RESILIENT ESTIMATION AND SAFE CONTROL FOR CYBER-PHYSICAL SYSTEMS

BY

WENBIN WAN

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mechanical Engineering
in the Graduate College of the
University of Illinois Urbana-Champaign, 2022

Urbana, Illinois

Doctoral Committee:

Professor Naira Hovakimyan, Chair
Professor Lui Sha
Professor Srinivasa Salapaka
Professor Petros Voulgaris, University of Nevada, Reno
Assistant Professor Hunmin Kim, Mercer University

Abstract

The recent decade has been critical in designing and deploying cyber-physical systems (CPS). CPS Security and CPS safety often are essential. The research proposed in this dissertation aims to enable safe operation for cyber-physical systems (CPS) subject to significant uncertainties, such as malicious attacks, unforeseen environments, and model uncertainties, by integrating resilient estimation algorithms and safe control methods. First, we consider the problem of a safety-constrained control architecture design against GPS spoofing/jamming attacks. We develop a resilient estimation algorithm to detect attacks and design control algorithms based on the model predictive controller (MPC) subject to limited sensor availability due to the sensor attacks. In another scenario of actuator attacks, we propose a constrained attack-resilient estimation algorithm (CARE) against the CPS attacks. The CARE can simultaneously estimate the compromised system states and the attack signals. In particular, CARE first provides minimum-variance unbiased estimates and then projects the estimates onto the constrained space induced by physical constraints and operational limitations. The proposed CARE performs better in estimation and attack detection by reducing estimation errors, covariances, and false negative rates. Following that, we extend our resilient estimation algorithm to a spatio-temporal framework. Building on the proposed resilient spatio-temporal filtering, we design a proactive adaptation architecture for connected vehicles in unforeseen envi-

ronments, synthesizing techniques in spatio-temporal data fusion and robust adaptive control. Finally, we propose an efficient interval estimation method for estimating systems under faulty model uncertainties. The method applies to a broad class of systems with a large uncertainty setup.

To My Dear Parents

别　归

意　期

终　岂

感　烂

激　漫

Acknowledgments

To my **advisor**, Professor Naira Hovakimyan, thank you for your patience, encouragement, guidance, and support.

To my **members of committee**, Professor Lui Sha, Professor Srinivasa Salapaka, Professor Petros Voulgaris, and Professor Hunmin Kim, thank you for taking the time to serve on my committee and providing valuable feedback.

To all of my **collaborators**, thank your for your dedication and providing me valuable research insights from other perspectives.

To the current and past **members of Advanced Control Research Lab**, Aditya, Andrew, Arun, Christoph, Chuyuan, Donglei, Erin, Gabriel, Hamid, Hunmin, Hyungjin, Hyungsoo, Hyungyu, Javier, Jin, John, Lin, Mikayel, Minjun, Minkyung, Neng, Pan, Ran, Sheng, Vivek, Yanbing, Yikun, Yuliang, Zhuohuan, Ziyao, thank you all for the research discussions and other enjoyable memories.

To all of the other **friends**, thank you for making my time at MIZZOU and ILLINI memorable.

To my **family**, thank you for your support and love.

Table of Contents

List of Abbreviations

ALT	Attacker Location Tracker
BLUE	Best Linear Unbiased Estimator
CARE	Constrained Attack-Resilient Estimation
CDL	Communication Data Link
CPS	Cyber-Physical Systems
CUSUM	CUmulative SUM
ESC	EScape Controller
FRRF	Fixed Rank Resilient Filtering
GCS	Ground Control Station
GPS	Global Positioning System
ICC	Individual Chance Constraint
IMU	Inertial Measurement Unit
ISE	Input and State Estimation
LP	Linear Programming
LTV	Linear Time-Varying
MPC	Model Predictive Control
MVUE	Minimum-Variance Unbiased Estimator
PD	Proportional-Derivative
UAV	Unmanned Aerial Vehicle
UKF	Unscented Kalman Filter

Chapter 1

Introduction

Cyber-physical systems (CPS) and their safety-critical applications have grown exponentially in recent decades, from large-scale industrial systems to autonomous systems. For instance, smart grids, transportation networks, unmanned aerial vehicles (UAVs), and self-driving cars are transforming the way we live and work. While the cyber and physical components of CPS are tightly connected, unlike traditional physical systems, the research in CPS incorporates interdisciplinary approaches, combining concepts from computer science, information theory, distributed systems, and control theory. The integration of the aforementioned technologies induces unprecedented complex system behaviors, making it challenging to achieve safe operation for CPS under uncertainties. Malicious attacks on cyber infrastructures are one of the significant uncertainties which have become common daily, posing a constant threat to our nation's security and well-being. Cyber attacks have clearly illustrated their susceptibility and raised awareness of the security challenges. These include attacks on large-scale critical infrastructures, such as the German steel mill cyber attack [1], the Maroochy Water breach [2], and the StuxNet virus attack on an industrial supervisory control and data acquisition (SCADA) system [3]. The goal of all these cyber attacks is to deceive the control and monitoring mechanisms, potentially causing the system to become unstable and malfunction, resulting in catastrophic physical damage.

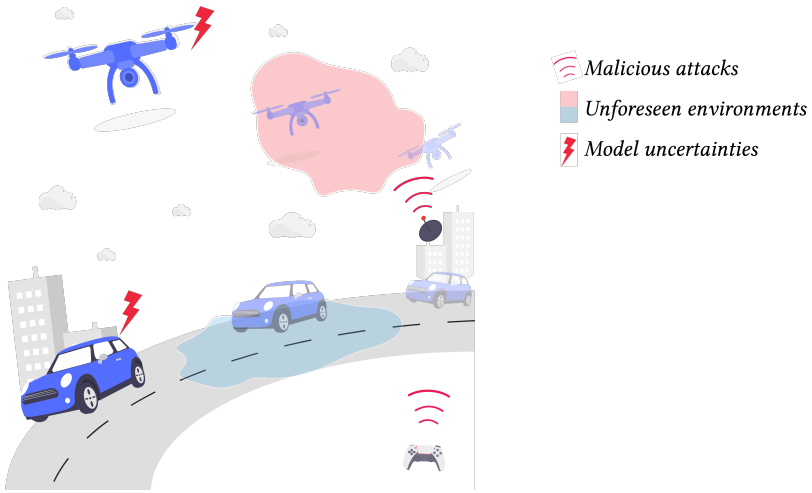


Figure 1.1: Autonomous vehicles suffering from malicious attacks, unforeseen environments, and model uncertainties.

Autonomous vehicles, such as UAVs and self-driving cars, are one of the fast-growing safety-critical applications of CPS, and they are also not immune to such attacks. Similarly, malicious attacks on avionics and automotive vehicles have been reported, such as the global positioning systems (GPS) attack on the U.S. drone RQ-170 in Iran [4], and disabling the brakes and stopping the engine on civilian cars [5, 6]. Furthermore, safe operation for autonomous vehicles remains challenging because autonomous vehicles typically operate in dynamic environments with unforeseen challenges. For instance, the state of the road is an important environmental factor for autonomous vehicle control. A significant change in road condition from the nominal status creates uncertainties and can lead to system failures. When a vehicle encounters an uncertain environment, such as an ice patch, it is too late and not allowed to reduce the speed, and the vehicle can lose control. Moreover, the safe operation of autonomous vehicles depends on the current state and the accuracy of the dynamic modeling. In practice, state estimates may fail to converge to the true state in the presence of model uncertainties, resulting in potentially hazardous situations. A notable example is the inci-

dent of Miracle on the Hudson [7]. After a bird strike caused all engines to fail, Captain Sullenberger (Sully) made the correct decision by landing the plane on the Hudson River rather than attempting to land at any airport, saving all the lives of the 155 people on board. Sully is a well-trained and experienced pilot who could resiliently estimate the parameters of the compromised model and safely land the plane in the nearby Hudson River. The Challenges of resilient estimation and safe control design in autonomous vehicles to achieve safety when dealing with such model uncertainties must be ideally handled by the autonomy architecture. Figure 1.1 depicts the scenarios of autonomous vehicles under significant uncertainties such as malicious attacks, unforeseen environments, and model uncertainties. In light of the above, this dissertation is dedicated to addressing the security and safety issues raised by various uncertainties. The research aims to robustly achieve safe operation for CPS by developing resilient estimation and safe control algorithms and architectures built on solid theoretical foundations. The following presents an overview of the attack detection and resilience estimation of CPS.

Because the cyber and physical components of CPS are inextricably linked, safety can only be achieved if security is assured; therefore, the attack detection mechanism in CPS is the first line of defense for safety. Traditionally, most research in the field of attack detection has concentrated solely on monitoring cyber-space misbehavior [8]. With the emergence of CPS, it is critical to monitor physical misbehavior as well because the impact of the attack on physical systems must also be addressed [9]. In the last decade, attention has been drawn from the perspective of the control theory that exploits some prior information on the system dynamics for detection and attack-resilient control. For instance, a unified modeling framework for CPS

and attacks is proposed in [10]. A typical control architecture for the networked system under both cyber and physical attacks is proposed in [11]; then attack scenarios, such as Denial-of-Service (DoS) and false-data injection (FDI) are analyzed using this control architecture in [12].

In recent years, model-based detection has been tremendously studied. Attack detection has been formulated as an ℓ_0/ℓ_∞ optimization problem, which is NP-hard [13]. A convex relaxation has been studied in [14]. Furthermore, the worst-case estimation error has been analyzed in [15]. Multi-rate sampled data controllers have been studied to guarantee detectability in [16] and to detect zero-dynamics attacks in [17]. A residual-based detector has been designed for power systems against false-data injection attacks, and the impact of attacks has been analyzed in [18]. In addition, some papers have studied active detection, such as [19, 20], where the control input is watermarked with a pre-designed scheme that sacrifices optimality. The aforementioned methods have the problem that the state estimate is not resilient concerning the attack signal, and incorrect state estimates consequently make it more challenging for defenders to react to malicious attacks.

Attack-resilient estimation and detection problems have been studied to address the above challenge in [21, 22, 23], where attack detection has been formulated as a simultaneous input and state estimation problem, and the minimum-variance unbiased estimation technique has been applied. More specifically, the approach has been applied to linear stochastic systems in [21], stochastic random set methods in [22], and nonlinear systems in [23]. These detection algorithms rely on statistical thresholds, such as the χ^2 test, which is widely used in attack detection [20, 24]. Since the detection accuracy improves when the covariance decreases, a smaller covariance is desired.

On top of the minimum-variance estimation approach, the covariance

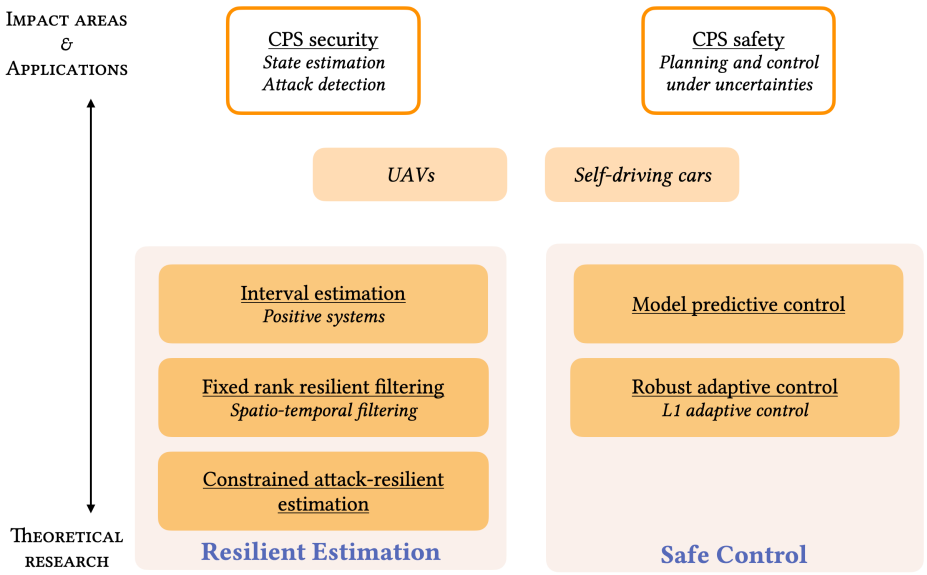


Figure 1.2: Overview of the contributions. Proposed methods on the left and right are related to *resilient estimation* and *safe control*, respectively. Theoretical research developments are at the bottom, and applications are at the top.

can be further reduced when we incorporate the information of the input and state in terms of constraints. There have been several investigations on Kalman filtering with state constraints [25, 26, 27, 28]. The state constraints are induced by unmodeled dynamics and operational processes. Some of these examples include vision-aided inertial navigation [29], target tracking [30] and power systems [31]. Constraints on inputs are also considered, such as avoiding reachable dangerous states under the assumption that the attack input is constrained [32] and designing a resilient controller based on the partial knowledge of the attacker in terms of inequality constraints [33]. The methods in [32, 33] can efficiently be used to maneuver a class of attacks when input inequality constraints are available but cannot resiliently address the estimation problem due to the false-data injection. This problem remains to be solved with a stability guarantee in the presence of inequality constraints.

1.1 Contributions and Dissertation Organization

This dissertation contributes at multiple levels, as depicted in Figure 1.2. At the lowest level, this dissertation presents two novel resilient estimation techniques for improving estimation accuracy under adversarial perturbations and model uncertainties with a stability guarantee. At a higher level, this dissertation proposes corresponding safe control solutions supported by the proposed resilient estimation methods for autonomous vehicles under significant uncertainties. Furthermore, at the highest level, this dissertation contributes to improving cyber security and physical safety in CPS through resilient estimation and safe control architecture designs.

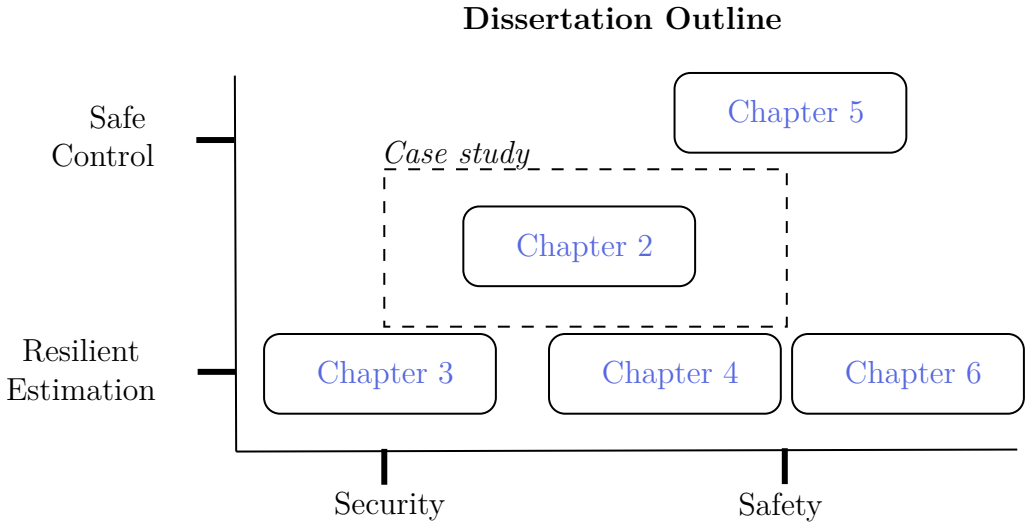


Figure 1.3: This dissertation is structured around two disjunctions: security *vs.* safety on the one hand, and resilient estimation *vs.* safe control on the other dimension.

The dissertation outline is summarized in Figure 1.3. The detailed contributions and organization are listed as follows.

- Chapter 2 presents a case study of resilient estimation and safe control

design for UAVs in GPS denied environments. The first contribution is in providing solutions from attack detection to control strategy by proposing a safety constrained control framework. In the framework, we design an attack-resilient monitor for detecting the attack and estimating the system state. On the other hand, an attacker location tracking algorithm (ALT) is developed to estimate the attacker's location and find the effective range. Using the estimates obtained by ALT, we design and compare model predictive control (MPC)-based controllers that re-plan the UAV trajectory to escape the effective range. The framework has been extended to multi-UAV systems for time-critical coordination tasks. Simulation examples are provided to illustrate the effectiveness of the designs.

- In Chapter 3, we propose a constrained attack-resilient estimation algorithm (`CARE`). The main contributions of this chapter can be summarized as follows. *i)* The proposed `CARE` can simultaneously estimate the compromised system states and attack signals. `CARE` first provides minimum-variance unbiased estimates, and then they are projected onto the constrained space induced by information aggregation. *ii)* The proposed `CARE` has better estimation performance. The projection strictly reduces the estimation errors and covariances. *iii)* We are the first to investigate the stability of the estimation algorithm with inequality constraints and prove that the estimation errors are practically exponentially stable in mean square. *iv)* The proposed `CARE` has better attack detection performance. We provide rigorous analysis that the false negative rate is reduced by using the proposed algorithm. *v)* The proposed algorithm is compared with the state-of-the-art method

to show the improved estimation and attack detection performance.

- In Chapter 4, the proposed fixed rank resilient filter (FRRF) deals with computational complexity and model accuracy problems in spatio-temporal data fusion. The strategy is to improve the computational efficiency using spatio-temporal models defined on a fixed dimensional space. However, getting an exact model of the fixed dimensional space is difficult. The proposed design extends the spatio-temporal fixed rank filter to capture model uncertainty and unmodeled biased noises in the fixed dimensional space. We show the stability of the FRRF when each measurement is obtained as a Poisson arrival process. In addition, we apply the method to estimate environmental factors for autonomous vehicles by synthesizing weather forecasts and local measurements from anonymous vehicles. Simulation examples are provided to validate the theoretical findings.

- In Chapter 5, the results on FRRF design are extended by designing a novel network-enabled proactive control architecture for autonomous vehicles that systematically deals with a large-scale uncertainty at the proactive design level and a small-scale uncertainty at the robust feedback control level. The estimates of the environmental factor considered in Chapter 4 contribute to designing a robust controller for adaptation to environmental uncertainties. We provide the systematic proactive-design procedure for the $\mathcal{L}_1$ robust adaptive controller for lateral vehicle control, containing many design parameters and complex propagated uncertainties. Simulation scenarios for vehicles on different road conditions are provided to validate the theoretical findings.

- Chapter 6 presents a novel interval estimation method. The first con-

tribution is the formulation of state estimation error dynamics as two positive systems. The gains that minimize the upper and maximize lower bounds can be efficiently solved using the linear programming optimization method. The proposed method is compared with the interval observer and a set-membership method to show the proposed method's estimation accuracy and computational efficiency. Furthermore, we extend the method to a class of systems with a large uncertainty setup.

- Concluding remarks and future research directions are provided in Chapter 7.

List of publications

- Wan, W., Kim, H., Hovakimyan, N., Voulgaris, P. G., and Sha, L.. *Resilient Estimation and Safe Planning for UAVs in GPS Denied Environments.* Advances in Control of Autonomous Aerial Vehicles, Springer. [To appear] (Used in Chapter 2)

- Wan, W., Kim, H., Hovakimyan, N.. (2022) *Towards Trustworthy Autonomy: Reliable and Efficient Interval Estimation and Learning for Robust Model Predictive Control.* In *The 36th AAAI Workshop on Trustworthy Autonomous Systems Engineering.* (Used in Chapter 6)

- Wan, W., Kim, H., Hovakimyan, N., and Voulgaris, P. (2022). Constrained *Attack-resilient Estimation of Stochastic Cyber-physical Systems.* arXiv preprint arXiv:2109.12255. (Used in Chapter 3)

- Wan, W., Kim, H., Cheng, Y., Hovakimyan, N., Voulgaris, P. G., and Sha, L.. (2021) *Safety Constrained Multi-UAV Time Coordination: A Bi-*

level Control Framework in GPS Denied Environment. In *AIAA Aviation Virtual Forum*, p. 2463. (Used in Chapter 2)

- Kim, H., Wan, W., Hovakimyan, N., Sha, L., and Voulgaris, P.G.. (2021) *Robust Vehicle Lane Keeping Control with Networked Proactive Adaptation.* In *2021 American Control Conference (ACC)*, pp. 136-141. (Used in Chapters 4 and 5)

- Wan, W., Kim, H., Hovakimyan, N., Sha, L., and Voulgaris, P. G.. (2020) *A Safety Constrained Control Framework for UAVs in GPS Denied Environment.* In *IEEE 59th Conference on Decision and Control (CDC)*, pp. 214-219. (Used in Chapter 2)

- Wan, W., Kim, H., Hovakimyan, N., and Voulgaris, P. G.. (2019) *Attack-resilient Estimation for Linear Discrete-time Stochastic Systems with Input and State Constraints.* In *IEEE 58th Conference on Decision and Control (CDC)*, pp. 5107-5112. (Used in Chapter 3)

- Yoon, H. J., Wan, W., Kim, H., Hovakimyan, N., Sha, L., and Voulgaris, P. G.. (2019) *Towards Resilient UAV: Escape Time in GPS Denied Environment with Sensor Drift.* In *21st IFAC Symposium on Automatic Control in Aerospace*, IFAC-PapersOnLine, 52(12), 423-428. (Used in Chapter 2)

Collaborations not presented in this dissertation

- Tao, C., Wan, W., Kim, H., Pan, Z., and Hovakimyan, N. (2023). *Sampling-based Resilient Control Barrier Functions for Uncertain Nonlinear Systems.* AIAA SciTech. [To appear]

- Yang, J., Kim, H., Wan, W., Hovakimyan, N., and Vorobeychik, Y. (2023). *Certified Robust Control under Adversarial Perturbations.* [Under review]

- Kim, H., Yoon, HJ., Wan, W., Hovakimyan, N., Voulgaris, P. G., and Sha, L.. (2021) *Backup Plan Constrained Model Predictive Control.* In *IEEE 60th Conference on Decision and Control (CDC)*, pp. 289-294.

Chapter 2

Safe Control for UAVs in GPS Denied Environments

Unmanned aerial vehicles (UAVs) are cyber-physical systems (CPS) and have been used worldwide for commercial, civilian, and educational applications over the decades. A UAV architecture typically consists of three main elements: unmanned aircraft, the ground control station (GCS), and the communication data link (CDL) [34]. Moreover, the aircraft consists of a flight controller, sensors, and actuators. The physical components of UAVs use a network to communicate with the GCS via the CDL. As a result, UAV systems are vulnerable to attacks that target either the cyber or physical elements or a combination of both [35]. Most security attacks against the different components of the UAV system can potentially lead to taking over control or crashing the aircraft. First, attacks on CDL are an essential class of attacks that can violate the communication between the UAV and the GCS. For instance, the attacks that include denial of service, GCS signal jamming/spoofing, and unauthorized communication disclosure have been studied in [36, 37, 38], respectively. On the other hand, attacks do not involve the CDL, such as malicious hardware or software trojans. Maldrone [39], for example, is a virus that enables the attacker to control the UAV by acting as a proxy for the flight controller. Furthermore, sophisticated attack aims to take over the control by combining the attacks on both CDL and flight controller. A malicious GPS attack on U.S. drone RQ-170 has been reported in [4], where the attacker started to attack CDL first and then carried on

with an attack on the flight controller by spoofing the GPS signal.

One of the most effective GPS spoofing attack detection techniques is to analyze raw antenna signals or utilize multi-antenna receiver systems. The GPS spoofing attack can be detected by checking whether the default radiation pattern is changed in [40]. A multi-antenna receiver system was used to detect GPS spoofing attacks by monitoring the angle-of-arrival of the spoofing attempts in [41]. As an extension of this work, GPS spoofing mitigation has also been investigated where an array of antennas is utilized to obtain genuine GPS signals by spatial filtering [42, 43, 44]. However, those solutions require hardware modifications or low-level computing modules and assume that attackers can only use single-antenna spoofing systems. Furthermore, the attacker can spoof the GPS receivers without being detected if multi-antenna spoofing devices are available [45].

The biggest challenge remains how to encrypt GPS since it is very costly and requires complex software or/and hardware modification. This chapter introduces an alternative approach from a control theoretic perspective through a safety-constrained control framework that adapts UAVs at a path re-planning level to support resilient state estimation against GPS spoofing attacks.

2.1 Problem Formulation

Consider the discrete-time stochastic system model:

$$\boldsymbol{x}_k = \boldsymbol{A}\boldsymbol{x}_{k-1} + \boldsymbol{B}\boldsymbol{u}_{k-1} + \boldsymbol{w}_{k-1} \tag{2.1a}$$

$$\boldsymbol{y}_k^G = \boldsymbol{C}^G\boldsymbol{x}_k + \boldsymbol{d}_k + \boldsymbol{v}_k^G \tag{2.1b}$$

$$\boldsymbol{y}_k^I = \boldsymbol{C}^I(\boldsymbol{x}_k - \boldsymbol{x}_{k-1}) + \boldsymbol{v}_k^I \tag{2.1c}$$

$$\boldsymbol{y}_k^S = \begin{cases} \boldsymbol{C}^S \frac{\boldsymbol{\eta}_k}{d(\boldsymbol{x}_k^a, \boldsymbol{x}_k)^2} + \boldsymbol{v}_k^S, & \textit{under the attack} \\ \boldsymbol{\eta}^S + \boldsymbol{v}_k^S, & \textit{otherwise} \end{cases}, \tag{2.1d}$$

where $\boldsymbol{x}_k \in \mathbb{R}^n$ is the state. System matrices $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}^G$, $\boldsymbol{C}^I$ and $\boldsymbol{C}^S$ are known and bounded with appropriate dimensions. There are three types of outputs available. Output $\boldsymbol{y}_k^G \in \mathbb{R}^{m_G}$ is the GPS measurement which may be corrupted by unknown GPS spoofing signal $\boldsymbol{d}_k \in \mathbb{R}^{m_G}$. The signal $\boldsymbol{d}_k$ is injected by the attacker when the UAV is in the effective range of the spoofing device. Output $\boldsymbol{y}_k^I \in \mathbb{R}^{m_I}$ is the inertial measurement unit (IMU) measurement which returns a noisy measurement of the state difference. Output $\boldsymbol{y}_k^S \in \mathbb{R}^{m_S}$ represents the GPS signal strength. The defender is unaware of $\boldsymbol{x}_k^a$ and $\boldsymbol{\eta}_k$, where $\boldsymbol{x}_k^a \in \mathbb{R}^n$ is the unknown attacker location, and $\boldsymbol{\eta}_k \in \mathbb{R}^{m_S}$ is the nominal power of the spoofing device. If GPS is under attack, $\boldsymbol{y}_k^S$ is an inverse function of the distance between the attacker and the UAV. The function $d(\boldsymbol{a}, \boldsymbol{b})$ measures the distance between $\boldsymbol{a}$ and $\boldsymbol{b}$. If the UAV receives genuine GPS signals, this output represents the genuine GPS signal strength $\boldsymbol{\eta}^S$. We assume that the attacker can inject any signal $\boldsymbol{d}_k$ into $\boldsymbol{y}_k^G$. The noise signals $\boldsymbol{w}_k$, $\boldsymbol{v}_k^G$, $\boldsymbol{v}_k^I$, and $\boldsymbol{v}_k^S$ are assumed to be independent and identically distributed Gaussian random variables with zero means and covariances $\mathbb{E}[\boldsymbol{w}_k\boldsymbol{w}_k^\top] = \boldsymbol{\Sigma}_w \geq 0$, $\mathbb{E}[\boldsymbol{v}_k^G(\boldsymbol{v}_k^G)^\top] = \boldsymbol{\Sigma}_G > 0$, $\mathbb{E}[\boldsymbol{v}_k^I(\boldsymbol{v}_k^I)^\top] = \boldsymbol{\Sigma}_I > 0$,

and $\mathbb{E}[\boldsymbol{v}_k^S(\boldsymbol{v}_k^S)^\top] = \boldsymbol{\Sigma}_S > 0$, respectively.

Remark 2.1 *The sensor measurement $\boldsymbol{y}_k^I$ represents any relative sensor measurement, such as velocity measurement by a camera. In this chapter, we use IMU for the illustration.*

Remark 2.2 *The signal strength output $\boldsymbol{y}_k^S$ in Equation (2.1d) is derived by the GPS signal attenuation due to free-space path loss. Friis transmission equation [46] is given by:*

$$\boldsymbol{P}_r = \boldsymbol{P}_t \boldsymbol{G}_t \boldsymbol{G}_r \frac{\lambda^2}{(4\pi r)^2},$$

where $\boldsymbol{P}_t$ and $\boldsymbol{P}_r$ are the transmit power and the receive power, $\boldsymbol{G}_t$ and $\boldsymbol{G}_r$ are the transmit and receive antenna gains, r is the distance between two antennas, λ is the wavelength. We write $\boldsymbol{G}_r(\frac{\lambda}{4\pi})^2$ as the output matrix $\boldsymbol{C}^S$, $\boldsymbol{G}_t\boldsymbol{P}_t$ as the nominal power of the spoofing device $\boldsymbol{\eta}_k$, and r as the distance between the attacker and the UAV, i.e., $d(\boldsymbol{x}_k^a, \boldsymbol{x}_k)$.

Problem Statement 2.1 *Given the system in Equation (2.1) with sensor measurements Equations (2.1b) to (2.1d), the defender aims to detect the GPS spoofing attack, achieve resilient state estimation when considering the limited sensor availability, and complete the global mission securely.*

2.2 Methods

To address the problem described in Problem Statement 2.1, we propose a safety constrained control framework in Figure 2.1, which consists of an attack detector, a resilient state estimator, a robust controller, an attacker location tracker (ALT), and an escape controller (ESC). The proposed safety

constrained control framework drives the UAV to the outside of the effective range of the spoofing device. The following explains each module in the proposed framework as shown in Figure 2.1.

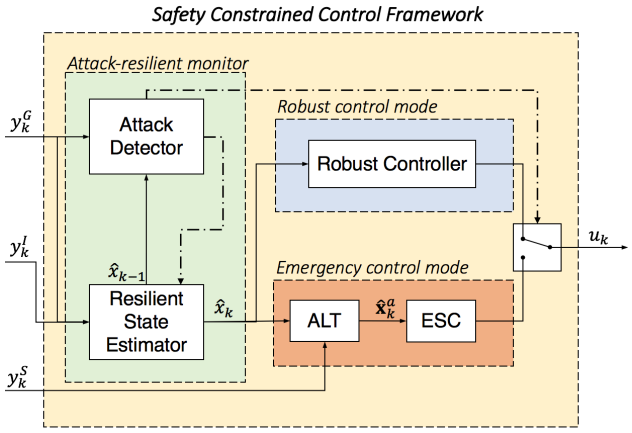


Figure 2.1: A safety constrained control framework consisting of an attack detector, a resilient state estimator, a robust controller, an ALT, and an ESC.

Robust Control Mode. The robust controller is a complex controller that operates the UAV to the destination in the presence of noise but without the presence of attacks. Any robust control technique can be implemented in this module.

Emergency Control Mode. ALT is designed for tracking the attacker's location and estimating the spoofing device's output power by applying UKF with sliding window outputs. ESC is an MPC-based controller that drives the UAV out of the effective range of the spoofing device based on the estimation of the attacker location obtained by ALT.

Attack-resilient Monitor & Decision Logic. The resilient state estimator is developed based on the Kalman-filter-like state estimator. The attack detector is designed by the χ^2-based anomaly detection algorithm. Based on the previous estimation from the resilient state estimator, the Boolean output (dotted-dashed line in Figure 2.1) of the attack detector determines

i) whether the GPS measurement should be used for the state estimation; and *ii*) the switching rule between two control modes: the robust control mode and the emergency control mode.

ALT and ESC adapt the UAV at a path re-planning level for safe operation. In what follows, each subsection describes a new resilience measure, escape time, and the details of the corresponding component.

Escape Time

It has been revealed in Theorem 4.2 in [47] that the state estimation becomes less trustful if GPS signals are compromised for a long time. Therefore, the UAV should escape from the GPS spoofing device at a certain time before the estimation becomes unreliable. The definition of the escape time is provided as follows for completeness.

Definition 2.1 (Escape time) *The escape time $k^{esc} \geq 0$ is the time difference between the attack time k^a and the first time instance when the estimation error $\boldsymbol{x}_k - \hat{\boldsymbol{x}}_k$ may not be in a tolerable error distance $\boldsymbol{\zeta} \in \mathbb{R}^n$ with the significance α, i.e.*

$$\begin{aligned} k^{esc} = &\arg\min_{k \geq k^a} k - k_a \\ &\text{s.t. } \boldsymbol{\zeta}^\top \boldsymbol{P}_k^{-1} \boldsymbol{\zeta} < \chi^2_{df}(\alpha), \end{aligned}$$

where $\boldsymbol{P}_k \triangleq \mathbb{E}[(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_k)(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_k)^\top]$ is the error covariance, and $\chi^2_{df}(\alpha)$ is the χ^2 value with degree of freedom df and statistical significance level α.

The escape time calculation is presented in Algorithm 1. Given the attack time k^a, the state estimation errors may not remain in the tolerable region with the predetermined confidence α after the escape time k^{esc}.

Algorithm 1 Escape time calculation

Require: k^a, α, df, $\boldsymbol{\zeta}$;
Ensure: k^{esc};

```
k = k^a;
while ζ^⊤ P_k^{-1} ζ > χ^2_{df}(α) do
    k = k + 1;
end while
k^{esc} = k − k^a;
```

Resilient Estimation and Attack Detection

The following Kalman-filter-like state estimator is used to estimate the current state. The state estimate $\hat{\boldsymbol{x}}_k$ can be obtained by

$$\hat{\boldsymbol{x}}_k = \hat{\boldsymbol{x}}_k^- + \boldsymbol{K}_k^G(\boldsymbol{y}_k^G - \boldsymbol{C}^G\hat{\boldsymbol{x}}_k^-) + \boldsymbol{K}_k^I\big(\boldsymbol{y}_k^I - \boldsymbol{C}^I(\hat{\boldsymbol{x}}_k^- - \hat{\boldsymbol{x}}_{k-1})\big), \tag{2.2}$$

where $\hat{\boldsymbol{x}}_k^- \triangleq \boldsymbol{A}\hat{\boldsymbol{x}}_{k-1}+\boldsymbol{B}\boldsymbol{u}_{k-1}$ is the priori state estimate. The state estimation error covariance $\boldsymbol{P}_k$ is given as follows:

$$\begin{aligned}\boldsymbol{P}_k =&(\boldsymbol{A} - \boldsymbol{K}_k\boldsymbol{C}\boldsymbol{A} + \boldsymbol{K}_k\boldsymbol{D}\boldsymbol{C})\boldsymbol{P}_{k-1}(\boldsymbol{A} - \boldsymbol{K}_k\boldsymbol{C}\boldsymbol{A} + \boldsymbol{K}_k\boldsymbol{D}\boldsymbol{C})^\top \\ &+ (\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{C})\boldsymbol{\Sigma}_w(\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{C})^\top + \boldsymbol{K}_k\boldsymbol{\Sigma}_y\boldsymbol{K}_k^\top,\end{aligned} \tag{2.3}$$

where $\boldsymbol{K}_k \triangleq \begin{bmatrix} \boldsymbol{K}_k^G & \boldsymbol{K}_k^I \end{bmatrix}$, $\boldsymbol{C} \triangleq \begin{bmatrix} \boldsymbol{C}^G \\ \boldsymbol{C}^I \end{bmatrix}$, $\boldsymbol{\Sigma}_y \triangleq \begin{bmatrix} \boldsymbol{\Sigma}_G & 0 \\ 0 & \boldsymbol{\Sigma}_I \end{bmatrix}$, and $\boldsymbol{D} \triangleq \begin{bmatrix} 0 & 0 \\ 0 & \boldsymbol{I} \end{bmatrix}$.

The optimal gain $\boldsymbol{K}_k$ is obtained by minimizing the trace of $\boldsymbol{P}_k$, i.e.

$$\min_{\boldsymbol{K}_k} \operatorname{tr}(\boldsymbol{P}_k). \tag{2.4}$$

The solution of Equation (2.4) is given by

$$\begin{aligned}\boldsymbol{K}_k =&(\boldsymbol{A}\boldsymbol{P}_{k-1}(\boldsymbol{C}\boldsymbol{A}-\boldsymbol{D}\boldsymbol{C})^\top+\boldsymbol{\Sigma}_w\boldsymbol{C}^\top)\\ &\times\left((\boldsymbol{C}\boldsymbol{A}-\boldsymbol{D}\boldsymbol{C})\boldsymbol{P}_{k-1}(\boldsymbol{C}\boldsymbol{A}-\boldsymbol{D}\boldsymbol{C})^\top+\boldsymbol{C}\boldsymbol{\Sigma}_w\boldsymbol{C}^\top+\boldsymbol{\Sigma}_y\right)^{-1}. \qquad (2.5)\end{aligned}$$

In [47], it has been shown that the covariance in Equation (2.3) is bounded when the GPS signal is available. If the GPS is denied, and only the relative sensor $\boldsymbol{y}_k^I$ is available, the covariance is strictly increasing and unbounded in time. That is, the sensor drift problem can be formulated as instability of the covariance matrix.

