Concurrent Receding Horizon Control and Estimation against Stealthy Attacks

Filippos Fotiadis, *Student Member, IEEE,* and Kyriakos. G. Vamvoudakis, *Senior Member, IEEE*

***Abstract*—In this work, we consider a game-theoretic framework for cyber-physical systems, where a defender develops a mitigation strategy against an intelligent attacker who exploits the system's uncertainty to remain undetected. The goal of the defender is to optimize a performance cost constructed specifically to account for robustness against stealthy attacks, so that the system is regulated. Conversely, the goal of the attacker is to disrupt the system's performance by leveraging its significant information advantage against the defender. Both players implement their policies in a moving horizon fashion, according to the principles of receding horizon control. However, because the defender has no access to the full state of the system, it concurrently employs receding horizon estimation to overcome this limitation. A rigorous theoretical analysis shows that such a concurrent policy can guarantee closed-loop boundedness, despite the stealthy attacks and the information disadvantage. Simulations verify and clarify these findings.**

***Index Terms*—Cyber-physical systems, game-theory, actuation attacks.**

I. Introduction

Cyber-physical systems (CPS) are sophisticated systems, which comprise interacting digital, analog and human components engineered for function through integrated physics and logic. Because of their complexity, CPS are extraordinarily exposed to adversaries that can potentially cause failure or malfunction while remaining undetected. For instance, CPS are vulnerable to actuation attacks [1], i.e. false-data injection and spoofing attacks, which can introduce perturbations in the CPS's control input through interference with its software, hardware or communication channels. As a result, there has been an increasing demand for secure methods that can guarantee the integrity and normal operation of CPS under stealthy attacks [2].

Game-theoretic tools [3] have been used to develop resilience towards worst-case attacks in CPS. In particular, it is often for two-player competition to arise between the operator of a CPS and a potential intruder, which can be modeled as a game with a common utility. In this case, game theory can yield resilient decision-making mechanisms, which can guarantee an upper or lower bound on the utility for each player. The corresponding decisions can also be implemented in a moving horizon fashion to create feedback policies, according to the principles of receding horizon control (RHC).

Related Work: RHC is a computationally efficient control method that can stabilize a system using predictions of future costs over a moving time horizon [4]. Especially relevant to the present work is the so-called min-max RHC [5]–[9], which yields game-theoretic policies that account for the worst case scenario regarding a potential disturbance or uncertainty. Owing to this property, min-max RHC can be effectively used on the field of CPS security, and guarantee CPS stability, optimality, and robustness [10]–[12].

This work uses a heavily modified version of min-max RHC, which significantly differs from results in the literature. In particular, a constrained version of game-theoretic RHC is employed, which generates robustness targeted specifically against stealthy attacks – not against a general class of adversarial inputs. As a result, the proposed RHC contains coupled, time-varying state-control constraints that account for undetectability, hence classical min-max RHC cannot be directly employed without significant modifications and a novel closed-loop analysis. Additionally, we consider that only a partial state can be measured by the CPS operator – even though the attacker can measure the full state – and still prove boundedness of the closed loop using concurrent moving horizon estimation and RHC. Such a concurrent combination was studied in [13], [14], but only in discrete-time, without any attacks and without coupled state-control constraints.

Regarding the attackers that can affect a CPS, the distinction of them between stealthy and non-stealthy ones is crucial. For the latter case, detection mechanisms can be employed as a tool to deal with malicious adversaries [15]. For example, for continuous-time systems and in the absence of uncertainties, the authors in [16] provided conditions for the detection and identification of various types of cyber-physical attacks. Additionally, for sampled-data continuous-time systems affected by deterministic disturbances, a method to detect adversarial inputs was developed in [17]. Nevertheless, in the case that the attacks remain stealthy and hide under the uncertainties of large-scale CPS, one must develop appropriate mitigation strategies.

Towards dealing with undetectable adversaries, various types of stealthy attacks for discrete-time systems were characterized in [18]. In a similar fashion, the authors in [19] investigated the response of a state estimation problem given different kinds of stealthy attacks. They derived conditions under which the attackers can remain undetected, though no robustness guarantees were provided. Similar to our work, the authors in [20] solved a game to find the best-response policies for the defender towards a stealthy attacker who manipulates the system's output and actuating data; however, the derived policies were applied only in a non-receding time horizon. A similar continuous-time optimization was proposed in [21] for secure trajectory planning of robotic systems, while the authors in [22] considered a game between an attacker that attempts to maximize damage on a CPS and a defender who wants to minimize it.

Unlike the aforementioned studies, this is the first work wherein a defender is tasked with controlling an uncertain system against stealthy attacks using concurrent RHC and estimation. By targeting exclusively stealthy attacks through the construction and the incorporation of appropriate constraints in the defender's receding horizon optimization, the conservatism of considering only worst-case attacks is reduced. In addition, no knowledge of the full state of the system is needed by the defender to guarantee boundedness of the closed-loop. From the perspective of the attacker, the corresponding optimal policies are also studied using Pontryagin's principle. A preliminary subset of this study has appeared in [23], where a game between a defender and a stealthy attacker was also considered, but the behavior of the corresponding closed-loop was not analyzed or studied. On the other hand, in the present work we prove that the proposed defending policy is secure, and can keep the closed-loop bounded despite the stealthy attacks and the information disadvantage.

Notation: Given $z \in \mathbb{R}^q$, $R \in \mathbb{R}^{q\times q}$, $\|z\|$ and $\|z\|_\infty$ are the l_2 and l_∞ norm of z, and $\|z\|_R = \frac{1}{2} z^{\mathrm{T}} R z$. If $\|z\|_\infty \leqslant \bar{z}$ and $\bar{z} > 0$, then per [24]: $\|z\|_{R,\bar{z}} = \int_0^z \left(\tanh^{-1}\left(\frac{w}{\bar{z}}\right)\right)^{\mathrm{T}} R \mathrm{d}w$. $I_q \in \mathbb{R}^{q\times q}$ is the identity matrix, and $\mathbb{1}_q \in \mathbb{R}^q$ is the vector of ones. The operators $\lambda_{\min}(\cdot)/\lambda_{\max}(\cdot)$ yield the minimum/maximum eigenvalue of a symmetric matrix.

F. Fotiadis and K. G. Vamvoudakis are with the School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, GA, 30332, USA

This work was supported by ARO under grant No. W911NF-19−1−0270, by ONR Minerva under grant No. N00014 − 18 − 1 − 2160, by NSF under grant Nos. CAREER CPS-1851588, S&AS 1849198, and SATC-1801611, and by the Onassis Foundation - Scholarship ID: F ZQ 064 − 1/2020 − 2021.

II. Problem Formulation

Consider the following system, $\forall t \geqslant t_0 \geqslant 0$:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B\Big(u(t) + d(t) + a(t)\Big), \\ y(t) &= Cx(t),\ x(t_0) = x_0, \end{aligned} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state vector, $y(t) \in \mathbb{R}^p$ is the system's output, $u(t) \in \mathbb{R}^m$ is the defender's input, $a(t) \in \mathbb{R}^m$ is the attacker's input, $d(t) \in \mathbb{R}^m$ is an exogenous disturbance, $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $C \in \mathbb{R}^{p\times n}$ are the plant, input, and output matrices, respectively.

We will consider a framework where the defender and the attacker choose their policies based on a RHC setting. In particular, at every time instant $t_j,\ j \in \mathbb{N}$, the defender and the attacker each compute a policy that optimizes a specific performance cost over a prediction horizon $[t_j,\ t_j + T]$, $T > 0$. The defender and the attacker then implement their policies on system (1), $\forall t \in [t_j,\ t_{j+1}]$, where $\delta \triangleq t_{j+1} - t_j \leqslant T$ a strictly positive control horizon. Even though the attacker chooses its control input by optimizing a performance cost at each time instant $t_j,\ j \in \mathbb{N}$, it still wants to produce an output that is compatible with the model of the uncertainty generated by the disturbance. When such a compatibility is achieved for the output, we will call the attack control input, as well as the corresponding attacker, as *undetectable*. The following assumptions are now needed.

Assumption 1. The disturbance d is bounded by norm, so that $\|d(t)\|_\infty < \Delta,\ \forall t \geqslant t_0$. The constant Δ is strictly positive and known by both the attacker and the defender. □

Assumption 2. At each optimization instant $t_j,\ j \in \mathbb{N}$:

- The attacker knows the initial condition $x(t_j) \triangleq x_j$ and the future disturbance $d(t),\ \forall t \in [t_j,\ t_j + T]$.
- The defender knows only the output history $y(t),\ \forall t \leqslant t_j$. □

Assumption 3. The pair (A, C) is observable. □

Remark 1. Assumption 1 characterizes the model of the uncertainty under which the attacker wants to hide. A larger disturbance bound shall allow it to employ relatively high control effort, while a smaller one will restrict its flexibility. Assumption 2 denotes that there is an information asymmetry between the attacker and the defender, which gives an advantage to the former. Moreover, no assumption was imposed on whether each side knows the decision-making mechanism of the other side. Finally, Assumption 3 is an observability requirement that is common in output-based frameworks [13]. □

Define at each time instant $t_j,\ j \in \mathbb{N}$, the cost functional

$$\begin{aligned} J^d(t_j) = \int_{t_j}^{t_j+T} \Big(&\Big\|x^d(\tau)\Big\|_{Q^d} + \|u(\tau)\|_{R^d} \\ &- \Big\|a^d(\tau)\Big\|_{K^d}\Big)\mathrm{d}\tau + \Big\|x^d(t_j+T)\Big\|_{F^d}, \end{aligned}$$

where x^d is a trajectory of (1) given inputs $(u, d, a) \equiv (u, d^d, a^d)$, and $Q^d,\ R^d,\ K^d,\ F^d \succ 0$, are weighting matrices of appropriate dimensions. Then, the defender's objective at each instant $t_j,\ j \in \mathbb{N}$, is described by the following optimization problem:

$$\begin{aligned} &\text{minimize} && J^d(t_j), \\ &\text{subject to:} && \text{Dynamics (1) and Assumptions } 1-3, \\ &\text{considering:} && \text{Stealthy attack } a^d \text{ and disturbance} \\ & && d^d \text{ maximizing } J^d(t_j). \end{aligned} \tag{2}$$

