

# LQR Control with Sparse Adversarial Disturbances

Samuel Pfrommer and Somayeh Sojoudi

**Abstract**—Recent developments in cyber-physical systems and event-triggered control have led to an increased interest in the impact of sparse disturbances on dynamical processes. We study Linear Quadratic Regulator (LQR) control under sparse disturbances by analyzing three distinct policies: the blind online policy, the disturbance-aware policy, and the optimal offline policy. We derive the two-dimensional recurrence structure of the optimal disturbance-aware policy, under the assumption that the controller has information about future disturbance values with only a probabilistic model of their locations in time. Under mild conditions, we show that the disturbance-aware policy converges to the blind online policy if the number of disturbances grows sublinearly in the time horizon. Finally, we provide a finite-horizon regret bound between the blind online policy and optimal offline policy, which is proven to be quadratic in the number of disturbances and in their magnitude. This provides a useful characterization of the suboptimality of a standard LQR controller when confronted with unexpected sparse perturbations.

## I. INTRODUCTION

Much of the recent focus on sparse disturbances is motivated by the study of cyber-physical systems, which couple physical processes, networking, and computation into a larger controller architecture. Research in this area seeks to provide robustness against malicious cyberattacks and Stuxnet-style adversaries. Here, adversaries often act sparsely in both measurement channels and time in order to avoid detection and efficiently use their limited computational resources. Early works on this topic focused largely on state estimation where adversaries can perturb a sparse subset of measurement channels [1, 2, 3, 4]. In [5], the authors examined the signal reconstruction problem for cyber-physical systems with limited knowledge of the support of the attack vector. This was further explored in [6], which studied state estimation in the context of sparse actuator attacks. Sparsity in time was first introduced by [7], which restricted attacks to a small sequence of consecutive time steps and considered the adversarial goal of maximizing the system estimation error of a Kalman filter. We generalize this notion of sparsity to nonconsecutive time steps.

Sparsity has also gained significant attention in the realm of event-triggered control (ETC). Many cyber-physical systems face communication bandwidth constraints and actuation limits, inspiring event-triggered techniques that provide sparse-in-time control signals [8, 9, 10]. Model-based ETC instead addresses the issue of sparse disturbances with time-varying magnitudes [11]. In model-based ETC, both the

sensor and the actuator maintain an internal model of the system, and the sensor only communicates to the actuator if it is triggered by a large deviation from the nominal state. Numerical experiments in [11] demonstrate that this approach is particularly sample-effective when dealing with sparse disturbances.

Fault detection is a related field which aims to detect and predict sparse anomalies in system operation. Early work focused on linear systems, using techniques such as detection filters [12] and parameter estimation [13]. More recently, [14] considers non-sparse disturbance prediction for continuous-time systems by computing higher order derivatives of the disturbance signal. Interesting related work on distributed parameter systems employed detection residuals to estimate fault functions and time to failure [15]. Learning-based approaches have also been considered for model-unknown nonlinear systems [16]. Our novel disturbance-aware policy assumes access to such probabilistic predictions of future disturbances. Modeling and estimating future disturbances is outside of the scope of this work and would rely on techniques similar to those in the fault detection literature.

Other recent research efforts have focused on the role of sparsity in identification of dynamical systems. Inspired by modeling challenges in large-scale control problems, [17] considers the identification of linear time-invariant systems under large and sparse disturbances. These disturbances can model both stealthy adversarial attacks and faults in system operation. The authors introduce sparsity via the  $\Delta$ -spaced disturbance model, which assumes that adversaries are unable to perturb the system twice within  $\Delta$  time steps. Under this assumption, it is shown that perfect recovery of the system matrix is possible under certain sufficient conditions. This work builds off of [18] and [19], which examine system identification when the dynamics matrices themselves have a sparse structure and provide sample complexity guarantees for accurate system estimation.

While this is the first work to explicitly examine sparse disturbances in an LQR context, we draw inspiration from several recent advancements in the area of policy regret. Leveraging new techniques from the online convex optimization community, [20] formulates a regret minimization problem in the case of a linear dynamical system with convex cost functions and arbitrary bounded disturbances. Their proposed algorithm achieves  $O(\sqrt{T})$  regret against the optimal stable linear policy. This is extended in [21], which considers the case of unknown dynamics matrices and provides an algorithm with an  $O(T^{2/3})$  regret bound. [22] reimposes the LQR condition of quadratic cost functions and fully characterizes the recursive structure of the optimal

This work was supported by grants from ONR, NSF and C3.ai Digital Transformation Institute. Samuel Pfrommer and Somayeh Sojoudi are with the Department of Electrical Engineering and Computer Sciences at the University of California, Berkeley. Email: sam.pfrommer@berkeley.edu, sojoudi@berkeley.edu

offline policy under this framework. Furthermore, they show that the time-averaged regret of the blind online policy with respect to the optimal offline policy grows linearly in the time horizon. We extend these results to the sparse-disturbance setting with a bound that is independent of the time horizon and varies quadratically with the number of disturbances and their magnitude. Our complete contributions are summarized in II-A.

### A. Notation

The spectral norm of a matrix is denoted by  $\rho(\cdot)$ , and the  $l_2$  norm of a vector is denoted by  $\|\cdot\|$ . We let  $M \succ 0$  and  $M \succeq 0$  indicate that  $M$  is positive definite and positive semidefinite, respectively. The minimum eigenvalue of a matrix is given by  $\lambda_{\min}(\cdot)$ . An upper bound on the norm of a collection of matrices or vectors is generally denoted using a hat; e.g.,  $\hat{w} \geq \|w_k\| \forall k$ . We denote the set of integers by  $\mathbb{Z}$ , the set of nonnegative integers by  $\mathbb{Z}_+$ , the set of real numbers by  $\mathbb{R}$ , and the expectation of a random variable by  $\mathbb{E}$ . The set of integers between  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z}$  inclusive is denoted by  $[a \dots b]$ , with  $(a \dots b)$  corresponding to the open integer interval omitting  $a$  and  $b$ .

## II. PROBLEM STATEMENT

We consider the control of a linear time-invariant system that evolves according to

$$x_{t+1} = Ax_t + Bu_t + d_t, \quad t = 0, 1, \dots, T-1,$$

where  $A \in \mathbb{R}^{n \times n}$  and  $B \in \mathbb{R}^{n \times m}$  are system matrices,  $x_t \in \mathbb{R}^n$  is the system state,  $u_t \in \mathbb{R}^m$  is the control input,  $d_t \in \mathbb{R}^n$  is an external disturbance, and  $T$  is the time horizon. Moreover, we focus on the scenario where the disturbances  $d_t$  are *sparse*; i.e.,  $d_t \neq 0$  if and only if  $t \in D$ , for some index set  $D = \{t_1, t_2, \dots, t_{|D|}\}$ , where  $|D|$  denotes the cardinality of  $D$ . The nonzero disturbances are given by  $d_{t_k} = w_k$ ,  $k \in 1, \dots, |D|$ , and are bounded in  $l_2$  norm by  $\hat{w} \geq \|w_k\| \forall k$ .

