Extremum Seeking Under Persistent Gradient Deception: A Switching Systems Approach

Felipe Galarza-Jimenez, Jorge I. Poveda, *Member, IEEE*, Gianluca Bianchin, *Member, IEEE*, and Emiliano Dall'Anese, *Member, IEEE*

***Abstract*—This letter focuses on extremum seeking (ES) controllers with adversarial attacks in the form of deception signals. While a persistent attack in a feedback controller may be difficult to identify or mitigate, for a broad class of algorithms it suffices to achieve mitigation "sufficiently often" in order to preserve the stability properties of the system. In this letter, we explore for the first time the resilience properties of ES controllers with respect to a class of persistent multiplicative attacks that are purposely designed to destabilize optimization-based feedback controllers. By leveraging Lyapunov-based arguments for switching systems and singular-perturbation theory for hybrid dynamical systems, we characterize a family of persistent multiplicative attacks under which gradient-based ES, Newton-Like ES, and Accelerated gradient ES controllers provably preserve their stability properties.**

***Index Terms*—Extremum seeking, switching systems, cyber-security.**

I. Introduction

SELF-TUNING control methods and gradient-free optimization algorithms have been adopted in many engineering applications, ranging from process control, traffic systems, and multi-agent systems. Extensive efforts have focused on extremum seeking (ES) control thanks to its practical success and theoretical guarantees; see [1]–[6]. ES is a gradient-free optimization method that combines probing input signals with output-feedback information to regulate a dynamical system to the extremum of an unknown cost function. However, as illustrated in the left plot of Fig. 1, in practice, the physical process and the different components of the controller might be connected by means of different communication links that can be prone to cyberattacks. Nevertheless, while the resilience and robustness properties of different control systems under attacks have been recently studied in the literature, see, e.g., [7]–[10], in the context of ES they remain mostly unexplored.

Manuscript received September 13, 2020; revised November 28, 2020; accepted December 23, 2020. Date of publication January 11, 2021; date of current version June 23, 2021. This work was supported in part by the NSF under Award 1941896 and Award 1947613, and in part by the CU Boulder Autonomous Systems IRT. Recommended by Senior Editor S. Tarbouriech. *(Corresponding author: Felipe Galarza-Jimenez.)*

The authors are with the Department of Electrical, Computer, and Energy Engineering, University of Colorado at Boulder, Boulder, CO 80302 USA (e-mail: fega5085@colorado.edu).

Digital Object Identifier 10.1109/LCSYS.2021.3050451

In this letter, we study the resilience properties of ES controllers aiming to minimize an unknown cost function $\phi : \mathbb{R}^n \to \mathbb{R}$ that is accessible only via its evaluations. We focus on controllers described by the equations:

$$\dot{x} = F(x, \xi), \qquad u = x + a\hat{\mu}, \qquad a > 0, \tag{1}$$

where $x \in \mathbb{R}^n$ is the main state of the ES controller, $F : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ describes the optimization dynamics of the controller, $\xi \in \mathbb{R}^n$ is an auxiliary state that represents an estimate of the gradient (or higher derivatives) of ϕ, and $\hat{\mu} \in \mathbb{R}^n$ is a periodic probing signal. Under a *nominal* operation, ES controllers have been extensively studied; see [1]–[3], [5], [6], [11]. In contrast to these results, in this letter we consider a situation where the controller is subject to external attacks that *persistently* modify the estimated gradient ξ, generating a deceptive signal $\hat{\xi} \in \mathbb{R}^n$, defined as follows:

$$\hat{\xi} = \begin{cases} Q_s\xi, & \text{without attack, i.e., } Q_s := \mathbb{I}_n, \\ Q_u\xi, & \text{under attack, i.e., } Q_u := \text{diag}(q_1, \ldots, q_n), \end{cases} \tag{2}$$

where $\text{diag}(q_1, \ldots, q_n)$ represents a diagonal matrix with entries given by the vector $[q_1, \ldots, q_n]^\top \in \mathbb{R}^n$. Such type of deceptive signals can easily destabilize a gradient-based controller. In this letter, we consider a general class of *deception* attacks characterized by matrices Q_u that satisfy, for a given pair $(q, N) \in \mathbb{R}_{>0} \times \mathbb{Z}_{\geq 1}$, the following *Three Properties*:

1) $\forall\ i$, q_i can take values in a finite set $\{q_{i,1}, \ldots, q_{i,N}\}$.
2) $\forall\ i$, $|q_i| \leq q$, where $0 < q < \infty$.
3) $\exists\ i$, such that $q_i \leq 0$.

We denote by $\mathcal{Q}_u$ the set of all matrices Q_u that satisfy the *Three Properties*. This model is quite general, and it captures classes of multiplicative attacks that can persistently modify the sign and/or the magnitude of the estimated gradient of ϕ, including signals that effectively vanish the gradient, i.e., $q_i = 0$, $\forall\ i$, or completely deceive the gradient, i.e., $q_i = -1$, $\forall\ i$. Similar types of attacks have been extensively studied in the cyber-physical security literature [4]–[6], [10]–[17], particularly in the context of Denial of Service (DoS) or jamming attacks; see [7] and references therein.

The design and analysis of resilient control algorithms operating under jamming and communication drops was studied in [12]. In [13], an event-triggered controller with stability guarantees for systems under DoS attacks was presented. Jamming in networks was investigated in [14] and references therein. For matrices Q_u with non-zero diagonal entries, the model (2) captures *deception attacks* [7], which were the focus of [15] and [16]. Recent works have investigated the security

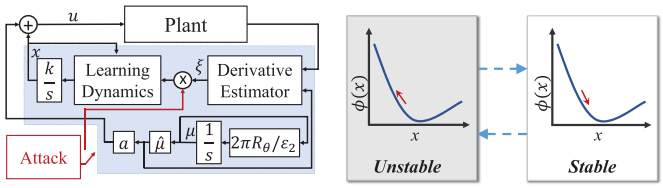

Fig. 1. ES controller under persistent gradient deception. The system is modeled as a switched system with unstable modes.

of distributed optimization under Byzantine attacks [17]–[19]. A similar model was considered in [10] for sub-gradient methods, and in [9] for centralized optimization under DoS attacks. However, to the best of our knowledge, the study of ES controllers under attacks remains completely unexplored.