Similarly, we define at each instant $t_j,\ j \in \mathbb{N}$, the cost functional

$$\begin{aligned} J^a(t_j) = \int_{t_j}^{t_j+T} \Big(&\|x^a(\tau)\|_{Q^a} + \|u^a(\tau)\|_{R^a} \\ &- \|a(\tau)\|_{K^a}\Big)\mathrm{d}\tau + \|x^a(t_j+T)\|_{F^a}, \end{aligned}$$

where x^a is a trajectory of (1) generated with inputs $(u, d, a) \equiv (u^a, d, a)$, and $Q^a,\ R^a,\ K^a,\ F^a \succ 0$ are weighting matrices of appropriate dimensions. Then, the attacker's objective at $t = t_j,\ j \in \mathbb{N}$, can be described by the following optimization:

$$\begin{aligned} &\text{maximize} && J^a(t_j), \\ &\text{subject to:} && \text{Dynamics (1) and Assumptions } 1-3, \\ &\text{so that:} && \text{Undetectability is achieved,} \\ &\text{considering:} && \text{Defense } u^a \text{ minimizing } J^a(t_j). \end{aligned} \tag{3}$$

Notice that the expressions of J^d and J^a are chosen to be linear quadratic, because such costs accurately capture the potential goals of the defender and the attacker. Particularly, in the common scenario where the defender wants to regulate the system to the origin, it is of interest to minimize J^d so that the state x is driven to zero optimally. Accordingly, to optimally disrupt the defender's objective and lead the system in undesired regions far from the origin, it is of interest for the attacker to maximize the cost function J^a. Due to these properties, linear-quadratic costs are commonly used in the context of CPS and security [12], [20].

Remark 2. The attacker's input is included in J^a because the attacker wants to maximize the damage on the plant, while at the same time avoiding creating disruption that will attract attention. That is, the stealthy attacker wants to avoid creating large attacks that will expose it through physical means. Moreover, the addition of the attacker's input in J^d and J^a is important in order to guarantee that problems (2)-(3) are well-defined and feasible, and that they will not have singular solutions stemming from the linearity of (1) [25]. □

Remark 3. Owing to Assumption 2, which defines (2), the defender has to exploit the past output data that are available to estimate the initial condition $x_j,\ \forall j \in \mathbb{N}$. However, since it does not know the past disturbances and attack signals that affected those data, it has to consider the worst-case (maximizing) ones and find a worst-case estimate of x_j to guarantee closed-loop boundedness and robustness, as it will be shown in Section IV. The same holds for the future disturbance and attack; since the defender does not know them, it assumes that they will maximize J^d, for the sake of robustness. □

Remark 4. Besides designing defending policies, methods for understanding the behavior of attackers are also crucial in enhancing CPS security. In that respect, providing an efficient defending policy by solving (2) does not suffice; the solution to the attacker's problem (3) is also important to derive, as it provides the basis for profiling and modeling attacking behavior. Towards this end, a brief solution to (3) will also be provided in the upcoming sections, which can enable the defending side to better handle realistic attacks should the information between the two sides be symmetric. □

III. Output Data and Stealthiness

In this section, we present some results needed to solve (2)-(3).

A. Time Reversal

To estimate $x_j,\ j \in \mathbb{N}$, the defender has to utilize output data from a past horizon while simultaneously guaranteeing robustness for the receding horizon policy that minimizes J^d over a future horizon. However, in our continuous-time framework, the Hamiltonian-based conditions for optimality consist of boundary value problems that are defined over only one horizon, so we cannot consider both a past and a future horizon. Therefore, we redefine the past horizon over which the output data are defined, so that it coincides with the future horizon where J^d is optimized, as in the following Lemma.

Lemma 1. *Consider, $\forall t \in [t_j, t_j + T]$, $j \in \mathbb{N}$, a trajectory $x_p : [t_j, t_j + T] \to \mathbb{R}^n$ evolving according to the dynamics*

$$\dot{x_p}(t) = -Ax_p(t) - B\big(u(2t_j - t) + d(2t_j - t) + a(2t_j - t)\big). \tag{4}$$

Let Assumption 3 hold. Then, the equation

$$Cx_p(t) = y(2t_j - t), \forall t \in [t_j, t_j + T], \tag{5}$$

holds if and only if $x_p(t_j) = x_j$.

Proof. Integrating (1) backwards on $t \in [t_j - T, t_j]$, $j \in \mathbb{N}$, one has

$$y(t) = Ce^{A(t-t_j)}x_j + C\int_{t_j}^{t} e^{A(t-\tau)}B \cdot (u(\tau) + d(\tau) + a(\tau))\,\mathrm{d}\tau,\ \forall t \in [t_j - T, t_j]. \tag{6}$$

Setting $t' = 2t_j - t$ in (6) and changing the integration variable yields

$$y(2t_j - t') = Ce^{-A(t'-t_j)}x_j - C\int_{t_j}^{t'} e^{-A(t'-\tau)}B \cdot (u(2t_j - \tau) + a(2t_j - \tau) + d(2t_j - \tau))\,\mathrm{d}\tau. \tag{7}$$

Integrating (4) over $[t_j, t_j + T]$, we derive, $\forall t' \in [t_j, t_j + T]$, that

$$Cx_p(t') = Ce^{-A(t'-t_j)}x_p(t_j) - C\int_{t_j}^{t'} e^{-A(t'-\tau)}B \cdot (u(2t_j - \tau) + a(2t_j - \tau) + d(2t_j - \tau))\,\mathrm{d}\tau. \tag{8}$$

Deducting (8) from (7), for all $t' \in [t_j, t_j + T]$ we obtain

$$y(2t_j - t') - Cx_p(t') = Ce^{-A(t'-t_j)}\left(x_j - x_p(t_j)\right).$$

Using Assumption 3, we conclude that $Cx_p(t') = y(2t_j - t')$, $\forall t' \in [t_j, t_j + T]$, if and only if $x_p(t_j) = x_j$. ∎

Remark 5. The differential equation (4) along with the constraint (5) provided by Lemma 1 are defined over the future horizon $[t_j, t_j + T]$, $j \in \mathbb{N}$, yet they still allow one to estimate the initial condition x_j using past output data. It should be reminded, however, that the past disturbance and stealthy attack, which affect (4), are not known by the defender and thus the true x_j cannot be computed. Instead, to guarantee robustness, the objective is to find the past disturbance and attack that yield a worst-case estimate of x_j while simultaneously optimizing J^d, as noted in (2) and Remark 3. □

B. Characterization of Stealthy Attacks

Consider the attack-free model of (1)

$$\begin{aligned} \dot{x}_h(t) &= Ax_h(t) + B\left(u(t) + d_h(t)\right), \\ y_h(t) &= Cx_h(t),\ x_h(t_0) = x_0,\ t \geqslant t_0, \end{aligned} \tag{9}$$

where $x_h(t) \in \mathbb{R}^n$, $y_h(t) \in \mathbb{R}^p$ are the states and the output if there is no attack, and $d_h(t) \in \mathbb{R}^m$ is any signal satisfying the bound from Assumption 1, i.e., $\|d_h(t)\|_\infty < \Delta$, $\forall t \geqslant t_0$. Many realizations of the attack-free model (9) may exist, based on the choice of d_h. To remain stealthy over a horizon $t \in [t_j,\ t_j + T]$, $j \in \mathbb{N}$, the attacker needs to imitate the behavior of one of these realizations, and find a signal d_h satisfying $\|d_h(t)\|_\infty < \Delta$, $\forall t \in [t_j, t_j + T]$, for which

$$y(t) = y_h(t),\ \forall t \in [t_j, t_j + T]. \tag{10}$$

We will denote this class of signals as *admissible*. Although the attacker does not know the actual input that the defender will employ, it is still able to guarantee that (10) holds for some admissible signal d_h; hence, it can also guarantee undetectability as stated next.

Fact 1. *Let* $u^a, d_h^a : [t_j,\ t_j + T] \to \mathbb{R}^m$, $j \in \mathbb{N}$, *be functions of time, such that* $\|d_h^a(t)\|_\infty < \Delta$ *over the corresponding domain. Consider also the states* $x^a, x_h^a : [t_j, t_j + T] \to \mathbb{R}^n$ *evolving according to*

$$\begin{aligned} \dot{x}^a(t) &= Ax^a(t) + B(u^a(t) + d(t) + a(t)), \\ \dot{x}_h^a(t) &= Ax_h^a(t) + B\left(u^a(t) + d_h^a(t)\right), \\ x^a(t_j) &= x_h^a(t_j) = x_j,\ t \in [t_j, t_j + T]. \end{aligned} \tag{11}$$

Given that the function d_h^a *and the attack vector* a *are chosen so that*

$$C\left(x^a(t) - x_h^a(t)\right) = 0,\ \forall t \in [t_j,\ t_j + T], \tag{12}$$

then (10) *holds, with the attacker's admissible signal being* d_h^a. □

Remark 6. Based on Fact 1, as long as the attacker enforces (12) and $\|d_h^a(t)\|_\infty < \Delta$ to hold for all $\forall t \in [t_j,\ t_j + T]$, $j \in \mathbb{N}$, it can pick u^a and d_h^a in any way it desires, while still guaranteeing undetectability. As a result, no knowledge of the defender's control input u is needed to enforce these conditions. □

IV. Main Results

We will now solve the defender's and the attacker's problems (2)-(3). To this end, let us denote as $\mathcal{F}^j$ the set of piece-wise continuous mappings from $[t_j,\ t_j + T]$ to $\mathbb{R}^m$, and as $\mathcal{F}_d^j$ the set of piece-wise continuous mappings from $[t_j,\ t_j + T]$ to $\mathbb{R}^m$, such that if $z \in \mathcal{F}_d^j$ then $\|z(t)\|_\infty < \Delta$ for all $t \in [t_j,\ t_j + T]$.

