Periodic Sparse Control to Prevent Undetectable Attacks on Over-Actuated Systems

Wolleswinkel, Bart; van Straalen, Ivo; Ballotta, Luca; Gallo, Alexander J.; Ferrari, Riccardo M.G.

DOI
10.1109/LCSYS.2025.3581865

Publication date
2025

Document Version
Final published version

Published in
IEEE Control Systems Letters

Periodic Sparse Control to Prevent Undetectable Attacks on Over-Actuated Systems

Bart Wolleswinkel, *Graduate Student Member, IEEE*, Ivo van Straalen, *Graduate Student Member, IEEE*, Luca Ballotta, Alexander J. Gallo, and Riccardo M. G. Ferrari, *Senior Member, IEEE*

***Abstract*—Over-actuated systems, namely systems with more inputs than outputs, can increase control performance, yet are susceptible to model-based undetectable attacks if the actuator channel is compromised. In this paper, we show how implementing a sparse actuator schedule can introduce security by rendering these attacks ineffective. We formulate a novel methodology whereby a periodic sparse schedule, implemented at the actuators, secures the system by ensuring that a malicious adversary cannot exploit actuator redundancy to deploy undetectable attacks. The schedule is designed offline and repeats periodically at the actuators, so that the adversary is constrained to only tamper with the active actuators. We devise a degeneracy-aware greedy selection procedure with low computational complexity to design an actuator schedule that renders undetectable attacks ineffective, whilst simultaneously providing relatively small performance degradation. We illustrate the effectiveness of our approach using a reference tracking model predictive controller on the IEEE-39 bus power network employing the designed sparse schedule.**

***Index Terms*—Actuator scheduling, over-actuated system, sparse control, undetectable attacks.**

I. Introduction

RECENT years have seen an increase in automation in regulating industrial control tasks, leading to so-called cyber-physical systems (CPSs). Along with automation, the use of communication networks for transferring both control commands and sensor measurements has risen as well. These networked control system (NCS) offer many advantages, ranging from a low cost of deployment to increased modularity. However, alongside these benefits, there is also an increased vulnerability to cyberattacks, especially with critical infrastructure being a high-value target for nation-state actors [1].

Received 17 March 2025; revised 14 May 2025; accepted 3 June 2025. Date of publication 20 June 2025; date of current version 23 July 2025. This work was supported in part by the Horizon Europe Projects TWAIN under Grant 101122194; in part by SUDOCO under Grant 101122256; and in part by RVO through the TKI Offshore Project PHYSIA. Recommended by Senior Editor A. P. Aguiar. *(Corresponding author: Bart Wolleswinkel.)*

Bart Wolleswinkel, Ivo van Straalen, Luca Ballotta, and Riccardo M. G. Ferrari are with the Delft Center for Systems and Control, Delft University of Technology, 2628 CD Delft, The Netherlands (e-mail: b.wolleswinkel@tudelft.nl).

Alexander J. Gallo is with the Dipartimento di Elettronica, Bioingegneria e Informatica, Politecnico di Milano, 20133 Milan, Italy.

Digital Object Identifier 10.1109/LCSYS.2025.3581865

Securing these systems against cyberattacks has given rise to the area of secure control [2], an area that studies attacks on CPSs and appropriate defense mechanisms. A class of attacks on system actuators that has gained significant attention is that of undetectable attacks [3] (see also zero-dynamics attacks (ZDAs) [4] or masking attacks [5]), which exploit unstable zeros of the system dynamics.

As it turns out, systems that are *over-actuated* (systems with more inputs than outputs) are susceptible to undetectable attacks, which poses a vulnerability an adversary can exploit. This leads to two competing objectives; from a control perspective, more control inputs are desirable for performance [6], yet over-actuation exposes the system to a security risk. Several instances of industrial control systems (ICSs) are over-actuated, ranging from automotive and aerospace applications [6], [7], to high-precision robotics [8]. Geographically distributed control systems, such as heating, gas, and water distribution networks, are also frequently over-actuated, as they are generally poorly instrumented [9].

Undetectable attacks on over-actuated systems have been studied before in the literature [5], [10]. Several countermeasures against undetectable attacks have been proposed, such as modifying the system dynamics [4], [11], generalized hold [12], [13], and multi-rate sampling or control [10].

Contribution: Contrary to current works, we propose a novel angle for security and impose sparse control inputs to prevent undetectable attacks on over-actuated systems. Intuitively, these actuator attacks can exploit redundant inputs to mask disrupted state trajectories from the output. Reducing actuator redundancy through a few (*sparse*) smartly chosen inputs fundamentally limits undetectable attacks, making these ineffective. We focus on *sparse actuator scheduling*, whereby only a subset of the actuators are enabled at any time, to secure the system while maintaining controllability. Indeed, the latter objective may not be possible by merely statically selecting a subset of actuators. Sparse actuator scheduling has received attention for large-scale NCSs where simultaneously controlling many actuators is impractical [14], [15], [16]. However, to the best of our knowledge, we are the first to purposely design sparse control inputs as a countermeasure against cyberattacks. Compared to existing countermeasures [4], [10], [11], [12], [13], our strategy can be easily implemented, requiring minimally invasive adaptations of the controllers and actuators, as neither altering system dynamics nor changing sensor or actuator sampling rate is necessary.

Organization: We unroll the contribution of this paper along three steps. In Section III, we formalize periodic sparse actuator schedules, and formulate an original optimization problem to select a schedule that prevents disruptive undetectable attacks, without significantly degrading control performance. Then, in Section IV, we provide a greedy algorithm that heuristically solves the combinatorial optimization problem with low computational complexity. The proposed algorithm falls within a class of algorithms that is widely adopted in literature, and embeds the security guarantee as a constraint, making the resulting schedule *secure by design*. Finally, we show via simulations on a CPS in Section V that our algorithm works well in practice, and prevents undetectable attacks.

Notation: Let $\mathbb{N}$ denote the natural numbers, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, and $\mathbb{N}_{a:b} = \{a, a+1, \dots, b\}$. Let col stack its operands vertically, such that $\text{col}(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m) = [\boldsymbol{v}_1^\mathsf{T} \quad \cdots \quad \boldsymbol{v}_m^\mathsf{T}]^\mathsf{T}$. Given a matrix $\boldsymbol{B} = \begin{bmatrix}\boldsymbol{b}_1 & \cdots & \boldsymbol{b}_m\end{bmatrix} \in \mathbb{R}^{n\times m}$ and a set $\mathbb{S} = \{s_1, \dots, s_q\} \subseteq \mathbb{N}_{1:m}$, let $\boldsymbol{B}_\mathbb{S} = \begin{bmatrix}\boldsymbol{b}_{s_1} & \dots & \boldsymbol{b}_{s_q}\end{bmatrix} \in \mathbb{R}^{n\times q}$ denote the selection of columns of $\boldsymbol{B}$. Given natural numbers $a, p \in \mathbb{N}_0$, we use $\overline{a}|^{p} \in \mathbb{N}_{0:p-1}$ to denote the remainder of a when divided by p. The cardinality of a finite set $\mathbb{S} \subset \mathbb{N}$ is denoted by $|\mathbb{S}|$.