Contributions: The contribution of this letter is threefold. First, we propose a new set-valued model of persistent, non necessarily periodic, multiplicative attacks against ES algorithms, which generalizes existing classes of jamming attacks studied in the literature of cyber-security. Such types of attacks are difficult to mitigate due to their lack of periodicity and predictability. Second, we present the *first* stability analysis of averaging-based ES dynamics operating under persistent deceptive attacks of the form (2). In particular, by using Lyapunov-based tools for Hybrid Dynamical Systems [4], [20], we characterize an entire family of persistent attacks under which the stability properties of the ES controllers are preserved. This characterization is provided for three common types of ES dynamics: (a) Gradient descent-based ES [1], [2], [21], (b) Newton-Like ES [3], [5], and (c) Accelerated gradient ES [6]. Our results reveal the effect of the parameters of the cost function on the resilience properties of the controllers. Moreover, we uncover novel trade-offs between fast convergence and resilience to attacks in nominal and accelerated ES algorithms. Finally, we present the first stability result for controllers that continuously switch between Gradient ES and Newton-Like ES, a result that may be of independent interest.

II. Preliminaries

Given a compact set $\mathcal{A} \subset \mathbb{R}^n$ and a vector $z \in \mathbb{R}^n$, we let $|z|_{\mathcal{A}} := \min_{s\in\mathcal{A}} |z - s|$, where $|z|$ denotes the Euclidean norm of z. We use $\mathbb{S}^1 := \{z \in \mathbb{R}^2 : z_1^2 + z_2^2 = 1\}$ to denote the unit circle in $\mathbb{R}^2$, and $\mathbb{T}^n := \mathbb{S}^1 \times \mathbb{S}^1 \times \ldots \times \mathbb{S}^1$ to denote the nth Cartesian product of $\mathbb{S}^1$. For a set X and $A \subseteq X$, we denote the set indicator function by $\mathcal{I}_A : X \to \{0, 1\}$, where $\mathcal{I}_A(x) = 1$ if $x \in A$, and $\mathcal{I}_A(x) = 0$ if $x \notin A$. Given two vectors $p_1, p_2 \in \mathbb{R}^n$, we use $(p_1, p_2) = (p_1^\top, p_2^\top)^\top$ to denote their concatenation. In this letter, we deal with algorithms modeled as hybrid dynamical systems (HDS) [20], of the form

$$p \in C, \ \dot{p} \in F(p), \qquad p \in D, \ p^+ \in G(p), \tag{3}$$

where $p \in \mathbb{R}^n$ is the state, $F : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ is the flow map, $G : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ is the jump map, $C \subset \mathbb{R}^n$ is the flow set, and $D \subset \mathbb{R}^n$ is the jump set. We note that solutions p to (3) are defined on hybrid time domains, denoted by $\mathrm{dom}(p)$, and we refer to [20, Ch. 2] for a precise definition. Given a compact set $\mathcal{A} \subset C \cup D$, system (3) is said to render $\mathcal{A}$ uniformly globally asymptotically stable (UGAS) if there exists a class $\mathcal{KL}$ function β (see [20, Definition 3.38]) such that every solution of (3) satisfies $|p(t, j)|_{\mathcal{A}} \leq \beta(|p(0, 0)|_{\mathcal{A}}, t+j)$ for all $(t, j) \in \mathrm{dom}(p)$.

We also consider ε-parametrized HDS of the form

$$p \in C, \quad \dot{p} \in F_\varepsilon(p), \qquad p \in D, \quad p^+ \in G(p), \tag{4}$$

where $\varepsilon > 0$. For this system, a compact set $\mathcal{A} \subset C$ is said to be Semi-Globally Practically Asymptotically Stable (SGPAS) as $\varepsilon \to 0^+$ if there exists a class $\mathcal{KL}$ function β such that for every $\delta_0 > \nu > 0$ there exists $\varepsilon^* > 0$ such that for all $\varepsilon \in (0, \varepsilon^*)$ every solution of (4) with $|p(0, 0)|_{\mathcal{A}} \leq \delta_0$ satisfies $|p(t, j)|_{\mathcal{A}} \leq \beta(|p(0, 0)|_{\mathcal{A}}, t + j) + \nu, \ \forall \ (t, j) \in \mathrm{dom}(p)$. The notion of SGPAS can be extended to systems that depend on multiple parameters $\varepsilon = [\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\ell]^\top$. In this case, and with some abuse of notation, we say that the system (4) renders the set $\mathcal{A}$ SGPAS as $(\varepsilon_\ell, \ldots, \varepsilon_2, \varepsilon_1) \to 0^+$, where the parameters are tuned *in order*, starting from ε_1; see also [6], [11] for a similar definition.

III. Model and Main Results

We begin by characterizing the class of static plants that we consider in this letter.

Assumption 1: The function $u \mapsto \phi(u)$ is strongly convex with minimizer $u^* \in \mathbb{R}^n$, and it is twice continuously differentiable with Lipschitz continuous gradient.

By Assumption 1, there exist $\kappa, \ell > 0$ such that $\frac{\kappa}{2}|u-u^*|^2 \leq \phi(u)-\phi(u^*) \leq \frac{\ell}{2}|u-u^*|^2$ for all $u \in \mathbb{R}^n$. These constants will play an important role in our results. Note that Assumption 1 is standard in ES; see [1], [3], [5], [6] and [11].

A. Hybrid Automaton With Monitoring States

To model the persistent deception attacks acting on the ES controller, we model the attack as a switching signal $t \mapsto Q(t)$ taking values in the set $\mathcal{Q} := \mathcal{Q}_s \cup \mathcal{Q}_u$, where $\mathcal{Q}_s := \{\mathbb{I}_n\}$ denotes the nominal operation (i.e., no attacks), and $\mathcal{Q}_u$ is the set of adversarial matrices that satisfy the *Three Properties* listed in the introduction. Let $N(s, t)$ denote the number of switches of Q in the interval $[s, t]$. We assume that $Q(t)$ satisfies a standard *average dwell-time condition* (ADTC) of the form $N(s, t) \leq \eta_1(t - s) + N_0$, for all $0 \leq s \leq t$, [20], where $N_0 \in \mathbb{Z}_{\geq 1}$ and $\eta_1 > 0$. Further, let $T(s, t)$ denote the total activation time of the unstable modes during the interval $[s, t]$, i.e., $T(s, t) = \int_s^t \mathcal{I}_{\mathcal{Q}_u}(Q(r))dr$. Further, we assume that Q satisfies a *time-ratio constraint* (TRC) of the form $T(s, t) \leq \eta_2(t - s) + T_0$, [4], where $T_0 \in \mathbb{R}_{\geq 0}$ and $\eta_2 \in [0, 1)$. Condition (TRC) imposes an upper bound on the activation time of the adversarial modes in the set $\mathcal{Q}_u$, during any interval $[s, t]$. To generate switching signals $t \mapsto Q(t)$ that satisfy both conditions (ADTC) and (TRC), we make use of the following lemma, corresponding to [4, Lemma 7].

