

# On Resilience Analysis and Quantification for Wide-Area Control of Power Systems

Yueyun Lu, Chin-Yao Chang, Wei Zhang, Laurentiu D. Marinovici and Antonio J. Conejo

**Abstract**—Wide-area control is an effective mean to reduce inter-area oscillations of large power systems. Its dependence on communication of remote measurement signals makes the closed-loop system vulnerable to cyber attacks. This paper develops a framework to analyze and quantify resilience of a given wide-area controller under disruptive attacks on certain communication links. Resilience of a given controller is measured in terms of closed-loop eigenvalues under the worst possible attack strategy. The computation of such a resilience index is challenging especially for large-scale power systems due to the discrete nature of the attack strategies. To address the challenge, we propose an optimization-based formulation and a convex relaxation approach to facilitate the computation. Conditions under which the relaxation is exact are derived and an efficient algorithm with guaranteed convergence is also developed. The proposed framework and the algorithm allow us to quantify resilience for given wide-area controllers and also provide sufficient conditions to guarantee closed-loop stability under all possible communication attacks. Simulations are performed on the IEEE 39-bus system to illustrate the proposed resilience analysis and computation framework.

## I. INTRODUCTION

With the power grid increasingly working close to its operation limit, inter-area oscillation becomes ever more lightly damped, which easily results in instability [1]. Local decentralized controllers, such as power system stabilizers (PSSs), are designed to suppress local oscillations. They may interact in an adverse way, if not carefully tuned, that aggravates inter-area oscillations. Motivated by the advancement in the Wide-Area Measurement System (WAMS) technology, recent research efforts have been focusing on wide-area control (WAC) problems [2], [3], [4]. The goal of WAC is to achieve better closed-loop performance, such as inter-area oscillation damping, by the use of remote measurement signals via the Phasor Measurement Units (PMUs) installed across the grid.

One important class of literature on WAC is concerned with optimal control design under certain performance met-

ric. The main control objective is inter-area oscillation damping, for which various metrics have been proposed. In the design of supplementary damping controller (SDC) using Linear Parameter Varying (LPV) model [5], the metric is given by the signal amplification from disturbance to output. To design FACTS (Flexible AC Transmission Systems)-based control facilitated by an aggregate model [6], the metric is defined on the closed-loop transient response of inter-area oscillation modes. A mixed  $H_2/H_\infty$  output feedback control design is studied in [7] where the metric is concerned with geometric measures of modal controllability/observability. Another control objective is voltage stability. For the automatic scheduling and coordination of voltage control devices [8], [9], [10], the metric is composed of several terms regarding switching cost, penalty on voltage violations and penalty on circular VAR flow. Typically, the controllers are designed for a fixed structure, that is to say, the communication network has a pre-specified structure. There has been a recent interest in incorporating communication structure into the design. Due to the fact that most optimal control formulations result in controllers without any sparsity pattern and require centralized implementation, a sparsity-promoting optimal control scheme is proposed in [11] where the  $\ell_1$  regularization term in the objective accounts for the structural design.

Another body of literature is concerned with delays and failures arising in the communication network of WAMS. To deal with network delays, a predictor-based  $\mathcal{H}_\infty$  control design strategy is discussed in [4] to account for a delayed arrival of feedback signals. Furthermore, an arbitration approach is proposed in [12] to exploit the flexibility of communication network so that the designed controllers are in sync with network delays, making the closed-loop system delay-aware, rather than just delay-tolerant. To counteract the impact of communication failures on the closed-loop system, a framework proposed in [13] utilizes a hierarchical set of wide-area measurements for feedback and employs channel switching based on mathematical morphology identification.

Existing works on WAC resilience mostly focus on communication delays or failures. There has been limited discussion on resilience under adversaries. Due to the increasing threat on cyber security [14], [15], remote signal transmission via communication channels is prone to cyber attacks. As WAC relies heavily on the availability of remote signals, the integrity of communication network plays a crucial role in the closed-loop performance. In this paper, we consider the adversary has disruptive resources [15] that can result in unavailability of the signals transmitted over communication

Y. Lu, C.-Y. Chang are with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210, USA

W. Zhang is with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210, USA, with a joint appointment in the Electricity Infrastructure Group, Pacific Northwest National Laboratory, Richland, WA 99354, USA

L. D. Marinovici is with the Electricity Infrastructure Group, Pacific Northwest National Laboratory, Richland, WA 99354, USA

A. J. Conejo is with the Departments of Electrical and Computer Engineering and the Department of Integrated Systems Engineering, The Ohio State University, Columbus, OH 43210, USA

This work was funded by Laboratory Directed Research and Development funding under the Control of Complex Systems Initiative at Pacific Northwest National Laboratory, which is operated for the US Department of Energy by Battelle Memorial Institute under Contract DE-AC05-76RL01830.

channels. Such an attack model is commonly referred to as Denial of Service (DoS) attack [16]. To launch a DoS attack, the adversary can jam the communication channels, compromise devices and prevent them from sending data, attack the routing protocols, flood network traffic, among others. Our goal is to develop a framework to analyze and quantify resilience under DoS attacks. In particular, we aim to design effective ways to determine whether a given wide-area controller is resilient, and how resilient it is under certain attack strategy. To achieve this, we use network-reduced linearized power system model under linear feedback control. Such a model is widely used in the literature on WAC problems [5], [10], [6], [17], [7]. We first define resilience in terms of closed-loop spectral abscissa (the largest real part of eigenvalues) under the worst possible attack strategy. The direct computation of such a resilience metric is challenging, especially in large-scale network due to its combinatorial nature. We then propose an equivalent optimization-based formulation and a convex relaxation approach to facilitate the computation. On the theoretic side, we derive a condition under which the relaxation is exact. On the practical side, we develop an efficient algorithm for the relaxed problem with guaranteed convergence. The algorithm not only provides resilience criterion but also reveals structural vulnerabilities. These results contribute new perspectives to WAC with an emphasis on resilience under DoS communication attacks. They also allow us to systematically analyze resilience properties of a given wide-area controller.

## II. PROBLEM FORMULATION

In this paper, we consider a network-reduced power system model commonly used in the literature [18], [12], [5], [10], [6], [17], [7]. The overall power system is represented by an interconnected dynamical system defined on a graph  $\mathcal{G} = (\mathcal{N}, \mathcal{E})$ , where  $\mathcal{N} \triangleq \{1, \dots, N\}$  denotes the set of buses and  $\mathcal{E}$  denotes the set of transmissions lines between buses. Let  $x_i(t) \in \mathbb{R}^{n_i}$  be the state variables associated with bus  $i$ . Depending on the level of details used in the generator model,  $x_i$  can represent generator phase angle, frequency, quadrature-axis internal emf, state variables of Power System Stabilizer (PSS) or other local controllers. Typically, local dynamics and local controllers can be described by linear systems subject to nonlinear coupling terms due to power exchange with neighboring buses. The overall system can be written is the following form:

$$\dot{x}_i = A_{ii}x_i + c_i + \sum_{(i,j) \in \mathcal{E}, j \neq i} h(x_i, x_j),$$

where  $A_{ii} \in \mathbb{R}^{n_i \times n_i}$  is the system matrix that has incorporated local controls,  $c_i$  is a constant term regarding mechanical power input and  $h(x_i, x_j)$  is a nonlinear function representing the power flow between buses  $i$  and  $j$ . By linearization at a stationary operating point, we arrive at a distributed control system of the following form:

