Quantifying Cyber Attacks on Industrial MMC-HVDC Control System Using Structured Pseudospectrum

Ding, Tao; Zeng, Ziyu; Qin, Boyu; Zhao, Junbo; Yang, Y.; Blaabjerg, F.; Dong, Zhaoyang

Published in:
IEEE Transactions on Power Electronics

DOI (link to publication from Publisher):
10.1109/TPEL.2020.3032883

Publication date:
2020

Document Version
Accepted author manuscript, peer reviewed version

Quantifying Cyber Attacks on Industrial MMC-HVDC Control System Using Structured Pseudospectrum

Tao Ding, *Senior Member, IEEE*, Ziyu Zeng, Boyu Qin, *Member, IEEE*, Junbo Zhao, *Member, IEEE*, Yongheng Yang, *Senior Member*, Frede Blaabjerg, *Fellow, IEEE*, and Zhaoyang Dong, *Fellow, IEEE*

***Abstract*—This letter assesses the impact of cyber-attacks on the control system of the Modular Multilevel Converter (MMC) based High-Voltage DC (MMC-HVDC) transmission technology. Specifically, the small-signal model of the MMC-HVDC is characterized by a closed-loop matrix and the distance to the small-signal instability is then quantified by structured pseudospectrum. Furthermore, a vertical search method is proposed to quantify the boundary of the structured pseudospectrum. The proposed quantification model with the vertical search method can be extended to the control of other power electronics-based systems. Case studies on a two-terminal MMC-HVDC system verify the effectiveness of the qualification method.**

***Index Terms*—MMC-HVDC, cyber physical system, pseudospectrum, robust stability, cyberattacks**

I. Introduction

With the development of power electronics and smart grids, Modular Multilevel Converter based High Voltage Direct Current transmission systems (MMC-HVDC) have been deployed in many countries in recent years to interconnect large-scale offshore wind power systems through long distance cables [1]-[3]. This is still increasing.

Nowadays, the control and physical systems are integrated with the cyber infrastructure, leading to a cyber-physical system (CPS). At the cyber level, the network information of monitoring systems and controllers is interacted on embedded computers. Meanwhile, at the physical level, physical components are controlled to follow signals from the cyber level. Due to the increasing dependence on communication, the CPS security becomes more and more serious. Thus, it requires to fully understand potential impact of successful cyberattacks on the entire system. To do so, for instance, a Bayesian network-based risk assessment method was utilized in [4] to characterize the attack propagation and investigate the impact of cyberattacks on the physical system. A zone partition using an anomaly detection approach was developed in [5] to detect potential cyberattacks. Furthermore, a cooperative stealth cyberattack detection strategy was proposed in [6] to effectively observe the attacked agents under various possible scenarios by using vulnerability factors. An interoperability layer between cyber and physical systems was investigated in [7] without the change of legacy devices for practical industrial systems. In addition, a testbed with the phase-locked-loop (PLL) techniques was set up in [8] to identify undetectable false data injection attacks to distributed energy resource controllers. Event-driven resilient control strategies were subsequently proposed in [9], [10] to mitigate attacks to AC and DC microgrids.

However, the prior-art research has not quantitatively assessed how cyberattacks will affect the system stability. Thus, in this letter, the structured ε-pseudospectrum theory is extended to quantitatively analyze the impact of cyberattacks on the small-signal stability of the MMC-HVDC system. This study in this letter serves to innovate solutions to improving the performance of power electronics-based power systems in terms of anti-cyberattacks. Case studied have validated the efficiency of the proposed quantification with a vertical search method.

T. Ding Z. Zeng and B. Qin are with the State Key Laboratory of Electrical Insulation and Power Equipment, Department of Electrical Engineering, Xi'an Jiaotong University, Xi'an, China (e-mail: tding15@mail.xjtu.edu.cn).

J. Zhao is with Department of Department of Electrical and Computer Engineering, Mississippi State University, Starkville, MS, 39762, USA.

Y. Yang and F. Blaabjerg are with the Department of Energy Technology, Aalborg University, Aalborg DK-9220, Denmark.

Z. Dong is with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW.

II. Small-Signal Model of MMC-HVDC System

According to [2], for a typical MMC-HVDC system, the state-space dynamic model of the MMC power stage can be formulated as

$$\begin{cases} \dfrac{\mathrm{d}I_{\mathrm{sd}}}{\mathrm{d}t}=\dfrac{U_{\mathrm{sd}}}{L_{\mathrm{eq}}}-\dfrac{NU_{\mathrm{cd}}u_{\mathrm{c}}}{L_{\mathrm{eq}}U_{\mathrm{dc}}}-\dfrac{R_{\mathrm{eq}}}{L_{\mathrm{eq}}}I_{\mathrm{sd}}-\omega I_{\mathrm{sq}} \\ \dfrac{\mathrm{d}I_{\mathrm{sq}}}{\mathrm{d}t}=\dfrac{U_{\mathrm{sq}}}{L_{\mathrm{eq}}}-\dfrac{NU_{\mathrm{cq}}u_{\mathrm{c}}}{L_{\mathrm{eq}}U_{\mathrm{dc}}}-\dfrac{R_{\mathrm{eq}}}{L_{\mathrm{eq}}}I_{\mathrm{sq}}+\omega I_{\mathrm{sd}} \\ \dfrac{\mathrm{d}u_{\mathrm{c}}}{\mathrm{d}t}=\dfrac{U_{\mathrm{cd}}I_{\mathrm{sd}}}{4CU_{\mathrm{dc}}}+\dfrac{U_{\mathrm{cq}}I_{\mathrm{sq}}}{4CU_{\mathrm{dc}}}+\dfrac{I_{\mathrm{dc}}}{6C}+\dfrac{U_{\mathrm{cirq}}I_{\mathrm{cirq}}}{2CU_{\mathrm{dc}}}+\dfrac{U_{\mathrm{cird}}I_{\mathrm{cird}}}{2CU_{\mathrm{dc}}} \\ \dfrac{\mathrm{d}I_{\mathrm{dc}}}{\mathrm{d}t}=\dfrac{3U_{\mathrm{dc}}}{2L_{\mathrm{arm}}}-\dfrac{R_{\mathrm{arm}}}{L_{\mathrm{arm}}}I_{\mathrm{dc}}-\dfrac{3Nu_{\mathrm{c}}}{2L_{\mathrm{arm}}} \\ \dfrac{\mathrm{d}I_{\mathrm{cird}}}{\mathrm{d}t}=-\dfrac{NU_{\mathrm{cird}}u_{\mathrm{c}}}{L_{\mathrm{arm}}U_{\mathrm{dc}}}-\dfrac{R_{\mathrm{arm}}}{L_{\mathrm{arm}}}I_{\mathrm{sd}}-2\omega I_{\mathrm{cirq}} \\ \dfrac{\mathrm{d}I_{\mathrm{cirq}}}{\mathrm{d}t}=-\dfrac{NU_{\mathrm{cirq}}u_{\mathrm{c}}}{L_{\mathrm{arm}}U_{\mathrm{dc}}}-\dfrac{R_{\mathrm{arm}}}{L_{\mathrm{arm}}}I_{\mathrm{cirq}}+2\omega I_{\mathrm{cird}} \end{cases} \tag{1}$$