Lemma 1: Consider a set-valued HDS with state $\vartheta := (\tau_1, \tau_2, Q) \in \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \times \mathcal{Q}$, and hybrid dynamics:

$$\vartheta \in C_M := [0, N_0] \times [0, T_0] \times \mathcal{Q}, \tag{5a}$$

$$\begin{pmatrix} \dot{\tau}_1 \\ \dot{\tau}_2 \\ \dot{Q} \end{pmatrix} \in F_M(\vartheta) := \begin{pmatrix} [0, \eta_1] \\ [0, \eta_2] - \mathcal{I}_{\mathcal{Q}_u}(Q) \\ 0 \end{pmatrix}, \tag{5b}$$

$$\vartheta \in D_M := [1, N_0] \times [0, T_0] \times \mathcal{Q}, \tag{5c}$$

$$\begin{pmatrix} \tau_1^+ \\ \tau_2^+ \\ Q^+ \end{pmatrix} \in G_M(\vartheta) := \begin{pmatrix} \tau_1 - 1 \\ \tau_2 \\ \mathcal{Q}\backslash\{Q\} \end{pmatrix}, \tag{5d}$$

where $T_0 \geq 0$, $N_0 \in \mathbb{Z}_{\geq 1}$, $\eta_1 > 0$, and $\eta_2 \in (0, 1)$. Then: (i) for each solution ϑ of (5), the hybrid time-domain $\mathrm{dom}(\vartheta)$

satisfies (ADTC)-(TRC); (ii) for every time-domain satisfying (ADTC)-(TRC) there exists a solution of (5) with the same time-domain.

B. Extremum Seeking Under Persistent Attacks

The ES algorithms that we consider in this letter make use of a periodic probing signal that can be generated by dynamic oscillators of the form:

$$\varepsilon_2 \dot{\mu} = 2\pi \mathcal{R}_\theta \mu, \quad \mu \in \mathbb{T}^n, \varepsilon_2 > 0, \tag{6}$$

where $\mathcal{R}_\theta \in \mathbb{R}^{2n\times 2n}$ is block-diagonal with blocks $\mathcal{R}_{\theta_i} := [0, \theta_i; -\theta_i, 0]$, and $\theta_i > 0$. The odd components of the solutions of system (6) can be computed as:

$$\mu_i(t) = \mu_i(0)\cos\left(\frac{2\pi}{\varepsilon_2}\theta_i t\right) + \mu_{i+1}(0)\sin\left(\frac{2\pi}{\varepsilon_2}\theta_i t\right), \tag{7}$$

for all $i \in \{1, 3, 5, \ldots\}$, with $\mu_i(0)^2 + \mu_{i+1}(0)^2 = 1$, and we define $\hat{\mu} := [\mu_1, \mu_3, \mu_5, \ldots, \mu_{2n-1}]^\top$.

Assumption 2: For all i, the parameters θ_i are positive rational numbers, and $\theta_i \neq \theta_j$, for all $i \neq j$.

To facilitate our analysis, the ES algorithms shall also implement the following gradient and gradient-Hessian estimation dynamics, with states $\xi_1 \in \mathbb{R}^n$ and $\xi_2 \in \mathbb{R}^n$, respectively:

$$\varepsilon_1 \dot{\xi}_1 = -\xi_1 + G(\hat{\mu}, u), \ \ \varepsilon_1 \dot{\xi}_2 = -H(\hat{\mu}, u)\xi_2 + G(\hat{\mu}, u), \tag{8}$$

where u is given by (1), ε_1 is a tunable parameter satisfying $0 < \varepsilon_2 \ll \varepsilon_1$, and where the mappings $G : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ and $H : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^{n\times n}$ are defined as $G(\hat{\mu}, u) := \frac{2}{a}\hat{\mu}\phi(u)$, and H is symmetric with entries satisfying the following equations:

$$H_{ii} = \frac{16}{a^2}\left(\hat{\mu}_i^2 - \frac{1}{2}\right)\phi(u), \ \ H_{ij} = \frac{4}{a^2}\hat{\mu}_i\hat{\mu}_j\phi(u), \ \ \forall\ i \neq j.$$

By using the formalism (3), and in particular, the hybrid automaton (5), we can simultaneously study three different types of ES controllers under gradient deception:

1) Gradient descent-based ES dynamics (GDES) [1], [21]:

$$C := \mathbb{R}^n, \quad \dot{x} = F_Q(\xi_1) := -kQ\xi_1, \tag{9}$$

2) Newton-Like ES dynamics (NLES) [3], [5]:

$$C := \mathbb{R}^n, \quad \dot{x} = F_Q(\xi_2) := -kQ\xi_2, \tag{10}$$

3) Hybrid Accelerated ES dynamics (HAES) [6]:

$$C := \mathbb{R}^n \times \mathbb{R}^n \times [\delta, \Delta], \quad \Delta > \delta > 0, \tag{11a}$$
$$(\dot{x}, \dot{y}, \dot{z}) = F_Q := \left(\tfrac{2}{z}(y - x), -2zkQ\xi_1, \tfrac{1}{2}\right), \tag{11b}$$
$$D := \mathbb{R}^n \times \mathbb{R}^n \times \{\Delta\}, \tag{11c}$$
$$\left(x^+, y^+, z^+\right) = G_u(x) := (x, x, \delta), \tag{11d}$$

where (y, z) are extra auxiliary states, and the parameters are selected such that $\Delta^2 - \delta^2 \geq \frac{1}{2k\kappa}$; see [6, Th. 2].

C. Main Results

The following theorem corresponds to the first main result of this letter. It characterizes, for each ES algorithm, a broad family of persistent deceptive attacks $t \mapsto Q(t)$ under which the controllers preserve their ability to solve the ES problem. For the GDES and the NLES, we state the stability properties with respect to the set (singleton) $\mathcal{O} := \{u^*\}$, whereas for the HAES we use $\mathcal{O} := \{u^*\} \times \{u^*\} \times [\delta, \Delta]$. We also use the set $\mathcal{T} := [0, N_0] \times [0, T_0] \times \mathcal{Q}$ to assert the stability properties of the hybrid automaton (5).

Theorem 1: Consider the ES controllers with dynamics (6), (8), (9)-(11), interconnected with the hybrid automaton (5). Suppose that Assumptions 1-2 hold. Then, when $\eta_1 > 0$ and $0 < \eta_2 < 1/(1 + \gamma)$, the compact set $\mathcal{A} := \mathcal{T} \times \mathcal{O} \times \{0\} \times \mathbb{T}^n$ is SGPAS as $(\varepsilon_2, a, \varepsilon_1) \to 0^+$, where:

(a) For *GDES* and *NLES*: $\gamma = q\ell/\kappa$.

(b) For *HAES*: $\gamma = \frac{2\Delta}{\delta}\frac{\max\{2, k\ell\delta\Delta\bar{q}\}\max\{1, \frac{2}{3}k\Delta^2\ell\}}{\min\{1, k\Delta\delta\kappa\}\min\{1, 2k\delta^2\kappa\}}$,

where $\bar{q} = \max\{2(2 + q), (5 + q)\}$, and (κ, ℓ) satisfy the inequality given by Assumption 1.

