On the Stability of Power Transmission Systems Under Persistent Inverter Attacks: A Bi-Linear Matrix Approach

Antonin Colot, Vishal Shenoy, Guido Cavraro, Emiliano Dall'Anese, Jorge I. Poveda

***Abstract*— We investigate the stability and robustness properties of a power transmission system under persistent deceiving attacks on inverter-interfaced energy resources. The attacks can corrupt the damping coefficients in the inverters' controllers and measurements of the frequency at the points of coupling. Leveraging tools from hybrid dynamical systems theory, we characterize a broad family of persistent (and not necessarily periodic) attacks acting on the inverters, under which the stability properties of the transmission system can be shown to not be compromised. To address potentially conservative conditions identified through conventional bounding techniques, sufficient conditions on the average activation time of the attacks are identified via Lyapunov theory, as well as the formulation and solution of a class of bilinear matrix inequalities (BMI). The results are obtained for constant and slowly time-varying loads via input-to-state stability (ISS) tools. Numerical simulations on the IEEE 39-bus test system are also presented.**

***Index Terms*— Cybersecurity in Power Systems, Hybrid Systems, Stability Analysis.**

I. Introduction

THE integration of inverter-interfaced distributed energy resources (DERs) in power systems, at both transmission and distribution levels, is a key driver for modernizing the power infrastructure. While the goal is to enhance reliability, efficiency, and sustainability, the emerging 'cyber' layer faces increasing vulnerability to attacks and security threats [1], [2]. Evidence of this vulnerability exists [3], prompting the need for new methodologies to study the resilience of modern grids [4], [5]. Inspired by these challenges, this paper investigates the stability and robustness properties of a *power transmission system* subjected to persistent, dynamic, and deceptive attacks on inverter-interfaced energy resources.

A. Colot and V. Shenoy contributed equally. V. Shenoy and J. I. Poveda are with the ECE Department at UC San Diego. A. Colot is a Research Fellow of the F.R.S-FNRS with the Montefiore Institute, University of Liège, and a visiting student at the University of Colorado Boulder. G. Cavraro is with NREL. E. Dall'Anese is with the ECEE Department, University of Colorado, Boulder. V. Shenoy and J. I. Poveda were supported in part by the grant NSF ECCS CAREER 2305756.

This work was authored by NREL, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by DOE Office of Electricity, Advanced Grid Modeling Program. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

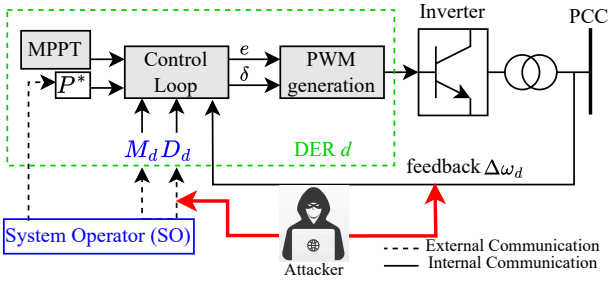

Fig. 1: Scheme of DER under attack. The attacker can modify the inverter controller and the frequency feedback.

Prior works: During recent years, tools from dynamical systems have been utilized to study the behavior of cyber-physical systems (CPSs) under attacks, as seen in, for example, [6], and for investigating the robustness of feedback optimization methods [7] and energy management [8] in power systems. For instance, in [9] the authors considered a DC microgrid subject to persistent denial of service attacks and established stability conditions in terms of linear matrix inequalities (LMIs); however, no practical bounds were obtained. In [10], the resilience properties of wide-area control systems were studied with respect to a variety of attacks, deriving suitable bounds via BMIs. In [11], the load frequency problem in AC microgrids subject to data injection attacks was studied, leading to the design of a stabilizing controller via BMIs. However, the analysis was restricted to certain non-persistent attacks. Similarly, [12] considered a discrete-time setup for persistent denial of service attacks, and studied the design of stabilizing controllers based on feasibility properties of BMIs. Finally, [4] studied operating constraints able to prevent attacks from driving the system's frequency to unsafe conditions using an approach based on ellipsoidal approximations. In [13], the authors studied the power system state estimator (PSSE) of the SCADA system of a power grid subject to false data injection attacks seeking to deceive the system. Similarly, in [14] the authors considered a discrete-time LTI system using an infinite-horizon LQG controller subject to deception via replay attacks. In both works, the analysis is stochastic and the attacks under study are not persistent.

Contributions: In contrast to existing works, we consider DERs partaking in frequency regulation at the transmission level [15], and study a class of *persistent* and intermittent

attacks acting on the controllers of the inverters. These attacks are capable of evading detection due to their *non-periodic* nature and can significantly affect the frequency response of the DERs depending on their "persistency". We leverage a hybrid dynamical system's formalism to model the effects of the attacks and analyze the stability properties of the system under attacks via Lyapunov theory. Constant and time-varying loads are both considered in the analysis. In both cases, we provide computable certificates for stability based on the feasibility of a set of BMIs. The obtained certificates turn out to be orders of magnitude less conservative compared to previous approaches [7]. Lastly, we validate our theoretical results via simulations on the IEEE 39-bus test system. To the best of our knowledge, this is the first work considering persistent, non-periodic, inverter-level attacks via BMI-based stability certificates for both constant and time-varying loads using tools frol hybrid dynamical systems theory.

The rest of this paper is organized as follows: Section II presents the preliminaries. Section III describes the model of the power transmission system. Section IV characterizes the attacks, and Section V presents the main theoretical and numerical results. Finally, Section VI presents the conclusions.