II. Setup

We consider discrete-time ($t \in \mathbb{N}_0$) linear time-invariant (LTI) systems of the following form:

$$\mathcal{P}: \quad \boldsymbol{x}[t+1] = \boldsymbol{A}\boldsymbol{x}[t] + \boldsymbol{B}\boldsymbol{u}[t], \tag{1a}$$
$$\boldsymbol{y}[t] = \boldsymbol{C}\boldsymbol{x}[t], \tag{1b}$$

with state vector $\boldsymbol{x}[t] \in \mathbb{R}^n$, actuation vector $\boldsymbol{u}[t] \in \mathbb{R}^m$, measurement vector $\boldsymbol{y}[t] \in \mathbb{R}^q$, and $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{C}$ all of appropriate dimension. A controller $\mathcal{C}: \boldsymbol{y}[t] \mapsto \boldsymbol{u}_\text{c}[t]$ transmits control inputs $\boldsymbol{u}_\text{c}[t]$ to $\mathcal{P}$ over a communication network. We make the following standard assumption:

Assumption 1: The pairs $(\boldsymbol{A}, \boldsymbol{B})$ and $(\boldsymbol{A}, \boldsymbol{C})$ are controllable and observable, respectively.

Central to this work is the following assumption:

Assumption 2 (Weakly Input-Redundant [8]): For the system $\mathcal{P}$ in (1), it holds that $m > q$ and $\text{rank}(\boldsymbol{B}) = m$.

A. Preliminaries on Geometric Control

Let us recall some concepts from geometric control that we use later for design. Further details can be found in [17], [18].

Definition 1 (Controlled Invariant Subspace [18, Sec. 4.1]): A subspace V is an $(\boldsymbol{A}, \boldsymbol{B})$-controlled invariant subspace if $\boldsymbol{A}V \subseteq V + \text{Im}(\boldsymbol{B})$, or, equivalently, if there exists a matrix $\boldsymbol{F}$, called a *friend* of V, such that $(\boldsymbol{A} + \boldsymbol{B}\boldsymbol{F})V \subseteq V$.

Notably, $(\boldsymbol{A}, \boldsymbol{B})$-controlled invariant subspaces contained in $\ker(\boldsymbol{C})$ gather all initial conditions of (1) such that $\boldsymbol{x}[t] \in V$ and $\boldsymbol{y}[t] = 0$ hold for all $t \geq 0$, for a suitable choice of input. Thus, they represent opportunities for actuator attacks to be *undetectable*. Of particular interest is $V^\star$, the unique $(\boldsymbol{A}, \boldsymbol{B})$-controlled invariant subspace $V \subseteq \ker(\boldsymbol{C})$ with largest dimension. We denote the set of all friends of $V^\star$ by $\mathbb{F}(V^\star)$.

Definition 2 (Conditioned Invariant Subspace [18, Sec. 5.1]:) A subspace S is a $(\boldsymbol{C}, \boldsymbol{A})$-conditioned invariant subspace if $\boldsymbol{A}(S \cap \ker(\boldsymbol{C})) \subseteq S$.

Let $S^\star$ denote the smallest $(\boldsymbol{C}, \boldsymbol{A})$-conditioned invariant subspace containing $\text{Im}(\boldsymbol{B})$. Both $V^\star$ and $S^\star$ can be efficiently computed in at most $n-1$ steps [17]. We denote by $R^\star = V^\star \cap S^\star$ the largest reachable subspace contained in $\ker(\boldsymbol{C})$. The eigenvalues of $\boldsymbol{A} + \boldsymbol{B}\boldsymbol{F}$ whose corresponding eigenvectors lie in $V^\star$, but not in $R^\star$, are the *invariant zeros* of $\mathcal{P}$, and are fixed for every $\boldsymbol{F} \in \mathbb{F}(V^\star)$. On the contrary, the eigenvalues of $\boldsymbol{A} + \boldsymbol{B}\boldsymbol{F}$ with eigenvectors in $R^\star$ are the *assignable zeros* of $\mathcal{P}$, whose location depends on $\boldsymbol{F} \in \mathbb{F}(V^\star)$.

Definition 3 (Degeneracy, Adapted from [19, Definition 1.i]): A triple $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})$ is *degenerate* if $\dim(R^\star) > 0$.

If $R^\star \neq \{\boldsymbol{0}\}$, an adversary can exploit assignable zeros and deploy undetectable attacks, as we discuss next.

B. Adversary Model

Following the taxonomy of [2], the adversary $\mathcal{A}$ has *disruption capabilities* only on the controller-to-actuators (C2A) channel. The actuation vector $\boldsymbol{u}[t]$ in (1a) is thus given by

$$\boldsymbol{u}[t] = \boldsymbol{u}_\text{c}[t] + \boldsymbol{a}[t], \tag{2}$$

where $\boldsymbol{a}[t]$ is the adversarial input. We consider the scenario where the adversary has knowledge of the plant dynamics, which allows them to craft model-based undetectable attacks:

Assumption 3 (Strong Adversary, Adapted from [2]:) The information $\mathbb{I}[t]$ known to the adversary $\mathcal{A}$ satisfies $\mathbb{I}[t] \supseteq \{\mathcal{P}\}$ for all $t \geq 0$.

The adversary $\mathcal{A}$ aims to damage the plant while remaining undetected from output measurements, as defined below.

Definition 4 (Disruptive Attack, Adapted from [20, ii]): An attack $\boldsymbol{a}[t]$ is *disruptive* if $\lim_{t\to\infty} \|\boldsymbol{x}[t]\| = \infty$.

Let $\boldsymbol{y}_0[t]$ be the nominal output (1b) produced if there is no attack, namely with $\boldsymbol{a}[t] = 0$ for all $t \geq 0$ in (2).

Definition 5 (ϵ-Stealthy Attack [20, i]:) An attack $\boldsymbol{a}[t]$ is *ϵ-stealthy*, with $\epsilon \in \mathbb{R}_{\geq 0}$, if $\left\|\boldsymbol{y}[t] - \boldsymbol{y}_0[t]\right\| \leq \epsilon$ for all $t \geq 0$.