where I_{sd} and I_{sq} are the AC currents in the synchronous dq reference frame; U_{sd} and U_{sq} are the AC voltages at the point of common coupling (PCC) in the dq frame; u_{c} is the voltage of the submodule capacitor with its capacitance being C; I_{dc} and U_{dc} are the DC current and voltage of MMC; ω is the angular frequency of the AC system; U_{cd} and U_{cq} are the outputs of the MMC control system in the dq frame; R_{arm} and L_{arm} are the resistance and inductance of each bridge arm; R_{eq} and L_{eq} are the equivalent resistance and inductance with $R_{\mathrm{eq}} = R_{\mathrm{T}}/2 + R_{\mathrm{arm}}$, $L_{\mathrm{eq}} = L_{\mathrm{T}}/2 + L_{\mathrm{arm}}$ in which R_{T} and L_{T} are the transformer equivalent resistance and inductance, respectively; N indicates the number of submodules; U_{cird}, U_{cirq} are the circulating current suppression voltages; I_{cird}, I_{cirq} are the circulating currents.

The control system consists of vector current controls (VCCs), PLLs and circulating current suppression controllers (CCSCs). The VCC typically adopts the *dq* decoupling control strategy for the power or voltage with proportional-integral (PI) controllers. It should be noted that the proposed method can also be applied to other control strategies, such as voltage balancing and circulating current suppression control. The state-space dynamic model of the control is given as

$$\begin{cases} \dfrac{\mathrm{d}i_{\mathrm{sdm}}}{\mathrm{d}t}=\dfrac{I_{\mathrm{sd}}}{T_{\mathrm{id}}I_{\mathrm{sbase}}}-\dfrac{i_{\mathrm{sdm}}}{T_{\mathrm{id}}},\dfrac{\mathrm{d}i_{\mathrm{sqm}}}{\mathrm{d}t}=\dfrac{I_{\mathrm{sq}}}{T_{\mathrm{iq}}I_{\mathrm{sbase}}}-\dfrac{i_{\mathrm{sqm}}}{T_{\mathrm{iq}}} \\ \dfrac{\mathrm{d}u_{\mathrm{sdm}}}{\mathrm{d}t}=\dfrac{U_{\mathrm{sd}}}{T_{\mathrm{ud}}U_{\mathrm{sbase}}}-\dfrac{u_{\mathrm{sdm}}}{T_{\mathrm{ud}}},\dfrac{\mathrm{d}u_{\mathrm{sqm}}}{\mathrm{d}t}=\dfrac{U_{\mathrm{sq}}}{T_{\mathrm{uq}}U_{\mathrm{sbase}}}-\dfrac{u_{\mathrm{sqm}}}{T_{\mathrm{uq}}} \end{cases} \tag{2}$$

$$\begin{cases} \dfrac{\mathrm{d}x_1}{\mathrm{d}t}=i_{\mathrm{dref}}-i_{\mathrm{sdm}} \\ \dfrac{\mathrm{d}x_2}{\mathrm{d}t}=i_{\mathrm{qref}}-i_{\mathrm{sqm}} \\ \dfrac{\mathrm{d}x_3}{\mathrm{d}t}=P_{\mathrm{ref}}/S_{\mathrm{base}}-P,\ \text{ or }\ \dfrac{\mathrm{d}x_3}{\mathrm{d}t}=U_{\mathrm{dcref}}/U_{\mathrm{dcbase}}-U_{\mathrm{dc}}/U_{\mathrm{dcbase}} \\ \dfrac{\mathrm{d}x_4}{\mathrm{d}t}=Q_{\mathrm{ref}}/S_{\mathrm{base}}-Q \end{cases} \tag{3}$$

where I_{sbase} and U_{sbase} are the base values of the AC current and AC voltage; T_{id}, T_{iq}, T_{ud}, and T_{uq} are the time constants of four first-order measurement elements; i_{sdm}, i_{sqm}, u_{sdm}, and u_{sqm} are the measurement values of I_{sd}, I_{sq}, U_{sd}, and U_{sq}; S_{base} and U_{dcbase} are the base values of the system capacity and DC voltage; P_{ref}, Q_{ref} and U_{dcref} are the reference values of active power, reactive power and DC voltage, respectively; $P=i_{\mathrm{sdm}}u_{\mathrm{sdm}}+i_{\mathrm{sqm}}u_{\mathrm{sqm}}$ denotes the measured active power; $Q=i_{\mathrm{sqm}}u_{\mathrm{sdm}}-i_{\mathrm{sdm}}u_{\mathrm{sqm}}$ denotes the measured reactive power; x_i (i = 1, 2, 3, 4) indicates the intermediate control variables, denoting the integral of the i-th PI controller's error signals. The reference currents i_{dref} and i_{qref} are given as

