Resilient Adaptive Control with Application to Vehicle Cruise Control

James Weimer, Nicola Bezzo, Miroslav Pajic,
George Pappas, Oleg Sokolsky, and Insup Lee

School of Engineering and Applied Sciences
University of Pennsylvania
Philadelphia, PA 19104, USA
{weimerj,nicbezzo,pajic,pappasg}@seas.upenn.edu
{sokolsky,lee}@cis.upenn.edu

Abstract. This work address the general problem of resilient control of unknown stochastic linear time-invariant (LTI) systems in the presence of sensor attacks. Motivated by a vehicle cruise control application, this work considers a first order system with multiple measurements, of which a bounded subset may be corrupted. A frequency-domain-designed resilient adaptive controller is introduced that simultaneously minimizes the effect of corrupted sensors, while maintaining a desired closed-loop performance, invariant to unknown model parameters. Simulated results illustrate that the resilient parameter-invariant controller is capable of stabilizing unknown state disturbances and can perform state trajectory tracking with a lag.

Keywords: Secure Cyber-Physical Systems, Adaptive Control, Resilient Sensor Fusion

1 Introduction

Modern large-scale control systems are becoming more and more integrating into our daily lives. As the integration of smart devices in modern control systems increases, so does the need for potential for attacks. Today, our dependence on integrated controllers automates everything from inter-home appliances to nation-wide power distribution, where the effect of unpredicted behaviors can range from a minor inconvenience of resetting a smart device to a regional blackout. Our dependence on these closed-loop automated systems requires that their performance be robust to both malicious behavior and non-malicious behavior.

With respect to the vehicle cruise control system, non-malicious agents include environmental variables (gravity, wind speed, parts fatigue and failure, etc.) while malicious behavior can be introduces through sensor spoofing. Employing redundant measurements is a well established method of providing better estimates of control variables and model parameters; however, when attacked, a redundant measurement can be used as a means to destabilize a control system. Thus, to ensure safe performance of the vehicle cruise control requires securing

the sensory data, while simultaneously designing controllers robust to unknown environmental parameters.

Literature review: The design of algorithms which are resilient against faults or unknown parameters has been addressed from many points of view, including fault detection [1], robust control [2], adaptive control [3], and more generally from estimation and hypothesis testing [4]. In general, these approaches address the issue of maximizing some performance measure with respect to a known or bounded disturbances. In the context of security against malicious attacks, many of these approaches are not applicable because of their assumption that the attack is either known or bounded, with notable exceptions being approaches which ask for invariance to the unknown parameters [5]. The remainder of this literature review focuses on secure estimation/control and control of unknown systems, respectively.

Secure estimation and control system design in the presence of disturbances or attacks has received increasing research interest [6,7,8,9,10,11]. Most closely related to the work presented herein is [12], which addresses the secure estimation and control of linear deterministic systems under malicious sensor attacks. While the approach in [12] is shown to stabilize the systems under consideration, their approach requires full knowledge of the underlying system dynamics in order to secure the closed-loop system. When the underlying dynamics are unknown (and potentially stochastic) more robust detection and control algorithms are needed.

Control of unknown linear continuous-time systems can be approached through adaptive control techniques [3], typically based on a Lyapunov stability requirement. Adaptive control is generally classified as either indirect (estimation of model parameters) or direct (estimation of the control sequence), where direct adaptive control is more robust than indirect adaptive control, since the parameter estimation may not be accurate over all frequencies. In general, however, these continuous-time techniques do not extend to discrete-time systems [13,14], in large part, due to the difficulty in identifying a candidate Lyapunov function. Although the design of discrete-time adaptive controllers have been studied [15], their stochastic formulations and specification-based design with respect to closed-loop security requirements are, to the best of our knowledge, open research problems.

Statement of contributions: Beyond the previous work, this work focuses on the specification-based design of resilient adaptive controllers for stochastic linear time-invariant systems, with specific interest in vehicle cruise control systems. The primary technical contributions of this work are: (a) a resilient sensor fusion strategy for unknown attacks on noisy measurements; (b) a finite-horizon mean-stabilizing adaptive controller; (c) a sensor fusion and controller co-design requirement that satisfies a stochastic Lyapunov criteria.

Structure of the paper: Section 2 identifies notation and preliminary definitions that will be utilized repeatedly throughout the paper. Section 3 formulates pre-

cisely the problem considered in this work. We introduce the resilient sensor fusion strategy and adaptive controller in Section 4. A co-design requirement for satisfying the performance specification is provided in Section 5. Section 6 presents numerical evaluations of the resilient adaptive controller in the presence of sensor attacks for vehicle cruise control. The concluding section provides discussion and proposes future extensions.

2 Notation and Preliminaries

This section introduces notation and preliminary definitions that prove useful in the remainder of this work.

2.1 Notation

In this subsection, we illustrate the various variable notations using varying fonts and capitalization of the letter z:

- plain upper case italic fonts $\rightarrow$ constant, Z;
- plain lower case italic fonts $\rightarrow$ scalar (or function with scalar range), z;
- bold lower case italic fonts $\rightarrow$ vector (or function with vectoral range), $\boldsymbol{z}$;
- bold lower case plain fonts $\rightarrow$ vector of concatenated vectors, $\mathbf{z}$;
- bold upper case italic fonts $\rightarrow$ matrix, $\boldsymbol{Z}$;

For vectors we write $\boldsymbol{z}_i$ to denote the i-th position of $\boldsymbol{z}$ and $\boldsymbol{z}_{i:j}$ to be the sub-vector of $\boldsymbol{z}$ consisting of the i-th through j-th elements, inclusively. Similarly, For vectors of vectors we write $\mathbf{z}_i$ to denote the i-th sub-vector and $\mathbf{z}_{i:j}$ to be the sub-vector of $\mathbf{z}$ consisting of the i-th through j-th sub-vectors, inclusively. Lastly, for matrices we write $\boldsymbol{Z}_i$ to be the i-th column of $\boldsymbol{Z}$ and $\boldsymbol{Z}_{i:j}$ to be the sub-matrix consisting of the i-th through j-th columns, inclusively.