The result of Theorem 1 provides a novel characterization of the resilience properties of ES algorithms under a broad class of attacks. In certain cases, the sufficient conditions of Theorem 1 can be shown to be also necessary, e.g., for the GDES and the NLES with $\phi(u) = u^2$, and $Q_u = -\mathbb{I}_n$, the controller becomes unstable when $\eta_2 \geq 1/(1 + \gamma)$.

Remark 1: For the GDES and the NLES, Theorem 1 can be interpreted as follows: larger condition numbers ℓ/κ require less frequent attacks to guarantee SGPAS. For instance, when ϕ is quadratic with Hessian matrix W, we have that $\gamma = q\lambda_{\max}(W)/\lambda_{\min}(W)$. Since this ratio is related to the eccentricity of the sub-level sets of ϕ [22, Exercise 9.1], they serve as a qualitative indicator of the resilience of the algorithms under persistent deception attacks.

Remark 2: As shown in the proof of Theorem 1 (see Proof of Lemma 3), when $Q_u := -\mathbb{I}_n$ in the NLES, a tighter bound for η_2 can be derived. In particular, in this case one obtains $\gamma = 1$, which leads to SGPAS whenever $\eta_2 < \frac{1}{2}$, i.e., when the activation time in the unstable mode Q_u is less than 50%. Interestingly, in this case the bound is independent of the parameters (κ, ℓ) of the cost function.

Remark 3: For HAES, Theorem 1 establishes a bound for η_2 that depends on: (i) the gain k and the parameters (κ, ℓ) of the cost, and (ii) the parameters (δ, Δ) describing the restarting mechanism in (11c)-(11d). Moreover, when $Q_u = -\mathbb{I}_n$ and $\ell > \frac{1}{2k\delta\Delta} > \kappa$, then $\gamma = 48(\ell/\kappa)^2(\Delta/\delta)^3$. Since $\gamma \geq 1$, the result establishes a trade-off between the fast convergence of the HAES and the less conservative bound obtained for the GDES, i.e., a persistent attack that might destabilize the HAES may not necessarily destabilize the GDES or the NLES.

The previous remark suggests that in some cases it may be of interest to switch between different nominal ES algorithms. The next theorem addresses this case.

Theorem 2: Consider the ES controllers with dynamics (6), (8), interconnected with the hybrid automaton (5), where now $\mathcal{Q}_u := \{\emptyset\}$ and $\mathcal{Q}_s := \{\text{System (9)}\} \cup \{\text{System (10)}\}$, i.e., switching between GDES and NLES. Let Assumptions 1 and 2 hold, and suppose $Q = \mathbb{I}_n$, and η_1^* is given by

$$\eta_1^* = \frac{2k\min\{1, \kappa\}}{\log(\max\{1, \ell^2\}) - \log(\min\{1, \kappa^2\})}.$$

Then, whenever $\eta_2 = 0$ and $0 < \eta_1 < \eta_1^*$ the compact set $\mathcal{A} := \mathcal{T} \times \{u^*\} \times \{0\} \times \mathbb{T}^n$ is SGPAS as $(\varepsilon_2, a, \varepsilon_1) \to 0^+$.

The result of Theorem 2 establishes a sufficient condition on how frequently the ES controller can switch between nominal GDES and NLES in order to preserve SGPAS. To the best knowledge of the authors, this result is also new in the literature of ES, and it may be of independent interest.

IV. Analysis

In this section, we present the proofs of Theorems 1 and 2. We first construct a unified model that formalizes the interconnection between the ES controller and the Hybrid Automaton. After this, we establish UGAS for the (averaged) hybrid dynamics, and then we leverage singular perturbation arguments in hybrid ES to finalize the claims.

A. Unified Modeling Framework

Let $\sigma := (\vartheta, \psi)$, where $\psi = x$ for GDES and the NLES, and $\psi = (x, y, z)$ for the HAES, and $p_0 = \dim(\psi)$. First, we define a set-valued map F_σ as follows

$$F_\sigma(\sigma, \xi_1, \xi_2) := F_M(\vartheta) \times \{F_Q(\psi, \xi_1, \xi_2)\}, \tag{12}$$

where F_M is given by (5b), and F_Q is defined in equations (9)-(11) for each of the ES dynamics. Next, we define the set $C_\sigma := C_M \times C$, where C_M is defined in (5a) and C is defined in equations (9)-(11) for each ES. Subsequently, we define two set-valued mappings $G_{\sigma,1}$, $G_{\sigma,2}$ as follows:

$$G_{\sigma,1}(\sigma) := G_M(\vartheta) \times \{\psi\}, \;\; G_{\sigma,2}(\sigma) := \{\vartheta\} \times \{G_u(\psi)\}, \tag{13}$$

where $G_u(\psi) = x$ for GDES and NLES, and G_u is given by (11d) for HAES. Next, we define two sets $D_{\sigma,1}, D_{\sigma,2}$ as follows: $D_{\sigma,1} := D_M \times \mathbb{R}^{p_0}$, and $D_{\sigma,2} := C_M \times D$, where D is given by (11c) for HAES, and $D := \emptyset$ for GDES and NLES. Using this construction, the closed-loop system (1)-(5) can be modeled by a HDS with states $(\sigma, \xi_1, \xi_2, \mu)$, flow set $C_\sigma \times \mathbb{R}^n \times \mathbb{R}^n \times \mathbb{T}^n$, continuous-time dynamics:

$$\begin{pmatrix} \dot\sigma \\ \dot\xi_1 \\ \dot\xi_2 \\ \dot\mu \end{pmatrix} \in \begin{pmatrix} F_\sigma(\sigma, \xi_1, \xi_2) \\ \frac{1}{\varepsilon_1}\big(-\xi_1 + G(\hat\mu, x + a\hat\mu)\big) \\ \frac{1}{\varepsilon_1}\big(-H(\hat\mu, x + a\hat\mu)\xi_2 + G(\hat\mu, x + a\hat\mu)\big) \\ \frac{1}{\varepsilon_2} 2\pi \mathcal{R}_\theta \mu \end{pmatrix},$$

jump set $D_\sigma \times \mathbb{R}^n \times \mathbb{R}^n \times \mathbb{T}^n$, and discrete-time dynamics $(\sigma^+, \xi_1^+, \xi_2^+, \mu^+) \in G_\sigma(\sigma) \times \{\xi_1\} \times \{\xi_2\} \times \{\mu\}$, where

$$G_\sigma(\sigma) := \begin{cases} G_{\sigma,1}(\sigma), & \text{if } \sigma \in D_{\sigma,1} \\ G_{\sigma,2}(\sigma), & \text{if } \sigma \in D_{\sigma,2} \\ G_{\sigma,1}(\sigma) \cup G_{\sigma,2}(\sigma), & \text{if } \sigma \in D_{\sigma,1} \cap D_{\sigma,2}. \end{cases}$$

This map captures the jumps of the hybrid automaton (i.e., switches of Q) *and* any intrinsic jump of the ES controllers (9)-(11). Naturally, the solutions of this HDS are not unique.

