Data-Driven Robust Control Under Input-Output Stealthy Attacks

Arijit Bhowmik Shaunak D. Bopardikar João P. Hespanha

***Abstract*— We consider the problem of robust control of an unknown but minimal linear time-invariant system under input and output disturbances and adversarial manipulation. An attacker can (i) corrupt sensor measurements (deception attacks) and (ii) perturb the control channel (actuation attacks). To address the lack of model knowledge, we adapt the Data-enabled Predictive Control (DeePC) framework, which constructs predictors directly from input–output data with bounded disturbance. We formulate a finite-horizon open-loop control problem as a two-player zero-sum game with asymmetric information: the defender selects control inputs based on measured data and only knows an upper bound on disturbances, whereas the attacker has access to the true disturbance realization and can remain stealthy by hiding within this uncertainty set. The main contributions are (i) sufficient conditions for the existence of a Nash equilibrium corresponding to saddle-point policies for this game, and (ii) an analysis of the defender's security strategy against deception and actuation attacks. Simulation studies on finite-horizon control demonstrate the effectiveness of the proposed approach.**

I. Introduction

Cyber–physical systems (CPSs) integrate sensing, communication, and control to enable critical infrastructures such as autonomous transportation, industrial automation, and water networks [1], [2]. Their reliance on networked communication, however, exposes them to malicious manipulation. Stealthy attacks such as false data injection, sensor deception, and actuator perturbations can cause significant performance degradation while evading conventional monitoring [3], [4]. These attacks exploit information asymmetry, where adversaries leverage additional knowledge or flaws in system design to ensure that abnormal behavior appears normal.

Most existing studies on attack detection and resilient control assume that system dynamics are known [5]–[7]. While powerful, this assumption often limits practicality, as accurate models of large-scale CPSs are difficult to obtain. Data-driven approaches offer a more realistic alternative by operating directly on input–output data without requiring explicit models. Recent works have explored this perspective, including data-driven attack detection, adversarial learning of control policies, and false data injection design [8]–[10]. These results highlight the promise of data-driven methods: by eliminating reliance on precise system models, they enable control and attack-detection strategies without explicit knowledge of the system dynamics.

Within this direction, Data-enabled Predictive Control (DeePC) [11] has emerged as a recent and powerful tool. Rooted in Willems' Fundamental Lemma [12], it enables predictive control without explicit knowledge of the system dynamics. DeePC has been extended to incorporate robustness, solving a min–max optimization problem to compute the control sequence resilient to all possible uncertainties within a prescribed set [13].

In this paper, we study data-driven robust control under actuation and deception attacks using DeePC. Building on the model-based framework from our conference version [6], we pose the problem as a two-player game: (i) the defender minimizes tracking error and control effort using input–output data, while (ii) the adversary maximizes deviation by injecting stealthy attacks into actuation and measurement channels. The defender knows only an upper bound on the ℓ_2 norm of the disturbance, whereas the adversary has access to the true disturbance vector and can hide within this uncertainty set to remain undetected. We derive sufficient conditions for the existence of a saddle-point equilibrium for this game and characterize the resulting defender strategy. Our focus is on open-loop finite-horizon control, which can naturally extend to a receding-horizon setting.

The main contribution of this paper is to establish sufficient conditions for the existence of a Nash equilibrium corresponding to a saddle-point policy. Section II presents preliminaries, Section III the problem formulation, Section IV the main results, Section V simulation studies, and Section VI concludes with future directions.

II. System Dynamics and Control objective

Consider a discrete time linear time-invariant (LTI) system

$$\begin{aligned} x_{t+1} &= A_x x_t + B u_t \\ y_t &= C_y x_t + D u_t \end{aligned} \tag{1}$$

in a minimal representation, where $x_t \in \mathbb{R}^n$ is the state of the system, $u_t \in \mathbb{R}^m$ is the input to the system and $y_t \in \mathbb{R}^p$ is the output vector $\forall t \in \mathbb{Z}_{\geq 0}$. Here n denotes the minimal representation order of the system, m is the input dimension and p is the output dimension. The observability matrix for system (1) is given by $\mathcal{O}_l(A_x, C_y) = [C_y; C_y A_x; \ldots; C_y A_x^{l-1}]$, where l is the *lag* of the system defined by the minimum number of block rows in the observability matrix $\mathcal{O}_l(A_x, C_y)$ for its rank to become n.

In this paper, we consider an unknown but controllable LTI system, for which upper bounds on the system order n and lag l are assumed to be available from prior knowledge.

A. Bhowmik and S. D. Bopardikar are with the ECE Department, Michigan State University. Emails: {bhowmika, shaunak}@msu.edu. J. P. Hespanha (hespanha@ece.ucsb.edu) is with the ECE Department, University of California Santa Barbara.

This work was supported in part by the National Science Foundation SaTC Award CNS-2134076, in part by the National Science Foundation CAREER Award ECCS-2236537, in part by the National Science Foundation under grant no. 2229876 and in part by the U.S. Office of Naval Research grant No. N00014-24-1-2492.

An offline system trajectory dataset of length T, denoted by $[u^d; y^d] \in \mathbb{R}^{(m+p)T}$, is collected from the system. From this dataset, the Hankel matrices are constructed as in (2)–(3). By the Fundamental Lemma (Th. 1 in [12]), these Hankel matrices span all system trajectories of length $(T_{\text{ini}} + T_{\text{future}})$, provided that the input u^d is persistently exciting of order $(T_{\text{ini}} + T_{\text{future}} + n)$.