$$\begin{cases} i_{\mathrm{dref}}=k_{\mathrm{p1}}\left(P_{\mathrm{ref}}/S_{\mathrm{base}}-P\right)+k_{i1}x_3 \\ \text{or } k_{\mathrm{p1}}\left(U_{\mathrm{dcref}}/U_{\mathrm{debase}}-U_{\mathrm{dc}}/U_{\mathrm{dcbase}}\right)+k_{i1}x_3 \\ i_{\mathrm{qref}}=k_{\mathrm{p2}}\left(Q_{\mathrm{ref}}/S_{\mathrm{base}}-Q\right)+k_{i2}x_4 \end{cases} \tag{4}$$

in which k_{pj} and k_{ij} are the proportional and integral gain of the j-th PI controller, respectively.

The outputs of the MMC control system U_{cd} and U_{cq} are the dynamic phasors of the fundamental frequency components in the *dq* frame that can be expressed as

$$\begin{cases} U_{\mathrm{cd}}=U_{\mathrm{sbase}}\left(U_{\mathrm{sdm}}-\dfrac{\omega L_{\mathrm{eq}}}{Z_{\mathrm{base}}}i_{\mathrm{sqm}}-k_{\mathrm{p3}}\left(i_{\mathrm{dref}}-i_{\mathrm{sdm}}\right)-k_{\mathrm{i3}}x_1\right) \\ U_{\mathrm{cq}}=U_{\mathrm{sbase}}\left(U_{\mathrm{sqm}}+\dfrac{\omega L_{\mathrm{eq}}}{Z_{\mathrm{base}}}i_{\mathrm{sdm}}-k_{\mathrm{p4}}\left(i_{\mathrm{qref}}-i_{\mathrm{sqm}}\right)-k_{\mathrm{i4}}x_2\right) \end{cases} \tag{5}$$

with $Z_{\mathrm{base}}=U_{\mathrm{sbase}}^2/S_{\mathrm{base}}$.

The CCSC contains two PI controllers, the dynamics of which can be expressed as

$$\frac{\mathrm{d}f_1}{\mathrm{d}t}=I_{\mathrm{cirdref}}-I_{\mathrm{cird}},\qquad \frac{\mathrm{d}f_2}{\mathrm{d}t}=I_{\mathrm{cirqref}}-I_{\mathrm{cirq}} \tag{6}$$

with I_{cirdref} and I_{cirqref} being the reference value of the circulating current. f_1 and f_2 indicate the intermediate control variables, denoting the integral of the PI controller's error signals

The output of the CCSC, which is denoted by U_{cird} and U_{cirq}, can be expressed as

$$\begin{cases} U_{\mathrm{cird}}=k_{\mathrm{pcir}}\left(I_{\mathrm{cirdref}}-I_{\mathrm{cird}}\right)+k_{\mathrm{icir}}f_1+2\omega L_{\mathrm{arm}}I_{\mathrm{cirq}} \\ U_{\mathrm{cirq}}=k_{\mathrm{pcir}}\left(I_{\mathrm{cirqref}}-I_{\mathrm{cirq}}\right)+k_{\mathrm{icir}}f_2-2\omega L_{\mathrm{arm}}I_{\mathrm{cird}} \end{cases} \tag{7}$$

in which k_{pcir} and k_{icir} are the proportional and integral gain of the PI controllers in the CCSC.

The dynamic of the PLL can be described as

$$\begin{cases} \dfrac{\mathrm{d}x_5}{\mathrm{d}t}=U_{\mathrm{sq}} \\ \dfrac{\mathrm{d}x_{\mathrm{pll}}}{\mathrm{d}t}=-k_{\mathrm{ppll}}U_{\mathrm{sq}}-k_{\mathrm{ipll}}x_5 \end{cases} \tag{8}$$

where k_{ppll} and k_{ipll} are the parameters of the PLL; x_5 and x_{pll} are the intermediate control variables, denoting the integral of the PI controller's error signals in PLL.

The outputs of the PLL can be expressed as

$$\begin{cases} \theta=\omega_0 t+x_{\mathrm{pll}} \\ \omega=\omega_0-k_{\mathrm{ppll}}U_{\mathrm{sq}}-k_{\mathrm{ipll}}x_5 \end{cases} \tag{9}$$

where ω_0 is the angle frequency reference value of AC system; θ is the phase signal park transforms.

The AC system is modelled by a resistance-inductance series circuit with an ideal AC voltage source. The AC voltage at PCC satisfies the following differential equations:

$$\begin{cases} U_{\mathrm{sd}}=U_{\mathrm{ed}}-R_{\mathrm{ac}}I_{\mathrm{sd}}-L_{\mathrm{ac}}\dfrac{\mathrm{d}I_{sd}}{\mathrm{d}t}-\omega L_{\mathrm{ac}}I_{\mathrm{sq}} \\ U_{\mathrm{sq}}=U_{\mathrm{eq}}-R_{\mathrm{ac}}I_{\mathrm{sq}}-L_{\mathrm{ac}}\dfrac{\mathrm{d}I_{\mathrm{sq}}}{\mathrm{d}t}+\omega L_{\mathrm{ac}}I_{\mathrm{sd}} \end{cases} \tag{10}$$

where U_{ed} and U_{eq} are the voltages of an ideal AC voltage source in the *dq* frame; R_{ac} and L_{ac} are the equivalent AC resistance and inductance, respectively.