If an attack $\boldsymbol{a}[t]$ is both disruptive and 0-stealthy, we call such an attack *successful*, and *unsuccessful* otherwise. Undetectable attacks are a class of disruptive 0-stealthy attacks, provided that $\boldsymbol{x}[0] \in V^\star \setminus \{\boldsymbol{0}\}$ [4],[1] and the existence of undetectable attacks is equivalent to the existence of unstable zeros [3]. Asm. 3 characterizes the least information $\mathbb{I}$ the adversary $\mathcal{A}$ must possess in order to be successful.

Proposition 1: Suppose Asm. 1, 2 and 3 hold. Then, for every $\epsilon \in \mathbb{R}_{\geq 0}$, there exists a successful attack $\boldsymbol{a}[t]$, $t \geq 0$.

Proof: Let $\boldsymbol{R}(z)$ denote the Rosenbrock matrix of (1) with $z \in \mathbb{C}$ [18]. Note that $\text{nrank}(\boldsymbol{R}(z)) = \max_{z\in\mathbb{C}} \text{rank}(\boldsymbol{R}(z)) \leq n + \min\{m, q\} = n + q < n + m$, where the latter follows from Asm. 2. As $\mathcal{P}$ is *left-invertible* if and only if $\text{nrank}(\boldsymbol{R}(z)) = n + m$ [18, Corollary 8.10], this implies $\mathcal{P}$ is not left-invertible. From [18, Theorem 8.26, iii], as $\text{rank}(\boldsymbol{B}) = m$ (Asm. 2) implies the map is injective, and $\boldsymbol{D} = \boldsymbol{0}$, we have that $R^\star \neq \{\boldsymbol{0}\}$. This implies $\dim(R^\star) \geq 1$, which means there exists at least one *assignable zero* $z \in \mathbb{C}$. Therefore, the adversary can construct a 0-stealthy attack, which is disruptive for any $|z| > 1$. ■

Remark 1: The adversary can construct $\boldsymbol{a}[t]$ as

$$\mathcal{A}: \quad \boldsymbol{f}[t+1] = (\boldsymbol{A} + \boldsymbol{B}\boldsymbol{F})\boldsymbol{f}[t], \tag{3a}$$
$$\boldsymbol{a}[t] = \boldsymbol{F}\boldsymbol{f}[t], \tag{3b}$$

[1]Note that if $\boldsymbol{x}_0 \notin V^\star \setminus \{\boldsymbol{0}\}$, one can still create an ϵ-stealthy attack for any $\epsilon \in \mathbb{R}_{>0}$ by choosing $\boldsymbol{a}[0]$ sufficiently small [4, Corollary 3].

where $\boldsymbol{f}[0] \in R^\star \setminus \{\boldsymbol{0}\}$ is sufficiently small, and $\boldsymbol{F} \in \mathbb{F}(V^\star)$ is a solution to the linear matrix equalities given by[2]

$$(\boldsymbol{A}+\boldsymbol{BF})\boldsymbol{V} = \boldsymbol{VX}, \qquad (\boldsymbol{A}+\boldsymbol{BF})\boldsymbol{R} = z\cdot\boldsymbol{R}, \tag{4}$$

for some $\boldsymbol{X} \in \mathbb{R}^{\dim(V^\star)\times n}$, $\mathrm{Im}(\boldsymbol{V}) = V^\star$, $\mathrm{Im}(\boldsymbol{R}) = R^\star$, and arbitrary $z \in \mathbb{C}$ satisfying $|z| > 1$. Alternatively, $\boldsymbol{a}[t]$ can be constructed using an output-zeroing direction of (1); see [19].

III. Periodic Sparse Control

Intuitively, the undetectable attacks previously described disrupt a state variable $[\boldsymbol{x}[t]]_i$ through some input(s) $[\boldsymbol{u}[t]]_{i'}$, and simultaneously exploit other input(s) $[\boldsymbol{u}[t]]_{i''}$ to mask the degraded trajectory of $[\boldsymbol{x}[t]]_i$ from the output $\boldsymbol{y}[t]$. To remedy this vulnerability, we turn our attention to sparse control. Formally, we say control inputs are sparse if $\|\boldsymbol{u}[t]\|_0 \le s < m$ at each time instant [15], or on average across time [14], where $\|\boldsymbol{v}\|_0$ is the number of nonzero elements of $\boldsymbol{v}$, and s is the *sparsity* of $\boldsymbol{u}[t]$. Sparse inputs $\boldsymbol{u}[t]$ can fundamentally impair undetectable attacks by reducing redundancy of active actuators. Enforcing sparsity by just transmitting sparse inputs $\boldsymbol{u}_\mathrm{c}[t]$ is insufficient, as the adversary can set $[\boldsymbol{a}[t]]_i \neq 0$ even if $[\boldsymbol{u}_\mathrm{c}[t]]_i = 0$ in (2). As such, we impose a preset periodic schedule implemented at the actuators instead, that determines which actuators are physically active at each time instant.

Definition 6 (Schedule): A schedule $\mathcal{S} = (\mathbb{S}_0, \mathbb{S}_1, \ldots, \mathbb{S}_{\ell-1})$ of length ℓ is a sequence of sets $\mathbb{S}_j \subseteq \mathbb{N}_{1:m}$, where $i \notin \mathbb{S}_j$ indicates that $[\boldsymbol{u}[j]]_i = 0$. $\mathcal{S}$ has period $p \in \mathbb{N}$ if p is the smallest integer for which $\mathcal{S} = (\mathbb{S}_0, \ldots, \mathbb{S}_{p-1}, \mathbb{S}_0, \ldots, \mathbb{S}_{p-1}, \ldots)$.

With some abuse of notation, we denote the total number of actuators that are active across the period of a schedule by $\|\mathcal{S}\|_0 = \sum_{j=0}^{p-1} |\mathbb{S}_j|$. A schedule $\mathcal{S}$ is in *irreducible form* if $p = \ell$.

The schedule is implemented at the actuators and repeats in a periodic fashion. To maintain adequate control performance, we assume that the actuators and the controller $\mathcal{C}_\mathcal{S}$, where the subscript $\mathcal{S}$ highlights the dependence of the controller on the schedule, share synchronized clocks, such that the latter is aware of which actuators are active. Crucially, the adversary $\mathcal{A}$ can attack only actuators enabled by the schedule, meaning $[\boldsymbol{a}[t]]_i = 0$ if $i \notin \mathbb{S}_{\overline{t}^{\,p}}$.

Remark 2: Whilst maintaining clock synchronization is important for control performance, desynchronization does not impact system security. Indeed, as shown in the following section, security is guaranteed by construction (sparsity) of the schedule itself, such that undetectable attacks are unsuccessful.

Whenever a schedule $\mathcal{S}$ prevents successful undetectable attacks, we say that this implementation is *secure by design*. One might argue that simply removing enough actuators can prevent undetectable attacks on over-actuated systems while maintaining controllability. However, the next example demonstrates that this is not always the case.