We use the notation $\Pr[x|y]$ and $\mathbb{E}[x|y]$ to denote the probability of x given y and the expected value of x given y, respectively,

2.2 Preliminaries

This subsection defines matrices and constants which appear in the remainder of this work. Consistent with the previous subsection's use of the letter z to illustrate various properties, we write $\boldsymbol{P}_{\boldsymbol{Z}}$ to be the projection matrix corresponding the general matrix $\boldsymbol{Z}$ and $\boldsymbol{P}_{\boldsymbol{Z}}^{\perp}$ to be the projection matrix corresponding to the null-space of $\boldsymbol{Z}$,

$$\boldsymbol{P}_{\boldsymbol{Z}} = \boldsymbol{Z}\left(\bar{\boldsymbol{Z}}^{\top}\boldsymbol{Z}\right)^{-1}\bar{\boldsymbol{Z}}^{\top} \quad \text{and} \quad \boldsymbol{P}_{\boldsymbol{Z}}^{\perp} = \boldsymbol{I} - \boldsymbol{P}_{\boldsymbol{Z}},$$

where $\bar{\boldsymbol{Z}}^{\top}$ is notation denoting the transpose of the complex conjugate of $\boldsymbol{Z}$ and $\boldsymbol{I}$ the identity matrix.

For an arbitrary positive integer $N \in \mathbb{N}^+$, $\omega = \frac{2\pi\sqrt{-1}}{N}$, $\lambda(n) = \mathbf{e}^{\omega n}$, we define the matrices $\boldsymbol{V}, \boldsymbol{\Lambda} \in \mathbb{C}^{N\times N}$ as

$$\begin{aligned}\boldsymbol{\Lambda} &= \text{diag}[\lambda(0), \ldots, \lambda(N-1)] \\ \boldsymbol{V}_n &= \frac{1}{\sqrt{N}}\left[1, \quad (\lambda(n))^1, \quad \ldots, \quad (\lambda(n))^{N-1}, \right]^\top\end{aligned}$$

and note that $\boldsymbol{V}$ is the normalized N-point Discrete Fourier Transform (DFT) matrix [], such that

$$\bar{\boldsymbol{V}}^\top \boldsymbol{V} = \boldsymbol{V}\bar{\boldsymbol{V}}^\top = \boldsymbol{I}$$

The notation and preliminaries introduced in this section will be employed throughout the remainder of this work to formulate a resilient parameter-invariant controller.

3 Problem Formulation

This section introduces a resilient control problem for a system with unknown LTI-Gaussian dynamics and (potentially) corrupted measurements.

Specifically, we consider an LTI system with a single state that evolves according to

$$\begin{aligned}x(k+1) &= ax(k) + bu(k) + w(k) \\ \boldsymbol{y}(k) &= \boldsymbol{c}x(k) + \boldsymbol{v}(k) + \boldsymbol{d}(k)\end{aligned} \tag{1}$$

where:

- $x, u \in \mathbb{R}$, are the state and control input, respectively;
- $a, b \in \mathbb{R}$ are the state dynamic and control input gains;
- $\boldsymbol{y}, \boldsymbol{c}, \boldsymbol{d} \in \mathbb{R}^{\mathbb{N}}$, are the measurements, state measurement gain, and corruption, respectively;
- $w \in \mathbb{R}$ and $\boldsymbol{v} \in \mathbb{R}^N$ are uncorrelated i.i.d. Gaussian process noise and measurement noise with central moments[1]:

$$\begin{aligned}\mathbb{E}\left[w\right] &= \mu & \mathbb{E}\left[\boldsymbol{v}\right] &= \boldsymbol{0} \\ \mathbb{E}\left[\left(w-\mu\right)^2\right] &= \sigma & \mathbb{E}\left[\left(\boldsymbol{v}\boldsymbol{v}^\top\right)^2\right] &= \boldsymbol{I}\end{aligned}$$

At time k, the model information available in this work is summarized in the following assumption:

[1] Without loss of generality, we assume the measurement noise is white and normalized to unit variance, where colored noise and non-unit variance white noise can be whitened by applying a normalizing pre-whitening filter.

Assumption 1 - Available Information:

- the time-series measurements, $\mathbf{y} = \left[\boldsymbol{y}^\top(0), \ldots, \boldsymbol{y}^\top(k)\right]^\top$;
- the time-series control inputs, $\mathbf{u} = \left[u(0), \ldots, u(k)\right]^\top$;
- the variance of the process noise, σ;
- the state measurement gain, $\boldsymbol{c}$;
- the state dynamics, control gain, and process noise mean are constant.

In words, we assume that the measurements, measurement state gain, inputs, and noise covariances are known; however, the dynamics and process bias governing the evolution of the state are unknown, but constant. For completeness, we summarize the unavailable information in the following assumption:

Assumption 2 - Unavailable Information:

- the state dynamics, a
- the control gain, b;
- the process noise mean, μ;
- the time-series measurement corruption, $\mathbf{d} = \left[\boldsymbol{d}^\top(0), \ldots, \boldsymbol{d}^\top(k)\right]^\top$.

