He is currently the vice-chair of IEEE PELS Technical Committee (TC) 10 on Design Methodologies. He is an Associate Editor on IEEE TRANSACTIONS ON TRANSPORTATION ELECTRIFICATION.

His research interests are control, optimization, cybersecurity and stability of power electronic dominated grids, application of artificial intelligence and machine learning in power electronic systems.

Frede Blaabjerg (Fellow, IEEE) was with ABB-Scandia, Randers, Denmark, from 1987 to 1988. From 1988 to 1992, he got a Ph.D. degree in Electrical Engineering at Aalborg University in 1995. He became an Assistant Professor in 1992, an Associate Professor in 1996, and a Full Professor of power electronics and drives in 1998. From 2017 he became a Villum Investigator. He is honoris causa at University Politehnica Timisoara (UPT), Romania, and Tallinn Technical University (TTU) in Estonia. His current research interests include power electronics and its applications, such as in wind turbines, PV systems, reliability, harmonics, and adjustable speed drives. He has published more than 600 journal papers in the fields of power electronics and its applications. He is the co-author of four monographs and editor of ten books in power electronics and its applications.

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