A. Decision-Making for the Defender

Let $\mathcal{A} \triangleq \{a^d, a_p^d, d^d, d_p^d, d_h^d\} \in \mathcal{F}_{\mathcal{A}}^j \triangleq [\mathcal{F}^j]^2 \times [\mathcal{F}_d^j]^3$. Then, $\forall j \in \mathbb{N}$, a relaxed version of the optimization problem (2) for the defender can be written as the following zero-sum game:

$$\begin{aligned} \min_{u \in \mathcal{F}^j} \max_{\mathcal{A} \in \mathcal{F}_{\mathcal{A}}^j} \tilde{J}^d(u,\ \mathcal{A};\ t_j) = \int_{t_j}^{t_j+T} \Big(\left\|x^d(\tau)\right\|_{Q^d} \\ + \|u(\tau)\|_{R^d} - \left\|a^d(\tau)\right\|_{K^d} - \left\|a_p^d(\tau)\right\|_{K^d} - \left\|d^d(\tau)\right\|_{D^d,\Delta} \\ - \left\|d_p^d(\tau)\right\|_{D^d,\Delta} - \left\|d_h^d(\tau)\right\|_{D^d,\Delta} \Big) \mathrm{d}\tau + \left\|x^d(t_j + T)\right\|_{F^d}, \end{aligned} \tag{13}$$

subject to the following dynamics, $\forall t \in [t_j, t_j + T]$,

$$\dot{x}^d(t) = Ax^d(t) + B\left(u(t) + a^d(t) + d^d(t)\right), \tag{14}$$

$$\dot{x}_p^d(t) = -Ax_p^d(t) - B\left(u_p(t) + a_p^d(t) + d_p^d(t)\right), \tag{15}$$

$$\dot{x}_h^d(t) = Ax_h^d(t) + B\left(u(t) + d_h^d(t)\right) \tag{16}$$

$$\dot{\epsilon}_h^d(t) = \left\|Cx_h^d(t) - Cx^d(t)\right\|_{I_p}, \tag{17}$$

$$\dot{\epsilon}_p^d(t) = \left\|Cx_p^d(t) - y(2t_j - t)\right\|_{I_p}, \tag{18}$$

where $u_p(t) = u(2t_j - t)$, with boundary conditions

$$\epsilon_\sigma^d(t_j) = \epsilon_\sigma^d(t_j + T) = 0, \quad \sigma \in \{h, p\}, \tag{19}$$

$$x_h^d(t_j) = x_p^d(t_j) = x^d(t_j), \tag{20}$$

and $D^d \succ 0$. In the equations above, the dependence of all signals on t_j has been omitted to moderate notation. For example, the complete notation for $x^d(t)$ in (14) would be to denote it as $x^d(t; t_j)$; such an extended notation will be used only when needed to avoid confusion.

The constraints imposed by (17)-(19) build on the following fact.

Fact 2. *[26] Let* $a,\ b$ *be positive constants such that* $a < b$. *Consider a continuous function* $f : [a,\ b] \to \mathbb{R}^q$, *and a scalar trajectory* $\epsilon : [a,\ b] \to \mathbb{R}$ *evolving according to*

$$\dot{\epsilon}(t) = \|f(t)\|_{I_q}, \forall t \in [a,\ b],\ \epsilon(a) = 0. \tag{21}$$

If $\epsilon(b) = 0$, *then* $f(t) = 0$, $\forall t \in [a,\ b]$. □

The dynamics in optimization (13)-(20) may now be explained:

- The state x^d is a prediction of the future state x, assuming a worst-case future disturbance d^d and worst-case future attack a^d. The consideration of a worst-case future adversarial input is important to guarantee robustness, as the actual future adversarial input is not known by the defender [27].
- The state x_h^d is a prediction of the future state x in an attack-free scenario. Equations (17), (19) guarantee that the output of this predicted attack-free state is compatible with the output of the predicted attacked state x^d. In particular, due to Fact 2, equations (17), (19) enforce the undetectability condition of Fact 1. Hence,

only worst-case stealthy attacks are considered by the defender in its optimization problem, and not general types of attacks.

- The state x_p^d is a prediction of the past state $x_p(t) = x(2t_j - t)$, $\forall t \in [t_j,\ t_j + T]$. By considering worst-case past inputs d_p^d and a_p^d, equations (18)-(19) yield a worst-case estimate of the initial condition x_j owing to Lemma 1 and Fact 2. This worst-case initial state is then used as an initial condition for the worst-case predictions of the future states $x^d,\ x_h^d$.
- Since the predicted future, past, and attack-free trajectories x^d, x_p^d, x_h^d computed by the defender may not coincide with the real trajectories x, x_p, x_h, the superscript d is used to distinguish them. This superscript is also used for the predicted future and past attacks a^d, a_p^d, the predicted future and past disturbances d^d, d_p^d, and the disturbance d_h^d in the attack-free case.

Remark 7. The running cost in (13) includes a few more terms than the running cost in (2), which explains why (13)-(20) is only a relaxed version of (2). The purpose of these is to ensure that the solution to (13)-(20) is sufficiently smooth [25], while also ensuring that Assumption 1 is satisfied [24]. One could omit those extra terms, but this would lead to the solutions of (13)-(20) being bang-bang or singular [25], thus creating numerical difficulties. Therefore, from a computational perspective, it is preferable to obtain a sub-optimal solution by slightly modifying the cost in (2) into the cost (13). □

Remark 8. The suboptimality induced by the extra terms in (13) depends on their weighting matrices D^d and K^d. Since $D^d \preceq \lambda_{\max}(D^d) I_m$ and $K^d \preceq \lambda_{\max}(K^d) I_m$, then as these matrices' maximum eigenvalues approach zero, the extra terms in (13) vanish, and (13) becomes equivalent to (2). On the other hand, as these matrices' maximum eigenvalues are increased, the optimal value of (13) will monotonically decline and move further away from the value of (2). Consequently, the induced suboptimality in (13) is proportional to the maximum eigenvalues of these matrices. It should also be noted that the term $\left\|a^d(\tau)\right\|_{K^d}$ in the cost (13) is weighted with the same matrix K^d as the one used in (2) only for the sake of moderating notation; a different weighing matrix can be used otherwise. □

We now obtain the optimality conditions for problem (13)-(20).

Theorem 1. *Let* $\{u^\star, \mathcal{A}^\star\} \in \mathcal{F}^j \times \mathcal{F}_{\mathcal{A}}^j$ *be a Nash equilibrium to the defender's zero-sum game* (13) *subject to* (14)-(20)*, with,* $\mathcal{A}^\star \triangleq \{a^{d\star}, a_p^{d\star}, d^{d\star}, d_p^{d\star}, d_h^{d\star}\}$*. Then,* $\forall t \in [t_j,\ t_j + T],\ j \in \mathbb{N}$*:*

$$u^\star(t) = -{R^d}^{-1} B^{\mathrm{T}} (\lambda(t) + \lambda_h(t)), \tag{22}$$

$$a^{d\star}(t) = {K^d}^{-1} B^{\mathrm{T}} \lambda(t), \tag{23}$$

$$d^{d\star}(t) = \Delta \cdot \tanh({D^d}^{-1} B^{\mathrm{T}} \lambda(t)), \tag{24}$$

$$d_h^{d\star}(t) = \Delta \cdot \tanh({D^d}^{-1} B^{\mathrm{T}} \lambda_h(t)), \tag{25}$$

$$a_p^{d\star}(t) = -{K^d}^{-1} B^{\mathrm{T}} \lambda_p(t), \tag{26}$$

$$d_p^{d\star}(t) = -\Delta \cdot \tanh({D^d}^{-1} B^{\mathrm{T}} \lambda_p(t)), \tag{27}$$

where $\lambda, \lambda_h, \lambda_p$:$[t_j,\ t_j + T] \to \mathbb{R}^n$, ρ_p, ρ_h:$[t_j,\ t_j + T] \to \mathbb{R}$ *satisfy*

$$\dot\lambda(t) = -A^{\mathrm{T}} \lambda(t) - Q^d x^d(t) - C^{\mathrm{T}} C (x^d(t) - x_h^d(t)) \rho_h(t), \tag{28}$$

$$\dot\lambda_p(t) = A^{\mathrm{T}} \lambda_p(t) - C^{\mathrm{T}} (C x_p^d(t) - y(2t_j - t)) \rho_p(t), \tag{29}$$

$$\dot\lambda_h(t) = -A^{\mathrm{T}} \lambda_h(t) - C^{\mathrm{T}} C (x_h^d(t) - x^d(t)) \rho_h(t), \tag{30}$$

$$\dot\rho_p(t) = \dot\rho_h(t) = 0, \tag{31}$$

$$\lambda_p(t_j + T) = \lambda_h(t_j + T) = 0, \tag{32}$$

$$\lambda(t_j + T) = F^d x^d(t_j + T), \tag{33}$$

$$\lambda(t_j) + \lambda_h(t_j) + \lambda_p(t_j) = 0, \tag{34}$$

subject to (14)-(20) *for* $u = u^\star$ *and* $\mathcal{A} = \mathcal{A}^\star$.