The defender implements an estimator and χ^2 detector to estimate the state and detect the GPS spoofing attack. To be specific, we detect the GPS spoofing attacks by χ^2 test (see Appendix A) using CUSUM (CUmulative SUM) algorithm. Since $\boldsymbol{d}_k = \boldsymbol{y}_k^G - \boldsymbol{C}^G x_k - \boldsymbol{v}_k^G$, given the previous state estimate $\hat{\boldsymbol{x}}_{k-1}$, we estimate the attack vector by comparing the sensor output and the output prediction:

$$\hat{\boldsymbol{d}}_k = \boldsymbol{y}_k^G - \boldsymbol{C}^G(\boldsymbol{A}\hat{\boldsymbol{x}}_{k-1} + \boldsymbol{B}\boldsymbol{u}_{k-1}). \qquad (2.6)$$

Note that the current estimate $\hat{\boldsymbol{x}}_k$ should not be used for the prediction because it is correlated with the current output; i.e., $\mathbb{E}[\hat{\boldsymbol{x}}_k(\boldsymbol{y}_k^G)^\top] \neq 0$. Due to the Gaussian noises $\boldsymbol{w}_k$ and $\boldsymbol{v}_k$ injected to the linear system in Equation (2.1), the states follow Gaussian distribution since any finite linear combination of Gaussian distributions is also Gaussian. Similarly, $\hat{\boldsymbol{d}}_k$ is Gaussian as well, and thus the use of the χ^2 test is justified. In particular, the χ^2 test compares

the normalized attack vector estimate $\hat{\boldsymbol{d}}_k^\top (\boldsymbol{P}_k^d)^{-1} \hat{\boldsymbol{d}}_k$ with $\chi^2_{df}(\alpha)$:

$$\begin{aligned} &\text{accept null hypothesis } H_0, \text{ if } \hat{\boldsymbol{d}}_k^\top (\boldsymbol{P}_k^d)^{-1} \hat{\boldsymbol{d}}_k \leq \chi^2_{df}(\alpha) \\ &\text{accept alternative hypothesis } H_1, \text{ if } \hat{\boldsymbol{d}}_k^\top (\boldsymbol{P}_k^d)^{-1} \hat{\boldsymbol{d}}_k > \chi^2_{df}(\alpha), \end{aligned} \tag{2.7}$$

where $\boldsymbol{P}_k^d \triangleq \mathbb{E}[(\boldsymbol{d}_k - \hat{\boldsymbol{d}}_k)(\boldsymbol{d}_k - \hat{\boldsymbol{d}}_k)^\top] = \boldsymbol{C}^G(\boldsymbol{A}\boldsymbol{P}_{k-1}\boldsymbol{A}^\top + \boldsymbol{\Sigma}_w)(\boldsymbol{C}^G)^\top + \boldsymbol{\Sigma}_G$, and $\chi^2_{df}(\alpha)$ is the threshold found in the Chi-square table. We use the test Equation (2.7) in a cumulative form. The proposed χ^2 CUSUM detector is characterized by the detector state $S_k \in \mathbb{R}_+$:

$$S_k = \delta S_{k-1} + \hat{\boldsymbol{d}}_k^\top (\boldsymbol{P}_k^d)^{-1} \hat{\boldsymbol{d}}_k, \quad S_0 = 0, \tag{2.8}$$

where $0 < \delta < 1$ is the pre-determined forgetting factor. At each time k, the CUSUM detector Equation (2.8) is used to update the detector state S_k and detect the attack.

The attack detector will i) update the estimated state $\hat{\boldsymbol{x}}_k$ and the error covariance $\boldsymbol{P}_k$ in Equation (2.3) with $\boldsymbol{K}_k^G = 0$ and ii) switch the controller to ESC, if

$$S_k > \sum_{i=0}^{\infty} \delta^i \chi^2_{df}(\alpha) = \frac{\chi^2_{df}(\alpha)}{1-\delta}. \tag{2.9}$$

If $S_k < \frac{\chi^2_{df}(\alpha)}{1-\delta}$, then it returns to the robust control mode.

Remark 2.3 *As shown in Figure 2.2, the resilient state estimation uses the GPS measurement and the IMU measurement to estimate the state by Equation (2.2) for the detection purpose as in Equation (2.6). When the GPS attack is detected, only the IMU measurement is used to estimate the state for the control purpose as in Equation (2.2) and Equation (2.3) with* $\boldsymbol{K}_k^G = 0$.

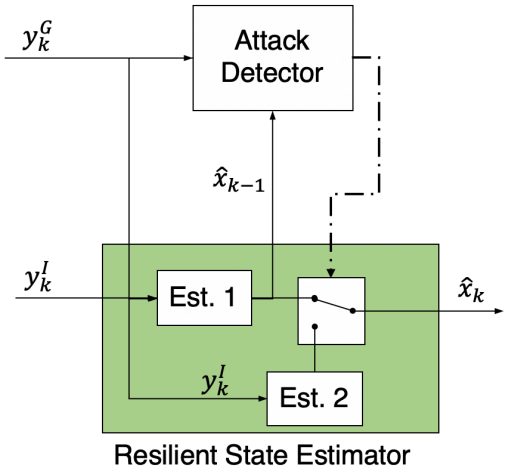


Figure 2.2: Resilient state estimator. GPS and IMU measurements are used in estimator one (Est. 1). Estimator two (Est. 2) only uses the IMU measurement. Est. 1 is used to estimate the state by Equation (2.2) for the detection as in Equation (2.6). When GPS is free of attacks, Est. 1 is also used to estimate the state for the control since the GPS measurement is trustful. In the presence of the GPS attack, Est. 2 is used for the control.

Attacker Location Tracking

We formulate the simultaneous estimation of the attacker location $\boldsymbol{x}_k^a$ and unknown parameter $\boldsymbol{\eta}_k$ as a target tracking problem of the attacker state $\mathbf{x}_k^a \triangleq [(\boldsymbol{x}_k^a)^\top, \boldsymbol{\eta}_k]^\top$.

Estimating the attacker state $\mathbf{x}_k^a$ encounters two major problems: i) the output equation $\boldsymbol{y}_k^S$ in Equation (2.1d) is highly nonlinear, and ii) a single measurement of the signal strength suffers from the infinite number of solutions.

To address the first issue, we use the UKF [48, 49], which has been developed to deal with highly nonlinear systems and provides a better estimation than the extended Kalman filter. Motivated by the fact that locating the epicenter of an earthquake can be done with at least three measurements from different seismic stations, we resolve the second issue by using M-sized

sliding window outputs, as shown in Figure 2.3. To be specific, we estimate

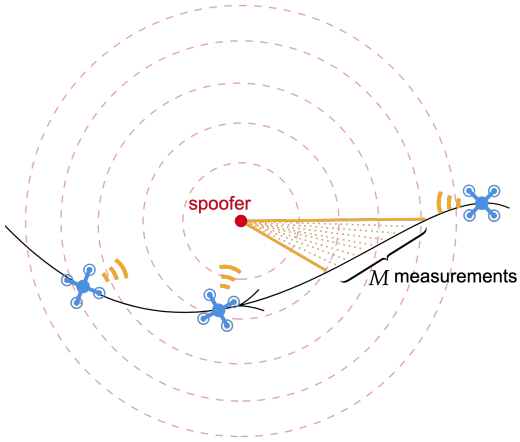


Figure 2.3: Attacker location tracking using M-sized sliding window outputs.

$\mathbf{x}_{k+1}^a$ using UKF with M-sized sliding window outputs:

$$\mathbf{x}_{k+1}^a = \mathbf{x}_k^a + \mathbf{w}_k^a \tag{2.10a}$$

$$\mathbf{y}_k^S = \begin{bmatrix} \boldsymbol{y}_k^S \\ \boldsymbol{y}_{k-1}^S \\ \vdots \\ \boldsymbol{y}_{k-M+1}^S \end{bmatrix}. \tag{2.10b}$$

The signal strength measurements from Equation (2.1d) can be written as

$$\boldsymbol{y}_k^S = f(\mathbf{x}_k^a) + \boldsymbol{v}_k^S,$$

where

$$f(\mathbf{x}_k^a) \triangleq \boldsymbol{C}^S \frac{\boldsymbol{\eta}_k}{d(\boldsymbol{x}_k^a, \boldsymbol{x}_k)^2}.$$

The state estimation by using UKF with sliding window outputs can track the location of the moving attacker, while nonlinear regression algorithms may fail to track it. The algorithm design and detailed derivation can be

found in Appendix B.

Safe Control Design

Escape Controller (ESC)

In the presence of the GPS spoofing attack, the variance of the state estimation errors $\boldsymbol{P}_k$ in Equation (2.3) is strictly increasing and unbounded in time (Theorem 4.2 [47]). The goal of ESC is to drive the UAV outside of the effective range of the spoofing device within the escape time so that the state estimation error remains within the tolerable region with a predetermined probability. In particular, ESC is designed to drive the UAV outside the spoofing device's effective range within the escape time.

Given the estimates of UAV state $\hat{\boldsymbol{x}}_k$ and attacker state $\hat{\mathbf{x}}_k^a$ with their covariances, the problem can be formulated as a finite horizon constrained MPC problem:

Program 2.1

$$
\begin{aligned}
\min_{\boldsymbol{u}} \quad & \sum_{i=k^a}^{k^a+N} \hat{\tilde{\boldsymbol{x}}}_{i+1}^{\top} \boldsymbol{Q}_i \hat{\tilde{\boldsymbol{x}}}_{i+1} + \boldsymbol{u}_i^{\top} \boldsymbol{R}_i \boldsymbol{u}_i \\
s.t. \quad & \hat{\boldsymbol{x}}_{i+1} = \boldsymbol{A}\hat{\boldsymbol{x}}_i + \boldsymbol{B}\boldsymbol{u}_i \\
& d(\hat{\boldsymbol{x}}^a_{k^a+k^{esc}}, \hat{\boldsymbol{x}}_{k^a+k^{esc}}) - r_{effect} > 0 \qquad (2.11) \\
& h(\hat{\boldsymbol{x}}_i, \boldsymbol{u}_i) \leq 0 \qquad (2.12) \\
& for\ i = k^a, k^a+1, \cdots, k^a+N,
\end{aligned}
$$

where $N \geq k^{esc}$ is the prediction horizon, $\hat{\tilde{\boldsymbol{x}}}_i$ is defined as the difference between the state estimation and the goal state at time index i, i.e., $\hat{\tilde{\boldsymbol{x}}}_i \triangleq \hat{\boldsymbol{x}}_i - \boldsymbol{x}_i^{goal}$, $\boldsymbol{Q}_i$ and $\boldsymbol{R}_i$ are symmetric positive definite weight matrices, and $\hat{\boldsymbol{x}}_i^a$

is the estimate of the attacker location. Value r_{effect} is the upper bound of the effective range of the spoofing device. The constraint Equation (2.11) implies that ESC should drive the UAV outside of the effective range of the spoofing device. Inequality Equation (2.12) is any nonlinear constraint on the state estimation $\hat{\boldsymbol{x}}_i$ (e.g., velocity) and the control input $\boldsymbol{u}_i$ (e.g., acceleration).

Remark 2.4 *The upper bound of the effective range r_{effect} can be assumed to be known. Due to hardware constraints, the output power/nominal strength of the spoofing device $\boldsymbol{\eta}_k$ is bounded, and $\boldsymbol{\eta}_k$ also can be estimated by ALT. The output power determines the effective range of the spoofing device, and r_{effect} can be found by*

$$r_{effect} = \arg\max_{r} g(r),$$

where $g(r) \triangleq \boldsymbol{C}^S \dfrac{\boldsymbol{\eta}_k}{r^2} > \boldsymbol{\eta}^S$.

There are two key challenges in Program 2.1. First, the states and the attacker location are unknown, and their estimates $\hat{\boldsymbol{x}}_i$ and $\hat{\boldsymbol{x}}_i^a$ are subject to stochastic noise. Moreover, we cannot guarantee that constraint Equation (2.11) is always feasible, i.e., Program 2.1 may not have a solution. Addressing the above two challenges, we introduce two programs for ESC in the following Sections.

ESC with Tube

Since the constraint Equation (2.11) is the safety-critical constraint, we can reformulate it as a conservative constraint such that ESC should drive the UAV outside of the effective range of the spoofing device with probability γ by the single individual chance constraint (ICC):

$$\mathbb{P}[d(\boldsymbol{x}^a_{k^a+k^{esc}}), \boldsymbol{x}_{k^a+k^{esc}}] - r_{effect} > 0) > \gamma. \tag{2.13}$$

Then Program 2.1 becomes a new stochastic MPC with ICC.

The chance constraints can be handled by constraint backoffs, which originate in linear MPC with additive stochastic noise [50]. However, we consider nonlinear constraints in Program 2.1, which makes the backoff intractable to compute. In [51], the tube is constructed based on sublevel sets of the incremental Lyapunov function by online predicted tube size, and then it is used to ensure robust constraint satisfaction by tightening the nonlinear state and input constraints. In [52], this is extended to allow for ICCs and stochastic uncertainty. Similar to [51, 52], the stochastic MPC with ICC can be formulated as:

Program 2.2

$$
\begin{aligned}
\min_{\boldsymbol{u}} \quad & \sum_{i=k^a}^{k^a+N} \hat{\tilde{\boldsymbol{x}}}_{i+1}^{\top} \boldsymbol{Q}_i \hat{\tilde{\boldsymbol{x}}}_{i+1} + \boldsymbol{u}_i^{\top} \boldsymbol{R}_i \boldsymbol{u}_i \\
s.t. \quad & \hat{\boldsymbol{x}}_{i+1} = \boldsymbol{A}\hat{\boldsymbol{x}}_i + \boldsymbol{B}\boldsymbol{u}_i \\
& d(\hat{\boldsymbol{x}}^a_{k^a+k^{esc}}, \hat{\boldsymbol{x}}_{k^a+k^{esc}}) - r_{effect} > s(\boldsymbol{P}_{k^a+k^{esc}}, \boldsymbol{P}^a_k, \gamma) \qquad (2.14) \\
& h(\hat{\boldsymbol{x}}_i, \boldsymbol{u}_i) \leq 0 \qquad (2.15) \\
& for \quad i = k^a, k^a+1, \cdots, k^a+N,
\end{aligned}
$$

where $\boldsymbol{P}_{k^a+k^{esc}}$ is the UAV state covariance at escape time, and $\boldsymbol{P}^a_k$ is the attacker state covariance. Function $s(\cdot)$ is the probabilistic tube size that can be seen as a margin to fulfill the second constraint in Equation (2.11).

To provide the theoretical guarantees on the capability of Program 2.2 and the equivalence between the stochastic MPC with ICC and Program 2.2, we use the results from [51, 52]. Since the newly formulated MPC with ICC Equation (2.13) is the standard nonlinear stochastic MPC problem, Assumptions in [52] can be verified.

Theorem 2.1 *Under Assumptions 1-4, 6, and 9 in [52], if Program 2.2 is feasible at $t = k^a$, then it is recursively feasible; the constraints in Equation (2.12) and Equation (2.13) are satisfied, and the origin is practically asymptotically stable for the resulting closed loop system. The impact of the hard constraint in Equation (2.14) is equivalent to the nonlinear ICCs in Equation (2.13).*

Proof: See proofs of Theorem 1 in [51] and Theorem 8 & 10 in [52]. □

From Theorem 2.1, we can conclude that as long as Program 2.2 is feasible at the time of attack k^a, we can guarantee that the UAV can escape within the escape time in probability. However, in some cases, Program 2.2 may not be feasible. To address this issue, we introduce a program with a soft constraint in the subsequent section.

ESC with Potential Function

The hard constraint in Equation (2.14) can be replaced by the repulsive potential function [53] as a high penalty in the cost function which is active only after the escape time $k^a + k^{esc}$. The repulsive potential function $U_{rep}(D)$ is defined as the following:

$$U_{rep}(D) \triangleq \begin{cases} \frac{1}{2}\beta\left(\frac{1}{D} - \frac{1}{r_{effect}}\right)^2 & \text{if } D \leq r_{effect} \\ 0 & \text{if } D > r_{effect} \end{cases},$$

which can be constructed based on the distance between the location of the attacker and the location of UAV, $D \triangleq d(\hat{\boldsymbol{x}}^a_{k^a+k^{esc}}, \hat{\boldsymbol{x}}_{k^a+k^{esc}})$. The scaling parameter β is a large constant, which represents a penalty when the constraint has not been fulfilled. Utilizing the soft constraint, we reformulate the MPC problem as follows:

Program 2.3

$$\min_{\boldsymbol{u}} \sum_{i=k^a}^{k^a+N} \hat{\tilde{\boldsymbol{x}}}_{i+1}^{\top} \boldsymbol{Q}_i \hat{\tilde{\boldsymbol{x}}}_{i+1} + \boldsymbol{u}_i^{\top} \boldsymbol{R}_i \boldsymbol{u}_i + \sum_{i=k^a+k^{esc}}^{k^a+N} U_{rep}(D_i)$$

$$s.t.\ \hat{\boldsymbol{x}}_{i+1} = \boldsymbol{A}\hat{\boldsymbol{x}}_i + \boldsymbol{B}\boldsymbol{u}_i$$

$$h(\hat{\boldsymbol{x}}_i, \boldsymbol{u}_i) \leq 0$$

$$for\ \ i = k^a, k^a+1, \cdots, k^a+N.$$

Remark 2.5 *Comparing to the use of the repulsive potential function U_{rep} in the collision avoidance literature [54, 55, 56], the proposed application of the repulsive potential function in Program 2.3 has two differences. First of all, the repulsive potential function is known before the collision happens in collision avoidance literature, while we can only get the repulsive potential function U_{rep} after the collision happens, i.e., only after the UAV has entered the effective range of the spoofing device. Second, the repulsive potential function U_{rep} is only counted in the cost function in Program 2.3 after the escape time.*

2.3 Illustrative Example

In this example, the UAV is moving from the start position with the coordinates at $(0, 0)$ to the target position $(300, 300)$ by using feedback control[1], based on the state estimate from Equation (2.2). When the GPS attack happens, the state estimate will no longer be trustworthy. After GPS measurement is turned off, the only available relative state measurement causes the sensor drift problem [47]. The UAV will switch the control mode from

[1]We implemented a proportional-derivative (PD) like tracking controller, which is widely used for double integrator systems.

the robust control mode to the emergency control mode when the attack is detected, using ESC to escape away from the attacker within the escape time. We solve the problem with *ESC with Potential Function* described in Program 2.3. The online computation is done using `Julia`, and ESC is implemented by using `JuMP` [57] package with `Ipopt` solver.

UAV Model

We use a double integrator UAV dynamics under the GPS spoofing attack as in [58]. The discrete-time state vector $\boldsymbol{x}_k$ considers planar position and velocity at time step k, i.e. $\boldsymbol{x}_k = [r_k^x, r_k^y, v_k^x, v_k^y]^\top$, where r_k^x, r_k^y denote x, y position coordinates, and v_k^x, v_k^y denote velocity coordinates. We consider the acceleration of UAV as the control input $\boldsymbol{u}_k = [u_k^x, u_k^y]^\top$. We assume that the state constraint and control input constraint are given as $\sqrt{(v_k^x)^2 + (v_k^y)^2} \leq 5$ and $\sqrt{(u_k^x)^2 + (u_k^y)^2} \leq 2$. With sampling time at 0.1 seconds, the double integrator model is discretized into the following matrices:

$$\boldsymbol{A} = \begin{bmatrix} 1 & 0 & 0.1 & 0 \\ 0 & 1 & 0 & 0.1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \boldsymbol{B} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0.1 & 0 \\ 0 & 0.1 \end{bmatrix},$$

and the outputs $\boldsymbol{y}_k^G$, $\boldsymbol{y}_k^I$, and $\boldsymbol{y}_k^S$ are the position measurements from GPS, the velocity measurements from IMU, and GPS signal strength measurements respectively, with the output matrices:

$$\boldsymbol{C}^G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad \boldsymbol{C}^I = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \text{ and } \boldsymbol{C}^S = \boldsymbol{I}.$$

The covariance matrices of the sensing and disturbance noises are chosen as $\boldsymbol{\Sigma}_w = 0.1\boldsymbol{I}$, $\boldsymbol{\Sigma}_G = \boldsymbol{I}$, $\boldsymbol{\Sigma}_I = 0.01\boldsymbol{I}$ and $\boldsymbol{\Sigma}_S = \boldsymbol{I}$.

GPS Spoofing Attack and Attack Signal Estimation

The GPS attack happens when the UAV is in the effective range of the spoofing device. The attack signal in this scenario is $\boldsymbol{d}_k = [10, 10]^\top$. The location of the attacker and the nominal power of the spoofing device are $\boldsymbol{x}_k^a = [100, 100]^\top$ and $\boldsymbol{\eta}_k = [200]$, which are both unknown to the UAV. The estimation obtained by Equation (2.6) is shown in Figure 2.4.

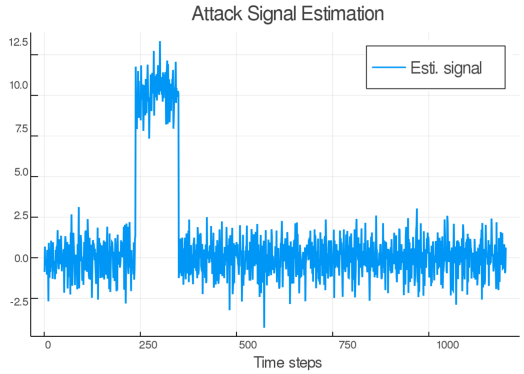


Figure 2.4: Attack signal estimation. The UAV stays in the effective range of the spoofing device from time step 231 to 356.

Attack Detection

Using the estimated attack signal to calculate the detector state S_k by Equation (2.8), the attack detector can detect the attack using the normalized attack vector as shown in Figure 2.5. In Figure 2.5, there are abnormal high detector state values, implying an attack. The statistical significance of the attack is tested using the CUSUM detector described in Equation (2.9) with the significance α at 1%.

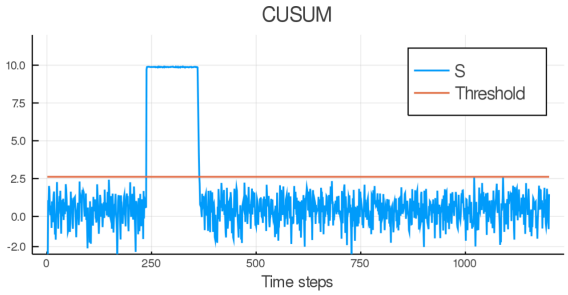


Figure 2.5: Attack detection. The detector state S_k is defined in Equation (2.8) of the CUSUM detector. The threshold is calculated by $\frac{\chi^2_{df}(\alpha)}{1-\delta}$ with $\alpha = 0.01$ and $\delta = 0.15$.

Attacker State Estimation

When the GPS attack is detected, the UAV first estimates the attacker state $\mathbf{x}^a_k$ by using Algorithm 4 with window size $M = 5$. The estimation result is shown in Figure 2.6. The estimated location and the estimated nominal power quickly converge to the true values. The estimates are drifting when the UAV remains in GPS denied environment. After obtaining an estimate of the attacker state, ESC is used to escape away from the effective range of the spoofing device.

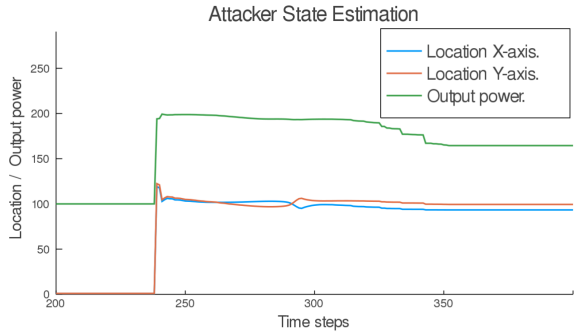


Figure 2.6: Attacker state estimation.

Trajectory Generation

Program 2.3 with the prediction horizon $N = k^{esc} + 40$ and the scaling parameter $\beta = 50000$ is used to generate the estimated and true trajectories

of the simulated scenario shown in Figure 2.7. As shown in Figure 2.8, the state estimation error $\|\boldsymbol{x}_k - \hat{\boldsymbol{x}}_k\|$ is increasing when the UAV is in the effective range of the spoofing device, and the error is bounded by the tolerable error distance $\boldsymbol{\zeta} = 3$ corresponding to $k^{esc} = 125$.

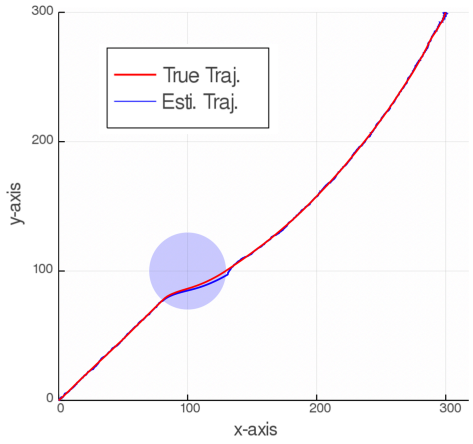


Figure 2.7: Estimated and true trajectories of the simulated scenario. The attacker is located at $(100, 100)$ with $r_{effect} = 30$, which is displayed as the light blue circle.

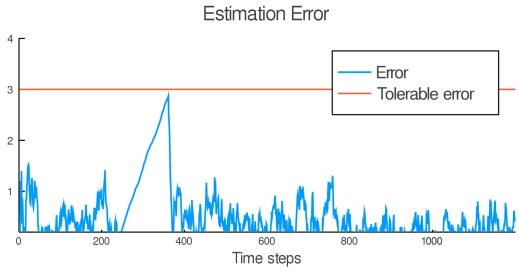
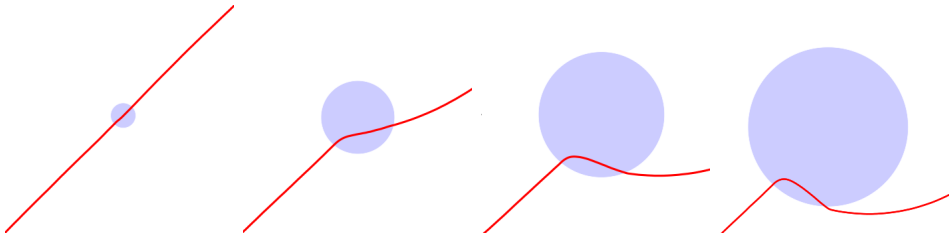


Figure 2.8: Bounded estimation error $\|\boldsymbol{x}_k - \hat{\boldsymbol{x}}_k\|$.

Figure 2.9 presents how the proposed control framework performs in different cases where $r_{effect} \in \{10, 30, 50, 70\}$. Regardless of the size of r_{effect}, the UAV will escape the effective range within the escape time.



(a) $r_{effect} = 10$ **(b)** $r_{effect} = 30$ **(c)** $r_{effect} = 50$ **(d)** $r_{effect} = 70$

Figure 2.9: Trajectories with different effective ranges. In (a), the UAV can pass the attacker without changing the direction, or even its speed since r_{effect} is small enough. From (b)-(d), the UAV drives away from the effective range within the escape time and tries to get as close to the global goal as possible.

2.4 Extension to Time Coordination Tasks for Multi-UAV Systems

Multi-Agent Network

Let $\boldsymbol{x}_{i,k} \in \mathbb{R}^n$, $i = 1, \cdots, N_a$ be the state of the i^{th} agent associated with dynamic system model in Equation (2.1), where N_a is the total number of the agents. Graph theory can provide the natural abstractions for how information is shared between agents in a network [59]. An undirected graph $\mathcal{G} = (V, E)$ consists of a set of nodes $V = \{1, 2, \cdots, N_a\}$, which corresponds to the different agents, and a set of edges $E \subset V \times V$, which relates to a set of unordered pairs of agents. In particular, $(i, j), (j, i) \in E$ if and only if a communication channel exists between agents i and j. The neighborhood $\mathcal{N}(i) \subseteq V$ of the agent i will be understood as the set $\{j \in V \mid (i, j) \in E\}$.

Path Following Consensus

Each agent $i \in V$ has a desired trajectory $g_i : s_{i,k} \to \mathbb{R}^{n_s}$ that is parameterized by coordination state variable $s_{i,k} \in [0, 1]$ as shown in Figure 2.10.

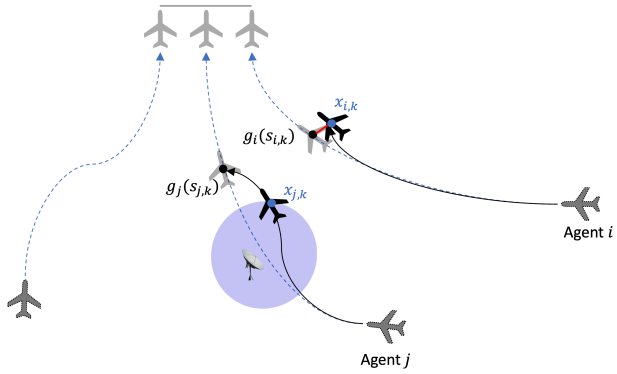


Figure 2.10: Illustration of the path following consensus. The goal of the multi-agent system is for all agents to reach the desired goal state simultaneously. For the agent i at time k, the virtual target/predetermined desired state is $g_i(s_{i,k})$ and the true state is $\boldsymbol{x}_{i,k}$. The error between the virtual target $g_i(s_{i,k})$ and the true state $\boldsymbol{x}_{i,k}$ (marked in red) is to be minimized. The attacker is on the path of the agent j, and the effective spoofing area is displayed as a light blue circle. When the attack is detected, the agent j will be re-planning the trajectory so that the state estimation errors remain in the tolerable region, while the other agents will adjust their coordination states accordingly to achieve time coordination.

Dimension n_s is usually 2 (2−D mission) or 3 (3−D mission).

At time k, $g_i(s_{i,k})$ is the virtual target that the agent i follows at that time, i.e., agent i pursues to minimize the error $\|g_i(s_{i,k}) - \boldsymbol{x}_{i,k}\|$ which is marked in red in Figure 2.10. The state $s_{i,k}$ can be seen as a normalized length of the trajectory. The agents also desire to achieve a consensus on the coordination state variable

$$s_{i,k} - s_{j,k} \overset{k\to\infty}{\longrightarrow} 0 \quad \forall i, j \in V,$$

so that the virtual targets of the agents arrive at the destination at the same time. The agent i knows the coordination state $s_{i,k}$ as well as the coordination states $s_{j,k}$ for neighboring agents $j \in \mathcal{N}(i)$.

Time Coordination Task

Given a multi-agent network consisting of number of N_a agents described in Equation (2.1), the agent i, where $i = 1, \cdots, N_a$, aims to follow its desired trajectory $g_i(\cdot)$ with a reference rate ρ, i.e.

$$g_i(s_{i,k}) - x_{i,k} \overset{k\to\infty}{\longrightarrow} 0 \tag{2.16a}$$

$$s_{i,k+1} - s_{i,k} \overset{k\to\infty}{\longrightarrow} \rho, \tag{2.16b}$$

and to achieve time coordination, i.e.

$$s_{i,k} - s_{j,k} \overset{k\to\infty}{\longrightarrow} 0 \tag{2.17}$$

for all $i, j \in V$, and for all $k \geq 0$. Meanwhile, each agent aims to detect the GPS spoofing attack, obtain the attack-resilient state estimation when considering the limited sensor availability, and complete the path following mission securely.

Consensus Protocol

Consider the coordination state of the consensus network model

$$s_{i,k+1} = s_{i,k} + z_{i,k}, \tag{2.18}$$

where $z_{i,k} \geq 0$ is the control input for the coordination state of the agent i at time index k. To solve the path following consensus problem in Equation (2.16) and Equation (2.17), we propose the design of the control input

$z_{i,k}$. The control input $z_{i,k}$ is designed by

$$z_{i,k} = \max \left\{ -k_e \|g_i(s_{i,k}) - \boldsymbol{x}_{i,k}\| - k_s \sum_{j \in \mathcal{N}(i)} (s_{i,k} - s_{j,k}) + \rho + \mathbf{1}_{i,\text{attacked}} \hat{z}_{i,k}, 0 \right\}, \tag{2.19}$$

where $k_e > 0$ and $k_s > 0$ are coordination control gains, and the reference rate ρ is the desired rate of progress that is a constant. The first term $-k_e \|g_i(s_{i,k}) - \boldsymbol{x}_{i,k}\|$ indicates that the agent reduces the coordination speed when there is a tracking error. The second term $-k_s \sum_{j \in \mathcal{N}(i)} (s_{i,k} - s_{j,k})$ is the consensus term which reduces errors between the local coordination state with those of the neighbors. The third term ρ is the desired rate if there is no tracking error and no coordination error. The last term $\hat{z}_{i,k} = k_e \|g_i(s_{i,k}) - \boldsymbol{x}_{i,k}\|$ drives the virtual target away from the spoofing device even when the UAV detours the planned trajectory. The indicator function $\mathbf{1}_{i,\text{attacked}}$ is defined as follows:

$$\mathbf{1}_{i,\text{attacked}} = \begin{cases} 1, & \textit{if an attack is detected by agent } i \\ 0, & \textit{otherwise} \end{cases}.$$

Moreover, if $-k_e \|g_i(s_{i,k}) - \boldsymbol{x}_{i,k}\| - k_s \sum_{j \in \mathcal{N}(i)} (s_{i,k} - s_{j,k}) + \rho + \mathbf{1}_{i,\text{attacked}} \hat{z}_{i,k}$ is less than zero, then the virtual target chooses to stay at the current state rather than go backward.

Illustrative Example

Trajectory Generation and Time Coordination for Multi-UAV Systems

The nominal trajectories of a three-UAV system $g_i(s_{i,k})$, where $i \in \{1, 2, 3\}$, are generated by the cubic Bézier curves [60]:

$$g_i(s_{i,k}) \triangleq (1 - s_{i,k})^3 \mathbf{P}_i^{(0)} + 3(1 - s_{i,k})^2 s_{i,k} \mathbf{P}_i^{(1)} + 3(1 - s_{i,k}) s_{i,k}^2 \mathbf{P}_i^{(2)} + s_{i,k}^3 \mathbf{P}_i^{(3)}, \tag{2.20}$$

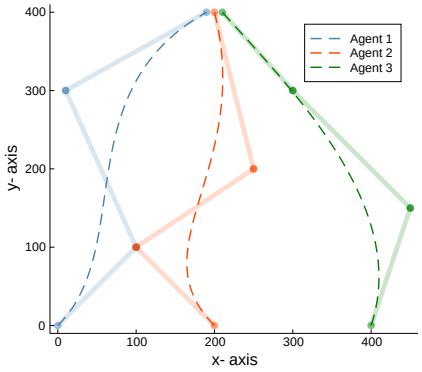
where $s_{i,k} \in [0, 1]$ is the coordination state and $\mathbf{P}_i^{(j)}$, where $j \in \{0, 1, 2, 3\}$, are the control points for the agent i. The control points we used are listed in Table 2.1.

Table 2.1: Bézier curve control points $\mathbf{P}_i^{(j)}$

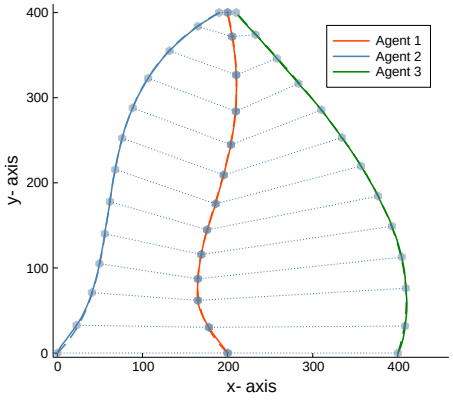
$i/(j)$	(0)	(1)	(2)	(3)
1	$[0\ ,\ \ 0]^\top$	$[100,\ 100]^\top$	$[10,\ 300]^\top$	$[190,\ 400]^\top$
2	$[200,\ 0]^\top$	$[100,\ 100]^\top$	$[250,\ 200]^\top$	$[200,\ 400]^\top$
3	$[400,\ 0]^\top$	$[450,\ 150]^\top$	$[300,\ 300]^\top$	$[210,\ 400]^\top$

Figure 2.11a shows the trajectories generated by Equation (2.20), and the Bézier curve control points for each agent are marked with colored dots. Agent i aims to follow the trajectory starting from point $\mathbf{P}_i^{(0)}$ and plans to arrive at the destination point $\mathbf{P}_i^{(3)}$ simultaneously. To achieve these goals, the time coordination controller proposed in Equation (2.19) is used to update the consensus network in Equation (2.18); then a proportional-derivative (PD) tracking controller is used to track the virtual target generated by the coordination state in Equation (2.18).