B. Averaging and Singular Perturbation Analysis

The previous HDS is in standard form to apply singular perturbation theory for hybrid systems [23], where μ acts as the fast state. By using the periodicity of (7), and standard averaging arguments in ES, we compute the average dynamics of the system by averaging the flow map along $t \mapsto \hat\mu(t)$. By direct computation, the average system has states (σ, ξ_1, ξ_2), flow set given by $C_\sigma \times \mathbb{R}^n \times \mathbb{R}^n$, flow map given by[1]:

$$\begin{pmatrix} \dot\sigma \\ \dot\xi_1 \\ \dot\xi_2 \end{pmatrix} \in \begin{pmatrix} F_\sigma(\sigma, \xi_1, \xi_2) \\ \frac{1}{\varepsilon_1}(-\xi_1 + \nabla\phi(x) + O(a)) \\ \frac{1}{\varepsilon_1}\big(-\nabla^2\phi(x)\xi_2 + \nabla\phi(x) + O(a)\big) \end{pmatrix}, \tag{14}$$

jump set given by $D_\sigma \times \mathbb{R}^n \times \mathbb{R}^n$, and jump map given by

$$\big(\sigma^+, \xi_1^+, \xi_2^+\big) \in G_\sigma(\sigma) \times \{\xi_1\} \times \{\xi_2\}. \tag{15}$$

[1]We use the notation $f(x) = O(g(x))$ to denote that there exists $c_1 > 0$ and $c_2 > 0$ such that $|f(x)| \le c_1 |g(x)|$ for all $|x| \le c_2$.

In turn, this HDS is also in standard form for the application of singular perturbation theory, with the states (ξ_1, ξ_2) having fast dynamics. To analyze this system, we first set $O(a) = 0$, and we compute the reduced hybrid dynamics, which are obtained by substituting ξ_1 and ξ_2 in the right-hand side of $\dot\sigma$ by their respective equilibrium points $\xi_1^* := \nabla\phi(x)$ and $\xi_2^* = (\nabla^2\phi(x))^{-1}\nabla\phi(x)$, which are exponentially stable under Assumption 1, uniformly in x. The resulting reduced dynamics are given by

$$\sigma \in C_\sigma, \quad \dot\sigma \in F_\sigma(\sigma, \nabla\phi, (\nabla^2\phi)^{-1}\nabla\phi), \tag{16a}$$
$$\sigma \in D_\sigma, \quad \sigma^+ \in G_\sigma(\sigma), \tag{16b}$$

where we recall that $\sigma := (\vartheta, \psi)$, with $\psi = x$ for GDES and NLES, and $\psi = (x, y, z)$ for HAES.

C. Switching Optimization Dynamics

We now proceed to characterize the stability properties of system (16). Since the compact set $\mathcal{T}$ is strong forward pre-invariant under (5), it suffices to study the convergence properties of ψ.

In the following lemmas, we assume that Assumption 1 holds.

Lemma 2: Consider the HDS (16) with F_σ as in (9) and $G_\sigma = x$. Then, the set $\mathcal{A} = \mathcal{T} \times \{u^*\}$ is UGAS whenever $\eta_1 > 0$ and $0 < \eta_2 < 1/(1+\gamma)$, where γ is as in Theorem 1-(a).

Proof: Consider the quadratic Lyapunov function $V(x) = \frac{1}{2}|x - u^*|^2$. When $Q = \mathbb{I}_n$, the time derivative of V satisfies $\dot V(x) = -k(x-u^*)^\top Q \nabla\phi(x) \le -\kappa k |x - u^*|^2$, hence, $\dot V(x) \le -\lambda_s V(x)$, where $\lambda_s = 2\kappa k$. Similarly, when $Q \in \mathcal{Q}_u$ we obtain $\dot V(x) \le k|x-u^*||Q||\nabla\phi(x)| \le qk|x-u^*||\nabla\phi(x)| \le q\ell k|x-u^*|^2$, hence, $\dot V(x) \le \lambda_u V(x)$, where $\lambda_u = 2q\ell k$. Thus, $\frac{\lambda_s}{\lambda_s+\lambda_u} = \frac{1}{1+q\frac{\ell}{\kappa}}$. The result follows by Lemma 6 in the Appendix with $\omega = 1$ and $D = \emptyset$. ∎

Lemma 3: Consider the HDS (16) with F_σ as in (10) and $G_\sigma = x$. Then, the set $\mathcal{A} = \mathcal{T} \times \{u^*\}$ is UGAS whenever $\eta_1 > 0$ and $0 < \eta_2 < 1/(1+\gamma)$, where γ is as in Theorem 1-(a).

Proof: Consider the Lyapunov function $V(x) = \frac{1}{2}|\nabla\phi(x)|^2$. By Assumption 1, it satisfies $\frac{\kappa^2}{2}|x-u^*|^2 \le \frac{1}{2}|\nabla\phi(x)|^2 \le \frac{\ell^2}{2}|x-u^*|^2$. When $Q = \mathbb{I}_n$, we have:

$$\dot V(x) = -k\nabla\phi(x)^\top \nabla^2\phi(x)[\nabla^2\phi(x)]^{-1}\nabla\phi(x) = -\lambda_s V(x),$$

where $\lambda_s = 2k$. Similarly, when $Q \in \mathcal{Q}_u$, we obtain

$$\begin{aligned} \dot V(\hat u) &\le k|\nabla\phi(x)||\nabla^2\phi(x)||Q||[\nabla^2\phi(x)]^{-1}||\nabla\phi(x)|, \\ &\le 2qk\frac{\ell}{\kappa}V(x) = \lambda_u V(x), \end{aligned}$$

with $\lambda_u = 2qk\ell/\kappa$. Thus, $\frac{\lambda_s}{\lambda_s+\lambda_u} = \frac{1}{1+q\frac{\ell}{\kappa}}$, and the result follows by Lemma 6 with $\omega = 1$ and $D = \emptyset$. ∎

Lemma 4: Consider the HDS (16) with F_σ as in (11b) and G_σ as in (11d). The set $\mathcal{A} := \mathcal{T} \times \{u^*\} \times \{u^*\} \times [\delta, \Delta]$ is UGAS whenever $\eta_1 > 0$ and $0 < \eta_2 < 1/(1+\gamma)$, where γ is as in Theorem 1-(b).