The objective of our policies is to minimize the cost

$$\mathbb{E}_{d_0, \dots, d_{T-1}} \left( x_T^T Q_T x_T + \sum_{t=0}^{T-1} [x_t^T Q x_t + u_t^T R u_t] \right), \quad (1)$$

where  $Q_T, Q \in \mathbb{R}^{n \times n}$  are positive semidefinite and  $R \in \mathbb{R}^{m \times m}$  is positive definite. We compare the following three policies in this work:

- 1) The **blind online policy** executes standard LQR control assuming no disturbances; i.e., assuming  $d_t = 0$  for all  $t$ , even though this assumption may not hold. This is the same policy that would be executed under the typical condition that disturbances  $d_t$  are independent with zero mean. It is well-known that that the optimal disturbance-free policy is a linear controller of the form  $u_t = -K_t x_t$ , for  $t = [0 \dots T)$ , where

$$K_t = (B^T P_{t+1} B + R)^{-1} B^T P_{t+1} A, \quad (2)$$

and the sequence  $P_t$  arises from solving the discrete-time Riccati equation

$$P_t = A^T (P_{t+1} - P_{t+1} B (B^T P_{t+1} B + R)^{-1} B^T P_{t+1}) A + Q, \quad (3)$$

with  $P_T = Q_T$  [23, 24].

- 2) The **disturbance-aware policy** has knowledge of the disturbances  $w_k$  and their ordering but is unaware of their exact locations in time. More specifically, at time step  $t$ , the policy is aware of potential future disturbances  $w_{k'}, \dots, w_{|D|}$ , where  $k'$  is the smallest  $k$  such that  $t_k > t$ . Instead of knowing the precise disturbance locations  $t_k$ , the policy is given access to a probabilistic model of a disturbance occurring at time step  $t$  when there are  $k$  disturbances remaining. We denote this probability as  $p_t^k$ . One simple probabilistic model is the uniform conditional model  $p_t^k = k/(T-t)$ , which assumes that the remaining disturbances are distributed uniformly over the time horizon. The form of the policy is derived explicitly in Section III-A.
- 3) The **optimal offline policy** has complete knowledge of all disturbances  $d_t$ . Under this setting, the optimal control and cost have the following structure, first derived in [22]:

$$u_t^* = -K_t x_t - (B^T P_{t+1} B + R)^{-1} B^T (P_{t+1} d_t + 1/2 v_{t+1}), \quad (4a)$$

$$V_t(x) = x^T P_t x + v_t^T x + q_t, \quad (4b)$$

$$v_t = 2A^T S_t d_t + A^T S_t P_{t+1}^{-1} v_{t+1}, \quad (4c)$$

$$q_t = q_{t+1} + d_t^T S_{t+1} d_t + v_{t+1}^T P_{t+1}^{-1} S_t d_t - 1/4 v_{t+1}^T B (B^T P_{t+1} B + R)^{-1} B^T v_{t+1}, \quad (4d)$$

$$S_t := P_{t+1} - P_{t+1} B (B^T P_{t+1} B + R)^{-1} B^T P_{t+1}, \quad (4e)$$

where  $V_t(x)$  represents the cost-to-go of a state  $x$  at time  $t$ , and  $v_t \in \mathbb{R}^n$ ,  $q_t \in \mathbb{R}$  are recurrences that depend only on the noise  $d_t$  and are initialized to  $v_T = 0$ ,  $q_T = 0$ . We note that the optimal control is determined by the optimal online policy action and a counterfactual second term depending exclusively on future disturbances.

### A. Contributions

We begin by deriving the optimal structure for the disturbance-aware policy in Section III-A, which involves a two-dimensional recurrence over the time step  $t$  and the number of remaining disturbances  $k$ . This holds for any arbitrary disturbance sequence. Unlike the optimal offline policy originally considered by [22], we only assume probabilistic knowledge about the possibility of a disturbance. In practice, future disturbances and their probabilities could be inferred from data using techniques similar to the fault prediction literature, although this is outside the scope of our work.

Section III-B establishes that under mild conditions, the disturbance-aware policy converges to the blind online policy in the infinite-horizon case if the number of disturbances grows sublinearly in the time horizon. This formalizes the intuition that as disturbances become more sparse, without exact knowledge of disturbance times, the disturbance-aware policy eventually takes the same actions as the blind policy. We note that this is not the case for the optimal offline policy,

which can leverage its precise knowledge of disturbance times to modify its control strategy.

Section IV provides a regret bound between the blind online policy and the optimal offline policy. Specifically, we show that the regret grows quadratically in the number of disturbances and in their magnitude. We accomplish this via an intermediate reduction to the cost of the blind online policy without disturbances, which is also of independent interest. This bound is relevant in a practical setting where naive LQR controllers are deployed in a real-world environment with sparse disturbances.

### III. THE DISTURBANCE-AWARE POLICY

We derive the structure of the disturbance-aware policy, which takes the form of a two-dimensional recursion. We then show that under a particular sparsity condition the optimal control action converges to that of the blind online policy in the infinite-horizon case. For notational convenience, in this section disturbances  $d_k = w_k$  are indexed in reverse chronological order, such that  $t_1 \geq t_2 \geq \dots \geq t_{|D|}$ .

#### A. Disturbance-aware policy structure

**Theorem 1.** *The form of the optimal disturbance-aware policy described in Section II is given by*

$$\begin{aligned} (u_t^k)^* &= -K_t x_t - (R + B^T P_{t+1} B)^{-1} B^T (p_t^k P_{t+1} w_k + \tilde{r}_{t+1}^k), \\ J_t^k(x) &= x^T P_t x + 2r_t^{kT} x + c_t^k, \end{aligned}$$

$$\begin{aligned} r_t^k &= A^T (I - F_t P_{t+1})^T (\tilde{r}_{t+1}^k + p_t^k P_{t+1} w_k), \\ c_t^k &= \tilde{c}_{t+1}^k - (\tilde{r}_{t+1}^k + p_t^k P_{t+1} w_k)^T F_t (\tilde{r}_{t+1}^k + p_t^k P_{t+1} w_k) \\ &\quad + p_t^k w_k^T P_{t+1} w_k + 2p_t^k r_{t+1}^{k-1} w_k, \end{aligned} \quad (5)$$

$$\begin{aligned} F_t &:= B(R + B^T P_{t+1} B)^{-1} B^T, \\ \tilde{r}_t^k &= \bar{p}_t^k r_t^k + p_t^k r_t^{k-1}, \\ \tilde{c}_t^k &= \bar{p}_t^k c_t^k + p_t^k c_t^{k-1}, \end{aligned}$$

where  $P_t$  is obtained from  $P_{t+1}$  via the Riccati sequence (3) and  $r_t^k \in \mathbb{R}^n$  and  $c_t^k \in \mathbb{R}$  are recurrences indexed by both  $t \in [0 \dots T]$  and  $k \in [0 \dots |D|]$ , initialized to  $P_T = Q_T$ ,  $r_T^k = 0$ , and  $c_T^k = 0$  for all  $k$ . Here  $(u_t^k)^*$  is the expectation-optimal action at time step  $t$  with  $k$  possible future disturbances.