II. Preliminaries

We use $\mathbb{I}$ to denote the identity matrix, and $\mathcal{S}$ to denote the class of right-continuous, piece-wise constant functions from $\mathbb{R}_{\geq 0}$ to $\mathcal{Q} \subset \mathbb{Z}_{>0}$. In this paper, we are interested in signals $\sigma \in \mathcal{S}$ that satisfy the following notions:

Definition 1: A signal $\sigma \in \mathcal{S}$ is said to satisfy the *average dwell-time* (ADT) condition with parameters $\tau_d > 0$ and $N_0 \geq 1$, if $\forall\ t_2 > t_1 \geq 0$, such that $t_2, t_1 \in \text{dom}(\sigma)$:

$$N_\sigma(t_1, t_2) \leq N_0 + \frac{t_2 - t_1}{\tau_d}, \tag{1}$$

where $N_\sigma(t_1, t_2)$ is the number of switches of σ in $(t_1, t_2]$. The class of such signals is denoted as $\Sigma_{\text{ADT}}(\tau_d, N_0)$. □

Definition 2: A signal $\sigma \in \mathcal{S}$ is said to satisfy the *average activation time* (AAT) condition with parameters $\tau_a > 1$ and $T_0 \geq 0$, if $\forall\ t_2 \geq t_1 \geq 0$ such that $t_2, t_1 \in \text{dom}(\sigma)$:

$$\int_{t_1}^{t_2} \mathbf{1}_{\mathcal{Q}_\mu}(\sigma(\tau))\, d\tau \leq T_0 + \frac{(t_2 - t_1)}{\tau_a}, \tag{2}$$

where, for a given set $\mathcal{Q}_\mu$, $\mathbf{1}_{\mathcal{Q}_\mu}(\sigma) = 1$ if $\sigma \in \mathcal{Q}_\mu$, and $\mathbf{1}_{\mathcal{Q}_\mu}(\sigma) = 0$ otherwise. The class of such signals is denoted as $\Sigma_{\text{AAT}}(\tau_a, T_0)$. □

To study dynamical systems under persistent, intermittent attacks, we will use the framework of hybrid dynamical systems, which are modeled by the following inclusions:

$$x \in C, \qquad \dot{x} \in F(x, u), \tag{3a}$$
$$x \in D, \qquad x^+ \in G(x). \tag{3b}$$

In system (3), $x \in \mathbb{R}^n$ denotes the state and $u \in \mathbb{R}^m$ denotes the input. The state evolves via the differential inclusion (3a) when it is in the flow set C, and jumps according to (3b) when x is in the jump set D. Solutions to system (3) evolve on hybrid time domains, which are special subsets of $\mathbb{R}_{\geq 0} \times \mathbb{N}$. They are parameterized by a continuous-time index t which increases continuously during the flows, and by a discrete-time index j which increases by one after every jump. The distance of $x \in \mathbb{R}^n$ to a compact set $\mathcal{A} \subset \mathbb{R}^n$ is defined as $|x|_\mathcal{A} = \inf_{y \in \mathcal{A}} |x - y|$. A compact set $\mathcal{A}$ is said to be exponentially input-to-state stable (E-ISS) for (3) if every solution satisfies

$$|x(t,j)|_\mathcal{A} \leq \kappa_1 e^{-\kappa_2 (t+j)} |x(0,0)|_\mathcal{A} + \kappa_3 \sup_{0 \leq \tau \leq t} |u(\tau)|, \tag{4}$$

for some $\kappa_1 > 0, \kappa_2 > 0, \kappa_3 > 0$. For further details on hybrid dynamical systems, we refer the reader to [16].

III. Power Transmission System Model

In this section, we outline the model of the power transmission network. We consider a power transmission system with buses $\mathcal{N} := \{1, ..., N\}$ and lines $\mathcal{E} := \{(m, n)\} \subset \mathcal{N} \times \mathcal{N}$. Let $\mathcal{D} \subset \mathcal{N}$ be the set of buses where inverter-interfaced DERs are connected, and let $\mathcal{G} \subset \mathcal{N}$ be the set of buses where conventional fossil-fuel generators are located. For simplicity of exposition, and without loss of generality, we assume that $\mathcal{N} = \mathcal{D} \cup \mathcal{G}$ and $\mathcal{D} \cap \mathcal{G} = \emptyset$. Assuming lossless lines, we collect in $\mathcal{I}_\ell \in \mathcal{E}$ all the lines connected to the bus ℓ. Next, we formalize the models for generators, inverter-interfaced DERs, and the transmission network.

1) Conventional Generators: We assume that the exciter operates at a stable output, such that the terminal voltage magnitude is constant. Based on this, we consider the following model for the generator $g \in \mathcal{G}$ [17]:

$$\dot{\delta}_g = \omega_\text{s} \Delta\omega_g, \tag{5a}$$
$$M_g \Delta\dot{\omega}_g = P_g^\text{m} - D_g \Delta\omega_g + P_g - \sum_{\ell \in \mathcal{I}_g} P_{g\ell}, \tag{5b}$$
$$\tau_g \dot{P}_g^\text{m} = -P_g^\text{m} + P_g^\text{r} - K_{\text{gov},g} \Delta\omega_g, \tag{5c}$$

where δ_g, $\Delta\omega_g$, ω_s, and P_g^m are the rotor electrical angle, the rotor speed deviation in per unit, the synchronous angular speed, and the turbine mechanical power, respectively. Furthermore, M_g is the constant of inertia, and D_g models the equivalent load damping, which includes the damper windings. The dynamics of the turbine mechanical power are captured by a first-order turbine model [18], where $K_{\text{gov},g}$ is the governor gain, modeling the inverse of the speed-droop regulation constant, τ_g is the turbine time constant, and P_g^r denotes the reference-power setting computed from a higher layer control. Finally, P_g is the real power injection at bus g, and $P_{g\ell}$ is the real power flow from bus g to ℓ.