$$\dot{x}_i = A_{ii}x_i + \sum_{j \in \mathcal{N}, j \neq i} A_{ij}x_j + B_i u_i, \quad i \in \mathcal{N}, \quad (1)$$

where with slight abuse of notation,  $x_i$  represents the deviation of state variables from the nominal operating point,  $A_{ij}$  captures the linearized coupling between buses  $i$  and  $j$  ( $A_{ij} = 0$  if there is no coupling), and  $B_i u_i$  is an introduced wide-area control action that reacts to deviations from the nominal operating point based on both local and remote state information. We consider wide-area control  $u_i$  to be composed of local component  $u_{i,loc}$  that depends on local state information and wide-area component  $u_{i,wac}$  that depends on remote state information in the following form:

$$u_i = u_{i,loc} + u_{i,wac} = K_{ii}x_i + \sum_{j \in \mathcal{N}, j \neq i} K_{ij}x_j, \quad (2)$$

where  $K_{ij} \in \mathbb{R}^{m_i \times n_j}$ ,  $i, j \in \mathcal{N}$  are feedback gains. The local component  $u_{i,loc}$  is an additional correction on top of local controllers, which can be set to zero if there is no such correction. Note that the sparsity pattern of feedback gains captures the structure of communication network. Define  $n \triangleq \sum_{i=1}^N n_i$ ,  $m \triangleq \sum_{i=1}^N m_i$ . Let  $x = [x_1^T, \dots, x_N^T]^T \in \mathbb{R}^n$  and  $u = [u_1^T, \dots, u_N^T]^T \in \mathbb{R}^m$ . The overall system can be described by

$$\dot{x}(t) = (A + BK)x(t), \quad (3)$$

where  $A = [A_{ij}]_{1 \leq i, j \leq N} \in \mathbb{R}^{n \times n}$ ,  $B = \text{diag}\{B_j\}_{1 \leq j \leq N} \in \mathbb{R}^{n \times m}$ ,  $K = [K_{ij}]_{1 \leq i, j \leq N} \in \mathbb{R}^{m \times n}$  are in block form.

Wide-area control is prone to cyber attacks due to its dependence on remote measurement signals that can be compromised by a malicious adversary. In this paper, we consider DoS attacks [16] that can result in unavailability of the signals transmitted over the attacked channels. We describe an *attack strategy* by  $\alpha \in \{0, 1\}^{N \times N}$  where entry  $\alpha_{ij} = 1$  means the channel from subsystem  $j$  to  $i$  is intact whereas  $\alpha_{ij} = 0$  means it is under attack. By assumption,  $\alpha_{ii} = 1, \forall i \in \mathcal{N}$ . The set of all possible attack strategies is called (*pure*) *attack space* and is defined as  $\mathcal{A}_0 \triangleq \{\alpha \in \{0, 1\}^{N \times N} : \alpha_{ii} = 1, i \in \mathcal{N}\}$ . The consequence of DoS attack is modeled by infinite delay of feedback signals.

We assume that an attack strategy  $\alpha$  impacts the wide-area control in the following way:

$$u_i = K_{ii}x_i + \sum_{j \in \mathcal{N}, j \neq i} \alpha_{ij} K_{ij}x_j.$$

This corresponds to the case where the controller will ignore the component  $K_{ij}x_j$  if the measurement signal of  $x_j$  does not arrive within a certain time period. Such a reaction scheme is natural and commonly used in the literature [12]. Now we can write the post-attack closed-loop system under attack strategy  $\alpha \in \mathcal{A}_0$  as

$$\dot{x} = (A + BK \circ \alpha)x, \quad (4)$$

where  $K \circ \alpha \triangleq [K_{ij}\alpha_{ij}]_{1 \leq i, j \leq N}$  denotes the elementwise multiplication between entries of  $\alpha$  (scalar) and subblocks of  $K$  (matrix). Define  $A(\alpha) \triangleq A + BK \circ \alpha$ . To write the elementwise multiplication  $\circ$  as a matrix multiplication, we

consider the following transformation:

$$\begin{aligned}\tilde{K} &= \mathbf{diag}\{\tilde{K}_{[j]}\}_{1 \leq j \leq N} \in \mathbb{R}^{n \times nN}, \text{ where} \\ \tilde{K}_{[j]} &= \begin{bmatrix} K_{j1} & | & K_{j2} & | & \cdots & | & K_{jN} \end{bmatrix}_{n_j \times n}, \\ \tilde{\alpha} &= \begin{bmatrix} \tilde{\alpha}_{[1]} & | & \tilde{\alpha}_{[2]} & | & \cdots & | & \tilde{\alpha}_{[N]} \end{bmatrix}^T \in \mathbb{R}^{nN \times n}, \text{ where} \\ \tilde{\alpha}_{[k]} &= \mathbf{diag}\{\alpha_{kj} \mathbf{I}_{n_j}\}_{1 \leq j \leq N} \in \mathbb{R}^{n \times n}.\end{aligned}$$

Then,  $K \circ \alpha = \tilde{K} \tilde{\alpha}$ . Furthermore,  $\tilde{\alpha}$  can be written as the linear combination of a collection of constant matrices  $\{M_{ij} \in \mathbb{R}^{Nn \times n} : 1 \leq i, j \leq N\}$  with entries of  $\alpha$  as linear coefficients, i.e.,

$$\begin{aligned}\tilde{\alpha} &= \sum_{1 \leq i, j \leq N} \alpha_{ij} M_{ij}, \text{ where} \\ M_{ij}(p, q) &= \begin{cases} 1, & \text{if } p - q = (i - 1)n + \sum_{k=1}^{j-1} n_k, \\ & \text{and } q \in \{1, 2, \dots, n_j\} \\ 0, & \text{otherwise} \end{cases}.\end{aligned}$$

Now, the closed-loop system matrix  $A(\alpha)$  can be written in the following form that is affine in entries of  $\alpha$ .

$$A(\alpha) \triangleq A + BK \circ \alpha = A + \sum_{1 \leq i, j \leq N} B \tilde{K} M_{ij} \alpha_{ij}. \quad (5)$$

We consider a wide-area controller to be resilient if it can survive all possible (pure) attack strategies on the communication channel.

**Definition 1.** A controller  $K$  is called *resilient* if system (4) is stable for all  $\alpha \in \mathcal{A}_0$ . Conversely, it is called *not resilient* if there exists an  $\alpha \in \mathcal{A}_0$  under which system (4) is unstable.

In what follows, we will analyze and quantify the resilience notion given in Definition 1. The first problem to address is under what condition the resilience of a given controller is guaranteed. We aim to derive conditions in terms of optimization problems whose structure can facilitate the analysis. A further problem is concerned with the degree of resilience. We want to define a resilience index as a normalized factor to quantify how resilient a given controller is to certain attack strategies. For the practical aspect, the goal is to develop an efficient algorithm to check the proposed resilience conditions as well as identify structural vulnerabilities.

### III. A MOTIVATING EXAMPLE

WAC makes use of state information from remote buses to improve the closed-loop performance under local decentralized controllers. One may naturally think that a loss of part of remote measurement signals will only gracefully degrade closed-loop performance without causing instabilities. However, such an intuition is unfortunately not true in general. In fact, a wide-area controller can become destabilizing under a loss of a small subset of communication links. We now use a simple hypothetical example to illustrate this fact.