The DC system can be represented by a resistance inductance series circuit as

$$\frac{\mathrm{d}I_{\mathrm{dc}}}{\mathrm{d}t}=\frac{U_{\mathrm{dc1}}}{L_{\mathrm{d}}}-\frac{U_{\mathrm{dc2}}}{L_{\mathrm{d}}}-\frac{R_{\mathrm{d}}I_{\mathrm{dc}}}{L_{\mathrm{d}}} \tag{11}$$

in which U_{dc1} and U_{dc2} are the DC voltages at each end of the DC line; R_{d} and L_{d} are the equivalent resistance and inductance, respectively.

The above small-signal models of a typical MMC-HVDC system can be formulated in a compact way as

$$\begin{cases} \dot{\boldsymbol{x}}=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{B}\boldsymbol{u} \\ \boldsymbol{y}=\boldsymbol{C}\boldsymbol{x} \end{cases},\quad \begin{cases} \dot{\boldsymbol{x}}_c=\boldsymbol{A}_c\boldsymbol{x}_c+\boldsymbol{B}_c\boldsymbol{u}_c \\ \boldsymbol{y}_c=\boldsymbol{C}_c\boldsymbol{x}_c+\boldsymbol{D}_c\boldsymbol{u}_c \end{cases} \tag{12}$$

in which $\boldsymbol{x}\in\mathbb{R}^n$, $\boldsymbol{u}\in\mathbb{R}^p$, $\boldsymbol{y}\in\mathbb{R}^q$, $\boldsymbol{x_c}\in\mathbb{R}^m$, $\boldsymbol{u_c}\in\mathbb{R}^q$, and $\boldsymbol{y_c}\in\mathbb{R}^p$ are the system state vector, the control input vector, the output vector, the control state vector, the stabilizing signal vector and the controller output vector, respectively; $\boldsymbol{A}\in\mathbb{R}^{n\times n}$, $\boldsymbol{B}\in\mathbb{R}^{n\times p}$, and $\boldsymbol{C}\in\mathbb{R}^{q\times n}$ are the coefficient matrices of the power systems; $\boldsymbol{A_c}\in\mathbb{R}^{m\times m}$, $\boldsymbol{B_c}\in\mathbb{R}^{m\times q}$, $\boldsymbol{C_c}\in\mathbb{R}^{p\times m}$, and $\boldsymbol{D_c}\in\mathbb{R}^{p\times q}$ are the coefficient matrices of the control systems. Using the augmented vector $\boldsymbol{x}_a=[\boldsymbol{x}^T,\boldsymbol{x}_c^T]^T$, $\boldsymbol{u}_a=[\boldsymbol{u}^T,\boldsymbol{u}_c^T]^T$ and $\boldsymbol{y}_a=[\boldsymbol{y}^T,\boldsymbol{y}_c^T]^T$, an augmented system model can be derived according to [11] as

$$\begin{cases} \dot{\boldsymbol{x}}_a=\boldsymbol{A}_a\boldsymbol{x}_a+\boldsymbol{B}_a\boldsymbol{u}_a \\ \boldsymbol{y}_a=\boldsymbol{C}_a\boldsymbol{x}_a,\ \boldsymbol{u}_a=-\boldsymbol{K}\boldsymbol{y}_a \end{cases} \tag{13}$$

$$\boldsymbol{A}_a=\begin{bmatrix}\boldsymbol{A} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{0}\end{bmatrix},\ \boldsymbol{B}_a=\begin{bmatrix}\boldsymbol{B} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{I}\end{bmatrix},\boldsymbol{C}_a=\begin{bmatrix}\boldsymbol{C} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{I}\end{bmatrix},\ \boldsymbol{K}=\begin{bmatrix}\boldsymbol{D}_c & \boldsymbol{C}_c\\ \boldsymbol{B}_c & \boldsymbol{A}_c\end{bmatrix} \quad (14)$$

which leads to the closed-loop matrix:

$$\boldsymbol{A}_{cl}=\boldsymbol{A}_a+\boldsymbol{B}_a\boldsymbol{K}\boldsymbol{C}_a \quad (15)$$

Accordingly, the system is stable if and only if all the eigenvalues of the closed-loop matrix $\boldsymbol{A}_{cl}$ lie in the open left-half plane of the complex plane; otherwise, it is unstable. Denote the unstable region to be $\mathbb{C}_b$ and its boundary to be $\partial\mathbb{C}_b$.

Since the control system (including parameters, topology, etc.) is attacked by any type of cyberattacks, the gain matrix $\boldsymbol{K}$ in (15) will be disturbed to be $\bar{\boldsymbol{K}}=\boldsymbol{K}+\Delta$, where the attack matrix Δ is also an uncertain matrix that can be any value resulted from the cyberattacks. Then, we will use the uncertain attack matrix Δ to describe the cyberattack. Mathematically, the 2-norm of the attack matrix Δ, i.e., $\|\Delta\|_2$, can be used to quantify the severity from the attack matrix. The closed-loop matrix for the system under attacks will become

$$\bar{\boldsymbol{A}}_{cl}=\boldsymbol{A}_a+\boldsymbol{B}_a\bar{\boldsymbol{K}}\boldsymbol{C}_a=\boldsymbol{A}_{cl}+\boldsymbol{B}_a\Delta\boldsymbol{C}_a \quad (16)$$

