MECH 6327 Project Report: Examining Discrete-Time Polytopic Linear Parameter-Varying Systems under threat of malicious actuator and sensor manipulation

Jonas Wagner

2021 May 14

Abstract

In this project they dynamics of Discrete-Time Polytopic Linear Parameter-Varying (LPV) Systems will be examined. Specifically, various methods for the dual state and parameter estimation will be reproduced with the intent of analyzing effectiveness of these observers against various attacks. Each method performs optimization to minimize the estimation error in various ways while remaining stable and achieving certain performance criteria. Potentially the reachability of the system may be determined for various fault and attack scenarios through the minimization of an ellipsoidal bound.

Contents

1 Polytopic Systems Background

Polytopic LPV system models are essentially a smooth interpolation of a set of LTI submodels constructed using a specified weighting function. This can be looked at as decomposing a system into multiple operating spaces that operate as linear submodels. It is possibile for a Polytopic model to take a complex nonlinear model and redefine it as a time-varying interpolation of multiple linear submodels.

Section references:[1] [2] [3] [1]

1.1 General Continuous Time Polytopic Model

The simple polyotopic LPV structure can be described by the following weighted linear combination of LTI submodels:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{r} \mu_i(\xi(t))\{A_i x(t) + B_i u(t)\} \\ y(t) = \sum_{i=1}^{r} \mu_i(\xi(t)) C_i x(t) \end{cases} \tag{1}$$

with state variable $x \in \Re^n$ common to all submodels, control input $u \in \Re^m$, output $y \in \Re^p$, weighting function $\mu_i(\cdot)$ and premise variable $\xi(t) \in \Re^w$.

Additionally, the weighting functions $\mu_i(\cdot)$ for each subsystem must satisfy the convex sum constraints:

$$0 \leq \mu_i(\xi),\ \forall i = 1, \ldots, r \ \text{ and } \ \sum_{i=1} \mu_i(\xi) = 1 \tag{2}$$

One notable downside, for our application, is the requirement for $\xi(t)$ to be explicitly known in real-time for the model to function. This requirement is the primary driving factor in investigating this system as when $\xi(t)$ is not explicitly known additional uncertainties now exist in a system that are open for exploitation by an attacker.

1.2 Discrete Time Polytopic Model

In the DT-Polytopic Model the CT-Polytopic Model, (1), is extended into the discrete time equivalence (either through sampling and zero-order holds or by definition) by the following parameter-varying system:

$$\begin{cases} x_{k+1} & = \sum_{i=1}^{N} \alpha^i (A_i x_k + B_i u_k) \\ y & = C x_k \end{cases} \tag{3}$$

with state variable $x \in \Re^n$, control input $u \in \Re^m$, and output $y \in \Re^p$ common to all submodels. Each submodel is also associated with state matricies A_i and B_i while the output is calculated from the actual state by matrix C.

The scheduling parameter, $\alpha \in \mathcal{A}$ is unknown and time-varying, with $\mathbf{A}$ defined as:

$$\mathcal{A} = \{\alpha \in \Re^N \mid \sum_{i=1}^{N} \alpha^i = 1,\ \alpha^i \geq 0 \ \ \forall\ i \in \{1, 2, \ldots, N\}\} \tag{4}$$

In the discrete time case, the unknown scheduling parameter, α, is problematic for when developing a state-estimator, thus a Joint State-Parameter estimator must be used. The discrete nature of the measurements may also prove to be even more problematic if an attack is injected in any discrete measurement.

[1] Each subsection is basically a summary of sections from these sources

1.3 Joint State-Parameter Estimation Problem

The problem of developing joint state and parameter estimator is defined as finding recursive update rules to ensure that state and parameter estimates approach the actual states and parameters. This can be described as finding f_x and f_α such that

$$\begin{cases} \hat{x}_{k+1} & = f_x(\hat{x}_k, \hat{\alpha}_k, \{u_l, y_l\}_{l=\bar{k}_x}) \\ \hat{\alpha}_{k+1} & = f_\alpha(\hat{x}_k, \hat{\alpha}_k, \{u_l, y_l\}_{l=\bar{k}_\alpha}) \end{cases} \tag{5}$$

with $\bar{k}_x, \bar{k}_\alpha < k$ result in $\|x_k - \hat{x}_k\| \to 0$ and $\|\alpha - \hat{\alpha}_k\| \to 0$ as $k \to \infty$.