Consider a networked system in the form (3) with  $N = 3$  subsystems and each of which has two states and two

control inputs. For simplicity, we assume there is no physical coupling among the three subsystems. Assume that  $A_{11} = A_{22} = \frac{1}{2}E_2, A_{33} = E_1, B_1 = B_2 = B_3 = \mathbf{I}_2, 2K_{11} = -K_{13} = K_{21} = -\frac{1}{2}K_{23} = -K_{31} = K_{33} = E_1, K_{12} = 2K_{22} = K_{32} = E_2$ , where

$$E_1 = \begin{bmatrix} -3 & -1 \\ 12 & 2 \end{bmatrix} \text{ and } E_2 = \begin{bmatrix} -3 & 1 \\ -12 & 2 \end{bmatrix}.$$

Let  $A_c$  and  $A_d$  be the closed-loop system matrices under controller  $K$  and its full distributed realization, respectively.

$$\begin{aligned}A_c \triangleq (A + BK) &= \begin{bmatrix} E_1 & E_2 & -E_1 \\ E_1 & E_2 & -2E_1 \\ -E_1 & E_2 & 2E_1 \end{bmatrix}, \\ A_d \triangleq A + BK \circ \mathbf{I}_6 &= \begin{bmatrix} E_1 & 0 & 0 \\ 0 & E_2 & 0 \\ 0 & 0 & 2E_1 \end{bmatrix}.\end{aligned}$$

It is easy to check that both  $A_c$  and  $A_d$  are stable. Now consider the attack strategy  $\alpha$  that targets at the communication channel from subsystem 3 to 2, i.e.  $\alpha_{23} = 0$ . The post-attack closed-loop system matrix is

$$A_a \triangleq A + BK \circ \alpha = \begin{bmatrix} E_1 & E_2 & -E_1 \\ E_1 & E_2 & 0 \\ -E_1 & E_2 & 2E_1 \end{bmatrix}.$$

As  $A_a$  has eigenvalues 5.1596, 0.6968,  $-0.8631, -1.3561 \pm 6.5185i, -6.2811$ , two of which are on the right half of the plane, the system is no longer stable. We can see that controller  $K$  is vulnerable under the attack on the communication channel  $3 \rightarrow 2$ .

### IV. RESILIENCE ANALYSIS AND QUANTIFICATION

In this section, we develop a Lyapunov-based framework to analyze and quantify resilience under DoS communication attacks as formulated in Section II.

#### A. Resilience Conditions

A system is stable if and only if all its eigenvalues have negative real part, and conversely it is unstable if and only if at least one of its eigenvalues has positive real part. Given a square matrix, we call the maximum among the real part of its eigenvalues the *spectral abscissa*. One direct approach for resilience condition is to first seek for the attack strategy that results in the largest spectral abscissa of closed-loop system matrix and then determine the sign of the largest spectral abscissa. For the case where it is negative, the system remains stable under all attack strategies; while for the case where it is positive, there exists at least one attack strategy that drives the system unstable. The direct formulation of resilience condition takes the following form:

$$\mathbf{P0} \quad \gamma_0^* \triangleq \max_{\alpha \in \mathcal{A}_0} \mathbf{Re}(\lambda_{\max}(A(\alpha)))$$

If  $\gamma_0^* < 0$ , then wide-area controller  $K$  can survive all possible attacks on the communication channels, otherwise it

inherits structural vulnerabilities. The optimization problem **P0** exhibits several main challenges: i) It is an unsymmetric eigenvalue problem for which the spectral theorem does not apply and thus  $\lambda_{\max}$  does not have an explicit expression. ii) The objective is essentially nonconvex due to the maximization of the largest real part of eigenvalues. Typically, eigenvalue optimization problems are formulated as the minimization of the largest eigenvalue or the maximization of the smallest eigenvalue, both of which are convex. However, this is not the case for **P0**. iii) The decision variable is binary and not continuous, making the problem combinatorial in nature. To address the above challenges, we next reformulate the problem via Lyapunov stability theory.

1) *A Lyapunov Formulation:* Recall that the post-attack system (4) is stable if and only if it admits a quadratic Lyapunov function  $V(x) = x^T P x$  for some  $P \succeq 0$ . The condition can be written in the form of SDP: There exists a  $P_0 \succeq 0$  such that

$$A(\alpha)^T P_0 + P_0 A(\alpha) \prec 0. \quad (6)$$

Conversely, the post-attack system (4) is unstable if and only if for all  $P \succeq 0$ , we can find a unit directional vector  $x_P \in \{z : \|z\| = 1\}$ , where the subscript emphasizes the dependence of the vector on  $P$ , such that

$$x_P^T (A(\alpha)^T P + P A(\alpha)) x_P \geq 0. \quad (7)$$

Inspired by the above Lyapunov characterization, we consider the following formulation:

$$\mathbf{Lya0} \quad \gamma_{L0}^* \triangleq \max_{\alpha \in \mathcal{A}_0} \min_{P \succeq 0} \lambda_{\max}(A(\alpha)^T P + P A(\alpha))$$

**Theorem 1** (Sufficient and Necessary Condition). *A controller  $K$  is resilient if and only if  $\gamma_{L0}^* = -\infty$ , and is not resilient if and only if  $\gamma_{L0}^* \geq 0$ .*

*Proof.* We partition the pure attack space into two disjoint sets, i.e.  $\mathcal{A}_0 = \mathcal{A}_0^s \sqcup \mathcal{A}_0^u$ , where  $\mathcal{A}_0^s$  is the set of stabilizing attack strategies and  $\mathcal{A}_0^u$  is the set of destabilizing attack strategies. Let  $\alpha^s \in \mathcal{A}_0^s$ . Then, system (4) under  $\alpha^s$  is stable, that is to say there exists  $P(\alpha^s) \succeq 0$  dependent on  $\alpha^s$  such that  $A(\alpha^s)^T P(\alpha^s) + P(\alpha^s) A(\alpha^s) \prec 0$ . Then,

$$\begin{aligned} & \min_{P \succeq 0} \lambda_{\max}(A(\alpha^s)^T P + P A(\alpha^s)) \leq \\ & \lambda_{\max}(A(\alpha^s)^T cP(\alpha^s) + cP(\alpha^s) A(\alpha^s)) \rightarrow -\infty \text{ as } c \rightarrow \infty. \end{aligned}$$

Let  $\alpha^u \in \mathcal{A}_0^u$ . Then, system (4) under  $\alpha^u$  is not asymptotically stable, which implies that for all  $P \succeq 0$ , there exists a unit directional vector  $x_P \in \{z : \|z\| = 1\}$  dependent on  $P$  such that  $x_P^T (A(\alpha^u)^T P + P A(\alpha^u)) x_P \geq 0$ . Then,

$$\begin{aligned} & \lambda_{\max}(A(\alpha^u)^T P + P A(\alpha^u)) \\ & = \max_{\|x\|=1} x^T (A(\alpha^u)^T P + P A(\alpha^u)) x \\ & \geq x_P^T (A(\alpha^u)^T P + P A(\alpha^u)) x_P \geq 0, \quad \forall P \succeq 0. \end{aligned}$$

Thus,  $\min_{P \succeq 0} \lambda_{\max}(A(\alpha^u)^T P + P A(\alpha^u)) \geq 0$ .