A question can then be raised—how large should the attack matrix Δ be so that the system may suffer from small-signal instabilities? Intuitively, if $\|\Delta\|_2$ is sufficiently small, the stability of the system will not be affected (i.e., the eigenvalues of $\bar{\boldsymbol{A}}_{cl}$ still lie in the open left-half plane). With the increase of $\|\Delta\|_2$, the stability margin decreases. Up to a certain value $\|\Delta\|_2^{\max}$, the system becomes unstable. We define the distance from the current stable point to unstable status as the distance to instability subject to attacks with the matrix Δ. This distance will strictly characterize the relationship between the 2-norm $\|\Delta\|_2$ and the system instability. To calculate this distance, the ε-pseudospectrum is introduced. Let $\bar{\Delta}=\boldsymbol{B}_a\Delta\boldsymbol{C}_a$ be the disturbance matrix of the attack matrix Δ in the closed-loop system matrix. The ε-pseudospectrum is defined as

$$\Lambda_\varepsilon\left(\boldsymbol{A}_{cl}\right)=\left\{z\in\ \ :\ \det\left(\boldsymbol{A}_{cl}+\bar{\Delta}-z\boldsymbol{I}\right)=0,\forall\left\|\bar{\Delta}\right\|\le\varepsilon\right\} \quad (17)$$

According to [12] and [13], the definition of the pseudospectrum by (17) can be rewritten as

$$\Lambda_\varepsilon\left(\boldsymbol{A}_{cl}\right)=\left\{z\in\ \ :\ \sigma_{\min}\left(\boldsymbol{A}_{cl}-z\boldsymbol{I}\right)\le\varepsilon\right\} \quad (18)$$

where $\sigma_{\min}(\cdot)$ is the minimum singular value. Clearly, the distance to the instability under the disturbance matrix $\bar{\Delta}$ is the largest distance when the attacked system is just on the boundary of stability, yielding

$$\beta\left(\boldsymbol{A}_{cl}\right)=\inf\left\{\left\|\bar{\Delta}\right\|_2:\ \ \boldsymbol{A}_{cl}+\bar{\Delta}\in\partial\ \ _b,\forall\left\|\bar{\Delta}\right\|\le\varepsilon\right\} \quad (19)$$

which means that there is at least one eigenvalue only with an imaginary part. Moreover, according to the equivalence between (17) and (18), we can obtain

$$\beta\left(\boldsymbol{A}_{cl}\right)=\inf_{z\in\partial\ \ _b}\left\{\sigma_{\max}^{-1}\left(\boldsymbol{A}_{cl}-z\boldsymbol{I}\right)\right\}=\inf_{\omega\in}\left\{\sigma_{\min}\left(\boldsymbol{A}_{cl}-i\omega\boldsymbol{I}\right)\right\} \quad (20)$$

It should be noted that the distance to instability under any disturbance matrix $\bar{\Delta}$ can be inferred by (20). However, the original attack matrix Δ is a control matrix. As a result, the distance of the attack matrix Δ should be calculated instead of using the disturbance matrix $\bar{\Delta}$. To achieve so, a structured ε-pseudospectrum scheme is proposed to assess the impacts of the attack matrix Δ on the system closed-loop matrix $\boldsymbol{A}_{cl}$. Similar to the results in (19), let $\beta(\boldsymbol{A}_{cl}, \boldsymbol{B}_a, \boldsymbol{C}_a)$ be the structured ε-pseudospectrum, and then, we have

Table I. The flowchart of the vertical search method.

Steps	
	Input: Given $(\boldsymbol{A}_{cl}, \boldsymbol{B}_a, \boldsymbol{C}_a)$ and the convergence error δ
	Output: Distance to instability $\beta(\boldsymbol{A}_{cl}, \boldsymbol{B}_a, \boldsymbol{C}_a)$
1	Set $j\leftarrow 0$, $\Phi^0=\{\omega_0\}$ with $\omega_0\in\partial\ \ _b$ and $\beta^0\leftarrow$a large number;
2	**while 1**
3	$\beta^{j+1}=\min\{g(\omega):\ \ \omega\in\Phi^j\}$;
4	Compute the eigenvalues of $V(0,\beta^{j+1})$ and extract the eigenvalues whose real parts are close enough to 0, such that $\Gamma^{j+1}=\left\{\omega_0,\omega_1,...,\omega_{s_{j+1}}\right\}$;
5	**if** $\Gamma^{j+1}=[]$
6	$\Phi^{j+1}=[]$, **goto 13**;
7	**end**
8	Select ω form Γ^{j+1} with $g(\omega)=\beta^{j+1}$, giving the set of intersection points $\Omega=\left\{\omega_0,\omega_1,...,\omega_{m_{j+1}}\right\}$;
9	**if** $\Omega=[]$
10	$\Phi^{j+1}=[]$, **goto 14**;
11	**end**
12	Obtain the open intervals $\left(l_d^{j+1},u_d^{j+1}\right)$ for $d=1,...,m_{j+1}$, where $\forall\omega_d\in\left(l_d^{j+1},u_d^{j+1}\right)$, $g(\omega_d)<\beta^{j+1}$;
13	Calculate $\Phi^{j+1}=\left(u_d^{j+1}+l_d^{j+1}\right)/2$ for $d=1,...,m_{j+1}$;
14	$j\leftarrow j+1$;
15	**if** $\beta^{j-1}-\beta^j\le\delta\mid\Phi^j=[]$
16	**return** β^j;
17	**end**
18	**end**

$$\beta\left(\boldsymbol{A}_{cl},\boldsymbol{B},\boldsymbol{C}\right)=\inf\left\{\left\|\Delta\right\|_2:\ \ \boldsymbol{A}_{cl}+\boldsymbol{B}_a\Delta\boldsymbol{C}_a\in\partial\ \ _b,\forall\left\|\Delta\right\|\le\varepsilon\right\} \quad (21)$$