The parameters used in Equation (2.19) and the PD controller were set



(a) Trajectories of the three agents in dashed lines generated by Bézier curves Equation (2.20) using the control points summarized in Table 2.1.



(b) Path following trajectories of three agents are plotted in solid lines. Every three hex points connected by two dotted lines indicate the locations of three agents at the same coordination state.

Figure 2.11: Trajectory generation and time coordination.

to the following values:

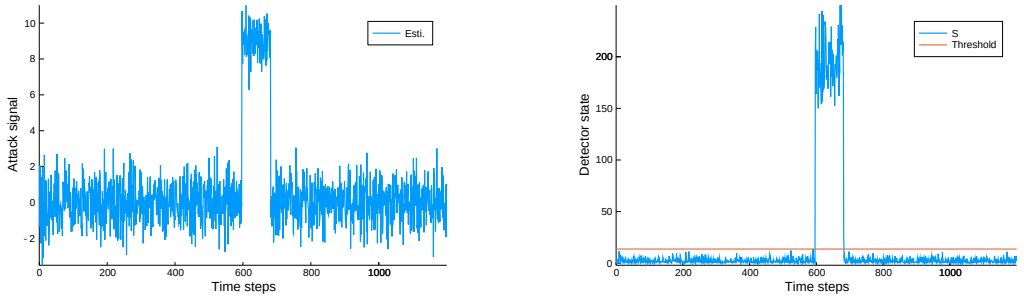
$$\rho = \frac{1}{1200}, \quad k_e = 0.005, \quad k_s = 0.005, \quad k_p = 0.05 \quad \text{and} \quad k_d = 0.315,$$

where k_p and k_d are the proportional gain and the derivative gain.

Figure 2.11b shows the path following and time coordination results. A series of locations of the three agents are plotted by the hex points. Their connections by the dotted lines indicate that they have the same coordination states. We can see that the time coordination and PD control are well-designed, and all agents arrived at the goal destination simultaneously.

In the Presence of GPS Spoofing Attack

The GPS attack happens when the UAV is in the effective range of the spoofing device. In this attack scenario, the attack signal is $\boldsymbol{d}_k = [10, 10]^\top$ and the effective range of the spoofing device is $r_{effect} = 30$. The location



(a) Attack signal estimation. **(b)** Attack detection.

Figure 2.12: Attack estimation and detection.

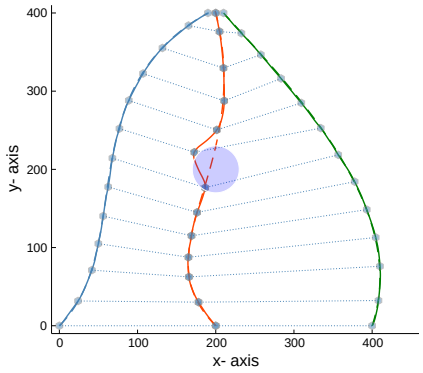
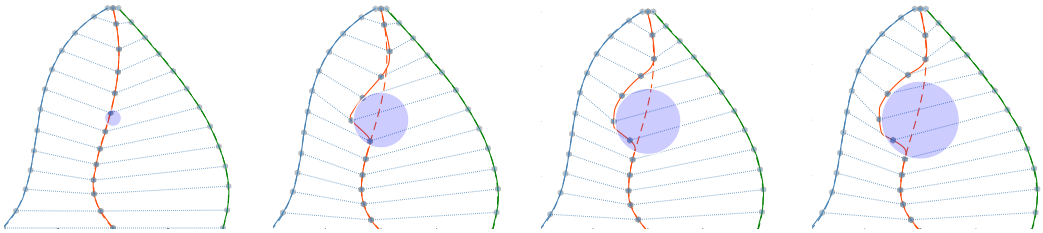


Figure 2.13: Trajectory in the presence of the attack. The attacker is located at $[200, 200]^\top$ with $r_{effect} = 30$, which is displayed as the light blue circle.

of the attacker is $\boldsymbol{x}_k^a = [200, 200]^\top$, which is unknown to the UAV until it is inside the effective range of the spoofing device. The estimation obtained by Equation (2.6) is shown in Figure 2.12a. The detector state S_k can be obtained by using the estimated attack signal as in Equation (2.8). The abnormal high detector state values shown in Figure 2.12b imply that there is an attack. Statistical significance of the attack is tested using the CUSUM detector described in Equation (2.9) with the significance α at 1%. The threshold is calculated by $\frac{\chi^2_{df}(\alpha)}{1-\delta}$ with $\alpha = 0.01$ and $\delta = 0.15$.

ESC in Program 2.3 with the prediction horizon $N = k^{esc} + 50$ and the scaling parameter $\beta = 10000$ is used to generate the new trajectory for safety operation. Figure 2.13 shows the trajectory of the simulated attack scenario.



(a) $r_{effect} = 15$ **(b)** $r_{effect} = 50$ **(c)** $r_{effect} = 60$ **(d)** $r_{effect} = 70$

Figure 2.14: Trajectories when attacker is located at $[200, 200]^\top$ with different effective ranges.

ESC drives the attacked UAV away from the effective range of the spoofing device; time coordination is achieved, and all of the agents arrive at the destination points simultaneously.

Figure 2.14 presents how the proposed control framework performs in different cases where $r_{effect} \in \{15, 50, 60, 70\}$. Regardless of the size of r_{effect}, the UAV will escape the effective range within the escape time and achieve time coordination. In Figure 2.14a, the attacked UAV can pass the attacker without changing the direction or even its speed since r_{effect} is small enough. From Figure 2.14b to Figure 2.14d, the UAV drives away from the effective range within the escape time and tries to get back to the assigned trajectory.

2.5 Discussion

This chapter introduces an alternative approach from a control theoretic perspective contributing to existing GPS attack mitigation literature. Once an attack is detected, the UAV will not use GPS signals for navigation. By using relative sensors (e.g., IMU), the navigation needs to be more accurate due to the sensor drift, where the navigation errors gradually increase over time. In particular, compared to the literature on GPS anti-spoofing techniques, we provided an end-to-end approach with the following contributions:

- We designed a control theoretic attack detector that checks whether the provided position information coincides with the one derived by control theory. Therefore, any GPS attack would be detected if the GPS signals differ from the actual ones. If the injected signals are identical to the authentic ones, then it does not have any physical impact, such as a crash or over-control.

- After the GPS attack is detected, we identified the safe time problem for UAVs in GPS denied environment by formally defining the escape time. To the best of our knowledge, We are the first to investigate the sensor drift problem and escape time analysis.

- Using the fact that the spoofing power should be higher than the authentic signal power in order to mislead the UAVs, we proposed an algorithm, ALT, to obtain the attacker's location and the effective range resiliently by monitoring the signal strength. The proposed algorithm also supports the safety-constrained controller designs.

- Considering the safety constraints, we designed an MPC-based controller to re-plan the UAV trajectory to escape from the effect range. When Programs 2.1 and 2.2 are not feasible, we proposed an alternative approach with the help of the potential function as in Program 2.3 to ensure that the escape controller is executable.

While this case study generated an alternative solution framework compared to the antenna community, as discussed at the beginning of the chapter, the proposed approach has its limitations. Although in robust control mode, the controller can operate the UAV in the presence of noise and disturbances, the assumption is that the UAV is not subject to large external disturbances. For example, wind gusts can also affect the UAV location. The

sudden location change could be confused for a GPS attack. Future exploration to overcome these limitations involves integrating a resilient estimation algorithm for model uncertainties, developing spatio-temporal estimation and robust control framework to cope with unforeseen environments.

Chapter 3

Constrained Attack-Resilient Estimation (CARE)

In this chapter, we aim to solve the resilient estimation problem and investigate the stability and performance of the algorithm design that integrates with information aggregation. To the best of our knowledge, this is the first investigation that considers both state and input inequality constraints for attack-resilient estimation with guaranteed stability.

3.1 Problem Formulation

Consider the following linear time-varying (LTV) discrete-time stochastic system[1]

$$\boldsymbol{x}_{k+1} = \boldsymbol{A}_k \boldsymbol{x}_k + \boldsymbol{B}_k \boldsymbol{u}_k + \boldsymbol{G}_k \boldsymbol{d}_k + \boldsymbol{w}_k \tag{3.1a}$$

$$\boldsymbol{y}_k = \boldsymbol{C}_k \boldsymbol{x}_k + \boldsymbol{v}_k, \tag{3.1b}$$

where $\boldsymbol{x}_k \in \mathbb{R}^m$, $\boldsymbol{u}_k \in \mathbb{R}^n$ and $\boldsymbol{y}_k \in \mathbb{R}^{n_y}$ are the state, the control input, and the sensor measurement, respectively. The attack signal is modeled as a simultaneous input $\boldsymbol{d}_k \in \mathbb{R}^{n_d}$, which is unknown to the defender. System matrices $\boldsymbol{A}_k$, $\boldsymbol{B}_k$, $\boldsymbol{C}_k$ and $\boldsymbol{G}_k$ are known and bounded with appropriate dimensions. We assume that $\text{rank}(\boldsymbol{C}_k \boldsymbol{G}_{k-1}) = n_d$, $0 \leq n_d \leq n_y$. This is a

[1]We consider a general formulation for the attack input matrix $\boldsymbol{G}_k$. If $\boldsymbol{d}_k$ is injected into the control input, then $\boldsymbol{G}_k = \boldsymbol{B}_k$. If $\boldsymbol{d}_k$ is directly injected into the system, then $\boldsymbol{G}_k = \boldsymbol{I}$.

typical assumption as in [61, 62]. The interpretation of this assumption is that the impact of the attack $\boldsymbol{d}_{k-1}$ on the system dynamics can be observed by $\boldsymbol{y}_k$. The process noise $\boldsymbol{w}_k$ and the measurement noise $\boldsymbol{v}_k$ are assumed to be i.i.d. Gaussian random variables with zero means and covariances $\boldsymbol{Q}_k \triangleq \mathbb{E}[\boldsymbol{w}_k \boldsymbol{w}_k^\top] \geq 0$ and $\boldsymbol{R}_k \triangleq \mathbb{E}[\boldsymbol{v}_k \boldsymbol{v}_k^\top] > 0$. Moreover, the measurement noise $\boldsymbol{v}_k$, the process noise $\boldsymbol{w}_k$, and the initial state $\boldsymbol{x}_0$ are uncorrelated with each other.

The adopted attack model in Equation (3.1) is known as the FDI attack that is a very general type of attack and includes physical attacks, Trojans, replay attacks, overflow bugs, packet injection, etc [63]. Because of this generality, this attack model has been widely used in CPS security literature (e.g., [10, 12, 21]).

In the cyber-space, digital attack signals could be unconstrained, but their impact on the physical world is restricted by physical and operational constraints (i.e., $\boldsymbol{x}_k$ and $\boldsymbol{d}_k$ are constrained). For example, a vehicle has a limit on acceleration, velocity, steering angle, and change of steering angle. Any physical constraints and ability limitations on attack signals and states are presented by the inequality constraints

$$\mathcal{A}_k \boldsymbol{d}_k \leq \boldsymbol{b}_k, \ \mathcal{B}_k \boldsymbol{x}_k \leq \boldsymbol{c}_k, \tag{3.2}$$

where matrices $\mathcal{A}_k$, $\mathcal{B}_k$, and vectors $\boldsymbol{b}_k$, $\boldsymbol{c}_k$ are known and bounded with appropriate dimensions. Throughout this paper, we assume that the feasible sets of the constraints in Equation (3.2) are non-empty.

Remark 3.1 *Gaussian noise in Equation (3.1) is one of the general ways to model physical systems so that the filtering algorithms use this model to track the level of uncertainties. Therefore, many pieces of work consider Gaussian*

noise even in the presence of bounded constraints [64, 25, 27].

Problem Statement 3.1 *Given the stochastic system in Equation (3.1), we aim to design an attack-resilient estimation algorithm that can simultaneously estimate the compromised system state $\boldsymbol{x}_k$ and the attack signal $\boldsymbol{d}_k$. In addition, we seek to improve estimation accuracy and detection performance with a stability guarantee when incorporating the information of the input and state in terms of constraints in Equation (3.2).*

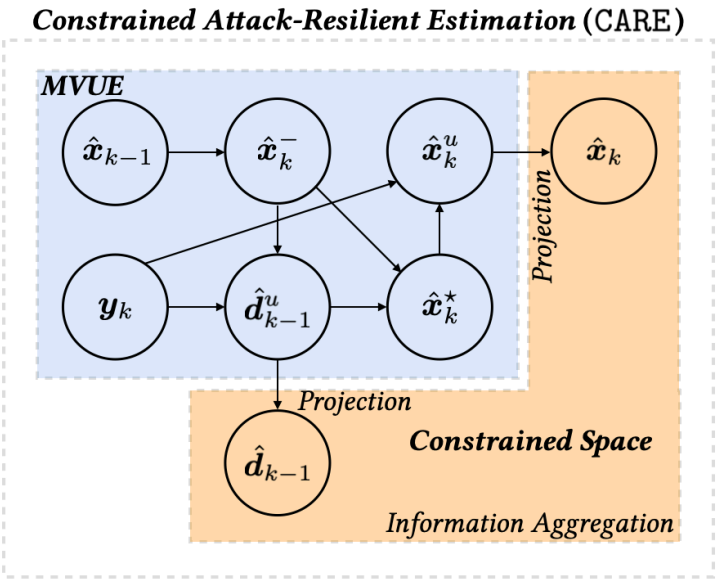


Figure 3.1: Constrained Attack-Resilient Estimation (CARE).

3.2 Algorithm Design

To address Problem Statement 3.1, we propose a constrained attack-resilient estimation algorithm (CARE), as sketched in Figure 3.1, which consists of a minimum-variance unbiased estimator (MVUE) and an information aggregation step via projection. In particular, the optimal estimation provides minimum-variance unbiased estimates, and these estimates are projected

onto the constrained space eventually in the information aggregation step. We outline the essential steps of `CARE` and provide a detailed derivation of the algorithm in the following.

Algorithm Statement

The proposed `CARE` can be summarized as follows:

1. **prediction**:

$$\hat{\boldsymbol{x}}_k^- = \boldsymbol{A}_{k-1}\hat{\boldsymbol{x}}_{k-1} + \boldsymbol{B}_{k-1}\boldsymbol{u}_{k-1}; \tag{3.3}$$

2. **attack estimation**:

$$\hat{\boldsymbol{d}}_{k-1}^u = \boldsymbol{M}_k(\boldsymbol{y}_k - \boldsymbol{C}_k\hat{\boldsymbol{x}}_k^-); \tag{3.4}$$

3. **time update**:

$$\hat{\boldsymbol{x}}_k^\star = \hat{\boldsymbol{x}}_k^- + \boldsymbol{G}_{k-1}\hat{\boldsymbol{d}}_{k-1}^u; \tag{3.5}$$

4. **measurement update**:

$$\hat{\boldsymbol{x}}_k^u = \hat{\boldsymbol{x}}_k^\star + \boldsymbol{L}_k(\boldsymbol{y}_k - \boldsymbol{C}_k\hat{\boldsymbol{x}}_k^\star); \tag{3.6}$$

5. **projection update**:

$$\hat{\boldsymbol{d}}_{k-1} = \arg\min_{\boldsymbol{d}} (\boldsymbol{d} - \hat{\boldsymbol{d}}^u_{k-1})^\top (\boldsymbol{P}^{d,u}_{k-1})^{-1} (\boldsymbol{d} - \hat{\boldsymbol{d}}^u_{k-1})$$
$$\text{subject to } \mathcal{A}_{k-1}\boldsymbol{d} \leq \boldsymbol{b}_{k-1}; \tag{3.7}$$
$$\hat{\boldsymbol{x}}_k = \arg\min_{\boldsymbol{x}} (\boldsymbol{x} - \hat{\boldsymbol{x}}^u_k)^\top (\boldsymbol{P}^{x,u}_k)^{-1} (\boldsymbol{x} - \hat{\boldsymbol{x}}^u_k)$$
$$\text{subject to } \mathcal{B}_k\boldsymbol{x} \leq \boldsymbol{c}_k. \tag{3.8}$$

Given the previous state estimate $\hat{\boldsymbol{x}}_{k-1}$ and its error covariance $\boldsymbol{P}^x_{k-1} \triangleq \mathbb{E}[\tilde{\boldsymbol{x}}_{k-1}(\tilde{\boldsymbol{x}}_{k-1})^\top]$, the current state can be predicted by $\hat{\boldsymbol{x}}^-_k$ in Equation (3.3) under the assumption that the attack signal $\boldsymbol{d}_{k-1}$ is absent. The unconstrained attack estimate $\hat{\boldsymbol{d}}^u_{k-1}$ can be obtained by comparing the difference between the predicted output $\boldsymbol{C}_k\hat{\boldsymbol{x}}^-_k$ and the measured output $\boldsymbol{y}_k$ in Equation (3.4), where $\boldsymbol{M}_k$ is the optimal filter gain that can be obtained by applying Gauss-Markov theorem, as shown in Proposition 3.2 later. The state prediction $\hat{\boldsymbol{x}}^-_k$ can be updated incorporating the unconstrained attack estimate $\hat{\boldsymbol{d}}^u_{k-1}$ in Equation (3.5). The output $\boldsymbol{y}_k$ is used to correct the current state estimate in Equation (3.6), where $\boldsymbol{L}_k$ is the filter gain that is obtained by minimizing the state error covariance $\boldsymbol{P}^{x,u}_k$. In the information aggregation step (projection update), we apply the input constraint in Equation (3.7) by projecting $\hat{\boldsymbol{d}}^u_{k-1}$ onto the constrained space and obtain the constrained attack estimate $\hat{\boldsymbol{d}}_{k-1}$. Similarly, the state constraint in Equation (3.8) is applied to obtain the constrained state estimate $\hat{\boldsymbol{x}}_k$. The complete algorithm is presented in Algorithm 2.

Algorithm Derivation

Prediction The current state can be predicted by Equation (3.3) under the assumption that the attack signal $\boldsymbol{d}_{k-1} = 0$. The prediction error covariance is

$$\boldsymbol{P}_k^{x,-} \triangleq \mathbb{E}[\tilde{\boldsymbol{x}}_k^-(\tilde{\boldsymbol{x}}_k^-)^\top] = \boldsymbol{A}_{k-1}\boldsymbol{P}_{k-1}^x\boldsymbol{A}_{k-1}^\top + \boldsymbol{Q}_{k-1}. \tag{3.9}$$

Attack estimation The linear attack estimator in Equation (3.4) utilizes the difference between the measured output $\boldsymbol{y}_k$ and the predicted output $\boldsymbol{C}_k\hat{\boldsymbol{x}}_k^-$. Substituting Equation (3.1) and Equation (3.3) into Equation (3.4), we have

$$\begin{aligned}\hat{\boldsymbol{d}}_{k-1}^u = \boldsymbol{M}_k\big(&\boldsymbol{C}_k\boldsymbol{A}_{k-1}\tilde{\boldsymbol{x}}_{k-1} + \boldsymbol{C}_k\boldsymbol{G}_{k-1}\boldsymbol{d}_{k-1} \\ &+ \boldsymbol{C}_k\boldsymbol{w}_{k-1} + \boldsymbol{v}_k\big),\end{aligned}$$

which is a linear function of the attack signal $\boldsymbol{d}_{k-1}$. Under the assumption that there is no projection update, i.e., the state and attack estimates are unconstrained, we design the optimal gain matrix $\boldsymbol{M}_k$ such that the estimate becomes the best linear unbiased estimate (BLUE) by the following two propositions.

Proposition 3.1 *Assume that there is no projection update and* $\mathbb{E}[\tilde{\boldsymbol{x}}_0] = \mathbb{E}[\tilde{\boldsymbol{x}}_0^\star] = 0$. *The state estimates* $\hat{\boldsymbol{x}}_k$ *and the unconstrained attack estimates* $\hat{\boldsymbol{d}}_k^u$ *are unbiased for all* k, *i.e.* $\mathbb{E}[\tilde{\boldsymbol{x}}_k] = \mathbb{E}[\tilde{\boldsymbol{d}}_{k-1}^u] = 0$, $\forall k$, *if and only if* $\boldsymbol{M}_k\boldsymbol{C}_k\boldsymbol{G}_{k-1} = \boldsymbol{I}$.

Proof: Sufficiency: Assuming that $\boldsymbol{M}_k\boldsymbol{C}_k\boldsymbol{G}_{k-1} = \boldsymbol{I}$, the statement can be proved by induction. First, we will show the statement holds when $k = 0$

as a base case. By the definition, the errors of the time update and the measurement update in Equation (3.5) and Equation (3.6) are given by

$$\tilde{\boldsymbol{x}}_k^\star \triangleq \boldsymbol{x}_k - \hat{\boldsymbol{x}}_k^\star = \boldsymbol{A}_{k-1}\tilde{\boldsymbol{x}}_{k-1} + \boldsymbol{G}_{k-1}\tilde{\boldsymbol{d}}_{k-1}^u + \boldsymbol{w}_{k-1} \tag{3.10}$$

$$\tilde{\boldsymbol{x}}_k^u \triangleq \boldsymbol{x}_k - \hat{\boldsymbol{x}}_k^u = (\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)\tilde{\boldsymbol{x}}_k^\star - \boldsymbol{L}_k\boldsymbol{v}_k, \tag{3.11}$$

and the error of the unconstrained attack estimate is

$$\begin{aligned}
\tilde{\boldsymbol{d}}_{k-1}^u \triangleq \boldsymbol{d}_{k-1} - \hat{\boldsymbol{d}}_{k-1}^u &= \boldsymbol{d}_{k-1} - \boldsymbol{M}_k\big(\boldsymbol{C}_k\boldsymbol{A}_{k-1}\tilde{\boldsymbol{x}}_{k-1} \\
&\quad + \boldsymbol{C}_k\boldsymbol{G}_{k-1}\boldsymbol{d}_{k-1} + \boldsymbol{C}_k\boldsymbol{w}_{k-1} + \boldsymbol{v}_k\big) \\
&= (\boldsymbol{I} - \boldsymbol{M}_k\boldsymbol{C}_k\boldsymbol{G}_{k-1})\boldsymbol{d}_{k-1} && \text{(3.12a)} \\
&\quad - \boldsymbol{M}_k\big(\boldsymbol{C}_k\boldsymbol{A}_{k-1}\tilde{\boldsymbol{x}}_{k-1} + \boldsymbol{C}_k\boldsymbol{w}_{k-1} + \boldsymbol{v}_k\big). && \text{(3.12b)}
\end{aligned}$$

Under the assumptions that $\mathbb{E}[\tilde{\boldsymbol{x}}_0] = \mathbb{E}[\tilde{\boldsymbol{x}}_0^\star] = 0$ and the process noise and measurement noise are zero-mean Gaussian, i.e. $\mathbb{E}[\boldsymbol{w}_k] = \mathbb{E}[\boldsymbol{v}_k] = 0,\ \forall k$, the expectation of the term (3.12b) is zero at $k = 1$. Since $\boldsymbol{d}_{k-1}$ is deterministic for all k, i.e., $\mathbb{E}[\boldsymbol{d}_{k-1}] \neq 0$, we have $\mathbb{E}[\tilde{\boldsymbol{d}}_0^u] = 0$ if $\boldsymbol{I} - \boldsymbol{M}_1\boldsymbol{C}_1\boldsymbol{G}_0 = 0$, i.e., the expectation of the term Equation (3.12a) is zero at $k = 1$. Then we have $\mathbb{E}[\tilde{\boldsymbol{x}}_1^\star] = \mathbb{E}[\tilde{\boldsymbol{x}}_1^u] = 0$ by applying expectation operation on Equation (3.10) and Equation (3.11). In the inductive step, suppose $\mathbb{E}[\tilde{\boldsymbol{x}}_k^u] = \mathbb{E}[\tilde{\boldsymbol{x}}_k^\star] = 0$; then $\mathbb{E}[\tilde{\boldsymbol{d}}_k^u] = 0$ if $\boldsymbol{M}_{k+1}\boldsymbol{C}_{k+1}\boldsymbol{G}_k = \boldsymbol{I}$. Then, similarly, we have $\mathbb{E}[\tilde{\boldsymbol{x}}_{k+1}^\star] = \mathbb{E}[\tilde{\boldsymbol{x}}_{k+1}^u] = 0$ by Equation (3.10) and Equation (3.11). Since there is no projection update, we have $\mathbb{E}[\tilde{\boldsymbol{x}}_k] = \mathbb{E}[\tilde{\boldsymbol{x}}_k^u] = 0\ \forall k$.

Necessity: Assuming that $\mathbb{E}[\tilde{\boldsymbol{x}}_k] = \mathbb{E}[\tilde{\boldsymbol{d}}_{k-1}] = 0$ for all k, or equivalently $\mathbb{E}[\tilde{\boldsymbol{x}}_k^u] = \mathbb{E}[\tilde{\boldsymbol{d}}_{k-1}^u] = 0$, the statement also can be proved by induction. In Equation (3.12), if $\mathbb{E}[\tilde{\boldsymbol{d}}_0^u] = 0$ for any $\boldsymbol{d}_0$, we have $\boldsymbol{M}_1\boldsymbol{C}_1\boldsymbol{G}_0 = \boldsymbol{I}$. Therefore, following a similar procedure, we can show that the necessity holds. □

Proposition 3.2 *Assume that there is no projection update and* $\mathbb{E}[\tilde{\boldsymbol{x}}_0] = \mathbb{E}[\tilde{\boldsymbol{x}}_0^\star] = 0$. *The unconstrained attack estimates* $\hat{\boldsymbol{d}}_k^u$ *are BLUE if*

$$\boldsymbol{M}_k = \left(\boldsymbol{G}_{k-1}^\top \boldsymbol{C}_k^\top \tilde{\boldsymbol{R}}_k \boldsymbol{C}_k \boldsymbol{G}_{k-1}\right)^{-1} \boldsymbol{G}_{k-1}^\top \boldsymbol{C}_k^\top \tilde{\boldsymbol{R}}_k, \tag{3.13}$$

where $\tilde{\boldsymbol{R}}_k \triangleq (\boldsymbol{C}_k \boldsymbol{P}_k^{x,-} \boldsymbol{C}_k^\top + \boldsymbol{R}_k)^{-1}$.

Proof: Substituting Equation (3.1a) into Equation (3.1b), we have

$$\begin{aligned} \boldsymbol{y}_k &= \boldsymbol{C}_k \boldsymbol{G}_{k-1} \boldsymbol{d}_{k-1} \\ &\quad + \boldsymbol{C}_k \left(\boldsymbol{A}_{k-1} \boldsymbol{x}_{k-1} + \boldsymbol{B}_{k-1} \boldsymbol{u}_{k-1} + \boldsymbol{w}_{k-1}\right) + \boldsymbol{v}_k. \end{aligned} \tag{3.14}$$

Subtraction of $\boldsymbol{C}_k \hat{\boldsymbol{x}}_{k-1}$ on the both sides of Equation (3.14) yields

$$\begin{aligned} \boldsymbol{y}_k - \boldsymbol{C}_k \hat{\boldsymbol{x}}_{k-1} &= \boldsymbol{C}_k \boldsymbol{G}_{k-1} \boldsymbol{d}_{k-1} \\ &\quad \underbrace{+ \boldsymbol{C}_k \left(\boldsymbol{A}_{k-1} \tilde{\boldsymbol{x}}_{k-1}^- + \boldsymbol{w}_{k-1}\right) + \boldsymbol{v}_k}_{\text{error term}}. \end{aligned} \tag{3.15}$$

Since the covariances of the process noise $\boldsymbol{w}_{k-1}$ and the measurement noise $\boldsymbol{v}_k$ are known, with Equation (3.9), the covariance of the error term in Equation (3.15) can be expressed as $\boldsymbol{C}_k \boldsymbol{P}_k^{x,-} \boldsymbol{C}_k^\top + \boldsymbol{R}_k$. Applying the Gauss-Markov theorem (see Appendix C), we can get the minimum-variance-unbiased linear estimator (BLUE) of $\boldsymbol{d}_{k-1}$ in Equation (3.4) with

$$\boldsymbol{M}_k = \left(\boldsymbol{G}_{k-1}^\top \boldsymbol{C}_k^\top \tilde{\boldsymbol{R}}_k \boldsymbol{C}_k \boldsymbol{G}_{k-1}\right)^{-1} \boldsymbol{G}_{k-1}^\top \boldsymbol{C}_k^\top \tilde{\boldsymbol{R}}_k,$$

where $\tilde{\boldsymbol{R}}_k \triangleq (\boldsymbol{C}_k \boldsymbol{P}_k^{x,-} \boldsymbol{C}_k^\top + \boldsymbol{R}_k)^{-1}$. □

Remark 3.2 *The rank condition rank*$(\boldsymbol{C}_k \boldsymbol{G}_{k-1}) = n_d$ *is the sufficient condition of* $\boldsymbol{M}_k \boldsymbol{C}_k \boldsymbol{G}_{k-1} = \boldsymbol{I}$ *needed in Proposition 3.1 if* $\boldsymbol{M}_k$ *is found by Equa-*

tion (3.13) in Proposition 3.2.

The error covariance can be found by

$$\boldsymbol{P}_{k-1}^{d,u} = \boldsymbol{M}_k \tilde{\boldsymbol{R}}_k^{-1} \boldsymbol{M}_k^\top = \left(\boldsymbol{G}_{k-1}^\top \boldsymbol{C}_k^\top \tilde{\boldsymbol{R}}_k \boldsymbol{C}_k \boldsymbol{G}_{k-1}\right)^{-1}.$$

The cross error covariance of the state estimate and the attack estimate is $\boldsymbol{P}_{k-1}^{xd} = -\boldsymbol{P}_{k-1}^{x} \boldsymbol{A}_{k-1}^\top \boldsymbol{C}_k^\top \boldsymbol{M}_k^\top$.

Time update Given the unconstrained attack estimate $\hat{\boldsymbol{d}}_{k-1}^u$, the state prediction $\hat{\boldsymbol{x}}_k^-$ can be updated as in Equation (3.5). We derive the error covariance of $\hat{\boldsymbol{x}}_k^\star$ as

$$\begin{aligned}
\boldsymbol{P}_k^{x\star} &\triangleq \mathbb{E}\left[\tilde{\boldsymbol{x}}_k^\star (\tilde{\boldsymbol{x}}_k^\star)^\top\right] \\
&= \boldsymbol{A}_{k-1} \boldsymbol{P}_{k-1}^{x} \boldsymbol{A}_{k-1}^\top + \boldsymbol{A}_{k-1} \boldsymbol{P}_{k-1}^{xd} \boldsymbol{G}_{k-1}^\top \\
&+ \boldsymbol{G}_{k-1} \boldsymbol{P}_{k-1}^{dx} \boldsymbol{A}_{k-1}^\top + \boldsymbol{G}_{k-1} \boldsymbol{P}_{k-1}^{d,u} \boldsymbol{G}_{k-1}^\top + \boldsymbol{Q}_{k-1} \\
&- \boldsymbol{G}_{k-1} \boldsymbol{M}_k \boldsymbol{C}_k \boldsymbol{Q}_{k-1} - \boldsymbol{Q}_{k-1} \boldsymbol{C}_k^\top \boldsymbol{M}_k^\top \boldsymbol{G}_{k-1}^\top,
\end{aligned}$$

where $\boldsymbol{P}_{k-1}^{dx} = (\boldsymbol{P}_{k-1}^{xd})^\top$.

Measurement update In this step, the measurement $\boldsymbol{y}_k$ is used to update the propagated estimate $\hat{\boldsymbol{x}}_k^\star$ as shown in Equation (3.6). The covariance of the state estimation error is

$$\begin{aligned}
\boldsymbol{P}_k^{x,u} \triangleq& \mathbb{E}[(\tilde{\boldsymbol{x}}_k^u)(\tilde{\boldsymbol{x}}_k^u)^\top] \\
=& (\boldsymbol{I} - \boldsymbol{L}_k \boldsymbol{C}_k) \boldsymbol{G}_{k-1} \boldsymbol{M}_k \boldsymbol{R}_k \boldsymbol{L}_k^\top + \boldsymbol{L}_k \boldsymbol{R}_k \boldsymbol{L}_k^\top \\
&+ \boldsymbol{L}_k \boldsymbol{R}_k \boldsymbol{M}_k^\top \boldsymbol{G}_{k-1}^\top (\boldsymbol{I} - \boldsymbol{L}_k \boldsymbol{C}_k)^\top \\
&+ (\boldsymbol{I} - \boldsymbol{L}_k \boldsymbol{C}_k) \boldsymbol{P}_k^{x\star} (\boldsymbol{I} - \boldsymbol{L}_k \boldsymbol{C}_k)^\top.
\end{aligned}$$

The gain matrix $\boldsymbol{L}_k$ is obtained by minimizing the trace of $\boldsymbol{P}_k^{x,u}$, i.e.

$$\min_{\boldsymbol{L}_k} \operatorname{tr}(\boldsymbol{P}_k^{x,u}).$$

The solution is given by

$$\boldsymbol{L}_k = (\boldsymbol{P}_k^{x\star}\boldsymbol{C}_k^\top - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{R}_k)\tilde{\boldsymbol{R}}_k^{\star\dagger},$$

where $\tilde{\boldsymbol{R}}_k^\star \triangleq \boldsymbol{C}_k\boldsymbol{P}_k^{x\star}\boldsymbol{C}_k^\top + \boldsymbol{R}_k - \boldsymbol{C}_k\boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{R}_k - \boldsymbol{R}_k\boldsymbol{M}_k^\top\boldsymbol{G}_{k-1}^\top\boldsymbol{C}_k^\top$.