By definition, u^d is persistently exciting of order L if the associated Hankel matrix has full row rank. To guarantee this condition for $L = T_{\text{ini}} + T_{\text{future}} + n$, T must satisfy

$$T \geq (m+1)(T_{\text{ini}} + T_{\text{future}} + n) - 1.$$

$$\begin{bmatrix} U_p \\ U_f \end{bmatrix} \triangleq \begin{bmatrix} u_1^d & \cdots & u_{T-T_{\text{future}}-T_{\text{ini}}+1}^d \\ \vdots & \cdots & \vdots \\ u_{T_{\text{ini}}}^d & \cdots & u_{T-T_{\text{future}}}^d \\ u_{T_{\text{ini}}+1}^d & \cdots & u_{T-T_{\text{future}}+1}^d \\ \vdots & \cdots & \vdots \\ u_{T_{\text{ini}}+T_{\text{future}}}^d & \cdots & u_T^d \end{bmatrix}, \tag{2}$$

$$\begin{bmatrix} Y_p \\ Y_f \end{bmatrix} \triangleq \begin{bmatrix} y_1^d & \cdots & y_{T-T_{\text{future}}-T_{\text{ini}}+1}^d \\ \vdots & \cdots & \vdots \\ y_{T_{\text{ini}}}^d & \cdots & y_{T-T_{\text{future}}}^d \\ y_{T_{\text{ini}}+1}^d & \cdots & y_{T-T_{\text{future}}+1}^d \\ \vdots & \cdots & \vdots \\ y_{T_{\text{ini}}+T_{\text{future}}}^d & \cdots & y_T^d \end{bmatrix}. \tag{3}$$

The Hankel matrix is partitioned into two parts: the past (subscript p), corresponding to the first T_{ini} block rows (U_p, Y_p) and used to encode the system's initial condition, and the future data (subscript f), corresponding to the last T_{future} block rows (U_f, Y_f) and used to predict the future trajectories.

Using the Fundamental Lemma, a trajectory $[u_{\text{ini}}; u; y_{\text{ini}}; y] \in \mathbb{R}^{(m+p)(T_{\text{ini}}+T_{\text{future}})}$ is a valid behavior for the given system if and only if there exists a vector $g \in \mathbb{R}^{n_g}$ such that

$$[U_p; Y_p; U_f; Y_f]g = [u_{\text{ini}}; y_{\text{ini}}; u; y] \tag{4}$$

where $n_g = T - T_{\text{ini}} - T_{\text{future}} + 1$. If $T_{\text{ini}} \geq l$, then by Lemma 1 from [14], there exists a unique initial state x_{ini} consistent with the input-output measurements $[u_{\text{ini}}; y_{\text{ini}}]$. This state is reached by the input sequence u_{ini}, from which the future trajectory $[u; y]$ evolves. Leveraging this property, future trajectories can be predicted directly from the initial input–output data $[u_{\text{ini}}; y_{\text{ini}}]$ together with the pre-collected Hankel matrices U_p, U_f, Y_p, and Y_f.

So, given an initial trajectory of length $T_{\text{ini}} \geq l$ and a desired output y, one can compute the vector $g \in \mathbb{R}^{T-T_{\text{ini}}-T_{\text{future}}+1}$, and consequently the corresponding feedforward control input $u = U_f g$.

Consider a system tasked with tracking a reference signal $y_{\text{ref}} \in \mathbb{R}^{p\,T_{\text{future}}}$ over a fixed prediction horizon T_{future} while minimizing control effort. In practice, however, systems are often affected by unpredictable factors such as measurement noise or external disturbances, which requires one to appropriately modify the system equations in (4).

To address this, we explicitly model these uncertainties as a single disturbance term, D. While we may not know the exact nature of this disturbance, we assume it is bounded in magnitude, such that $\|D\| \leq \Delta_D$. This disturbance term $D \in \mathbb{R}^{n_d}$, where $n_d = (m+p)T_{\text{ini}} + mT_{\text{future}}$, is strategically introduced into the system constraints to absorb any inconsistencies and ensure the problem remains feasible at all times. Similar approaches can be seen in [11], [13].

By accounting for the *worst-case disturbance* within this admissible set, we ensure that the resulting controller is robust to bounded uncertainties. With these conditions in place, the robust tracking problem can be posed as

$$\min_{\substack{g\in\mathbb{R}^{n_g} \\ u\in\mathbb{R}^{mT_{\text{future}}}}} \max_{D\in\mathbb{R}^{n_d}} \|Y_f g - y_{\text{ref}}\|_2^2 + \|u\|_2^2 + \lambda_g \|g\|_2^2$$

subject to

$$\begin{bmatrix} u_{\text{ini}} \\ y_{\text{ini}} \\ u \end{bmatrix} = \begin{bmatrix} U_p \\ Y_p \\ U_f \end{bmatrix} g + \begin{bmatrix} F_{d_1} \\ F_{d_2} \\ F_{d_3} \end{bmatrix} D, \quad \|D\| \leq \Delta_D. \tag{5}$$

The matrices F_{d_i} $(i = 1, 2, 3)$ act as injection matrices that determine how the disturbance vector D contribute to different parts of the stacked trajectory. For simplicity, we assume that the predicted future output is disturbance-free and is given by the direct relationship $y = Y_f g$. The cost also includes a regularization penalty $(\lambda_g > 0)$ on g, which is closely related to distributionally robust optimization formulations [11]. If a solution exists, the min–max optimization problem yields $(g^\star, D^\star)$ as a saddle point of the objective, representing the optimal trajectory coefficients $g^\star$ and the worst-case disturbance $D^\star$.