Although we assume the measurement corruption is unknown, we assume a maximum of M measurements are corrupted, as defined in the following assumption:

Assumption 3 - Measurement Corruption Structure: At each time step, at most M measurements are corrupted, $\|\boldsymbol{d}(k)\|_0 \leq M$, where

$$M = \begin{cases} \frac{N}{2} - 1\,, & N \text{ even} \\ \frac{N-1}{2}\,, & N \text{ odd} \end{cases}$$

such that for

$$\left\{\boldsymbol{P}_{\boldsymbol{d}}^{\perp}\right\} := \left\{\boldsymbol{Q}^\top\boldsymbol{Q} \middle|\ \boldsymbol{Q} \in \{0,1\}^{T\times N},\ \ \boldsymbol{Q}\boldsymbol{Q}^\top = \boldsymbol{I},\ \ T > N - M\right\}$$

the following is true:

$$\boldsymbol{F}\boldsymbol{d}(k) = \mathbf{0},\ \ \exists \boldsymbol{F} \in \left\{\boldsymbol{P}_{\boldsymbol{d}}^{\perp}\right\}$$

Assumption 3 is consistent with the assumption in [12] and implies a maximum of M corrupted measurements since elements of $\boldsymbol{d}(k)$ which equal zero, imply no

corruption is applied to the corresponding measurement. Under the assumptions introduced in this section, we wish to solve the following problem:

Problem 4 - Stochastic Boundedness: Given (1) and assumptions 1-3, show that

$$\mathbb{E}\left[\|x(k+1)\|^2\right] \leq \alpha^\star \|x(k)\|^2, \quad \forall \quad \|x(k)\|^2 \geq \eta \tag{2}$$

where $\eta \in \mathbb{R}$ is a desired state convergence threshold and $\alpha^\star \in [0,1]$ denotes a desired state convergence rate.

The problem introduced in this section is addressed in the following section by introducing criteria for resilient sensor fusion and parameter-invariant control.

4 Main Contributions

The main contributions of this work are summarized in the following propositions:

Proposition 5 Resilient Sensor Fusion: Given (1), then

$$\hat{\boldsymbol{P}}_{\boldsymbol{d}}^{\perp} = \arg \min_{\boldsymbol{Q} \in \{\boldsymbol{P}_{\boldsymbol{d}}^{\perp}\}} \frac{\left(\|\boldsymbol{P}_{\boldsymbol{Qc}}^{\perp} \boldsymbol{y}(k)\|^2 - \|Q\|_0 + 1\right)^2}{2\left(\|Q\|_0 - 1\right)} \quad \Longrightarrow \quad \mathbb{E}\left[\hat{\boldsymbol{P}}_{\boldsymbol{d}}^{\perp} \boldsymbol{d}(k)\right] = \boldsymbol{0}$$

Proposition 6 Parameter Invariant Control: Given (1), $\alpha \in [0,1]$, positive integers $k, \kappa \in \mathbb{N}$ satisfying

$$k \leq \kappa \leq 2k - 4,$$

a $(\kappa+1)$-point DFT matrix, $\boldsymbol{V}$, and

$$\boldsymbol{s}_n = \begin{cases} \mathbb{E}\left[x(n)|\boldsymbol{y}(n)\right], & n \in \{0, \ldots, k-1\} \\ \alpha^{n-k}\mathbb{E}\left[x(k)|\boldsymbol{y}(k)\right], & n \in \{k, \ldots, \kappa\} \end{cases}$$

$$\boldsymbol{H} = [\boldsymbol{\Lambda V s}, \quad \boldsymbol{V s}, \quad \textstyle\sum_{n=0}^{\kappa} \boldsymbol{V}_n, \quad \boldsymbol{V}_0]$$

then, assuming $\mathbf{u}_{0:k-1} \neq \boldsymbol{0}$,

$$\boldsymbol{P}_{\boldsymbol{H}}^{\perp} \boldsymbol{V} \mathbf{u}_{0:\kappa-1} = \boldsymbol{0} \quad \Longrightarrow \quad \mathbb{E}\left[x(t)|\mathbf{y}_{0:k}\right] = \alpha^{t-k}\mathbb{E}\left[x(k)|\boldsymbol{y}(k)\right] \quad \forall k \leq t \leq \kappa$$

The following subsections discuss proposition 5 and proposition 6, respectively. The propositions discussed in this section are utilized in the following section to design a resilient model-invariant controller that satisfies the stochastic boundedness constraint in problem 4.

4.1 Resilient Sensor Fusion

Designing a stabilizing controller for problem 4 requires information feedback through sensor measurements. When corrupted by an unmodelled attacker, the sensor contains no information with respect to the system state. Moreover, inclusion of corrupted measurements in state estimation infects the information provided by the uncorrupted sensors. The purpose of resilient sensor fusion is to identify a set of sensors that are expected to be unaffected by the measurement corruption vector, $d(k)$, (i.e. reside in the null space of $d(k)$) and to generate a minimum mean squared estimate of the state, $x(k)$. From assumption 3, and consistent with the standard assumptions in the related work [12], we assume that there are at least $M+1$ sensors which are uncorrupted. However, unlike the previous work, this problem considers uncorrupted measurements that are inherently noisy and that corrupted sensors can change at each time-step. Coupled with the fact that the underlying dynamics are unknown (by assumption 2), the resilient sensor fusion strategy at time k is limited to using only sensor measurements provided at time k, and no prior information on the state (as prior information on the state will propagate previously corrupted information). In this subsection, we develop a resilient sensor fusion strategy that estimates the null space of the corruption, denoted as $\hat{\boldsymbol{P}}_{\boldsymbol{d}}^{\perp} \in \{\boldsymbol{P}_{\boldsymbol{d}}^{\perp}\}$, invariant to the value of the state and corruption, which is employed to generate a MMSE state estimate. Specifically, the design of the resilient sensor fusion strategy is organized into three steps

1. formulate a maximally invariant statistic;
2. estimate the measurement corruption null space;
3. generate a MMSE state estimate.

These steps are respectively addressed in the remainder of this subsection.

Maximally Invariant Statistic: Assuming a candidate null space, $Q \in\in \{\boldsymbol{P}_{\boldsymbol{d}}^{\perp}\}$, and consistent with optimal signal detection theory [5], we write a maximally invariant statistic for $d(k)$, invariant to the unknown state, $x(k)$, as

$$\boldsymbol{P}_{\boldsymbol{Q_c}}^{\perp}\boldsymbol{y}(k) = \boldsymbol{P}_{\boldsymbol{Q_c}}^{\perp}\left(\boldsymbol{d}(k) + \boldsymbol{v}(k)\right).$$

The maximally invariant statistic is a statistic of the measurements which contains all the information with respect to $d(k)$ that is invariant to the unknown state, $x(k)$.