Projection update We are now in the position to project the estimates onto the constrained space. Apply the first constraint in Equation (3.2) to the unconstrained attack estimate $\hat{\boldsymbol{d}}_{k-1}^u$, and the attack estimation problem can be formulated as the following constrained convex optimization problem

$$\begin{aligned} \hat{\boldsymbol{d}}_{k-1} = \arg\min_{\boldsymbol{d}} &(\boldsymbol{d} - \hat{\boldsymbol{d}}_{k-1}^u)^\top \boldsymbol{W}_{k-1}^d (\boldsymbol{d} - \hat{\boldsymbol{d}}_{k-1}^u) \\ \text{subject to } &\mathcal{A}_{k-1}\boldsymbol{d} \leq \boldsymbol{b}_{k-1}, \end{aligned} \tag{3.16}$$

where $\boldsymbol{W}_{k-1}^d$ can be any positive definite symmetric weighting matrix. In the current paper, we select $\boldsymbol{W}_{k-1}^d = (\boldsymbol{P}_{k-1}^{d,u})^{-1}$ which results in the smallest error covariance as shown in [25]. From Karush-Kuhn-Tucker (KKT) conditions of optimality, we can find the corresponding active constraints. We denote $\bar{\mathcal{A}}_k$ and $\bar{\boldsymbol{b}}_k$ the rows of $\mathcal{A}_k$ and the elements of $\boldsymbol{b}_k$ corresponding to the active constraints of $\mathcal{A}_{k-1}\boldsymbol{d} \leq \boldsymbol{b}_{k-1}$. Then Equation (3.16) becomes

$$\begin{aligned} \hat{\boldsymbol{d}}_{k-1} = \arg\min_{\boldsymbol{d}} &(\boldsymbol{d} - \hat{\boldsymbol{d}}_{k-1}^u)^\top (\boldsymbol{P}_{k-1}^{d,u})^{-1} (\boldsymbol{d} - \hat{\boldsymbol{d}}_{k-1}^u) \\ \text{subject to } &\bar{\mathcal{A}}_{k-1}\boldsymbol{d} = \bar{\boldsymbol{b}}_{k-1}. \end{aligned} \tag{3.17}$$

The solution of Equation (3.17) can be found by

$$\hat{\boldsymbol{d}}_{k-1} = \hat{\boldsymbol{d}}^u_{k-1} - \boldsymbol{\gamma}^d_{k-1}(\bar{\mathcal{A}}_{k-1}\hat{\boldsymbol{d}}^u_{k-1} - \bar{\boldsymbol{b}}_{k-1}),$$

where

$$\boldsymbol{\gamma}^d_{k-1} \triangleq \boldsymbol{P}^{d,u}_{k-1}\bar{\mathcal{A}}^\top_{k-1}(\bar{\mathcal{A}}_{k-1}\boldsymbol{P}^{d,u}_{k-1}\bar{\mathcal{A}}^\top_{k-1})^{-1}. \tag{3.18}$$

The attack estimation error is

$$\begin{aligned}\tilde{\boldsymbol{d}}_{k-1} &= (\boldsymbol{I} - \boldsymbol{\gamma}^d_{k-1}\bar{\mathcal{A}}_{k-1})\tilde{\boldsymbol{d}}^u_{k-1} + \boldsymbol{\gamma}^d_{k-1}(\bar{\mathcal{A}}_{k-1}\boldsymbol{d}_{k-1} - \bar{\boldsymbol{b}}_{k-1}) \\ &= \hat{\boldsymbol{d}}^u_{k-1} - \boldsymbol{\gamma}^d_{k-1}(\bar{\mathcal{A}}_{k-1}\hat{\boldsymbol{d}}^u_{k-1} - \bar{\boldsymbol{b}}_{k-1}).\end{aligned} \tag{3.19}$$

The error covariance can be found by

$$\begin{aligned}\boldsymbol{P}^d_{k-1} &\triangleq \mathbb{E}[\tilde{\boldsymbol{d}}_{k-1}\tilde{\boldsymbol{d}}^\top_{k-1}] \\ &= (\boldsymbol{I} - \boldsymbol{\gamma}^d_{k-1}\bar{\mathcal{A}}_{k-1})\boldsymbol{P}^{d,u}_{k-1}(\boldsymbol{I} - \boldsymbol{\gamma}^d_{k-1}\bar{\mathcal{A}}_{k-1})^\top\end{aligned} \tag{3.20}$$

under the assumption that $\boldsymbol{\gamma}^d_{k-1}(\bar{\mathcal{A}}_{k-1}\boldsymbol{d}_{k-1} - \bar{\boldsymbol{b}}_{k-1}) = 0$ holds. Notice that this assumption holds when the ground truth $\boldsymbol{d}_{k-1}$ satisfies the active constraint $\bar{\mathcal{A}}_{k-1}\boldsymbol{d}_{k-1} = \bar{\boldsymbol{b}}_{k-1}$. From Equation (3.18), it can be verified that $\boldsymbol{\gamma}^d_{k-1}\bar{\mathcal{A}}_{k-1}\boldsymbol{P}^{d,u}_{k-1} = \boldsymbol{\gamma}^d_{k-1}\bar{\mathcal{A}}_{k-1}\boldsymbol{P}^{d,u}_{k-1}(\boldsymbol{\gamma}^d_{k-1}\bar{\mathcal{A}}_{k-1})^\top$. Therefore, from Equation (3.20) we have

$$\begin{aligned}\boldsymbol{P}^d_{k-1} =& \boldsymbol{P}^{d,u}_{k-1} - \boldsymbol{\gamma}^d_{k-1}\bar{\mathcal{A}}_{k-1}\boldsymbol{P}^{d,u}_{k-1} - \boldsymbol{P}^{d,u}_{k-1}(\boldsymbol{\gamma}^d_{k-1}\bar{\mathcal{A}}_{k-1})^\top \\ &+ \boldsymbol{\gamma}^d_{k-1}\bar{\mathcal{A}}_{k-1}\boldsymbol{P}^{d,u}_{k-1}(\boldsymbol{\gamma}^d_{k-1}\bar{\mathcal{A}}_{k-1})^\top \\ =& (\boldsymbol{I} - \boldsymbol{\gamma}^d_{k-1}\bar{\mathcal{A}}_{k-1})\boldsymbol{P}^{d,u}_{k-1}.\end{aligned} \tag{3.21}$$

Similarly, applying the second constraint in Equation (3.2) to the unconstrained state estimate $\hat{\boldsymbol{x}}_k^u$, we formalize the state estimation problem as follows:

$$\begin{aligned} \hat{\boldsymbol{x}}_k = \arg\min_{\boldsymbol{x}} & (\boldsymbol{x} - \hat{\boldsymbol{x}}_k^u)^\top \boldsymbol{W}_k^x (\boldsymbol{x} - \hat{\boldsymbol{x}}_k^u) \\ \text{subject to } & \mathcal{B}_k \boldsymbol{x} \leq \boldsymbol{c}_k, \end{aligned} \tag{3.22}$$

where we select $\boldsymbol{W}_k^x = (\boldsymbol{P}_k^{x,u})^{-1}$ for the smallest error covariance. We denote $\bar{\mathcal{B}}_k$ and $\bar{\boldsymbol{c}}_k$ the rows of $\mathcal{B}_k$ and the elements of $\boldsymbol{c}_k$ corresponding to the active constraints of $\mathcal{B}_k \boldsymbol{x} \leq \boldsymbol{c}_k$. Using the active constraints, we reformulate Equation (3.22) as follows:

$$\begin{aligned} \hat{\boldsymbol{x}}_k = \arg\min_{\boldsymbol{x}} & (\boldsymbol{x} - \hat{\boldsymbol{x}}_k^u)^\top (\boldsymbol{P}_k^{x,u})^{-1} (\boldsymbol{x} - \hat{\boldsymbol{x}}_k^u) \\ \text{subject to } & \bar{\mathcal{B}}_k \boldsymbol{x} = \bar{\boldsymbol{c}}_k. \end{aligned} \tag{3.23}$$

The solution of Equation (3.23) is given by $\hat{\boldsymbol{x}}_k = \hat{\boldsymbol{x}}_k^u - \boldsymbol{\gamma}_k^x (\bar{\mathcal{B}}_k \hat{\boldsymbol{x}}_k^u - \bar{\boldsymbol{c}}_k)$, where

$$\boldsymbol{\gamma}_k^x \triangleq \boldsymbol{P}_k^{x,u} \bar{\mathcal{B}}_k^\top (\bar{\mathcal{B}}_k \boldsymbol{P}_k^{x,u} \bar{\mathcal{B}}_k^\top)^{-1}. \tag{3.24}$$

Under the assumption that $\boldsymbol{\gamma}_k^x (\bar{\mathcal{B}}_k \hat{\boldsymbol{x}}_k^u - \bar{\boldsymbol{c}}_k) = 0$ holds, the state estimation error covariance can be expressed as

$$\boldsymbol{P}_k^x = \bar{\boldsymbol{\Gamma}}_k \boldsymbol{P}_k^{x,u} \bar{\boldsymbol{\Gamma}}_k^\top, \tag{3.25}$$

where $\bar{\boldsymbol{\Gamma}}_k \triangleq \boldsymbol{I} - \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k$. Notice that this assumption holds when the ground truth $\boldsymbol{x}_k$ satisfies the active constraint $\bar{\mathcal{B}}_k \boldsymbol{x}_k = \bar{\boldsymbol{c}}_k$.

3.3 Performance and Stability Analysis

We will show that the projection induced by inequality constraints improves attack-resilient estimation accuracy and detection performance by decreasing estimation errors and the false negative rate in attack detection. Notice that the estimate $\hat{\boldsymbol{d}}_{k-1}$ and the ground truth $\boldsymbol{d}_{k-1}$ satisfy the active constraint $\bar{\mathcal{A}}_{k-1}\hat{\boldsymbol{d}}_{k-1} - \bar{\boldsymbol{b}}_{k-1} = 0$ in Equation (3.17) and the inequality constraint $\mathcal{A}_{k-1}\boldsymbol{d}_{k-1} \leq \boldsymbol{b}_{k-1}$ in Equation (3.2), respectively. However, it is uncertain whether the ground truth satisfies the active constraints or not. In this case, from Equation (3.19) we have

$$\mathbb{E}[\tilde{\boldsymbol{d}}_{k-1}] = \boldsymbol{\gamma}^d_{k-1}(\bar{\mathcal{A}}_{k-1}\boldsymbol{d}_{k-1} - \bar{\boldsymbol{b}}_{k-1}) \neq 0. \tag{3.26}$$

A similar statement holds for the state estimation error:

$$\mathbb{E}[\tilde{\boldsymbol{x}}_k] = \boldsymbol{\gamma}^x_k(\bar{\mathcal{B}}_k\boldsymbol{x}_k - \bar{\boldsymbol{c}}_k) \neq 0. \tag{3.27}$$

These considerations indicate that the projection potentially induces biased estimates, rendering the traditional stability analysis for unbiased estimation invalid. In this context, we will prove that estimation errors of the `CARE` are practically exponentially stable in mean square.

Estimation Performance

For the analysis of the performance through the projection, we first decompose the state estimation error $\tilde{\boldsymbol{x}}_k$ into two orthogonal spaces as follows:

$$\tilde{\boldsymbol{x}}_k = (\boldsymbol{I} - \boldsymbol{\gamma}^x_k\bar{\mathcal{B}}_k)\tilde{\boldsymbol{x}}_k + \boldsymbol{\gamma}^x_k\bar{\mathcal{B}}_k\tilde{\boldsymbol{x}}_k. \tag{3.28}$$

We will show that the errors in the space $\boldsymbol{I} - \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k$ remain identical after the projection, while the errors in the space $\boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k$ reduce through the projection, as in Lemma 3.1.

Lemma 3.1 *The decomposition of $\tilde{\boldsymbol{x}}_k$ in the space $\boldsymbol{I} - \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k$ is equal to that of $\tilde{\boldsymbol{x}}_k^u$, and the decomposition of $\tilde{\boldsymbol{x}}_k$ in the space $\boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k$ is equal to that of $\tilde{\boldsymbol{x}}_k^u$ scaled by $\boldsymbol{\alpha}_k$, i.e.*

$$(\boldsymbol{I} - \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k)\tilde{\boldsymbol{x}}_k = (\boldsymbol{I} - \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k)\tilde{\boldsymbol{x}}_k^u \tag{3.29}$$

$$\boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k \tilde{\boldsymbol{x}}_k = \boldsymbol{\alpha}_k \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k \tilde{\boldsymbol{x}}_k^u, \tag{3.30}$$

where $\boldsymbol{\alpha}_k = diag\,(\boldsymbol{\alpha}_k^1, \cdots, \boldsymbol{\alpha}_k^n)$, and

$$\boldsymbol{\alpha}_k^i \triangleq (\boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k \tilde{\boldsymbol{x}}_k)(i)((\boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k \tilde{\boldsymbol{x}}_k^u)(i))^\dagger \in [0, 1)$$

for $i = 1, \cdots, n$. Similarly, it holds that

$$(\boldsymbol{I} - \boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k)\tilde{\boldsymbol{d}}_k = (\boldsymbol{I} - \boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k)\tilde{\boldsymbol{d}}_k^u$$

$$\boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k \tilde{\boldsymbol{d}}_k = \boldsymbol{\kappa}_k \boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k \tilde{\boldsymbol{d}}_k^u,$$

where $\boldsymbol{\kappa}_k = diag\,(\boldsymbol{\kappa}_k^1, \cdots, \boldsymbol{\kappa}_k^n)$, and $\boldsymbol{\kappa}_k^i \triangleq (\boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k \tilde{\boldsymbol{d}}_k)(i)((\boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k \tilde{\boldsymbol{d}}_k^u)(i))^\dagger \in [0, 1)$ for $i = 1, \cdots, n$.

Proof: The relationship in Equation (3.29) can be obtained by applying

$\bar{\mathcal{B}}_k \hat{\boldsymbol{x}}_k = \bar{\boldsymbol{c}}_k$ to

$$\begin{aligned}
\tilde{\boldsymbol{x}}_k &= \boldsymbol{x}_k - \hat{\boldsymbol{x}}_k = \boldsymbol{x}_k - (\hat{\boldsymbol{x}}_k^u - \boldsymbol{\gamma}_k^x(\bar{\mathcal{B}}_k \hat{\boldsymbol{x}}_k^u - \bar{\boldsymbol{c}}_k)) \\
&= \tilde{\boldsymbol{x}}_k^u + \boldsymbol{\gamma}_k^x(\bar{\mathcal{B}}_k \hat{\boldsymbol{x}}_k^u - \bar{\boldsymbol{c}}_k) \\
&= \tilde{\boldsymbol{x}}_k^u + \boldsymbol{\gamma}_k^x(\bar{\mathcal{B}}_k \hat{\boldsymbol{x}}_k^u - \bar{\mathcal{B}}_k \hat{\boldsymbol{x}}_k) \\
&= \tilde{\boldsymbol{x}}_k^u - \boldsymbol{\gamma}_k^x(\bar{\mathcal{B}}_k \tilde{\boldsymbol{x}}_k^u - \bar{\mathcal{B}}_k \tilde{\boldsymbol{x}}_k),
\end{aligned}$$

which implies Equation (3.29). The solution of $\bar{\mathcal{B}}_k \boldsymbol{x} \leq \bar{\boldsymbol{c}}_k$ defines a closed convex set $\mathcal{C}_k$. The point $\hat{\boldsymbol{x}}_k^u$ is not an element of the convex set. The point $\hat{\boldsymbol{x}}_k$ has the minimum distance from $\hat{\boldsymbol{x}}_k^u$ with metric $d(a,b) \triangleq \|a-b\|_{\boldsymbol{W}_k^x}$ in the convex set $\mathcal{C}_k$ by Equation (3.23). Since the solution $\hat{\boldsymbol{x}}_k$ is in the closed set $\mathcal{C}_k$, and $\boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k$ is a weighted projection with weight $\boldsymbol{W}_k^x$, the relationship Equation (3.30) holds. The statements for attack estimation errors can be proven by a similar procedure, which is omitted here. □

With the results from Lemma 3.1, we can show that the projection reduces the estimation errors and the error covariances, as formulated in Theorem 3.1.

Theorem 3.1 *CARE reduces the state and attack estimation errors and their error covariances from the unconstrained algorithm, i.e.,* $\|\tilde{\boldsymbol{x}}_k\| \leq \|\tilde{\boldsymbol{x}}_k^u\|$ *and* $\|\tilde{\boldsymbol{d}}_k\| \leq \|\tilde{\boldsymbol{d}}_k^u\|$, $\boldsymbol{P}_k^x \leq \boldsymbol{P}_k^{x,u}$ *and* $\boldsymbol{P}_k^d \leq \boldsymbol{P}_k^{d,u}$. *Strict inequality holds if* $rank(\bar{\mathcal{B}}_k) \neq 0$, *and* $rank(\bar{\mathcal{A}}_k) \neq 0$, *respectively.*

Proof: The statement for $\|\tilde{\boldsymbol{x}}_k\| \leq \|\tilde{\boldsymbol{x}}_k^u\|$ is the direct result of Lemma 3.1, where strict inequality holds if $\boldsymbol{\alpha}_k^i \neq 0$ for some i. The statement for $\|\tilde{\boldsymbol{d}}_k\| \leq \|\tilde{\boldsymbol{d}}_k^u\|$ can be proved by a similar procedure. To show the rest of the properties, we first identify the equality

$$(\boldsymbol{I} - \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k)^\top \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k = 0. \tag{3.31}$$

Since we have $\bar{\mathcal{B}}_k \boldsymbol{\gamma}_k^x = \boldsymbol{I}$ by Equation (3.24), it holds that $\boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k \boldsymbol{\gamma}_k^x = \boldsymbol{\gamma}_k^x$, and $\bar{\mathcal{B}}_k \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k = \bar{\mathcal{B}}_k$, i.e. $\boldsymbol{\gamma}_k^x = \bar{\mathcal{B}}_k^\dagger$. Then, we have $\bar{\mathcal{B}}_k^\top (\boldsymbol{\gamma}_k^x)^\top \boldsymbol{\gamma}_k^x = \boldsymbol{\gamma}_k^x$, which implies $\tilde{\boldsymbol{x}}_k^\top (\boldsymbol{I} - \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k)^\top \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k \tilde{\boldsymbol{x}}_k = \tilde{\boldsymbol{x}}_k^\top (\boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k - \bar{\mathcal{B}}_k^\top (\boldsymbol{\gamma}_k^x)^\top \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k) \hat{\boldsymbol{x}}_k = 0$. Notice that Equation (3.31) holds for $(\tilde{\boldsymbol{x}}_k^u)^\top (\boldsymbol{I} - \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k)^\top \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k \tilde{\boldsymbol{x}}_k^u = 0$ as well. Similar to Equation (3.21), we have $\boldsymbol{P}_k^x = (\boldsymbol{I} - \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k) \boldsymbol{P}_k^{x,u} = \boldsymbol{P}_k^{x,u} - \boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k \boldsymbol{P}_k^{x,u}$. Given that $\boldsymbol{\gamma}_k^x \bar{\mathcal{B}}_k \boldsymbol{P}_k^{x,u} = \boldsymbol{P}_k^{x,u} \bar{\mathcal{B}}_k^\top (\bar{\mathcal{B}}_k \boldsymbol{P}_k^{x,u} \bar{\mathcal{B}}_k^\top)^{-1} \bar{\mathcal{B}}_k \boldsymbol{P}_k^{x,u} > 0$ is positive definite, we have the desired result $\boldsymbol{P}_k^x < \boldsymbol{P}_k^{x,u}$. The relation for $\boldsymbol{P}_k^d$ can be obtained by a similar procedure. □

The properties in Theorem 3.1 are desired for accurate estimation as well as attack detection.

Detection Performance

More specifically, since the false negative rate of a χ^2 attack detector (see Appendix A) is a function of the estimate $\hat{\boldsymbol{\sigma}}_k$ and the covariance $\boldsymbol{\Sigma}_k$ as in Equation (A.1), more accurate estimations can reduce the false negative rate under the following assumption.

Assumption 3.1 *In the presence of the attack ($\boldsymbol{d}_k \neq 0$), the following two conditions hold: (i) $\|\tilde{\boldsymbol{d}}_k^u\| < \frac{1}{2}\|\boldsymbol{d}_k\|$, and (ii) the ground truth $\boldsymbol{d}_k$ satisfies the condition $\boldsymbol{d}_k^\top (\boldsymbol{P}_k^{d,u})^{-1} \boldsymbol{d}_k > \chi_{df}^2(\alpha)$.*

Remark 3.3 *Assumption 3.1 implies that the unconstrained attack estimation error $\tilde{\boldsymbol{d}}_k^u$ is small with respect to the ground truth $\boldsymbol{d}_k$, and the normalized ground truth attack signal is larger than $\chi_{df}^2(\alpha)$; otherwise, it cannot be distinguished from the noise. Notice that Assumption 3.1 is only considered for smaller false negative rates (Theorem 3.2), but not for the estimation performance (Theorem 3.1) and stability analysis, where we will show the stability*

of the attack estimation error $\tilde{\boldsymbol{d}}_k$ *(Theorem 3.4) which renders the stability of* $\tilde{\boldsymbol{d}}_k^u$.

According to Equation (A.1), we denote the false negative rates of the proposed `CARE` and the unconstrained algorithm as $F_{neg}(\{\hat{\boldsymbol{d}}_k\}, \{\boldsymbol{P}_k^d\})$ and $F_{neg}(\{\hat{\boldsymbol{d}}_k^u\}, \{\boldsymbol{P}_k^{d,u}\})$, respectively. The following Theorem 3.2 demonstrates that the false negative rate of `CARE` is less or equal to that of the unconstrained algorithm.

Theorem 3.2 *Under Assumption 3.1, given a set of attack vectors* $\{\boldsymbol{d}_k\}$*, the following inequality holds*

$$F_{neg}(\{\hat{\boldsymbol{d}}_k\}, \{\boldsymbol{P}_k^d\}) \leq F_{neg}(\{\hat{\boldsymbol{d}}_k^u\}, \{\boldsymbol{P}_k^{d,u}\}). \tag{3.32}$$

Proof: The proof of Equation (3.32) is equivalent to showing that the number of false negative test results of `CARE` is less or equal to that of the unconstrained algorithm

$$\sum_k (\mathbf{1}_k) \leq \sum_k (\mathbf{1}_k^u). \tag{3.33}$$

If there is no projection ($\boldsymbol{\gamma}_k^d = 0$), it holds that $\hat{\boldsymbol{d}}_k = \hat{\boldsymbol{d}}_k^u$ and $\boldsymbol{P}_k^d = \boldsymbol{P}_k^{d,u}$. And, if there is no attack ($\boldsymbol{d}_k = 0$), it holds that $\mathbf{1}_k = \mathbf{1}_k^u = 0$. Therefore, we have

$$\sum_{k \in \mathcal{K}_0} (\mathbf{1}_k) = \sum_{k \in \mathcal{K}_0} (\mathbf{1}_k^u), \tag{3.34}$$

where $\mathcal{K}_0 \triangleq \{k \mid \boldsymbol{\gamma}_k^d = 0 \ or \ \boldsymbol{d}_k = 0\}$. In the rest of the proof, we consider the case for $k \in \mathcal{K} \triangleq \{k \mid \boldsymbol{\gamma}_k^d \neq 0 \ and \ \boldsymbol{d}_k \neq 0\}$. Rewriting the normalized test value from `CARE` by substituting $\boldsymbol{P}_k^d$ with $(\boldsymbol{I} - \boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k)\boldsymbol{P}_k^{d,u}(\boldsymbol{I} - \boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k)^\top$

according to Equation (3.20), we have the following:

$$\begin{aligned}
\hat{\boldsymbol{d}}_k^\top(\boldsymbol{P}_k^d)^{-1}\hat{\boldsymbol{d}}_k &= \hat{\boldsymbol{d}}_k^\top\big((\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)\boldsymbol{P}_k^{d,u}(\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)^\top\big)^{-1}\hat{\boldsymbol{d}}_k \\
&=\big((\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)^{-1}\hat{\boldsymbol{d}}_k\big)^\top(\boldsymbol{P}_k^{d,u})^{-1}\big((\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)^{-1}\hat{\boldsymbol{d}}_k\big) \\
&=\big(\hat{\boldsymbol{d}}_k^u+(\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)^{-1}\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k\big)^\top(\boldsymbol{P}_k^{d,u})^{-1} \\
&\quad\times\big(\hat{\boldsymbol{d}}_k^u+(\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)^{-1}\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k\big),
\end{aligned} \tag{3.35}$$

where $(\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)^{-1}\hat{\boldsymbol{d}}_k=\hat{\boldsymbol{d}}_k^u+(\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)^{-1}\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k$ has been applied. Now we expand and rearrange Equation (3.35), resulting in the following:

$$\begin{aligned}
&\hat{\boldsymbol{d}}_k^\top(\boldsymbol{P}_k^d)^{-1}\hat{\boldsymbol{d}}_k=(\hat{\boldsymbol{d}}_k^u)^\top(\boldsymbol{P}_k^{d,u})^{-1}\hat{\boldsymbol{d}}_k^u \\
&+\big((\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)^{-1}\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k\big)^\top(\boldsymbol{P}_k^{d,u})^{-1}\big((\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)^{-1}\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k\big) \\
&+2(\hat{\boldsymbol{d}}_k^u)^\top(\boldsymbol{P}_k^{d,u})^{-1}\big((\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)^{-1}\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k\big) \\
&=(\hat{\boldsymbol{d}}_k^u)^\top(\boldsymbol{P}_k^{d,u})^{-1}\hat{\boldsymbol{d}}_k^u \\
&+\big(\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k\big)^\top\big((\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)\boldsymbol{P}_k^{d,u}(\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)^\top\big)^{-1}\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k \\
&+2(\hat{\boldsymbol{d}}_k^u)^\top\big((\boldsymbol{I}-\boldsymbol{\gamma}_k^d\bar{\mathcal{A}}_k)\boldsymbol{P}_k^{d,u}\big)^{-1}\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k.
\end{aligned} \tag{3.36}$$

Applying Equation (3.20) and Equation (3.21) to Equation (3.36), we have

$$\begin{aligned}
\hat{\boldsymbol{d}}_k^\top(\boldsymbol{P}_k^d)^{-1}\hat{\boldsymbol{d}}_k &= (\hat{\boldsymbol{d}}_k^u)^\top(\boldsymbol{P}_k^{d,u})^{-1}\hat{\boldsymbol{d}}_k^u \\
&+\underbrace{\big(\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k\big)^\top(\boldsymbol{P}_k^d)^{-1}\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k+2(\hat{\boldsymbol{d}}_k^u)^\top(\boldsymbol{P}_k^d)^{-1}\boldsymbol{\gamma}_k^d\bar{\boldsymbol{b}}_k}_{\triangleq\ residue\ (res.)}.
\end{aligned} \tag{3.37}$$

Since $\hat{\boldsymbol{d}}_k$ satisfies the input active constraint, we can substitute $\bar{\boldsymbol{b}}_k$ with $\bar{\mathcal{A}}_k\hat{\boldsymbol{d}}_k$.

Then the residue defined in Equation (3.37) can be written as follows:

$$\begin{aligned} res. = &\left(\boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k \hat{\boldsymbol{d}}_k\right)^\top (\boldsymbol{P}_k^d)^{-1} \boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k \hat{\boldsymbol{d}}_k \\ &+ 2(\hat{\boldsymbol{d}}_k^u)^\top (\boldsymbol{P}_k^d)^{-1} \boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k \hat{\boldsymbol{d}}_k. \end{aligned} \tag{3.38}$$

Expanding and rearranging Equation (3.38), we have the following:

$$res. = 2\boldsymbol{d}_k^\top \boldsymbol{P}_k' \boldsymbol{d}_k - 2\tilde{\boldsymbol{d}}_k^\top \boldsymbol{P}_k' \boldsymbol{d}_k - 2(\tilde{\boldsymbol{d}}_k^u)^\top \boldsymbol{P}_k' \boldsymbol{d}_k \tag{3.39}$$

$$+ 2\tilde{\boldsymbol{d}}_k^\top \boldsymbol{P}_k' \tilde{\boldsymbol{d}}_k + \|\boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k\|^2 \tilde{\boldsymbol{d}}_k^\top (\boldsymbol{P}_k^d)^{-1} \tilde{\boldsymbol{d}}_k \tag{3.40}$$

$$+ \|\boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k\|^2 \boldsymbol{d}_k^\top (\boldsymbol{P}_k^d)^{-1} \boldsymbol{d}_k - 2\|\boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k\|^2 \boldsymbol{d}_k^\top (\boldsymbol{P}_k^d)^{-1} \tilde{\boldsymbol{d}}_k, \tag{3.41}$$

where $\boldsymbol{P}_k' \triangleq (\boldsymbol{\gamma}_k^d \bar{\mathcal{A}}_k)^\top (\boldsymbol{P}_k^d)^{-1} > 0$. Using the result $\|\tilde{\boldsymbol{d}}_k\| < \|\tilde{\boldsymbol{d}}_k^u\|$ from Theorem 3.1 and the first inequality in Assumption 3.1, we obtain $\|\tilde{\boldsymbol{d}}\| < \|\tilde{\boldsymbol{d}}^u\| < \frac{1}{2}\|\boldsymbol{d}\|$. Then we have $res. > 0$, since expressions in Equation (3.39) to Equation (3.41) are positive, respectively. Therefore, from Equation (3.37), we have

$$(\hat{\boldsymbol{d}}_k^u)^\top (\boldsymbol{P}_k^{d,u})^{-1} \hat{\boldsymbol{d}}_k^u < \hat{\boldsymbol{d}}_k^\top (\boldsymbol{P}_k^d)^{-1} \hat{\boldsymbol{d}}_k. \tag{3.42}$$

Considering the condition in Equation (3.42), we can divide the set $\mathcal{K} = \cup_{i=1}^3 \mathcal{K}_i$ into three partitions as follows:

$$\begin{aligned} \mathcal{K}_1 &\triangleq \left\{k \mid (\hat{\boldsymbol{d}}_k^u)^\top (\boldsymbol{P}_k^{d,u})^{-1} \hat{\boldsymbol{d}}_k^u < \hat{\boldsymbol{d}}_k^\top (\boldsymbol{P}_k^d)^{-1} \hat{\boldsymbol{d}}_k \le \chi_{df}^2(\alpha)\right\} \\ \mathcal{K}_2 &\triangleq \left\{k \mid \chi_{df}^2(\alpha) < (\hat{\boldsymbol{d}}_k^u)^\top (\boldsymbol{P}_k^{d,u})^{-1} \hat{\boldsymbol{d}}_k^u < \hat{\boldsymbol{d}}_k^\top (\boldsymbol{P}_k^d)^{-1} \hat{\boldsymbol{d}}_k\right\} \\ \mathcal{K}_3 &\triangleq \left\{k \mid (\hat{\boldsymbol{d}}_k^u)^\top (\boldsymbol{P}_k^{d,u})^{-1} \hat{\boldsymbol{d}}_k^u \le \chi_{df}^2(\alpha) < \hat{\boldsymbol{d}}_k^\top (\boldsymbol{P}_k^d)^{-1} \hat{\boldsymbol{d}}_k\right\}. \end{aligned}$$

According to Equation (A.2), we have

$$\sum_{k\in\mathcal{K}_i}(\mathbf{1}_k) = \sum_{k\in\mathcal{K}_i}(\mathbf{1}_k^u) \text{ for } i = 1, 2 \text{ and} \tag{3.43}$$

$$\sum_{k\in\mathcal{K}_3}(\mathbf{1}_k) < \sum_{k\in\mathcal{K}_3}(\mathbf{1}_k^u). \tag{3.44}$$

Therefore, from Equation (3.34), Equation (3.43) and Equation (3.44) we conclude that Equation (3.33) holds, which completes the proof. □

Stability Analysis

Although the projection reduces the estimation errors and their error covariances as shown in Theorem 3.1, it trades the unbiased estimation off according to Equation (3.26) and Equation (3.27). In the absence of the projection, Algorithm 2 reduces to the algorithm in [61], which is an unbiased estimation, while the traditional stability analysis for unbiased estimation becomes invalid after the projection is applied.

To prove the recursive stability of the biased estimation, it is essential to construct a recursive relation between the current estimation error $\tilde{\boldsymbol{x}}_k$ and the previous estimation error $\tilde{\boldsymbol{x}}_{k-1}$. However, the construction is not straightforward compared to that in filtering with equality constraints [25, 31] or filtering without constraints [65, 61]. Especially, it is difficult to find the exact recursive relation between $\tilde{\boldsymbol{x}}_k$ and $\tilde{\boldsymbol{x}}_k^u$, since $\tilde{\boldsymbol{x}}_k$ is also a function of $\hat{\boldsymbol{x}}_k^u$, i.e. $\tilde{\boldsymbol{x}}_k = \tilde{\boldsymbol{x}}_k^u - \boldsymbol{\gamma}_k^x(\bar{\mathcal{B}}_k\hat{\boldsymbol{x}}_k^u - \bar{\boldsymbol{c}}_k)$. Then, we have $\tilde{\boldsymbol{x}}_k \neq (\boldsymbol{I} - \boldsymbol{\gamma}_k^x\bar{\mathcal{B}}_k)\tilde{\boldsymbol{x}}_k^u$, since the inequality $\bar{\mathcal{B}}_k\boldsymbol{x}_k \leq \bar{\boldsymbol{c}}_k$ holds. To address this issue, we decompose the estimation error $\tilde{\boldsymbol{x}}_k$ into two orthogonal spaces as in Equation (3.28). By Lemma 3.1, Equation (3.28) becomes $\tilde{\boldsymbol{x}}_k = \boldsymbol{\Gamma}_k\tilde{\boldsymbol{x}}_k^u$, where $\boldsymbol{\Gamma}_k \triangleq (\boldsymbol{I} - \boldsymbol{\gamma}_k^x\bar{\mathcal{B}}_k) + \boldsymbol{\alpha}_k\boldsymbol{\gamma}_k^x\bar{\mathcal{B}}_k$. Note that $\boldsymbol{\alpha}_k$ is an unknown matrix and thus cannot be used for the

algorithm. We use it only for analytical purposes. Now under the following assumptions, we present the stability analysis of the proposed Algorithm 2.

Assumption 3.2 *We have rank*$(\mathcal{B}_k) < n\ \forall k$. *There exist* $\bar{a}$, $\bar{c}_y$, $\bar{g}$, $\bar{m}$, $\underline{q}$, $\underline{\beta}$, $\bar{\beta} > 0$, *such that the following holds for all* $k \geq 0$*:*

$$\|\boldsymbol{A}_k\| \leq \bar{a}, \qquad \|\boldsymbol{C}_k\| \leq \bar{c}_y, \qquad \|\boldsymbol{G}_k\| \leq \bar{g},$$
$$\|\boldsymbol{M}_k\| \leq \bar{m}, \qquad \boldsymbol{Q}_k \geq \underline{q}\boldsymbol{I}.$$

Remark 3.4 *In Assumption 3.2, it is assumed that rank*$(\mathcal{B}_k) < n\ \forall k$, *i.e., the number of the state constraints are less than the number of state variables. The rest of Assumption 3.2 is widely used in the literature on extended Kalman filtering [66] and nonlinear input and state estimation [62].*

To show the boundedness of the unconstrained state error covariance $\boldsymbol{P}_k^{x,u}$, we first define the matrices $\bar{\boldsymbol{A}}_{k-1} \triangleq (\boldsymbol{I} - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{C}_k)\boldsymbol{A}_{k-1}$ and $\tilde{\boldsymbol{A}}_{k-1} \triangleq (\boldsymbol{I} - \boldsymbol{G}_{k-1}\boldsymbol{M}_k(\boldsymbol{C}_k\boldsymbol{G}_{k-1}\boldsymbol{M}_k)^{-1}\boldsymbol{C}_k)\bar{\boldsymbol{A}}_{k-1}\bar{\boldsymbol{\Gamma}}_{k-1}$.

Theorem 3.3 *Let the pair* $(\boldsymbol{C}_k, \tilde{\boldsymbol{A}}_{k-1})$ *be uniformly detectable*[2], *then the unconstrained state error covariance* $\boldsymbol{P}_k^{x,u}$ *is bounded, i.e., there exist non-negative constants* $\underline{p}$ *and* $\bar{p}$ *such that* $\underline{p}\boldsymbol{I} \leq \boldsymbol{P}_k^{x,u} \leq \bar{p}\boldsymbol{I}$ *for all* k.

Proof:

The unconstrained state estimation error can be found by

$$\begin{aligned}\tilde{\boldsymbol{x}}_k^u =& (\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)\bar{\boldsymbol{A}}_{k-1}\tilde{\boldsymbol{x}}_{k-1} \\ &+ (\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)\bar{\boldsymbol{w}}_{k-1} + \bar{\boldsymbol{L}}_k\boldsymbol{v}_k,\end{aligned} \tag{3.45}$$

where $\bar{\boldsymbol{w}}_{k-1} \triangleq (\boldsymbol{I} - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{C}_k)\boldsymbol{w}_{k-1}$, and $\bar{\boldsymbol{L}}_k \triangleq \boldsymbol{L}_k\boldsymbol{C}_k\boldsymbol{G}_{k-1}\boldsymbol{M}_k - \boldsymbol{L}_k -$

[2]Please refer to [65] for the definition of uniform detectability.