III. Problem Set-up And Player Strategies

Building on the attack-free robust tracking problem discussed in Section II, we now formulate a two-player game that explicitly accounts for adversarial attacks. Player P_U selects g (implicitly u) to minimize a cost Z, as given in (6), based on the initial trajectory measurements and the bound Δ_D on $\|D\|$. Conversely, the adversarial player P_A attempts to maximize Z by injecting an attack $A \in \mathbb{R}^{n_a}$ into the initial measurement data and the system input as described in (7). We consider two classes of attacks:

1) actuation attacks, which manipulate the actual input signals (u_{ini}, u), and
2) deception attacks, which perturbs the actual initial output measurements (y_{ini}).

$$Z = \|Y_f g - y_{\text{ref}}\|_2^2 + \|u\|_2^2 \tag{6}$$

$$\begin{bmatrix} \overline{u}_{\text{ini}} \\ \overline{y}_{\text{ini}} \\ \overline{u} \end{bmatrix} = \begin{bmatrix} U_p \\ Y_p \\ U_f \end{bmatrix} g + \begin{bmatrix} F_{d_1} \\ F_{d_2} \\ F_{d_3} \end{bmatrix} D + \begin{bmatrix} F_{a_1} \\ F_{a_2} \\ F_{a_3} \end{bmatrix} A. \tag{7}$$

Here, $(u_{\text{ini}}, y_{\text{ini}})$ are the actual initial input-output sequence measured by P_A , and $(\overline{u}_{\text{ini}}, \overline{y}_{\text{ini}})$ are the corresponding

manipulated input-output sequence measured by P_U. The matrices F_{a_i} $(i = 1, 2, 3)$ act as injection matrices that determine how the attack vector A contributes to different parts of the stacked trajectory.

The game involves *asymmetric information*: both players, P_A and P_U, have access to the initial trajectory $(u_{\text{ini}}, y_{\text{ini}})$. Player P_A additionally knows P_U's control action u and the true disturbance D, whereas Player P_U only knows a constant Δ_D that upper bounds D. Both players operate with the same Hankel matrices (U_p, Y_p, U_f, Y_f), constructed from attack-free input–output data $[u^d, y^d]$.

In this problem formulation, we consider a basic attack detection mechanism: if the system behavior is inconsistent with the nominal system behavior given in (5) or violates any norm constraint, then Player P_U detects the attack and wins the game, regardless of the value of the cost Z.

The disturbance-selection matrices are defined as

$$F_{d_1} = \begin{bmatrix} I_{n_1} & 0 & 0 \end{bmatrix}_{n_1 \times n_d}, \qquad F_{d_2} = \begin{bmatrix} 0 & I_{n_2} & 0 \end{bmatrix}_{n_2 \times n_d},$$
$$F_{d_3} = \begin{bmatrix} 0 & 0 & I_{n_3} \end{bmatrix}_{n_3 \times n_d},$$

which partition the disturbance vector D across inputs, outputs, and future inputs.

The attack-selection matrices are binary matrices with entries in $\{0, 1\}$, that specify where attack signals are injected. An example is

$$F_{a_1} = \mathbf{1}_{n_1} e_1', F_{a_2} = \begin{bmatrix} 0 & I_{n_2} \end{bmatrix}_{n_2 \times (n_2+1)}, F_{a_3} = \mathbf{1}_{n_3} e_1',$$

where $\mathbf{1}_k \in \mathbb{R}^k$ is the all-ones column vector and $e_1 = [1\ 0\ \cdots\ 0]' \in \mathbb{R}^{n_2+1}$. This example corresponds to a constant actuation attack (via F_{a_1}, F_{a_3}) and a deception attack on the initial outputs (via F_{a_2}). Here $n_1 = mT_{\text{ini}}, n_2 = pT_{\text{ini}}$, $n_3 = mT_{\text{future}}$ and $n_d = (n_1 + n_2 + n_3)$.

Definition 1(Local Nash equilibrium [15]): A pair of strategies $(g^\star, A^\star)$ is a *local Nash equilibrium* of f if there exists $\delta > 0$ such that for any (g, A) satisfying $\|g - g^\star\| \le \delta$ and $\|A - A^\star\| \le \delta$, such that

$$f(g^\star, A) \le f(g^\star, A^\star) \le f(g, A^\star), \forall g \in \mathbb{R}^{n_g} \text{ and } A \in \mathbb{R}^{n_a}.$$

The following result is a useful computational tool for finding local Nash equilibria of our game.

Lemma 3.1 (Second-order Sufficient Condition for Local Nash Equilibrium **[15], Proposition 5**): Assuming f is twice differentiable, a stationary point $(g^\star, A^\star)$ (i.e., $\nabla f(g^\star, A^\star) = 0$) is a *local Nash equilibrium* if it satisfies

$$\nabla^2_{gg} f(g^\star, A^\star) \succ 0 \quad \text{and} \quad \nabla^2_{AA} f(g^\star, A^\star) \prec 0.$$

A stationary point satisfying these conditions is also called a *strict local Nash equilibrium*.

A. P_A's best response

Given that Player P_U selects the action u, Player P_A's best response is to choose A so as to maximize the cost. Using $[u_{\text{ini}}; y_{\text{ini}}; u]$ and the true disturbance D, P_A can solve the robust tracking problem in (5) to obtain the corresponding trajectory coefficient vector $g^\star$. Player P_A selects A subject to a *stealth constraint* that the system behavior has to remain consistent with the nominal model in (5). Formally, there must exist some $\tilde{g}$ within a δ_g-ball around $g^\star$, and some norm-bounded disturbance $\tilde{D}$ satisfying $\|\tilde{D}\| \le \Delta_D$, that can explain the observed trajectories in (8).