*Sketch of proof.* The derivation of the optimal disturbance-aware policy mirrors the classic dynamic programming approach [23]. Our induction hypothesis is that the cost at time step  $t+1$  with  $k$  possible future disturbances is of the form

$$J_{t+1}^k(x) = x^T P_{t+1} x + 2r_{t+1}^{kT} x + c_{t+1}^k.$$

We proceed backwards by induction, optimizing for the expected cost-minimizing control

$$J_t^k(x) = \min_u \left\{ x^T Q x + u^T R u + \bar{p}_t^k J_{t+1}^k(Ax + Bu) + p_t^k J_{t+1}^{k-1}(Ax + Bu + w_k) \right\},$$

where  $\bar{p}_t^k = 1 - p_t^k$ . The last two terms represent the expected value of the cost-to-go, which is decomposed over the probability of a disturbance at that time step. Since we

assume access to the probabilistic model  $p_t^k$  and disturbances  $w_k$ , this recursion can be evaluated. Paralleling derivations in [22], we expand  $J_{t+1}^k$  and  $J_{t+1}^{k-1}$  and collect terms to write

$$J_t^k(x) = \min_u \begin{bmatrix} u \\ a \end{bmatrix}^T \begin{bmatrix} R + B^T P_{t+1} B & z \\ z^T & M \end{bmatrix} \begin{bmatrix} u \\ a \end{bmatrix} + \tilde{c}_{t+1}^k,$$

with the following additional definitions:

$$\begin{aligned} a &= [x^T \quad w_k^T \quad r_{t+1}^{kT} \quad r_{t+1}^{k-1T}]^T, \\ z &= [B^T P_{t+1} A \quad p_t^k B^T P_{t+1} \quad \bar{p}_t^k B^T \quad p_t^k B^T], \\ M &= \begin{bmatrix} Q + A^T P_{t+1} A & A^T P_{t+1} & \bar{p}_t^k A^T & p_t^k A^T \\ P_{t+1} A & p_t^k P_{t+1} & 0 & p_t^k I \\ \bar{p}_t^k A & 0 & 0 & 0 \\ p_t^k A & p_t^k I & 0 & 0 \end{bmatrix}. \end{aligned}$$

We now apply the Schur complement to write the optimal control and cost in closed form, attaining the form specified in the theorem statement.  $\square$

As in [22], the optimal control is affine in  $x$  with the same feedback matrix (2) as the blind online policy and an additional term that depends on future disturbances and the probability model. Note that  $(u_t^k)^*$  now depends on both  $k$  and  $t$ .

#### B. Convergence to the blind online policy

We show that under mild conditions on the system and probability model, the optimal disturbance-aware policy derived in the previous section converges to the blind online policy if the number of disturbances grows sublinearly in the time horizon.

**Assumption 1.** *The pair  $(A, B)$  is controllable and  $Q$  can be decomposed as  $Q = LL^T$  for some matrix  $L$  such that  $(A, L)$  is observable. Moreover, the Riccati sequence  $P_t$  is stabilizing such that*

$$\rho(A - BK_t) < 1 - \gamma$$

for all  $t$  and some  $\gamma > 0$ , where  $K_t$  is the feedback matrix (2) in the standard LQR controller.

Controllability and observability are standard assumptions in the classic LQR derivation and are sufficient to show that the controller converges to a stabilizing solution. Assumption 1 also stipulates that intermediate iterations of the Riccati equation produce stabilizing controllers. This is immediately satisfied for many choices of the terminal cost  $Q_T$  [25, 26]. Additionally, the Riccati sequence is known to converge exponentially to a stable solution [27], and hence the number of intermediate iterations violating Assumption 1 is generally negligible. The positive constant  $\gamma$  simply quantifies the level of stability.

**Assumption 2.** *The disturbance probability  $p_t^k$  approaches zero if the number of disturbances  $k$  grows sublinearly in  $t$ . Formally, let  $k_i$  be a monotonically increasing sequence in  $\mathbb{Z}_+$  and  $t_i$  be a monotonically strictly decreasing sequence in  $(-\infty \dots T]$ . Then if  $k_i/t_i \rightarrow 0$  as  $i \rightarrow \infty$ , the disturbance probability  $p_{t_i}^{k_i} \rightarrow 0$ .*

Note that in order to show infinite-horizon convergence of the disturbance-aware policy, we adopt a slight abuse of notation by letting  $t \rightarrow -\infty$  with a fixed final time  $T$ . This is a standard approach in LQR derivations; see [23] for reference. Assumption 2 is satisfied by most natural disturbance priors. For instance, the uniform distribution  $p_t^k = k/(T-t)$  decays to zero if  $t \rightarrow -\infty$  faster than  $k \rightarrow \infty$ . We now introduce a lemma before presenting the main result of this section.

**Lemma 1.** *Under Assumption 1, we have that  $\|r_t^k\| \leq \hat{r}$  for all  $k \in \mathbb{Z}_+$  and  $t \in (-\infty \dots T]$ , where  $\hat{r}$  is some scalar.*

*Proof.* The recurrence for  $r_t^k$  can be written as

$$r_t^k = U_t \tilde{r}_{t+1}^k + p_t^k H_t w_k, \quad (6)$$

with

$$\begin{aligned} U_t &= A^\top (I - F_t P_{t+1})^\top = (A - BK_t)^\top, \\ H_t &= A^\top (I - F_t P_{t+1})^\top P_{t+1}. \end{aligned}$$

Note that  $U_t$  and  $H_t$  depend only on  $P_t$ . By Assumption 1,  $P_t$  converges to a positive definite solution and therefore  $U_t \rightarrow U^*$  and  $H_t \rightarrow H^*$  where  $\|U_t\| < 1 - \gamma$  and  $\|U^*\| < 1 - \gamma$ .

We now prove the claim by upper bounding a sequence of upper bounds given by  $\hat{r}_t \geq \|r_t^k\| \forall k$ . Since  $r_T^k = 0$  for all  $k$ , we have that  $\hat{r}_T = 0$ . By induction,

$$\begin{aligned} \|r_t^k\| &\leq \|\tilde{r}_{t+1}^k\| \|U_t\| + p_t^k \|w_k\| \|H_t\| \\ &\leq \hat{r}_{t+1} (1 - \gamma) + \hat{w} \hat{H} \\ &= \hat{r}_t, \end{aligned}$$

where  $\hat{r}_t := \hat{r}_{t+1} (1 - \gamma) + \hat{w} \hat{H}$ ,  $\hat{w} \geq \|w_k\|$  for all  $k$  by assumption and  $\hat{H} \geq \|H_t\|$  for all  $t$  by convergence. Since  $\gamma > 0$ ,  $\hat{r}_t$  is a geometrically decaying sequence with a bounded additive term which cannot diverge. Hence,  $\hat{r}_t < \hat{r} \forall t$  for some  $\hat{r}$  and therefore  $\|r_t^k\| < \hat{r}$  for all  $k$  and  $t$ .  $\square$

**Lemma 2.** *Under Assumptions 1 and 2, let  $k_i/t_i \rightarrow 0$  as  $i \rightarrow \infty$  for strictly monotonic sequences  $k_i$  and  $t_i$ . Since only one disturbance can occur on a particular time step, we further assume  $k_i - k_{i-1} \in \{0, 1\} \forall i$ . Then  $\|r_{t_i}^{k_i}\| \rightarrow 0$  as  $i \rightarrow \infty$ .*