$\boldsymbol{G}_{k-1}\boldsymbol{M}_k$. Therefore, the update law of unconstrained covariance is calculated from Equation (3.45) and Equation (3.25) as follows:

$$\begin{aligned}\boldsymbol{P}_k^{x,u} =&(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)\bar{\boldsymbol{A}}_{k-1}\bar{\boldsymbol{\Gamma}}_{k-1}\boldsymbol{P}_{k-1}^{x,u}\bar{\boldsymbol{\Gamma}}_{k-1}^\top\\ &\times\bar{\boldsymbol{A}}_{k-1}^\top(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top+\bar{\boldsymbol{L}}_k\boldsymbol{R}_k\bar{\boldsymbol{L}}_k^\top\\ &+(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)\bar{\boldsymbol{Q}}_{k-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top,\end{aligned}\tag{3.46}$$

where $\bar{\boldsymbol{Q}}_{k-1}\triangleq\mathbb{E}[\bar{\boldsymbol{w}}_{k-1}(\bar{\boldsymbol{w}}_{k-1})^\top]$. The covariance update law Equation (3.46) is identical to the covariance update law of the Kalman filtering solution of the transformed system

$$\begin{aligned}\boldsymbol{x}_k&=\bar{\boldsymbol{A}}_{k-1}\bar{\boldsymbol{\Gamma}}_{k-1}\boldsymbol{x}_{k-1}+\hat{\boldsymbol{w}}_{k-1}\\ \boldsymbol{y}_k&=\boldsymbol{C}_k\boldsymbol{x}_k+\boldsymbol{v}_k,\end{aligned}\tag{3.47}$$

where $\hat{\boldsymbol{w}}_{k-1}\triangleq-\boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{C}_k\boldsymbol{w}_{k-1}-\boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{v}_k+\boldsymbol{w}_{k-1}$. However, in the transformed system, the process noise and measurement noise are correlated, i.e., $\mathbb{E}[\hat{\boldsymbol{w}}_{k-1}\boldsymbol{v}_k^\top]=-\boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{R}_k\neq 0$. To decouple the noises, we add a zero term $\boldsymbol{Z}_k(\boldsymbol{y}_k-\boldsymbol{C}_k(\bar{\boldsymbol{A}}_{k-1}\bar{\boldsymbol{\Gamma}}_{k-1}\boldsymbol{x}_k+\hat{\boldsymbol{w}}_{k-1})-\boldsymbol{v}_k)$ to the state equation in Equation (3.47), and obtain the following:

$$\boldsymbol{x}_k=\tilde{\boldsymbol{A}}_{k-1}\boldsymbol{x}_{k-1}+\tilde{\boldsymbol{u}}_{k-1}+\tilde{\boldsymbol{w}}_{k-1},$$

where $\tilde{\boldsymbol{A}}_{k-1}=(\boldsymbol{I}-\boldsymbol{Z}_k\boldsymbol{C}_k)\bar{\boldsymbol{A}}_{k-1}\bar{\boldsymbol{\Gamma}}_{k-1}$, $\tilde{\boldsymbol{u}}_{k-1}\triangleq\boldsymbol{Z}_k\boldsymbol{y}_k$ is the known input, and $\tilde{\boldsymbol{w}}_{k-1}\triangleq(\boldsymbol{I}-\boldsymbol{Z}_k\boldsymbol{C}_k)\hat{\boldsymbol{w}}_{k-1}-\boldsymbol{Z}_k\boldsymbol{v}_k$ is the new process noise. The new process noise and the measurement noise could be decoupled by choosing the gain $\boldsymbol{Z}_k$ such that $\mathbb{E}[\tilde{\boldsymbol{w}}_{k-1}\boldsymbol{v}_k^\top]=0$. The solution can be found by $\boldsymbol{Z}_k=$

$\boldsymbol{G}_{k-1}\boldsymbol{M}_k(\boldsymbol{C}_k\boldsymbol{G}_{k-1}\boldsymbol{M}_k)^{-1}$. Then, the system Equation (3.47) becomes

$$\begin{aligned}\boldsymbol{x}_k &= \tilde{\boldsymbol{A}}_{k-1}\boldsymbol{x}_{k-1} + \tilde{\boldsymbol{u}}_{k-1} + \tilde{\boldsymbol{w}}_{k-1}\\ \boldsymbol{y}_k &= \boldsymbol{C}_k\boldsymbol{x}_k + \boldsymbol{v}_k.\end{aligned}$$

Since the pair $(\boldsymbol{C}_k, \tilde{\boldsymbol{A}}_{k-1})$ is uniformly detectable, by Theorem 5.2 in [65], the statement holds. □

Theorem 3.3 shows that the uniform detectability of the transformed system is one of the sufficient conditions of boundedness of $\boldsymbol{P}_k^{x,u}$. Under the assumption of boundedness of $\boldsymbol{P}_k^{x,u}$ from Theorem 3.3, we show that the constrained estimation errors $\tilde{\boldsymbol{x}}_k$ and $\tilde{\boldsymbol{d}}_k$ are practically exponentially stable in mean square as in Theorem 3.4.

Theorem 3.4 *Consider Assumption 3.2 and assume that there exist non-negative constants $\underline{p}$ and $\bar{p}$ such that $\underline{p}\boldsymbol{I} \leq \boldsymbol{P}_k^{x,u} \leq \bar{p}\boldsymbol{I}$ holds for all k. Then the estimation errors $\tilde{\boldsymbol{x}}_k$ and $\tilde{\boldsymbol{d}}_k$ are practically exponentially stable in mean square, i.e., there exist constants $a_x, a_d, b_x, b_d, c_x, c_d$ such that for all k*

$$\begin{aligned}\mathbb{E}[\|\tilde{\boldsymbol{x}}_k\|^2] &\leq a_x e^{-b_x k}\mathbb{E}[\|\tilde{\boldsymbol{x}}_0\|^2] + c_x\\ \mathbb{E}[\|\tilde{\boldsymbol{d}}_k\|^2] &\leq a_d e^{-b_d k}\mathbb{E}[\|\tilde{\boldsymbol{d}}_0\|^2] + c_d.\end{aligned}$$

Proof:

Consider the Lyapunov function $V_k = (\tilde{\boldsymbol{x}}_k^u)^\top(\boldsymbol{P}_k^{x,u})^{-1}(\tilde{\boldsymbol{x}}_k^u)$. After substi-

tuting Equation (3.45) into the Lyapunov function, we obtain

$$
\begin{aligned}
V_k =&(\tilde{\boldsymbol{x}}^u_{k-1})^\top \boldsymbol{\Gamma}^\top_{k-1}\bar{\boldsymbol{A}}^\top_{k-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top(\boldsymbol{P}^{x,u}_k)^{-1}\\
&\times(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)\bar{\boldsymbol{A}}_{k-1}\boldsymbol{\Gamma}_{k-1}\tilde{\boldsymbol{x}}^u_{k-1}\\
&+2(\tilde{\boldsymbol{x}}^u_{k-1})^\top \boldsymbol{\Gamma}^\top_{k-1}\bar{\boldsymbol{A}}^\top_{k-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top\\
&\times(\boldsymbol{P}^{x,u}_k)^{-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)\bar{\boldsymbol{w}}_{k-1}\\
&+2(\tilde{\boldsymbol{x}}^u_{k-1})^\top \boldsymbol{\Gamma}^\top_{k-1}\bar{\boldsymbol{A}}^\top_{k-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top(\boldsymbol{P}^{x,u}_k)^{-1}\bar{\boldsymbol{L}}_k\boldsymbol{v}_k\\
&+\bar{\boldsymbol{w}}^\top_{k-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top(\boldsymbol{P}^{x,u}_k)^{-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)\bar{\boldsymbol{w}}_{k-1}\\
&+2\boldsymbol{w}^\top_{k-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top(\boldsymbol{P}^{x,u}_k)^{-1}\bar{\boldsymbol{L}}_k\boldsymbol{v}_k\\
&+\boldsymbol{v}^\top_k\bar{\boldsymbol{L}}_k(\boldsymbol{P}^{x,u}_k)^{-1}\bar{\boldsymbol{L}}_k\boldsymbol{v}_k. \qquad (3.48)
\end{aligned}
$$

By the uncorrelatedness property [67] of $\boldsymbol{w}_{k-1}$, $\boldsymbol{v}_k$ and $\tilde{\boldsymbol{x}}^u_{k-1}$, the Lyapunov function Equation (3.48) becomes

$$
\begin{aligned}
\mathbb{E}[V_k] =& \mathbb{E}[(\tilde{\boldsymbol{x}}^u_{k-1})^\top \boldsymbol{\Gamma}^\top_{k-1}\bar{\boldsymbol{A}}^\top_{k-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top(\boldsymbol{P}^{x,u}_k)^{-1}\\
&\times\bar{\boldsymbol{A}}_{k-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)\boldsymbol{\Gamma}_{k-1}(\tilde{\boldsymbol{x}}^u_{k-1})]\\
&+\mathbb{E}[\bar{\boldsymbol{w}}^\top_{k-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top(\boldsymbol{P}^{x,u}_k)^{-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)\bar{\boldsymbol{w}}_{k-1}]\\
&+\mathbb{E}[\boldsymbol{v}^\top_k\bar{\boldsymbol{L}}_k(\boldsymbol{P}^{x,u}_k)^{-1}\bar{\boldsymbol{L}}_k\boldsymbol{v}_k]. \qquad (3.49)
\end{aligned}
$$

The following statements are formulated to deal with each term in Equation (3.49).

Claim 3.1 There exists a constant $\delta \triangleq (\frac{q'}{\bar{a}'^2\bar{p}}+1)^{-1} \in (0,1)$, *such that* $\boldsymbol{\Gamma}^\top_{k-1}\bar{\boldsymbol{A}}^\top_{k-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top(\boldsymbol{P}^{x,u}_k)^{-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)\bar{\boldsymbol{A}}_{k-1}\boldsymbol{\Gamma}_{k-1} < \delta(\boldsymbol{P}^{x,u}_{k-1})^{-1}$.

Proof: Since $rank(\mathcal{B}_k) < n\ \forall k$, *it holds that* $rank(\bar{\mathcal{B}}_k) < n\ \forall k$ *and thus* $\bar{\boldsymbol{\Gamma}} \neq 0$. *Therefore,* $\|\bar{\boldsymbol{\Gamma}}_{k-1}\| = 1$ *because* $\boldsymbol{\gamma}^x_{k-1}\bar{\mathcal{B}}_{k-1}$ *is a projection matrix. From Assumption 3.2 and Theorem 3.3, we have* $\bar{\boldsymbol{Q}}_{k-1} \geq \underline{q}'\boldsymbol{I}$, *and* $\boldsymbol{P}^x_{k-1} \leq \bar{p}\boldsymbol{I}$. *Since*

$\|\bar{\boldsymbol{A}}_{k-1}\|$ *is upper bounded by* $\bar{a}' \triangleq \bar{a}(1+\bar{g}\bar{m}\bar{c}_y)$*, we can have* $\bar{\boldsymbol{A}}_{k-1}\bar{\boldsymbol{A}}_{k-1}^\top \leq \bar{a}'^2\boldsymbol{I}$*. Then we have*

$$\begin{aligned}\bar{\boldsymbol{Q}}_{k-1} &\geq \underline{q}'\frac{\bar{\boldsymbol{A}}_{k-1}\bar{\boldsymbol{A}}_{k-1}^\top}{\bar{a}'^2} \geq \frac{\underline{q}'}{\bar{a}'^2}\bar{\boldsymbol{A}}_{k-1}\bar{\boldsymbol{\Gamma}}_{k-1}\bar{\boldsymbol{\Gamma}}_{k-1}^\top\bar{\boldsymbol{A}}_{k-1}^\top \\ &\geq \frac{\underline{q}'}{\bar{a}'^2\bar{p}}\bar{\boldsymbol{A}}_{k-1}\bar{\boldsymbol{\Gamma}}_{k-1}\boldsymbol{P}_{k-1}^{x,u}\bar{\boldsymbol{\Gamma}}_{k-1}^\top\bar{\boldsymbol{A}}_{k-1}^\top. \end{aligned} \tag{3.50}$$

Substitution of Equation (3.50) into Equation (3.46) yields

$$\begin{aligned}&\boldsymbol{P}_k^{x,u} - (1+\frac{\underline{q}'}{\bar{a}'^2\bar{p}})(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)\bar{\boldsymbol{A}}_{k-1}\bar{\boldsymbol{\Gamma}}_{k-1}\boldsymbol{P}_{k-1}^{x,u}\bar{\boldsymbol{\Gamma}}_{k-1}^\top\bar{\boldsymbol{A}}_{k-1}^\top \\ &\times(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top > 0, \end{aligned} \tag{3.51}$$

where the inequality holds because $\boldsymbol{R}_k > 0$*. As* $(1+\frac{\underline{q}'}{\bar{a}'^2\bar{p}})\boldsymbol{P}_{k-1}^{x,u} > 0$*, the inverse of the left hand side of Equation (3.51) exists and is symmetric positive definite. By the matrix inversion lemma [68], it follows that*

$$\begin{aligned}&(1+\frac{\underline{q}'}{\bar{a}'^2\bar{p}})^{-1}(\boldsymbol{P}_{k-1}^{x,u})^{-1} - \bar{\boldsymbol{\Gamma}}_{k-1}^\top\bar{\boldsymbol{A}}_{k-1}^\top(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)^\top \\ &\times(\boldsymbol{P}_k^{x,u})^{-1}(\boldsymbol{I}-\boldsymbol{L}_k\boldsymbol{C}_k)\bar{\boldsymbol{A}}_{k-1}\bar{\boldsymbol{\Gamma}}_{k-1} > 0. \end{aligned} \tag{3.52}$$

Since $\boldsymbol{\gamma}_{k-1}^x\bar{\mathcal{B}}_{k-1}$ *is a positive definite matrix, and* $\|\boldsymbol{\alpha}_{k-1}\| \leq 1$*, we have*

$$\begin{aligned}\boldsymbol{I} - \boldsymbol{\gamma}_{k-1}^x\bar{\mathcal{B}}_{k-1} &\leq \boldsymbol{\Gamma}_{k-1} \\ &= \boldsymbol{I} - \boldsymbol{\gamma}_{k-1}^x\bar{\mathcal{B}}_{k-1} + \boldsymbol{\alpha}_{k-1}\boldsymbol{\gamma}_{k-1}^x\bar{\mathcal{B}}_{k-1} \leq \boldsymbol{I}, \end{aligned}$$

which implies $\|\boldsymbol{\Gamma}_{k-1}\| \leq 1$*. Since* $\|\bar{\boldsymbol{\Gamma}}_{k-1}\| = 1$ *and* $\|\boldsymbol{\Gamma}_{k-1}\| \leq 1$*, inequality Equation (3.52) proves the claim.* □

Claim 3.2 There exists a positive constant $c \triangleq \bar{p}(1+\bar{l}\bar{c}_y)^2(1+\bar{g}\bar{m}\bar{c}_2)^2\bar{q}$ *rank*$(\boldsymbol{Q}_{k-1})+$

$\bar{p}(\bar{l}\bar{c}_y\bar{g}\bar{m} - \bar{l} - \bar{g}\bar{m})^2\bar{r}_2 \ \ rank(\boldsymbol{R}_k)$, *such that*

$$\begin{aligned}\mathbb{E}[\|(\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)^\top(\boldsymbol{P}_k^{x,u})^{-1}(\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)\|\|\bar{\boldsymbol{w}}_{k-1}\|^2] \\ +\mathbb{E}[\|\bar{\boldsymbol{L}}_k(\boldsymbol{P}_k^{x,u})^{-1}\bar{\boldsymbol{L}}_k\|\|\boldsymbol{v}_k]\|^2] \leq c.\end{aligned}$$

Proof: The first term is bounded by

$$\begin{aligned}&\mathbb{E}[\|(\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)^\top(\boldsymbol{P}_k^{x,u})^{-1}(\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)\|\|\bar{\boldsymbol{w}}_{k-1}\|^2] \\ =&\mathbb{E}[\|(\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)^\top(\boldsymbol{P}_k^{x,u})^{-1}(\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)\| \\ &\|(\boldsymbol{I} - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{C}_k)\|^2\|\boldsymbol{w}_{k-1}\|^2] \\ &\leq \bar{p}(1 + \bar{l}\bar{c}_y)^2(1 + \bar{g}\bar{m}\bar{c}_2)^2\bar{q} \ \ rank(\boldsymbol{Q}_{k-1}),\end{aligned}$$

where we apply $\|\boldsymbol{w}_{k-1}\|^2 = tr(\boldsymbol{w}_{k-1}\boldsymbol{w}_{k-1}^\top) \leq \bar{q} \ \ rank(\boldsymbol{Q}_{k-1})$. *Likewise, the second term is bounded by*

$$\begin{aligned}&\mathbb{E}[\|\bar{\boldsymbol{L}}_k(\boldsymbol{P}_k^{x,u})^{-1}\bar{\boldsymbol{L}}_k\|\|\boldsymbol{v}_k]\|^2] \\ &\leq \bar{p}(\bar{l}\bar{c}_y\bar{g}\bar{m} + \bar{l} + \bar{g}\bar{m})^2\bar{r}_2 \ \ rank(\boldsymbol{R}_k).\end{aligned}$$

These complete the proof. □

Through Claims 3.1 and 3.2, Equation (3.49) becomes

$$\mathbb{E}[V_k] \leq \delta\mathbb{E}[V_{k-1}] + c.$$

By recursively applying the above relation, we have

$$\begin{aligned}\mathbb{E}[V_k] &\leq \delta^k \mathbb{E}[V_0] + \sum_{i=0}^{k-1} \delta^i c \leq \delta^k \mathbb{E}[V_0] + \sum_{i=0}^{\infty} \delta^i c \\ &= \delta^k \mathbb{E}[V_0] + \frac{c}{1-\delta},\end{aligned}$$

which implies practical exponential stability of the estimation error

$$\begin{aligned}\mathbb{E}[\|\tilde{\boldsymbol{x}}_k^u\|^2] &\leq \frac{\bar{p}}{\underline{p}} \delta^k \mathbb{E}[\|\tilde{\boldsymbol{x}}_0^u\|^2] + \frac{c\bar{p}}{(1-\delta)} \\ &= a'_x e^{-b'_x k} \mathbb{E}[\|\tilde{\boldsymbol{x}}_0^u\|^2] + c'_x,\end{aligned}$$

where $(\tilde{\boldsymbol{x}}_k^u)^\top (\boldsymbol{P}_k^x)^{-1} (\tilde{\boldsymbol{x}}_k^u) \geq \lambda_{\min}((\boldsymbol{P}_k^x)^{-1}) \|\tilde{\boldsymbol{x}}_k^u\|^2 \geq \frac{1}{\bar{p}} \|\tilde{\boldsymbol{x}}_k^u\|^2$ and $(\tilde{\boldsymbol{x}}_0^u)^\top (\boldsymbol{P}_0^x)^{-1} \tilde{\boldsymbol{x}}_0^u \leq \lambda_{\max}((\boldsymbol{P}_0^x)^{-1}) \|\tilde{\boldsymbol{x}}_0^u\|^2 \leq \frac{1}{\underline{p}} \|\tilde{\boldsymbol{x}}_0^u\|^2$ have been applied. Constants are defined by

$$a'_x \triangleq \frac{\bar{p}}{\underline{p}}, \qquad b'_x \triangleq \ln(1 + \frac{\underline{q}'}{\bar{h}^2 \bar{a}'^2 \bar{p}}) \qquad c'_x \triangleq \frac{c\bar{p}}{(1-\delta)}.$$

Since $\tilde{\boldsymbol{x}}_k$ is a linear transformation of $\tilde{\boldsymbol{x}}_k^u$, the same stability holds for $\tilde{\boldsymbol{x}}_k$. Likewise, the same stability holds for $\tilde{\boldsymbol{d}}_k$ in Equation (3.19) because it is a linear transformation of $\tilde{\boldsymbol{x}}_k$. We omit its details. □

3.4 Illustrative Example

In this example, we test Algorithm 2 on a vehicle model with input and state constraints and compare the estimation accuracy and the detection performance with an unconstrained algorithm.

Table 3.1: Performance comparison.

	$\sum_k \|\tilde{\boldsymbol{x}}_k\|$	$\sum_k \|\tilde{\boldsymbol{d}}_k\|$	$\sum_k \|\operatorname{tr}(\boldsymbol{P}_k^x)\|$	$\sum_k \|\operatorname{tr}(\boldsymbol{P}_k^d)\|$
`CARE`	88.928	672.914	0.455	27.351*
`ISE`	123.623	1041.837	0.613	40.577*

* *The summation ranges from $k = 100$ to $k = 1000$ due to the large initialization (10^4-scale), as shown in Figure 3.4.*

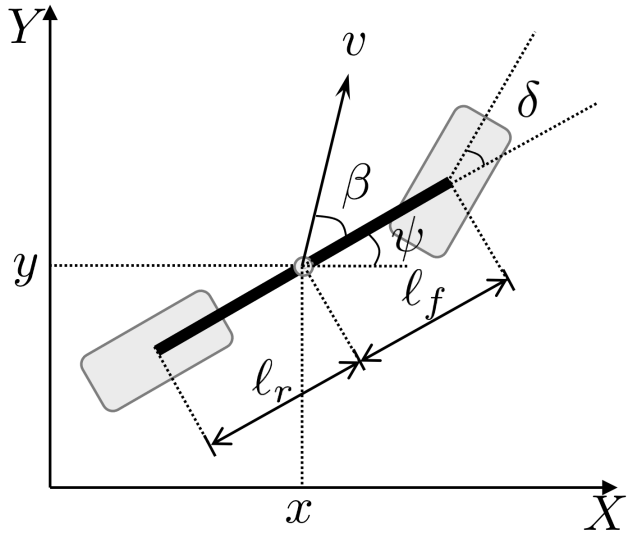


Figure 3.2: Kinematic Bicycle Model.

Experimental Setup

We consider a kinematic bicycle model (Figure 3.2) in [69]. The nonlinear continuous-time model is given as

$$\begin{aligned}
\dot{x} &= v\cos(\psi+\beta)\\
\dot{y} &= v\sin(\psi+\beta)\\
\dot{\psi} &= \frac{v}{l_r}\sin(\beta)\\
\dot{v} &= a\\
\beta &= \arctan\Big(\frac{l_r}{l_f+l_r}\tan(\delta)\Big),
\end{aligned}$$

where x and y are the coordinates of the center of mass, v is the velocity of the center of mass, β is the angle of the velocity v with respect to the longitudinal axis of the vehicle, a is the acceleration, ψ is the heading angle of the vehicle, δ is the steering angle of the front wheel, and l_f and l_r represent the distance from the center of mass of the vehicle to the front and rear axles, respectively.

Since the proposed algorithm is for linear discrete-time systems, we perform the linearization and discretization as in [70] with sampling time $T_s = 0.01s$. We rewrite the system in the form of Equation (3.1), where $\boldsymbol{x}_k = [x_k, y_k, \psi_k, v_k]^\top$ is the state vector, $\boldsymbol{u}_k = [\beta_k^u, a_k^u]^\top = \left[\arctan\left(\frac{l_r}{l_f+l_r}\tan(\delta_k^u)\right), a_k^u\right]^\top$ is the input vector, and $\boldsymbol{d}_k = [\beta_k^d, a_k^d]^\top = \left[\arctan\left(\frac{l_r}{l_f+l_r}\tan(\delta_k^d)\right), a_k^d\right]^\top$ is the attack input vector. We consider the scenario that attack input is injected into the input, i.e. $\boldsymbol{G}_k = \boldsymbol{B}_k$. The system matrices are given as follows:

$$\boldsymbol{A}_k = \begin{bmatrix} 1 & 0 & 0 & T_s \\ 0 & 1 & v_k T_s & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \boldsymbol{B}_k = \boldsymbol{G}_k = \begin{bmatrix} 0 & 0 \\ v_k T_s & 0 \\ \frac{v_k T_s}{l_r} & 0 \\ 0 & T_s \end{bmatrix},$$

and $\boldsymbol{C}_k = \boldsymbol{I}$. The noise covariances $\boldsymbol{Q}_k$ and $\boldsymbol{R}_k$ are considered as diagonal matrices with $\text{diag}(\boldsymbol{Q}_k) = [0.1, 0.1, 0.001, 0.0001]$ and $\text{diag}(\boldsymbol{R}_k) = [0.01, 0.01, 0.001, 0.00001]$.

The vehicle is assumed to have state constraints on the location $0 \leq x_k \leq 20$, $0 \leq y_k \leq 5$ and the velocity $0 \leq v_k \leq 22$, and input constraints on the steering angle $|\delta| \leq 1.0472$ and the acceleration $|a| \leq 3.5$.

The unknown attack signals are

$$\delta_k^d = \begin{cases} 0, & 0 \le k < 100 \\ 1.1\sin(0.05k), & 0 \le k < 100 \end{cases}$$

$$a_k^d = \begin{cases} 0 & 0 \le k < 100 \\ 3.5, & 100n \le k < 100(n+1) \\ -3.5, & 100(n+1) \le k < 100(n+2) \end{cases},$$

where $n = 1, 2, \cdots, 5$.

The constraints on the vehicle can be formulated by inequality constraints as in Equation (3.2):

$$\underbrace{\begin{bmatrix} 1 & 0 \\ -1 & 0 \\ 0 & 1 \\ 0 & -1 \end{bmatrix}}_{\mathcal{A}_{k-1}} \begin{bmatrix} \delta_{k-1}^d \\ a_{k-1}^d \end{bmatrix} \le \underbrace{\begin{bmatrix} 1.0472 - \delta_{k-1}^u \\ 1.0472 + \delta_{k-1}^u \\ 3.5 - a_{k-1}^u \\ 3.5 + a_{k-1}^u \end{bmatrix}}_{\boldsymbol{b}_{k-1}}$$

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \end{bmatrix}}_{\mathcal{B}_k} \begin{bmatrix} x_k \\ y_k \\ \psi_k \\ v_k \end{bmatrix} \le \underbrace{\begin{bmatrix} 20 \\ 0 \\ 5 \\ 0 \\ 22 \\ 0 \end{bmatrix}}_{\boldsymbol{c}_k}.$$

To reduce the effect of instantaneous noises, the cumulative sum algorithm (CUSUM) is adopted [71]. The χ^2 test is utilized in a cumulative form. The

χ^2 CUSUM detector is characterized by the detector state $S_k \in \mathbb{R}_+$:

$$S_k = \phi S_{k-1} + \hat{\boldsymbol{d}}_k^\top \boldsymbol{P}_k^{-1} \hat{\boldsymbol{d}}_k, \quad S_0 = 0, \tag{3.53}$$

where $0 < \phi < 1$ is the pre-determined forgetting rate. At each time k, the CUSUM detector Equation (3.53) is used to update the detector state S_k and detect the attack. In particular, we conclude that the attack is presented if

$$S_k > \sum_{i=0}^{\infty} \phi^i \chi^2_{df}(\alpha) = \frac{\chi^2_{df}(\alpha)}{1-\phi}. \tag{3.54}$$

All values are in standard SI units: m (meter) for l_f, l_r, x_k, and y_k; rad for δ_k^u, δ_k^d, β_k^u, β_k^d, and ψ_k; m/s for v_k; m/s^2 for a_k^u and a_k^d.

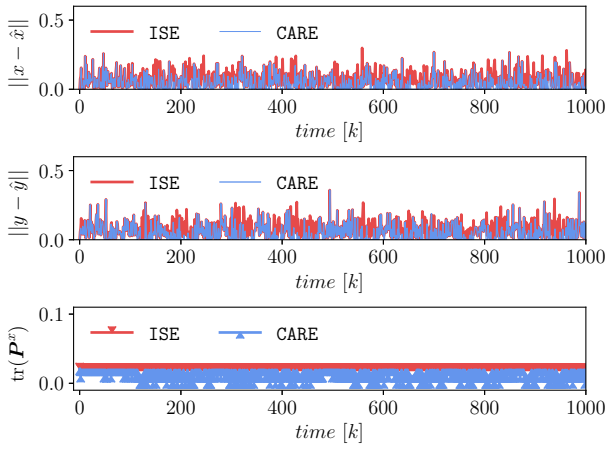


Figure 3.3: Estimation errors of constrained states and traces of the state error covariance.

Results

We show a comparison of the proposed algorithm (`CARE`) and the unified linear input and state estimator (`ISE`) introduced in [61]. Figure 3.3 shows the estimation errors of the constrained states (x_k and y_k) and the traces of

the state error covariances, and Figure 3.4 shows the unknown attack signals and their estimates and traces of the attack estimation error covariances. As expected, `CARE` produces smaller state estimation error and lower covariance. When the attack happens after $k = 100$, the estimates obtained by `CARE` are closer to the true values and have lower error covariances (cf. Table 3.1). The

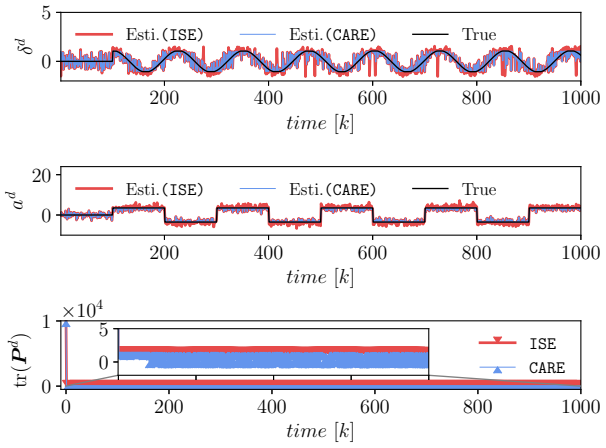


Figure 3.4: Attack signal estimation and traces of error covariance of the attack signals.

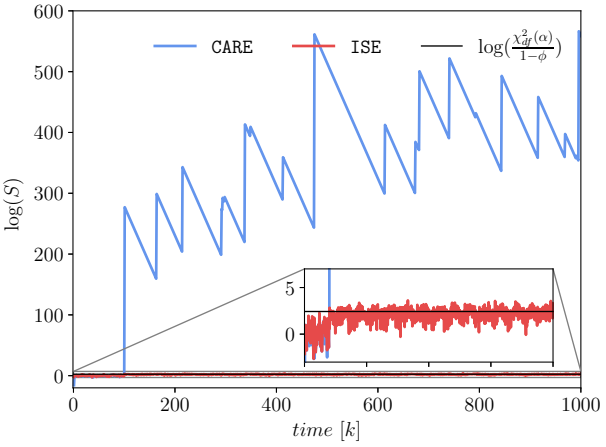


Figure 3.5: Attack detection.

estimates are used to calculate the detector state S_k in Equation (3.53). The statistical significance of the attack is tested using the CUSUM detector. The

threshold is calculated by $\chi^2_{df}/(1-\phi)$ in Equation (3.54) with the significance level $\alpha = 0.01$ and the forgetting rate $\phi = 0.15$. The detector states and the threshold are plotted in $log-$scale (Figure 3.5). When the attack is present, `CARE` can detect the attack by producing high detector state values above the threshold, while the detector state values from `ISE` are oscillating around the threshold, suffering from a high false negative rate of 66.44%.

Algorithm 2 Constrained Attack-Resilient Estimation (`CARE`):

▷ Prediction

$\hat{\boldsymbol{x}}_k^- = \boldsymbol{A}_{k-1}\hat{\boldsymbol{x}}_{k-1} + \boldsymbol{B}_{k-1}\boldsymbol{u}_{k-1}$;

$\boldsymbol{P}_k^{x,-} = \boldsymbol{A}_{k-1}\boldsymbol{P}_{k-1}^{x}\boldsymbol{A}_{k-1}^\top + \boldsymbol{Q}_{k-1}$;

▷ Attack estimation

$\tilde{\boldsymbol{R}}_k = (\boldsymbol{C}_k\boldsymbol{P}_k^{x,-}\boldsymbol{C}_k^\top + \boldsymbol{R}_k)^{-1}$;

$\boldsymbol{M}_k = (\boldsymbol{G}_{k-1}^\top\boldsymbol{C}_k^\top\tilde{\boldsymbol{R}}_k\boldsymbol{C}_k\boldsymbol{G}_{k-1})^{-1}\boldsymbol{G}_{k-1}^\top\boldsymbol{C}_k^\top\tilde{\boldsymbol{R}}_k$;

$\hat{\boldsymbol{d}}_{k-1}^u = \boldsymbol{M}_k(\boldsymbol{y}_k - \boldsymbol{C}_k\hat{\boldsymbol{x}}_k^-)$;

$\boldsymbol{P}_{k-1}^{d,u} = (\boldsymbol{G}_{k-1}^\top\boldsymbol{C}_k^\top\tilde{\boldsymbol{R}}_k\boldsymbol{C}_k\boldsymbol{G}_{k-1})^{-1}$;

$\boldsymbol{P}_{k-1}^{xd} = -\boldsymbol{P}_{k-1}^{x}\boldsymbol{A}_{k-1}^\top\boldsymbol{C}_k^\top\boldsymbol{M}_k^\top$;

▷ Time update

$\hat{\boldsymbol{x}}_k^\star = \hat{\boldsymbol{x}}_k^- + \boldsymbol{G}_{k-1}\hat{\boldsymbol{d}}_{k-1}^u$;

$$\begin{aligned}\boldsymbol{P}_k^{x\star} = {} & \boldsymbol{A}_{k-1}\boldsymbol{P}_{k-1}^{x}\boldsymbol{A}_{k-1}^\top + \boldsymbol{A}_{k-1}\boldsymbol{P}_{k-1}^{xd}\boldsymbol{G}_{k-1}^\top \\ & + \boldsymbol{G}_{k-1}(\boldsymbol{P}_{k-1}^{xd})^\top\boldsymbol{A}_{k-1}^\top + \boldsymbol{G}_{k-1}\boldsymbol{P}_{k-1}^{d,u}\boldsymbol{G}_{k-1}^\top \\ & - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{C}_k\boldsymbol{Q}_{k-1} - \boldsymbol{Q}_{k-1}\boldsymbol{C}_k^\top\boldsymbol{M}_k^\top\boldsymbol{G}_{k-1}^\top \\ & + \boldsymbol{Q}_{k-1};\end{aligned}$$

$$\begin{aligned}\tilde{\boldsymbol{R}}_k^\star = {} & \boldsymbol{C}_k\boldsymbol{P}_k^{x\star}\boldsymbol{C}_k^\top - \boldsymbol{C}_k\boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{R}_k - \boldsymbol{R}_k\boldsymbol{M}_k^\top\boldsymbol{G}_{k-1}^\top\boldsymbol{C}_k^\top \\ & + \boldsymbol{R}_k;\end{aligned}$$

▷ Measurement update

$\boldsymbol{L}_k = (\boldsymbol{P}_k^{x\star}\boldsymbol{C}_k^\top - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{R}_k)\tilde{\boldsymbol{R}}_k^{\star\dagger}$;

$\hat{\boldsymbol{x}}_k^u = \hat{\boldsymbol{x}}_k^\star + \boldsymbol{L}_k(\boldsymbol{y}_k - \boldsymbol{C}_k\hat{\boldsymbol{x}}_k^\star)$;

$$\begin{aligned}\boldsymbol{P}_k^{x,u} = {} & (\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)\boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{R}_k\boldsymbol{L}_k^\top \\ & + \boldsymbol{L}_k\boldsymbol{R}_k\boldsymbol{M}_k^\top\boldsymbol{G}_{k-1}^\top(\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)^\top \\ & + (\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)\boldsymbol{P}_k^{x\star}(\boldsymbol{I} - \boldsymbol{L}_k\boldsymbol{C}_k)^\top + \boldsymbol{L}_k\boldsymbol{R}_k\boldsymbol{L}_k^\top;\end{aligned}$$

▷ Projection update

$\boldsymbol{\gamma}_{k-1}^d = \boldsymbol{P}_{k-1}^{d,u}\bar{\boldsymbol{\mathcal{A}}}_{k-1}^\top(\bar{\boldsymbol{\mathcal{A}}}_{k-1}\boldsymbol{P}_{k-1}^{d,u}\bar{\boldsymbol{\mathcal{A}}}_{k-1}^\top)^{-1}$;

$\hat{\boldsymbol{d}}_{k-1} = \hat{\boldsymbol{d}}_{k-1}^u - \boldsymbol{\gamma}_{k-1}^d(\bar{\boldsymbol{\mathcal{A}}}_{k-1}\hat{\boldsymbol{d}}_{k-1}^u - \bar{\boldsymbol{b}}_{k-1})$;

$\boldsymbol{P}_{k-1}^{d} = (\boldsymbol{I} - \boldsymbol{\gamma}_{k-1}^d\bar{\boldsymbol{\mathcal{A}}}_{k-1})\boldsymbol{P}_{k-1}^{d,u}(\boldsymbol{I} - \boldsymbol{\gamma}_{k-1}^d\bar{\boldsymbol{\mathcal{A}}}_{k-1})^\top$;

$\boldsymbol{\gamma}_k^x = \boldsymbol{P}_k^{x,u}\bar{\boldsymbol{\mathcal{B}}}_k^\top(\bar{\boldsymbol{\mathcal{B}}}_k\boldsymbol{P}_k^{x,u}\bar{\boldsymbol{\mathcal{B}}}_k^\top)^{-1}$;

$\hat{\boldsymbol{x}}_k = \hat{\boldsymbol{x}}_k^u - \boldsymbol{\gamma}_k^x(\bar{\boldsymbol{\mathcal{B}}}_k\hat{\boldsymbol{x}}_k^u - \bar{\boldsymbol{c}}_k)$;

$\boldsymbol{P}_k^{x} = (\boldsymbol{I} - \boldsymbol{\gamma}_k^x\bar{\boldsymbol{\mathcal{B}}}_k)\boldsymbol{P}_k^{x,u}(\boldsymbol{I} - \boldsymbol{\gamma}_k^x\bar{\boldsymbol{\mathcal{B}}}_k)^\top$;

Chapter 4

Fixed Rank Resilient Filtering

Spatio-temporal modeling and filtering have been widely used in environmental process estimation [72]. These methodologies' main idea is to model spatial and temporal random effects in dynamic systems and recursively estimate the target variable. Since these methodologies consider both spatial and temporal correlation for a large-scale system, they provide a smooth geostatistical mapping. Recent research focuses on reducing the computational complexity for potentially massive datasets [73, 74, 75]. In particular, the spatio-temporal fixed rank filter in [74] improves the computational efficiency using spatio-temporal models defined on a fixed dimensional space. However, getting an exact model of the fixed dimensional space is difficult. The chapter proposes to extend the spatio-temporal fixed rank filter [74] to a fixed rank resilient filter (FRRF) such that the filter captures model uncertainty and unmodeled biased noises.