2) Frequency-Responsive DERs: For each DER $d \in \mathcal{D}$, we consider the following dynamics [15]:

$$\dot{\delta}_d = \omega_\text{s} \Delta\omega_d, \tag{6a}$$
$$M_d \Delta\dot{\omega}_d = -D_d \Delta\omega_d + P_d - \sum_{\ell \in \mathcal{I}_d} P_{d\ell}, \tag{6b}$$

where D_d models the frequency response of the DER, M_d determines the (virtual) inertial response, P_d is the real power injected, and $P_{d\ell}$ is the real power flow from bus d to ℓ. Notice that D_d and M_d do not represent mechanical parameters as in (5). Instead, for DERs, these are *digital* parameters that may be tuned to obtain a desired response [19], [20]. In Fig. 1, these parameters are computed by the system operator (SO) and communicated to the inverters.

3) Secondary Controller: To steer the average angular speed deviation $\Delta\omega \in \mathbb{R}$ to zero, we consider a supervisory *secondary controller* that generates time-varying reference-power signals $P^{\mathrm{r}}_{\mathcal{G}} \in \mathbb{R}^{|\mathcal{G}|}$ (collecting $\{P^{\mathrm{r}}_i\}_{i\in\mathcal{G}}$) [21, Ch. 9]. Let $z \in \mathbb{R}$ be the supervisory controller's state and let $P^*_{\mathcal{G}} \in \mathbb{R}^{|\mathcal{G}|}$ denote the baseline reference obtained via economic dispatch. The controller's equations are given by:

$$\tau_z \dot{z} = -z + \beta\Delta\omega + \mathbb{1}^\top P^{\mathrm{m}}_{\mathcal{G}}, \tag{7a}$$

$$P^{\mathrm{r}}_{\mathcal{G}} = P^*_{\mathcal{G}} + \zeta(z - \mathbb{1}^\top P^*_{\mathcal{G}}), \tag{7b}$$

where $\zeta \in \mathbb{R}^{|\mathcal{G}|}_{>0}$ is the vector of participation factors (i.e., $\zeta_i \in (0,1)$ and $\mathbb{1}^\top\zeta = 1$), $\beta \in \mathbb{R}_{<0}$ is a tunable gain, and $P^{\mathrm{m}}_{\mathcal{G}} := [\{P^{\mathrm{m}}_i\}_{i\in\mathcal{G}}]^\top$ collects the mechanical powers of every generator $g \in \mathcal{G}$. To ensure sufficient time-scale separation between the primary and secondary frequency controllers, the constant $\tau_z \in \mathbb{R}_{>0}$ is assumed to be larger than τ_g, $\forall\, g \in \mathcal{G}$.

4) State-space model: We now present a unifying state space model that combines the dynamics (5), (6) and (7). We assume that the system initially operates at steady-state with $\Delta\omega_g = \Delta\omega_d = 0$, $\forall g \in \mathcal{G}, d \in \mathcal{D}$. Moreover, we assume that $\Delta\omega$ is the same for all nodes, which is a valid assumption for networks where electrical distances are negligible and all the buses have the same frequency even during transients (see, e.g., [22]). For a lossless network, $\sum_{g\in\mathcal{G}}\sum_{\ell\in\mathcal{I}_g} P_{g\ell} + \sum_{d\in\mathcal{D}}\sum_{\ell\in\mathcal{I}_d} P_{d\ell} = 0$ holds. Using (5) and (6) we obtain

$$M_{\mathrm{eff}}\Delta\dot{\omega} = \sum_{g\in\mathcal{G}} P^{\mathrm{m}}_g - D_{\mathrm{net}}\Delta\omega - P_{\mathrm{load}}, \tag{8}$$

where $P_{\mathrm{load}} := -\sum_{g\in\mathcal{G}} P_g - \sum_{d\in\mathcal{D}} P_d$ is the total electrical load, and the *effective inertia constant* M_{eff} and the *net damping constant* D_{net} are defined, respectively, as:

$$M_{\mathrm{eff}} := \sum_{g\in\mathcal{G}} M_g + \sum_{d\in\mathcal{D}} M_d, \quad D_{\mathrm{net}} := \sum_{g\in\mathcal{G}} D_g + \sum_{d\in\mathcal{D}} D_d. \tag{9}$$

Furthermore, from (5c) we have:

$$\mathsf{diag}(\tau)\dot{P}^{\mathrm{m}}_{\mathcal{G}} = -P^{\mathrm{m}}_{\mathcal{G}} + P^{\mathrm{r}}_{\mathcal{G}} - K_{\mathrm{gov},\mathcal{G}}\Delta\omega, \tag{10}$$

where τ is a vector collecting $\{\tau_i\}_{i\in\mathcal{G}}$ and $K_{\mathrm{gov},\mathcal{G}}$ is a vector collecting $\{K_{\mathrm{gov},i}\}_{i\in\mathcal{G}}$. Combining (7), (8) and (10) yields the final state-space model of the power transmission system:

$$\dot{x} = Ax + Bu, \qquad \dot{u} = \begin{bmatrix}\Pi(u)\\ 0\end{bmatrix}, \tag{11}$$

with the following state vector $x \in \mathbb{R}^{|\mathcal{G}|+2}$, input $u \in \mathbb{R}^{|\mathcal{G}|+1}$, and matrices $A \in \mathbb{R}^{(|\mathcal{G}|+2)\times(|\mathcal{G}|+2)}$ and $B \in \mathbb{R}^{(|\mathcal{G}|+2)\times(|\mathcal{G}|+1)}$:

$$\begin{aligned} x &= [\Delta\omega, (P^{\mathrm{m}}_{\mathcal{G}})^\top, z]^\top, \quad u = [P_{\mathrm{load}}, (P^*_{\mathcal{G}})^\top]^\top,\\ A &= \begin{bmatrix} -D_{\mathrm{net}}M_{\mathrm{eff}}^{-1} & M_{\mathrm{eff}}^{-1}\mathbb{1}^\top & 0\\ A_\tau K_{\mathrm{gov},\mathcal{G}} & A_\tau & -A_\tau\zeta\\ \tau_z^{-1}\beta & \tau_z^{-1}\mathbb{1}^\top & -\tau_z^{-1}\end{bmatrix},\\ B &= \begin{bmatrix} -M_{\mathrm{eff}}^{-1} & \mathbb{0}^\top\\ 0 & -A_\tau\left(\mathbb{I} - \zeta\mathbb{1}^\top\right)\\ 0 & \mathbb{0}^\top\end{bmatrix}, \end{aligned} \tag{12}$$

where $A_\tau := -\mathrm{diag}(\tau)^{-1}$. In (11), the time-varying loads are modeled as signals generated by the exosystem $\dot{u} \in \Pi(u)$ where $\Pi : \mathbb{R} \to \mathbb{R}$ is a Lipschitz continuous function that renders a compact set $\mathcal{U} \subset \mathbb{R}$ forward invariant. The set $\mathcal{U}$ abstracts the set of feasible electrical loads. Note that, in our model, we do not consider frequency-sensitive loads, load buses, and buses with no loads or DERs. However, incorporating these elements into our model would not change the results presented in the next section; see the remarks in [15].

5) Steady-state Analysis: At steady-state, i.e., when $\dot{x} = 0$ and $\dot{u} = 0$, equations (11) and (12) yield the following algebraic conditions:

$$D_{\mathrm{net}}\Delta\omega_{ss} = \mathbb{1}^\top P^{\mathrm{m}}_{\mathcal{G},ss} - P_{\mathrm{load}}, \tag{13a}$$

$$P^{\mathrm{m}}_{\mathcal{G},ss} = -K_{\mathrm{gov},\mathcal{G}}\Delta\omega_{ss} + \zeta z_{ss} + \left(\mathbb{I} - \zeta\mathbb{1}^\top\right)P^*_{\mathcal{G}}, \tag{13b}$$

$$z_{ss} = \beta\Delta\omega_{ss} + \mathbb{1}^\top P^{\mathrm{m}}_{\mathcal{G},ss}, \tag{13c}$$

and, since $\mathbb{1}^\top\zeta = 1$, equation (13b) leads to:

$$\mathbb{1}^\top P^{\mathrm{m}}_{\mathcal{G},ss} = -\mathbb{1}^\top K_{\mathrm{gov},\mathcal{G}}\Delta\omega_{ss} + z_{ss}. \tag{14}$$

Substituting (13c) in (14), we obtain the steady state condition $(-\mathbb{1}^\top K_{\mathrm{gov}} + \beta)\Delta\omega_{ss} = 0$. Thus, since the elements of $K_{\mathrm{gov},\mathcal{G}}$ are nonnegative and $\beta < 0$, we finally obtain that $\Delta\omega_{ss} = 0$, $\mathbb{1}^\top P^{\mathrm{m}}_{\mathcal{G},ss} = P_{\mathrm{load}}$ and $z_{ss} = P_{\mathrm{load}}$. We note that the equilibrium point does not depend on D_{net}.

IV. Hybrid Model of The System Under Attacks

In this section, we study the dynamics of the power transmission system under attacks using the formalism of hybrid dynamical systems (3).

1) Attack model: We consider intermittent attacks able to modify the feedback term $D_d\Delta\omega_d$ in the inverters' control law (6b). This modification can be accomplished through a variety of attacks, including deception attacks that can change the sign and magnitude of the coefficient D_d [1], or by altering the sign and magnitude of $\Delta\omega_d$ [4]. In general, the impact of these attacks can be represented by sudden changes in the coefficient D_{net} in equation (12). While the effects on D_{net} resulting from attacks on D_d are evident from equation (9), the effect of an erroneous frequency measurement $\tilde{\Delta}\omega_d$ can be modeled as $D_d\tilde{\Delta}\omega_d = (D_d\tilde{\Delta}\omega_d/\Delta\omega_d)\Delta\omega_d$ (whenever $\Delta\omega_d \neq 0$), with the term $D_d\tilde{\Delta}\omega_d/\Delta\omega_d$ subsequently impacting D_{net} via equation (9). Since, in general, the attacks that we study are not constant but rather intermittent and aperiodic, their detection and mitigation becomes more challenging [9].

From a dynamical systems perspective, the attacks can be seen as signals that are intentionally designed to render the matrix A in (11) non-Hurwitz. Such modifications can be viewed as switches in the matrix A, thus introducing multiple *unstable* modes; in particular, each mode is associated with a given value of D_{net} and its corresponding state matrix in (12). We denote the set of unstable modes (induced by the attacks) as $\mathcal{Q}_\mu$. When an attack is detected and corrected by the System Operator (SO) (or if there is no attack) the system dynamics revert back to operating in the nominal stable mode, denoted by the singleton set $\mathcal{Q}_s$. In this way, using $\mathcal{Q} := \mathcal{Q}_s \cup \mathcal{Q}_\mu$, the transmission power system operating under persistent adversarial attacks can be modeled as the following switching dynamical system:

$$\dot{x} = A_{\sigma(t)}x + Bu, \tag{15}$$

where $\sigma \in \mathcal{S}$, and $A_{\sigma(t)} = A$ in case of no attacks and $A_{\sigma(t)} \neq A$ if $\sigma(t) \in \mathcal{Q}_\mu$. It is important to note that the equilibrium point of (15), under a given input u, does not depend on D_{net}. In fact, $A_{\sigma(t)}$ is invertible for any value of σ, leading to a unique equilibrium x_{eq}. Therefore, using the change of variable $\tilde{x} = x - x_{eq}$ to shift the equilibrium to the origin, the dynamics (15) become

$$\dot{\tilde{x}} = A_{\sigma(t)}\tilde{x} + A_{\sigma(t)}^{-1} B\dot{u}. \tag{16}$$

Since the switching signal σ takes values in the unstable modes $\mathcal{Q}_\mu$ (corresponding to attacks) and also in the stable modes $\mathcal{Q}_s$ (corresponding to rejected attacks or no attacks), we can use Definitions 1 and 2 to model different families of attacks that satisfy the bounds (1) and (2). Based on this, we pose the following problem.