*Proof.* Let  $\bar{t}_i = t_{i+1} - t_i$ . Using (6) and expanding  $\tilde{r}_{t_i+1}^{k_i}$  yields

$$r_{t_i}^{k_i} = \bar{p}_{t_i}^{k_i} U_{t_i} r_{t_i+1}^{k_i} + p_{t_i}^{k_i} U_{t_i} r_{t_i+1}^{k_i-1} + p_{t_i}^{k_i} H_{t_i} w_{k_i}. \quad (7)$$

We focus on bounding our two terms  $r_{t_i+1}^{k_i}$  and  $r_{t_i+1}^{k_i-1}$ . By inspection of (6),

$$\begin{aligned} \|r_{t_i+1}^{k_i}\| &\leq (1 - \gamma)^{\bar{t}_i-1} \hat{r} + \sum_{j=1}^{\bar{t}_i-1} p_{t_i+j}^{k_i} (1 - \gamma)^j (\hat{r} + \hat{w} \hat{H}) \\ &\leq (1 - \gamma)^{\bar{t}_i-1} \hat{r} + \hat{p}_i \cdot \frac{\hat{r} + \hat{w} \hat{H}}{\gamma}, \end{aligned}$$

where  $\hat{w} \geq \|w_k\|$  upper bounds the disturbance magnitude,  $\hat{H}$  upper bounds  $\|H_t\|$ ,  $\hat{r}$  is as in Lemma 1, and

$$\hat{p}_i = \max_{j=1, \dots, \bar{t}_i-1} \{p_{t_i+j}^{k_i}\}.$$

It is evident that under Assumption 2 with  $k_i/t_i \rightarrow 0$  that  $\hat{p}_i \rightarrow 0$  as well. Note that we leverage the observation that

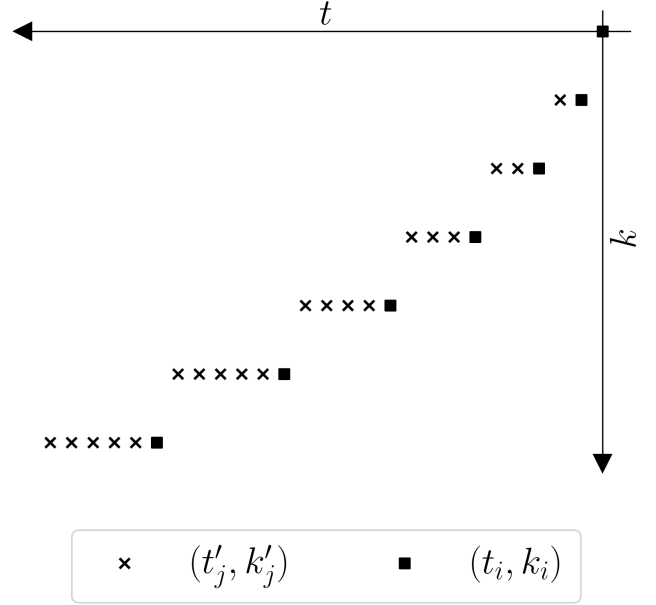


Fig. 1: An illustration of a trajectory disturbance budget  $k$  growing sublinearly in the time horizon. An increase in  $k$  corresponds to a nonzero disturbance in the system dynamics. Lemma 2 shows that along the tuples  $(t_i, k_i)$  demarcated by black squares, the norm of the linear cost coefficient  $\|r_{t_i}^{k_i}\|$  vanishes. Theorem 2 extends this to the intermediate values  $(t'_j, k'_j)$ , and establishes that the disturbance-aware policy converges to the blind online policy.

$\|U_t\| < 1 - \gamma$  as in the proof for Lemma 1. We similarly bound

$$\begin{aligned} \|r_{t_i+1}^{k_i-1}\| &\leq (1 - \gamma)^{\bar{t}_i-1} \|r_{t_i-1}^{k_i-1}\| + \sum_{j=1}^{\bar{t}_i-1} p_{t_i+j}^{k_i-1} (1 - \gamma)^j (\hat{r} + \hat{w} \hat{H}) \\ &\leq (1 - \gamma)^{\bar{t}_i-1} \|r_{t_i-1}^{k_i-1}\| + \hat{p}'_i \cdot \frac{\hat{r} + \hat{w} \hat{H}}{\gamma}, \end{aligned}$$

where

$$\hat{p}'_i = \max_{j=1, \dots, \bar{t}_i-1} \{p_{t_i+j}^{k_i-1}\}.$$

Similarly to  $\hat{p}_i$ , as  $i \rightarrow \infty$  we have  $\hat{p}'_i \rightarrow 0$ . We can now bound the expression for  $r_{t_i}^{k_i}$  in (7):

$$\|r_{t_i}^{k_i}\| \leq (1 - \gamma)^{\bar{t}_i} \|r_{t_i-1}^{k_i-1}\| + (\hat{p}_i + \hat{p}'_i) \frac{\hat{r} + \hat{w} \hat{H}}{\gamma} + p_{t_i}^{k_i} \hat{w} \hat{H}.$$

We now have a recurrence for  $\|r_{t_i}^{k_i}\|$  in terms of  $\|r_{t_i-1}^{k_i-1}\|$ . Note that since  $\hat{p}_i$ ,  $\hat{p}'_i$ , and  $p_{t_i}^{k_i}$  all decay to zero, this is an exponentially decaying recurrence with an additional term that also decays to zero, and hence  $\|r_{t_i}^{k_i}\| \rightarrow 0$ .  $\square$

Note that Lemma 2 only shows that the norm of the linear cost coefficient  $\|r_{t_i}^{k_i}\| \rightarrow 0$  for a subsequence of the indices that would be observed for a full trajectory. We now need to include the intermediate time steps where a disturbance does not incur, as illustrated in Figure 1. The following

theorem makes this rigorous and presents the main result of this section.

**Theorem 2.** *Under the conditions of Lemma 2, we relax strict monotonicity to include intermediate time steps and obtain our desired sequences of the form*

$$(t'_j, k'_j) := (t_0, k_0), (t_0 - 1, k_0), \dots, (t_1 + 1, k_0), (t_1, k_1), \dots$$

where with some abuse of notation  $(t'_j, k'_j)$  refers to the  $j$ th pair from the right hand side sequence, with  $j \in \mathbb{Z}_+$ . If  $k_i/t_i \rightarrow 0$  as  $i \rightarrow \infty$ , then  $\|r_{t'_j}^{k'_j}\| \rightarrow 0$  and the disturbance-aware policy converges to the blind online policy.