The adversarial optimization problem thus reduces to

$$\max_{\substack{\tilde{g} \in \mathbb{R}^{n_g}, \\ \tilde{D} \in \mathbb{R}^{n_d},\ A \in \mathbb{R}^{n_a}}} \|Y_f \tilde{g} - y_{\text{ref}}\|_2^2 + \|U_f \tilde{g} + F_{d_3} \tilde{D}\|_2^2$$

subject to:

$$\|g^\star - \tilde{g}\| \le \delta_g, \|\tilde{D}\| \le \Delta_D$$
$$\begin{bmatrix} u_{\text{ini}} \\ y_{\text{ini}} \\ u \end{bmatrix} + \begin{bmatrix} F_{a_1} \\ F_{a_2} \\ F_{a_3} \end{bmatrix} A = \begin{bmatrix} U_p \\ Y_p \\ U_f \end{bmatrix} \tilde{g} + \begin{bmatrix} F_{d_1} \\ F_{d_2} \\ F_{d_3} \end{bmatrix} \tilde{D}. \tag{8}$$

The constraints, imposed as norm bounds, ensure that the cost remains bounded. Keeping $\tilde{g}$ close to $g^\star$ makes the manipulated data appear attack-free, while the bound on $\tilde{D}$ ensures it represents a valid system disturbance. In this setting, the future trajectory satisfies $[u; y] = [U_f \tilde{g} + F_{d_3} \tilde{D}; Y_f \tilde{g}]$.

B. P_U's best response

Given that Player P_A selects the action A (unknown to P_U), which must be compatible with the actual, attack-free system behavior described in (5), Player P_U's best strategy is to choose $\hat{g}$ to minimize the cost under worst-case assumptions on the unknown disturbance $\hat{D}$ and the unknown attack $\hat{A}$. Moreover, the stealth constraint on the attacker ensures that the strategies $(\hat{g}, \{\hat{D}, \hat{A}\})$ must explain the manipulated initial behavior $(\overline{u}_{\text{ini}}, \overline{y}_{\text{ini}})$ as shown in (7).

Formally, Player P_U solves the min–max problem:

$$\min_{\hat{g} \in \mathbb{R}^{n_g}} \max_{\substack{\hat{A} \in \mathbb{R}^{n_a}, \\ \hat{D} \in \mathbb{R}^{n_d}}} \|Y_f \hat{g} - y_{\text{ref}}\|_2^2 + \|U_f \hat{g} + F_{d_3} \hat{D} + F_{a_3} \hat{A}\|_2^2 + \lambda_g \|\hat{g}\|_2^2$$

subject to

$$\begin{bmatrix} \overline{u}_{\text{ini}} \\ \overline{y}_{\text{ini}} \end{bmatrix} = \begin{bmatrix} U_p \\ Y_p \end{bmatrix} \hat{g} + \begin{bmatrix} F_{d_1} \\ F_{d_2} \end{bmatrix} \hat{D} + \begin{bmatrix} F_{a_1} \\ F_{a_2} \end{bmatrix} \hat{A}, \quad \|\hat{D}\| \le \Delta_D. \tag{9}$$

In this setting, the future trajectory satisfies $[u; y] = [U_f \hat{g} + F_{d_3} \hat{D} + F_{a_3} \hat{A}; Y_f \hat{g}]$. When the min and max commute, we say that $(\hat{g}, (\hat{D}, \hat{A}))$ is a strict local Nash equilibrium, and $\hat{g}$ is a security policy for P_U.

Although P_U and P_A have opposing goals, a saddle-point equilibrium does not exist because of information asymmetry: P_U lacks knowledge of the true D, while P_A has access to them. Additionally, the constraints are also different in both best response computations.

Since the optimization in (9) accounts for worst-case assumptions on A and D unknown to P_U, it results in a security policy for P_U, valid regardless of the attack A and the true disturbance D. In contrast, (8) does not define a policy for P_A, as the optimal A can only be computed once u is known, which is not available to P_A apriori.

IV. Existence of Nash Equilibrium

This section provides sufficient conditions for the existence of a strict local Nash equilibrium. For ease of presentation, we introduce the following compact notation.

$$\overline{F}_D = \begin{bmatrix} F_{d_1} \\ F_{d_2} \end{bmatrix}; \overline{F}_A = \begin{bmatrix} F_{a_1} \\ F_{a_2} \end{bmatrix}; \overline{H} = \begin{bmatrix} U_p \\ Y_p \end{bmatrix}$$

$$F_D = \begin{bmatrix} \overline{F}_D \\ F_{d_3} \end{bmatrix}; F_A = \begin{bmatrix} \overline{F}_A \\ F_{a_3} \end{bmatrix}; H = \begin{bmatrix} \overline{H} \\ U_f \end{bmatrix}; \overline{b} = \begin{bmatrix} \overline{u}_{\text{ini}} \\ \overline{y}_{\text{ini}} \end{bmatrix}$$

$$\hat{a} = \begin{bmatrix} \overline{F}_D & \overline{F}_A \end{bmatrix}; \hat{b} = \begin{bmatrix} \overline{u}_{\text{ini}} - F_{d_1}\hat{D} - F_{a_1}\hat{A} \\ \overline{y}_{\text{ini}} - F_{d_2}\hat{D} - F_{a_2}\hat{A} \end{bmatrix}$$

$$b = \begin{bmatrix} u_{\text{ini}} \\ y_{\text{ini}} \\ u \end{bmatrix}; a = \begin{bmatrix} H & F_D & -F_A \end{bmatrix}; Q_f = Y_f'Y_f + U_f'U_f.$$

A. P_U's saddle-point

Assuming that P_A injects an attack A that results in $(\overline{u}_{\text{ini}}, \overline{y}_{\text{ini}})$ that is compatible with the attack free system behavior. We provide a sufficient condition for the existence of a saddle-point for the min-max problem in (9).