Corruption Null Space: It is known that there exists no uniformly most powerful (UMP) test for detecting an unknown vectored signal [5], where the UMP test is considered optimal in hypothesis testing. Following well established practices employed in bad-data detection, we estimate the corruption null space according to proposition 5, the implication of which is described in the following proof:

Proof. Given the maximally invariant statistic, $\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}\boldsymbol{y}(k)$, the norm-squared of the measurement statistic, $\|\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}\boldsymbol{y}(k)\|^2$, has a non-central chi-squared distribution of $\|Q\|_0 - 1$ degrees of freedom and non-centrality parameter $\|\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}\boldsymbol{d}(k)\|^2$. Observing that when $\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}\boldsymbol{d}(k) = 0$, the following central moments of the norm-squared measurement statistic are known:

$$\mathbb{E}\left[\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}\boldsymbol{y}(k)|\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}\boldsymbol{d}(k) = 0\right] = \|Q\|_0 - 1$$
$$\mathrm{Cov}\left[\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}\boldsymbol{y}(k)|\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}\boldsymbol{d}(k) = 0\right] = 2(\|Q\|_0 - 1)$$

From assumption 3, we recall $\boldsymbol{P}_{\boldsymbol{Qc}}\boldsymbol{d}(k) = \boldsymbol{0}, \;\; \exists \boldsymbol{Q} \in \{\boldsymbol{P}^{\perp}_{\boldsymbol{d}}\}$. Thus, it is expected $\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}$ is in the null space of $\boldsymbol{d}(k)$ when the normalized mean-squared error of the norm-squared measurement is minimized, conditioned on $\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}\boldsymbol{d}(k) = 0$. None

State Estimation: Given the expected null space of the corruption, the minimum mean-squared error estimate of the state is

$$\mathbb{E}\left[x(k)|\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}, \boldsymbol{y}(k)\right] = \left(\boldsymbol{c}^{\top}\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}\boldsymbol{c}\right)^{-1}\boldsymbol{c}^{\top}\boldsymbol{P}^{\perp}_{\boldsymbol{Qc}}\boldsymbol{y}(k).$$

4.2 Parameter Invariant Control

The parameter invariant controller utilizes a time-history of the state estimates and control inputs to design a finite-horizon controller that stabilizes the mean and is invariant to the unknown system dynamics.

Proof. Defining $\hat{x}(k) = \mathbb{E}\left[x(k)|\boldsymbol{y}(k)\right]$, we consider the following time-series generated by (1),

$$\begin{bmatrix} \hat{x}(0) \\ \hat{x}(1) \\ \vdots \\ \hat{x}(k) \\ \alpha\hat{x}(k) \\ \vdots \\ \alpha^{\kappa-k}\hat{x}(\kappa) \end{bmatrix} = \begin{bmatrix} 1 & & & & & & \\ -a & 1 & & & & & \\ & \ddots & \ddots & & & & \\ & & -a & 1 & & & \\ & & & -a & 1 & & \\ & & & & \ddots & \ddots & \\ & & & & & -a & 1 \end{bmatrix}^{-1} \begin{bmatrix} \hat{x}(0) \\ \mu + bu(0) \\ \vdots \\ \mu + bu(k-1) \\ \mu + bu(k) \\ \vdots \\ \mu + bu(\kappa-1) \end{bmatrix}$$

$$\iff \begin{bmatrix} \hat{x}(0) \\ \hat{x}(1) \\ \vdots \\ \hat{x}(k) \\ \alpha\hat{x}(k) \\ \vdots \\ \alpha^{\kappa-k}\hat{x}(\kappa) \end{bmatrix} = \begin{bmatrix} 1 & & & & & & -a \\ -a & 1 & & & & & \\ & \ddots & \ddots & & & & \\ & & -a & 1 & & & \\ & & & -a & 1 & & \\ & & & & \ddots & \ddots & \\ & & & & & -a & 1 \end{bmatrix}^{-1} \begin{bmatrix} \hat{x}(0) - a\alpha^{\kappa-k}\hat{x}(k) \\ \mu + bu(0) \\ \vdots \\ \mu + bu(k-1) \\ \mu + bu(k) \\ \vdots \\ \mu + bu(\kappa-1) \end{bmatrix}$$

$$\iff \boldsymbol{s} = \bar{\boldsymbol{V}}^{\top} \left(\boldsymbol{I} + a\boldsymbol{\Lambda}\right)^{-1} \boldsymbol{V} \begin{bmatrix} \hat{x}(0) - a\alpha^{\kappa-k}\hat{x}(k) \\ b\mathbf{u}_{0:\kappa-1} + \mu\mathbf{1} \end{bmatrix}$$

$$\iff \boldsymbol{V}\boldsymbol{s} = \left(\boldsymbol{I} + a\boldsymbol{\Lambda}\right)^{-1} \boldsymbol{V} \begin{bmatrix} \hat{x}(0) - a\alpha^{\kappa-k}\hat{x}(k) \\ b\mathbf{u}_{0:\kappa-1} + \mu\mathbf{1} \end{bmatrix}$$

$$\iff \mathbf{0} = \boldsymbol{H}\boldsymbol{\theta} + \boldsymbol{V}_{1:\kappa}\mathbf{u}_{0:\kappa-1}$$

$$\iff \boldsymbol{P}_{\boldsymbol{H}}^{\perp}\boldsymbol{V}_{1:\kappa}\mathbf{u}_{0:\kappa-1} = \mathbf{0} \qquad \text{(by Nyquist-Shannon Theorem)}$$

where

$$\boldsymbol{\theta} = \left[-\tfrac{a}{b}, -\tfrac{1}{b}, \tfrac{\mu}{b}, \tfrac{x(0) - ax(\kappa) - \mu}{b} \right]^{\top}.$$