Example 1: Consider $\boldsymbol{A}$ as in [14, Example 1], $\boldsymbol{B} = \boldsymbol{I}_8$, and

$$\boldsymbol{C} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}. \tag{5}$$

Note that the triple $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})$ satisfies Asm. 1. We can remove at most five columns of $\boldsymbol{B}$ whilst maintaining controllability [14], but as $3 > q = 2$, this system would still be vulnerable to undetectable attacks.

[2]The existence of a (possibly non-unique) solution $\boldsymbol{F}$ follows from the definition of $V^\star$ and $R^\star$. All matrices $\boldsymbol{F}$ that satisfy (4) provide identical disruptiveness and stealthiness guarantees.

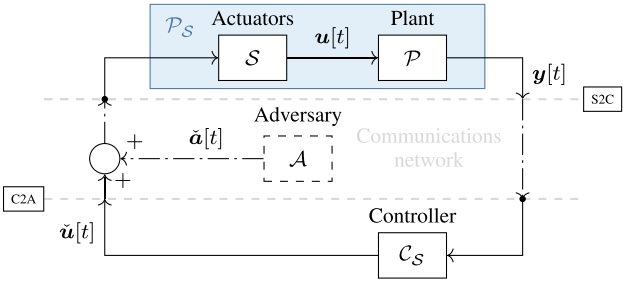

Fig. 1. Architecture of the NCS with periodic schedule $\boldsymbol{\mathcal{S}}$.

The implementation of a schedule $\mathcal{S}$ at the actuators results in a linear p-periodic system (see Fig. 1) as

$$\mathcal{P}_\mathcal{S}: \quad \boldsymbol{x}[t+1] = \boldsymbol{A}\boldsymbol{x}[t] + \boldsymbol{B}_\mathcal{S}[t]\check{\boldsymbol{u}}[t], \tag{6a}$$

$$\boldsymbol{y}[t] = \boldsymbol{C}\boldsymbol{x}[t], \tag{6b}$$

where $\boldsymbol{B}_\mathcal{S}[t] = \boldsymbol{B}_{\mathbb{S}_{\overline{t}^{\,p}}}$ (the submatrix of $\boldsymbol{B}$ selected by $\mathbb{S}_{\overline{t}^{\,p}}$ in $\mathcal{S}$), and the vector $\check{\boldsymbol{u}}[t]$ gathers all control inputs commanded to the actuators scheduled (active) at time t.

In practice, ICSs run continually, and therefore the notion of an initial set of active actuators is not meaningful in our context. This leads us to the following definition of *equivalence* between two schedules $\mathcal{S}$ and $\mathcal{S}'$.

Definition 7 (Equivalence): Define the shift operation as $\mathrm{shift}(\mathcal{S}, j) = (\mathbb{S}_j, \ldots, \mathbb{S}_{\ell-1}, \mathbb{S}_0, \ldots, \mathbb{S}_{j-1})$. Two schedules $\mathcal{S}$ and $\mathcal{S}'$ are (shift) equivalent, denoted by $\mathcal{S} \equiv \mathcal{S}'$, if, in irreducible form, there exists a j such that $\mathrm{shift}(\mathcal{S}, j) = \mathcal{S}'$.

We can now formulate our schedule design problem.

Problem 1: For a system $\mathcal{P}$, schedule length ℓ, and cost function f, find the optimal sparse actuator schedule $\mathcal{S}$ which renders the resulting p-periodic system $\mathcal{P}_\mathcal{S}$ secure, namely:

$$\min_{\mathcal{S}} \ f(\mathcal{S}) \quad \text{s.t.} \tag{7a}$$

$$f(\mathcal{S}') = f(\mathcal{S}), \tag{7b}$$

$$\text{for all } \mathcal{S}' \equiv \mathcal{S}: \quad \mathcal{P}_{\mathcal{S}'} \text{ is controllable}, \tag{7c}$$

$$\mathcal{P}_{\mathcal{S}'} \text{ has no unstable zeros}. \tag{7d}$$

The cost minimization in (7a) and constraint (7c) are in conflict with constraint (7d): while the former benefit from larger $\|\mathcal{S}\|_0$, the latter implicitly constrains $\|\mathcal{S}\|_0 \le \ell\cdot q$, as the periodic system $\mathcal{P}_\mathcal{S}$ would be degenerate otherwise. In actuator selection, typical choices for f aim to reduce control energy [21]. We make a tailored choice in the next section to accommodate constraints (7b) and (7c), which are motivated by the argument above about continual operation. Constraint (7c) ensures that $\mathcal{P}_\mathcal{S}$ can track a state reference in p steps (p being the period of $\mathcal{S}$) without waiting for the schedule to restart from $\mathbb{S}_0$. Note that any $\mathcal{S}$ satisfying (7d) implies the system $\mathcal{P}_\mathcal{S}$ is *secure by design*, as defined prior. Next, we discuss how to deal with (7c) and (7b), and in §IV, we address (7d) and present our algorithm to tackle Prb. 1.

Cyclic Reformulation

Using lifting techniques, we can transform the linear p-periodic system $\mathcal{P}_\mathcal{S}$ into an equivalent LTI system. For a

vector $\boldsymbol{v}[t] \in \mathbb{R}^v$, we define its associated lifted vector $\bar{\boldsymbol{v}}[t]$ as

$$\bar{\boldsymbol{v}}[t] = \operatorname{col}(\mathbf{0}_{\overline{t}\,|\,p-1}, 1, \mathbf{0}_{v-\overline{t}\,|\,p}) \otimes \boldsymbol{v}[t] \in \mathbb{R}^{p \cdot v}. \tag{8}$$

This allows us to introduce the *cyclic reformulation* [22, 3.2] $\mathring{\mathcal{P}}_{\mathcal{S}}$ of the linear p-periodic system $\mathcal{P}_{\mathcal{S}}$, given by

$$\mathring{\mathcal{P}}_{\mathcal{S}}: \quad \begin{aligned} \bar{\boldsymbol{x}}[t+1] &= \mathring{\boldsymbol{A}}\,\bar{\boldsymbol{x}}[t] + \mathring{\boldsymbol{B}}_{\mathcal{S}}\bar{\boldsymbol{u}}[t], && \text{(9a)} \\ \bar{\boldsymbol{y}}[t] &= \mathring{\boldsymbol{C}}\,\bar{\boldsymbol{y}}[t], && \text{(9b)} \end{aligned}$$

with $\bar{\boldsymbol{x}}[t]$, $\bar{\boldsymbol{u}}[t]$, and $\bar{\boldsymbol{y}}[t]$ as in (8), and with matrices

$$\mathring{\boldsymbol{A}} = \begin{bmatrix} \mathbf{0} & \boldsymbol{A} \\ \boldsymbol{I}_{p-1} \otimes \boldsymbol{A} & \mathbf{0} \end{bmatrix}, \qquad \mathring{\boldsymbol{C}} = \boldsymbol{I}_p \otimes \boldsymbol{C}, \tag{10a}$$

$$\mathring{\boldsymbol{B}}_{\mathcal{S}} = \begin{bmatrix} \mathbf{0} & \boldsymbol{B}_{\mathbb{S}_{p-1}} \\ \operatorname{diag}(\boldsymbol{B}_{\mathbb{S}_0}, \ldots, \boldsymbol{B}_{\mathbb{S}_{p-2}}) & \mathbf{0} \end{bmatrix}. \tag{10b}$$