Proof: Consider the Lyapunov function presented in [6]: $V(\psi) = \frac{1}{4}|y-x|^2 + \frac{1}{4}|y-u^*|^2 + kz^2(\phi(x) - \phi(u^*))$. It was shown in [6] that under Assumption 1 this function satisfies $\underline{c}|\psi|_{\mathcal{A}}^2 \le V(\psi) \le \bar c|\psi|_{\mathcal{A}}^2$, with $\underline{c} := 0.25\min\{1, 2k\delta^2\kappa\}$, and

$\bar{c} := 0.75\max\{1, \frac{2}{3}k\Delta^2\ell\}$. When $Q = \mathbb{I}_n$, it was also shown in [6] that the following inequality holds

$$\dot{V}(\psi) \leq -\rho|\psi|_{\mathcal{A}}^2 \leq -\frac{\rho}{\bar{c}}V(\psi) = -\lambda_s V(\psi), \ \forall \psi \in C, \ (17)$$

with $\rho := 0.5\min\{\frac{1}{\Delta}, 0.25k\delta\kappa\}$ and

$$\lambda_s = \frac{2}{3\Delta}\frac{\min\{1, k\delta\Delta\kappa\}}{\max\left\{1, \frac{2}{3}k\Delta^2\ell\right\}}.$$

Similarly, when $Q \in \mathcal{Q}_u$ the derivative of V satisfies:

$$\dot{V}(\psi) \leq \frac{1}{\delta}|y-x|^2 + \frac{k\Delta}{2}\big[(4+q)|y-x||\nabla\phi(x)| \ldots + q|y-u^*||\nabla\phi(x)| + \ell|x-u^*|^2\big], \quad \forall \ \psi \in C.$$

Since $|y-x| \leq |y-u^*| + |u^*-x|$, it follows that

$$\dot{V}(\psi) \leq \frac{1}{\delta}|y-x|^2 + \frac{k\ell\Delta}{2}\max\{2(2+q), (5+q)\} \ldots \times (|y-u^*||x-u^*| + |x-u^*|^2),$$

for all $\psi \in C$, where we used the Lipschitz property of $\nabla\phi$. Define $\eta := \max\{\frac{1}{\delta}, \frac{k\ell\Delta}{2}\max\{2(2+q), (5+q)\}\}$. It then follows that $\dot{V}(\psi) \leq 1.5\eta(|y-u^*|^2 + |x-u^*|^2) = 1.5\eta|\psi|_{\mathcal{A}}^2$, for all $\psi \in C_u$. By using the quadratic lower bound of V we obtain $\dot{V}(\psi) \leq 1.5\frac{\eta}{\underline{c}}V(\psi) = \lambda_u V(\psi)$, for all $\psi \in C_u$, which implies that

$$\lambda_u = 1.5\frac{\eta}{\underline{c}} = \frac{4}{3\delta}\frac{\max\{2, k\ell\delta\Delta\max\{2(2+q), (5+q)\}\}}{\min\{1, 2k\kappa\delta^2\}}.$$

On the other hand, it was shown in [6] that during jumps triggered by ψ the Lyapunov function satisfies $V(\psi^+) \leq \exp(-\tilde{\gamma})V(\psi) = (1-\varrho)V(\psi)$, for all $\psi \in D_u$, where $\tilde{\gamma}$ is given by $\tilde{\gamma} := 1 - \frac{\delta^2}{\Delta^2} - \frac{1}{2k\kappa\Delta^2}$, which satisfies $\tilde{\gamma} \in (0,1)$ whenever $\Delta^2 - \delta^2 > \frac{1}{2k\kappa}$. The result follows by Lemma 6 in the Appendix with $\omega = 1$. ■

The previous Lemmas 2–4 studied the stability properties of system (16) when the switching occurs between an unstable mode and a stable mode. The following lemma now focuses on two stable modes. With some abuse of notation, we use $\{1\}$ and $\{-1\}$ to indicate the two stable modes.

Lemma 5: Consider the HDS (16) with F_σ given by $F_1(x) = -k\nabla\phi(x)$, $F_{-1}(x) = -k(\nabla^2\phi(x))^{-1}\nabla\phi(x)$, and $G_u(\psi) = x$. Then, the set $\mathcal{A} = \mathcal{T} \times \{u^*\}$ is UGAS whenever $\eta_2 = 0$ and $0 < \eta_1 < \eta_1^*$, where η_1^* is as in Theorem 2.

Proof: We consider the Lyapunov function $V_1(x) = 0.5|x-u^*|^2$ studied in Lemma 2, and the Lyapunov function $V_{-1}(x) = 0.5|\nabla\phi(x)|^2$ studied in Lemma 3. It follows that $\dot{V}_h \leq -\lambda_s V_h(x)$, for all $h \in \{-1, 1\}$, with $\lambda_s = 2k\min\{1, \kappa\}$. Moreover, $V_g(x) \leq \omega V_h(x)$, for all $(g,h) \in \{-1,1\}^2$, with $\omega = \max\{1, \ell^2\}/\min\{1, \kappa^2\}$. The result follows by Lemma 6 in the Appendix with $\eta_2 = 0$, $D = \emptyset$.

Since Lemmas 2–5 have established UGAS for each of the switching reduced average dynamics (16), the stability results of Theorems 1-2 follow now by direct application of singular perturbation theory for hybrid ES [6, Th. 7].

V. Numerical Examples

Consider the cost function $\phi(u) = 2(u_1-5)^2 + 0.5(u_2-10)^2$, which satisfies Assumption 1 with $\kappa = 1$ and $\ell = 4$. We implement the GDES, the NLES and the HAES under persistent attacks modeled by the matrix $Q_u = -[1\ 0; 0\ 0]$, thus only affecting the first component of ξ_1. The left plot of Fig. 2 shows the resulting trajectories of the GDES with parameters $k = 0.1$, $\eta_1 = 0.376$, $\eta_2 = 0.25$, $\tau_1(0,0) = \tau_2(0,0) = 0$, $1/\varepsilon_1 = 0.9$, $a = 0.1$, $\varepsilon_2 = 1\times10^{-3}$, and frequencies satisfying $2\pi\theta_1 = 8.1$ and $2\pi\theta_4 = 4.2$. The inset shows the frequency of the attacks, where mode 1 here represents no attack and mode -1 represents an attack. It can be observed that, in spite of the persistent attacks, the ES algorithm preserves its stability properties. On the other hand, as shown in the right-plot in black, when $\eta_2 = 0.55$ (which does not satisfy the conditions of Theorem 1) the ES becomes unstable.

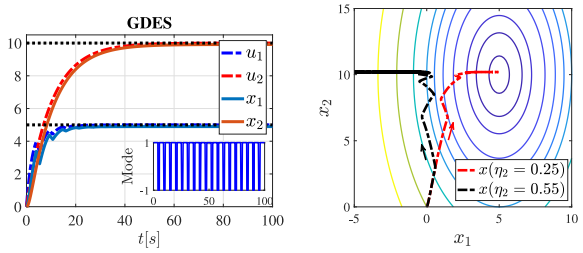

Fig. 2. GDES under persistent gradient jamming.