The first implication transforms the time-series signal into an equivalent κ-step periodic signal by augmenting the initial condition. By the Nyquist-Shannon Theorem, the future control inputs, $\mathbf{u}_{k:\kappa-1}$, can be reconstructed from the previous measurements, a desired state trajectory, and the past control inputs, $\mathbf{u}_{0:k-1}$ if $\kappa < 2k - \|\Theta\|_0$. Since this criteria is satisfied in the worst-case by assuming all parameters are non-zero, the control sequence that generates the desired future state trajectory is reconstructed by solving

$$\boldsymbol{P}_{\boldsymbol{H}}^{\perp}\boldsymbol{V}_{1:\kappa}\mathbf{u}_{0:\kappa-1} = \mathbf{0}$$

assuming $\kappa < 2k - 4$. None

Recalling that the controller is design to stabilize the mean through an additive control input, the predicted covariance of the state is given in the following corollary:

Corollary 7 - Covariance of Predicted State:

$$\mathrm{Cov}\left[x(t)|\boldsymbol{P}^{\perp}_{\bar{\boldsymbol{Q}}\boldsymbol{c}}, \boldsymbol{y}(k)\right] = \mathrm{Cov}\left[x(k)|\boldsymbol{P}^{\perp}_{\bar{\boldsymbol{Q}}\boldsymbol{c}}, \boldsymbol{y}(k)\right] + a^{t-k-1}\sigma, \quad \forall t \geq k$$

Satisfying the equality constraint in proposition 6 restricts the horizon for which the controller can be designed. As a best estimate of the control sequence which satisfies proposition 6, we employ a maximum likelihood estimate of the future control sequence as

$$\mathbf{u}_{k:\kappa-1} = -\boldsymbol{G}\mathbf{u}_{0:k-1} \tag{3}$$

where

$$\boldsymbol{G} = \left(\bar{\boldsymbol{V}}^{\top}_{k+1:\kappa}\boldsymbol{P}^{\perp}_{\boldsymbol{H}}\boldsymbol{V}_{k+1:\kappa}\right)^{-1}\bar{\boldsymbol{V}}^{\top}_{k+1:\kappa}\boldsymbol{P}^{\perp}_{\boldsymbol{H}}\boldsymbol{V}_{0:k-1} \tag{4}$$

The resilient sensor fusion strategy presented in this section identifies a maximum likelihood estimate of the corruption null space, consistent with commonly adopted goodness-of-fit approaches. The resulting estimator is employed to design a parameter-invariant control sequence which stabilizes the mean of the estimate at a convergence rate of α.

5 Resilient Parameter-Invariant Controller Design

From the previous section, it is clear that the performance of the resilient state estimator affects the parameter-invariant controller. Since it is a primary concern to secure the measurements against malicious attacks, and a secondary concern to maximize the performance with respect to the environmental unknowns, we propose the following lemma to design the parameter-invariant controller convergence rate, α:

Lemma 8 - Controller Design : Given problem 4, $\hat{\boldsymbol{P}}^{\perp}_{\boldsymbol{d}}$ from proposition 5, then a control sequence $\mathbf{u}$ in proposition 6 designed assuming α will satisfy (2) if and only if

$$0 \leq \alpha \leq \sqrt{\frac{\alpha^{\star} - \frac{\sigma + \boldsymbol{c}^{\top}\hat{\boldsymbol{P}}^{\perp}_{\boldsymbol{d}}\boldsymbol{c}}{\eta}}{\frac{1}{\eta\boldsymbol{c}^{\top}\hat{\boldsymbol{P}}^{\perp}_{\boldsymbol{d}}\boldsymbol{c}} + 1}}$$

Proof. We define $\boldsymbol{l} = \hat{\boldsymbol{P}}_{\boldsymbol{d}}^{\perp}\boldsymbol{c}(\boldsymbol{c}^{\top}\hat{\boldsymbol{P}}_{\boldsymbol{d}}^{\perp}\boldsymbol{c})^{-1}$, and write

$$
\begin{aligned}
\alpha \leq \sqrt{\frac{\alpha^{\star} - \frac{\sigma + \boldsymbol{l}^{\top}\boldsymbol{l}}{\eta}}{\frac{1}{\eta}\boldsymbol{l}^{\top}\boldsymbol{l} + 1}} \quad &\Longleftrightarrow \quad \alpha^2\left(\frac{\boldsymbol{l}^{\top}\boldsymbol{l}}{\eta} + 1\right) + \frac{\sigma + \boldsymbol{l}^{\top}\boldsymbol{l}}{\eta} \leq \alpha^{\star} \\
\Longleftrightarrow \alpha^2\left(\boldsymbol{l}^{\top}\boldsymbol{l} + \|x(k)\|^2\right) + \left(\boldsymbol{l}^{\top}\boldsymbol{l} + \sigma\right) &\leq \alpha^{\star}\|x(k)\|, \quad \forall \quad \|x\|^2 \geq \eta \\
\Longleftrightarrow \mathbb{E}\left[\|\alpha\mathbb{E}\left[x(k)|\boldsymbol{y}(k)\right]\|^2 + \mathrm{Cov}\left[x(k+1)|\boldsymbol{y}(k)\right]\right] &\leq \alpha^{\star}\|x(k)\|, \quad \forall \quad \|x\|^2 \geq \eta \\
\Longleftrightarrow \mathbb{E}\left[\|\mathbb{E}\left[x(k+1)|\boldsymbol{y}(k)\right]\|^2 + \mathrm{Cov}\left[x(k+1)|\boldsymbol{y}(k)\right]\right] &\leq \alpha^{\star}\|x(k)\|, \quad \forall \quad \|x\|^2 \geq \eta \\
\Longleftrightarrow \mathbb{E}\left[\|x(k+1)\|^2\right] &\leq \alpha^{\star}\|x(k)\|, \quad \forall \quad \|x\|^2 \geq \eta
\end{aligned}
\tag{5}
$$

None

A direct consequence of lemma (8) is the following corollary identifying when a resilient parameter-invariant controller exists that satisfies the performance criteria in (2).