Now, we want to show the statement for the ‘‘resilient’’ part. ( $\Rightarrow$ ): Assume  $K$  is resilient. By Definition 1, all the attack strategies are stabilizing, i.e.  $\mathcal{A}_0 = \mathcal{A}_0^s$ . Thus,

$$\begin{aligned} \gamma_{L0}^* & = \max_{\alpha \in \mathcal{A}_0^s} \min_{P \succeq 0} \lambda_{\max}(A(\alpha)^T P + P A(\alpha)) \\ & = \max_{\alpha \in \mathcal{A}_0^s} -\infty = -\infty. \end{aligned}$$

( $\Leftarrow$ ): On the other hand, if  $\gamma_{L0}^* = -\infty$ , then for all  $\alpha \in \mathcal{A}_0$ ,  $\min_{P \succeq 0} \lambda_{\max}(A(\alpha)^T P + P A(\alpha)) = -\infty$ , i.e.  $\alpha \in \mathcal{A}_0^s$ . Now  $\mathcal{A}_0 = \mathcal{A}_0^s$  and thus  $K$  is resilient.

Next, we want to show the statement for the ‘‘not resilient’’ part. ( $\Rightarrow$ ): Assume  $K$  is not resilient. By Definition 1,  $\mathcal{A}_0^u \neq \emptyset$ . Let  $\alpha^u \in \mathcal{A}_0^u$  be a destabilizing attack strategy. Then,

$$\begin{aligned} \gamma_{L0}^* & = \max_{\alpha \in \mathcal{A}_0} \min_{P \succeq 0} \lambda_{\max}(A(\alpha)^T P + P A(\alpha)) \\ & \geq \min_{P \succeq 0} \lambda_{\max}(A(\alpha^u)^T P + P A(\alpha^u)) \geq 0. \end{aligned}$$

( $\Leftarrow$ ): On the other hand, if  $\gamma_{L0}^* \geq 0$ , then there exists an  $\alpha^u \in \mathcal{A}_0$  such that  $\min_{P \succeq 0} \lambda_{\max}(A(\alpha^u)^T P + P A(\alpha^u)) \geq 0$ . In other words, there exists a destabilizing attack strategy and thus  $K$  is not resilient.  $\square$

2) *A Lyapunov Relaxation:* The optimal value of **Lya0** provides an equivalent characterization of resilience as proved in Theorem 1. However, the development of efficient algorithm for **Lya0** is highly nontrivial due to its binary decision variables and unbounded optimal value. For the practical use, we now consider a relaxation of **Lya0** by embedding the binary variables into closed interval  $[0, 1]$  and upper bounding the largest eigenvalue of positive semidefinite (P.S.D.) variable. Let  $\mathcal{A} \triangleq \{\alpha \in [0, 1]^{N \times N} : \alpha_{ii} = 1, i = 1, \dots, N\}$  and  $\mathcal{P} \triangleq \{P \in \mathcal{S}^n : 0 \preceq P \preceq \lambda_P I\}$  for some fixed  $\lambda_P > 0$ .

$$\mathbf{LyaP} \quad \gamma_{LP}^* \triangleq \max_{\alpha \in \mathcal{A}} \min_{P \in \mathcal{P}} \lambda_{\max}(A(\alpha)^T P + P A(\alpha))$$

By relaxing the feasible set for the min and constraining the one for the max, **LyaP** provides a surrogate certificate to **Lya0**, which leads to a sufficient condition for resilience.

**Theorem 2.** *A controller  $K$  is resilient if  $\gamma_{LP}^* < 0$ . Conversely, it is not resilient only if  $\gamma_{LP}^* \geq 0$ .*

*Proof.* Since  $\mathcal{P} \subset \{P \succeq 0\}$  and minimization over smaller set gives larger optimal value,

$$\begin{aligned} g(\alpha) & \triangleq \min_{P \in \mathcal{P}} \lambda_{\max}(A(\alpha)^T P + P A(\alpha)) \\ & \geq \min_{P \succeq 0} \lambda_{\max}(A(\alpha)^T P + P A(\alpha)) \triangleq g_0(\alpha). \end{aligned}$$

Furthermore,  $\mathcal{A} \supset \mathcal{A}_0$  and maximization over larger set gives larger optimal value,

$$\gamma_{LP}^* = \max_{\alpha \in \mathcal{A}} g(\alpha) \geq \max_{\alpha \in \mathcal{A}_0} g(\alpha) \geq \max_{\alpha \in \mathcal{A}_0} g_0(\alpha) = \gamma_{L0}^*. \quad (8)$$

For the ‘‘if’’ part, assume  $\gamma_{LP}^* < 0$ . By relation (8),  $\gamma_{L0}^* < 0$ . It then follows from Theorem 1 that  $K$  is resilient. For the ‘‘only if’’ part, assume  $K$  is not resilient. By Theorem 1,  $\gamma_{L0}^* \geq 0$ . Then,  $\gamma_{LP}^* \geq 0$  by relation (8).  $\square$

Recall that for a symmetric matrix  $M \in \mathcal{S}$ , the largest eigenvalue of  $M$  can be written as  $\lambda_{\max}(M) = \min\{t : M \preceq tI\}$ . Since the inner problem of **LyaP** is the minimization of the largest eigenvalue, it can be equivalently formulated in the form of SDP program. Let  $g : \mathcal{A} \rightarrow \mathbb{R}$  be the optimal value of the inner minimization (over  $P$ ) of **LyaP** defined as

$$g(\alpha) \triangleq \min_{P \in \mathcal{P}} \lambda_{\max}(A(\alpha)^T P + PA(\alpha)). \quad (9)$$

Then for any fixed  $\alpha \in \mathcal{A}$ ,  $g(\alpha)$  is the optimal value of the following SDP:

$$\begin{aligned} g(\alpha) = \min \quad & t \\ \text{s.t.} \quad & A(\alpha)^T P + PA(\alpha) \preceq tI \\ & P \in \mathcal{P} \end{aligned} \quad (10)$$

Consider the following optimization problem.

$$\begin{aligned} \text{LyaD} \quad & \gamma_{LD}^* \triangleq \min_{\alpha \in \mathcal{A}} t \\ \text{s.t.} \quad & A(\alpha)^T P + PA(\alpha) \preceq tI \\ & P \in \mathcal{P} \end{aligned}$$

Note that the first constraint in **LyaD** is a Bilinear Matrix Inequality (BMI) in decision variables  $P, \alpha$  and  $t$ . Next, we will show that the dual problem **LyaD** is equivalent to the primal problem **LyaP**.

**Theorem 3.**  $\gamma_{LD}^* = \gamma_{LP}^*$ .

*Proof.* Let  $\alpha_P^*$  be the optima of **LyaP**. Then,  $\gamma_{LP}^* = g(\alpha_P^*)$ , for which there exists  $P_P^* \in \mathcal{P}$  such that  $A(\alpha_P^*)^T P_P^* + P_P^* A(\alpha_P^*) \preceq \gamma_{LP}^* I$ . For the “ $\leq$ ” part, it follows from the triple  $(\alpha_P^*, P_P^*, \gamma_{LP}^*)$  being a feasible solution of **LyaD**. For the “ $\geq$ ” part, consider the BMI constraint of **LyaD**. For  $\alpha_P^* \in \mathcal{A}$ , there exists  $P \in \mathcal{P}$  such that  $A(\alpha_P^*)^T P + PA(\alpha_P^*) \preceq \gamma_{LD}^* I$ . By the equivalent characterization of  $g(\alpha)$  given in SDP (10),  $g(\alpha_P^*) \leq \gamma_{LD}^*$  and thus  $\gamma_{LD}^* \geq \gamma_{LP}^*$ .  $\square$

To take one step further, a natural question to ask is when the relaxed problem **LyaP** is “exact” in terms of resilience. In other words, whether there are cases for which solving **LyaP** results in *sufficient and necessary* condition. The answer is yes under some assumption. We first define *Lyapunov space*  $\mathcal{P}_\alpha \subseteq \mathcal{P}$  for each pure attack strategy  $\alpha \in \mathcal{A}_0$  as

$$\mathcal{P}_\alpha \triangleq \{P \in \mathcal{P} : A(\alpha)^T P + PA(\alpha) \preceq 0, P \neq 0\}. \quad (11)$$

To ensure the exactness of the relaxed problem **LyaP**, we require the intersection of Lyapunov spaces of any two pure attack strategies to be nonempty.