The LTI system $\mathring{\mathcal{P}}_{\mathcal{S}}$ is controllable if and only if its controllability Gramian matrix $\mathring{\boldsymbol{W}}_{\mathcal{S}} = \mathring{\boldsymbol{\Phi}}_{\mathcal{S}}\,\mathring{\boldsymbol{\Phi}}_{\mathcal{S}}^{\mathsf{T}}$ is full rank, where

$$\mathring{\boldsymbol{\Phi}}_{\mathcal{S}} = \begin{bmatrix} \mathring{\boldsymbol{A}}^{\,p-1}\mathring{\boldsymbol{B}}_{\mathcal{S}} & \mathring{\boldsymbol{A}}^{\,p-2}\mathring{\boldsymbol{B}}_{\mathcal{S}} & \cdots & \mathring{\boldsymbol{B}}_{\mathcal{S}} \end{bmatrix}. \tag{11}$$

The analogous characterization holds for the periodic system $\mathcal{P}_{\mathcal{S}}$ and its associated p-step controllability matrix $\boldsymbol{\Phi}_{\mathcal{S}}$. Interestingly, controllability of $\mathring{\mathcal{P}}_{\mathcal{S}}$ is equivalent to satisfaction of the controllability constraint (7c).

Lemma 1: For the controllability Gramian of $\mathring{\mathcal{P}}_{\mathcal{S}}$, $\operatorname{rank}(\mathring{\boldsymbol{W}}_{\mathcal{S}}) = p \cdot n \iff \operatorname{rank}(\boldsymbol{\Phi}_{\mathcal{S}'}) = n$ for all $\mathcal{S}' \equiv \mathcal{S}$.

Proof: It follows directly from the block anti-diagonal structure of both $\mathring{\boldsymbol{A}}$ and $\mathring{\boldsymbol{B}}_{\mathcal{S}}$. ∎

Lem. 1 states that if the controllability Gramian of $\mathring{\mathcal{P}}_{\mathcal{S}}$ is full rank, system $\mathcal{P}_{\mathcal{S}'}$ is controllable for all $\mathcal{S}' \equiv \mathcal{S}$. The following property involves common scalar functions ρ of $\mathring{\boldsymbol{W}}_{\mathcal{S}}$, which quantify control energy [14, Table 1], and is convenient to satisfy constraint (7b).

Lemma 2: For every systemic controllability metric ρ as per [14], it holds that $\rho(\mathring{\boldsymbol{W}}_{\mathcal{S}'}) = \rho(\mathring{\boldsymbol{W}}_{\mathcal{S}})$ for all $\mathcal{S}' \equiv \mathcal{S}$.

Proof: It readily follows from the block-diagonal structure of $\mathring{\boldsymbol{W}}_{\mathcal{S}}$ combined with the fact that the blocks in $\mathring{\boldsymbol{W}}_{\mathcal{S}'}$ are a permutation (in fact, a shifting) of the blocks in $\mathring{\boldsymbol{W}}_{\mathcal{S}}$. ∎

In light of Lem. 2 and 1, we choose $f(\mathcal{S}) = \rho(\mathring{\boldsymbol{W}}_{\mathcal{S}})$ in problem (7), where ρ is increasing with control energy.

The definition of zeros of the periodic system $\mathcal{P}_{\mathcal{S}}$, as well as degeneracy can be derived from the cyclic reformulation in (10) as well [22]. Zeros of linear p-periodic systems have been shown to have a geometric characterization, focused on the notation of p-periodic invariants [23]. In the interest of brevity, we do not elaborate on this further, but it can be shown that $\mathring{V}^\star$ and $\mathring{R}^\star$ belonging to $\mathring{\mathcal{P}}_{\mathcal{S}}$ are the invariants of the linear p-periodic system [24]. As such, to study the zero dynamics of $\mathcal{P}_{\mathcal{S}}$, it suffices to consider $\mathring{V}^\star$ and $\mathring{R}^\star$ of $\mathring{\mathcal{P}}_{\mathcal{S}}$.

IV. Degeneracy-Aware Design Algorithm

Having dealt with constraints (7b) and (7c), we turn our attention to minimizing (7a) while making attacks ineffective via (7d). Prb. 1 is combinatorial and can be solved by exhaustively evaluating all possible schedules of length ℓ. However, the computational complexity of brute-force search scales poorly with parameters m and ℓ. Hence, we opt for a greedy selection because it is computationally efficient, easy to implement, and works well in practice [14], [21], [25].

Algorithm 1: Forward Degeneracy-Aware Greedy

Requires: $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \ell$ (parameters: ρ, ϵ)
Returns: $\mathcal{S}$

$\mathcal{S} \leftarrow (\emptyset, \emptyset, \ldots, \emptyset)$ ▷ Empty schedule of length ℓ
while $\|\mathcal{S}\|_0 \leq \ell \cdot q$ **do**
  for $\mathbb{S}_j$ **in** $\mathcal{S}$ **for** i **in** $\{1, \ldots, m\} \setminus \mathbb{S}_j$ **do**
    $\mathcal{S}' \leftarrow (\mathbb{S}_0, \ldots, \mathbb{S}_j \cup \{i\}, \ldots, \mathbb{S}_{\ell-1})$
    ▷ Degeneracy-aware check
    $\mathring{V}^\star, \mathring{R}^\star \leftarrow$ subspaces belonging to $\mathring{\mathcal{P}}_{\mathcal{S}'}$
    if $\dim(\mathring{R}^\star) > 0$ **or** $\mathring{V}^\star$ contains unstable zeros
      $c_{ij} \leftarrow \infty$
    else
      $c_{ij} \leftarrow \rho(\mathring{\boldsymbol{W}}_{\mathcal{S}'} + \epsilon \cdot \boldsymbol{I})$
  $\mathbb{S}_j^*, i^* \leftarrow \arg\min c_{ij}$
  if $\mathbb{S}_j^*, i^*$ is undefined
    return $\mathcal{S}$
  else
    $\mathcal{S} \leftarrow (\mathbb{S}_0, \ldots, \mathbb{S}_j^* \cup \{i^*\}, \ldots, \mathbb{S}_{\ell-1})$
return $\mathcal{S}$

To satisfy (7d), one might suspect that ensuring the triple $(\boldsymbol{A}, \boldsymbol{B}_{\mathbb{S}}, \boldsymbol{C})$ is nondegenerate for *at least* one set of actuators $\mathbb{S}$ in $\mathcal{S}$ is sufficient, but the counter-example below illustrates that this need not be the case.