Proof. Define the Hamiltonian of the problem (13)-(20) as:

$$\begin{aligned} H^d(\cdot) = &\left\|x^d(t)\right\|_{Q^d} + \|u(t)\|_{R^d} - \left\|a^d(t)\right\|_{K^d} - \left\|a_p^d(t)\right\|_{K^d} \\ &- \left\|d^d(t)\right\|_{D^d,\Delta} - \left\|d_p^d(t)\right\|_{D^d,\Delta} - \left\|d_h^d(t)\right\|_{D^d,\Delta} + \lambda^{\mathrm{T}}(t) \dot x^d(t) \\ &+ \lambda_p^{\mathrm{T}}(t) \dot x_p^d(t) + \lambda_h^{\mathrm{T}}(t) \dot x_h^d(t) + \rho_p(t) \dot\epsilon_p^d(t) + \rho_h(t) \dot\epsilon_h^d(t), \end{aligned}$$

where $\dot x^d,\ \dot x_p^d,\ \dot x_h^d,\ \dot\epsilon_p^d,\ \dot\epsilon_h^d$ are given by (14)-(18), and $\lambda,\ \lambda_p,\ \lambda_h,\ \rho_p,\ \rho_h$, denote the corresponding co-states. The conditions for optimality demand that $\dot\lambda(t) = -\partial H^d / \partial x^d(t)$, $\dot\lambda_h(t) = -\partial H^d / \partial x_h^d(t)$, $\dot\lambda_p(t) = -\partial H^d / \partial x_p^d(t)$, $\dot\rho_p(t) = -\partial H^d / \partial \epsilon_p^d(t)$, $\dot\rho_h(t) = -\partial H^d / \partial \epsilon_h^d(t)$, from which we obtain (28)-(31). In addition, the transversality necessary conditions yield (32)-(33). Next, notice that due to the boundary condition (20), the possible variations with respect to the initial conditions need to satisfy $\delta x^d(t_0) = \delta x_p^d(t_0) = \delta x_h^d(t_0)$. Therefore, following [25], it is not difficult to prove that (34) is also a necessary condition for optimality. Finally, by applying the stationarity conditions $\frac{\partial H^d(\cdot)}{\partial u} = 0$, $\frac{\partial H^d(\cdot)}{\partial \sigma} = 0$, $\forall \sigma \in \mathcal{A}$, the candidate optimal inputs $u^\star$, $\mathcal{A}^\star$ given by (22)-(27) are derived.

Subsequently, notice that the Hamiltonian is strictly convex with respect to u and strictly concave with respect to $d^d, d_p^d, d_h^d, a^d, a_p^d$. Therefore, the stationary points (22) and (23)-(27) are global minimizers and maximizers of the Hamiltonian, respectively. In addition, the Hamiltonian is separable w.r.t. u and $d^d, d_p^d, d_h^d, a^d, a_p^d$, hence the turn in which the Hamiltonian is minimized or maximized does not affect the corresponding optimal solution. Therefore, we deduce that

$$H^d(\cdot, u^\star, \mathcal{A}) \leqslant H^d(\cdot, u^\star, \mathcal{A}^\star) \leqslant H^d(\cdot, u, \mathcal{A}^\star) \tag{35}$$

Hence, the pair $\{u^\star, \mathcal{A}^\star\}$ satisfies all conditions characterizing a saddle-point solution to problem (13)-(20). As a result, the existence of a saddle point concludes, for all $\mathcal{A} \in \mathcal{F}_{\mathcal{A}}^j$ and $u \in \mathcal{F}^j$, that

$$\tilde J^d(u^\star,\ \mathcal{A};\ t_j) \leqslant \tilde J^d(u^\star,\ \mathcal{A}^\star;\ t_j) \leqslant \tilde J^d(u,\ \mathcal{A}^\star;\ t_j),$$

i.e., $\{u^\star, \mathcal{A}^\star\}$ is a Nash equilibrium for (13)-(20) [3]. ■

Control law: Having solved the optimization problem (13)-(20), the defender can choose its controller u by implementing (22) in a receding horizon fashion. In particular, if $u^\star(\cdot;\ t_j)$ is the signal (22) derived in the j-th instance of the optimization problem (13)-(20), $j \in \mathbb{N}$, then the defender's receding horizon controller is given by

$$u(t) = u^\star(t;\ t_j),\ \forall t \in [t_j,\ t_{j+1}],\ j \in \mathbb{N}. \tag{36}$$

B. Decision-Making for the Attacker

We now proceed to study the attacker's decision-making mechanism. To this end, $\forall j \in \mathbb{N}$, a relaxed version of the optimization problem (3) for the attacker can be written as the following game:

$$\begin{aligned} \min_{u^a \in \mathcal{F}^j} \max_{a \in \mathcal{F}^j,\ d_h^a \in \mathcal{F}_d^j} &\tilde J^a(u^a, a, d_h^a;\ t_j) \\ = &\int_{t_j}^{t_j + T} \Big(\|x^a(\tau)\|_{Q^a} + \|u^a(\tau)\|_{R^a} - \|a(\tau)\|_{K^a} \\ &- \|d_h^a(\tau)\|_{D^a,\Delta} \Big) \mathrm{d}\tau + \|x^a(t_j + T)\|_{F^a}, \end{aligned} \tag{37}$$

subject to the following dynamics, $\forall t \in [t_j, t_j + T]$,

$$\dot x^a(t) = A x^a(t) + B\big(u^a(t) + a(t) + d(t)\big), \tag{38}$$

$$\dot x_h^a(t) = A x_h^a(t) + B\left(u^a(t) + d_h^a(t)\right), \tag{39}$$

$$\dot\eta^a(t) = \|C x_h^a(t) - C x^a(t)\|_{I_p}, \tag{40}$$

with boundary conditions

$$x^a(t_j) = x_h^a(t_j) = x_j, \tag{41}$$

$$\eta^a(t_j) = \eta^a(t_j + T) = 0, \tag{42}$$

where $D^a \succ 0$, and $\left\{u^{a\star}, \{a^\star, d_h^{a\star}\}\right\}$ is the saddle point of $\tilde J^a(\cdot, \cdot;\ t_j)$. To distinguish between the different future and attack-

free trajectories x^a, x_h^a predicted by the attacker, the superscript a is used. This is also used for the admissible disturbance d_h^a in the attack-free scenario and for the considered defender's input u^a. Next, it is shown that the solution to (37)-(42) yields an undetectable attack.

Theorem 2. *Assume that the attacker chooses its policy a to be equal to $a^\star$ for all $t \in [t_j,\ t_j + T]$, $j \in \mathbb{N}$. Then, the attacker will remain undetected, $\forall t \in [t_j,\ t_j + T]$.*

Proof. Due to the constraints (40) and (42) of the optimization problem (37)-(42), it follows from Fact 2 that $C(x_h^{a\star}(t) - x^{a\star}(t)) = 0$, $\forall t \in [t_j,\ t_j + T]$, where $x^{a\star},\ x_h^{a\star}$ are the trajectories of (38)-(39) for $\left\{u^a,\ a,\ d_h^a\right\} \equiv \left\{u^{a\star},\ a^\star,\ d_h^{a\star}\right\}$. Since the infinity norm of $d_h^{a\star}$ is bounded by Δ, we can invoke Fact 1 and conclude that the attacker will remain undetected, with $d_h^{a\star}$ being the corresponding admissible signal for the attacker. ∎

Next, we present a formal statement that describes the Nash equilibrium solution of the game (37)-(42) for the attacker.

Theorem 3. *Let the tuple $\{u^{a\star}, \{a^\star, d_h^{a\star}\}\}$ constitute a Nash equilibrium to the game* (37) *subject to* (38)-(42)*. Then, $\forall t \in [t_j,\ t_j + T]$, it follows that*

$$\begin{aligned} u^{a\star}(t) &= -R^{a-1}B^{\mathrm{T}}\big(\mu^a(t) + \mu_h^a(t)\big),\\ a^\star(t) &= K^{a-1}B^{\mathrm{T}}\mu^a(t),\\ d_h^{a\star}(t) &= \Delta \cdot \tanh\Big(D^{a-1}B^{\mathrm{T}}\mu_h^a(t)\Big) \end{aligned}$$

where $\mu^a, \mu_h^a : [t_j,\ t_j + T] \to \mathbb{R}^n$, $\xi^a : [t_j,\ t_j + T] \to \mathbb{R}$ satisfy

$$\begin{aligned} &\dot{\mu}^a(t) = -A^{\mathrm{T}}\mu^a(t) - Q^a x^a(t) - C^{\mathrm{T}}C\left(x^a(t) - x_h^a(t)\right)\xi^a(t),\\ &\dot{\mu}_h^a(t) = -A^{\mathrm{T}}\mu_h^a(t) - C^{\mathrm{T}}C\left(x_h^a(t) - x^a(t)\right)\xi^a(t),\\ &\dot{\xi}^a(t) = 0,\\ &\mu^a(t_j + T) = F^a x^a(t_j + T),\ \mu_h^a(t_j + T) = 0, \end{aligned}$$

subject to (38)-(42) *for $u^a = u^{a\star}$, $d_h^a = d_h^{a\star}$ and $a = a^\star$.*

Proof. The proof is omitted as it is similar to that of Theorem 1. ∎

Similar to the defender, the attacker can choose its controller a by implementing $a^\star$ in a receding horizon. In particular, if $a^\star(\cdot;\ t_j)$ is the signal $a^\star$ derived in the j-th instance of the optimization (37)-(42), $j \in \mathbb{N}$, then the attacker's RHC will be given by

$$a(t) = a^\star(t;\ t_j),\ \forall t \in [t_j,\ t_{j+1}],\ j \in \mathbb{N}. \tag{43}$$

C. Boundedness of the Closed-Loop Trajectories

Given that the solutions provided by Theorems 1, 3 are applied to (1) iteratively in a receding horizon fashion $\forall t \geqslant t_0$, it is crucial to guarantee safety of the closed loop, in the sense of proving boundedness of the resulting trajectories of (1). The following lemmas, which are needed for the overall analysis, show that the solutions of (1), as well as the control signals arising in (13)-(20) and (37)-(42), scale according to x_j, $\forall t \in [t_j,\ t_j + T]$.