**Assumption 1.** For any  $\alpha_1, \alpha_2 \in \mathcal{A}_0$ ,  $\mathcal{P}_{\alpha_1} \cap \mathcal{P}_{\alpha_2} \neq \emptyset$ .

The above assumption ensures the sign preserving property of the function  $g$  defined in (9) in the sense that if  $g$  is strictly negative on the vertex set  $\mathcal{A}_0$ , it is strictly negative on the convex hull of  $\mathcal{A}_0$ , i.e. the relaxed attack space  $\mathcal{A}$ . On the other hand, if  $g$  fails to be strictly negative on  $\mathcal{A}$ , it fails to be strictly negative on  $\mathcal{A}_0$ .

**Lemma 1.** Under Assumption 1, if  $g(\alpha) < 0, \forall \alpha \in \mathcal{A}_0$ , then  $g(\alpha) < 0, \forall \alpha \in \mathcal{A}$ ; and conversely, if  $\exists \alpha \in \mathcal{A}$  s.t.  $g(\alpha) \geq 0$ , then  $\exists \alpha_0 \in \mathcal{A}_0$  s.t.  $g(\alpha_0) \geq 0$ .

*Proof.* Since  $\mathcal{A}$  is a polytope with vertex set  $\mathcal{A}_0$ , it is enough to show the claim that for any  $\alpha_1, \alpha_2 \in \mathcal{A}_0, \theta \in [0, 1]$ , there exists  $\kappa_1, \kappa_2 > 0$  such that

$$g(\theta\alpha_1 + (1-\theta)\alpha_2) \leq \kappa_1 g(\alpha_1) + \kappa_2 g(\alpha_2).$$

Assume that the claim holds. Consider  $\alpha_\theta \in \mathcal{A}$  where  $\alpha_\theta = \sum_{\alpha_k \in \mathcal{A}_0} \theta_k \alpha_k$  for some  $\theta_k \in [0, 1], \sum_k \theta_k = 1$ . If  $g(\alpha_k) < 0, \forall \alpha_k \in \mathcal{A}_0$ , then  $g(\alpha_\theta) < 0$ . On the other hand, if  $g(\alpha_\theta) \geq 0$ , then  $g(\alpha_k) \geq 0$  for some  $\alpha_k \in \mathcal{A}_0$ . Now we are left to show the claim.

For the ease of notation, let  $f(\alpha, P) \triangleq \lambda_{\max}(A(\alpha)^T P + PA(\alpha))$  in the rest of the proof. Let  $\alpha_1, \alpha_2 \in \mathcal{A}_0, \theta \in [0, 1], P_k = \arg \min_{P \in \mathcal{P}} f(\alpha_k, P), k = 1, 2$ . Consider  $\alpha_\theta = \theta\alpha_1 + (1-\theta)\alpha_2$ . Recall that  $A(\alpha)$  defined in (5) is affine in  $\alpha$ . Then,  $A(\alpha_\theta) = \theta A(\alpha_1) + (1-\theta)A(\alpha_2)$ . By the convexity of  $\lambda_{\max}(\cdot) : \mathcal{S}^n \rightarrow \mathbb{R}$ ,

$$f(\alpha_\theta, P) \leq \theta f(\alpha_1, P) + (1-\theta)f(\alpha_2, P) \triangleq h_\theta(P).$$

By assumption,  $\mathcal{P}_{\alpha_1} \cap \mathcal{P}_{\alpha_2} \neq \emptyset$ . Let  $P_0 \in \mathcal{P}_{\alpha_1} \cap \mathcal{P}_{\alpha_2}$ . Since the Lyapunov space (11) is defined by Linear Matrix Inequality (LMI), the sets  $\mathcal{P}_{\alpha_k}, k = 1, 2$  are convex and so is their intersection  $\mathcal{P}_{\alpha_1} \cap \mathcal{P}_{\alpha_2}$ . Then,  $\exists t_1 \in (0, 1)$  s.t.  $P'_1 = t_1 P_1 + (1-t_1)P_0 \in \mathcal{P}_{\alpha_2}$ . Similarly,  $\exists t_2 \in (0, 1)$  s.t.  $P'_2 = t_2 P_2 + (1-t_2)P_0 \in \mathcal{P}_{\alpha_1}$ . As  $P_0 \in \mathcal{P}_{\alpha_1}$ , we have  $f(\alpha_1, P_0) \leq 0$ . By the convexity of  $f(\alpha, P)$  in  $P$  for any fixed  $\alpha$ ,  $f(\alpha_1, P'_1) \leq t_1 f(\alpha_1, P_1) + (1-t_1)f(\alpha_1, P_0) \leq t_1 f(\alpha_1, P_1)$ . Similarly,  $f(\alpha_2, P'_2) \leq t_2 f(\alpha_2, P_2)$ . Notice that the function  $h_\theta : \mathcal{P} \rightarrow \mathbb{R}$  parameterized by  $\theta \in [0, 1]$  is the sum of two convex functions and thus is also convex. Consider  $P = \beta P'_1 + (1-\beta)P'_2$  for some  $\beta \in [0, 1]$ . Then,

$$\begin{aligned} h_\theta(P) &\leq \theta \beta f(\alpha_1, P'_1) + \theta(1-\beta)f(\alpha_1, P'_2) + \\ &\quad (1-\theta)\beta f(\alpha_2, P'_1) + (1-\theta)(1-\beta)f(\alpha_2, P'_2). \end{aligned}$$

Since  $P'_1 \in \mathcal{P}_{\alpha_2}, P'_2 \in \mathcal{P}_{\alpha_1}$  by construction,  $f(\alpha_1, P'_2) \leq 0$  and  $f(\alpha_2, P'_1) \leq 0$ . We prove the claim that  $g(\alpha_\theta) \leq \kappa_1 g(\alpha_1) + \kappa_2 g(\alpha_2)$  where  $\kappa_1 = \theta \beta t_1$  and  $\kappa_2 = (1-\theta)(1-\beta)t_2$ .  $\square$

With Lemma 1, it is easy to obtain the following sufficient and necessary condition.

**Theorem 4** (Sufficient and Necessary Condition II). Under Assumption 1, a controller  $K$  is resilient if and only if  $\gamma_{LP}^* < 0$ , and it is not resilient if and only if  $\gamma_{LP}^* \geq 0$ .

### B. Resilience Index

The conditions derived in Section IV-A allow us to determine whether a given wide-area controller is resilient to all possible attack strategies. A natural additional question is how resilient the controller is to certain attack strategies. This calls for a proper definition of a normalized index to quantify the degree of resilience. Denoted by  $r_K : \mathcal{A}_0 \rightarrow [0, 1]$  the resilience index of controller  $K$  on the pure attack space. We consider  $r_K$  to be normalized with respect to the nominal

condition. In particular,  $r_K$  needs to satisfy the following two conditions: i) It takes value 1 under the nominal condition when  $K$  is intact, i.e.  $r_K(\mathbf{1}_{N \times N}) = 1$ ; ii) It takes value 0 under destabilizing attack strategies, i.e.  $r_k(\alpha) = 0$  for all  $\alpha \in \mathcal{A}_0$  under which system (4) is unstable.