Example 2: Consider the system given by

$$\boldsymbol{A} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1/4 & 3/4 & 1/4 \end{bmatrix}, \quad \boldsymbol{C} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \tag{12}$$

$\boldsymbol{B} = \boldsymbol{I}_3$, and $\ell = 3$. Note that $(\boldsymbol{A}, \boldsymbol{B}_{\{3\}}, \boldsymbol{C})$ is nondegenerate. However, $(\boldsymbol{A}, \boldsymbol{B}_{\{2,3\}}, \boldsymbol{C})$ is degenerate, and for $\mathcal{S}' \equiv (\{3\}, \{2, 3\}, \{2, 3\})$, we have that $\dim(\mathring{R}^\star) > 0$, meaning that undetectable attacks are possible after implementing $\mathcal{S}'$, even though one set of actuators $\mathbb{S}$ in $\mathcal{S}'$ yields a nondegenerate triple. On the other hand, for the schedule $\mathcal{S} \equiv (\{1\}, \{1, 3\}, \{1, 3\})$, all triples $(\boldsymbol{A}, \boldsymbol{B}_{\mathbb{S}}, \boldsymbol{C})$ for $\mathbb{S}$ in $\mathcal{S}$ are nondegenerate, and it results in $\mathring{V}^\star = \{\mathbf{0}\}$.

Motivated by Example 2, we propose an adaptation to the standard (forward) greedy selection, ensuring that, at every iteration, the candidate schedule $\mathcal{S}'$ makes the periodic system both nondegenerate and with no unstable invariant zeros.[3] As such, the schedule returned by the algorithm is *secure by design*, guaranteeing that undetectable attacks are unsuccessful. The algorithm designs a schedule $\mathcal{S}$ by iteratively adding actuators until all candidate schedules are either degenerate or contain unstable invariant zeros. It starts from the empty schedule and, at each iteration, it adds the actuator that causes the smallest cost increase. In our adaptation, every time the algorithm evaluates a schedule $\mathcal{S}'$, it constructs its associated cyclic reformulation $\mathring{\mathcal{P}}_{\mathcal{S}'}$ and computes the corresponding subspaces $\mathring{V}^\star$ and $\mathring{R}^\star$. If $\mathring{R}^\star \neq \{\mathbf{0}\}$ or if $\mathring{V}^\star$ contains unstable invariant zeros, we exclude $\mathcal{S}'$ as a candidate. When no viable candidates remain, the last selected schedule $\mathcal{S}$ is returned. The pseudo-code of the algorithm is shown in Alg. 1.

An inherent advantage of using the finite-horizon controllability Gramian $\mathring{\boldsymbol{W}}_{\mathcal{S}'}$ is that it can not only be used for unstable

[3]Note that the latter is necessary as, when $\mathcal{S} \in \mathbb{I}[t]$, the adversary can still craft a successful attack even if $\mathcal{S}$ is implemented at the actuators.

systems [26] but also for uncontrollable systems. Some metrics ρ are only defined if $\mathring{\boldsymbol{W}}_{\mathcal{S}'}$ is full rank, and during early iterations, the system $\mathcal{P}_{\mathcal{S}'}$ is likely uncontrollable. To remedy this, we perturb the controllability Gramian as $\mathring{\boldsymbol{W}}_{\mathcal{S}'} + \epsilon \cdot \boldsymbol{I}$, with $\epsilon > 0$ small, which heuristically provides a controllable system with low cost [14], [25], [27].

The schedule length ℓ contributes to feasibility of constraint (7c) and control performance of $\mathcal{P}_{\mathcal{S}}$. A larger schedule length ℓ provides better control performance, but might lead to additional implementation complexity at the actuators. Note that, whenever Alg. 1 returns a feasible solution $\mathcal{S}$, the implementation is *secure by design*; as such, ℓ does not impact security of the proposed solution. Quantifying the impact of ℓ on *a priori* feasibility of Prb. 1 is left to future work.

V. Numerical Simulations

Consider the IEEE 39-bus power system model defined in [28], with parameters from [29], consisting of ten generators and discretized with a sampling time of 0.2 seconds. We measure the states of the first generator, meaning the resulting LTI system is characterized by $n = 20$, $m = 10$, and $q = 2$. As $\operatorname{rank}(\boldsymbol{B}) = m > q$, the system is susceptible to a successful undetectable attack according to Lem. 1. As the system is output feedback, we use the Luenberger observer

$$\hat{\boldsymbol{x}}[t+1] = (\boldsymbol{A} - \boldsymbol{LC})\hat{\boldsymbol{x}}[t] + \boldsymbol{B}\boldsymbol{u}[t] + \boldsymbol{L}\boldsymbol{y}[t], \tag{13}$$

where $\boldsymbol{L}$ is chosen such that $(\boldsymbol{A} - \boldsymbol{LC})$ is stable. The controller uses model predictive control (MPC) and tracks the reference $\boldsymbol{y}_{\text{ref}} = \operatorname{col}(0.01, 0)$, with $\mathcal{C}$ given by

$$\min_{\boldsymbol{x}_{i|t}, \boldsymbol{u}_{i|t}} \sum_{i=0}^{N-1} \|\boldsymbol{C}\boldsymbol{x}_{i|t} - \boldsymbol{y}_{\text{ref}}\|_{\boldsymbol{Q}}^2 + \|\boldsymbol{u}_{i|t}\|_{\boldsymbol{R}}^2 \quad \text{s.t.} \tag{14a}$$

$$\boldsymbol{x}_{0|t} = \hat{\boldsymbol{x}}[t], \quad \text{for all } i \in \{0, \dots, N-1\}: \tag{14b}$$

$$\mathcal{C}: \qquad \boldsymbol{x}_{i+1|t} = \boldsymbol{A}\boldsymbol{x}_{i|t} + \boldsymbol{B}\boldsymbol{u}_{i|t}, \tag{14c}$$

$$\boldsymbol{C}\boldsymbol{x}_{N|t} = \boldsymbol{y}_{\text{ref}}, \tag{14d}$$

with $\boldsymbol{Q} = \boldsymbol{I}_{20}$, $\boldsymbol{R} = \boldsymbol{I}_{10}$, and $N = 20$. At time t, $\boldsymbol{x}_{i|t}$ and $\boldsymbol{u}_{i|t}$, $i \in \mathbb{N}_{0:N-1}$ are decision variables defining the predicted state and control input. The MPC controller is implemented in a receding horizon fashion such that $\boldsymbol{u}_{\text{c}}[t] = \boldsymbol{u}^*_{0|t}$.