Problem 1: For any signal $\sigma \in \mathcal{S}$ satisfying (1) and (2), characterize the values of τ_a and τ_d under which the power transmission system, modeled as in (16), remains asymptotically stable.

When the loads are constant (i.e., $\dot{u} = 0$), the stability properties of (16) can be studied with respect to the origin. However, when the load is time-varying, the stability properties of (16) will be studied via the notion of E-ISS with respect to a suitable compact set.

2) Hybrid Dynamics: To analyze the stability properties of (16) under persistent attacks, we adopt the formalism of hybrid dynamical systems (HDSs) [16]. In particular, the switching signal is modeled as a logic state $q \in \mathcal{Q}$ that switches between different modes in $\mathcal{Q}$. Since switching signals satisfying bounds of the form (1) and (2) can be generated using dynamic time-invariant hybrid automatons with auxiliary states τ_1 and τ_2 (see [16], [23]) we can write the complete system as (3), with state $\xi = [\tilde{x}, \tau_1, \tau_2, q, u]^\top$, input $v = \dot{u}$, and

$$C = \mathbb{R}^{|\mathcal{G}|+2} \times [0, N_0] \times [0, T_0] \times \mathcal{Q} \times \mathcal{U}, \tag{17a}$$

$$D = \mathbb{R}^{|\mathcal{G}|+2} \times [1, N_0] \times [0, T_0] \times \mathcal{Q} \times \mathcal{U}, \tag{17b}$$

$$\dot{\xi} \in F(\xi, u) = \begin{pmatrix} A_q\tilde{x} + A_q^{-1}Bv \\ \left[0, \frac{1}{\tau_d}\right] \\ \left[0, \frac{1}{\tau_a}\right] - \mathbf{1}_{\mathcal{Q}_u}(q) \\ 0 \\ \Pi(u) \end{pmatrix}, \tag{17c}$$

$$\xi^+ \in G(\xi) = \tilde{x} \times \{\tau_1 - 1\} \times \{\tau_2\} \times \mathcal{Q} \setminus \{q\} \times \{u\}. \tag{17d}$$

Note that, during the flows (17c), the state $\tilde{x}$ evolves according to the vector field dictated by the current mode q. The autonomous set-valued dynamics of τ_1 and τ_2 ensure that the switching state q obeys the ADT condition [16, p. 40] and also the AAT condition [23, Lemma 7] for all times. In this way, studying the stability properties of system (17) is equivalent to studying the stability properties of (16) under ADT and AAT conditions on σ.

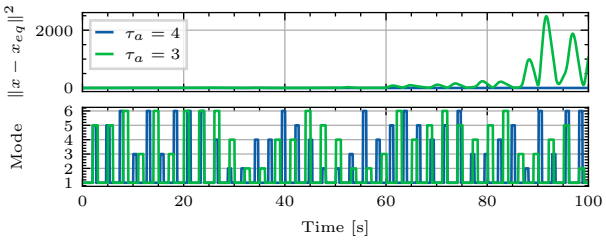

Fig. 2: Distance from equilibria when the system starts off equilibria and is under attack for $\tau_a = 3$ and $\tau_a = 4$.

V. Main Results: Theory and Applications

1) Theoretical Results: The following theorem is the first main result of the paper. We provide sufficient conditions under which system (17) is E-ISS.

Theorem 1: Suppose there exist a symmetric positive definite matrix $P \in \mathbb{R}^{|\mathcal{G}|+2 \times |\mathcal{G}|+2}$ and constants $\lambda_s, \lambda_\mu > 0$ such that the following bilinear matrix inequalities hold:

$$A_s^\top P + PA_s + \lambda_s P \preceq 0, \tag{18a}$$

$$A_\mu^\top P + PA_\mu - \lambda_\mu P \preceq 0, \tag{18b}$$

for all $s \in \mathcal{Q}_s$ and $\mu \in \mathcal{Q}_\mu$. Let

$$\lambda_s - \frac{(\lambda_s + \lambda_\mu)}{\tau_a} - \frac{\kappa(\lambda_s, \lambda_\mu) \cdot \theta}{\lambda_{min}(P)} > 0, \tag{19}$$

where $\kappa(\lambda_s, \lambda_\mu) = 2\max_{q \in \mathcal{Q}} \|PA_q^{-1}B\| e^{(\lambda_s + \lambda_\mu)T_0}$ and $\theta > 0$. Then, the set

$$\mathcal{A} = \{0\}^{|\mathcal{G}|+2} \times [0, N_0] \times [0, T_0] \times \mathcal{Q} \times \mathcal{U}$$

is E-ISS for system (17) with respect to the input v. □

Proof: Let $V_q(\tilde{x}) = \tilde{x}^\top P\tilde{x}$, $\forall q \in \mathcal{Q}$. For each $q \in \mathcal{Q}$, the time-derivative of V_q satisfies:

$$\dot{V}_q(\tilde{x}) = \dot{\tilde{x}}^\top P\tilde{x} + \tilde{x}^\top P\dot{\tilde{x}} \tag{20a}$$

$$= \tilde{x}^\top (A_q^\top P + PA_q)\tilde{x} + 2\tilde{x}^\top PA_q^{-1}B\Pi(u). \tag{20b}$$