4.1 Problem Formulation

Consider a spatio-temporal process

$$\{\boldsymbol{q}_{s,k} : s \in D, k \in \{1, 2, \cdots, n_D\}\},$$

where $\boldsymbol{q}_{s,k} \in \mathbb{R}^{n_q}$, and D is the index set of spatial domains (or area), and k is the discrete-time index. Domain D could be finite or countably infinite. Now consider the spatio-temporal mixed effect model [74, 75]:

$$\boldsymbol{q}_{s,k} = \boldsymbol{\mu}_{s,k} + \boldsymbol{S}_{s,k}\boldsymbol{\eta}_k + \boldsymbol{\xi}_{s,k} \tag{4.1a}$$

$$\boldsymbol{z}_k = [\boldsymbol{z}_{s_{1_k},k}, \boldsymbol{z}_{s_{2_k},k}, \cdots, \boldsymbol{z}_{s_{n_k},k}]^\top \tag{4.1b}$$

$$\boldsymbol{z}_{s,k} = \boldsymbol{q}_{s,k} + \boldsymbol{\epsilon}_{s,k}, \tag{4.1c}$$

where $\boldsymbol{z}_{s,k} \in \mathbb{R}^{n_q}$ is the output of area s at time k and is subject to measurement noise $\boldsymbol{\epsilon}_{s,k}$. At the time k, we observe n_k sensor outputs, and the collection of outputs is denoted by $\boldsymbol{z}_k \in \mathbb{R}^{n_k n_q}$. The collection of measured area indices is denoted by $O_k = \{s_{1_k}, s_{2_k}, \cdots, s_{n_k}\} \subseteq D$.

The first term $\boldsymbol{\mu}_{s,k} \in \mathbb{R}^{n_q}$ in Equation (4.1a) is a known time-varying value that models large-scale variation and is sometimes called a mean of $\boldsymbol{q}_{s,k}$ in literature.

The second term $\boldsymbol{S}_{s,k}\boldsymbol{\eta}_k$ captures a smooth small-scale variation that correlates the spatial relationship between different areas by the finite n_η-dimensional spatial basis $\boldsymbol{S}_{s,k}$. Matrix $\boldsymbol{S}_{s,k}$ is known, but the state variable $\boldsymbol{\eta}_k \in \mathbb{R}^{n_\eta}$ is unknown. The third term $\boldsymbol{\xi}_{s,k} \in \mathbb{R}^{n_q}$ presents time-dependent fine-scale variation that captures the nugget effect. The state variable $\boldsymbol{\eta}_k$ is supposed to evolve according to the following dynamic equation:

$$\boldsymbol{\eta}_{k+1} = \boldsymbol{H}_k\boldsymbol{\eta}_k + \boldsymbol{G}_k\boldsymbol{d}_k + \boldsymbol{\zeta}_k, \tag{4.2}$$

where $\boldsymbol{H}_k$ and $\boldsymbol{G}_k$ are known matrices. The first term $\boldsymbol{H}_k\eta_k$ captures temporal correlation, and the row of $\boldsymbol{H}_k$ can be chosen to be zeros if the corresponding component $\boldsymbol{\eta}_{k+1}$ does not change dynamically. The second term

$\boldsymbol{G}_k\boldsymbol{d}_k$ denotes a biased noise and model uncertainty, where $\boldsymbol{d}_k \in \mathbb{R}^{n_d}$ is unknown. This term is absent in [74, 75]. The last term $\boldsymbol{\zeta}_k \in \mathbb{R}^{n_\eta}$ represents a fine-scale variation of hidden state $\boldsymbol{\eta}_k$. All noises $\boldsymbol{\epsilon}_{s,k}$, $\boldsymbol{\xi}_{s,k}$, $\boldsymbol{\zeta}_k$ are independent zero-mean Gaussian with covariance $\boldsymbol{P}^{\epsilon}_{s,k}$, $\boldsymbol{P}^{\xi}_{s,k}$, and $\boldsymbol{P}^{\zeta}_{k}$, respectively.

The chapter extends the fixed rank filtering to FRRF, incorporating biased noise and model uncertainty $\boldsymbol{d}_k$, described in Equation (4.2). Our interest is to recursively estimate the hidden state $\boldsymbol{q}_{s_*,k}$ for the query area $s_* \in D$.

4.2 Algorithm Design

Denote $\boldsymbol{\mu}_k$, $\boldsymbol{S}_k$, $\boldsymbol{\epsilon}_k$, $\boldsymbol{\xi}_k$ the collection of the corresponding values for all $s \in O_k$ and define $\boldsymbol{P}^{\epsilon}_k = \mathrm{diag}(\boldsymbol{P}^{\epsilon}_{s,k})$ and $\boldsymbol{P}^{\xi}_k = \mathrm{diag}(\boldsymbol{P}^{\xi}_{s,k})$ for all $s \in O_k$ for simplicity. The matrix $\boldsymbol{E}_k \in \{0,1\}^{(n_k \times n_D) n_q}$ denotes the output matrix having $\boldsymbol{I} \in \mathbb{R}^{n_q \times n_q}$ for $(1, s_{1_k}), \cdots, (n_k, s_{n_k})$ blocks, and 0 for the others. Chapters 4.2 and 4.3 present detailed derivation and properties of FRRF. The derivation of the algorithm is motivated by fixed rank filtering [74] and simultaneous unknown input and state estimation algorithms [76, 77, 78], and, thus, they also share similar properties. In particular, the proposed algorithm is the best linear unbiased estimation (Lemma 4.1), and the expected estimation error is practically exponentially stable when measurements for each area are obtained as a Poisson process (Theorem 4.1).

Algorithm Summary

Given the output $\boldsymbol{z}_{s,k}$ and the previous estimate $\hat{\boldsymbol{\eta}}_{k-1}$, the unknown variable $\boldsymbol{\eta}_k$ in Equation (4.2) is estimated by rejecting the unmodeled uncertainty $\boldsymbol{d}_k$. The variable $\boldsymbol{q}_{s,k}$ in Equation (4.1) is estimated from $\hat{\boldsymbol{\eta}}_k$ compensating

for fine-scale variation $\boldsymbol{\xi}_{s,k}$ by its estimate $\hat{\boldsymbol{\xi}}_{s,k}$. The proposed algorithm is summarized as follows.

- **Recursive prediction:**

$$\begin{aligned}
\hat{\boldsymbol{\eta}}_{k|k-1} &= \boldsymbol{H}_{k-1}\hat{\boldsymbol{\eta}}_{k-1} + \boldsymbol{G}_{k-1}\boldsymbol{M}_k(\boldsymbol{z}_k - \boldsymbol{\mu}_k - \boldsymbol{S}_k\boldsymbol{H}_{k-1}\hat{\boldsymbol{\eta}}_{k-1}) \\
\boldsymbol{P}^{\eta}_{k|k-1} &= (\boldsymbol{I} - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{S}_k)\boldsymbol{H}_{k-1}\boldsymbol{P}^{\eta}_{k-1}\boldsymbol{H}^{\top}_{k-1}(\boldsymbol{I} - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{S}_k)^{\top} \\
&\quad + \boldsymbol{G}_{k-1}\boldsymbol{M}_k(\boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}^{\top}_k)\boldsymbol{M}^{\top}_k\boldsymbol{G}^{\top}_{k-1} \\
&\quad + (\boldsymbol{I} - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{S}_k)\boldsymbol{P}^{\zeta}_{k-1}(\boldsymbol{I} - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{S}_k)^{\top}, \qquad (4.3)
\end{aligned}$$

  where

$$\boldsymbol{M}_k = (\boldsymbol{G}^{\top}_{k-1}\boldsymbol{S}^{\top}_k\boldsymbol{R}^{-1}_k\boldsymbol{S}_k\boldsymbol{G}_{k-1})^{\dagger}\boldsymbol{G}^{\top}_{k-1}\boldsymbol{S}^{\top}_k\boldsymbol{R}^{-1}_k, \qquad (4.4)$$

  and $\boldsymbol{R}_k = \boldsymbol{S}_k(\boldsymbol{H}_{k-1}\boldsymbol{P}^{\eta}_{k-1}\boldsymbol{H}^{\top}_{k-1} + \boldsymbol{P}^{\zeta}_{k-1})\boldsymbol{S}^{\top}_k + \boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}^{\top}_k$.

- **Recursive estimation:**

$$\begin{aligned}
\hat{\boldsymbol{\eta}}_k &= \hat{\boldsymbol{\eta}}_{k|k-1} + \boldsymbol{K}_k(\boldsymbol{z}_k - \boldsymbol{\mu}_k - \boldsymbol{S}_k\hat{\boldsymbol{\eta}}_{k|k-1}) \\
\boldsymbol{P}^{\eta}_k &= (\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{S}_k)\boldsymbol{P}^{\eta}_{k|k-1}(\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{S}_k)^{\top} + \boldsymbol{K}_k(\boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}^{\top}_k)\boldsymbol{K}^{\top}_k \\
&\quad + (\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{S}_k)\boldsymbol{M}_k(\boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}^{\top}_k)\boldsymbol{K}^{\top}_k \\
&\quad + \boldsymbol{K}_k(\boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}^{\top}_k)\boldsymbol{M}^{\top}_k(\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{S}_k)^{\top}, \qquad (4.5)
\end{aligned}$$

  where

$$\boldsymbol{K}_k = (\boldsymbol{P}^{\eta}_{k|k-1}\boldsymbol{S}^{\top}_k - \boldsymbol{M}_k(\boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}^{\top}_k))\tilde{\boldsymbol{R}}^{-1}_k, \qquad (4.6)$$

  and $\tilde{\boldsymbol{R}}_k = \boldsymbol{S}_k\boldsymbol{P}^{\eta}_{k|k-1}\boldsymbol{S}^{\top}_k + (\boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}^{\top}_k) - \boldsymbol{S}_k\boldsymbol{M}_k(\boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}^{\top}_k) - (\boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}^{\top}_k)\boldsymbol{M}^{\top}_k\boldsymbol{S}^{\top}_k$.

- **Estimation of $\boldsymbol{q}_{s_*,k}$:**

$$\hat{\boldsymbol{q}}_{s_*,k} = \boldsymbol{\mu}_{s_*,k} + \boldsymbol{S}_{s_*,k}\hat{\boldsymbol{\eta}}_k + \hat{\boldsymbol{\xi}}_{s_*,k}$$
$$\hat{\boldsymbol{\xi}}_{s_*,k} = \boldsymbol{L}_{s_*,k}(\boldsymbol{z}_k^{s_*} - \bar{\boldsymbol{I}}\boldsymbol{\mu}_{s_*,k} - \bar{\boldsymbol{I}}\boldsymbol{S}_{s_*,k}\hat{\boldsymbol{\eta}}_{k|k-1})$$

and if $s_* \in O_k$, we have

$$\begin{aligned}\boldsymbol{P}^q_{s_*,k} = {} & \boldsymbol{S}_{s_*,k}\boldsymbol{K}_k\boldsymbol{S}_k\boldsymbol{P}^{\eta}_{k|k-1}(\boldsymbol{S}_{s_*,k}\boldsymbol{K}_k\boldsymbol{S}_k)^\top + \boldsymbol{L}_{s_*,k}\boldsymbol{P}^{\epsilon}_{s_*,k}\boldsymbol{L}^\top_{s_*,k} \\ & + \boldsymbol{S}_{s_*,k}\boldsymbol{K}_k(\boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}_k^\top)(\boldsymbol{S}_{s_*,k}\boldsymbol{K}_k)^\top + \boldsymbol{L}_{s_*,k}\boldsymbol{P}^{s_*,s,\epsilon}_k\boldsymbol{K}_k^\top\boldsymbol{S}^\top_{s_*,k} \\ & + \boldsymbol{S}_{s_*,k}\boldsymbol{K}_k\boldsymbol{S}_k\boldsymbol{G}_{k-1}\boldsymbol{M}_k((\boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}_k^\top)\boldsymbol{K}_k^\top\boldsymbol{S}^\top_{s_*,k} + \boldsymbol{P}^{s,s_*,\epsilon}_k\boldsymbol{L}^\top_{s_*,k}) \\ & + (\boldsymbol{S}_{s_*,k}\boldsymbol{K}_k(\boldsymbol{P}^{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{P}^{\xi}_k\boldsymbol{E}_k^\top) + \boldsymbol{S}_{s_*,k}\boldsymbol{K}_k\boldsymbol{P}^{s,s_*,\epsilon}_k\boldsymbol{L}^\top_{s_*,k} \\ & + \boldsymbol{L}_{s_*,k}\boldsymbol{P}^{s_*,s,\epsilon}_k)(\boldsymbol{S}_{s_*,k}\boldsymbol{K}_k\boldsymbol{S}_k\boldsymbol{G}_{k-1}\boldsymbol{M}_k)^\top; \end{aligned} \tag{4.7a}$$

otherwise,

$$\boldsymbol{P}^q_{s_*,k} = \boldsymbol{S}_{s_*,k}\boldsymbol{P}^{\eta}_k\boldsymbol{S}^\top_{s_*,k} + \boldsymbol{P}^{\xi}_{s_*,k}, \tag{4.7b}$$

where $\boldsymbol{z}_k^{s_*}$ is the collection of outputs $\boldsymbol{z}_{s,k}$ for $s = s^*$,

$$\boldsymbol{L}_{s_*,k} = \begin{cases} (\bar{\boldsymbol{I}}^\top\bar{\boldsymbol{R}}^{-1}_{s_*,k}\bar{\boldsymbol{I}})^{-1}\bar{\boldsymbol{I}}^\top\bar{\boldsymbol{R}}^{-1}_{s_*,k} & \text{if } s_* \in O_k \\ 0 & \text{otherwise,} \end{cases} \tag{4.8}$$

and $\bar{\boldsymbol{R}}_{s_*,k} = \boldsymbol{P}^{\epsilon}_{s_*,k}\boldsymbol{I} + \bar{\boldsymbol{I}}\boldsymbol{S}_{s_*,k}\boldsymbol{P}^{\eta}_{k|k-1}\boldsymbol{S}^\top_{s_*,k}\bar{\boldsymbol{I}}^\top - \bar{\boldsymbol{I}}\boldsymbol{S}_{s_*,k}\boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{P}^{s,s_*,\epsilon}_k - \boldsymbol{P}^{s_*,s,\epsilon}_k(\bar{\boldsymbol{I}}\boldsymbol{S}_{s_*,k}\boldsymbol{G}_{k-1}\boldsymbol{M}_k)^\top$, $\bar{\boldsymbol{I}} = [\boldsymbol{I}, \cdots, \boldsymbol{I}]^\top$, $\boldsymbol{P}^{s,s_*,\epsilon}_k \triangleq \mathbb{E}[\boldsymbol{\epsilon}_k(\boldsymbol{\epsilon}^{s_*}_k)^\top]$.

FRRF Derivation

Prediction of $\boldsymbol{\eta}_k$. The previous estimate $\hat{\boldsymbol{\eta}}_{k-1}$ and its covariance $\boldsymbol{P}^{\eta}_{k-1}$ are given in the last iteration. Assuming that the estimate $\hat{\boldsymbol{\eta}}_{k-1}$ is unbiased, the

uncertainty $\boldsymbol{d}_{k-1}$ can be estimated from the prediction error:

$$\begin{aligned}\hat{\boldsymbol{d}}_{k-1} &= \boldsymbol{M}_k(\boldsymbol{z}_k - \boldsymbol{\mu}_k - \boldsymbol{S}_k\boldsymbol{H}_{k-1}\hat{\boldsymbol{\eta}}_{k-1}) \\ &= \boldsymbol{M}_k(\boldsymbol{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{\xi}_k + \boldsymbol{S}_k(\boldsymbol{\zeta}_{k-1} + \boldsymbol{G}_{k-1}\boldsymbol{d}_{k-1} + \boldsymbol{H}_{k-1}\tilde{\boldsymbol{\eta}}_{k-1})),\end{aligned} \tag{4.9}$$

where the error is a function of $\boldsymbol{M}_k\boldsymbol{S}_k\boldsymbol{G}_{k-1}\boldsymbol{d}_{k-1}$. To provide an unbiased estimate, we will choose $\boldsymbol{M}_k$ later such that $\boldsymbol{M}_k\boldsymbol{S}_k\boldsymbol{G}_{k-1} = \boldsymbol{I}$. The error dynamics of the uncertainty estimate are

$$\tilde{\boldsymbol{d}}_{k-1} = -\boldsymbol{M}_k(\boldsymbol{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{\xi}_k + \boldsymbol{S}_k(\boldsymbol{\zeta}_{k-1} + \boldsymbol{H}_{k-1}\tilde{\boldsymbol{\eta}}_{k-1})). \tag{4.10}$$

Given $\hat{\boldsymbol{d}}_{k-1}$, the current state $\boldsymbol{\eta}_k$ can be predicted by the dynamical system in Equation (4.2):

$$\hat{\boldsymbol{\eta}}_{k|k-1} = \boldsymbol{H}_{k-1}\hat{\boldsymbol{\eta}}_{k-1} + \boldsymbol{G}_{k-1}\hat{\boldsymbol{d}}_{k-1}.$$

The estimation error $\tilde{\boldsymbol{\eta}}_{k|k-1} = \boldsymbol{\eta}_k - \hat{\boldsymbol{\eta}}_{k|k-1}$ becomes

$$\begin{aligned}\tilde{\boldsymbol{\eta}}_{k|k-1} &= \boldsymbol{H}_{k-1}\tilde{\boldsymbol{\eta}}_{k-1} + \boldsymbol{G}_{k-1}\tilde{\boldsymbol{d}}_{k-1} + \boldsymbol{\zeta}_{k-1} \\ &= (\boldsymbol{I} - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{S}_k)\boldsymbol{H}_{k-1}\tilde{\boldsymbol{\eta}}_{k-1} - \boldsymbol{G}_{k-1}\boldsymbol{M}_k(\epsilon_k + \boldsymbol{E}_k\boldsymbol{\xi}_k) \\ &+ (\boldsymbol{I} - \boldsymbol{G}_{k-1}\boldsymbol{M}_k\boldsymbol{S}_k)\boldsymbol{\zeta}_{k-1},\end{aligned}$$

where the relation in Equation (4.10) is applied. These error dynamics induce the covariance update for $\boldsymbol{P}^{\eta}_{k|k-1}$ in Equation (4.3).

Estimation of $\boldsymbol{\eta}_k$. Given $\hat{\boldsymbol{\eta}}_{k|k-1}$, the prediction is corrected by the prediction error $\boldsymbol{z}_k - \boldsymbol{\mu}_k - \boldsymbol{S}_k\hat{\boldsymbol{\eta}}_{k|k-1}$:

$$\hat{\boldsymbol{\eta}}_k = \hat{\boldsymbol{\eta}}_{k|k-1} + \boldsymbol{K}_k(\boldsymbol{z}_k - \boldsymbol{\mu}_k - \boldsymbol{S}_k\hat{\boldsymbol{\eta}}_{k|k-1}).$$

The estimation error becomes

$$\tilde{\boldsymbol{\eta}}_k = (\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{S}_k)\tilde{\boldsymbol{\eta}}_{k|k-1} - \boldsymbol{K}_k(\boldsymbol{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{\xi}_k), \tag{4.11}$$

which results in the covariance $\boldsymbol{P}_k^{\eta}$ in Equation (4.5).

Estimation of $\boldsymbol{q}_{s_*,k}$ Our interest is to estimate the hidden state $\boldsymbol{q}_{s_*,k}$ for the query area s_*, which can be estimated by the process model in Equation (4.1) as follows:

$$\hat{\boldsymbol{q}}_{s_*,k} = \boldsymbol{\mu}_{s_*,k} + \boldsymbol{S}_{s_*,k}\hat{\boldsymbol{\eta}}_k + \hat{\boldsymbol{\xi}}_{s_*,k},$$

where

$$\hat{\boldsymbol{\xi}}_{s_*,k} = \begin{cases} \boldsymbol{L}_{s_*,k}(\boldsymbol{z}_k^{s_*} - \bar{\boldsymbol{I}}\boldsymbol{\mu}_{s_*,k} - \bar{\boldsymbol{I}}\boldsymbol{S}_{s_*,k}\hat{\boldsymbol{\eta}}_{k|k-1}) & \text{if } s_* \in O_k \\ 0 & \text{otherwise} \end{cases}$$

and $\bar{\boldsymbol{I}} = [\boldsymbol{I}, \cdots, \boldsymbol{I}]^\top$. Since $\boldsymbol{\xi}_{s_*,k}$ is associated with the area s_*, the measurement $\boldsymbol{z}_{s,k}$ is not a function of $\boldsymbol{\xi}_{s_*,k}$ if $s \neq s_*$. Therefore, the estimate $\hat{\boldsymbol{\xi}}_{s_*,k}$ is available only when $s_* \in O_k$. Since

$$\hat{\boldsymbol{\xi}}_{s_*,k} = \boldsymbol{L}_{s_*,k}(\bar{\boldsymbol{I}}\boldsymbol{S}_{s_*,k}\tilde{\boldsymbol{\eta}}_{k|k-1} + \boldsymbol{\epsilon}_k^{s_*} + \bar{\boldsymbol{I}}\boldsymbol{\xi}_{s_*,k}),$$

we need to choose the gain $\boldsymbol{L}_{s_*,k}$ such that $\boldsymbol{L}_{s_*,k}\bar{\boldsymbol{I}} = \boldsymbol{I}$ for an unbiased estimate. Then, the estimation error becomes

$$\tilde{\boldsymbol{\xi}}_{s_*,k} = \boldsymbol{L}_{s_*,k}(\bar{\boldsymbol{I}}\boldsymbol{S}_{s_*,k}\tilde{\boldsymbol{\eta}}_{k|k-1} + \boldsymbol{\epsilon}_k^{s_*}). \tag{4.12}$$

The estimation error for $\boldsymbol{q}_{s_*,k}$ is given by

$$\begin{aligned}\tilde{\boldsymbol{q}}_{s_*,k} &= \boldsymbol{S}_{s_*,k}\tilde{\boldsymbol{\eta}}_k + \tilde{\boldsymbol{\xi}}_{s_*,k} \\ &= -\boldsymbol{S}_{s_*,k}\boldsymbol{K}_k\boldsymbol{S}_k\tilde{\boldsymbol{\eta}}_{k|k-1} - \boldsymbol{S}_{s_*,k}\boldsymbol{K}_k(\boldsymbol{\epsilon}_k + \boldsymbol{E}_k\xi_k) - \boldsymbol{L}_{s_*,k}\boldsymbol{\epsilon}_k^{s_*},\end{aligned} \tag{4.13}$$

where the relations $\boldsymbol{L}_{s_*,k}\bar{\boldsymbol{I}} = \boldsymbol{I}$ and Equation (4.11) are applied. If $s_* \notin O_k$, then we have

$$\tilde{\boldsymbol{q}}_{s_*,k} = \boldsymbol{S}_{s_*,k}\tilde{\boldsymbol{\eta}}_k + \boldsymbol{\xi}_{s_*,k}.$$

Considering the cross relations between the error terms, we can find the covariance $\boldsymbol{P}^q_{s_*,k}$ in Equation (4.7).

4.3 Properties of the FRRF

Lemma 4.1 *Assume $\hat{\boldsymbol{\eta}}_0$ is an unbiased estimate. The estimates $\hat{\boldsymbol{\eta}}_k$, $\hat{\boldsymbol{d}}_{k-1}$ and $\hat{\boldsymbol{q}}_k$ are the best linear unbiased estimates (BLUE), if the gains $\boldsymbol{M}_k$, $\boldsymbol{K}_k$, and $\boldsymbol{L}_{s_*,k}$ are chosen by Equations (4.4), (4.6) and (4.8), respectively.*

Proof: Assume $\hat{\boldsymbol{\eta}}_{k-1}$ is unbiased. The prediction error is given by

$$\boldsymbol{z}_k - \boldsymbol{\mu}_k - \boldsymbol{S}_k\boldsymbol{H}_{k-1}\hat{\boldsymbol{\eta}}_{k-1} = \boldsymbol{S}_k\boldsymbol{d}_{k-1} + (\boldsymbol{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{\xi}_k + \boldsymbol{S}_k(\boldsymbol{\zeta}_{k-1} + \boldsymbol{H}_{k-1}\tilde{\boldsymbol{\eta}}_{k-1})).$$

By normalizing the above equation with $\boldsymbol{R}_k^{-\frac{1}{2}}$, we have

$$\begin{aligned}&\boldsymbol{R}_k^{-\frac{1}{2}}(\boldsymbol{z}_k - \boldsymbol{\mu}_k - \boldsymbol{S}_k\boldsymbol{H}_{k-1}\hat{\boldsymbol{\eta}}_{k-1})\\ &= \boldsymbol{R}_k^{-\frac{1}{2}}\boldsymbol{S}_k\boldsymbol{d}_{k-1} + \boldsymbol{R}_k^{-\frac{1}{2}}(\boldsymbol{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{\xi}_k + \boldsymbol{S}_k(\boldsymbol{\zeta}_{k-1} + \boldsymbol{H}_{k-1}\tilde{\boldsymbol{\eta}}_{k-1})),\end{aligned}$$

where the variance of the last term is normalized, i.e., $Var(\boldsymbol{R}_k^{-\frac{1}{2}}(\boldsymbol{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{\xi}_k + \boldsymbol{S}_k(\boldsymbol{\zeta}_{k-1} + \boldsymbol{H}_{k-1}\tilde{\boldsymbol{\eta}}_{k-1}))) = \boldsymbol{I}$. Now, by the Gauss Markov theorem, we can get $\boldsymbol{M}_k$ in Equation (4.4). Therefore, $\hat{\boldsymbol{d}}_{k-1}$ in Equation (4.9) is BLUE as long as $\hat{\boldsymbol{\eta}}_{k-1}$ is unbiased.

Given that $\hat{\boldsymbol{\eta}}_{k-1}$ and $\hat{\boldsymbol{d}}_{k-1}$ are unbiased, the estimate $\hat{\boldsymbol{\eta}}_k$ is unbiased

$$\mathbb{E}[\tilde{\boldsymbol{\eta}}_k] = \mathbb{E}[(\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{S}_k)\tilde{\boldsymbol{\eta}}_{k|k-1} - \boldsymbol{K}_k(\boldsymbol{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{\xi}_k)] = 0$$

for any $\boldsymbol{K}_k$. Now consider the following optimization problem that minimizes the trace of the covariance $\boldsymbol{P}_k^{\eta}$ in Equation (4.5): $\min_{\boldsymbol{K}_k} \mathrm{tr}(\boldsymbol{P}_k^{\eta})$. The problem is an unconstrained convex optimization problem, and thus $\boldsymbol{K}_k$ is found by taking the objective function derivative with respect to the decision variable $\boldsymbol{K}_k$ and setting it equal to zero. The solution is $\boldsymbol{K}_k$ in Equation (4.6). Therefore, $\hat{\boldsymbol{\eta}}_k$ is BLUE, provided that $\hat{\boldsymbol{\eta}}_{k-1}$ and $\hat{\boldsymbol{d}}_{k-1}$ are unbiased.

Given $\hat{\boldsymbol{\eta}}_0$ is unbiased, $\hat{\boldsymbol{d}}_0$ and $\hat{\boldsymbol{\eta}}_1$ are BLUE by the above statements. Also, given $\hat{\boldsymbol{\eta}}_{k-1}$ is unbiased (because it is BLUE), $\hat{\boldsymbol{d}}_{k-1}$ and $\hat{\boldsymbol{\eta}}_k$ are BLUE. Therefore, $\hat{\boldsymbol{\eta}}_k$ and $\hat{\boldsymbol{d}}_k$ are BLUE for all k.

Given that $\hat{\boldsymbol{\eta}}_k$ is BLUE, one can show that $\hat{\boldsymbol{\xi}}_k$ is BLUE by the same logic of the first paragraph in this proof. In sequel, $\hat{\boldsymbol{q}}_k$ is BLUE as well. We omit its details. □

If we have multiple outputs in the same area, we can combine those measurements into a single output by the optimal combination considering

their covariance. So, now we assume that each region may have at most a single measurement. Consider the following assumption.

Assumption 4.1 *There exist* $\bar{s}$, $\bar{h}$, $\bar{g}$, $\bar{m}$, $\underline{\eta} > 0$, *such that the following holds for all* $k \geq 0$*:*

$$\|\boldsymbol{S}_{s,k}\| \leq \bar{s}, \qquad \|\boldsymbol{H}_k\| \leq \bar{h}, \qquad \|\boldsymbol{G}_k\| \leq \bar{g},$$
$$\|\boldsymbol{M}_k\| \leq \bar{m}, \qquad \boldsymbol{P}_k^{\eta} \geq \underline{\eta}\boldsymbol{I}.$$

Assumption 4.1 is widely used to show the stability of Kalman filter [79, 80]. In input-state estimation, $\boldsymbol{P}_k^{\eta}$ is bounded, if the transformed system is uniformly observable [77, 78].

Since the measurement $\boldsymbol{z}_{s,k}$ is provided by anonymous vehicles, the data center does not know when they can get a measurement $\boldsymbol{z}_{s,k}$. We assume the obtainment of measurement is a random arrival process. Poisson process is a commonly used model for random and independent message arrivals. Assumption 4.2 implies that the measurement $\boldsymbol{z}_{s,k}$ at area $s \in D$ is randomly and independently obtained.

Assumption 4.2 *For any* $s \in D$*, the measurement* $\boldsymbol{z}_{s,k}$ *is obtained as a Poisson arrival process with arrival rate* λ*. The value* $\boldsymbol{z}_{s,k}$ *is independent of the Poisson distribution.*

Under the assumptions mentioned above, we can show the performance of the state estimation error.

Theorem 4.1 *Under Assumptions 4.1 and 4.2, the expected error* $\mathbb{E}[\|\tilde{\boldsymbol{q}}_k\|]$ *is practically exponentially stable in probability, i.e., there exist a set of positive*

constants a, γ, and c such that

$$\mathbb{E}[\|\tilde{\boldsymbol{q}}_k\|] \leq ae^{-\gamma k} + c. \tag{4.14}$$

Proof: For this analysis, we reformulate the output model as follows:

$$\boldsymbol{z}_k = [\boldsymbol{z}_{s_1}^\top, \cdots, \boldsymbol{z}_{s_n}^\top]^\top, \tag{4.15}$$

which is the collection of outputs for all the areas, where $\boldsymbol{z}_{s_i} = 0$ if $s_i \notin O_k$. Let us introduce an indicator matrix $\mathcal{I}_k = \text{diag}(i_{s_1,k}, \cdots, i_{s_n,k})$, where $i_{s_j,k} = \boldsymbol{I}$ if $s_j \in O_k$, $i_{s_j,k} = 0$ otherwise.

Consider matrices $\mathbb{M}_k$ and $\mathbb{K}_k$ with appending zeros to M_k and K_k such that Equations (4.3) and (4.5) can be replaced with

$$\begin{aligned}
\hat{\boldsymbol{\eta}}_{k|k-1} &= \boldsymbol{H}_{k-1}\hat{\boldsymbol{\eta}}_{k-1} + \mathbb{M}_k\mathcal{I}_k(\boldsymbol{z}_k - \boldsymbol{\mu}_k - \boldsymbol{S}_k\boldsymbol{H}_{k-1}\hat{\boldsymbol{\eta}}_{k-1}) \\
\hat{\boldsymbol{\eta}}_k &= \hat{\boldsymbol{\eta}}_{k|k-1} + \mathbb{K}_k\mathcal{I}_k(\boldsymbol{z}_k - \boldsymbol{\mu}_k - \boldsymbol{S}_k\hat{\boldsymbol{\eta}}_{k|k-1}),
\end{aligned}$$

where $\mathbb{K}_k = \mathbb{K}_k\mathcal{I}_k$ and $\mathbb{M}_k = \mathbb{M}_k\mathcal{I}_k$ hold because we've appended zeros to $\boldsymbol{K}_k$ and $\boldsymbol{M}_k$. Note that $\boldsymbol{z}_k$ in the above equation represents all the measurements in Equation (4.15). Given this notation, we have the error dynamics:

$$\begin{aligned}
\tilde{\boldsymbol{\eta}}_k &= (\boldsymbol{I} - \mathbb{K}_k\boldsymbol{S}_k)\tilde{\boldsymbol{\eta}}_{k|k-1} - \mathbb{K}_k(\boldsymbol{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{\xi}_k) \\
&= (\boldsymbol{I} - \mathbb{K}_k\boldsymbol{S}_k)(\boldsymbol{I} - \boldsymbol{G}_{k-1}\mathbb{M}_k\boldsymbol{S}_k)\boldsymbol{H}_{k-1}\tilde{\boldsymbol{\eta}}_{k-1} + (\boldsymbol{I} - \mathbb{K}_k\boldsymbol{S}_k)(\boldsymbol{I} - \boldsymbol{G}_{k-1}\mathbb{M}_k\boldsymbol{S}_k)\boldsymbol{\zeta}_{k-1} \\
&\quad - ((\boldsymbol{I} - \mathbb{K}_k\boldsymbol{S}_k)\boldsymbol{G}_{k-1}\mathbb{M}_k + \mathbb{K}_k)(\boldsymbol{\epsilon}_k + \boldsymbol{E}_k\boldsymbol{\xi}_k).
\end{aligned}$$

Choose the Lyapunov function candidate

$$
\begin{aligned}
V_k &= \tilde{\boldsymbol{\eta}}_k^\top (\boldsymbol{P}_k^{\boldsymbol{\eta}})^{-1} \tilde{\boldsymbol{\eta}}_k \\
&= \tilde{\boldsymbol{\eta}}_{k-1}^\top \bar{\boldsymbol{H}}_{k-1}^\top (\boldsymbol{I} - \mathbb{K}_k \boldsymbol{S}_k)^\top (\boldsymbol{P}_k^{\eta})^{-1} (\boldsymbol{I} - \mathbb{K}_k \boldsymbol{S}_k) \bar{\boldsymbol{H}}_{k-1} \tilde{\boldsymbol{\eta}}_{k-1} \\
&+ 2\tilde{\boldsymbol{\eta}}_{k-1}^\top \bar{\boldsymbol{H}}_{k-1}^\top (\boldsymbol{I} - \mathbb{K}_k \boldsymbol{S}_k)^\top (\boldsymbol{P}_k^{\eta})^{-1} ((\boldsymbol{I} - \mathbb{K}_k \boldsymbol{S}_k) \bar{\boldsymbol{\zeta}}_{k-1} + \bar{\boldsymbol{K}}_k \bar{\boldsymbol{\epsilon}}_k) \\
&+ \bar{\boldsymbol{\zeta}}_{k-1}^\top (\boldsymbol{I} - \mathbb{K}_k \boldsymbol{S}_k)^\top (\boldsymbol{P}_k^{\eta})^{-1} (\boldsymbol{I} - \mathbb{K}_k \boldsymbol{S}_k) \bar{\boldsymbol{\zeta}}_{k-1} + 2\bar{\boldsymbol{\zeta}}_{k-1}^\top (\boldsymbol{I} - \mathbb{K}_k \boldsymbol{S}_k)^\top (\boldsymbol{P}_k^{\eta})^{-1} \bar{\boldsymbol{K}}_k \bar{\boldsymbol{\epsilon}}_k \\
&+ \bar{\boldsymbol{\epsilon}}_k^\top \bar{\boldsymbol{K}}_k^\top (\boldsymbol{P}_k^{\eta})^{-1} \bar{\boldsymbol{K}}_k \bar{\boldsymbol{\epsilon}}_k, \qquad (4.16)
\end{aligned}
$$

where

$$
\begin{aligned}
\bar{\boldsymbol{H}}_k &= (\boldsymbol{I} - \boldsymbol{G}_{k-1} \mathbb{M}_k \boldsymbol{S}_k) \boldsymbol{H}_{k-1} \\
\bar{\boldsymbol{K}}_k &= -(\boldsymbol{I} - \mathbb{K}_k \boldsymbol{S}_k) \boldsymbol{G}_{k-1} \mathbb{M}_k - \mathbb{K}_k \\
\bar{\boldsymbol{\zeta}}_{k-1} &= (\boldsymbol{I} - \boldsymbol{G}_{k-1} \mathbb{M}_k \boldsymbol{S}_k) \boldsymbol{\zeta}_{k-1}.
\end{aligned}
$$

Under Assumption 4.1, there exists $\delta \in (0, 1)$ such that

$$
\tilde{\boldsymbol{\eta}}_{k-1}^\top \bar{\boldsymbol{H}}_{k-1}^\top (\boldsymbol{I} - \mathbb{K}_k \boldsymbol{S}_k)^\top (\boldsymbol{P}_k^{\eta})^{-1} (\boldsymbol{I} - \mathbb{K}_k \boldsymbol{S}_k) \bar{\boldsymbol{H}}_{k-1} \tilde{\boldsymbol{\eta}}_{k-1} < \delta \tilde{\boldsymbol{\eta}}_{k-1}^\top (\boldsymbol{P}_{k-1}^{\eta})^{-1} \tilde{\boldsymbol{\eta}}_{k-1} \qquad (4.17)
$$

by Claim 3.1.