The adversary constructs $\boldsymbol{a}[t]$ according to Rmk. 1 with $z = 1.05$ and $\|\boldsymbol{f}[0]\| \sim 10^{-6}$. The results of a simulation with 500 time steps and initial condition $\boldsymbol{x}[0] = 0.01 \cdot \boldsymbol{1}$ can be seen in Fig. 2. For the sake of readability, we only include two control inputs (out of ten) to exemplify the effect of the undetectable attacks and of our proposed schedule. The attack is successful as the state diverges (top box, dashed line) whilst the output (bottom box) remains close to the nominal value.

We design a schedule $\mathcal{S}$ using Alg. 1 with $\ell = 10$ and $\rho(\boldsymbol{W}) = \operatorname{trace}(\boldsymbol{W}^{-1})$ as the metric. For the original system, $\rho_{\text{full}} = 810.5$. Alg. 1 returns the schedule

$$\mathcal{S} \equiv (\{2, 3\}, \{7\}, \{5\}, \{1\}, \{7\}, \{2, 5\}, \{8, 10\}, \{3, 5\}, \{1, 7, 10\}, \{4, 6, 8, 9\}), \tag{15}$$

with an associated metric $\rho_{\mathcal{S}} = 24882.6$. Interestingly, $\|\mathcal{S}\|_0 = 19 < \ell \cdot q$, suggesting that adding any more actuators either makes the system degenerate or generates an unstable zero. All actuators are used at least once during the schedule.

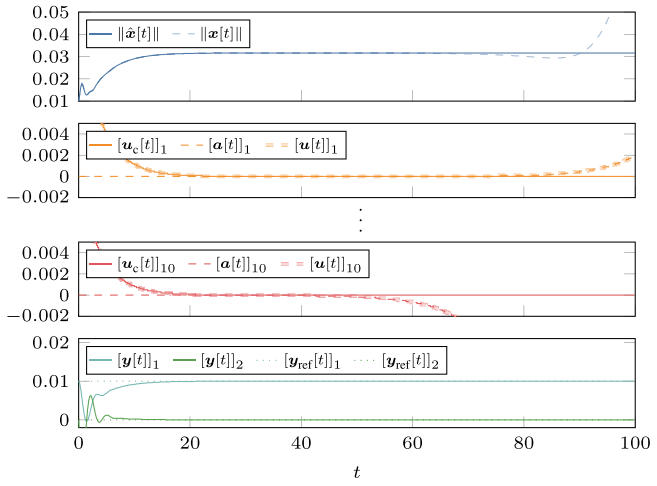

Fig. 2. Original system with successful undetectable attack.

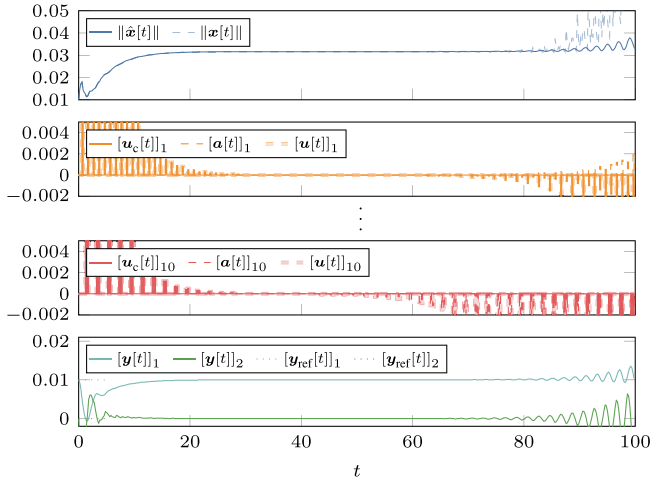

Fig. 3. Implementation of the 10-periodic system, with unsuccessful attack.

We illustrate, by means of simulation, the control performance with the schedule implemented and demonstrate its ability to prevent undetectable attacks. Considering an identical control objective, the only necessary change to the controller $\mathcal{C}$ is replacing (14c) with

$$\mathcal{C}_{\mathcal{S}}: \qquad \boldsymbol{x}_{i+1|t} = \boldsymbol{A}\boldsymbol{x}_{i|t} + \boldsymbol{B}_{\mathcal{S}}[t+i]\boldsymbol{u}_{i|t}, \tag{16}$$

and appropriately changing the dimensions such that $\boldsymbol{u}_{i|t} \in \mathbb{R}^{|\mathbb{S}\ \overline{t+i}\ p|}$. The resulting simulation results can be seen in Fig. 3, where the tracking performance is still satisfactory. The adversary launches the same attack $\boldsymbol{a}[t]$ but, due to the schedule, the output diverges and the attack is no longer stealthy.

VI. Conclusion

In this paper, we address undetectable attacks on over-actuated systems and propose a novel countermeasure based on the implementation of a periodic sparse schedule at the actuators. We devise a selection algorithm providing a schedule that renders the resulting periodic system resilient to undetectable attacks whilst heuristically keeping the performance degradation small. For future work, we will consider the

relaxation of Asm. 3 to see whether adversaries with partial knowledge [30] can still exploit degeneracy. Our method could be extended to square multiple-input and multiple-output (MIMO) systems with unstable invariant zeros upon careful design. Furthermore, it will be interesting to investigate whether multiplexed systems [31] can offer a similar resilience to undetectable attacks. The effect of network induced phenomena such as time delays, packet drops, noise, and desynchronization on the performance of the proposed sparse actuator schedule are currently under investigation. Finally, it is desired to obtain *a priori* formal guarantees on the feasibility of problem (7) and successful termination of Alg. 1 [15].