Let $\tau = \log(\omega)\tau_1 + (\lambda_s + \lambda_\mu)\tau_2$ and define the ISS Lyapunov function $V(\xi) = V_q(\tilde{x})e^\tau$, where, $\omega \geq 1$ is such that $V_q(\tilde{x}) \leq \omega V_{q'}(\tilde{x})$, for all $q, q' \in \mathcal{Q}$. During flows we have,

$$\begin{aligned}\dot{\tau} &\in \log(\omega)[0, 1/\tau_d] + (\lambda_s + \lambda_\mu)([0, 1/\tau_a] - \mathbf{1}_{\mathcal{Q}_\mu}(q)) \\ &= [0, \gamma] - (\lambda_s + \lambda_\mu)\mathbf{1}_{\mathcal{Q}_\mu}(q),\end{aligned}$$

where $\gamma = \frac{1}{\tau_a}(\lambda_s + \lambda_\mu) + \frac{\log \omega}{\tau_d}$. During stable modes, the time-derivative of V satisfies

$$\begin{aligned}\dot{V}(\xi) = \dot{V}_q(\tilde{x})e^\tau + V_q(\tilde{x})e^\tau\dot{\tau} \leq -(\lambda_s - \gamma)V_q(\xi)e^\tau \\ + 2 \cdot \|PA_q^{-1}B\| \cdot \|\Pi(u)\| \cdot \|\tilde{x}\| \cdot e^{\log(\omega)N_0 + (\lambda_s + \lambda_\mu)T_0}.\end{aligned}$$

The first inequality above follows from the feasibility of (18a). Completing the squares [24, eq 5] and setting $\tilde{\kappa} = 2 \cdot \max_{q \in \mathcal{Q}} \|PA_q^{-1}B\| \cdot e^{\log(\omega)N_0 + (\lambda_s + \lambda_\mu)T_0}$ yields

$$\begin{aligned}\dot{V}(\xi) &\leq -(\lambda_s - \gamma)V(\xi) + \tilde{\kappa} \cdot \theta\|\tilde{x}\|^2 + \frac{\tilde{\kappa}}{4 \cdot \theta}\|\Pi(u)\|^2 \\ &\leq -(\lambda_s - \gamma)V(\xi) + \frac{\tilde{\kappa} \cdot \theta}{\lambda_{min}(P)}V(\xi) + \frac{\tilde{\kappa}}{4 \cdot \theta}\|\Pi(u)\|^2 \\ &= -\left(\lambda_s - \gamma - \frac{\tilde{\kappa} \cdot \theta}{\lambda_{min}(P)}\right)V(\xi) + \frac{\tilde{\kappa}}{4 \cdot \theta}\|\Pi(u)\|^2.\end{aligned}$$

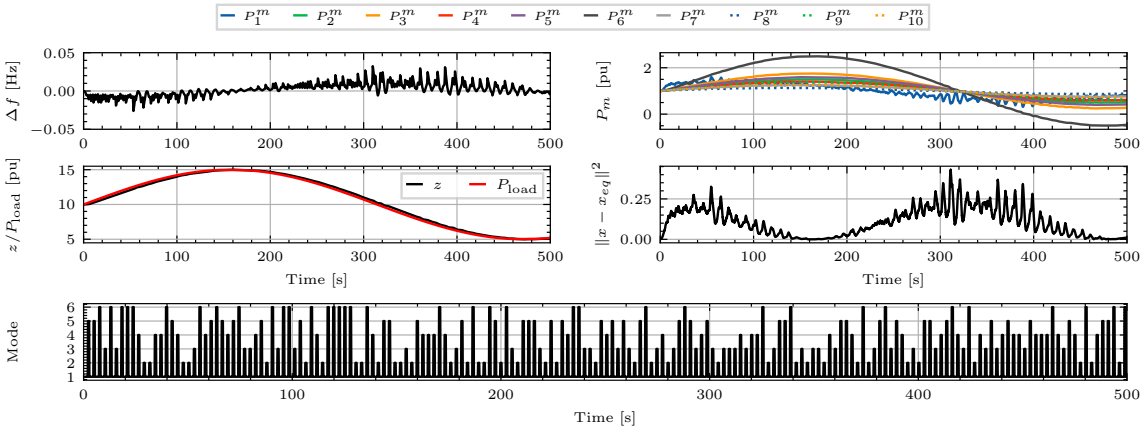

Fig. 3: Slowly time-varying load P_{load}. Stable system for $\tau_a = 4$. Unequal participation factors for the CGs.

L-CSS paper/Mosaic_Stable_Transient.pdf

Fig. 4: Step change in load P_{load}. Stable system for $\tau_a = 4$.

Similarly, during unstable modes $\dot{V}$ satisfies

$$\begin{aligned}\dot{V}(\xi) &= \dot{V}_q(\tilde{x})e^{\tau} + V_q(\tilde{x})e^{\tau}\dot{\tau} \\ &\leq \lambda_\mu V(\xi) + (\gamma - (\lambda_s + \lambda_\mu))V(\xi) + \tilde{\kappa}\cdot\|\Pi(u)\|\cdot\|\tilde{x}\| \\ &= -(\lambda_s - \gamma)V(\xi) + \tilde{\kappa}\cdot\|\Pi(u)\|\cdot\|\tilde{x}\| \\ &\leq -\left(\lambda_s - \gamma - \frac{\tilde{\kappa}\cdot\theta}{\lambda_{min}(P)}\right)V(\xi) + \frac{\tilde{\kappa}}{4\cdot\theta}\|\Pi(u)\|^2.\end{aligned}$$