Since the interarrival interval of measurements follows an exponential distribution with λ by Assumption 4.2, we have

$$
\mathbb{E}[i^\alpha] = 1^\alpha \int_0^\epsilon \lambda e^{-\lambda x} dx + 0^\alpha \int_\epsilon^\infty \lambda e^{-\lambda x} dx = 1 - e^{-\lambda \epsilon}
$$

for some non-negative integer $\alpha \geq 0$, where ϵ is a sampling interval.

The diagonal indicator matrix $\mathcal{I}_k$ satisfies $\mathbb{E}[\mathcal{I}] = \mathbb{E}[\mathcal{I}\mathcal{I}^\top] = (1 - e^{-\lambda \epsilon}) \boldsymbol{I}$

and thus

$$\mathbb{E}[\mathcal{I}Q\mathcal{I}^\top] = \mathbb{E}[\mathcal{I}\mathcal{I}^\top]\mathbb{E}[\boldsymbol{Q}] = (1 - e^{-\lambda\epsilon})\mathbb{E}[\boldsymbol{Q}] \tag{4.18}$$

for any independent square matrix $\boldsymbol{Q}$. Under Assumption 4.1, there exists positive constant c_0 such that

$$\mathbb{E}[\bar{\boldsymbol{\zeta}}_{k-1}^\top(\boldsymbol{I} - \mathbb{K}_k\boldsymbol{S}_k)^\top(\boldsymbol{P}_k^\eta)^{-1}(\boldsymbol{I} - \mathbb{K}_k\boldsymbol{S}_k)\bar{\boldsymbol{\zeta}}_{k-1} + \bar{\boldsymbol{\epsilon}}_k^\top\bar{\boldsymbol{K}}_k^\top(\boldsymbol{P}_k^\eta)^{-1}\bar{\boldsymbol{K}}_k\bar{\boldsymbol{\epsilon}}_k] \leq (1 - e^{-\lambda\epsilon})c_0 \tag{4.19}$$

by Equation (4.18) and Claim 3.2. From Equations (4.17) and (4.19), the Lyapunov function in Equation (4.16) becomes

$$\begin{aligned}\mathbb{E}[V_k] &\leq \delta\mathbb{E}[V_k] + (1 - e^{-\lambda\epsilon})c_0 \leq \delta^k\mathbb{E}[V_0] + \sum_{i=0}^{k-1}\delta^i(1 - e^{-\lambda\epsilon})c_0 \\ &\leq \delta^k\mathbb{E}[V_0] + \frac{(1 - e^{-\lambda\epsilon})c_0}{1 - \delta}.\end{aligned}$$

Therefore, we have

$$\mathbb{E}[\|\tilde{\boldsymbol{\eta}}_k\|^2] \leq \frac{\bar{p}}{\underline{p}}\delta^k\mathbb{E}[\|\tilde{\boldsymbol{\eta}}_0\|^2] + \frac{(1 - e^{-\lambda\epsilon})c_0\bar{p}}{1 - \delta}.$$

It follows that there exist $a_1, \gamma_1, c_1 > 0$ such that

$$\mathbb{E}[\|\tilde{\boldsymbol{\eta}}_k\|] \leq a_1e^{-\gamma_1 k}\mathbb{E}[\|\tilde{\boldsymbol{\eta}}_0\|] + c_1$$

Since $\mathbb{E}[\|\boldsymbol{\epsilon}_{s_*,k}\|] < c_2$, and $\mathbb{E}[\|\boldsymbol{\zeta}_k\|] < c_3$, by Equations (4.12) and (4.13), we have

$$\mathbb{E}[\|\tilde{\boldsymbol{q}}_{s_*,k}\|] \leq \mathbb{E}[\|\boldsymbol{S}_{s_*,k}\tilde{\boldsymbol{\eta}}_k\|] + \mathbb{E}[\|\tilde{\boldsymbol{\xi}}_{s_*,k}\|] \leq ae^{-\gamma k}\mathbb{E}[\|\tilde{\boldsymbol{\eta}}_0\|] + c$$

for some positive constants a, γ, and c. □

Constant c in Equation (4.14) can be seen as the expected error bound of the prior estimation, where the first term decays exponentially.

4.4 Simulation Examples

The cornering stiffness C_f (and C_r) is the coefficient related to the lateral force and sliding angle. This parameter is closely related to the road friction. In this simulation, we will conduct one FRRF algorithm by systematically combining environmental measurements $\boldsymbol{z}_{s,k}$ from anonymous vehicles and weather forecasts $\boldsymbol{\mu}_{s,k}$ and use the distribution of $\boldsymbol{q}_{s,k}$ to estimate both cornering stiffness through vehicle-to-cloud (V2C) communication.

For the cornering stiffness estimation problem, we assume $\boldsymbol{\mu}_{s,k}$ is a function of weather forecast $\mathcal{W}_{s,k}$ (including temperature, precipitation, humidity, wind, and more), i.e., $\boldsymbol{\mu}_{s,k} = \mathcal{F}(\mathcal{W}_{s,k})$. The mapping function $\mathcal{F}(\cdot)$ can be found by standard learning/regression algorithms (e.g., Gaussian process regression, neural network, basis function regression) by using historical input-output data. This chapter assumes that the function $\mathcal{F}$ is given.

We consider the road as the square area that is divided into 25 identical small squares, i.e., $n_D = 25$. The ground truth cornering stiffness holds $C_f = C_r$ for all the areas.

Consider the stochastic process $\boldsymbol{q}_{s,k}$ described in Equation (4.1) and Equation (4.2). Matrices $\boldsymbol{S}_{s,k}$ are chosen to be the W-wavelets as in [74, 81]. Matrices $\boldsymbol{H}_k$ and $\boldsymbol{G}_k$ are chosen to be identity matrices. Noises are zero-mean Gaussian with known covariance $\boldsymbol{P}^{\epsilon}_{s,k} = 10$, $\boldsymbol{P}^{\xi}_{s,k} = 100$, and $\boldsymbol{P}^{\boldsymbol{\zeta}}_{k} = 100\boldsymbol{I}$. Predictive cornering stiffnesses from the weather forecast are randomly generated by uniform distribution for each time k and each area,

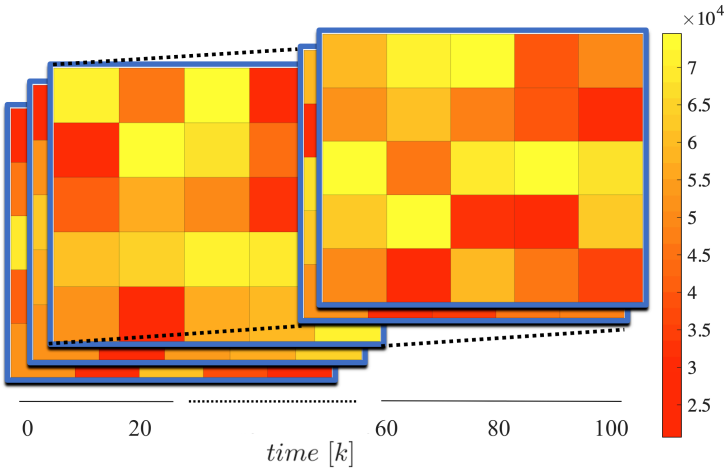


Figure 4.1: Estimation heatmap. The color represents the mean value of the estimate in the corresponding area.

i.e. $\boldsymbol{\mu}_{s,k} \sim Unif(C_{ice}, C_{dry})$ for $\forall k, s$, except $s = 1, 2$, where $C_{ice} = 19000$ and $C_{dry} = 84000$ are the conservative lower bound and upper bound. We intentionally choose time-invariant $\boldsymbol{\mu}_{1,k}$ and $\boldsymbol{\mu}_{2,k}$ for all k to compare the fine-scale tracking performance. The data center obtains the measurement $\boldsymbol{z}_{s,k}$ (for each area) as a Poisson distribution with parameter $\lambda = 20$. The unmodeled system uncertainty $\boldsymbol{d}_k$ is made up of $\boldsymbol{d}_k = 100\sin(k\pi)$.

Given the initial condition $\hat{\boldsymbol{\eta}}_0 = 0$ with covariance $\boldsymbol{P}_0^{\eta} = 1000\boldsymbol{I}$, we conduct FRRF algorithm, and present the simulation results in Figures 4.1 and 4.2. For each time k, FRRF generates a heat map for the cornering stiffness. Figure 4.1 presents a series of heat maps produced by the FRRF algorithm, where the color represents the mean value $\hat{\boldsymbol{q}}_{s,k}$ of the corresponding area s. Figure 4.2 compares the tracking errors when the outputs are sparsely measured (as a Poisson with $\lambda = 20$) and are fully measured at areas 1 and 2. Areas 1 and 2 are the left bottom corner and its right cell, respectively. The estimation errors for all areas remain in their noise level. FRRF algorithm estimates the ground truth cornering stiffness resiliently, where the errors do not depend on the presence of d_k, as shown in the first subfigure. FRRF

with the full measurement exhibits an improved tracking performance of fine-scale variation a lot than that with the sparse measurement, as presented in the second and third subfigures. This is because FRRF with the full measurement successfully reduces the estimation error by compensating for unmodeled uncertainty at each iteration. The average trace norm of variance in the whole area is $\mathrm{tr}(\boldsymbol{P}_k^{q,full}) = 1983.7$ with the full measurement and $\mathrm{tr}(\boldsymbol{P}_k^{q,\lambda=20}) = 3190.4$ with the sparse measurement.

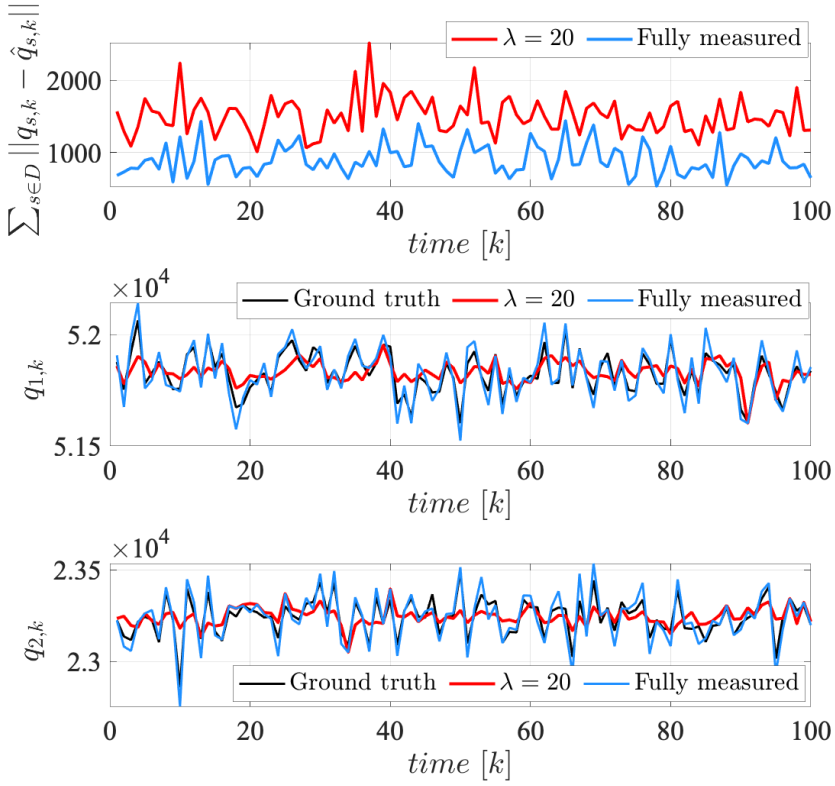


Figure 4.2: Prior estimation performance; (top) total estimation error; (middle, bottom) ground truth cornering stiffness and estimates with the full measurement and sparse measurement at areas 1 and 2.

Chapter 5

Proactive Control Architecture

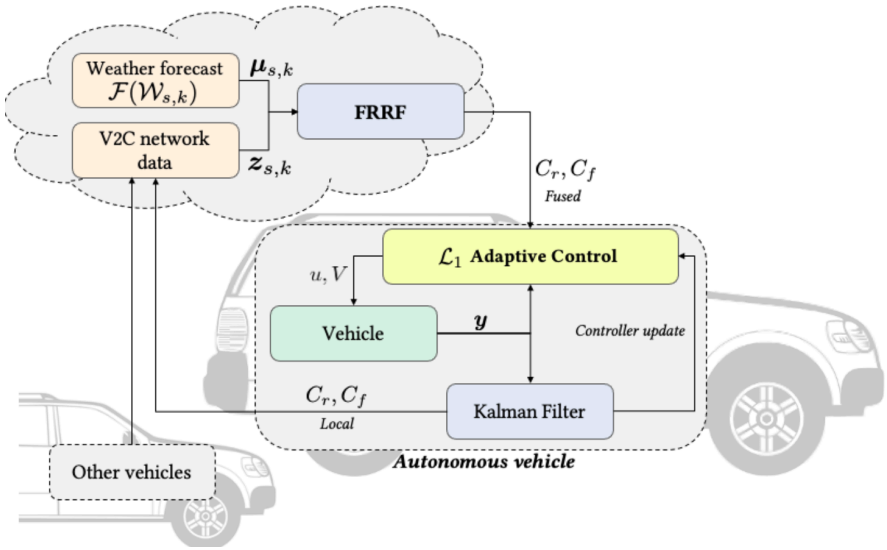


Figure 5.1: Overall architecture. The data center provides a prior estimate. Controller and velocity are proactively designed based on it for each area of the road.

This chapter proposes a novel proactive robust adaptive control architecture for autonomous vehicles to operate with guaranteed performance in various environmental conditions. Figure 5.1 illustrates the overall system architecture. The prior of the cornering stiffness for different areas is estimated by a newly developed fixed rank resilient filter (FRRF) in Chapter 4 that fuses information from the weather forecast and vehicle network data. The $\mathcal{L}_1$ adaptive heading controller and nominal longitudinal velocity are designed proactively for each area, based on the prior distribution of the cornering stiffness. The proactive adaptive controller design will reduce long-term

and large-scale uncertainty, while the $\mathcal{L}_1$ adaptive feedback controller deals with residue uncertainty from filtered data. Then, based on the posterior distribution of cornering stiffness obtained from the onboard measurements, the control parameters are updated.

5.1 Vehicle Lateral Dynamics and Problem Statement

The bicycle model is a simplified vehicle model that has been widely used and has been proven as a good approximation [82, 83, 69]. Consider Figure 5.2, in which the variables p^y, p^ψ, V, and δ denote the lateral position, yaw angle, (longitudinal) velocity, and front steering angle, respectively. Parameters C_f, C_r, m, I_z, ℓ_f, and ℓ_r are the front/rear cornering stiffness, mass, yaw moment of inertia, and distance of front/rear tire from the center of gravity, respectively.

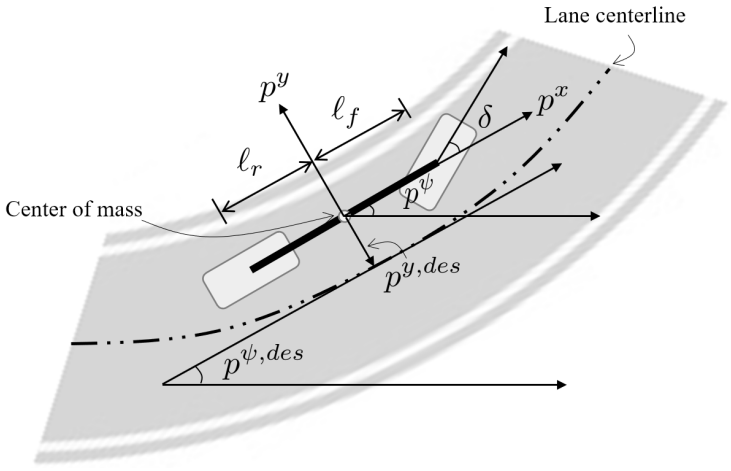


Figure 5.2: Vehicle lateral dynamics.

Given a constant velocity V, the dynamics of the collective state $p =$

$[p^y, \dot{p}^y, p^\psi, \dot{p}^\psi]^\top$ with heading input $u = \delta$ are described by ((2.31) in [69])

$$\dot{p} = A^o p + b^o u, \tag{5.1}$$

where the system matrices are

$$A^o = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -2\frac{C_f+C_r}{mV} & 0 & -V - 2\frac{C_f\ell_f - C_r\ell_r}{mV} \\ 0 & 0 & 0 & 1 \\ 0 & -2\frac{C_f\ell_f - C_r\ell_r}{I_z V} & 0 & -2\frac{C_f\ell_f^2 + C_r\ell_r^2}{I_z V} \end{bmatrix}, \quad b^o = \begin{bmatrix} 0 \\ \frac{2C_f}{m} \\ 0 \\ \frac{2C_f\ell_f}{I_z} \end{bmatrix}.$$

Given the desired lateral position $p^{y,des}$ (center of the lane) and the desired yaw angle $p^{\psi,des}$, the bicycle model in Equation (5.1) can be reformulated as error dynamics ((2.45) in [69]):

$$\dot{x} = A(V, C_f, C_r)x + b(C_f)u + g(V, C_f, C_r)\dot{p}^{\psi,des}, \tag{5.2}$$

where $x = [x_1, \dot{x}_1, x_2, \dot{x}_2]^\top$, $x_1 \triangleq p^y - p^{y,des}$ and $x_2 \triangleq p^\psi - p^{\psi,des}$ are the error states. The rate of the desired yaw angle is found by $\dot{p}^{\psi,des} = \frac{V}{R}$, where R is the radius of the road. The system matrices are

$$A(V, C_f, C_r) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -2\frac{C_f+C_r}{mV} & 2\frac{C_f+C_r}{m} & 2\frac{-C_f\ell_f + C_r\ell_r}{mV} \\ 0 & 0 & 0 & 1 \\ 0 & -2\frac{C_f\ell_f - C_r\ell_r}{I_z V} & 2\frac{C_f\ell_f - C_r\ell_r}{I_z} & -2\frac{C_f\ell_f^2 + C_r\ell_r^2}{I_z V} \end{bmatrix}$$

$$b(C_f) = b^o, \quad g(V, C_f, C_r) = \begin{bmatrix} 0 \\ -2\frac{C_f\ell_f - C_r\ell_r}{mV} - V \\ 0 \\ -2\frac{C_f\ell_f^2 + C_r\ell_r^2}{I_z V} \end{bmatrix}.$$

It is worth emphasizing that matrices A and g depend on velocity V, and that the matrices A, b, and g depend on cornering stiffnesses C_f and C_r. For notational simplicity, we express them as $A(V)$, b, and $g(V)$, when their dependency on cornering stiffnesses does not need to be emphasized.

The cornering stiffness varies for vehicles depending on many factors such as tire width, size, and type. In this chapter, we assume that the vehicles in the network have a similar hardware setup to avoid such complexity. Furthermore, any further inaccuracies can be considered uncertainties in estimation and prediction. The cornering stiffnesses C_f and C_r are assumed to be unknown, and we can estimate them using FRRF from Chapter 4. We formulate the problem of interest as follows.

Problem Statement 5.1 *The problem is to develop a robust control architecture that stabilizes the error dynamics (Equation (5.2)) of the vehicle operating under different environmental conditions through controlling the heading $u = \delta$ and designing the longitudinal velocity V.*

5.2 Proactive Robust Adaptive Control

Given prior estimates $\hat{C}_f$ and $\hat{C}_r$ of the cornering stiffness with their quantified uncertainties $\boldsymbol{P}^{C_f}$ and $\boldsymbol{P}^{C_r}$ found by $\hat{\boldsymbol{q}}_{s_*,k}$ and $\boldsymbol{P}^{q}_{s_*,k}$ in the FRRF described in Chapter 4, we implement the $\mathcal{L}_1$ adaptive controller [84] for the lane-keeping control, which provides rapid disturbance compensation within

the filter bandwidth, while guaranteeing transient and steady-state performance. Different controllers should be designed for different areas because the prior distribution of the cornering stiffness varies by location. The current section provides a controller design for one area s, and the same design procedure can be repeated for all other areas of interest.

Chapter 5.2.1 introduces the $\mathcal{L}_1$ adaptive controller on its nominal system [84]. Chapter 5.2.2 discusses how to transform the error dynamics (Equation (5.2)) to the nominal system for the $\mathcal{L}_1$ adaptive controller using the prior distribution of the cornering stiffness. In particular, the nominal system model for the $\mathcal{L}_1$ adaptive controller is determined by the mean of the prior distribution obtained in Chapter 4, and a 95% confidence interval of the uncertainty bounds. Chapter 5.2.3 provides the design procedure for the $\mathcal{L}_1$ adaptive controller and the velocity for the error dynamics.

5.2.1 $\mathcal{L}_1$ Adaptive Controller

Consider the following system:

$$\begin{aligned} \dot{x}(t) &= A_m x(t) + b_m(w u_{ad}(t) + \theta^\top x(t) + \sigma(t)) \\ y(t) &= c^\top x(t) \qquad x(0) = x_0, \end{aligned} \tag{5.3}$$

where A_m, b_m, and c are known system matrices/vectors, and A_m is Hurwitz. Parameter $w \in \mathbb{R}$ represents the unknown input gain, and the state-dependent uncertainty is represented by $b_m\theta^\top x(t)$, where θ is an unknown vector. The uncertain parameters satisfy Assumption 5.1. The signal $\sigma(t)$ represents the time-varying external disturbance that satisfies Assumption 5.2.

Assumption 5.1 *We have $w \in \Omega = [w_l, w_u]$, and $\theta \in \Theta$, where the bound $[w_l, w_u]$ and convex set Θ are known.*

Assumption 5.2 *The disturbance signal $\sigma(t)$ is continuously differentiable, and the signal and its derivative are uniformly bounded, i.e., $|\sigma(t)| \leq \Delta$, and $|\dot{\sigma}(t)| \leq d_\sigma < \infty$ for $\forall t \geq 0$, where the bounds Δ and d_σ are known.*

The control input $u_{ad}(t)$ is an adaptive controller that consists of state predictor, adaptation law, and low-pass filter. In what follows, we describe the $\mathcal{L}_1$ adaptive controller.

State predictor: The state predictor is given by

$$\dot{\hat{x}}(t) = A_m\hat{x}(t) + b_m(\hat{w}(t)u_{ad}(t) + \hat{\theta}^\top x(t) + \hat{\sigma}(t))$$
$$\hat{y}(t) = c^\top\hat{x}(t) \qquad \hat{x}(0) = \hat{x}_0.$$

Adaptation laws: The adaptation laws are given by:

$$\dot{\hat{w}}(t) = \Gamma Proj(\hat{w}(t), -\tilde{x}^\top(t)Pb_m u_{ad}(t)) \qquad \hat{w}(0) = \hat{w}_0$$
$$\dot{\hat{\theta}}(t) = \Gamma Proj(\hat{\theta}(t), -\tilde{x}^\top(t)Pb_m x(t)) \qquad \hat{\theta}(0) = \hat{\theta}_0$$
$$\dot{\hat{\sigma}}(t) = \Gamma Proj(\hat{\sigma}(t), -\tilde{x}^\top(t)Pb_m) \qquad \hat{\sigma}(0) = \hat{\sigma}_0,$$

where $\tilde{x}(t) = \hat{x}(t) - x(t)$ is the prediction error, and $\Gamma > 0$ is an adaptation gain, $Proj(\cdot,\cdot)$ is the projection operator defined in Definition B.3 in [84]. The projection operator guarantees that each estimate remains in its desired domain. Matrix P is a symmetric positive definite matrix, solving the algebraic Lyapunov equation $A_mP + PA_m^\top = -Q$ for a given symmetric positive definite matrix Q.

Control law: The adaptive control input is designed by

$$u_{ad}(s) = -kD(s)(\hat{\eta}(s) - k_g r(s)),$$

where $\hat{\eta}(t) = \hat{w}(t)u_{ad}(t) + \hat{\theta}^\top(t)x(t) + \hat{\sigma}(t)$ and $k_g = -1/(c^\top A_m^{-1} b_m)$, and $k > 0$ is a constant. The signal $r(s)$ is the Laplace transform of the reference signal, and $D(s)$ is a strictly proper transfer function that leads to a strictly proper stable low-pass filter

$$C(s) = \frac{wkD(s)}{1 + wkD(s)}$$

with $C(0) = 1$. We choose $D(s) = 1/s$ in this paper. We need to choose the controller such that the $\mathcal{L}_1$-norm condition is satisfied: $\|G(s)\|_{\mathcal{L}_1} L < 1$, where $G(s) = H(s)(1-C(s))$, $H(s) = (s\boldsymbol{I} - A_m)^{-1} b_m$, and $L = \max_{\theta \in \Theta} \|\theta\|_1$. Since θ is constant and $D(s) = 1/s$, the $\mathcal{L}_1$-norm condition reduces to

$$A_g = \begin{bmatrix} A_m + b_m \theta^\top & b_m w \\ -k\theta^\top & -kw \end{bmatrix} \tag{5.4}$$

being Hurwitz for all $\theta \in \Theta$ and $w \in \Omega_0$.

5.2.2 System Transformation and Bounds of Uncertainties

The system Equation (5.2) is uncertain, where the system matrices $A(V, C_f, C_r)$ and $b(C_f)$ depend on unknown cornering stiffness C_f and C_r, while A_m and b_m in Equation (5.3) are known. We will use the mean values $\hat{C}_f = \hat{q}_{s_*,k}$ (and $\hat{C}_r = \hat{q}'_{s_*,k}$ for rear cornering stiffness) of the prior distribution to construct uncontrolled nominal system matrices, i.e., $A(V, \hat{C}_f, \hat{C}_r)$ and $b(\hat{C}_f)$. Consider the control input $u = u_m + u_{ad}$, where we will later choose $u_m \triangleq -k_m x$ such that $A_m(V) = A(V, \hat{C}_f, \hat{C}_r) - b_m k_m$ becomes Hurwitz and $b_m \triangleq b(\hat{C}_f)$. Then, the system Equation (5.2) becomes the nominal system Equation (5.3) for

the $\mathcal{L}_1$ adaptive controller, where the following relations approximate the uncertainties:

$$
\begin{aligned}
b(C_f) &= b_m w \\
\theta &= \frac{1}{w} b_m^{\dagger}(A(V, C_f, C_r) - A(V, \hat{C}_f, \hat{C}_r)) + k_m(\frac{1}{w} - 1) \\
\sigma &= b_m^{\dagger} g \dot{p}^{\psi, des}
\end{aligned} \tag{5.5}
$$

with $b_m^{\dagger} = [0, \frac{m}{4\hat{C}_f}, 0, \frac{I_z}{4\hat{C}_f \ell_f}]$.

It is required to approximate the bounds of uncertainties Θ, Ω, Δ, and d_σ to design the $\mathcal{L}_1$ adaptive controller. To provide those sets, we assume that the cornering stiffness's actual value is bounded by its 95% confidence interval of the prior distribution $\mathcal{N}(\hat{C}_f, P^{C_f}) = \mathcal{N}(\hat{q}_{s_*,k}, P^{q}_{s_*,k})$ (or $\mathcal{N}(\hat{C}_r, P^{C_r}) = \mathcal{N}(\hat{q}'_{s_*,k}, P^{q'}_{s_*,k})$ for rear cornering stiffness), i.e., given the prior distributions, we have constants $\underline{C}_f, \bar{C}_f, \underline{C}_r$, and $\bar{C}_r$ that

$$
C_f \in [\underline{C}_f, \bar{C}_f], \; C_r \in [\underline{C}_r, \bar{C}_r]. \tag{5.6}
$$

Assumption 5.3 is a mild condition, because the typical vehicle model satisfies $\ell_r \geq \ell_f$ and $I_z \geq m$, as shown in [69]. In Assumption 5.4, the first condition implies that the road's curve is bounded, and the second condition implies that the change of the curve is bounded.

Assumption 5.3 (Vehicle model) *The vehicle model satisfies $\ell_r \geq \ell_f$ and $I_z \frac{\ell_r}{\ell_f} - m \geq 0$.*

Assumption 5.4 (Radius of road) *We have $R \geq \underline{R}$ and $|\frac{\dot{R}}{R^2}| \leq \bar{R}_d$ for some $\underline{R}, \bar{R}_d > 0$.*

Lemma 5.1 *Consider Assumptions 5.3 and 5.4. Given Equation (5.5) and*

Equation (5.6), the bounds of uncertainties are found by

$$\begin{aligned}
\Omega &= [\frac{\underline{C}_f}{\hat{C}_f}, \frac{\bar{C}_f}{\hat{C}_f}] \\
\Delta(V) &= \frac{1}{2\hat{C}_f \underline{R}}(2\bar{C}_f\ell_f + \bar{C}_r\ell_r(\frac{\ell_r}{\ell_f} - 1) + \frac{mV^2}{2}) \\
d_\sigma(V) &= \frac{\bar{R}_d}{2\hat{C}_f}(2\bar{C}_f\ell_f + \bar{C}_r\ell_r(\frac{\ell_r}{\ell_f} - 1) + \frac{mV^2}{2}) \\
\Theta(V) &= \frac{1}{V}(\Theta_1 \times \Theta_2 \times \Theta_3 \times \Theta_4),
\end{aligned} \tag{5.7}$$

where

$$\begin{aligned}
&\Theta_1 = k_m^{(1)} V\Xi, \quad \Theta_3 = k_m^{(3)} V\Xi \\
&\Theta_2 = [-\frac{(m + I_z)(\bar{C}_f - \hat{C}_f)}{2m\underline{C}_f} + \frac{(I_z\frac{\ell_r}{\ell_f} - m)(\underline{C}_r - \hat{C}_r)}{2m\bar{C}_f}, \\
&\quad - \frac{(m + I_z)(\underline{C}_f - \hat{C}_f)}{2m\bar{C}_f} + \frac{(I_z\frac{\ell_r}{\ell_f} - m)(\bar{C}_r - \hat{C}_r)}{2m\underline{C}_f}] + k_m^{(2)} V\Xi \\
&\Theta_4 = [-\frac{(m + I_z)(\bar{C}_f - \hat{C}_f)}{2m\underline{C}_f} + \frac{(I_z\frac{\ell_r}{\ell_f} - m)(\underline{C}_r - \hat{C}_r)}{2m\bar{C}_f}, \\
&\quad - \frac{(m + I_z)(\underline{C}_f - \hat{C}_f)}{2m\bar{C}_f} + \frac{(I_z\frac{\ell_r}{\ell_f} - m)(\bar{C}_r - \hat{C}_r)}{2m\underline{C}_f}] + k_m^{(4)} V\Xi
\end{aligned} \tag{5.8}$$

and $k_m^{(i)}$ is the i^{th} element of k_m, and $\Xi \triangleq [\frac{\hat{C}_f}{\bar{C}_f} - 1, \frac{\hat{C}_f}{\underline{C}_f} - 1]$.

Proof: The vector b in Equation (5.2) can be reformulated by $b = b_m\frac{C_f}{\hat{C}_f} = b_m w$. Therefore, for any $C_f \in [\underline{C}_f, \bar{C}_f]$, we have

$$w \in \Omega = [\frac{\underline{C}_f}{\hat{C}_f}, \frac{\bar{C}_f}{\hat{C}_f}]. \tag{5.9}$$

The uncertainty θ in Equation (5.5) can be found by

$$\theta = \frac{1}{2Vw}[0, -\frac{(m+I_z)\Delta C_f}{m\hat{C}_f} + \frac{(I_z\frac{\ell_r}{\ell_f} - m)\Delta C_r}{m\hat{C}_f}, 0, \\ -\frac{(m+I_z)\Delta C_f}{m\hat{C}_f} + \frac{(I_z\frac{\ell_r}{\ell_f} - m)\Delta C_r}{m\hat{C}_f}]^\top + k_m(w^{-1} - 1), \tag{5.10}$$

where $\Delta C_f \triangleq C_f - \hat{C}_f$ and $\Delta C_r \triangleq C_r - \hat{C}_r$. Given the bounds of C_f and C_r in Equation (5.6) and that of w in Equation (5.9), the bounds of each element θ_i in Equation (5.10) are found by Equation (5.8), where $I_z\frac{\ell_r}{\ell_f} - m \geq 0$ in Assumption 5.3 has been applied.

Likewise, $\sigma(t)$ in Equation (5.5) is expressed as

$$\sigma = -\frac{1}{2\hat{C}_f R}(2C_f\ell_f + C_r\ell_r(\frac{\ell_r}{\ell_f} - 1) + \frac{mV^2}{2}),$$

and its time-derivative becomes

$$\begin{aligned}\dot{\sigma} &= b_m^\dagger G\frac{\partial \dot{p}^{\psi,des}}{\partial R}\dot{R} \\ &= \frac{\dot{R}}{2\hat{C}_f R^2}(2C_f\ell_f + C_r\ell_r(\frac{\ell_r}{\ell_f} - 1) + \frac{mV^2}{2}).\end{aligned}$$

Since $\frac{\ell_r}{\ell_f} - 1 \geq 0$ by Assumption 5.3, we have $(2C_f\ell_f + C_r\ell_r(\frac{\ell_r}{\ell_f} - 1) + \frac{mV^2}{2}) > 0$. The bounds $R \geq \underline{R}$ and $|\frac{\dot{R}}{R^2}| \leq \bar{R}_d$ hold by Assumption 5.4 and lead to Equation (5.7). □

Notice that the sets $\Theta(V)$, $\Delta(V)$, and $d_\sigma(V)$ are a function of the velocity V.

5.2.3 Nominal Velocity Design

The $\mathcal{L}_1$ adaptive controller guarantees transient and steady-state performance with respect to the reference system and design system. The reference system is the non-adaptive version of the $\mathcal{L}_1$ adaptive controller. The design system is an ideal system that does not depend on the uncertainties. According to Theorem 2.2.2 in [84], the performance of the system can be rendered arbitrarily close to the reference system ($x_{ref}(t)$ and $u_{ref}(t)$) by increasing the adaptation gain Γ without sacrificing robustness. Lemma 2.1.4 in [84] analyzes the error between the reference system and the design system ($\|x_{ref} - x_{des}\|_{\mathcal{L}_\infty}$ and $\|u_{ref} - u_{des}\|_{\mathcal{L}_\infty}$), where its upper bound is proportional to $\|G(s)\|_{\mathcal{L}_1}$. The term $\|G(s)\|_{\mathcal{L}_1}$ can be close to zero by arbitrarily increasing the filter bandwidth k. However, this performance improvement trades off with the robustness. In particular, the time-delay margin decreases to zero, as k increases to infinity. Therefore, we need to design k_m, $C(s)$, and V balancing the performance and robustness optimally.

The matrix $A_m(V)$ must be Hurwitz, but it depends both on gain k_m and velocity V. To relax this complexity, we propose to use the common Lyapunov function approach. We first design control gains k_m and P such that $A_m(V)$ is Hurwitz for any velocity $V \in [V_{\min}, V_{\max}]$, where $V_{\min}$ and $V_{\max}$ are the minimum and maximum velocity of the area, respectively. Since the legal minimum and maximum speed (i.e., speed limits) on specific road traffic are known, we assume that $V_{\min}$ and $V_{\max}$ are known, and $V_{\min} = 0$ if no minimum speed is provided. Upon that, we choose the velocity V and filter $C(s)$ simultaneously through an optimization problem.