Corollary 9 - Controller Existence : A resilient parameter-invariant controller satisfying (2) exists if and only if

$$\boldsymbol{c}^{\top}\hat{\boldsymbol{P}}_{\boldsymbol{d}}^{\perp}\boldsymbol{c} \leq \alpha^{\star}\eta - \sigma$$

By applying Markov's inequality to lemma 8, a probabilistic bound on the likelihood the state diverges is provided in the following corollary:

Corollary 10 - Probability of Divergence: Assuming lemma 8,

$$\Pr\left[\|x(k+1)\| \geq \|x(k)\|\right] \leq \alpha^{\star}, \quad \forall \quad \|x\|^2 \geq \eta \quad \text{(Markov's inequality)}$$

The parameter invariant controller formulated in this section is evaluated through simulation in the following section.

6 Simulation Results

This section provides a qualitative evaluation of the resilient parameter-invariant controller. This evaluation is presented in two subsections. The following subsection presents disturbance rejection results considering first order systems, both unstable and stable, when sensor corruption is both present and absent. The final subsection presents a simulated cruise control scenario for a Landshark robotic platform.

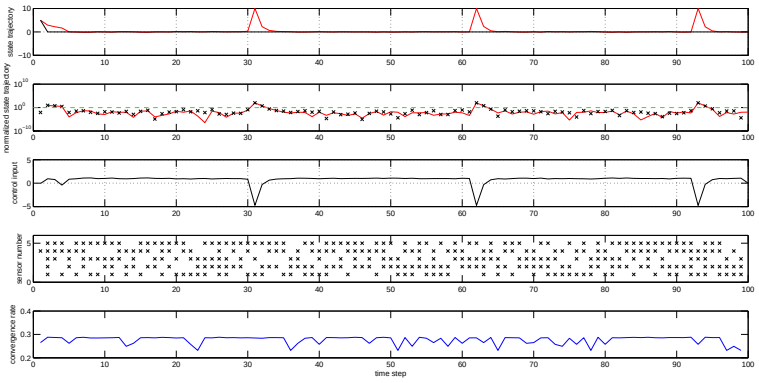

Fig. 1. Stable system ($a = 0.8$) with no sensor attacks.

6.1 Disturbance Rejection

In this subsection, we evaluate the resilient parameter-invariant controller with respect to disturbance rejection. We consider the following global variables for all simulations in this subsection

- $b = 0$ (input gain);
- $C = [2, 3, 4, 5, 10]^\top$ (measurement gain);
- $x(0) = 5$ (initial condition);
- $\mu = -1$ (process noise mean);
- $\sigma = .01$ (process noise covariance);
- $\alpha^\star = .1$, $\eta = 1$ (stochastic boundedness parameters);

Additionally, we use a windowed approach for the controller design, where we use the last 20 measurements (19 previous inputs), to design a 10-step finite horizon control sequence at each time step. Assuming this system and controller design strategy, we evaluate the resilient controller when the system is stable ($a = 0.8$) and unstable ($a = 1.8$) under the attack conditions when all the sensors are uncorrupted, and when the first and last sensors are corrupted by a random attacker using a zero-mean Gaussian attack with variance 10. The remainder of this subsection addresses these four scenarios: (a) stable, no corruption; (b) stable, with corruption; (c) unstable, no corruption; (d) unstable, with corruption.

Fig. 1 presents the results for a stable system with no sensor attacks. In Fig. 1, we simulate a state disturbance injection (beyond the process noise) occurring every 30 time steps. It is clear that the controller is capable of stabilizing the system, and achieves the performance bound on the norm of the state; however, we note that despite no attacks being present in this simulation it is assumed that some of the sensor measurements are corrupted at most time steps. This

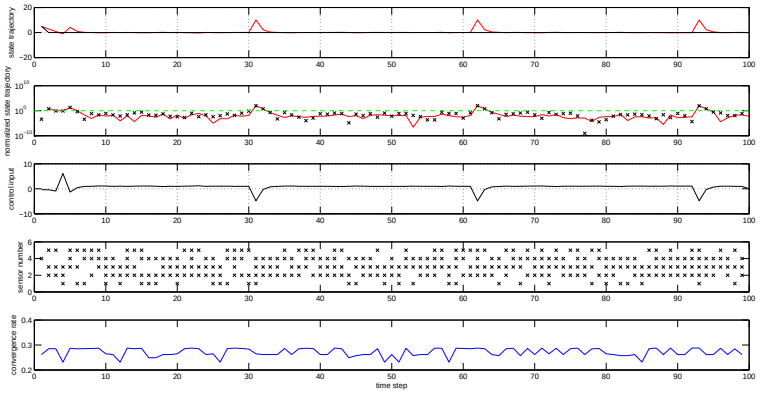

Fig. 2. Stable system ($a = 0.8$) with sensor 1 and 5 under attack.

results from the fact that unlike classical state-estimators, which minimize the mean-squared error of the state estimate, the resilient sensor fusion minimizes a normalized deviation of the measured sensor noise from a weighted average of the sensor measurements. This results in the rejection of measurements which are significantly different from the mean of the sensor measurements. As a consequence, depending on the specific subset of measurements accepted as secure, the controller convergence rate changes to maintain the performance specification.

Simulated results for a stable system in the presence of sensor attacks is presented in Fig. 2. We consider the same state disturbance injection as in Fig. 1, and observe a very similar performance in terms of disturbance rejection. However, this comes at the cost of an increased variance in the controller sequence (as compared to Fig. 1). The increased variance is undesirable in most physical actuators since this results in increased strain and fatigue on mechanical parts. The increased variance is a direct result of designing the controller sequence to match the performance specification, and can be reduced by upper bounding the desired state convergence rate, α, employed by the parameter-invariant controller. Through a comparison between Fig. 1 and Fig. 2 that in the presence of sensor attacks on sensor one and sensor five, sensor one is selected significantly less when under attack and sensor five is selected only marginally less, despite being corrupted by the same attack. This is expected since given the same attack, signal-to-corruption ratio is greater in sensor five than in sensor one. Recalling that the measurement model in (1) is normalized such that all the sensors have the same noise profile, sensor five having a higher signal-to-corruption ratio (assume the same attack) than sensor one is equivalent to stating that since sensor five is less noisy than sensor one, sensor five is more likely to be trusted.