Recall that  $g : \mathcal{A} \rightarrow \mathbb{R}$  defined in (9) is the optimal value of the inner minimization (over  $P$ ) of the relaxed problem **LyaP**. In fact, the mapping  $g$  defines a performance metric for stability in the sense that for any  $\alpha \in \mathcal{A}$ ,  $g(\alpha)$  is the fastest decreasing rate a Lyapunov function candidate could achieve along the trajectory of  $A(\alpha)$ . This naturally leads to a definition of resilience index satisfying the above two conditions. Guaranteed by the design objective, the system under the nominal condition has better stability performance than the one under attack. Since the nominal condition corresponds to  $\alpha = \mathbf{1}_{N \times N}$ , we have i)  $g(\mathbf{1}_{N \times N}) \leq g(\alpha), \forall \alpha \in \mathcal{A}_0$ . On the other hand, we know from the proof of Theorem 1 that ii)  $g(\alpha) \geq 0$  for any destabilizing  $\alpha \in \mathcal{A}_0$ . Based on i) and ii), we define resilience index  $r_K : \mathcal{A}_0 \rightarrow [0, 1]$  of controller  $K$  on the pure attack space  $\mathcal{A}_0$  as follows.

$$r_K(\alpha) = \begin{cases} 0 & \text{if } g(\alpha) \geq 0 \\ g(\alpha)/g(\mathbf{1}_{N \times N}) & \text{if } g(\alpha) < 0 \end{cases} \quad (12)$$

The definition in (12) captures stability degradation of controller  $K$  under different attack strategies. It is easy to see that the smaller the index  $r_K(\alpha)$  is, the less resilient controller  $K$  is to attack strategy  $\alpha$ , or in other words, the more disruption  $\alpha$  will incur on  $K$ . For the two boundary cases, if  $r_K(\alpha) = 0$ , controller  $K$  can be destabilized by  $\alpha$ , while if  $r_K(\alpha) = 1$ ,  $\alpha$  has no effect on controller  $K$ .

## V. A PATH-FOLLOWING PRIMAL-DUAL ALGORITHM

The goal of this section is to solve the relaxed problem **LyaP**. Notice that **LyaP** takes scalar continuous decision variables  $\alpha_{ij}, i \neq j$  and P.S.D. matrix variable  $P$ . By the definition of  $g$  given in (9), **LyaP** is actually the maximization of  $g$  on the polytope  $\mathcal{A}$ . A natural attempt is to apply gradient ascent algorithm. The key step of gradient-based algorithm is to compute the subgradient of the objective, that is  $\partial g$  for the case here. Let  $f_\alpha(x, P) \triangleq x^T (A(\alpha)^T P + PA(\alpha))x$ .

$$g(\alpha) = \min_{P \in \mathcal{P}} \max_{\|x\|=1} f_\alpha(x, P). \quad (13)$$

Notice that i)  $x \mapsto f_\alpha(x, P)$  is concave and continuous for each  $P$  and ii)  $P \mapsto f_\alpha(x, P)$  is convex (actually affine) for each  $x$ . By the general minimax theorem, the min and the max in (13) can be swapped, i.e.,

$$g(\alpha) = \max_{\|x\|=1} \min_{P \in \mathcal{P}} f_\alpha(x, P) = \max_{\|x\|=1} g_x(\alpha), \text{ where} \\ g_x(\alpha) \triangleq \min_{P \in \mathcal{P}} x^T (A(\alpha)^T P + PA(\alpha))x$$

Observe that  $g$  is the pointwise supremum of  $g_x$  and  $g_x(\alpha)$  is convex in  $\alpha$  (actually affine) for each  $x$ . By the weak rule for pointwise supremum, a subgradient of  $g$  at  $\alpha$  is any element in  $\partial g_{x^*(\alpha)}(\alpha)$  where  $x^*(\alpha) = \arg \max_{\|x\|=1} g_x(\alpha)$ . Now, let's focus on computing the subgradient of  $g_{x^*}$ . Let

$P^*(\alpha) = \arg \min_{P \in \mathcal{P}} \lambda_{\max}(A(\alpha)^T P + PA(\alpha))$ , which depends only on  $\alpha$ , not on  $x$ . Let  $X^* = x^* x^{*T}$ . Then,

$$g_{x^*}(\alpha) = 2 \text{trace}(P^* A(\alpha) X^*) \\ = 2 \text{trace}(X^* P^* (A + \sum_{1 \leq i, j \leq N} B \tilde{K} M_{ij} \alpha_{ij})).$$

Since  $g_{x^*}$  is affine in  $\alpha$ , the subgradient of  $g_{x^*}$  coincides with the gradient taking the following form:

$$\partial_{ij} g_{x^*}(\alpha) = \nabla_{ij} g_{x^*}(\alpha) = 2 \text{trace}(X^* P^* B \tilde{K} M_{ij}).$$

We are now ready to introduce the primal-dual gradient ascent algorithm.

---

### Algorithm 1 Primal-dual gradient ascent algorithm

---

- 1: **Inputs:**  
System matrices:  $A, B, K$
  - 2: **Initialize:**  
 $\alpha_{k-1} \leftarrow \mathbf{1}_{N \times N}$ , step size  $s$ , tolerance  $\epsilon$ ,  
 $\gamma_k = -\infty, \gamma_{k-1} = 0$
  - 3: **while**  $\gamma_k < 0$  or  $\gamma_k - \gamma_{k-1} > \epsilon$  **do**
  - 4:  $P_k \leftarrow$  optimality of **LyaD** with  $\alpha = \alpha_{k-1}$  ▷  
Update dual variable  $P$ : SDP with LMI constraints
  - 5:  $x_k \leftarrow$  eigenvector associated with the largest eigenvalue of  $A(\alpha_{k-1})^T P_k + P_k A(\alpha_{k-1})$ ,  $X_k \leftarrow x_k x_k^T$
  - 6:  $\eta_{ij} \leftarrow \text{trace}(X_k P_k B \tilde{K} M_{ij})$ ,  $\eta \leftarrow \eta / \|\eta\|_F$  ▷  
Compute gradient  $\nabla g(\alpha_{k-1})$
  - 7:  $\alpha_k \leftarrow \alpha_{k-1} + s \eta$  ▷ Update primal variable  $\alpha$ :  
gradient ascent
  - 8:  $\alpha_k \leftarrow \Pi_{\mathcal{A}}(\alpha_k)$  ▷ Project  $\alpha_k$  onto relaxed attack set
  - 9:  $\gamma_{k-1} \leftarrow \gamma_k, \gamma_k \leftarrow x_k^T (A(\alpha_k)^T P_k + P_k A(\alpha_k)) x_k$  ▷  
Compute objective
  - 10:  $\alpha_{k-1} \leftarrow \alpha_k$
  - 11: **end while**
  - 12: **Outputs:**  
optimality  $\gamma_k, \alpha_k$
- 

Let  $\{\gamma_k\}_{k \in \mathbb{N}}$  be the sequence of optimal value and  $\{\alpha_k\}_{k \in \mathbb{N}}$  be the sequence of optima returned by Algorithm 1.