REFERENCES

[1] K. E. Hemsley and D. R. E. Fisher, "History of industrial control system Cyber incidents," Idaho National Lab. (INL), Idaho Falls, ID, United States, Rep. INL/CON-18-44411-Rev002, Dec. 2018. [Online]. Available: https://www.osti.gov/biblio/1505628

[2] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0005109814004488

[3] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 110–127, Feb. 2015. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7011011

[4] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *Proc. Annu. Allerton Conf. Commun. Control Comput.*, Oct. 2012, pp. 1806–1813. [Online]. Available: https://ieeexplore.ieee.org/document/6483441

[5] J. Kim, G. Park, H. Shim, and Y. Eun, "Masking attack for sampled-data systems via input redundancy," *IET Control Theory Appl.*, vol. 13, no. 14, pp. 2300–2308, 2019. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1049/iet-cta.2018.6075

[6] C. Vermillion, J. Sun, and K. Butts, "Model predictive control allocation for overactuated systems—Stability and performance," in *Proc. IEEE Conf. Decision Control*, Dec. 2007, pp. 1251–1256. [Online]. Available: https://ieeexplore.ieee.org/document/4434722

[7] A. Argha, S. W. Su, and B. G. Celler, "Static output feedback fault tolerant control using control allocation scheme," *Int. J. Robust Nonlinear Control*, vol. 29, no. 1, pp. 98–116, 2019. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/rnc.4376

[8] A. Zürcher, K. Dimitrov, M. Schwartz, and S. Hohmann, "On control allocation and its applicability for dual-stage actuator systems," in *Proc. Eur. Control Conf.*, Jun. 2024, pp. 1704–1709. [Online]. Available: https://ieeexplore.ieee.org/document/10591318

[9] P. Carpentier and G. Cohen, "Applied mathematics in water supply network management," *Automatica*, vol. 29, no. 5, pp. 1215–1250, 1993. [Online]. Available: https://www.sciencedirect.com/science/article/pii/000510989390048X

[10] M. Naghnaeian, N. H. Hirzallah, and P. G. Voulgaris, "Security via multirate control in cyber–physical systems," *Syst. Control Lett.*, vol. 124, pp. 12–18, Feb. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167691118302184

[11] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 106–117, Mar. 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7478650

[12] B. Kim, K. Ryu, and J. Back, "A generalized hold based countermeasure against zero-dynamics attack with application to DC-DC converter," *IEEE Access*, vol. 10, pp. 44923–44933, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9758732

[13] J. Kim, J. Back, G. Park, C. Lee, H. Shim, and P. G. Voulgaris, "Neutralizing zero dynamics attack on sampled-data systems via generalized holds," *Automatica*, vol. 113, Mar. 2020, Art. no. 108778. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0005109819306417

[14] M. Siami, A. Olshevsky, and A. Jadbabaie, "Deterministic and randomized actuator scheduling with guaranteed performance bounds," *IEEE Trans. Autom. Control*, vol. 66, no. 4, pp. 1686–1701, Apr. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9112270/

[15] L. Ballotta, G. Joseph, and I. Rahul Thete, "Pointwise-sparse actuator scheduling for linear systems with controllability guarantee," *IEEE Control Syst. Lett.*, vol. 8, pp. 2361–2366, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10706838

[16] L. Ye, M. Chi, Z.-W. Liu, and V. Gupta, "Online actuator selection and controller design for linear quadratic regulation with an unknown system model," *IEEE Trans. Autom. Control*, vol. 70, no. 1, pp. 18–33, Jan. 2025. [Online]. Available: https://ieeexplore.ieee.org/document/10582506

[17] G. Basile and G. Marro, *Controlled and Conditioned Invariants in Linear System Theory*. Englewood Cliffs, NJ, USA: Prentice Hall, 1992.

[18] H. L. Trentelman, A. A. Stoorvogel, and M. Hautus, *Control Theory for Linear Systems*, 1st ed., E. D. Sontag and M. Thoma, Eds., London, U.K.: Springer, 2001.

[19] J. Tokarzewski, "Zeros in discrete-time MIMO LTI systems and the output-zeroing problem," *Int. J. Appl. Math. Comput. Sci.*, vol. 10, no. 3, pp. 537–557, 2000. [Online]. Available: https://www.infona.pl//resource/bwmeta1.element.baztech-article-BPZ1-0014-0029

[20] K. Kimura and H. Ishii, "Quantized zero dynamics attacks against sampled-data control systems," *IEEE Trans. Autom. Control*, vol. 69, no. 5, pp. 3418–3425, May 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10336373

[21] G. Baggio, F. Pasqualetti, and S. Zampieri, "Energy-aware controllability of complex networks," *Annu. Rev. Control Robot. Auton. Syst.*, vol. 5, pp. 465–489, May 2022. [Online]. Available: https://www.annualreviews.org/content/journals/10.1146/annurev-control-042920-014957

[22] S. Bittanti and P. Colaneri, "Analysis of discrete-time linear periodic systems," in *Control and Dynamic Systems* (Digital Control and Signal Processing Systems and Techniques), vol. 78, C. T. Leondes, Ed. Cambridge, MA, USA: Academic, Jan. 1996, pp. 313–339. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0090526796800569

[23] O. M. Grasselli and S. Longhi, "Zeros and poles of linear periodic multivariable discrete-time systems," *Circuits, Syst. Signal Process.*, vol. 7, pp. 361–380, Sep. 1988. [Online]. Available: https://link.springer.com/article/10.1007/BF01599976

[24] O. M. Grasselli and S. Longhi, "Disturbance localization with dead-beat control for linear periodic discrete-time systems," *Int. J. Control*, vol. 44, no. 5, pp. 1319–1347, 1986. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/00207178608933672

[25] B. Guo, O. Karaca, T. Summers, and M. Kamgarpour, "Actuator placement under structural controllability using forward and reverse greedy algorithms," *IEEE Trans. Autom. Control*, vol. 66, no. 12, pp. 5845–5860, Dec. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9292985

[26] T. H. Summers, F. L. Cortesi, and J. Lygeros, "On submodularity and controllability in complex dynamical networks," *IEEE Trans. Control Netw. Syst.*, vol. 3, no. 1, pp. 91–101, Mar. 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7151797/

[27] K. P. V. S. Kondapi, C. Sriram, G. Joseph, and C. R. Murthy, "Sparse actuator scheduling for discrete-time linear dynamical systems," in *Proc. Indian Control Conf.*, 2024, pp. 1–6. [Online]. Available: https://arxiv.org/pdf/2407.00385

[28] G. Fazelnia, R. Madani, A. Kalbat, and J. Lavaei, "Convex relaxation for optimal distributed control problems," *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 206–221, Jan. 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7464306

[29] I. E. Atawi, "An advance distributed control design for wide-area power system stability," Ph.D. dissertation, Dept. Elect. Eng., Univ. Pittsburgh, Pittsburgh, PA, USA, 2013. [Online]. Available: https://d-scholarship.pitt.edu/18840/

[30] G. Park, C. Lee, H. Shim, Y. Eun, and K. H. Johansson, "Stealthy adversaries against uncertain Cyber-physical systems: Threat of robust zero-dynamics attack," *IEEE Trans. Autom. Control*, vol. 64, no. 12, pp. 4907–4919, Dec. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8662680

[31] K. V. Ling, J. Maciejowski, A. Richards, and B. F. Wu, "Multiplexed model predictive control," *Automatica*, vol. 48, no. 2, pp. 396–401, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0005109811005280