It is further noted that the unstructured ε-pseudospectrum boundary from (19) is a special case of (20) with $\beta(\boldsymbol{A}_{cl}, \boldsymbol{I}, \boldsymbol{I})$. The matrix $\boldsymbol{A}_{cl}+\boldsymbol{B}_a\Delta\boldsymbol{C}_a\in\partial\mathbb{C}_b$ indicates $\det(i\omega\boldsymbol{I}-\boldsymbol{A}_{cl}-\boldsymbol{B}_a\Delta\boldsymbol{C}_a)=0$. That means, $\exists\|\boldsymbol{v}\|\neq\boldsymbol{0}$, $(i\omega\boldsymbol{I}-\boldsymbol{A}_{cl}-\boldsymbol{B}_a\Delta\boldsymbol{C}_a)\boldsymbol{v}=0$. Multiplying $\Delta\boldsymbol{C}_a(i\omega\boldsymbol{I}-\boldsymbol{A}_{cl})^{-1}$ on both sides of the equation yields $\det(\boldsymbol{I}-\Delta\boldsymbol{C}_a(i\omega\boldsymbol{I}-\boldsymbol{A}_{cl})^{-1}\boldsymbol{B}_a)=0$. Furthermore, according to [13], (21) can be reformulated as

$$\beta\left(\boldsymbol{A}_{cl},\boldsymbol{B}_a,\boldsymbol{C}_a\right)=\inf_{\omega\in}g\left(\omega\right)=\inf_{\omega\in}\left\{\sigma_{\max}^{-1}\left(\boldsymbol{C}_a\left(\boldsymbol{A}_{cl}-i\omega\boldsymbol{I}\right)^{-1}\boldsymbol{B}_a\right)\right\} \quad (22)$$

A vertical search method is designed to solve the optimization model and find the boundary of the proposed structured ε-pseudospectrum. The main flowchart is shown in Table I. Given the estimated $\beta^j(\boldsymbol{A}_{cl}, \boldsymbol{B}_a, \boldsymbol{C}_a)$, we can obtain ω^j according to **Theorem 1**. Furthermore, ω^j is corrected to be ω^{j+1} and $\beta(\boldsymbol{A}_{cl}, \boldsymbol{B}_a, \boldsymbol{C}_a)$ is gradually updated by $\beta^{j+1}=(\boldsymbol{A}_{cl}, \boldsymbol{B}_a, \boldsymbol{C}_a)=\inf\{g(\omega^{j+1})\}$. Note that correcting ω^j requires the intersection points on the ε-pseudospectrum boundary (i.e., satisfying $g(\omega^j)=\beta^{j+1}$). Since the singular value function $g(\omega)$ is a continuous function for ω, we can split the space ω-$g(\omega)$ (a.k.a., ω-β) into several alternative intervals. In Fig. 1, the intervals (l_d^{j+1}, u_d^{j+1}), $d=1,\ldots,m_{j+1}$ should be calculated in a way that $g(\omega)<\beta^{j+1}$ is satisfied for $\forall\ \omega_d\in(l_d^{j+1}, u_d^{j+1})$. Then, ω^j is approximately updated by a series of points, which are the midpoints of each interval.

Theorem 1 [13]: Let x and ε be positive real numbers. ε is one singular value of $\boldsymbol{A}_{cl}-(x+i\omega)\boldsymbol{I}$, if and only if the Hamiltonian matrix given in (23) has the imaginary eigenvalue of $i\omega$.

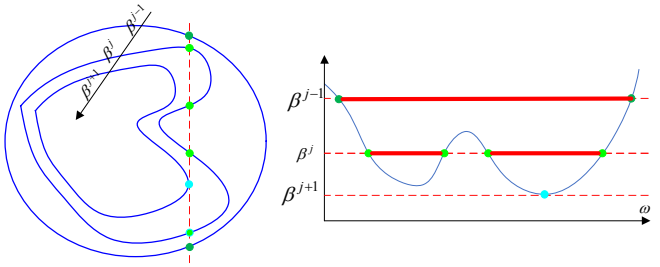

Fig. 1. Intervals in the space of ω-$g(\omega)$.

$$V(x,\varepsilon)=\begin{bmatrix} xI-A_{cl}^{H} & \varepsilon I \\ -\varepsilon I & A_{cl}-xI \end{bmatrix} \tag{23}$$

Last but not least, the proposed method is conducted under the given system parameters and operation points. Certainly, the quantification result can be affected by various parameters uncertainty or variation of operating points. Thus, the proposed method can be utilized for real-time quantification, where the metric $\|\Delta\|_2^{mx}$ can be calculated at each period even when system parameters or operation points are changed.

III. Case Studies

The effectiveness of the proposed method is validated through simulations on a two-terminal MMC-HVDC transmission system, whose parameters can be found in [14]. The test system is depicted in Fig. 2, where the MMC-HVDC system comprises two MMC stations (MMC1 and MMC2) and DC transmission lines. The control system consists of VCCs, PLLs and CCSCs, where PI controllers are designed for each control part, as shown in Fig. 3. Note that the MMC can adopt either an active/reactive power control mode or a DC voltage/reactive power control mode. In the study system, MMC1 adopts the active/reactive power control and MMC2 is controlled in the DC voltage/reactive power mode. The small-signal model is derived for both control systems for the MMC stations shown in Fig. 2 (i.e., MMC1 and MMC2). According to the control modes adopted for the MMC stations, the small signal model with the inputs of the active and reactive power is used for MMC1, while MMC2 adopts the small signal model with the inputs of the DC voltage and reactive power.