1.3.1 Problem Simplifications/Assumptions [1]

For simplicity, and probably for feasibility reasons, the following assumptions will also be made:

1. $\alpha \in \mathcal{A}$ is constant (or at least slowly time-varying)
2. The estimated system is observable $\forall\ \hat{\alpha} \in \mathcal{A}$, (i.e. $(\sum_{i=1}^N \hat{\alpha} A_i, C)$ is an observable pair)
3. A unique solution exists to the joint-estimation problem $C\Big(qI - \sum_{i=1}^N \alpha^i A_i x_k\Big)^{-1} \sum_{i=1}^N \alpha^i B_i = C\Big(qI - \sum_{i=1}^N \hat{\alpha}^i A_i x_k\Big)^{-1} \sum_{i=1}^N \hat{\alpha}^i B_i \implies \alpha = \hat{\alpha}$

1.3.2 Observer Definition

A

2 Project Objectives

The primary objective of this project will be to reproduce three joint state and parameter estimator methods for LPV systems then test the ability of each to react to malicious input and measurement interference. A secondary/future objective will be to calculate the reachability set and how it is manipulated due to an attack on the system.

The three estimation methods of interest [2] include:

1. Dual-Estimation (DE) approach is a method that first solves a two step optimization problem for parameters-estimation and then uses a "traditional" robust polytopic observer design for state estimation. [1]

2. Extended Kalman Filter (EKF) using prediction and update steps for the system estimates, but this version does require the assumption of Gaussian noise. [1]

3. Interacting Multiple Model estimation (IMM) method which uses a different kalmen filter for multiple modes and the probability that the system will be a certain mode.[4]

The next objective will be to show how much each attack method can effect the states (specifically the reachable set) for each estimator.[3] This work is very similar to [6] but will be expanding from stochastic DT-LTI systems to deterministic DT-LPV systems.

3 Proposed Methods

The following steps will be taken to complete the problem.

1. This project will begin by reproducing the results of joint state and parameter estimation from [1] using the same LPV system used in the paper. (This will likely be done using Simulink with custom estimator blocks.)

2. Next attacks will be introduced into the sensor and the response for each estimator will be compared.

3. This will then be expanded to a more interesting system[4] that will be more useful for sensor attack testing (i.e. more sensors then states or high noise system).

4. Finally, an analysis of the reachable set deviation due to attacks will be performed by finding a minimal ellipsoid constraining the states that would be reachable prior to attack detection.[5]

[2]taken directly from [1] and we are essentially recreating these results but performing additional tests

[3]and potentially develop a better solution... modifying [5]?

[4]Seperator Testbed? scheduling parameters being valve on/off and for various linearized tank level systems... is it possible to analyze with a scheduling parameter dependent on a state???... Otherwise a more complicated electrical network w/ switches or pneumatic system could be done instead

[5]possibly future work

References

[1] H. Beelen and M. Donkers, "Joint state and parameter estimation for discrete-time polytopic linear parameter-varying systems," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 9778–9783, 2017.

[2] R. Orjuela, D. Ichalal, B. Marx, D. Maquin, and J. Ragot, "Chapter 9 - polytopic models for observer and fault-tolerant control designs," in *New Trends in Observer-Based Control* (O. Boubaker, Q. Zhu, M. S. Mahmoud, J. Ragot, H. R. Karimi, and J. Dávila, eds.), Emerging Methodologies and Applications in Modelling, pp. 295–335, Academic Press, 2019.

[3] R. Orjuela, B. Marx, J. Ragot, and D. Maquin, "Nonlinear system identification using heterogeneous multiple models," *International Journal of Applied Mathematics and Computer Science*, vol. 23, no. 1, pp. 103–115, 2013.

[4] Y. Bar-Shalom, X. R. Li, and T. Kirubarajan, *Estimation with applications to tracking and navigation: theory algorithms and software*. John Wiley & Sons, 2004.

[5] M. H. Basiri, J. G. Thistle, J. W. Simpson-Porco, and S. Fischmeister, "Kalman filter based secure state estimation and individual attacked sensor detection in cyber-physical systems," in *2019 American Control Conference (ACC)*, pp. 3841–3848, 2019.

[6] N. Hashemi, C. Murguia, and J. Ruths, "A comparison of stealthy sensor attacks on control systems," in *2018 Annual American Control Conference (ACC)*, pp. 973–979, IEEE, 2018.