A unstable system with no sensor attacks is considered in Fig. 3. Similar to the results for the stable system, here we observe that resilient parameter-

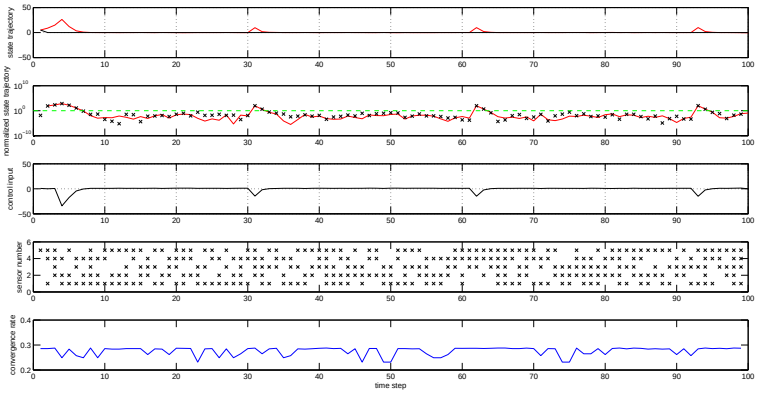

Fig. 3. Unstable system ($a = 1.8$) with no sensor attacks.

invariant controller stabilizes the system with respect to unknown disturbances, and has a response very similar to the stable system results in Fig. 1. Although the control input is different, the performance is nearly identical, which is a direct result of the controller design requirement to be invariant to the unknown system parameters, regardless of stability. Similarly, we notice a similar sensor selection and rejection profile as in Fig. 1. This result is consistent with the fact that the sensor fusion strategy is design invariant to the unknown state, which orthogonalizes the issues of stability and resilience for the purposes of identifying corrupted sensors.

The final figure in this subsection, Fig. 4, illustrates the results when considering an unstable system and with sensor attacks. Consistent with the results when no sensor attacks are present, we observe nearly identical results when senors are attacked, regardless of the underlying system stability. This further illustrates that the specification based-design of the resilient parameter-invariant controller can be achieved regardless of the underlying system parameters. We note, however, a multi-step design specification will vary with the system stability since the multi-step predicted state covariance is a non-linear function of the process noise and state dynamic gain, a. For this reason, it is necessary that the resilient parameter invariant controller be designed at each time step in order to satisfy the performance specification invariant to the unknown state dynamics.

6.2 Vehicle Cruise Control

To evaluate the resilient parameter-invariant controller as a potential cruise control mechanism, we consider a simplified first-order model of a mobile robot as

$$\begin{aligned} x(k+1) &= 0.95x(k) + u(k) + w(k) \\ y(k) &= [2,3,4]^\top x(k) + v(k) \end{aligned} \tag{6}$$

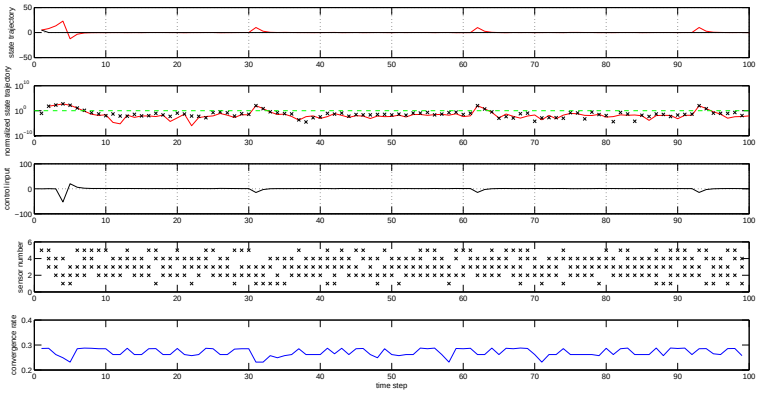

Fig. 4. Unstable system ($a = 1.8$) with sensor 1 and 5 under attack .

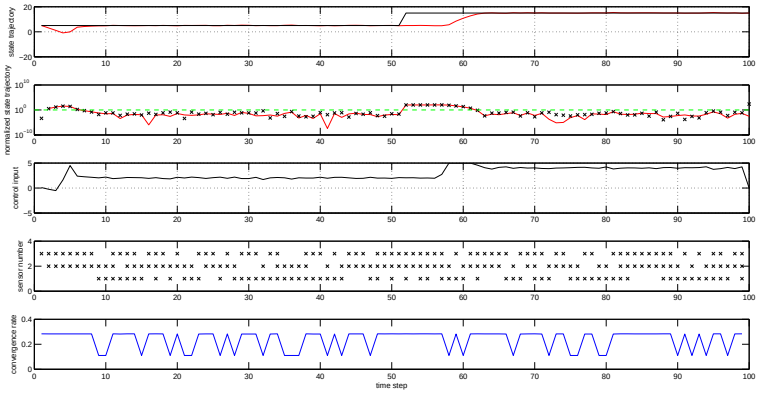

Fig. 5. Landshark cruise control with no corruption.

where $w(k)$ $[-1, .01]$, and we assume $\alpha^\star = .1$, and $\eta = 1$ for the performance constraint. In this simulation, we assume the initial vehicle speed is 5 miles per hour ($x(0) = 5$) and at time step 50 the speed is desired to increase to 15 miles per hour. Additionally, we assume the control input is bounded on the interval of -1 to 5. The result of employing the resilient parameter-invariant controller for cruise control is provided in Fig. 5 without sensor attacks. We observe in Fig. 5 that the vehicle speed is stabilized with a lag in the state trajectory. The lag is a result of the fact that a history of measurements is required to generate a control sequence. It remains a focus of future research to reduce this lag. A portion of the state trajectory lag is due to the saturation of the control signal,