Theorem 1. *Suppose there exist vectors $\hat{g}, \hat{D}, \hat{A}, \vartheta_{u_1}, \vartheta_{u_2}$ and scalar $\lambda_u > 0$ such that*

$$\begin{bmatrix} 2U_f'F_{a_3} & 2U_f'F_{d_3} & 2(Q_f+\lambda_g I) & \overline{H}' & 0 \\ 2F_{d_3}'F_{a_3} & 2(F_{d_3}'F_{d_3} - \lambda_u I) & 2F_{d_3}'U_f & 0 & -\overline{F}_D' \\ 2F_{a_3}'F_{a_3} & 2F_{a_3}'F_{d_3} & 2F_{a_3}'U_f & 0 & -\overline{F}_A' \\ \overline{F}_A & \overline{F}_D & \overline{H} & 0 & 0 \end{bmatrix} \times \begin{bmatrix} \hat{A} \\ \hat{D} \\ \hat{g} \\ \vartheta_{u_1} \\ \vartheta_{u_2} \end{bmatrix} = \begin{bmatrix} 2Y_f'y_{ref} \\ 0 \\ 0 \\ \overline{b} \end{bmatrix}, \tag{10a}$$

$$V_u' \begin{bmatrix} F_{d_3}'F_{d_3} - \lambda_u I & F_{d_3}'F_{a_3} \\ F_{a_3}'F_{d_3} & F_{a_3}'F_{a_3} \end{bmatrix} V_u < 0 \tag{10b}$$

and

$$\|\hat{D}\| = \Delta_D \tag{10c}$$

where V_u is any full column rank matrix such that

$$Im V_u = ker \begin{bmatrix} 2\hat{D}' & 0 \\ \overline{F}_D & \overline{F}_A \end{bmatrix}.$$

Then, $(\hat{g}, (\hat{D}, \hat{A}))$ is a strict local saddle-point of P_U's optimization problem.

Remark 1: In view of (Lemma 2, [6]), (10b) holds if and only if there exists some $\lambda_u > 0$ such that $ker[\overline{F}_D, \overline{F}_A] = \{0\}$. This condition depends on the structure of $\overline{F}_D$ and $\overline{F}_A$, which must be such that attacks cannot be completely masked by disturbances. Otherwise, if (10b) fails, attacks become indistinguishable from disturbances, making detection impossible.

Proof: The vectors $(\hat{g}, (\hat{D}, \hat{A}))$ are a strict local saddle-point for (9) if they are a strict local optima for the following coupled optimization:

$$\min_{\hat{g} \in \mathbb{R}^{n_g}} \|Y_f\hat{g} - y_{\text{ref}}\|_2^2 + \|U_f\hat{g} + F_{d_3}\hat{D} + F_{a_3}\hat{A}\|_2^2 + \lambda_g\|\hat{g}\|_2^2 \tag{11}$$

subject to:

$$\begin{bmatrix} U_p \\ Y_p \end{bmatrix} \hat{g} = \begin{bmatrix} \overline{u}_{\text{ini}} - F_{d_1}\hat{D} - F_{a_1}\hat{A} \\ \overline{y}_{\text{ini}} - F_{d_2}\hat{D} - F_{a_2}\hat{A} \end{bmatrix}.$$

The corresponding maximization problem is given by

$$\max_{\substack{\hat{A} \in \mathbb{R}^{n_a}, \\ \hat{D} \in \mathbb{R}^{n_d}}} \|Y_f\hat{g} - y_{\text{ref}}\|_2^2 + \|U_f\hat{g} + F_{d_3}\hat{D} + F_{a_3}\hat{A}\|_2^2 + \lambda_g\|\hat{g}\|_2^2 \tag{12}$$

subject to

$$\begin{bmatrix} F_{d_1} & F_{a_1} \\ F_{d_2} & F_{a_2} \end{bmatrix} \begin{bmatrix} \hat{D} \\ \hat{A} \end{bmatrix} = \begin{bmatrix} \overline{u}_{\text{ini}} - U_p\hat{g} \\ \overline{y}_{\text{ini}} - Y_p\hat{g} \end{bmatrix}, \quad \|\hat{D}\| \leq \Delta_D.$$

For the min problem, we keep the $\hat{D}$ and $\hat{A}$ fixed, while for the max problem, we keep the $\hat{g}$ fixed. We apply the *second-order sufficiency conditions for local optimality* (Th. 3 in [6]) as follows. Define the Lagrangian for problem (11) L_{u_1} as

$$\begin{aligned} L_{u_1}(\hat{g}, \vartheta_{u_1}) := \|Y_f\hat{g} - y_{\text{ref}}\|_2^2 + \vartheta_{u_1}'(\overline{H}\hat{g} - \hat{b}) \\ + \lambda_g\|\hat{g}\|_2^2 + \|U_f\hat{g} + F_{d_3}\hat{D} + F_{a_3}\hat{A}\|_2^2 \end{aligned}$$

For minimization, we must have

$$\begin{aligned} \frac{\partial L_{u_1}}{\partial \hat{g}} = 2Y_f'(Y_f\hat{g} - y_{\text{ref}}) + 2U_f'(U_f\hat{g} + F_{d_3}\hat{D} + F_{a_3}\hat{A}) \\ + 2\lambda_g\hat{g} + \overline{H}'\vartheta_{u_1} = 0. \end{aligned} \tag{13}$$

The Hessian of L_{u_1} with respect to $\hat{g}$ is

$$\nabla_{\hat{g}}^2 L_{u_1} = 2\big(Y_f'Y_f + U_f'U_f + \lambda_g I\big). \tag{14}$$

A sufficient condition for $\hat{g}$ to be a strict local minimum of (9) is

$$v'\nabla_{\hat{g}}^2 L_{u_1} v > 0 \quad \forall v \neq 0, \ \overline{H}v = 0, \tag{15}$$

i.e., positive definiteness of the Hessian on the null space of the equality constraint. In this work, condition (15) is always satisfied when Y_f and U_f are full rank and $\lambda_g > 0$.