Lemma 2. *There exists $K^{a\star} \in \mathbb{R}^{m\times m}$ and $k_1,\ k_2 > 0$, such that if $K^a \succ K^{a\star}$ then $\|a^\star(t)\| \leqslant k_1\|x_j\| + k_2$, $\forall t \in [t_j,\ t_j + T]$, $\forall j \in \mathbb{N}$.*

Proof. Due to the saddle-point property of $\{u^{a\star}, \{a^\star, d_h^{a\star}\}\}$, one has:

$$\begin{aligned} \tilde{J}^a\left(u^{a\star}, a^\star, d_h^{a\star};\ t_j\right) &\leqslant \tilde{J}^a\left(0, a^\star, d_h^{a\star};\ t_j\right)\\ &\leqslant \int_{t_j}^{t_j+T} \frac{1}{2}\Big(\lambda_{\max}(Q^a)\left\|x^a(\tau)\right\|^2 - \lambda_{\min}(K^a)\|a^\star(\tau)\|^2\Big)\mathrm{d}\tau\\ &\quad + \frac{1}{2}\lambda_{\max}(F^a)\left\|x^a(t_j + T)\right\|^2. \end{aligned} \tag{44}$$

Since the defending control input has been set to zero, the trajectory x^a satisfies $x^a(t) = e^{A(t-t_j)}x_j + \int_{t_j}^t e^{A(t-\tau)}B\left(a^\star(\tau) + d(\tau)\right)\mathrm{d}\tau$, for all $t \in [t_j,\ t_j + T]$. Hence, owing to Assumption 1 which bounds the disturbance norm, there exist constants $\lambda_1,\ \lambda_2,\ \lambda_3 > 0$, dependent on A, B, Δ, T, such that for all $t \in [t_j,\ t_j + T]$:

$$\left\|x^a(t)\right\|^2 \leqslant \lambda_1\left\|x_j\right\|^2 + \lambda_2\int_{t_j}^{t_j+T}\left\|a^\star(\tau)\right\|^2\mathrm{d}\tau + \lambda_3. \tag{45}$$

Assume now that the statement of the theorem does not hold. Then, for some interval $[t_s,\ t_e] \subseteq [t_j,\ t_j + T]$, $\|a^\star(t)\| \geqslant k_1\|x_j\| + k_2$ even as $\|x_j\| \to \infty$, no matter how large $k_1,\ k_2$ are picked. In this case, if we substitute the bound from (45) in (44) and pick $\lambda_{\min}(K^a)$, $k_1,\ k_2$ large enough, the right hand-side of (44) will tend to $-\infty$ as $\|x_j\| \to \infty$, meaning that $\tilde{J}^a\left(u^{a\star}, a^\star, d_h^{a\star};\ t_j\right)$ will also tend to $-\infty$. However, in the suboptimal scenario that the attacker does not attack, the tuple $\{u^{a\star}, \{0, d\}\}$ yields a cost $\tilde{J}^a\left(u^{a\star}, 0, d;\ t_j\right)$ that is lower bounded by construction, hence $\tilde{J}^a\left(u^{a\star}, 0, d;\ t_j\right) > \tilde{J}^a\left(u^{a\star}, a^\star, d_h^{a\star};\ t_j\right)$; a contradiction. ∎

Lemma 3. *Let Assumptions 1-3 hold. Then, there exist matrices $K^{d\star},\ K^{a\star}$ and constants $\mu_1,\ \mu_2,\ \delta^\star > 0$, such that if $K^d \succ K^{d\star}$, $K^a \succ K^{a\star}$ and $\delta < \delta^\star$, then $\left\{\|u^\star(t)\|, \left\|a^{d\star}(t)\right\|, \left\|a_p^{d\star}(t)\right\|\right\} \leqslant \mu_1\|x_j\| + \mu_2$, $\forall t \in [t_j,\ t_j + T]$, $\forall j \in \mathbb{N}$.*

Proof. We will use an inductive proof. Assume that there exist constants $\zeta_1, \zeta_2 > 0$, such that $\|x_{j-1}\| \leqslant \zeta_1\|x_j\| + \zeta_2$, $j \in \mathbb{N}$. This inequality holds trivially at $j = 0$, since x_0 is bounded.

First, we will prove the results for the attack vectors $a^{d\star}$ and $a_p^{d\star}$. Let $x_j^d = x^d(t_j)$ be the initial condition predicted by the defender. Owing to the constraints (17)-(20), it holds $\forall t \in [t_j - T,\ t_j]$ that:

$$\begin{aligned} y(t) = Ce^{A(t-t_j)}x_j^d + \int_{t_j}^t Ce^{A(t-\tau)}B\\ \cdot\left(d_p^{d\star}(2t_j - \tau) + u(\tau) + a_p^{d\star}(2t_j - \tau)\right)\mathrm{d}\tau. \end{aligned} \tag{46}$$

However, from (1), for all $t \in [t_j - T,\ t_j]$, it also holds that

$$\begin{aligned} y(t) = Ce^{A(t-t_j)}x_j + \int_{t_j}^t Ce^{A(t-\tau)}B\\ \cdot\left(d_p(2t_j - \tau) + u(\tau) + a_p(2t_j - \tau)\right)\mathrm{d}\tau. \end{aligned} \tag{47}$$

Subtracting (47) from (46) leads to:

$$\begin{aligned} 0 = Ce^{A(t-t_j)}(x_j^d - x_j) + \int_{t_j}^t Ce^{A(t-\tau)}B\Big(d_p^{d\star}(2t_j - \tau)\\ - d_p(2t_j - \tau) + (a_p^{d\star}(2t_j - \tau) - a_p(2t_j - \tau))\Big)\mathrm{d}\tau. \end{aligned} \tag{48}$$

Consequently, an integration of (48) yields:

$$\begin{aligned} x_j^d = x_j - \left[\int_{t_j}^{t_{j-1}} e^{A^{\mathrm{T}}(\sigma - t_j)}C^{\mathrm{T}}Ce^{A(\sigma-t_j)}\mathrm{d}\sigma\right]^{-1}\\ \cdot\Bigg[\int_{t_j}^{t_{j-1}} e^{A^{\mathrm{T}}(\sigma-t_j)}C^{\mathrm{T}}\int_{t_j}^{\sigma}Ce^{A(\sigma-\tau)}B\big(d_p^{d\star}(2t_j - \tau)\\ - d_p(2t_j - \tau) + (a_p^{d\star}(2t_j - \tau) - a_p(2t_j - \tau))\big)\mathrm{d}\tau\mathrm{d}\sigma\Bigg]. \end{aligned} \tag{49}$$

The matrix inversion in (49) is possible because the inverted term is an observability gramian of the pair (A, C); an observable pair, owing to Assumption 3. From (49) and (27), Lemma 2, Assumption 1 and the inductive assumption, we deduce that there exist constants $\lambda_1, \lambda_2, \lambda_3 > 0$, dependent on A, B, C, Δ, T, such that:

$$\left\|x_j^d\right\|^2 \leqslant \lambda_1\int_{t_j}^{t_j+T}\left\|a_p^{d\star}(\tau)\right\|^2\mathrm{d}\tau + \lambda_2\left\|x_j\right\|^2 + \lambda_3. \tag{50}$$

Subsequently, owing to the saddle-point property of $\{u^\star, \mathcal{A}^\star\}$:

$$\tilde{J}^d\left(u^\star,\ \mathcal{A}^\star;\ t_j\right) \leqslant \tilde{J}^d\left(0,\ \mathcal{A}^\star;\ t_j\right) \leqslant \int_{t_j}^{t_j+T}\frac{1}{2}\Big(\lambda_{\max}(Q^d)$$

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2022.3195922

$$\cdot \left\|x^d(\tau)\right\|^2 - \lambda_{\min}(K^d)\left(\left\|a^{d\star}(\tau)\right\|^2 + \left\|a_p^{d\star}(\tau)\right\|^2\right)\Big)\mathrm{d}\tau + \frac{1}{2}\lambda_{\max}(F^d)\left\|x^d(t_j+T)\right\|^2. \quad (51)$$

Since the defending control input has been set to zero, the trajectory x^d satisfies $x^d(t) = e^{A(t-t_j)}x_j^d + \int_{t_j}^{t} e^{A(t-\tau)}B\left(a^{d\star}(\tau)+d^{d\star}(\tau)\right)\mathrm{d}\tau$, for all $t \in [t_j,\ t_j+T]$. Therefore, given also (50) and the fact that the infinity norm of $d^{d\star}$ is bounded by Δ given (24), there exist constants $\rho_1,\rho_2,\rho_3,\rho_4>0$ dependent on A,B,C,Δ,T so that for all $t\in[t_j,\ t_j+T]$:

$$\left\|x^d(t)\right\|^2 \leqslant \rho_1\left\|x_j\right\|^2 + \rho_2\int_{t_j}^{t_j+T}\left\|a^{d\star}(\tau)\right\|^2\mathrm{d}\tau + \rho_3\int_{t_j}^{t_j+T}\left\|a_p^{d\star}(\tau)\right\|^2\mathrm{d}\tau + \rho_4. \quad (52)$$

Owing to (51)-(52), we can use the same arguments as in Lemma 3 to show that there exist $K^{d\star},K^{a\star}\in\mathbb{R}^{m\times m}$ and $\mu_1,\mu_2>0$, independent of x_j, such that if $K^d\succ K^{d\star}$ and $K^a\succ K^{a\star}$, then it holds that $\left\|a^{d\star}(t)\right\|\leqslant\mu_1\left\|x_j\right\|+\mu_2$ and $\left\|a_p^{d\star}(t)\right\|\leqslant\mu_1\left\|x_j\right\|+\mu_2$, $\forall t\in[t_j,\ t_j+T]$, $\forall j\in\mathbb{N}$.