The feedback gains indicated by $\boldsymbol{K}$ in this letter is derived through the linearization of the state space model of the control system. Moreover, inserting PI controllers will only increase the order of the control system, which, however, does not affect the proposed quantification method. The PI parameters are designed by an off-line dynamic simulation with a set of typical values under various working conditions. The detailed data can be found in [14]. The inputs of the MMC control systems consist of two kinds of variables, which can be attacked by the cyber-attackers. More specifically, one contains the measurements of electrical variables of the system. The other kind contains the reference values of the control demands. That is, the VCC of each MMC adopts the *dq* decoupling control strategy for powers or voltages. The CCSC suppresses the circulating current by providing the circulating current suppression voltages to the bridge arms of the MMC. The outputs of the VCC are the dynamic phasors of the fundamental frequency components in the *dq* frame. The output of the PLL is

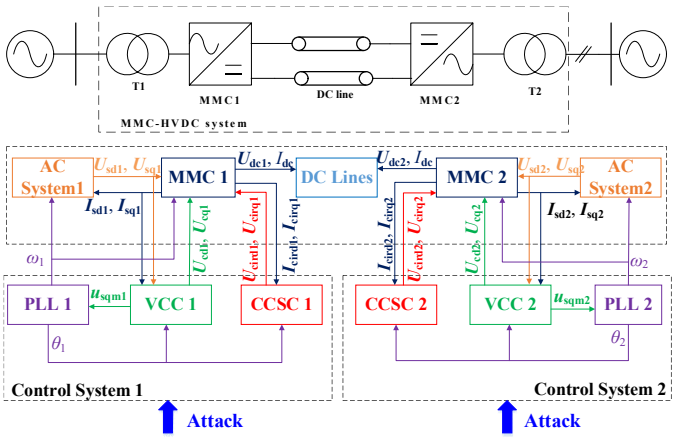

Fig. 2. System diagram of the two-terminal MMC-HVDC system.

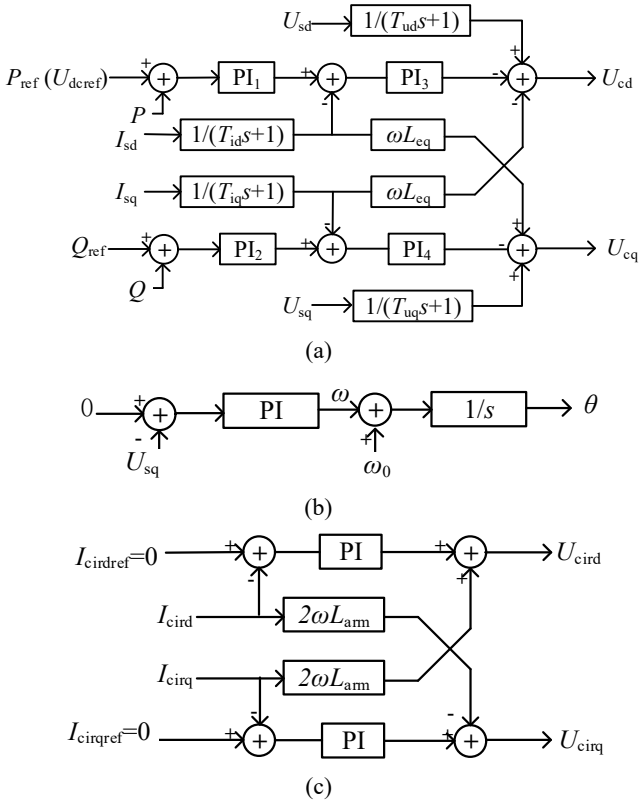

Fig. 3. Details of the control system for the MMC-HVDC in Fig. 2: (a) vector current control, (b) phase-locked loop, and (c) circulating current suppression control.

the phase signal park transforms. The output of the CCSC is the circulating current suppression voltage.

Using the proposed quantification method, the distance to instability is found to be 0.9456 for the current operating point in presence of cyberattacks. To verify the calculated result from the statistical perspective, another two distances are selected as 0.93 and 0.95 for comparison. Choosing 10000 samples with random attack matrices for the control system, the distribution of eigenvalues under different cyber-attacks is depicted in Fig. 4. It can be observed in Fig. 4 that if the distance to instability is 0.93 (smaller than 0.9456), the maximum real part of eigenvalues is – 0.73, which suggests that the system is always stable for any attacks. By contrast, if the distance to instability is 0.95 (larger than 0.9456), the maximum real part of eigenvalues is

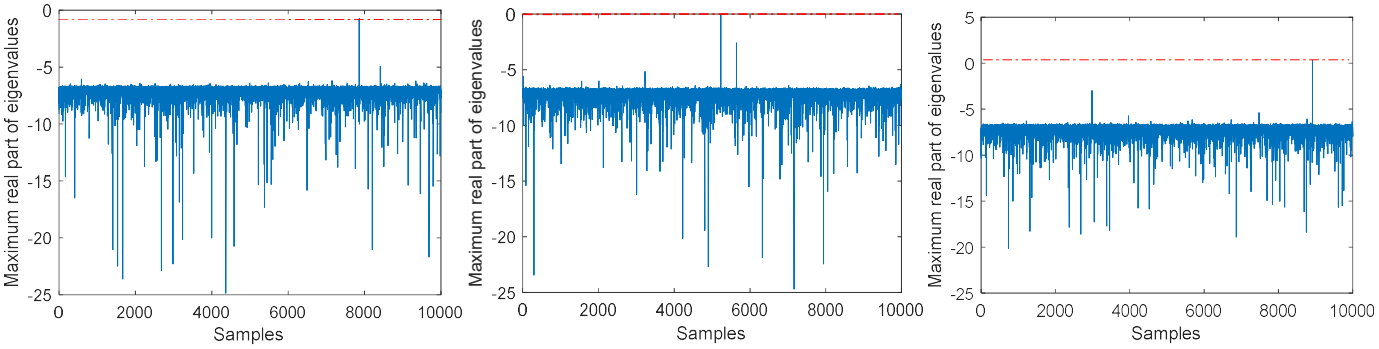

Fig. 4. Distribution of eigenvalues under different cyberattacks for the control system: (a) distance to instability is 0.93, (b) distance to instability is 0.9456, and (c) distance to instability is 0.95.