For problem (12), let us define $\overline{x} = (\hat{D}, \hat{A})$ and the Lagrangian L_{u_2} as

$$\begin{aligned} L_{u_2}(\hat{D}, \hat{A}, \lambda_u, \vartheta_{u_2}) := \|Y_f\hat{g} - y_{\text{ref}}\|_2^2 - \lambda_u(\|\hat{D}\|^2 - \Delta_D^2) \\ + \|U_f\hat{g} + F_{d_3}\hat{D} + F_{a_3}\hat{A}\|_2^2 - \vartheta_{u_2}'(\hat{a}\overline{x} - (\overline{b} - \overline{H}\hat{g})), \end{aligned}$$

$$g_u(\hat{D}, \hat{A}) := \|\hat{D}\|_2^2 - \Delta_D^2; \quad h_u(\hat{D}, \hat{A}) := \hat{a}\overline{x} - (\overline{b} - \overline{H}\hat{g})$$

$$\frac{\partial L_{u_2}}{\partial \hat{D}} = 2F_{d_3}'(U_f\hat{g} + F_{d_3}\hat{D} + F_{a_3}\hat{A}) - 2\lambda_u\hat{D} - \overline{F}_D'\vartheta_{u_2} = 0 \tag{16a}$$

$$\frac{\partial L_{u_2}}{\partial \hat{A}} = 2F_{a_3}'(U_f\hat{g} + F_{d_3}\hat{D} + F_{a_3}\hat{A}) - \overline{F}_A'\vartheta_{u_2} = 0 \tag{16b}$$

$$\overline{H}\hat{g} + \overline{F}_D\hat{D} + \overline{F}_A\hat{A} - \overline{b} = 0 \tag{16c}$$

$$\Delta_D^2 - \|\hat{D}\|^2 = 0 \tag{16d}$$

$$V_u' \begin{bmatrix} F_{d_3}'F_{d_3} - \lambda_u I & F_{d_3}'F_{a_3} \\ F_{a_3}'F_{d_3} & F_{a_3}'F_{a_3} \end{bmatrix} V_u < 0 \tag{16e}$$

Then, $\overline{x} = (\hat{D}, \hat{A})$ is a strict local maximum of (9). Specifically, condition (10a) guarantees that (13) and (16a)–(16c) hold, condition (10b) ensures (16e), and condition (10c) guarantees (16d). That completes this proof.

B. Nash Equilibrium

We now state a result that provides a sufficient condition for the existence of a Nash equilibrium $(g^\star, A^\star)$ when P_A and P_U play $A^\star$ and $\hat{g}^\star$, respectively.

Theorem 2. *Suppose that there exist vectors* $\hat{A}, \hat{D}, \hat{g}, \vartheta_{u_1}, \vartheta_{u_2}, A, \tilde{D}, \tilde{g}, \vartheta_a$ *and scalars* $\lambda_{a_1} > 0, \lambda_{a_2} > 0, \lambda_g > 0, \lambda_u > 0$ *such that*

$$[A_1 \mid A_2] \begin{bmatrix} \hat{A} \\ \hat{D} \\ \hat{g} \\ \vartheta_{u_1} \\ \vartheta_{u_2} \\ A \\ \tilde{D} \\ \tilde{g} \\ \vartheta_a \end{bmatrix} = \begin{bmatrix} 2(Y_f' y_{ref} - \lambda_{a_2} g^\star) \\ 0 \\ 0 \\ b \\ 2Y_f' y_{ref} \\ 0 \\ 0 \\ 0 \end{bmatrix}, \tag{17a}$$

where

$$A_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2U_f' F_{a_3} & 2U_f' F_{d_3} & 2(Q_f + \lambda_g I) & \overline{H}' \\ 2F_{d_3}' F_{a_3} & 2(F_{d_3}' F_{d_3} - \lambda_u I) & 2F_{d_3}' U_f & 0 \\ 2F_{a_3}' F_{a_3} & 2F_{a_3}' F_{d_3} & 2F_{a_3}' U_f & 0 \\ \overline{F}_A & \overline{F}_D & \overline{H} & 0 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 0 & 0 & 2U_f' F_{d_3} & 2(Q_f - \lambda_{a_2} I) & -H' \\ 0 & 0 & 2(F_{d_3}' F_{d_3} - \lambda_{a_1} I) & 2F_{d_3}' U_f & -F_D' \\ 0 & 0 & 0 & 0 & F_A' \\ 0 & -F_A & F_D & H & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -\overline{F}_D' & 0 & 0 & 0 & 0 \\ -\overline{F}_A' & 0 & 0 & 0 & 0 \\ 0 & 0 & -\overline{F}_D & -\overline{H} & 0 \end{bmatrix}$$

and

$$\|\tilde{D}\| = \|\hat{D}\| = \Delta_D, \tag{17b}$$

$$\|g^\star - \tilde{g}\| = \delta_g \tag{17c}$$

$$V_u' \begin{bmatrix} F_{d_3}' F_{d_3} - \lambda_u I & F_{d_3}' F_{a_3} \\ F_{a_3}' F_{d_3} & F_{a_3}' F_{a_3} \end{bmatrix} V_u < 0, \tag{17d}$$

$$V_a' \begin{bmatrix} Q_f - \lambda_{a_2} I & U_f' F_{d_3} & 0 \\ F_{d_3}' U_f & F_{d_3}' F_{d_3} - \lambda_{a_1} I & 0 \\ 0 & 0 & 0 \end{bmatrix} V_a < 0, \tag{17e}$$

where V_u *and* V_a *are full column rank matrices and*

$$Im V_u = ker \begin{bmatrix} 2\hat{D}' & 0 \\ \overline{F}_D & \overline{F}_A \end{bmatrix},$$

$$Im V_a = ker \begin{bmatrix} 0 & 2\tilde{D}' & 0 \\ 2(\tilde{g} - g^\star)' & 0 & 0 \\ H & F_D & -F_A \end{bmatrix}.$$

Then, $(\hat{g}, A)$ *is a strict local Nash equilibrium and* $\hat{g}$ *is also a security policy for* P_u.