The first inequality follows by the feasibility of (18b). For V to decrease during flows, we require $\left(\lambda_s - \gamma - \frac{\tilde{\kappa}(\lambda_s,\lambda_\mu)\cdot\theta}{\lambda_{min}(P)}\right) > 0$. Additionally, our choice of a common Lyapunov function implies $\omega = 1$. This reduces our assumption to the bound (19). Finally, during jumps we have $\tau^+ = \tau - \log(\omega) = \tau$ and $V(\xi^+) = V_{q^+}(\tilde{x}^+)e^{\tau^+} = \tilde{x}^\top P\tilde{x}\cdot e^{\tau} = V(\xi)$. The stability result follows now from [25, Lemma 9]. ∎

2) BMI Informed Bounds: The use of a non-convex formulation in terms of BMIs in (18) enables a less conservative estimate of the parameter τ_a that satisfies (19). Indeed, setting $\dot{u} = 0$, equation (20b) reduces to:

$$\dot{V}_q = \tilde{x}^\top(A_q^\top P + PA_q)\tilde{x}. \tag{22}$$

Requiring strong decrease of (22) during stable flows corresponds to the inequality $\tilde{x}^\top(A_q^\top P + PA_q)\tilde{x} \leq -\lambda_s\tilde{x}^\top P\tilde{x}$. On the other hand, during unstable modes, we require $\tilde{x}^\top(A_q^\top P + PA_q)\tilde{x} \leq \lambda_\mu\tilde{x}^\top P\tilde{x}$. The BMIs in (18) now follow readily. To solve the BMIs, we employ a grid search method for values of λ_s and λ_u^*, where λ_μ^* is defined as $\max_{\mu\in\mathcal{Q}_\mu}\lambda_u$ such that it satisfies equation (18b) for all $\mu \in \mathcal{Q}_\mu$. For each $(\lambda_s, \lambda_\mu^*)$ pair resulting from the grid search, we solve equation (18) for P. If it exists a symmetric positive definite matrix $P \in \mathbb{R}^{|\mathcal{G}|+2\times|\mathcal{G}|+2}$, we record the pair $(\lambda_s, \lambda_\mu^*)$. Upon grid search completion, we want to select the pair $(\lambda_s, \lambda_\mu^*)$ such that τ_a obtained from 19 is minimum; it corresponds to the tightest theoretical bound on τ_a we can find. In order to achieve this objective, we let the tunable parameter θ be sufficiently small, such that (19) can be approximated by $\tau_a > 1 + \frac{\lambda_\mu}{\lambda_s}$. Replacing λ_μ by λ_μ^*, the theoretical bound for τ_a is obtained such that, for every pair $(\lambda_s, \lambda_\mu^*)$ satisfying (18), $\tau_a^{\text{bound}} = 1 + \frac{\lambda_\mu^*}{\lambda_s}$ is minimum. The above procedure can generate bounds that are orders of magnitude less conservative compared to those obtained via worst-case analyses, thus providing a better assessment of the robustness properties of the power transmission system.

3) Numerical Results: We consider the IEEE 39-bus test system that is composed of 39 buses and 10 conventional generators (CGs). For the CGs, we fix $\tau_g = 2, D_g = 1.5$ and $K_{\text{gov},g} = \frac{1}{0.05}\frac{S_g}{S_{\text{base}}}$, $\forall g \in \mathcal{G}$ where S_g is the nominal power of generator g and S_{base} the system base power. This represents a droop coefficient of 5% for every generator. The other parameters for the generators are taken from the IEEE 39-bus test system data. For the DERs, we impose $M_d = 40, D_d \in \{1.5, -100, -200, -150, -120, -170\}$, $\forall d \in \mathcal{D}$ where $D_d = 1.5$ represents mode 1 and is the stable mode while $D_d \in \{-100, -200, -150, -120, -170\}$ represents modes 2 to 6 and are the unstable modes. For the secondary controller, we impose $\tau_z = 10$, $\beta = -0.1$ and $\zeta = \{\zeta_i\}_{i\in\mathcal{G}}$ such that every generator does not participate equivalently to the secondary frequency response, but $\sum_{i\in\mathcal{G}}\zeta_i = 1$. We assume that the participation factors are the solution of an optimization problem (i.e., maximizing efficiency or minimizing production costs). By using the BMI informed bounds we found that $\lambda_s = 0.21$ and $\lambda_\mu^* = 4.3$, giving us a theoretical bound $\tau_a > 21.47$. This result suggests that the transmission system remains stable whenever the "intensity" of the attacks on the grid is below 5%, i.e., if for any given window of time the attacks are rejected or corrected by the SO more than 95% of the time. This estimate is conservative since it considers *any* signal $\sigma \in \mathcal{S}$ satisfying (1) and (2).

Scenarios: Two different scenarios are considered: **a)** In the first scenario, we investigate the stability of the system for initial conditions different from the equilibria x_{eq}. We consider $x_0 = (1+\varepsilon_1)x_{eq} + \varepsilon_2\mathbb{1}_{|\mathcal{G}|+2}$, with $\varepsilon_1 = 0.05$ and $\varepsilon_2 = 0.0005$. Figure 2 shows the distance from equilibria under attack for $\tau_a = 4$ and $\tau_a = 3$, respectively. One can see that $\tau_a = 3$ leads to instability. Our theoretical bound $\tau_a > 21.47$ is in the same order of magnitude. **b)** For the second scenario, we investigate slowly time-varying loads modeled as $P_{\text{load}} = 10 + \sin(0.01t)$. The results are shown in Figure 3, illustrating the tracking capabilities of the system under attacks. We have performed additional numerical studies, which can be found in the extended manuscript [26]. Finally, Figure 4 illustrates the performance of the system under attacks for the case when the load is constant. As observed, the power transmission system remains stable provided the "persistency" of the attacks satisfies the established bounds. The code used in the simulations is available at `https://github.com/A-clt/GridResilience_BMIsApproach.git`.