From the minimizing perspective, notice that due to (51):

$$\tilde{J}^d\left(u^\star,\ \mathcal{A}^\star;\ t_j\right)\leqslant\int_{t_j}^{t_j+T}\frac{1}{2}\left(\lambda_{\max}(Q^d)\left\|x^d(\tau)\right\|^2\right)\mathrm{d}\tau + \frac{1}{2}\lambda_{\max}(F^d)\left\|x^d(t_j+T)\right\|^2, \quad (53)$$

where x^d satisfies (52). As a result, and since we have proved that $\left\|a^{d\star}(t)\right\|\leqslant\mu_1\left\|x_j\right\|+\mu_2$ and $\left\|a_p^{d\star}(t)\right\|\leqslant\mu_1\left\|x_j\right\|+\mu_2$, $\forall t\in[t_j,\ t_j+T]$, $\forall j\in\mathbb{N}$, it follows that there exist constants $\rho_5,\ \rho_6$, independent of t_j, such that for all $j\in\mathbb{N}$:

$$\tilde{J}^d\left(u^\star,\ \mathcal{A}^\star;\ t_j\right)\leqslant\rho_5\left\|x_j\right\|^2+\rho_6. \quad (54)$$

Hence, $\left\|u^\star(t)\right\|\leqslant\mu_1\left\|x_j\right\|+\mu_2$ must also hold for some $\mu_1,\ \mu_2$, otherwise (54) cannot hold for any $x_j\in\mathbb{R}^n$ by definition.

Finally, notice that for all $t\in[t_j,\ t_j+T]$, we have $\left\|u^\star(t)\right\|\leqslant\mu_1\left\|x_j\right\|+\mu_2$ and, due to Lemma 2, $\left\|a^\star(t)\right\|\leqslant k_1\left\|x_j\right\|+k_2$. Therefore, since $\left\|d(t)\right\|_\infty<\Delta$ and due to the linearity of the dynamics (1), we can pick δ small enough, below a threshold $\delta^\star$ that is inversely proportional to k_1 and μ_1, and guarantee that $\left\|x(t_j)\right\|\leqslant\zeta_1\left\|x(t_{j+1})\right\|+\zeta_2$. ■

Lemma 4. *Let the conditions of Lemmas 2-3 and Assumptions 1-3 hold. Then, for all $i,j\in\mathbb{N}$, there exist constants $\alpha_{i-j},\beta_{i-j},\gamma_{i-j},\delta_{i-j}>0$, so that, $\forall t\in[t_i,\ t_i+T]$, the following inequalities hold:*

$$\alpha_{i-j}\left\|x_j\right\|-\beta_{i-j}\leqslant\left\{\left\|x(t)\right\|,\left\|u^\star(t;t_i)\right\|,\left\|a^\star(t;t_i)\right\|,\left\|a_p^{d\star}(t;t_i)\right\|\right\}\leqslant\gamma_{i-j}\left\|x_j\right\|+\delta_{i-j}. \quad (55)$$

Proof. The proof is a direct consequence of Lemmas 2-3, Assumption 1 and the linearity of the dynamics (1). ■

While Lemmas 2-4 provide useful information regarding the derived control signals, they do not investigate whether the closed-loop trajectories will diverge to infinity after infinite time. In order to rule out this scenario, we will need the following controllability assumption, which is standard in the RHC literature [4], [14], [28].

Assumption 4. The terminal cost $F(x^d)=\left\|x^d\right\|_{F^d}$ is an input-to-state stability control Lyapunov function for the dynamics (14), i.e., there exists $\psi:\mathbb{R}^n\to\mathbb{R}^m$ such that

$$\frac{\mathrm{d}F(x^d(t))}{\mathrm{d}t}|_{u=\psi(x^d)}\leqslant-\left\|x^d(t)\right\|_{Q^d}-\left\|\psi(x^d(t))\right\|_{R^d}+\left\|a^d(t)\right\|_{K^d}+\left\|d^d(t)\right\|_{D^d,\Delta}. \quad \square$$

The following theorem presents the main result of this subsection.

Theorem 4. *Let Assumptions 1-4 hold, and the defending and attacking control laws be given by* (36) *and* (43)*. Then, there exists a constant $\delta^\star>0$ and symmetric matrices $K^{a\star},\ K^{d\star}\succ 0$, such that if $K^d\succeq K^{d\star}$, $K^a\succeq K^{a\star}$ and $\delta<\delta^\star$, then the trajectories of the system state $x(t)$ remain bounded, $\forall t\geqslant t_0$.*

Proof. Given (13)-(20) at $t=t_j$, $j\in\mathbb{N}$, we will denote the corresponding decision functions or trajectories $\forall t\in[t_j,\ t_j+T]$ with $\phi(t;t_j)$, where ϕ is any trajectory or function of $t\in[t_j,\ t_j+T]$ computed at $t=t_j$. Hence, let us denote the minimizing policy of the optimization problem (13)-(20) computed at $t=t_j$ as $u^\star(t;t_j)$, the corresponding maximizing functions as

$$\mathcal{A}^\star(t;t_j)=\left\{a^{d\star}(t;t_j),a_p^{d\star}(t;t_j),d^{d\star}(t;t_j),d_p^{d\star}(t;t_j),d_h^{d\star}(t;t_j)\right\},$$

the resulting optimal trajectory as $x^{d\star}(t;t_j)$, and the corresponding optimal value of (13)-(20) as $\tilde{J}^d(u^\star(t;t_j),\mathcal{A}^\star(t;t_j);t_j)=\tilde{J}^{d\star}(t_j)$.

Consider now the two first consecutive optimization problems $P_d(t_j)$ and $P_d(t_{j+1})$ of the form (13)-(20), solved at the time instants t_j and t_{j+1} respectively, with $j\in\mathbb{N}$. For problem $P_d(t_j)$ and for $t\in[t_j,t_j+T]$, given that the past attack is selected equal to the real past attack, i.e., $a_p^d(t;t_j)=a_p(t)=a(2t_j-t)$, and the past disturbance is selected equal to the real past disturbance, i.e., $d_p^d(t;t_j)=d_p(t)=d(2t_j-t)$, then the initial condition is constrained to be the true initial condition according to Assumption 3 and Lemma 1, i.e., $x^d(t_j;t_j)=x_0$. In addition, for problem $P_d(t_j)$ and for $t\in[t_j,t_{j+1}]$, given that the future attack and disturbance signals are selected equal to the worst-case past attack and disturbance signals of the problem $P_d(t_{j+1})$, i.e., $a^d(t;t_j)=a_p^{d\star}(2t_{j+1}-t;t_{j+1})$, and $d^d(t;t_j)=d_p^{d\star}(2t_{j+1}-t;t_{j+1})$, then $x^d(t_{j+1};t_j)=x^{d\star}(t_{j+1};t_{j+1})$. Now, note that since the future attack is assumed to be stealthy, the output that will be generated will always be compatible with the attack-free model (9). Therefore, for this particular choice of $a^d(t;t_j)$ and $d^d(t;t_j)$, over $t\in[t_j,t_{j+1}]$, there exists an admissible signal $\bar{d}_h^d:[t_j,\ t_{j+1}]\to\mathbb{R}^m$ with $\left\|\bar{d}_h^d(t)\right\|_\infty<\Delta$, $\forall t\in[t_j,\ t_{j+1}]$, so that if one sets $d_h(t)=\bar{d}_h^d(t)$, $\forall t\in[t_j,\ t_{j+1}]$, the constraints of the optimization problem $P_d(t_j)$ are satisfied $\forall t\in[t_j,t_{j+1}]$.

Finally, since for such a choice of past input signals over $t\in[t_j,t_j+T]$ and future signals over $t\in[t_j,t_{j+1}]$ we have $x^d(t_{j+1};t_j)=x^{d\star}(t_{j+1};t_{j+1})$, then $\forall t\in[t_{j+1},t_j+T]$ the inputs $a^d(t;t_j)=a^{d\star}(t;t_{j+1})$, $d^d(t;t_j)=d^{d\star}(t;t_{j+1})$ and $d_h^d(t;t_j)=d_h^{d\star}(t;t_{j+1})$ satisfy the output compatibility constraints of problem $P_d(t_j)$ because they also satisfy the output compatibility constraints of the problem $P_d(t_{j+1})$. Note that, owing to Fact 1, the choice of u does not affect the undetectability constraints.

Define now the policies:

$$\tilde{u}(t;t_{j+1})=\begin{cases}u^\star(t;t_j),\ t\in[t_{j+1},t_j+T],\\ \psi(\tilde{x}^d(t;t_{j+1})),\ t\in[t_j+T,t_{j+1}+T],\end{cases}$$

$$\tilde{a}^d(t;t_j)=\begin{cases}a_p^{d\star}(2t_{j+1}-t;t_{j+1}),\ t\in[t_j,t_{j+1}],\\ a^{d\star}(t;t_{j+1}),\ t\in[t_{j+1},t_j+T],\end{cases}$$

$$\tilde{a}_p^d(t;t_j)=a_p(t),t\in[t_j,t_j+T],$$

$$\tilde{d}^d(t;t_j)=\begin{cases}d_p^{d\star}(2t_{j+1}-t;t_{j+1}),t\in[t_j,t_{j+1}],\\ d^{d\star}(t;t_{j+1}),\ t\in[t_{j+1},t_j+T],\end{cases}$$

$$\tilde{d}_p^d(t;t_j)=d_p(t),t\in[t_j,t_j+T],$$

$$\tilde{d}_h^d(t;t_j)=\begin{cases}\bar{d}_h^d(t),t\in[t_j,t_{j+1}],\\ d_h^{d\star}(t;t_{j+1}),\ t\in[t_{j+1},t_j+T],\end{cases}$$

$$\tilde{\mathcal{A}}(t;t_j)=\left\{\tilde{a}^d(t;t_j),\tilde{a}_p^d(t;t_j),\tilde{d}^d(t;t_j),\tilde{d}_p^d(t;t_j),\tilde{d}_h^d(t;t_j)\right\},$$