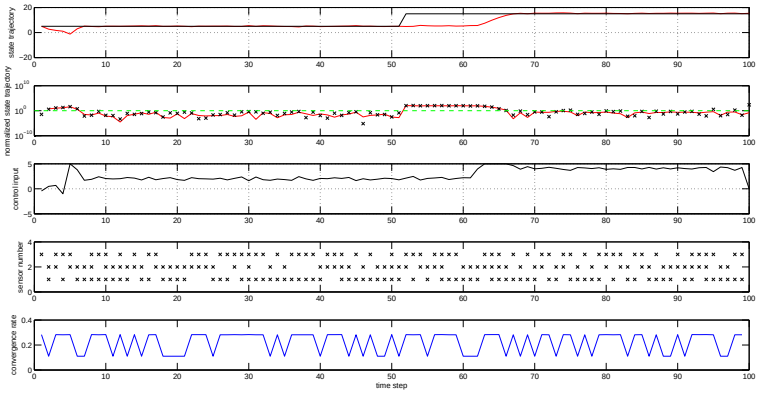

Fig. 6. Landshark cruise control with corruption.

which does not affect the stability of the system despite the resilient control law being designed without a constraint on the control sequence.

The cruise controller performance in the presence of a sensor attack on sensor three is illustrated in Fig. 6. Here we observe, and consistent with previous observations, that when attacked, the measurement of sensor three is accepted less often. In this case, sensor one (known to be more noisy) is selected more often. This results in the need for, on a average, a more aggressive control law to meet the performance criteria.

7 Discussion and Future Work

This work address the problem of resilient control of unknown first-order stochastic LTI systems in the presence of sensor attacks. A resilient sensor fusion strategy is introduced that minimizes the likelihood of a corrupted sensor being trusted. A time-series concatenation of secure estimates is utilized in cooperation with a desired state trajectory and previous control inputs to design a mean-stabilizing finite-horizon control sequence, invariant to the unknown system parameters. The parameter-invariant controller is designed using a frequency domain representation of an equivalent time-series representation of the system inputs to system outputs, thus allowing the design of a mean-stabilizing controller. Simulated results illustrate that the resilient parameter-invariant controller is capable of stabilizing unknown state disturbances and can perform state trajectory tracking with a lag.

Future work on this topic includes the extension of the scalar results in this paper to multi-dimensional systems with known dynamical structures but unknown parameters. Additionally, further insight is needed to investigate a method to reduce (or remove) the lag and to quantify its behavior in terms of

the underlying system and design parameters. Experimentation of the resilient parameter-invariant controller is planned on a robotic platform as a potentially cooperative approach with model-based approaches which assume knowledge of model parameters.

References

1. Willsky, A.: A survey of design methods for failure detection in dynamic systems. Automatica **12** (1976) 601–611
2. Qiu, L.: Essentials of robust control Kemin Zhou, John C. Doyle Prentice-Hall, Englewood Cliffs, NJ, 1998, ISBN: 0-13-790874-1. Automatica **38**(5) (May 2002) 910–912
3. Astrom, K.J., Wittenmark, B.: Adaptive Control. 2nd edn. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA (1994)
4. Trees, H.L.V.: Detection, Estimation, and Modulation Theory. John Wiley & Sons, Inc., New York (1968)
5. Scharf, L.L.: Statistical Signal Processing, Detection, Estimation, and Time Series Analysis. Addison-Welsley Publishing Company Inc., Reading, Massachusetts (1991)
6. Schenato, L., Sinopoli, B., Franceschetti, M., Poolla, K., Sastry, S.: Foundations of control and estimation over lossy networks. Proceedings of the IEEE **95**(1) (jan. 2007) 163 –187
7. Gupta, A., Langbort, C., Basar, T.: Optimal control in the presence of an intelligent jammer with limited actions. In: Decision and Control (CDC), 2010 49th IEEE Conference on. (dec. 2010) 1096 –1101
8. Pasqualetti, F., Dörfler, F., Bullo, F.: Attack detection and identification in cyber-physical systems – part ii: Centralized and distributed monitor design. Technical Report arXiv:1202.6049 (Feb 2012)
9. Sundaram, S., Pajic, M., Hadjicostis, C.N., Mangharam, R., Pappas, G.J.: The wireless control network: Monitoring for malicious behavior. In: CDC. (2010) 5979–5984
10. Weimer, J., Kar, S., Johansson, K.H.: Distributed detection and isolation of topology attacks in power networks. In: Proceedings of the 1st international conference on High Confidence Networked Systems. HiCoNS '12, New York, NY, USA, ACM (2012) 65–72
11. Weimer, J., Ahmadi, S.A., Araujo, J., Mele, F.M., Papale, D., Shames, I., Sandberg, H., Johansson, K.H.: Active actuator fault detection and diagnostics in hvac systems. In: 4th ACM Workshop On Embedded Systems For Energy-Efficiency In Buildings (BuildSys), Toronto, Canada (2012)
12. Fawzi, H., Tabuada, P., Diggavi, S.N.: Secure estimation and control for cyber-physical systems under adversarial attacks. CoRR **abs/1205.5073** (2012)
13. Pintelon, R., Guillaume, P., Rolain, Y., Schoukens, J., Van hamme, H.: Parametric identification of transfer functions in the frequency domain-a survey. Automatic Control, IEEE Transactions on **39**(11) (nov 1994) 2245 –2260
14. Ljung, L., ed.: System identification (2nd ed.): theory for the user. Prentice Hall PTR, Upper Saddle River, NJ, USA (1999)
15. Van Den Hof, P.: Identification and control - closed-loop issues. Automatica **31**(12) (December 1995) 1751–1770