VI. Conclusions

In this work, we considered an LTI aggregate model of a power transmission system subject to a class of persistent, possibly non-periodic, and deceiving attacks. The persistence of attacks was seen to be equivalent to a class of switching signals obeying specific ADT and AAT bounds. Using the framework of hybrid dynamical systems, a Lyapunov-based stability analysis resulted in a non-convex, BMI formulation for obtaining theoretical bounds on the parameters τ_a and τ_d. The feasibility of the BMIs was checked on the IEEE 39-bus test system via a grid search approach. It was seen that the theoretical bounds were in the same order of magnitude as the ones obtained via simulations of two scenarios with varying changes in loads and initial conditions. Future research will focus on relaxing the assumption of a common equilibrium point in the switching system, as well as incorporating sudden changes in the loads (deterministic and stochastic) by suitably modifying the jump map $G(\cdot)$ in the hybrid dynamics (17).

References

[1] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *An. Rev. in Control*, vol. 47, pp. 394–411, 2019.

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

[3] L. Robert, J. Michael, and C. Tim, "Analysis of the cyber attack on the Ukrainian power grid," *USA: Electricity Information Sharing and Analysis Centre (E-ISAC)*, 2016.

[4] J. Giraldo and M. Parvania, "Cyber-resilient frequency control of power grids with energy storage systems," in *11th Bulk Power Systems Dynamics and Control Symposium*, 2022.

[5] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, "Electric power grid resilience to cyber adversaries: State of the art," *IEEE Access*, vol. 8, pp. 87592–87608, 2020.

[6] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[7] F. Galarza-Jimenez, G. Bianchin, J. I. Poveda, and E. Dall'Anese, "Online optimization of LTI systems under persistent attacks: Stability, tracking, and robustness," *arXiv preprint arXiv:2102.09356*, 2021.

[8] Y. Li, J. Wang, R. Wang, W. Gao, Q. Sun, and H. Zhang, "A switched newton-raphson-based distributed energy management algorithm for multienergy system under persistent DoS attacks," *IEEE Trans. on Automation Science and Engineering*, vol. 19, pp. 1–13, 08 2021.

[9] J. Liu, X. Lu, and J. Wang, "Resilience analysis of DC microgrids under denial of service threats," *IEEE Trans. on Power Syst.*, vol. 34, no. 4, pp. 3199–3208, 2019.

[10] A. Patel, S. Roy, and S. Baldi, "Wide-area damping control resilience towards cyber-attacks: A dynamic loop approach," *IEEE Trans. on Smart Grid*, vol. 12, pp. 3438–3447, July 2021.

[11] H. Javanmardi, M. Dehghani, M. Mohammadi, S. Siamak, and M. R. Hezamsadeh, "BMI-based load frequency control in microgrids under false data injection attacks," *IEEE Syst. Journal*, vol. 16, pp. 1–11, 03 2021.

[12] M. S. Mahmoud and M. M. Hamdan, "Stabilization of distributed cyber physical systems subject to denial-of-service attack," *International Journal of Control*, vol. 95, no. 3, pp. 692–702, 2022.

[13] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *49th IEEE conference on decision and control (CDC)*, pp. 5991–5998, IEEE, 2010.

[14] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th annual Allerton conference on communication, control, and computing (Allerton)*, pp. 911–918, IEEE, 2009.

[15] S. S. Guggilam, C. Zhao, E. Dall'Anese, Y. C. Chen, and S. V. Dhople, "Optimizing DER participation in inertial and primary-frequency response," *IEEE Trans. on Power Syst.*, vol. 33, no. 5, pp. 5194–5205, 2018.

[16] R. Goebel, R. G. Sanfelice, and A. R. Teel, "Hybrid dynamical systems: Modeling, Stability, and Robustness," *Princeton, NJ, USA*, 2012.

[17] P. Kundur, *Power System Stability and Control*. McGraw-Hill, 1994.

[18] F. Dörfler and D. Groß, "Control of low-inertia power systems," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 6, pp. 415–445, 2023.

[19] H. Mavalizadeh, L. A. D. Espinosa, and M. R. Almassalkhi, "Improving frequency response with synthetic damping available from fleets of distributed energy resources," *IEEE Trans. on Power Syst.*, 2023.

[20] Y. Cheng, R. Azizipanah-Abarghooee, S. Azizi, L. Ding, and V. Terzija, "Smart frequency control in low inertia energy systems based on frequency response techniques: A review," *Applied Energy*, vol. 279, p. 115798, 2020.

[21] A. J. Wood, B. F. Wollenberg, and G. B. Sheblé, *Power generation, operation, and control*. John Wiley & Sons, 2013.

[22] P. M. Anderson and M. Mirheydar, "A low-order system frequency response model," *IEEE Trans. on Power Syst.*, vol. 5, no. 3, pp. 720–729, 1990.

[23] J. I. Poveda and A. R. Teel, "A framework for a class of hybrid extremum seeking controllers with dynamic inclusions," *Automatica*, vol. 76, pp. 113–126, 2017.

[24] Z. P. Jiang, A. R. Teel, and L. Praly, "Small-gain theorem for ISS systems and applications," *Mathematics of Control, Signals and Systems*, vol. 7, pp. 95–120, 1994.

[25] D. E. Ochoa, N. Espitia, and J. I. Poveda, "Prescribed-time control in switching systems with resets: A hybrid dynamical systems approach," *arXiv preprint arXiv:2308.16368*, 2023.

[26] A. Colot, V. Shenoy, G. Cavraro, E. Dall'Anese, and J. I. Poveda, "On the stability of power transmission systems under persistent inverter attacks: A Bi-linear matrix approach (extended manuscript)." `https://poveda.ucsd.edu/drafts`, 2024.