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2022.3195922

where $\tilde{x}^d(t;t_j)$ is the trajectory of x^d for $P_d(t_j)$ by applying $u=u^\star(t;t_j)$ and $\mathcal{A}=\tilde{\mathcal{A}}(t;t_j),\ \forall t\in[t_j,\ t_j+T]$, and $\tilde{x}^d(t;t_{j+1})$ the trajectory of x^d for $P_d(t_{j+1})$ by applying $u=\tilde{u}(t;t_{j+1})$ and $\mathcal{A}=\mathcal{A}^\star(t;t_{j+1}),\ \forall t\in[t_{j+1},\ t_{j+1}+T]$. Due to the preceding discussion, $\tilde{\mathcal{A}}(t;t_j)$ is feasible with respect to the constraints of the optimization problem $P_d(t_j)$, while $\tilde{u}(t;t_{j+1})$ is feasible for the optimization problem $P_d(t_{j+1})$. Hence, due to saddle-point optimality, the following hold

$$\tilde{J}^{d\star}(t_j)\geqslant \tilde{J}^d(u^\star(t;t_j),\tilde{\mathcal{A}}(t;t_j);t_j), \tag{56}$$

$$\tilde{J}^{d\star}(t_{j+1})\leqslant \tilde{J}^d(\tilde{u}(t;t_{j+1}),\mathcal{A}^\star(t;t_{j+1});t_{j+1}). \tag{57}$$

Then, given (56)-(57) we have that,

$$\begin{aligned}
&\tilde{J}^{d\star}(t_{j+1})-\tilde{J}^{d\star}(t_j)\\
&\leqslant \tilde{J}^d(\tilde{u}(t;t_{j+1}),\mathcal{A}^\star(t;t_{j+1});t_{j+1})-\tilde{J}^d(u^\star(t;t_j),\tilde{\mathcal{A}}(t;t_j);t_j)\\
&=\int_{t_{j+1}}^{t_{j+1}+T}\Big(\left\|\tilde{x}^d(\tau;t_{j+1})\right\|_{Q^d}+\|\tilde{u}(\tau;t_{j+1})\|_{R^d}-\left\|a^{d\star}(\tau;t_{j+1})\right\|_{K^d}\\
&-\left\|a_p^{d\star}(\tau;t_{j+1})\right\|_{K^d}-\left\|d^{d\star}(\tau;t_{j+1})\right\|_{D^d,\Delta}-\left\|d_p^{d\star}(\tau;t_{j+1})\right\|_{D^d,\Delta}\\
&-\left\|d_h^{d\star}(\tau;t_{j+1})\right\|_{D^d,\Delta}\Big)\mathrm{d}\tau+\left\|\tilde{x}^d(t_{j+1}+T;t_{j+1})\right\|_{F^d}\\
&-\int_{t_j}^{t_j+T}\Big(\left\|\tilde{x}^d(\tau;t_j)\right\|_{Q^d}+\|u^\star(\tau;t_j)\|_{R^d}-\left\|\tilde{a}^d(\tau;t_j)\right\|_{K^d}\\
&-\left\|\tilde{a}_p^d(\tau;t_j)\right\|_{K^d}-\left\|\tilde{d}^d(\tau;t_j)\right\|_{D^d,\Delta}-\left\|\tilde{d}_p^d(\tau;t_j)\right\|_{D^d,\Delta}\\
&-\left\|\tilde{d}_h^d(\tau;t_j)\right\|_{D^d,\Delta}\Big)\mathrm{d}\tau-\left\|\tilde{x}^d(t_j+T;t_j)\right\|_{F^d}.
\end{aligned}\tag{58}$$

Note that, it holds that $\tilde{x}^d(t_{j+1};t_j)=x^{d\star}(t_{j+1};t_{j+1})$. Since the past disturbance input and attack for the optimization problem $P_d(t_{j+1})$ are set equal to the worst-case ones, it also holds that $\tilde{x}^d(t_{j+1};t_{j+1})=x^{d\star}(t_{j+1};t_{j+1})$, and yields $\tilde{x}^d(t_{j+1};t_j)=\tilde{x}^d(t_{j+1};t_{j+1})$. Finally, given $t\in[t_{j+1},t_j+T]$ we have $\tilde{a}^d(t;t_j)=a^{d\star}(t;t_{j+1})$, $\tilde{d}^d(t;t_j)=d^{d\star}(t;t_{j+1})$, and $\tilde{u}(t;t_{j+1})=u^\star(t;t_j)$, thus owing to $\tilde{x}^d(t_{j+1};t_j)=\tilde{x}^d(t_{j+1};t_{j+1})$ we write $\tilde{x}^d(t;t_j)=\tilde{x}^d(t;t_{j+1}),\ \forall t\in[t_{j+1},t_j+T]$. Therefore, (58), after taking into account Assumption 4 reduces to,

$$\begin{aligned}
&\tilde{J}^{d\star}(t_{j+1})-\tilde{J}^{d\star}(t_j)\leqslant-\int_{t_j+T}^{t_{j+1}+T}\left\|d_h^{d\star}(\tau;t_{j+1})\right\|_{D^d,\Delta}\mathrm{d}\tau\\
&-\int_{t_{j+1}+\delta}^{t_{j+1}+T}\Big(\left\|a_p^{d\star}(\tau;t_{j+1})\right\|_{K^d}+\left\|d_p^{d\star}(\tau;t_{j+1})\right\|_{D^d,\Delta}\Big)\mathrm{d}\tau\\
&-\int_{t_j}^{t_{j+1}}\left(\left\|\tilde{x}^d(\tau;t_j)\right\|_{Q^d}+\|u^\star(\tau;t_j)\|_{R^d}-\left\|\bar{d}_h^d(\tau)\right\|_{D^d,\Delta}\right)\mathrm{d}\tau\\
&+\int_{t_j}^{t_j+T}\left(\|a_p(\tau)\|_{K^d}+\|d_p(\tau)\|_{D^d,\Delta}\right)\mathrm{d}\tau\\
&\leqslant-\int_{t_j}^{t_{j+1}}\left\|\tilde{x}^d(\tau;t_j)\right\|_{Q^d}\mathrm{d}\tau+\int_{t_j}^{t_j+T}\|a_p(\tau)\|_{K^d}\,\mathrm{d}\tau+M_1,
\end{aligned}\tag{59}$$

where $M_1=(T+\delta)\max_{d_M\in[-\Delta,\ \Delta]^m}\|d_M\|_{D^d,\Delta}$. This maximum exists even if any entry of d_M takes the values $\pm\Delta$ [24]. Letting $\epsilon>0$ be any arbitrary constant, there exist two cases: a) (Case $\|x_j\|\geqslant\epsilon$): Due to Lemma 4, it holds that $\|a_p(t)\|\leqslant\theta_1\|x_j\|+\theta_2,\ \forall t\in[t_j,\ t_j+T]$, for some $\theta_1,\theta_2>0$. On the other hand, $\int_{t_j}^{t_{j+1}}\left\|\tilde{x}^d(\tau;t_j)\right\|_{Q^d}\mathrm{d}\tau\geqslant\iota\|x_j\|^2$ for some $\iota>0$, because $\tilde{x}^d(t_j;t_j)=x_j$, and the evolution of the trajectories of $\tilde{x}^d(\cdot;t_j)$ is affected by $u^\star$ and $a_p^\star(\cdot,\ t_{j+1})$, whose norm is bounded by a linear function of $\|x_j\|$ as shown in Lemma 4, and by $\bar{d}_h^d(\cdot)$, whose infinity norm is bounded by Δ. In addition, $\theta_1,\theta_2\to0$ as $\lambda_{\min}(K^a)\to\infty$. Therefore, if $\lambda_{\min}(K^a)$ and ϵ are picked sufficiently large, the right-hand side of (59) is negative; b) if $\|x_j\|<\epsilon$ then the value of $\tilde{J}^{d\star}(t_j)$ is bounded by construction, by a value dependent on ϵ. Aggregating both cases and the requirements of Lemma 4, if $K^d\geq K^{d\star}$, $K^a\geq K^{a\star}$, and $\delta<\delta^\star$, then there exists a constant $J_M<\infty$, such that $\tilde{J}^{d\star}(t_j)\leqslant J_M,\ \forall j\in\mathbb{N}$.

Finally, consider the set $\mathcal{A}^r(t;t_j):=\{0,a_p(t),0,d_p(t),0\}$, where the future attack and disturbance are set equal to zero, and the past attack and disturbance are set equal to the real ones. Denote as $\tilde{x}^r$ the resulting trajectory of x^d in (14) if we apply $u=u^\star(t;t_j)$ and $\mathcal{A}=\mathcal{A}^r(t;t_j)$ at $t=t_j,\ \forall j\in\mathbb{N}$. Then, due to optimality, over the interval $[t_j,t_j+T]$ we obtain, $\forall j\in\mathbb{N}$,

$$\begin{aligned}
J_M&\geqslant\tilde{J}^{d\star}(t_j)\geqslant\tilde{J}^d(u^\star(t;t_j),\mathcal{A}^r(t;t_j);t_j)=\int_{t_j}^{t_j+T}\big(\|\tilde{x}^r(\tau)\|_{Q^d}\\
&+\|u^\star(\tau;t_j)\|_{R^d}-\|a_p(\tau)\|_{K^d}-\|d_p(\tau)\|_{D^d,\Delta}\big)\mathrm{d}\tau+\|\tilde{x}^r(t_j+T)\|_{F^d}\\
&\geqslant\int_{t_j}^{t_j+T}\big(\|\tilde{x}^r(\tau)\|_{Q^d}-\|a_p(\tau)\|_{K^d}\big)\mathrm{d}\tau-M_2,
\end{aligned}\tag{60}$$

where $M_2=T\cdot\max_{d_M\in[-\Delta,\ \Delta]^m}\|d_M\|_{D^d,\Delta}$. Since the past attack and disturbance were set equal to the actual ones, we have $\tilde{x}^r(t_j)=x_j$. Hence, using identical arguments as in the previous paragraph, due to Lemma 4, if $K^d\geq K^{d\star}$, $K^a\geq K^{a\star}$, and $\delta<\delta^\star$, then from the right part of (60) we derive $\tilde{J}^{d\star}(t_j)\geqslant\pi_1\|x_j\|^2-\pi_2$ for some $\pi_1,\pi_2>0,\ \forall j\in\mathbb{N}$. Thus, (60) gives $\|x_j\|\leqslant\sqrt{\frac{J_M+\pi_2}{\pi_1}},\ \forall j\in\mathbb{N}$, which combined with Lemma 4 yields $\sup_{t\geqslant t_0}\|x(t)\|<\infty$. ■