Proof: Let us define $x = (\tilde{g}, \tilde{D}, A)$ and the Lagrangian for problem (8) L_a as

$$\begin{aligned} L_a(\tilde{g}, \tilde{D}, A, \lambda_{a_1}, \lambda_{a_2}, \vartheta_a) &:= \|Y_f \tilde{g} - y_{\text{ref}}\|_2^2 \\ &+ \|U_f \tilde{g} + F_{d_3} \tilde{D}\|_2^2 - \lambda_{a_1}(\|\tilde{D}\|_2^2 - \Delta_D^2) \\ &- \lambda_{a_2}(\|g^\star - \tilde{g}\|_2^2 - \delta_g^2) - \vartheta_a'(ax - b), \end{aligned}$$

$$g_a(\tilde{g}, \tilde{D}, A) := \begin{bmatrix} \|\tilde{D}\|_2^2 - \Delta_D^2 \\ \|g^\star - \tilde{g}\|_2^2 - \delta_g^2 \end{bmatrix};\ h_a(\tilde{g}, \tilde{D}, A) := ax - b.$$

Using the *second-order sufficient optimality conditions*, we characterize the solution of problem (8) . Specifically, a point $x = (\tilde{g}, \tilde{D}, A)$ is a strict local maximum of (8) if there exists $\lambda_{a_1} > 0,\ \lambda_{a_2} > 0,\ \vartheta_a \in \mathbb{R}^{n_x}$ such that

$$\begin{aligned} \frac{\partial L_a}{\partial \tilde{g}} &= 2Y_f'(Y_f \tilde{g} - y_{\text{ref}}) + 2U_f'(U_f \tilde{g} + F_{d_3} \tilde{D}) \\ &+ 2\lambda_{a_2}(g^\star - \tilde{g}) - H' \vartheta_a = 0, \end{aligned} \tag{18a}$$

$$\frac{\partial L_a}{\partial \tilde{D}} = 2F_{d_3}'(U_f \tilde{g} + F_{d_3} \tilde{D}) - 2\lambda_{a_1} \tilde{D} - F_D' \vartheta_a = 0, \tag{18b}$$

$$\frac{\partial L_a}{\partial A} = F_A' \vartheta_a = 0, \tag{18c}$$

$$H\tilde{g} + F_D \tilde{D} = b + F_A A, \tag{18d}$$

$$V_a' \begin{bmatrix} Q_f - \lambda_{a_2} I & U_f' F_{d_3} & 0 \\ F_{d_3}' U_f & F_{d_3}' F_{d_3} - \lambda_{a_1} I & 0 \\ 0 & 0 & 0 \end{bmatrix} V_a < 0, \tag{18e}$$

$$\|\tilde{D}\|^2 - \Delta_D^2 = 0, \tag{18f}$$

$$\|g^\star - \tilde{g}\|^2 - \delta_g^2 = 0. \tag{18g}$$

Condition (17a) ensures that (10a) and (18a)–(18d) hold simultaneously. Similarly, (17b) implies (10c) and (18f), (17c) guarantees (18g), and (17e) ensures (18e). The theorem assumptions guarantee that all conditions are satisfied jointly.

V. Simulation Result

We consider the problem of position control for a double integrator system. The system dynamics are given by

$$A_x = \begin{bmatrix} 1 & 0.5 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad C_y = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

For this model, $n = l = 2$, the input dimension is $m = 1$, and the output dimension is $p = 2$. Persistently exciting data (u^d, y^d) are collected offline from the system to construct the Hankel matrices. For simulation, we use the disturbance matrices F_{d_i} and example attack injection matrices F_{a_i} $(i = 1, 2, 3)$ from Section III.

Figs. 1 and 2 illustrate how, for a fixed $\Delta_D = 0.01$, the attacker's ability to deviate the system from reference tracking diminishes as the true system disturbance norm increases from $\|D\| \to 0$ to $\|D\| \to 0.01$.

In both cases, the actuation attack is applied over (u_{ini}, u) while the deception attack perturbs y_{ini}. In the first two subplots of Figs. 1 and 2, the blue curve shows the actual (attack-free) behavior, the green curve illustrates the system response under attack, and the magenta curve represents the response when the proposed robust security policy is applied. The orange curve with markers corresponds to the injected deception attack. The third subplot depicts the corresponding input trajectories under these three conditions, with the orange attack signal highlighting the actuation attack.

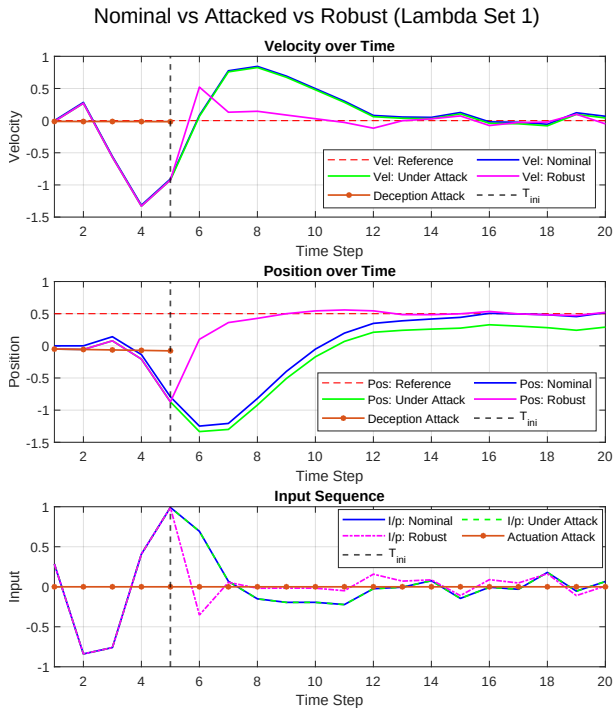

Fig. 1. Signals with $\|D\| = 0$, $\Delta_D = 0.01$, $\lambda_g = 1$,$y_{\text{ref}} = (0.5, 0)$, $T_{\text{ini}} = 5$, $T_f = 15$, $T = 43$, $D \in \mathbb{R}^{25}$, $A \in \mathbb{R}^{11}$.