*Proof.* Lemma 2 gives us that  $\|r_{t_i}^{k_i}\| \rightarrow 0$ . Consider an intermediate term  $\|r_{t_i - t'}^{k_i}\|$  where  $t' < \bar{t}_i$ . Using a similar strategy and notation to the proof of Lemma 2, we can note that

$$\|r_{t_i - t'}^{k_i}\| \leq (1 - \gamma)^{t'} \|r_{t_i}^{k_i}\| + \hat{p}_i \cdot \frac{\hat{r} + \hat{w}\hat{H}}{\gamma}$$

Since  $(1 - \gamma)^{t'} < 1$  and  $\hat{p}_i \rightarrow 0$ , we can upper bound the norm of intermediate terms by the norm of the previous  $\|r_{t_i}^{k_i}\|$  and an additional term that decays to zero as  $k_i/t_i \rightarrow 0$ . Therefore, we have that

$$\|r_{t'_j}^{k'_j}\| \rightarrow 0 \text{ as } j \rightarrow \infty.$$

This holds for an arbitrary sequence where  $k_i/t_i \rightarrow 0$ , and therefore it is easy to show also that

$$\|\tilde{r}_{t'_j}^{k'_j}\| \rightarrow 0 \text{ as } j \rightarrow \infty.$$

Inspection of (5) and noting that  $p_i^{k_i} \rightarrow 0$  yields

$$(u_{t'_j}^{k'_j})^* \rightarrow -K_{t'_j} x_{t'_j},$$

i.e. the disturbance-aware policy converges to the blind online policy for the sequence  $(k'_j, t'_j)$ , completing the proof.  $\square$

Theorem 2 conveys that as long as the number of disturbances grows sublinearly in the time horizon, the disturbance-aware policy converges to the blind online policy. This matches the natural intuition that if disturbances become more sparse, without knowing their exact locations it becomes less cost-effective to mitigate their potential impact by deviating from the blind online policy.

#### IV. BLIND POLICY REGRET

We establish a finite-horizon regret bound between the blind online policy and the optimal offline policy in the presence of sparse disturbances. This is accomplished by an intermediate reduction to the cost of the blind online policy without disturbances. Assumption 2 is not needed in this section, and the intermediate stability requirement in Assumption 1 is required for Theorem 5 but not Theorem 4. We revert the ordering of disturbances  $d_{t_k} = w_k$  to the natural chronological order  $t_1 \leq t_2 \leq \dots \leq t_{|D|}$ .

We let  $J_0^w(x_0)$  denote the cost-to-go under the blind policy for an initial state  $x_0$  with disturbances  $\{w_k\}$  added at times

$\{t_k\}$ ,  $k \in \{0, \dots, |D|\}$ . Similarly,  $J_0(x_0)$  is the cost-to-go of the blind policy *without* disturbances, i.e.  $d_t = 0 \forall t$ . The cost of the optimal offline policy with the disturbance sequence is denoted as  $V_0^w(x_0)$  and given by (4b). We will bound  $J_0^w(x_0) - V_0^w(x_0)$  by a reduction to  $J_0(x_0)$ .

**Lemma 3.** *Under Assumption 1, the Riccati sequence  $P_t$  is bounded such that  $\|P_t\| \leq \hat{P}$  for all  $t \in (-\infty .. T]$  for some constant  $\hat{P} \geq 1$ .*

*Proof.* Under the controllability and observability conditions in Assumption 1, it is well known that the Riccati sequence  $P_t$  converges as  $t \rightarrow -\infty$  [23]. Convergence of the matrix sequence implies convergence of the norm, and convergent sequences are bounded. If this bound is less than 1, we choose  $\hat{P} = 1$  to ensure that  $\hat{P} \geq 1$ .  $\square$

**Remark 1.** *Note that the previous lemma seems stronger than necessary, as in this section we are operating in the finite-horizon domain with  $t \in [0 .. T]$ . However, Lemma 3 is important for establishing that the bound  $\hat{P}$  is independent of the time horizon of the system.*

**Theorem 3.** *Consider the evolution of a trajectory starting from  $x_0$  which is perturbed by  $|D|$  disturbances of magnitude at most  $\hat{w}$ . The regret of the blind online policy compared to the optimal offline policy is bounded by*

$$|J_0^w(x_0) - V_0^w(x_0)| \leq O(|D|\hat{w}\|x_0\|) + O(|D|^2\hat{w}^2),$$

where  $O(\cdot)$  absorbs constants dependent on the dynamics matrices  $A$ ,  $B$  and design matrices  $Q$ ,  $Q_T$ ,  $R$ .

*Proof.* Using the triangle inequality

$$|J_0^w(x_0) - V_0^w(x_0)| \leq |J_0^w(x_0) - J_0(x_0)| + |J_0(x_0) - V_0^w(x_0)|$$

We can now apply Theorem 4 and Theorem 5 to derive

$$\begin{aligned} |J_0^w(x_0) - V_0^w(x_0)| &\leq 2|D|\hat{w}\hat{P}(2\|x_0\| + \hat{w}) \\ &\quad + |D|^2\hat{w}^2(2\hat{P}^2 + 3\hat{P}) \\ &\quad + \frac{|D|^2\hat{w}\hat{P}(3\hat{P}\hat{w} + \gamma^{-2})\|B\|^2}{\lambda_{\min}(R)}, \end{aligned}$$

where  $\gamma$  is as in Assumption 1,  $R$  is the control cost matrix in (1), and  $\hat{P}$  is from Lemma 3. This yields the desired expression as  $\gamma$  and  $\hat{P}$  are given by  $A$ ,  $B$ ,  $Q$ ,  $Q_T$ , and  $R$ .  $\square$

The main utility of Theorem 3 is that the asymptotic suboptimality of the blind online policy can be upper bounded by a quadratic function of  $|D|$  and  $\hat{w}$ . While the quadratic nature of the cost (1) hints at the result, this is nontrivial as the optimal offline policy is counterfactual in that it assumes complete knowledge of all future disturbances. Note that the derived bound has no dependence on the time horizon  $T$ . We derive the result by reducing to the cost  $J_0(x_0)$  of the blind online policy with no disturbances, and in doing so establish Theorems 4 and 5, which are also interesting standalone results.

### A. Blind policy additional cost bound

Consider the Riccati sequence  $P_0, \dots, P_T$ , with corresponding feedback matrices  $K_t$  as in (2). The cost-to-go of an initial state  $x_0$  under the blind policy with no disturbances is  $J_0(x_0) = x_0^\top P_0 x_0$ . We will bound the additional cost incurred by  $|D|$  disturbances of magnitude at most  $\hat{w}$  under the blind policy  $u_t = -K_t x_t$ .

**Theorem 4.** *Consider the blind online LQR policy for a controllable and observable system which is perturbed by  $|D|$  disturbances of bounded norm  $\hat{w}$  over a finite time horizon. The incurred cost difference compared to the unperturbed trajectory starting at the same initial state  $x_0$  is bounded by*

$$|J_0^w(x_0) - J_0(x_0)| \leq 2|D|\hat{w}\hat{P}(\|x_0\| + \hat{w} + |D|\hat{w}\hat{P}),$$

where  $\hat{P}$  is from Lemma 3.