Remark 9. The proposed game-theoretic methodology for the defender has some similarities with the methods of Chapter 5 in [29]. In particular, [29] also considers output-based game-theoretic control techniques for systems under the effect of unknown deterministic disturbances. However, different than [29], the optimal control problem of the defender presented here also considers attacks that are constrained by an undetectability equation, and the initial condition is not assumed to lie in a predefined compact set. In addition, [29] does not study the receding horizon version of its game-theoretic controller, nor provides closed-loop boundedness guarantees. □

V. Simulations

We consider a linearized version of the Aero-Data Model in Research Environment (ADMIRE) benchmark aircraft [30], whose state is initially at the origin. The disturbance signal is set equal to $d(t)=0.02\sin(2\pi t)\mathbb{1}_7$, and its known upper bound is $\Delta=0.1$. The goal is to keep the full state vector of the aircraft regulated around its nominal value despite the stealthy attacks and the additive disturbance. The parameters of the receding horizon framework are picked as: $Q^d=2I_5$, $R^d=0.1I_7$, $K^d=10I_7$, $D^d=2I_7$, $F^d=10I_5$, $Q^a=I_5$, $R^a=0.5I_7$, $K^a=6I_7$, $D^a=5I_7$, and $F^a=I_5$. The optimization horizon is set equal to $T=0.1$ [s], while the control horizon is set equal to $\delta=0.005$ [s].

We simulate the system for 8 seconds, with the defending and attacking policies as in (36) and (43). To showcase the performance deterioration that the stealthy attack can cause, we suppose that the stealthy attack vanishes after the 4th second. The states, control policies, and the predicted performance at each iteration are shown in Figures 1-2. It can be seen that, although the performance cost is worse while the undetectable attacker is compromising the system, closed-loop boundedness is maintained.

VI. Conclusion and Future Work

In this paper, we considered a disturbed system under the influence of a defender and an attacker that hides under the uncertainty created by an unknown disturbance, with information asymmetry. We provided a secure RHC mechanism for the defender, that guarantees the boundedness of the closed-loop system without knowledge of the full system state. In addition, we characterized the optimal policy for the attacker, which guarantees its undetectability.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2022.3195922

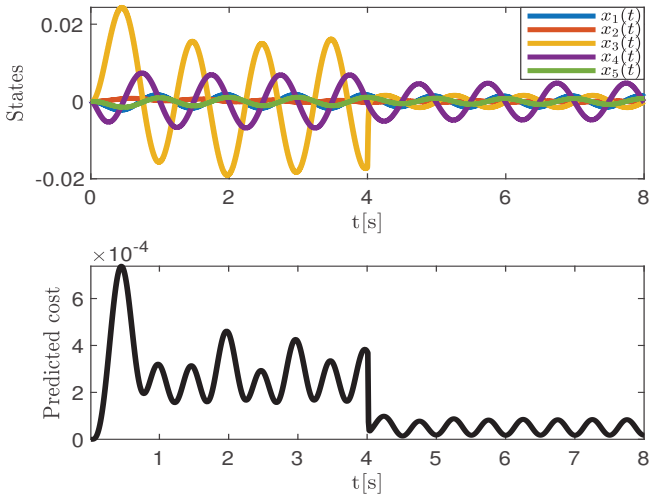

Fig. 1. Evolution of the states and the predicted cost when the system is under attack for $t \in [0,\ 4]$.

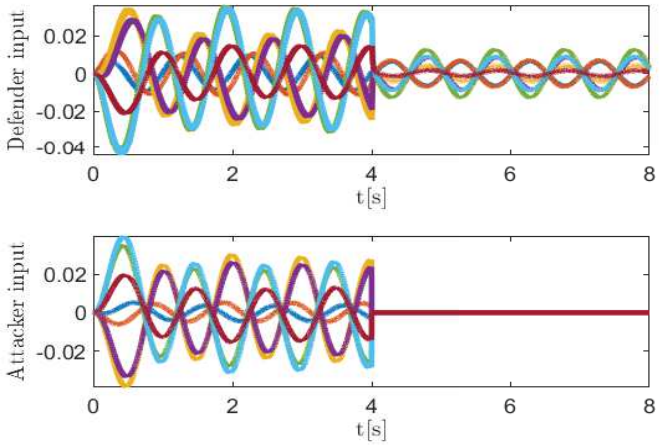

Fig. 2. Evolution of the control policies when the system is under attack for $t \in [0,\ 4]$.

Future work will extend the results to cases where the CPS is under attack by multiple adversaries, and where the defender and the attackers have bounded rationality.

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," *Annual Reviews in Control*, vol. 47, pp. 394–411, 2019.

[2] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *2008 The 28th International Conference on Distributed Computing Systems Workshops*, pp. 495–500, IEEE, 2008.

[3] T. Basar and G. J. Olsder, *Dynamic noncooperative game theory*, vol. 23. Siam, 1999.

[4] D. Q. Mayne, J. B. Rawlings, C. V. Rao, and P. O. Scokaert, "Constrained model predictive control: Stability and optimality," *Automatica*, vol. 36, no. 6, pp. 789–814, 2000.

[5] H. Chen, C. W. Scherer, and F. Allgower, "A game theoretic approach to nonlinear robust receding horizon control of constrained systems," in *Proceedings of the 1997 American Control Conference (Cat. No. 97CH36041)*, vol. 5, pp. 3073–3077, IEEE, 1997.

[6] M. Diehl and J. Bjornberg, "Robust dynamic programming for min-max model predictive control of constrained uncertain systems," *IEEE Transactions on Automatic Control*, vol. 49, no. 12, pp. 2253–2257, 2004.

[7] J. H. Lee and Z. Yu, "Worst-case formulations of model predictive control for systems with bounded parameters," *Automatica*, vol. 33, no. 5, pp. 763–781, 1997.

[8] D. Limon, T. Alamo, D. M. Raimondo, D. M. De La Peña, J. M. Bravo, A. Ferramosca, and E. F. Camacho, "Input-to-state stability: a unifying framework for robust model predictive control," in *Nonlinear model predictive control*, pp. 1–26, Springer, 2009.

[9] L. Magni, G. De Nicolao, R. Scattolini, and F. Allgöwer, "Robust model predictive control for nonlinear discrete-time systems," *International Journal of Robust and Nonlinear Control: IFAC-Affiliated Journal*, vol. 13, no. 3-4, pp. 229–246, 2003.

[10] M. Zhu and S. Martinez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 3, pp. 804–808, 2013.

[11] Y.-C. Sun and G.-H. Yang, "Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks," *International Journal of Robust and Nonlinear Control*, vol. 29, no. 14, pp. 4797–4811, 2019.

[12] M. Zhu and S. Martinez, "Stackelberg-game analysis of correlated attacks in cyber-physical systems," in *Proceedings of the 2011 American Control Conference*, pp. 4063–4068, IEEE, 2011.

[13] D. A. Copp and J. P. Hespanha, "Simultaneous nonlinear model predictive control and state estimation," *Automatica*, vol. 77, pp. 143–154, 2017.

[14] D. A. Copp, K. G. Vamvoudakis, and J. P. Hespanha, "Distributed output-feedback model predictive control for multi-agent consensus," *Systems & Control Letters*, vol. 127, pp. 52–59, 2019.

[15] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.

[16] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE transactions on automatic control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[17] F. Fotiadis and K. G. Vamvoudakis, "Detection of actuator faults for continuous-time systems with intermittent state feedback," *Systems & Control Letters*, vol. 152, p. 104938, 2021.

[18] Y. Chen, S. Kar, and J. M. Moura, "Dynamic attack detection in cyber-physical systems with side initial state information," *IEEE Transactions on Automatic Control*, vol. 62, no. 9, pp. 4618–4624, 2016.

[19] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *2013 American control conference*, pp. 3344–3349, IEEE, 2013.

[20] J. P. Hespanha and S. D. Bopardikar, "Output-feedback linear quadratic robust control under actuation and deception attacks," in *Proc. Amer. Control Conf.*, 2019.

[21] Y.-C. Liu, G. Bianchin, and F. Pasqualetti, "Secure trajectory planning against undetectable spoofing attacks," *Automatica*, vol. 112, p. 108655, 2020.

[22] A. Sanjab and W. Saad, "On bounded rationality in cyber-physical systems security: Game-theoretic analysis with application to smart grid protection," in *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*, pp. 1–6, IEEE, 2016.

[23] F. Fotiadis, A. Kanellopoulos, and K. G. Vamvoudakis, "Constrained differential games for secure decision-making against stealthy attacks," in *2020 American Control Conference (ACC)*, pp. 4658–4663, IEEE, 2020.

[24] S. E. Lyshevski, "Optimal control of nonlinear continuous-time systems: design of bounded controllers via generalized nonquadratic functionals," in *Proceedings of the 1998 American Control Conference. ACC (IEEE Cat. No. 98CH36207)*, vol. 1, pp. 205–209, IEEE, 1998.

[25] A. E. Bryson, *Applied optimal control: optimization, estimation and control*. Routledge, 2018.

[26] F. B. Hildebrand, *Methods of applied mathematics*. Courier Corporation, 2012.

[27] J. P. Hespanha, *Noncooperative game theory: An introduction for engineers and computer scientists*. Princeton University Press, 2017.

[28] F. Fontes, L. Magni, *et al.*, "Min-max model predictive control of nonlinear systems using discontinuous feedbacks," *IEEE Transactions on Automatic Control*, vol. 48, no. 10, pp. 1750–1755, 2003.

[29] T. Başar and P. Bernhard, *H-infinity optimal control and related minimax design problems: a dynamic game approach*. Springer Science & Business Media, 2008.

[30] J. Jiang and X. Yu, "Fault-tolerant control systems: A comparative study between active and passive approaches," *Annual Reviews in control*, vol. 36, no. 1, pp. 60–72, 2012.