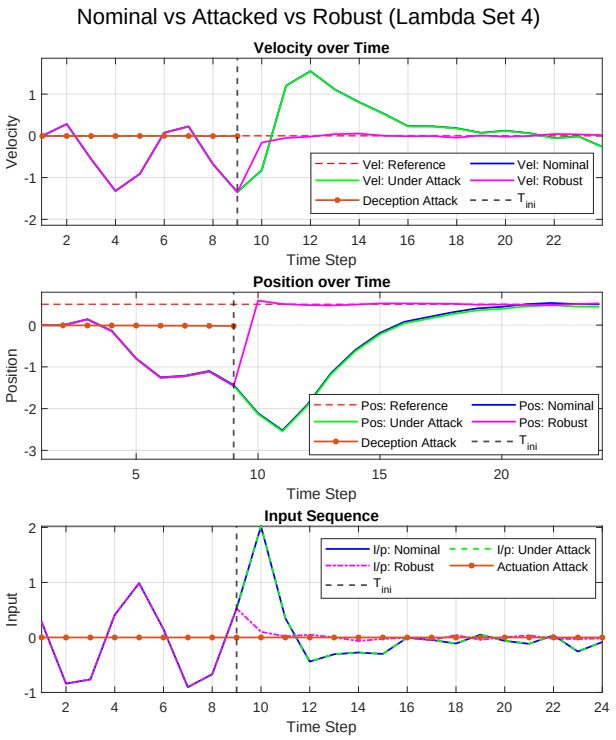

Fig. 2. Signals with $\|D\| = 0.01$, $\Delta_D = 0.01$, $\lambda_g = 1$,$y_{\text{ref}} = (0.5, 0)$, $T_{\text{ini}} = 9$, $T_f = 15$, $T = 51$, $D \in \mathbb{R}^{42}$, $A \in \mathbb{R}^{19}$.

VI. Conclusion and Future Directions

This paper studied data-driven robust control of an unknown but minimal linear system subject to unmeasured disturbances and noise, in the presence of an attacker capable of corrupting the measured output (deception attack) and perturbing the control signal (actuation attack). We formulated the problem as a zero-sum game between a defender, who selects the control signal based on the initial system trajectory, and an attacker, who selects the attack signals, under asymmetric information between the players with more advantage to the attacker. The main results are sufficient conditions for the existence of a Nash equilibrium corresponding to a saddle-point for the defender, and the application of this theory to finite-horizon control in data-driven setting with quadratic cost.

Future work will explore more general information structures for the players.

References

[1] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, "Robustness of attack-resilient state estimators," in *2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2014, pp. 163–174.

[2] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in *International conference on critical infrastructure protection*. Springer, 2007, pp. 73–82.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, 2011.

[4] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Preprints of the first workshop on secure control systems, CPSWEEK*, vol. 2010. Stockholm, Sweden, 2010.

[5] 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.

[6] J. P. Hespanha and S. D. Bopardikar, "Output-feedback linear quadratic robust control under actuation and deception attacks," in *American Control Conference (ACC)*, Philadelphia, PA USA, July 2019, pp. 489–496.

[7] F. Fotiadis and K. G. Vamvoudakis, "Concurrent receding horizon control and estimation against stealthy attacks," *IEEE Transactions on Automatic Control*, vol. 68, no. 6, pp. 3712–3719, 2022.

[8] Z. Zhao, Y. Huang, Z. Zhen, and Y. Li, "Data-driven false data-injection attack design and detection in cyber-physical systems," *IEEE Transactions on Cybernetics*, vol. 51, no. 12, pp. 6179–6187, 2020.

[9] F. Fotiadis, A. Kanellopoulos, K. G. Vamvoudakis, and U. Topcu, "Deception against data-driven linear-quadratic control," *arXiv preprint arXiv:2506.11373*, 2025.

[10] V. Krishnan and F. Pasqualetti, "Data-driven attack detection for linear systems," *IEEE Control Systems Letters*, vol. 5, no. 2, pp. 671–676, 2020.

[11] J. Coulson, J. Lygeros, and F. Dörfler, "Data-enabled predictive control: In the shallows of the deepc," in *2019 18th European Control Conference (ECC)*. IEEE, 2019, pp. 307–312.

[12] J. C. Willems, P. Rapisarda, I. Markovsky, and B. L. De Moor, "A note on persistency of excitation," *Systems & Control Letters*, vol. 54, no. 4, pp. 325–329, 2005.

[13] L. Huang, J. Zhen, J. Lygeros, and F. Dörfler, "Robust data-enabled predictive control: Tractable formulations and performance guarantees," *IEEE Transactions on Automatic Control*, vol. 68, no. 5, pp. 3163–3170, 2023.

[14] I. Markovsky and P. Rapisarda, "Data-driven simulation and control," *International Journal of Control*, vol. 81, no. 12, pp. 1946–1959, 2008.

[15] C. Jin, P. Netrapalli, and M. Jordan, "What is local optimality in nonconvex-nonconcave minimax optimization?" in *International conference on machine learning*. PMLR, 2020, pp. 4880–4889.