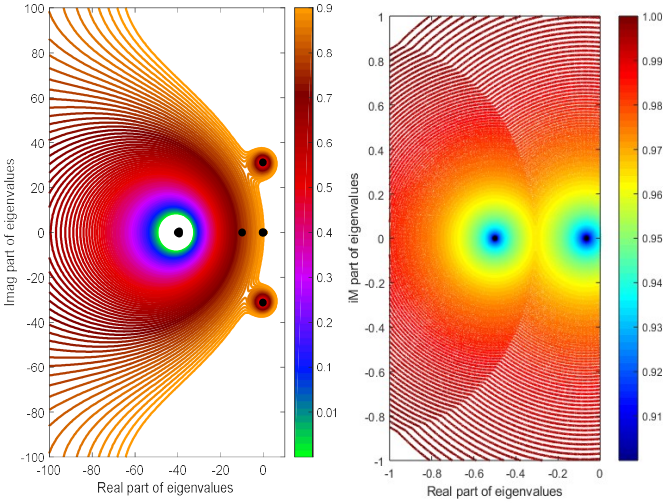

Fig. 5. Boundary of the structured pseudospectrum under two scales.

0.02, which implies that the system may lose the stability under certain attacks. If the distance to instability is 0.9456, the maximum real part of eigenvalues is nearly zero, which indicates that the system is stable for almost all the attacks except for specific attacks that may lead to the critical stability.

Finally, the boundary of the structured pseudospectrum under different scales is shown in Fig. 5. The pseudospectrum boundary is around the eigenvalues of the un-attacked matrix (see the left sub-figure). Focusing on the rightmost two eigenvalues, the pseudospectrum boundary is plotted with distance to be [0.9, 1.0]. It can be found that when the distance is small, the entire circle lies in the open left-half plane. With the increase of the distance, the circle for the rightmost eigenvalue approaches to the right-half plane, leading to system instability.

IV. Conclusions

In this letter, a structured pseudospectrum and a vertical search method are proposed to quantify the small-signal stability margin subject to cyberattacks on the MMC-HVDC control system. Simulation results carried out on a practical test system have demonstrated that the proposed method can quantitatively characterize the impact of the cyberattacks on the system small-signal stability by attack matrices. Increasing the distance to instability of attack matrices, the rightmost eigenvalues of the control system approaches to the right-half plane and the system becomes more instable. The proposed method can provide insights for the development of anti-cyberattacks strategies for power electronics-based power systems.

References

[1] M. Amin and M. Molinas, “Understanding the origin of oscillatory phenomena observed between wind farms and HVDC systems,” *IEEE J. Emerg. Sel. Top. Power Electron.*, vol. 5, no. 1, pp. 378-392, Mar. 2017.

[2] T. Li, A. M. Gole and C. Zhao, "Harmonic Instability in MMC-HVDC Converters Resulting from Internal Dynamics," *IEEE Trans. Power Del.*, vol. 31, no. 4, pp. 1738-1747, Aug. 2016.

[3] Q. R. Hao, Z. Li, F. Gao, and J. Zhang, “Reduced-Order Small-Signal Models of Modular Multilevel Converter and MMC-Based HVdc Grid,” *IEEE Trans. Ind. Electron.*, vol. 66, no. 3, pp. 2257–2268, Mar. 2019.

[4] K. X. Huang, C. J. Zhou, Y. C. Tian, S. Yang, and Y. Qin, “Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems,” *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 8153–8162, Oct. 2018.

[5] J. Yang, C. J. Zhou, S. H. Yang, H. Z. Xu, and B. Hu, “Anomaly detection based on zone partition for security protection of industrial cyber-physical systems,” *IEEE Trans. Ind. Electron.*, vol. 65, no. 5, pp. 4257-4267, 2018.

[6] S. Sahoo, S. Mishra, J. Peng and T. Dragicevic, “A Stealth Cyber-Attack Detection Strategy for DC Microgrids,” *IEEE Trans. Power Electron.,* vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[7] O. Givehchi, K. Landsdorf, and P. Simoens, “Interoperability for industrial cyber-physical systems: an approach for legacy systems,” *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3370–3378, 2017.

[8] H. Albunashee, C. Farnell, A. Suchanek, K. Haulmark, R. McCann, J. Di, and A. Mantooth, "A testbed for detecting false data injection attacks in systems with distributed energy resources," *IEEE J. Emerg. Sel. Top. Power Electron.,* Early Access, 2020.

[9] S. Sahoo, Y. Yang, and F. Blaabjerg, "Resilient synchronization strategy for ac microgrids under cyberattacks," *IEEE Trans. Power Electron.,* vol. 36, no. 1, pp. 73-77, Jan. 2021.

[10] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters–challenges and vulnerabilities," *IEEE J. Emerg. Sel. Top. Power Electron*., Early Access, 2020.

[11] M. Amin, M. Molinas, J. Lyu, and X. Cai, "Impact of Power Flow Direction on the Stability of VSC-HVDC Seen from the Impedance Nyquist Plot," *IEEE Trans. Power Electron.,* vol. 32, no. 10, pp. 8204-8217, 2017.

[12] G. K. Dill and A. S. e Silva, “Robust design of power system controllers based on optimization of pseudospectral functions”, *IEEE Trans. on Power Syst.*, vol. 28, no. 2, 2013, pp. 1756-1765.

[13] J. V. Burke, A. S. Lewis, and M. L. Overton, “Robust stability and a crisscross algorithm for pseudospectra”, *IMA Journal of Numerical Analysis*, vol. 23, no. 3, 2003, pp. 359-375.

[14] https://github.com/QuDaming/MMC_HVDC/blob/master/MMC_HVDC.m