*Proof.* Consider the perturbed trajectory  $x_t$ , with disturbances  $w_1, \dots, w_{|K|}$  being added at time steps  $t_1 \leq \dots \leq t_{|K|}$ . For notational simplicity, we let  $t'_k = t_k + 1$  and  $y_{t'_k} = x_{t'_k} - w_k$  with  $y_0 = x_0$ ; i.e.,  $y_{t'_k}$  represents what the state would have been at time step  $t_k + 1$  without the disturbance  $w_k$  at the previous time step. Using the cost-to-go, we can write the additional cost of the perturbed trajectory as

$$\begin{aligned} |J^w(x_0) - J(x_0)| &= \left| \sum_{t_k \in D} \left[ -y_{t'_k}^\top P_{t'_k} y_{t'_k} + x_{t'_k}^\top P_{t'_k} x_{t'_k} \right] \right| \\ &= \left| \sum_{t_k \in D} \left[ 2y_{t'_k}^\top P_{t'_k} w_k + w_k^\top P_{t'_k} w_k \right] \right| \\ &\leq 2|D|\hat{w}^2\hat{P} + 2\hat{w} \sum_{t_k \in D} \|y_{t'_k}^\top P_{t'_k}\|. \end{aligned} \quad (8)$$

We now wish to upper bound  $\|y_{t'_k}^\top P_{t'_k}\|$ . We first establish upper bounds  $y_{t'_k}^\top P_{t'_k} y_{t'_k} \leq b_k$  for a recurrence  $b_k$ . Proceeding by induction, let  $b_0 = x_0^\top P_0 x_0$ . The induction hypothesis states

$$y_{t'_k}^\top P_{t'_k} y_{t'_k} \leq b_k,$$

which also implies that

$$\|y_{t'_k}^\top P_{t'_k}\| \leq \sqrt{\hat{P}} \cdot \sqrt{y_{t'_k}^\top P_{t'_k} y_{t'_k}} = \sqrt{\hat{P}b_k}.$$

Therefore, with some manipulation we have that

$$x_{t'_k}^\top P_{t'_k} x_{t'_k} = (y_{t'_k} + w_k)^\top P_{t'_k} (y_{t'_k} + w_k) \leq b_k + 2\hat{w}\hat{P}^{3/2}\sqrt{b_k} + \hat{w}^2\hat{P}.$$

Since no disturbances act between  $x_{t'_k}$  and  $y_{t'_{k+1}}$ , by optimal control the cost-to-go must decrease and we have

$$y_{t'_{k+1}}^\top P_{t'_{k+1}} y_{t'_{k+1}} \leq x_{t'_k}^\top P_{t'_k} x_{t'_k} \leq b_k + 2\hat{w}\hat{P}^{3/2}\sqrt{b_k} + \hat{w}^2\hat{P} := b_{k+1}.$$

This is a nonlinear recurrence, for which closed-form solutions are difficult to find. We make the simplification  $\hat{w}^2\hat{P} \leq \hat{w}^2\hat{P}^3$  since  $\hat{P} \geq 1$  by Lemma 3; this is a small concession to our bound since  $\hat{P}$  is a fixed, precomputed quantity. The recurrence now reads

$$\begin{aligned} b_{k+1} &= b_k + 2\sqrt{\hat{w}^2\hat{P}^3 b_k} + \hat{w}^2\hat{P}^3 \\ &= \left( \sqrt{b_k} + \sqrt{\hat{w}^2\hat{P}^3} \right)^2. \end{aligned}$$

Square rooting both sides yields

$$\sqrt{b_k} = \sqrt{b_0} + k\sqrt{\hat{w}^2\hat{P}^3}.$$

We can now bound our original term of interest

$$\|y_{t'_k}^\top P_{t'_k}\| \leq \sqrt{\hat{P}}\sqrt{b_k} \leq \sqrt{\hat{P}} \cdot \left( \sqrt{x_0^\top P_0 x_0} + k\sqrt{\hat{w}^2\hat{P}^3} \right).$$

Noting that this expression is maximized by  $k = |D|$  and substituting into (8) completes the proof.  $\square$

Theorem 4 yields an easily-computable bound for the maximum incurable difference between the cost of a system under nominal, no-disturbance operation and the cost with the inclusion of sparse, unexpected disturbances. The bound scales quadratically in both  $|D|$  and  $\hat{w}$ , while the dependence on the initial state magnitude  $\|x_0\|$  is merely linear.

### B. Optimal offline policy cost bound

Here we desire to bound the difference between the cost of the blind policy without disturbances to the optimal online policy with disturbances.

**Theorem 5.** *Under Assumption 1, consider  $|D|$  disturbances over a finite time horizon, each with norm bounded by  $\hat{w}$ . The cost difference between the optimal online policy without disturbances and the optimal offline policy with disturbances is bounded by*

$$\begin{aligned} |J_0(x_0) - V_0^w(x_0)| &\leq 2\|x_0\||D|\hat{P}\hat{w} + |D|^2\hat{w}\hat{P} \left( 3\hat{w} + \frac{(3\hat{P}\hat{w} + \gamma^{-2})\|B\|^2}{\lambda_{\min}(R)} \right), \end{aligned}$$

where  $\gamma$  is as in Assumption 1,  $R$  is the control cost matrix in (1), and  $\hat{P}$  is from Lemma 3.

*Proof.* Since  $J_0(x_0) = x_0^\top P_0 x_0$ , we have

$$|J_0(x_0) - V_0^w(x_0)| \leq |v_0^\top x_0| + |q_0|. \quad (9)$$

We will bound each of these terms individually.

*Bounding  $|v_0^\top x_0|$ :* The structure of (4c) yields

$$v_0 = \sum_{t_k \in D} \left( \prod_{t=0}^{t_k-1} A^\top S_t P_{t+1}^{-1} \right) 2A^\top S_{t_k} w_k.$$

Note that  $P_{t+1}^{-1} S_t A = A - BK_t$ , therefore it follows from Assumption 1 that  $\rho(A^\top S_t P_{t+1}^{-1}) < 1 - \gamma \forall t$ . We now have

$$\begin{aligned} |v_0^\top x_0| &\leq \|x_0\| \cdot \sum_{t_k \in D} \|2A^\top S_{t_k} w_k\| \\ &= 2\|x_0\| \sum_{t_k \in D} \|A^\top S_{t_k} P_{t_k+1}^{-1}\| \|P_{t_k+1} w_k\| \\ &\leq 2\|x_0\||D|\hat{P}\hat{w}. \end{aligned} \quad (10)$$

*Bounding  $|q_0|$ :* The structure of the recurrence (4d) and the observation that  $d_t = 0$  if  $t \notin D$  yields

$$|q_0| \leq \sum_{t_k \in D} \|w_k^\top S_{t_k+1} w_k\| \quad (11a)$$

$$+ \sum_{t_k \in D} \|v_{t_k+1}^\top P_{t_k+1}^{-1} S_{t_k} w_k\| \quad (11b)$$

$$+ \sum_{t=0}^T 1/4 \|v_{t+1}\|^2 \|B(B^\top P_{t+1} B + R)^{-1} B^\top\|. \quad (11c)$$

We will bound (11a), (11b), and (11c) individually. Regarding (11a), we can write:

$$\begin{aligned} \sum_{t_k \in D} \|w_k^\top S_{t_k+1} w_k\| &\leq |D| \hat{w}^2 \|S_t\| \\ &\leq |D| \hat{w}^2 \hat{P} \|I - B(B^\top P_{t+1} B + R)^{-1} B^\top P_{t+1}\| \\ &\leq |D| \hat{w}^2 \hat{P} (1 + \|B\|^2 \hat{P} \|(B^\top P_{t+1} B + R)^{-1}\|) \\ &\leq |D| \hat{w}^2 \hat{P} \left(1 + \frac{\|B\|^2 \hat{P}}{\lambda_{\min}(R)}\right). \end{aligned}$$