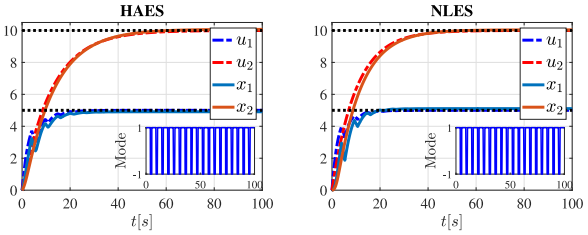

Fig. 3. HAES and NLES under persistent gradient jamming.

In Fig. 3 we show the trajectories generated by the HAES and the NLES. For the HAES, we used $k = 0.1$, $\eta_1 = 0.376$, $\eta_2 = 0.25$, and $\tau_1(0,0) = \tau_2(0,0) = 0$, $1/\varepsilon_1 = 0.9$, $a = 0.04$, $\varepsilon_2 = 1\times10^{-3}$. For the NLES we used $k = 0.1$, $\eta_1 = 0.376$, $\eta_2 = 0.25$, and $\tau_1(0,0) = \tau_2(0,0) = 0$, $1/\varepsilon_1 = 0.9$, $a = 0.14$, and $\varepsilon_2 = 1\times10^{-3}$.

VI. Conclusion

In this letter, we presented the first stability analysis of averaging-based ES dynamics under persistent deception attacks acting on the signals that provide estimations of the gradient. These attacks generalize different types of jamming signals studied in the literature, which include DoS attacks and deception attacks. For three different ES algorithms we showed that these types of attacks do not induce instability in the system provided their *persistency* satisfies particular bounds that depend on the unknown parameters of the cost functions. Our results were also illustrated via numerical examples.

Appendix

Consider a HDS with state $\upsilon = (\vartheta, (\zeta, s))$, where $\vartheta \in \mathbb{R}^3$ is defined in Lemma 1, $\zeta \in \mathbb{R}^p$, and $s \in \mathbb{R}$; continuous-time dynamics given by

$$\upsilon \in C_M \times C, \quad \dot{\vartheta} \in F_M(\vartheta), \ \dot{\zeta} = F_Q(\zeta, s), \ \dot{s} = \rho, \quad (18)$$

where $\rho > 0$, F_M:$\mathbb{R}^3 \rightrightarrows \mathbb{R}^3$, $C := \mathbb{R}^p \times [\underline{s}, \bar{s}]$ with $\bar{s} > \underline{s} > 0$; discrete-time dynamics given by

$$\upsilon \in D_1 \cup D_2, \qquad \upsilon^+ \in G_{1,2}(\upsilon), \quad (19)$$

where $D_1 := D_M \times C$, $D_2 := C_M \times D$, $D := \mathbb{R}^p \times \{\bar{s}\}$, D_M and C_M are defined in (5), and

$$G_{1,2}(\upsilon) := \begin{cases} G_1(\upsilon), & \text{if } \upsilon \in D_1 \\ G_2(\upsilon), & \text{if } \upsilon \in D_2 \\ G_1(\upsilon) \cup G_2(\upsilon), & \text{if } \upsilon \in D_1 \cap D_2, \end{cases} \tag{20}$$

with set-valued maps $G_1, G_2 : \mathbb{R}^{4+p} \rightrightarrows \mathbb{R}^{4+p}$ defined as $G_1(\upsilon) = G_M(\vartheta) \times \{\zeta\} \times \{s\}$, $G_2(\upsilon) = \{\vartheta\} \times \{G(\zeta)\} \times \{\underline{s}\}$, where $G : \mathbb{R}^p \to \mathbb{R}^p$, and G_M is defined in (5d).

The following lemma is a modest extension of [24, Proposition 2] and [4, Proposition 3] for switched systems with unstable modes where the main state ζ may also experience periodic jumps. In particular, when $D_2 = \emptyset$, the HDS (18)-(19) recovers the models of [24] and [4, Sec. 5].

Lemma 6: Suppose that G and F_Q are continuous functions for each $Q \in \mathcal{Q} := \mathcal{Q}_s \cup \mathcal{Q}_u \subset \mathbb{Z}_{\geq 1}$, where $(\mathcal{Q}_s, \mathcal{Q}_u)$ satisfy $\mathcal{Q}_s \cap \mathcal{Q}_u = \emptyset$, and $\mathcal{Q}$ is compact. Let $\psi := (\zeta, s)$ and $\mathcal{A} \subset C \cup D$ be compact. Suppose there exist continuously differentiable functions $V_Q : (C \cup D) \to \mathbb{R}_{\geq 0}$ such that:

1) There exists $c_1, c_2 > 0$ such that:
$$e^{c_1}|\psi|_{\mathcal{A}}^2 \leq V_Q(\psi) \leq e^{c_2}|\psi|_{\mathcal{A}}^2, \ \forall (\psi, Q) \in (C \cup D) \times \mathcal{Q}.$$
2) There exists $\lambda_s > 0$ such that
$$\langle \nabla V_{Q_s}(\psi), F_{Q_s}(\psi) \rangle \leq -\lambda_s V_{Q_s}(\psi), \ \forall (\psi, Q_s) \in C \times \mathcal{Q}_s.$$
3) There exists $\lambda_u > 0$ such that
$$\langle \nabla V_{Q_u}(\psi), F_{Q_u}(\psi) \rangle \leq \lambda_u V_{Q_u}(\psi), \ \forall (\psi, Q_u) \in C \times \mathcal{Q}_u.$$
4) There exists $\omega \geq 1$ such that
$$V_P(\psi) \leq \omega V_Q(\psi), \ \forall (\psi, P, Q) \in (C \cup D) \times \mathcal{Q} \times \mathcal{Q}.$$
5) There exists $\varrho \in (0, 1) > 0$ such that
$$V_Q(\psi^+) - V_Q(\psi) \leq -\varrho V_Q(\psi), \ \forall (\psi, Q) \in D \times \mathcal{Q}.$$

Then, if $\lambda_s > \eta_1 \log(\omega) + \eta_2(\lambda_s + \lambda_u)$, the set $\mathcal{T} \times \mathcal{A}$ is UGAS for the HDS (18)-(19).