**Theorem 5.** *A controller  $K$  is resilient if  $\gamma_k \uparrow \gamma^* < 0$ . Conversely, it is not resilient only if  $\gamma_k \uparrow 0$ .*

*Proof.* Given  $\alpha_{k-1}$ ,  $P_k$  is the optima of **LyaD** for  $\alpha = \alpha_{k-1}$  s.t.  $P_k = P^*(\alpha_{k-1})$ , where

$$P^*(\alpha) = \arg \min_{P \in \mathcal{P}} \lambda_{\max}(A(\alpha)^T P + PA(\alpha)).$$

Now given  $\alpha_{k-1}$  and  $P_k$ ,  $x_k$  is the eigenvector associated with the largest eigenvalue of  $A(\alpha_{k-1})^T P_k + P_k A(\alpha_{k-1})$ .

$$x_k = \arg \max_{\|x\|=1} x^T (A(\alpha_{k-1})^T P_k + P_k A(\alpha_{k-1})) x.$$

To evaluate the subgradient of  $g$ , we define a collection of functions  $g_x : \mathcal{A} \rightarrow \mathbb{R}$  parameterized by  $x \in \{z : \|z\| = 1\}$ .

$$g_x(\alpha; P^*(\alpha)) \triangleq x^T (A(\alpha)^T P^*(\alpha) + P^*(\alpha) A(\alpha)) x.$$

Observe that  $g(\cdot)$  is the pointwise maximum of  $g_x(\cdot; \cdot)$  where the second variable is determined by the first variable and

is uniform in  $x$ . By the weak rule for pointwise supremum, a subgradient of  $g$  at  $\alpha$  is any element in  $\partial g_{x^*}(\alpha)$  where  $x^*$  is such that  $g(\alpha) = g_{x^*}(\alpha)$ . For  $\alpha = \alpha_{k-1}$ , we have  $g(\alpha_{k-1}) = g_{x_k}(\alpha_{k-1}; P_k)$  and thus

$$\partial g(\alpha_{k-1}) \ni \partial g_{x_k}(\alpha_{k-1}; P_k).$$

Due to  $g_x(\cdot; \cdot)$  is affine in the first variable,  $\partial g_x = \nabla g_x$ . Let  $\eta = \nabla g_{x_k}(\alpha_{k-1}; P_k) \in \mathbb{R}^{N \times N}$ . Then,  $\eta \in \partial g(\alpha_{k-1})$ . By the property of subgradient, for  $s > 0$  small enough,

$$g(\alpha_k) = g(\alpha_{k-1} + s\eta) \geq g(\alpha_{k-1}) + s\langle \eta, \Pi_{\mathcal{T}_A(\alpha_{k-1})}(\eta) \rangle,$$

where  $\mathcal{T}_A(\alpha)$  denotes the tangent cone of  $\mathcal{A}$  at  $\alpha$  and  $\Pi_{\mathcal{M}}(\cdot)$  denotes the projection operator onto  $\mathcal{M}$ . For  $\alpha \in \text{int}(\mathcal{A})$ ,  $\Pi_{\mathcal{T}_A(\alpha)}(\eta) = \eta, \forall \eta \in \mathbb{R}^n$ . For  $\alpha \in \partial(\mathcal{A})$ ,  $0 \leq \langle \eta, \Pi_{\mathcal{T}_A(\alpha_{k-1})}(\eta) \rangle < \|\eta\|^2$ . Thus,

$$\gamma_k = g(\alpha_k) \geq g(\alpha_{k-1}) = \gamma_{k-1}, \forall k \in \mathbb{N}.$$

Now that the sequence  $\{\gamma_k\}_{k \in \mathbb{N}}$  is increasing and upper bounded by 0, the rest of the proof follows from Theorem 2.  $\square$

## VI. SIMULATION RESULTS

In this section, we illustrate the proposed resilience framework on the IEEE 39-bus system [19]. To obtain the linearized model of the form (3), an object-oriented version of PST has been used [20]. There are  $N = 10$  buses in the network-reduced model where bus 1 represents subtransient salient pole with  $n_1 = 7$  states, bus 2-9 represent subtransient round rotor with  $n_i = 8$  states for  $i = 2, \dots, 9$  and bus 10 represents subtransient round rotor with  $n_{10} = 4$  states. Each bus from 1 to 9 has a scalar wide-area control input,  $m_i = 1, i = 1, \dots, 9$  and bus 10 has no control, i.e.  $m_{10} = 0$ . The overall system has  $n = 75$  states and  $m = 9$  control inputs. The dimension of system matrices are summarized as follows:  $A \in \mathbb{R}^{75 \times 75}, B \in \mathbb{R}^{75 \times 9}, K \in \mathbb{R}^{9 \times 75}$ .

We consider two wide-area controllers  $K_1, K_2 \in \mathbb{R}^{9 \times 75}$  that are relatively centralized as compared with the spar promoting controller  $K_{sp}$  given in [11]. The spectral abscissas (maximal real part of eigenvalues) of closed-loop system under the three controllers are summarized in Table I. We can see that  $K_1, K_2$  have better closed loop performance than  $K_{sp}$  since the former two leverage more remote state information than the latter. However, the better closed-loop performance comes at the price of exposing vulnerability to cyber attacks. Next, we will analyze the resilience of  $K_1, K_2$  under attacks on the communication channels using the proposed framework.

We first give an overview on the resilience of the two controllers. In particular, we enumerate all possible single- and double-channel attack strategies and summarize the worst attack strategy of each scenario in Table II. We can see that  $K_1$  is resilient to all the 81 single-channel attack strategies, among which the worst attack 10 $\rightarrow$ 2 still results in negative spectral abscissa -0.1744. On the other hand,  $K_2$  is not resilient to single-channel attack and there are 2 out of 81 single-channel attack strategies that can destabilize the system. Furthermore, neither  $K_1$  nor  $K_2$  is resilient to

double-channel attack. But  $K_1$  is relatively more resilient than  $K_2$  as  $K_1$  has much less destabilizing double-channel attack strategies (total of 4) than  $K_2$  (total of 167). Overall,  $K_1$  is more resilient than  $K_2$ . In what follows, we quantify and analyze the resilience under cyber attacks of the two controllers by first computing their resilience indices and then identifying critical channels based on the machinery we developed in this paper.

TABLE I  
SPECTRAL ABSCISSA OF CLOSED-LOOP SYSTEM

	w/o feedback	w/ $K_1$	w/ $K_2$	w/ $K_{sp}$
$\max_i \text{Re}(\lambda_i)$	-4.9523e-06	-0.19184	-0.19195	-5.8433e-02

TABLE II  
SINGLE- AND DOUBLE-CHANNEL ATTACK

	total # of destabil.		worst attack		max spec. abs.	
	1-ch	2-ch	1-ch	2-ch	1-ch	2-ch
$K_1$	0/81	4/3240	10 $\rightarrow$ 2	5 $\rightarrow$ 4 6 $\rightarrow$ 4	-0.1744	0.1268
$K_2$	2/81	167/3240	5 $\rightarrow$ 4	4 $\rightarrow$ 1 5 $\rightarrow$ 4	0.1484	0.6332

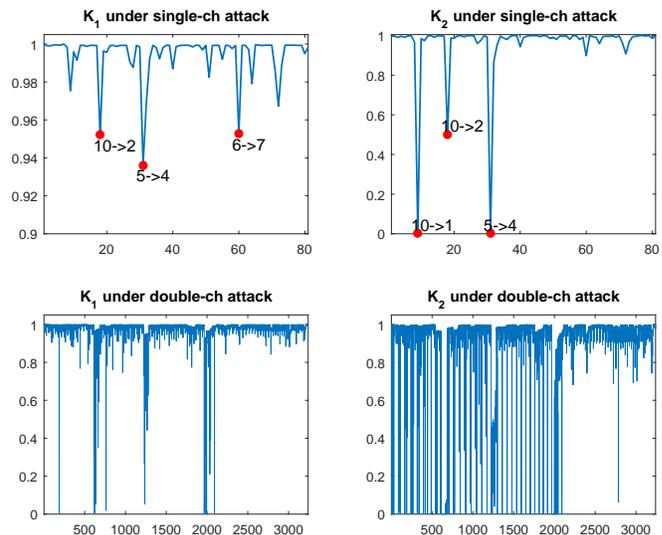


Fig. 1. resilience index under single- and double-channel attack

### A. Resilience Index

We compute resilience indices of the two controllers under single- and double-channel attack using the definition given in (12) and present them in Fig. 1. The worst three single-channel attack strategies, corresponding to the smallest three resilience indices, are highlighted by red dots. We can see that resilience index of  $K_1$  is larger than that of  $K_2$ , suggesting  $K_1$  is more resilient than  $K_2$ , as what is expected. This shows that our resilience index is an effective metric to quantify resilience.