The last step follows from  $R \succ 0$  and  $B^\top P_{t+1} B \succeq 0$ . We can now bound (11b):

$$\begin{aligned} \sum_{t_k \in D} \|v_{t_k+1}^\top P_{t_k+1}^{-1} S_{t_k} w_k\| &\leq \sum_{t_k \in D} \|v_{t_k+1}\| \hat{w} \left(1 + \frac{\|B\|^2 \hat{P}}{\lambda_{\min}(R)}\right) \\ &\leq 2|D|^2 \hat{w}^2 \hat{P} \left(1 + \frac{\|B\|^2 \hat{P}}{\lambda_{\min}(R)}\right). \end{aligned}$$

By noting that the previous  $\|v_0\|$  bound also holds similarly for any  $\|v_t\|$ . Finally, (11c) can be manipulated as:

$$\begin{aligned} &\sum_{t=0}^T \|v_{t+1}\|^2 \|B(B^\top P_{t+1} B + R)^{-1} B^\top\| \\ &\leq \frac{\|B\|^2}{\lambda_{\min}(R)} \sum_{t=0}^T \|v_{t+1}\|^2 \\ &\leq \frac{\|B\|^2}{\lambda_{\min}(R)} \left(\sum_{t=0}^T \|v_{t+1}\|\right)^2 \\ &\leq \frac{\|B\|^2}{\lambda_{\min}(R)} \left(\sum_{t=0}^T \sum_{\substack{t_k \in D \\ t_k > t}} \left\| \left(\prod_{t'=t}^{t_k-1} A^\top S_{t'} P_{t'+1}^{-1}\right) 2A^\top S_{t_k} w_k \right\|\right)^2. \end{aligned}$$

Recalling that  $\|A^\top S_{t'} P_{t'+1}^{-1}\| \leq 1 - \gamma$  by Assumption 1 yields

$$\begin{aligned} &\leq \frac{4\|B\|^2}{\lambda_{\min}(R)} \left(\sum_{t=0}^T \sum_{\substack{t_k \in D \\ t_k > t}} (1-\gamma)^{t_k-t} \left\|A^\top S_{t_k} P_{t_k+1}^{-1} P_{t_k+1} w_k\right\|\right)^2 \\ &\leq \frac{4\hat{P}\hat{w}\|B\|^2}{\lambda_{\min}(R)} \left(\sum_{t=0}^T \sum_{\substack{t_k \in D \\ t_k > t}} (1-\gamma)^{t_k-t}\right)^2 \\ &\leq \frac{4\hat{P}\hat{w}\|B\|^2}{\lambda_{\min}(R)} \left(\sum_{t_k \in D} \sum_{t=0}^{t_k} (1-\gamma)^{t_k-t}\right)^2 \\ &\leq \frac{4\hat{P}\hat{w}\|B\|^2}{\lambda_{\min}(R)} \left(\frac{|D|}{1-(1-\gamma)}\right)^2 \\ &\leq \frac{4\hat{P}\hat{w}|D|^2\|B\|^2}{\gamma^2\lambda_{\min}(R)}. \end{aligned}$$

We combine bounds for (11a), (11b), (11c), reintroducing

the factor  $1/4$ , to obtain

$$\begin{aligned} |q_0| &\leq (|D| + 2|D|^2) \hat{w}^2 \hat{P} \left(1 + \frac{\|B\|^2 \hat{P}}{\lambda_{\min}(R)}\right) + \frac{\hat{P}\hat{w}|D|^2\|B\|^2}{\gamma^2\lambda_{\min}(R)} \\ &\leq 3|D|^2 \hat{w}^2 \hat{P} \left(1 + \frac{\|B\|^2 \hat{P}}{\lambda_{\min}(R)}\right) + \frac{\hat{P}\hat{w}|D|^2\|B\|^2}{\gamma^2\lambda_{\min}(R)} \\ &\leq |D|^2 \hat{w} \hat{P} \left(3\hat{w} + \frac{(3\hat{P}\hat{w} + \gamma^{-2})\|B\|^2}{\lambda_{\min}(R)}\right). \end{aligned}$$

We combine this bound on  $|q_0|$  with the bound (10) for  $|v_0^\top x_0|$  to yield the result.  $\square$

## V. EXPERIMENTS

We illustrate our theoretical results on a planar double integrator system with the state

$$x = [y \quad \dot{y} \quad z \quad \dot{z}]^\top,$$

for horizontal position  $y$  and vertical position  $z$ . The dynamics and cost matrices are as follows:

$$A := \begin{bmatrix} 1 & \Delta t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \Delta t \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B := \begin{bmatrix} 0 & 0 \\ \Delta t & 0 \\ 0 & 0 \\ 0 & \Delta t \end{bmatrix},$$

$$Q = Q_T := \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 10^{-3} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 10^{-3} \end{bmatrix}, \quad R := \begin{bmatrix} 10^{-2} & 0 \\ 0 & 10^{-2} \end{bmatrix}.$$

We evaluate the blind, disturbance-aware, and optimal offline policies from the initial condition  $x_0 = [1, 0, 1, 0]$ . For simplicity of visualization, we consider disturbances drawn uniformly from the sphere with radius  $\hat{w} = 0.3$  with no velocity components. The time step  $\Delta t$  is 0.005. The disturbance-aware policy is provided the uniform disturbance probability model  $p_t^k = k/(T-t)$ .

Figure 2a shows example trajectories for the blind, disturbance-aware, and optimal offline policies with a single disturbance. The optimal offline policy anticipates the disturbance by preemptively steering the trajectory further downwards, while the disturbance-aware trajectory does the same but more cautiously since it does not know the precise disturbance location. Figure 2b shows the norm of the difference between the first action taken by the disturbance-aware policy ( $u_0^{da}$ ) and blind policy ( $u_0^b$ ) for various time horizons and disturbances. As expected from Theorem 2, as the time horizon increases or disturbance budget decreases, the actions of the disturbance-aware policy approach those of the blind policy.

## VI. CONCLUSION

This paper examines the problem of LQR control with bounded sparse perturbations. We derive the structure of the disturbance-aware policy, which knows the values of future disturbances but only has probabilistic knowledge of their locations in time. Under the condition that the number of disturbances grows sublinearly in the time horizon, we show