Proof: Define $\tau := \log(\omega)\tau_1 + (\lambda_s + \lambda_u)\tau_2$, and $V(\upsilon) = V_Q(\psi)e^{\tau}$. Using (5b), it follows that during flows we have $\dot{\tau} \in \log(\omega)[0, \eta_1] + (\lambda_s + \lambda_u)([0, \eta_2] - \mathcal{I}_{\mathcal{Q}_u}(Q)) = [0, \gamma] - (\lambda_s + \lambda_u)\mathcal{I}_{\mathcal{Q}_u}(Q)$, where $\gamma := \eta_2(\lambda_s + \lambda_u) + \eta_1 \log(\omega)$. It follows that if $Q \in \mathcal{Q}_s$ and $\psi \in C$, then

$$\begin{aligned} \dot{V}(\upsilon) &\leq V_Q(\psi)e^{\tau}\dot{\tau} - \lambda_s V_Q(\psi)e^{\tau} \\ &\leq -(\lambda_s - \gamma)V_Q(\psi)e^{\tau} = -\lambda V(\upsilon), \end{aligned} \tag{21}$$

where $\lambda := \lambda_s - \gamma > 0$ whenever $\lambda_s > \eta_2(\lambda_s + \lambda_u) + \eta_1 \log(\omega)$. Similarly, if $Q \in \mathcal{Q}_u$ and $\psi \in C$, then

$$\begin{aligned} \dot{V}(\upsilon) &\leq V_Q(\psi)e^{\tau}\dot{\tau} + \lambda_u V_Q(\psi)e^{\tau} \\ &\leq V_Q(\psi)e^{\tau}(\gamma - (\lambda_s + \lambda_u)) + \lambda_u V_Q(\psi)e^{\tau} \leq -\lambda V(\upsilon). \end{aligned}$$

During jumps of the form $\upsilon^+ \in G_2(\upsilon)$, we have that

$$V(\upsilon^+) = V_Q(\psi^+)e^{\tau} \leq (1 - \varrho)V_Q(\psi)e^{\tau} = (1 - \varrho)V(\upsilon).$$

for all $\upsilon \in D_2$. Similarly, since $\tau^+ = \tau - \log(\omega)$, during jumps of the form $\upsilon^+ \in G_1(\upsilon)$, we have:

$$\begin{aligned} V(\upsilon^+) = V_{Q^+}(\psi)e^{\tau^+} &\leq \max_{Q^+ \in \mathcal{Q}} V_{Q^+}(\psi)e^{\tau}e^{-\log(\omega)} \\ &\leq \omega V_Q(\psi)e^{\tau}e^{-\log(\omega)} = V(\upsilon). \end{aligned} \tag{22}$$

for all $\upsilon \in D_1$. Combining inequalities (21)-(22), the result follows by [20, Proposition 3.27]. ■

REFERENCES

[1] K. B. Ariyur and M. Krstić, *Real-Time Optimization by Extremum-Seeking Control*. Hoboken, NJ, USA: Wiley, 2003.

[2] D. Nešić, Y. Tan, W. H. Moase, and C. Manzie, "A unifying approach to extremum seeking: Adaptive schemes based on estimation of derivatives," in *Proc. 49th IEEE Conf. Decis. Control*, 2010, pp. 4625–4630.

[3] C. Labar, E. Garone, M. Kinnaert, and C. Ebenbauer, "Newton-based extremum seeking: A second-order lie bracket approximation approach," *Automatica*, vol. 105, pp. 356–367, Jul. 2019.

[4] 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, Feb. 2017.

[5] A. Ghaffari, M. Krstić, and D. Nešić, "Multivariable Newton-based extremum seeking," *Automatica*, vol. 48, pp. 1759–1767, Aug. 2012.

[6] J. I. Poveda and N. Li, "Robust hybrid zero-order optimization algorithms with acceleration via averaging in time," *Automatica*, vol. 123, Jan. 2021, Art. no. 109361.

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

[8] Y.-C. Liu, G. Bianchin, and F. Pasqualetti, "Secure trajectory planning against undetectable spoofing attacks," *Automatica*, vol. 112, Feb. 2020, Art. no. 108655.

[9] X.-F. Wang, A. R. Teel, K.-Z. Liu, and X.-M. Sun, "Stability analysis of distributed convex optimization under persistent attacks: A hybrid systems approach," *Automatica*, vol. 111, Jan. 2020, Art. no. 108607.

[10] B. Turan, C. A. Uribe, H.-T. Wai, and M. Alizadeh, "On robustness of the normalized subgradient method with randomly corrupted subgradients," Sep. 2020. [Online]. Available: arXiv:2009.13725.

[11] J. I. Poveda and M. Krstić, "Fixed-time gradient-based extremum seeking," in *Proc. Amer. Control Conf.*, 2020, pp. 2838–2843.

[12] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Networked control under random and malicious packet losses," *IEEE Trans. Autom. Control*, vol. 62, no. 5, pp. 2434–2449, May 2017.

[13] H. S. Foroush and S. Martinez, "On event-triggered control of linear systems under periodic denial-of-service jamming attacks," in *Proc. IEEE Conf. Decis. Control*, 2012, pp. 2551–2556.

[14] D. Senejohnny, P. Tesi, and C. De Persis, "A jamming-resilient algorithm for self-triggered network coordination," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 981–990, Sep. 2018.

[15] N. Forti, G. Battistelli, L. Chisci, and B. Sinopoli, "Secure state estimation of cyber-physical systems under switching attacks," *IFAC PapersOnLine*, vol. 50, no. 1, pp. 4979–4986, 2017.

[16] S. Z. Yong, M. Zhu, and E. Frazzoli, "Resilient state estimation against switching attacks on stochastic cyber-physical systems," in *Proc. IEEE Conf. Decis. Control*, Dec. 2015, pp. 5162–5169.

[17] S. Sundaram and B. Gharesifard, "Distributed optimization under adversarial nodes," *IEEE Trans. Autom. Control*, vol. 64, no. 3, pp. 1063–1076, Mar. 2019.

[18] L. Su and N. H. Vaidya, "Byzantine-resilient multi-agent optimization," *IEEE Trans. Autom. Control*, early access, Jul. 9, 2020, doi: 10.1109/TAC.2020.3008139.

[19] Y. Chen, L. Su, and J. Xu, "Distributed statistical machine learning in adversarial settings: Byzantine gradient descent," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 1, no. 2, pp. 1–25, Dec. 2017.

[20] R. Goebel, R. G. Sanfelice, and A. R. Teel, *Hybrid Dynamical Systems*. Princeton, NJ, USA: Princeton Univ. Press, 2012.

[21] Y. Tan, D. Nešić, and I. M. Mareels, "On non-local stability properties of extremum seeking control," *Automatica*, vol. 42, no. 6, pp. 889–903, 2006.

[22] S. Boyd and L. Vandenberghe, *Convex Optimization*. Boston, MA, USA: Cambridge, Univ. Press, 2004.

[23] W. Wang, A. Teel, and D. Nešić, "Analysis for a class of singularly perturbed hybrid systems via averaging," *Automatica*, vol. 48, no. 6, pp. 1057–1068, 2012.

[24] G. Yang and D. Liberzon, "Input-to-state stability for switched systems with unstable subsystems: A hybrid Lyapunov construction," in *Proc. 53rd IEEE Conf. Decis. Control*, 2014, pp. 6240–6245.