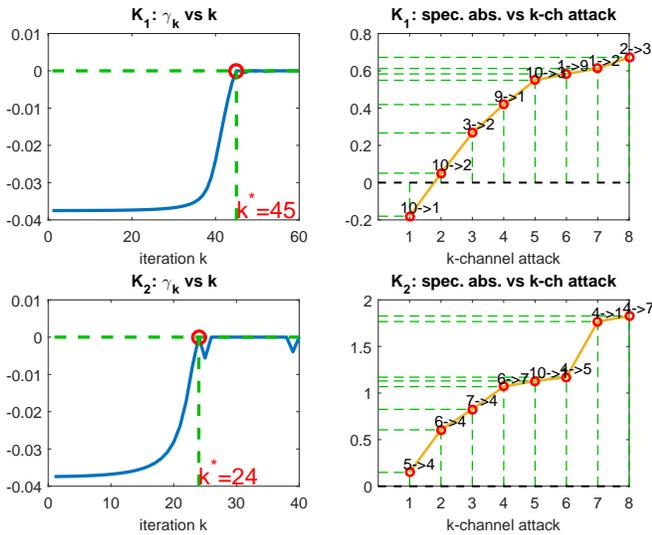


Fig. 2. left: convergence of Algorithm 1, right: spectral abscissa under  $k$ -channel attack

### B. Identification of Critical Channels

We apply Algorithm 1 to check the resilience criterion for the two controllers. The sequences of optimal value are plotted in the left panel of Fig. 2. We can see that  $\gamma_k \uparrow 0$  in both cases. By Theorem 5, we know that  $K_1$  and  $K_2$  both satisfy the necessary condition for non-resilience. To identify critical channels, we focus on the optimal relaxed strategy  $\alpha^*$  obtained at the instance  $k^*$  when the optimal value firstly reaches 0. We rank the criticality of channels by the magnitude of their corresponding entry of  $\alpha^*$ , that is the smaller  $\alpha_{ij}^*$  is, the more critical channel  $j \rightarrow i$  is. We consider  $k$ -channel attacks for  $k = 1, \dots, 8$  generated by the criticality ranking and plot the resulting spectral abscissa on the right panel of Fig. 2. The  $k$ -th most critical channel is labeled on top of the red circle corresponding to  $k$ -channel attack, whose attack set includes the first  $k$  most critical channels. We can see that the system is driven more and more unstable under the sequence of critical  $k$ -channel attack strategy. Therefore, we successfully identify structural vulnerabilities by the criticality ranking.

## VII. CONCLUSION

This paper proposes a novel framework for resilience analysis and quantification of wide-area control of power systems. We formally define the notion of resilience in the presence of cyber attacks. Resilience conditions are given in terms of Lyapunov-based optimization problems. A resilience index is defined to quantify the degree of resilience. We develop an efficient numerical algorithm to check the proposed resilience criterion as well as identify structural vulnerabilities.

## REFERENCES

[1] V. Venkatasubramanian and Y. Li, "Analysis of 1996 western american electric blackouts," *Bulk Power System Dynamics and Control-VI, Cortina d'Ampezzo, Italy*, pp. 22–27, 2004.

[2] A. Chakraborty and P. P. Khargonekar, "Introduction to wide-area control of power systems," in *Proceedings of American Control Conference*. IEEE, 2013, pp. 6758–6770.

[3] I. Kamwa, R. Grondin, and Y. Hebert, "Wide-area measurement based stabilizing control of large power systems—a decentralized/hierarchical approach," *IEEE Transactions on Power Systems*, vol. 16, no. 1, pp. 136–153, Feb 2001.

[4] B. Chaudhuri, R. Majumder, and B. C. Pal, "Wide-area measurement-based stabilizing control of power system considering signal transmission delay," *IEEE Transactions on Power Systems*, vol. 19, no. 4, pp. 1971–1979, Nov 2004.

[5] Q. Liu, V. Vittal, and N. Elia, "LPV supplementary damping controller design for a thyristor controlled series capacitor (tsc) device," *IEEE Transactions on Power Systems*, vol. 21, no. 3, pp. 1242–1249, Aug 2006.

[6] A. Chakraborty, "Wide-area damping control of power systems using dynamic clustering and tsc-based redesigns," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1503–1514, Sep 2012.

[7] Y. Zhang and A. Bose, "Design of wide-area damping controllers for interarea oscillations," *IEEE Transactions on Power Systems*, vol. 23, no. 3, pp. 1136–1143, Aug 2008.

[8] H. Vu, P. Pruvot, C. Launay, and Y. Harmand, "An improved voltage control on large-scale power system," *IEEE Transactions on Power Systems*, vol. 11, no. 3, pp. 1295–1303, Aug 1996.

[9] A. Zobian and M. D. Ilic, "A steady state voltage monitoring and control algorithm using localized least square minimization of load voltage deviations," *IEEE Transactions on Power Systems*, vol. 11, no. 2, pp. 929–938, May 1996.

[10] K. Tomovic, D. E. Bakken, V. Venkatasubramanian, and A. Bose, "Designing the next generation of real-time control, communication, and computations for large power systems," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 965–979, May 2005.

[11] F. Dorfler, M. R. Jovanovic, M. Chertkov, and F. Bullo, "Sparsity-promoting optimal wide-area control of power networks," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2281–2291, Sep 2014.

[12] D. Soudbakhsh, A. Chakraborty, F. Alvarez, and A. Annaswamy, "A delay-aware cyber-physical architecture for wide-area control of power systems," 2015.

[13] S. Zhang and V. Vittal, "Wide-area control resiliency using redundant communication paths," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2189–2199, Sep 2014.

[14] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[15] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[16] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control*. Springer, 2009, pp. 31–45.

[17] M. Zima, M. Larsson, P. Korba, C. Rehtanz, and G. Andersson, "Design aspects for wide-area monitoring and control systems," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 980–996, May 2005.

[18] S. Nabavi, J. Zhang, and A. Chakraborty, "Distributed optimization algorithms for wide-area oscillation monitoring in power systems using interregional pmu-pdc architectures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2529–2538, Sep 2015.

[19] G. Rogers, *Power system oscillations*. Springer Science & Business Media, 2012.

[20] J. H. Chow and K. W. Cheung, "A toolbox for power system dynamics and control engineering education and research," *IEEE Transactions on Power Systems*, vol. 7, no. 4, pp. 1559–1564, Nov 1992.