Averting Undetectable Attacks on Over-Actuated Systems with Sparse Control

van Straalen, I.; Wolleswinkel, B.G.; Ballotta, L.; Gallo, A.J.; Ferrari, Riccardo M.G.

Publication date
2025

Document Version
Final published version

Published in
Book of Abstracts 44th Benelux Meeting on Systems and Control

44^{th} Benelux Meeting

on

Systems and Control

March 18 – 20, 2025

Egmond aan Zee, The Netherlands

Book of Abstracts

The 44^{th} Benelux Meeting on Systems and Control is sponsored by

dutch institute of systems and control

Raffaella Carloni, Javier Alonso-Mora, Janset Dasdemir, and Erjen Lefeber (Eds.)

Book of Abstracts - 44^{th} Benelux Meeting on Systems and Control

University of Groningen
PO Box 72
9700 AB Groningen
The Netherlands

ISBN (PDF without DRM): 978-94-034-3117-8

Averting Undetectable Attacks on Over-Actuated Systems with Sparse Control

Ivo van Straalen[1,*], Bart Wolleswinkel[1], Luca Ballotta[1], Alexander J. Gallo[2], Riccardo M.G. Ferrari[1]
[1] Delft Center for Systems and Control, Delft University of Technology, The Netherlands
[2] Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Milano, Italia
[*] Corresponding author, i.vanstraalen@tudelft.nl

1 Introduction

Over-actuated systems, defined as having more inputs than outputs, arise in a multitude of applications, with the benefit of providing redundancy and increasing control performance. However, this property makes these systems susceptible to undetectable actuator attacks. This research focuses on a method to protect these over-actuated systems against these attacks.

2 Undetectable Cyber-Attacks

We consider the following LTI system:

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{u}_k, \quad \mathbf{y}_k = \mathbf{C}\mathbf{x}_k, \tag{1}$$

where $\mathbf{x}_k \in \mathbb{R}^n$, $\mathbf{u}_k \in \mathbb{R}^m$, $\mathbf{y}_k \in \mathbb{R}^p$, and we assume that $(\mathbf{A},\mathbf{B})$ is controllable, $(\mathbf{A},\mathbf{C})$ is observable, $\mathrm{rank}(\mathbf{B}) = m$, $\mathrm{rank}(\mathbf{C}) = p$ and $m > p$. The plant (1) is controlled over a network. We assume that this network has been compromised by an attacker that has gained access to the input channel, and can alter the input signal:

$$\mathbf{u}_k \longrightarrow \tilde{\mathbf{u}}_k = \mathbf{u}_k + \mathbf{a}_k,$$

where $\mathbf{a}_k \in \mathbb{R}^m$. The adversary has full knowledge of $\mathbf{A},\mathbf{B},\mathbf{C}$. The goal of such an adversary is to diverge the state trajectory from the nominal trajectory as much as possible while staying undetected. In this work we are specifically interested in the following subset of attack signals.

Definition 1 (Undetectable Attacks [1]). *The attack $\tilde{\mathbf{u}}_k$ is undetectable if $y(\mathbf{x}_0,\mathbf{a},k) = 0$, where $y(\mathbf{x}_0,\mathbf{u},k)$ denotes the output at time k driven by inputs $\mathbf{u}$ with initial condition $\mathbf{x}_0$.*

Note that knowledge of x_0 reduces the class of undetectable attacks. In this work, we consider the more general case where x_0 is *not* known.

Theorem 1 (Existence of Undetectable Attacks [1]). *An undetectable attack $\mathbf{a}$ exists iff there exist $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{g} \in \mathbb{R}^m$ and $z \in \mathbb{C}$ such that*

$$\begin{bmatrix} z\mathbf{I}_n - \mathbf{A} & -\mathbf{B} \\ \mathbf{C} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ \mathbf{g} \end{bmatrix} = \mathbf{0}. \tag{2}$$

Moreover, in the case that $m > p$, an undetectable attack that is able to drive the state unbounded is guaranteed to exist.

Note that condition (2) in Theorem 1 is equivalent to the existence of (invariant) zeros in system (1).

3 Removal of Undetectable Attacks

Motivated by the observation that changing the input matrix $\mathbf{B}$ impacts the existence of undetectable attacks, we employ *s-sparse control* [2]. In this framework, every time step only a subset of the actuators is utilized. That is, we constrain $\|\mathbf{u}_k\|_0 \leq s$ for some sparsity level s, where $\|\cdot\|_0$ counts the number of non-zero elements.

Theorem 2 (s-Sparse Controllability [2]). *The system* (1) *remains controllable, under the constraint $\|\mathbf{u}_k\|_0 \leq s$ if and only if $s \geq n - \mathrm{rank}(\mathbf{A})$.*

Furthermore, we are guaranteed to be able to find a *periodic* schedule $S \in \{1,\ldots,m\}^{\mathbb{N}}$, $S_{k+h} = S_k$ that dictates which actuators to utilize at a given time-step, enforcing the sparsity condition while guaranteeing controllability. By enforcing this schedule at both control and actuator side, we are able to fundamentally alter the input matrix $\mathbf{B}$ at every time-step: $\mathbf{B} \to \mathbf{B}_k$. The matrices $\mathbf{B}_k$ consist of the columns B^j of $\mathbf{B}$: $\mathbf{B}_k := [B^{j_1} \ldots B^{j_s}]$, where $S_k = \{j_1,\ldots j_s\} \subset \{1,\ldots,m\}$. Hence, system (1) can be regarded as an h-periodic linear system. For a given schedule, we are able to check the existence of undetectable attack by checking a condition analogous to (2) for periodic systems. However, finding such a schedule S is inherently combinatorial in nature. As such we are exploring other formulations and conditions that are computationally tractable. Furthermore, we demonstrate the principle by an example that admits a suitable schedule that removes undetectable attacks.

References

[1] F. Pasqualetti, F. Dörfler, and F. Bullo, "Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, 2015.

[2] G. Joseph and C. R. Murthy, "Controllability of Linear Dynamical Systems Under Input Sparsity Constraints," *IEEE Transactions on Automatic Control*, vol. 66, no. 2, 2021.