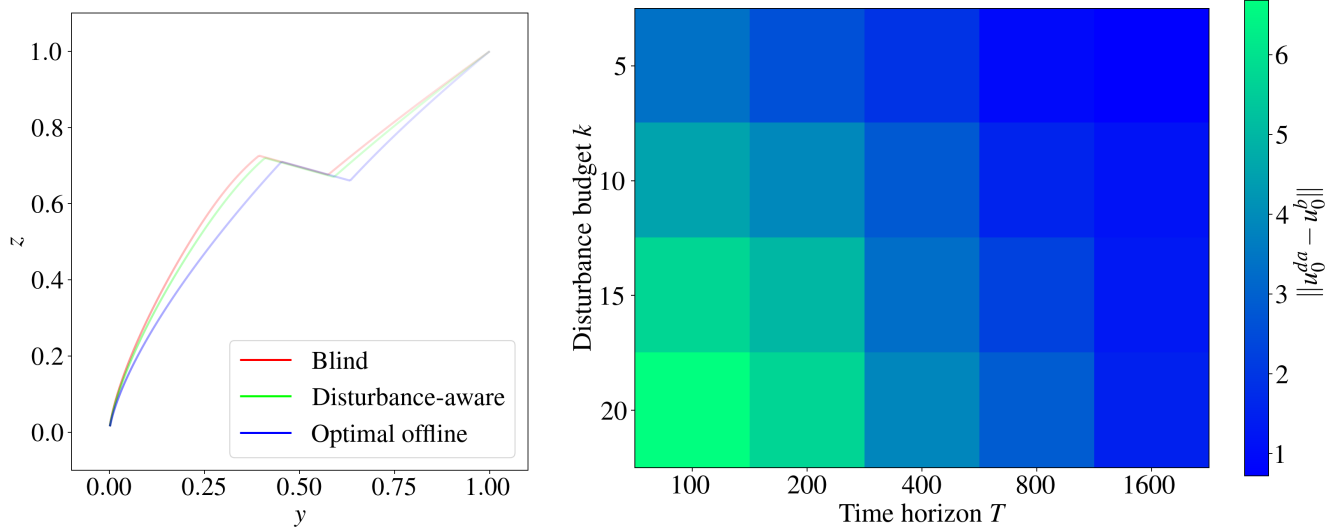


Fig. 2: (a) Example trajectories for the system in Section V. (b)  $\ell_2$  distance between the first action taken by the disturbance-aware policy ( $u_0^{da}$ ) and blind policy ( $u_0^b$ ).

that the disturbance-aware policy converges to the blind online policy. Section IV examines the regret between the blind online policy and the optimal offline policy via a reduction to the cost of the blind online policy without disturbances. The regret bound is shown to scale quadratically in the number of disturbances and their magnitude, but only linearly in the norm of the initial state. We conclude with some synthetic experiments illustrating our findings.

#### REFERENCES

- [1] Hamza Fawzi, Paulo Tabuada, and Suhas Diggavi. “Secure estimation and control for cyber-physical systems under adversarial attacks”. In: *IEEE Transactions on Automatic control* 59.6 (2014), pp. 1454–1467.
- [2] An-Yang Lu and Guang-Hong Yang. “Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer”. In: *Information sciences* 417 (2017), pp. 454–464.
- [3] Sze Zheng Yong, Ming Qing Foo, and Emilio Frazzoli. “Robust and resilient estimation for Cyber-Physical Systems under adversarial attacks”. In: *2016 American Control Conference (ACC)* (2016), pp. 308–315.
- [4] Yilin Mo and Bruno Sinopoli. “On the Performance Degradation of Cyber-Physical Systems Under Stealthy Integrity Attacks”. In: *IEEE Transactions on Automatic Control* 61 (2016), pp. 2618–2624.
- [5] Olugbenga Moses Anubi, Lalit K. Mestha, and Hema Kumari Achanta. “Robust Resilient Signal Reconstruction under Adversarial Attacks”. In: *arXiv: Optimization and Control* (2018).
- [6] Chun-Hua Xie and Guang-Hong Yang. “Secure estimation for cyber-physical systems under adversarial actuator attacks”. In: *IET Control Theory & Applications* 11.17 (2017), pp. 2939–2946.
- [7] Jingyang Lu and Ruixin Niu. “Sparse attacking strategies in multi-sensor dynamic systems maximizing state estimation errors”. In: *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2016, pp. 3151–3155. DOI: 10.1109/ICASSP.2016.7472258.
- [8] Ikumi Banno et al. “Data-Driven Sparse Event-Triggered Control of Unknown Systems”. In: *2021 American Control Conference (ACC)*. IEEE. 2021, pp. 3392–3397.
- [9] Tom Gommans and Maurice Heemels. “Resource-aware MPC for constrained nonlinear systems: A self-triggered control approach”. In: *Systems & Control Letters* 79 (2015), pp. 59–67.
- [10] Yuanxin Li and Guanghong Yang. “Model-Based Adaptive Event-Triggered Control of Strict-Feedback Nonlinear Systems”. In: *IEEE Transactions on Neural Networks and Learning Systems* 29 (2018), pp. 1033–1045.
- [11] Florian Brunner, Maurice Heemels, and Frank Allgower. “Dynamic thresholds in robust event-triggered control for discrete-time linear systems”. In: *2016 European Control Conference (ECC)*. IEEE. 2016, pp. 923–988.
- [12] John White and Jason Speyer. “Detection filter design: Spectral theory and algorithms”. In: *IEEE Transactions on Automatic Control* 32.7 (1987), pp. 593–603.
- [13] Rolf Isermann. “Process fault detection based on modeling and estimation methods-A survey”. In: *automatica* 20.4 (1984), pp. 387–404.
- [14] Ricardo Sanz, Pedro Garcia, and Pedro Albertos. “Enhanced disturbance rejection for a predictor-based control of LTI systems with input delay”. In: *Automatica* 72 (2016), pp. 205–208.
- [15] Jia Cai, Hasan Ferdowsi, and Jagannathan Sarangapani. “Model-based fault detection, estimation, and prediction for a class of linear distributed parameter systems”. In: *Automatica* 66 (2016), pp. 122–131.
- [16] Zhang Zhengdao and Hu Shousong. “A new method for fault prediction of model-unknown nonlinear system”. In: *Journal of the Franklin Institute* 345.2 (2008), pp. 136–153.
- [17] Han Feng and Javad Lavaei. “Learning of dynamical systems under adversarial attacks”. In: *2021 60th IEEE Conference on Decision and Control (CDC)*. IEEE. 2021, pp. 3010–3017.
- [18] Salar Fattahi and Somayeh Sojoudi. “Data-driven sparse system identification”. In: *2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE. 2018, pp. 462–469.
- [19] Salar Fattahi and Somayeh Sojoudi. “Sample complexity of sparse system identification problem”. In: *arXiv preprint arXiv:1803.07753* (2018).
- [20] Naman Agarwal et al. “Online control with adversarial disturbances”. In: *International Conference on Machine Learning*. PMLR. 2019, pp. 111–119.
- [21] Elad Hazan, Sham M. Kakade, and Karan Singh. “The Nonstochastic Control Problem”. In: *ALT*. 2020.
- [22] Gautam Goel and Babak Hassibi. “The power of linear controllers in LQR control”. In: *arXiv preprint arXiv:2002.02574* (2020).
- [23] Dimitri Bertsekas. *Dynamic programming and optimal control: Volume I*. Vol. 1. Athena scientific, 2012.
- [24] Rudolf Emil Kalman et al. “Contributions to the theory of optimal control”. In: *Bol. soc. mat. mexicana* 5.2 (1960), pp. 102–119.
- [25] C.E. De Souza. “On stabilizing properties of solutions of the Riccati difference equation”. In: *IEEE Transactions on Automatic Control* 34.12 (1989), pp. 1313–1316. DOI: 10.1109/9.40787.
- [26] Robert R. Bitmead et al. “Monotonicity and stabilizability- properties of solutions of the Riccati difference equation: Propositions, lemmas, theorems, fallacious conjectures and counterexamples”. In: *Systems & Control Letters* 5 (1985), pp. 309–315.
- [27] Thomas Kailath, Ali H Sayed, and Babak Hassibi. *Linear estimation*. BOOK. Prentice Hall, 2000.