Given $\hat{C}_f$ and $\hat{C}_r$, we should choose a constant vector k_m and a symmetric

positive definite matrix P such that

$$A_m(V)P + PA_m^\top(V) < 0 \tag{5.11}$$

holds for all $V_{\min} \leq V \leq V_{\max}$. One does not need to explore the entire domain of V, but only needs to check the minimum $V_{\min}$ and maximum $V_{\max}$.

Lemma 5.2 *Assume that there exists* $0 \leq \alpha(V) \leq 1$ *such that* $A_m(V) = \alpha(V)A_m(V_{\min}) + (1-\alpha(V))A_m(V_{\max})$ *for any* $V_{\min} \leq V \leq V_{\max}$. *Then there exists a positive definite matrix* $Q(V)$ *such that* $A_m(V)P + PA_m^\top(V) = -Q(V)$ *for any* $V_{\min} \leq V \leq V_{\max}$ *if and only if* $A_m(V_{\min})P + PA_m^\top(V_{\min}) = -Q_{\min}$, *and* $A_m(V_{\max})P + PA_m^\top(V_{\max}) = -Q_{\max}$ *for some symmetric positive definite matrices* P, $Q_{\min}$, *and* $Q_{\max}$.

Proof: If $A_m(V)P + PA_m^\top(V) < 0$ for all $V_{\min} \leq V \leq V_{\max}$, it is obvious that the same inequality holds for $V = V_{\min}$ and $V = V_{\max}$.

We prove sufficiency:

$$\begin{aligned}
&A_m(V)P + PA_m^\top(V) \\
&= \alpha(V)(A_m(V_{\min})P + PA_m^\top(V_{\min})) + (1-\alpha(V))(A_m(V_{\max})P + PA_m^\top(V_{\max})) \\
&= -\alpha(V)Q_{\min} - (1-\alpha(V))Q_{\max}.
\end{aligned}$$

Since the right hand side is negative definite, the statement holds with $Q(V) = \alpha(V)Q_{\min} + (1-\alpha(V))Q_{\max}$. □

For any $V \in [V_{\min}, V_{\max}]$, we have

$$A_m(V) = \alpha(V)A_m(V_{\min}) + (1-\alpha(V))A_m(V_{\max})$$

for $\alpha(V) = \frac{\frac{V_{\min}V_{\max}}{V} - V_{\min}}{V_{\max} - V_{\min}}$. Therefore, by Lemma 5.2, we can choose k_m and P such that the condition in Equation (5.11) holds both for $V_{\min}$ and $V_{\max}$. The adaptation gain $\Gamma > 0$ can be chosen as a very large number to enhance the adaptation performance.

We can choose the filter gain k and the velocity V balancing the performance and robustness. The performance is characterized by $\|G(s)\|_{\mathcal{L}_1}$ as in [85]. The robustness is characterized by an upper bound of k, which prevents the time-delay margin from converging to zero. The optimization problem can be formulated by

$$\begin{aligned} &\max_{k,V\in[V_{\min},V_{\max}]} V \\ &s.t.\ \|G(s)\|_{\mathcal{L}_1} \leq \lambda_{gp},\ \text{for } \forall w \in \Omega \\ &\quad k \leq \bar{k} \end{aligned} \tag{5.12}$$

for some constants $\bar{k} > 0$ and $\lambda_{gp} < \frac{1}{L}$. Recall that $G(s) = H(s)(1 - C(s))$. Given λ_{gp}, one could find the performance bounds of $\|x_{ref} - x_{des}\|_{\mathcal{L}_\infty}$ and $\|u_{ref} - u_{des}\|_{\mathcal{L}_\infty}$ in Lemma 7 in [86]. It is worth noticing that all existing performance and stability analyses on the $\mathcal{L}_1$ adaptive controller are still valid. This is because the current chapter designs the controller proactively while applying it with output feedback.

5.2.4 Real-Time Controller Update

It is critically important to ensure that the matrices A_m and A_g are Hurwitz for all possible uncertainties. Given the posterior distribution $\mathcal{N}(\hat{C}_f^{pos}, P^{C_f^{pos}})$ (or $\mathcal{N}(\hat{C}_r^{pos}, P^{C_r^{pos}})$ for rear cornering stiffness) from Kalman filter, we can construct the 95% confidence interval of the posterior distribution of C_f and

C_r. We check online whether $A_g(V)$ is Hurwitz for the new set of uncertainties. If it does not hold, we update k in real-time such that $A_g(V)$ is Hurwitz:

$$k = \arg\min_{k} |k - k_*|$$
$$\text{s.t. } A_g(V) \text{ being Hurwitz, } k \leq \bar{k}$$

where k_* is the current gain. It is worth to note that A_m does not need to be re-tuned, because it depends only on $\hat{C}_f$ and $\hat{C}_r$, and not on the bounds of uncertainties. Furthermore, we design it to be Hurwitz for the entire possible velocity range.

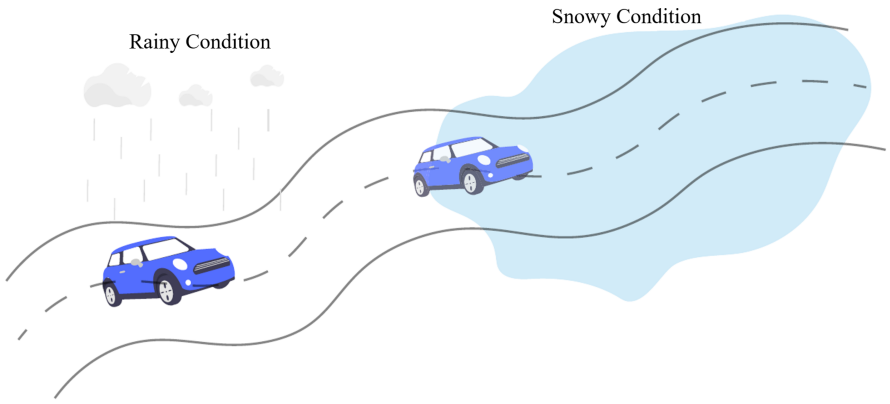


Figure 5.3: Simulation scenarios.

5.3 Simulations

The current section demonstrates the performance of the proposed control architecture. Based on the prior estimate, we design the $\mathcal{L}_1$ adaptive controller for the areas of interest and illustrate the lane keeping performance discussed in Chapter 5.3.1. The specific scenario is depicted in Figure 5.3. Lastly, we show a trend of maximum velocity in Equation (5.12) with respect

to changing nominal cornering stiffness in Chapter 5.3.2.

5.3.1 Proactive Adaptive control

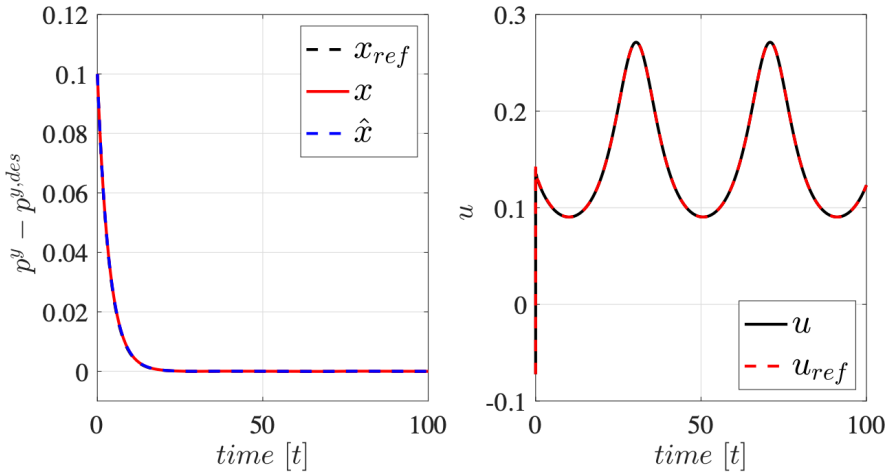


Figure 5.4: Rainy condition. Error states and control inputs in area 1 ($C_{1,f} = C_{1,r} = 51867$).

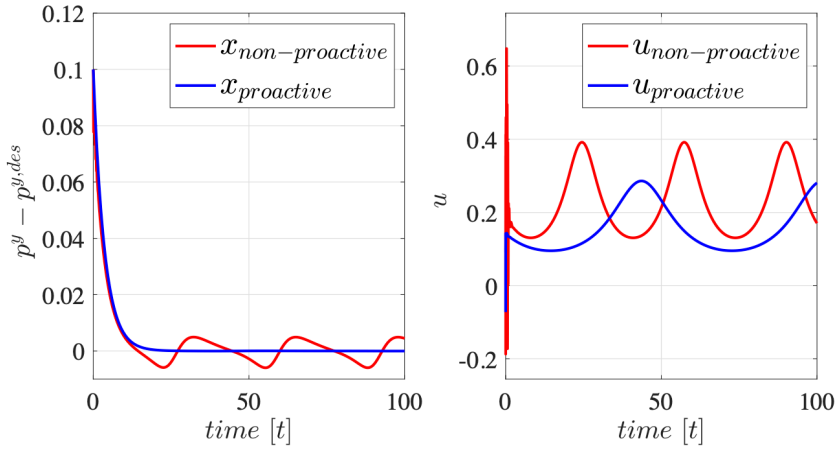


Figure 5.5: Snowy condition. Error states and control inputs in area 2 ($C_{2,f} = C_{2,r} = 23214$).

The current section compares the tracking performance of the proactive $\mathcal{L}_1$ adaptive control and a non-proactive version of it. We refer to [87] to compare the $\mathcal{L}_1$ adaptive controller's performance with that of other types of controllers.

The vehicle's system parameters are as follows [87]: $m = 1573$, $I_z = 2873$, $\ell_f = 1.1$, $\ell_r = 1.58$. To challenge the maneuver, we choose the time-varying radius of the road $R(s) = 15\sin(\frac{1}{120}s) + 30$ for area 1 and area 2, where s is the arc length. The vehicle operates in areas 1 and 2, where the ground truth cornering stiffnesses are $C_{1,f} = C_{1,r} = q_{1,50} = 51867$, and $C_{2,f} = C_{2,r} = q_{2,50} = 23214$ at time $k = 50$. Controllers are designed based on the prior distribution at time $k = 50$, i.e., $q_{1,k} \sim \mathcal{N}(51826, 1413)$ and $q_{2,k} \sim \mathcal{N}(23240, 1937)$. This scenario is depicted in Figure 5.3.

Performance bound is chosen to be $\lambda_{gp} = 0.585$, and $\bar{k} = 10$. Given the performance bound and distributions for areas 1 and 2 in Chapter 4.4, we design the $\mathcal{L}_1$ adaptive controller for areas 1 and 2 as follows:

$$k_{1,m} = k_{2,m} = \begin{bmatrix} 0.7223 & 2.5855 & -0.6669 & 0.1873 \end{bmatrix}^\top,$$

$k_1 = k_2 = 10$, $V_1 = 18.61$, $V_2 = 12.96$, $\Gamma_1 = \Gamma_2 = 100000$,

$$P_1 = \begin{bmatrix} 1.9111 & 0.0053 & 0.3485 & 0.0090 \\ 0.0053 & 0.0196 & -0.0052 & -0.0294 \\ 0.3485 & -0.0052 & 5.2183 & 0.0438 \\ 0.0090 & -0.0294 & 0.0438 & 0.0543 \end{bmatrix},$$

and

$$P_2 = \begin{bmatrix} 1.9064 & 0.0180 & 0.4485 & 0.0483 \\ 0.0180 & 0.0636 & -0.0211 & -0.0928 \\ 0.4485 & -0.0211 & 3.9649 & 0.1609 \\ 0.0483 & -0.0928 & 0.1609 & 0.1834 \end{bmatrix}.$$

For a comparison, we also consider the non-proactive controller for area 2

designed using $k_{np,m} = k_{2,m}$, $k_{np} = k_2$, $V_{np} = 22.96$, $\Gamma_{np} = \Gamma_2$, and

$$P_{np} = \begin{bmatrix} 1.9195 & 0.0153 & 0.3201 & 0.0119 \\ 0.0153 & 0.0360 & 0.0095 & -0.0532 \\ 0.3201 & 0.0095 & 8.0706 & 0.0908 \\ 0.0119 & -0.0532 & 0.0908 & 0.1015 \end{bmatrix}.$$

Figure 5.4 presents the performance of the proactively designed $\mathcal{L}_1$ adaptive controller under the rainy condition ($C_{1,f} = C_{1,r} = 51867$). The controller can successfully stabilize the error dynamics under the changing road radius. With a large adaptation gain, the system performance is arbitrarily close to that of the reference system.

Figure 5.5 compares the proactive $\mathcal{L}_1$ adaptive controller's tracking performance and the non-proactive version under the snowy condition and changing road radius. The system with the proactive controller does not have performance degradation compared to operation in the rainy condition. We found that the non-proactive controller designed for dry road conditions (around $C_f = C_r = 80000$) failed to stabilize the system. As discussed before, one could increase k to guarantee stability, but this will harm the robustness. To illustrate the performance difference between the proactive controller and non-proactive controller without increasing k, we consider the controller designed for $C_f = C_r = 60000$. The non-proactive controller could also stabilize the error dynamics through compensation of uncertainties, but presents a relatively large error, when the vehicle operates outside of its nominal status.

5.3.2 Vehicle Velocity Curve

We study a trend of maximum velocity chosen by the optimization problem in Equation (5.12). The control parameters, performance bound, and the bound of k remain unchanged throughout the range of cornering stiffness for a fair comparison. The maximum velocity decreases as the nominal cornering stiffness decreases, as shown in Figure 5.6. The proposed control architecture slows down the vehicle in advance to guarantee the desired performance and robustness, when the road is expected to be slippery from the prior estimate.

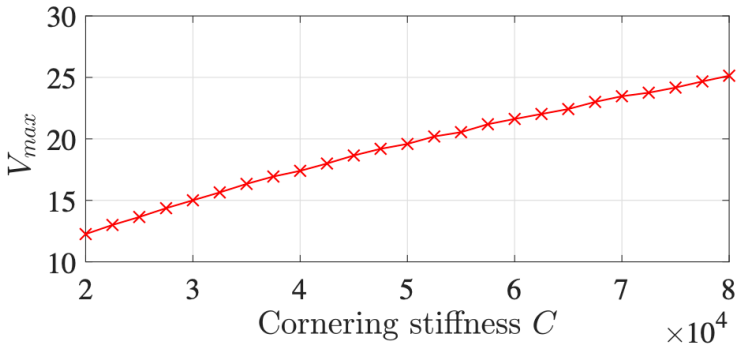


Figure 5.6: Velocity designed by Equation (5.12) with respect to changing nominal cornering stiffness $\hat{C}_f = \hat{C}_r$.

Chapter 6

Interval Estimation under Uncertainties

6.1 Positive System and Problem Formulation

Positive systems Consider the following system

$$\begin{aligned} \boldsymbol{x}_{k+1} &= \boldsymbol{A}_k \boldsymbol{x}_k + \boldsymbol{B}_k \boldsymbol{u}_k \\ \boldsymbol{y}_k &= \boldsymbol{C}_k \boldsymbol{x}_k, \end{aligned} \tag{6.1}$$

where $\boldsymbol{x}_k$, $\boldsymbol{u}_k$ and $\boldsymbol{y}_k$ are the state, control input and system output, respectively.

Definition 6.1 (Positive system) *The system in Equation (6.1) is a positive system if for every positive initial condition and control input, i.e.* $\boldsymbol{x}_0 \geq 0$ *and* $\boldsymbol{u}_0 \geq 0$*, the state and the system output are positive, i.e.* $\boldsymbol{x}_k \geq 0$ *and* $\boldsymbol{y}_k \geq 0$ $\forall k \in \mathbb{Z}^+$.

Definition 6.2 (Nonnegative matrix) *The matrix* $\boldsymbol{A}$ *is a nonnegative matrix if all of its elements* a_{ij} *are equal to or greater than zero, i.e.* $a_{ij} \geq 0$ $\forall i, j$.

Theorem 6.1 (Theorem 2.6 in [88]) *The system in Equation (6.1) is a positive system if* $\boldsymbol{A}_k$, $\boldsymbol{B}_k$, $\boldsymbol{C}_k$ *and* $\boldsymbol{D}_k$ *are nonnegative matrices.*

Consider the following system:

$$\begin{aligned} \boldsymbol{x}_{k+1} &= \boldsymbol{A}_k \boldsymbol{x}_k + \boldsymbol{B}_k \boldsymbol{u}_k + \boldsymbol{\omega}_k \\ \boldsymbol{y}_k &= \boldsymbol{C}_k \boldsymbol{x}_k + \boldsymbol{\nu}_k, \end{aligned} \tag{6.2}$$

where $\boldsymbol{x}_k \in \mathcal{X} \subseteq \mathbb{R}^n$, $\boldsymbol{u}_k \in \mathcal{U} \subseteq \mathbb{R}^p$ and $\boldsymbol{y}_k \in \mathbb{R}^m$ are the system state, the control input and the system output, respectively. The matrices $\boldsymbol{A}_k$, $\boldsymbol{B}_k$ and $\boldsymbol{C}_k$ are known. Noises $\boldsymbol{\omega}_k \in \mathbb{R}^n$ and $\boldsymbol{\nu}_k \in \mathbb{R}^m$ are unknown, but they are element-wise bounded by the known constant vectors, i.e., $\underline{\boldsymbol{w}} \leq \boldsymbol{\omega}_k \leq \overline{\boldsymbol{w}}$ and $\underline{\boldsymbol{v}} \leq \boldsymbol{\nu}_k \leq \overline{\boldsymbol{v}}$.

Problem Statement 6.1 *Consider the system in Equation (6.2). The objective of the interval estimation design is to recursively estimate the upper bounds and lower bounds of the ground truth state, i.e. to obtain an interval vector* $[\overline{\boldsymbol{x}}_k, \underline{\boldsymbol{x}}_k]$ *that contains* $\boldsymbol{x}_k$

$$\underline{\boldsymbol{x}}_k \leq \boldsymbol{x}_k \leq \overline{\boldsymbol{x}}_k$$

for all $k \in \mathbb{Z}^+$.

6.2 Algorithm Design

State prediction and estimation

Given the previous bounds of the system state $\overline{\boldsymbol{x}}_{k-1}$ and $\underline{\boldsymbol{x}}_{k-1}$, we predict the bounds of the state by

$$\begin{aligned} \overline{\boldsymbol{x}}_k^* &= \boldsymbol{A}_{k-1} \overline{\boldsymbol{x}}_{k-1} + \boldsymbol{B}_{k-1} \boldsymbol{u}_{k-1} + \overline{\boldsymbol{w}} \\ \underline{\boldsymbol{x}}_k^* &= \boldsymbol{A}_{k-1} \underline{\boldsymbol{x}}_{k-1} + \boldsymbol{B}_{k-1} \boldsymbol{u}_{k-1} + \underline{\boldsymbol{w}}. \end{aligned} \tag{6.3}$$

Then the state estimation is induced by utilizing the output $\boldsymbol{y}_k$ to correct the prediction in Equation (6.3) as follows:

$$\begin{aligned}\overline{\boldsymbol{x}}_k &= \overline{\boldsymbol{x}}_k^* + \overline{\boldsymbol{L}}_k(\boldsymbol{y}_k - \boldsymbol{C}_k\overline{\boldsymbol{x}}_k^* - \overline{\boldsymbol{v}}) \\ \underline{\boldsymbol{x}}_k &= \underline{\boldsymbol{x}}_k^* + \underline{\boldsymbol{L}}_k(\boldsymbol{y}_k - \boldsymbol{C}_k\underline{\boldsymbol{x}}_k^* - \underline{\boldsymbol{v}}),\end{aligned} \tag{6.4}$$

where gain matrices $\overline{\boldsymbol{L}}_k$ and $\underline{\boldsymbol{L}}_k$ will be selected later.

Positive error dynamics

To ensure the state and the uncertainty are bounded by Equation (6.4) is equivalent to requiring the estimation errors

$$\begin{aligned}\overline{\boldsymbol{e}}_k^x &\triangleq \overline{\boldsymbol{x}}_k - \boldsymbol{x}_k \\ \underline{\boldsymbol{e}}_k^x &\triangleq \boldsymbol{x}_k - \underline{\boldsymbol{x}}_k\end{aligned} \tag{6.5}$$

to be nonnegative for $\forall k \in \mathbb{Z}^+$, i.e. to be positive systems. The following lemma states the conditions such that the error dynamics are positive systems.

Assumption 6.1 *Assume* $\overline{\boldsymbol{e}}_0^x, \underline{\boldsymbol{e}}_0^x \geq 0$.

Lemma 6.1 (State Estimation) *Under Assumption 6.1, the ground truth of the state is bounded by Equation (6.4), i.e.* $\underline{\boldsymbol{x}}_k \leq \boldsymbol{x}_k \leq \overline{\boldsymbol{x}}_k$ $\forall k \in \mathbb{Z}^+$, *if the*

following conditions hold

$$(\boldsymbol{I} - \overline{\boldsymbol{L}}_k \boldsymbol{C}_k)\boldsymbol{A}_{k-1} \geq 0 \tag{6.6}$$

$$(\boldsymbol{I} - \underline{\boldsymbol{L}}_k \boldsymbol{C}_k)\boldsymbol{A}_{k-1} \geq 0 \tag{6.7}$$

$$(\boldsymbol{I} - \overline{\boldsymbol{L}}_k \boldsymbol{C}_k) \geq 0 \tag{6.8}$$

$$(\boldsymbol{I} - \underline{\boldsymbol{L}}_k \boldsymbol{C}_k) \geq 0 \tag{6.9}$$

$$-\overline{\boldsymbol{L}}_k \geq 0 \tag{6.10}$$

$$-\underline{\boldsymbol{L}}_k \geq 0. \tag{6.11}$$

Proof: The upper bound of the error dynamics $\overline{\boldsymbol{e}}_k^x$ is given by

$$\begin{aligned}\overline{\boldsymbol{e}}_k^x =& \boldsymbol{A}_{k-1}\overline{\boldsymbol{e}}_{k-1}^x + \overline{\boldsymbol{e}}_{k-1}^w \overline{\boldsymbol{L}}_k(\boldsymbol{C}_k\boldsymbol{A}_{k-1}\overline{\boldsymbol{e}}_{k-1}^x + \boldsymbol{C}_k\overline{\boldsymbol{e}}_{k-1}^w + \overline{\boldsymbol{e}}_k^v) \\ =& (\boldsymbol{I} - \overline{\boldsymbol{L}}_k\boldsymbol{C}_k)\boldsymbol{A}_{k-1}\overline{\boldsymbol{e}}_{k-1}^x + (\boldsymbol{I} - \overline{\boldsymbol{L}}_k\boldsymbol{C}_k)\overline{\boldsymbol{e}}_{k-1}^w - \overline{\boldsymbol{L}}_k\overline{\boldsymbol{e}}_k^v. \end{aligned} \tag{6.12}$$

We have $\overline{\boldsymbol{e}}_k^x \geq 0$ since the conditions in Equations (6.6), (6.8) and (6.10) hold. The statement $\underline{\boldsymbol{e}}_k^x \geq 0$ can be proven by a similar procedure. Therefore we have $\underline{\boldsymbol{x}}_k \leq \boldsymbol{x}_k \leq \overline{\boldsymbol{x}}_k \ \forall k \in \mathbb{Z}^+$. □

The gain matrices $\overline{\boldsymbol{L}}_k$ and $\underline{\boldsymbol{L}}_k$ are selected such that the upper bound is minimized and the lower bound is maximized:

$$\begin{aligned}&\min_{\overline{\boldsymbol{L}}_k \leq 0} \|\overline{\boldsymbol{x}}_k\| \\ &\textit{subject to } (6.6), (6.8)\end{aligned} \tag{6.13}$$

$$\begin{aligned}&\max_{\underline{\boldsymbol{L}}_k \leq 0} \|\underline{\boldsymbol{x}}_k\| \\ &\textit{subject to } (6.7), (6.9).\end{aligned} \tag{6.14}$$

Optimization problems in Equations (6.13) and (6.14) are linear programming (LP) problems, which can be solved efficiently.

6.3 Simulation Results

This simulation study compares the performance and efficiency of three interval estimation algorithms, i.e. the proposed approach, interval observer [89], and set-membership method [90]. Considering a DC servo motor described in [91], we use the same dynamic model and parameters used in [90]. The interval estimations of the motor speed n_{motor} by the aforementioned algorithms are shown in Figure 6.1. It shows that the proposed approach is more accurate than the interval observer and has similar accuracy as the set-membership method. In addition, the performance comparison including the running time and the averaged estimation width ($\frac{\sum \overline{n}_{motor} - \underline{n}_{motor}}{40}$) is provided in Table 6.1, which demonstrates the reliability and efficiency of the proposed approach.

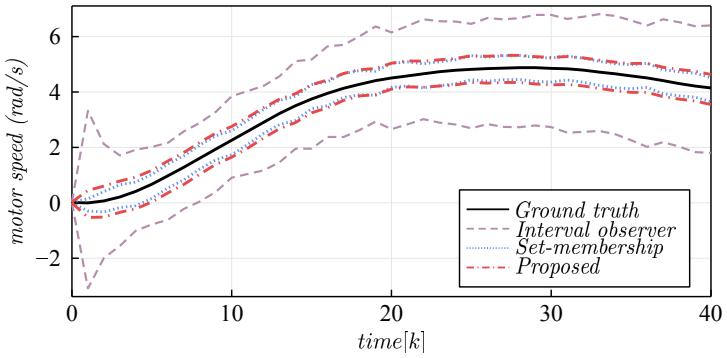


Figure 6.1: Comparison of interval estimation algorithms.

Table 6.1: Performance comparison.

Algorithm	Time (s)	Estimation width (rad/s)
Proposed	**0.880**	**1.003**
Interval observer	1.283	3.693
Set-membership	12.399	0.852

6.4 Extension

This section extends the approach to the discrete-time system with model uncertainties:

$$\begin{aligned} \boldsymbol{x}_{k+1} &= \underbrace{\boldsymbol{A}_k\boldsymbol{x}_k + \boldsymbol{B}_k\boldsymbol{u}_k}_{\textit{a priori model}} + \underbrace{f(\boldsymbol{x}_k, \boldsymbol{u}_k)}_{\textit{model uncertainty}} + \boldsymbol{\omega}_k \\ \boldsymbol{y}_k &= \boldsymbol{C}_k\boldsymbol{x}_k + \boldsymbol{\nu}_k, \end{aligned} \tag{6.15}$$

where $\boldsymbol{x}_k \in \mathcal{X} \subseteq \mathbb{R}^n$, $\boldsymbol{u}_k \in \mathcal{U} \subseteq \mathbb{R}^p$ and $\boldsymbol{y}_k \in \mathbb{R}^m$ are the system state, the control input and the system output, respectively. The matrices $\boldsymbol{A}_k$, $\boldsymbol{B}_k$ and $\boldsymbol{C}_k$ are known. The *unknown* nonlinear function $f : \mathcal{X} \times \mathcal{U} \to \mathcal{F} \subseteq \mathbb{R}^n$ represents the model uncertainty. Noises $\boldsymbol{\omega}_k \in \mathbb{R}^n$ and $\boldsymbol{\nu}_k \in \mathbb{R}^m$ are unknown, but they are element-wise bounded by the known constant vectors, i.e. $\underline{\boldsymbol{w}} \leq \boldsymbol{\omega}_k \leq \overline{\boldsymbol{w}}$ and $\underline{\boldsymbol{v}} \leq \boldsymbol{\nu}_k \leq \overline{\boldsymbol{v}}$. Note that the we have no further assumptions on $\mathcal{F}$, which allows $\mathcal{F}$ to represent an arbitrarily large model uncertainty set. At time k, we assume that the upper bound and the lower bound of the previous state estimates $\overline{\boldsymbol{x}}_{k-1}$ and $\underline{\boldsymbol{x}}_{k-1}$ are given.

Remark 6.1 *The proposed method can be applied to a wide class of systems because of the large uncertainty setup. The apriori model required in Equation (6.15) can be a rough model.*

6.4.1 Unknown Dynamics Estimation

We can obtain the posterior bounds by the updating laws as follows:

$$\begin{aligned} \overline{\boldsymbol{g}}_{k-1} &= \overline{\boldsymbol{M}}_k\big(\boldsymbol{y}_k - \boldsymbol{C}_k\overline{\boldsymbol{x}}_k^p - \overline{\boldsymbol{v}}\big) \\ \underline{\boldsymbol{g}}_{k-1} &= \underline{\boldsymbol{M}}_k\big(\boldsymbol{y}_k - \boldsymbol{C}_k\underline{\boldsymbol{x}}_k^p - \underline{\boldsymbol{v}}\big), \end{aligned} \tag{6.16}$$

where

$$\begin{aligned} \overline{\boldsymbol{x}}_k^p &\triangleq \boldsymbol{A}_{k-1}\overline{\boldsymbol{x}}_{k-1} + \boldsymbol{B}_{k-1}\boldsymbol{u}_{k-1} + \overline{\boldsymbol{w}} \\ \underline{\boldsymbol{x}}_k^p &\triangleq \boldsymbol{A}_{k-1}\underline{\boldsymbol{x}}_{k-1} + \boldsymbol{B}_{k-1}\boldsymbol{u}_{k-1} + \underline{\boldsymbol{w}} \end{aligned} \tag{6.17}$$

are the prior bounds of the state. The gain matrices $\overline{\boldsymbol{M}}_k$ and $\underline{\boldsymbol{M}}_k$ in Equation (6.16) will be selected later.

6.4.2 State Prediction and Estimation

Given the posterior bounds of the unknown dynamics $\overline{\boldsymbol{g}}_{k-1}$ and $\underline{\boldsymbol{g}}_{k-1}$, we predict the bounds of the state by

$$\begin{aligned} \overline{\boldsymbol{x}}_k^* &= \boldsymbol{A}_{k-1}\overline{\boldsymbol{x}}_{k-1} + \boldsymbol{B}_{k-1}\boldsymbol{u}_{k-1} + \overline{\boldsymbol{g}}_{k-1} + \overline{\boldsymbol{w}} \\ \underline{\boldsymbol{x}}_k^* &= \boldsymbol{A}_{k-1}\underline{\boldsymbol{x}}_{k-1} + \boldsymbol{B}_{k-1}\boldsymbol{u}_{k-1} + \underline{\boldsymbol{g}}_{k-1} + \underline{\boldsymbol{w}}. \end{aligned} \tag{6.18}$$

Then the state estimation is induced by utilizing the output $\boldsymbol{y}_k$ to correct the prediction in Equation (6.18) as follows:

$$\begin{aligned} \overline{\boldsymbol{x}}_k &= \overline{\boldsymbol{x}}_k^* + \overline{\boldsymbol{L}}_k(\boldsymbol{y}_k - \boldsymbol{C}_k\overline{\boldsymbol{x}}_k^* - \overline{\boldsymbol{v}}) \\ \underline{\boldsymbol{x}}_k &= \underline{\boldsymbol{x}}_k^* + \underline{\boldsymbol{L}}_k(\boldsymbol{y}_k - \boldsymbol{C}_k\underline{\boldsymbol{x}}_k^* - \underline{\boldsymbol{v}}), \end{aligned} \tag{6.19}$$

where gain matrices $\overline{\boldsymbol{L}}_k$ and $\underline{\boldsymbol{L}}_k$ will be selected later.

6.4.3 Positive Error Dynamics

To ensure the state and the uncertainty are bounded by Equation (6.19) and (6.16) is equivalent to requiring the estimation errors

$$\begin{aligned} \overline{\boldsymbol{e}}_k^x &\triangleq \overline{\boldsymbol{x}}_k - \boldsymbol{x}_k \\ \underline{\boldsymbol{e}}_k^x &\triangleq \boldsymbol{x}_k - \underline{\boldsymbol{x}}_k \end{aligned} \tag{6.20}$$

and

$$\begin{aligned} \overline{\boldsymbol{e}}_k^g &\triangleq \overline{\boldsymbol{g}}_k - \boldsymbol{g}_k \\ \underline{\boldsymbol{e}}_k^g &\triangleq \boldsymbol{g}_k - \underline{\boldsymbol{g}}_k \end{aligned} \tag{6.21}$$

to be nonnegative for $\forall k \in \mathbb{Z}^+$, i.e. to be positive systems. The following lemmas state the conditions such that the error dynamics are positive systems.

Assumption 6.2 *Assume* $\overline{\boldsymbol{e}}_0^x, \underline{\boldsymbol{e}}_0^x \geq 0$.

Lemma 6.2 (Uncertainty Estimation) *Consider Assumption 6.2 and assume that* $\overline{\boldsymbol{e}}_k^x, \underline{\boldsymbol{e}}_k^x \geq 0 \ \forall k \in \mathbb{Z}^+$. *Then the uncertainty* $\boldsymbol{g}_{k-1}$ *is bounded by Equation (6.16), i.e.*

$$\underline{\boldsymbol{g}}_{k-1} \leq \boldsymbol{g}_{k-1} \leq \overline{\boldsymbol{g}}_{k-1} \tag{6.22}$$

for all $k \in \mathbb{Z}^+$*, if the following conditions hold*

$$-\overline{\boldsymbol{M}}_k \boldsymbol{C}_k \boldsymbol{A}_{k-1} \geq 0 \tag{6.23}$$

$$-\underline{\boldsymbol{M}}_k \boldsymbol{C}_k \boldsymbol{A}_{k-1} \geq 0 \tag{6.24}$$

$$-\overline{\boldsymbol{M}}_k \boldsymbol{C}_k \geq 0 \tag{6.25}$$

$$-\underline{\boldsymbol{M}}_k \boldsymbol{C}_k \geq 0 \tag{6.26}$$

$$-\overline{\boldsymbol{M}}_k \geq 0 \tag{6.27}$$

$$-\underline{\boldsymbol{M}}_k \geq 0. \tag{6.28}$$

Proof: The proof of Equation (6.22) is equivalent to showing that the bounds of the error dynamics in Equation (6.21) are nonnegative

$$\overline{\boldsymbol{e}}^g_{k-1} \geq 0 \ \textit{and} \ \underline{\boldsymbol{e}}^g_{k-1} \geq 0. \tag{6.29}$$

The upper bound of the error dynamics $\overline{\boldsymbol{e}}^g_{k-1}$ can be described by

$$\begin{aligned} \overline{\boldsymbol{e}}^g_{k-1} &= -\overline{\boldsymbol{M}}_k (\boldsymbol{C}_k \boldsymbol{A}_{k-1} \overline{\boldsymbol{e}}^x_{k-1} + \boldsymbol{C}_k \overline{\boldsymbol{e}}^w_{k-1} + \overline{\boldsymbol{e}}^v_k) \\ &= -\overline{\boldsymbol{M}}_k \boldsymbol{C}_k \boldsymbol{A}_{k-1} \overline{\boldsymbol{e}}^x_{k-1} - \overline{\boldsymbol{M}}_k (\boldsymbol{C}_k \overline{\boldsymbol{e}}^w_{k-1} + \overline{\boldsymbol{e}}^v_k), \end{aligned} \tag{6.30}$$

where $\overline{\boldsymbol{e}}^w_{k-1} \triangleq \overline{\boldsymbol{w}} - \boldsymbol{\omega}_{k-1}$, and $\overline{\boldsymbol{e}}^v_k \triangleq \overline{\boldsymbol{v}} - \boldsymbol{\nu}_k$.

Since the conditions in Equations (6.23), (6.25) and (6.27) hold, all three terms in Equation (6.30) are nonnegative, i.e. $\overline{\boldsymbol{e}}^g_{k-1} \geq 0$. The statement $\underline{\boldsymbol{e}}^g_{k-1} \geq 0$ can be proven by a similar procedure, which is omitted here. Therefore we have Equation (6.29), which completes the proof. □

Remark 6.2 *Lemma 6.2 holds under the assumption of the nonnegativity of bounds of the state error dynamics. The following Lemma 6.3 demonstrates the nonnegativity of* $\overline{\boldsymbol{e}}^x_k$ *and* $\underline{\boldsymbol{e}}^x_k$*.*

Lemma 6.3 (State Estimation) *Under Assumption 6.2, the ground truth of the state is bounded by Equation (6.19), i.e.* $\underline{\boldsymbol{x}}_k \leq \boldsymbol{x}_k \leq \overline{\boldsymbol{x}}_k \ \forall k \in \mathbb{Z}^+$, *if the following conditions hold*

$$(\boldsymbol{I} - \overline{\boldsymbol{M}}_k \boldsymbol{C}_k)(\boldsymbol{I} - \overline{\boldsymbol{L}}_k \boldsymbol{C}_k)\boldsymbol{A}_{k-1} \geq 0 \tag{6.31}$$

$$(\boldsymbol{I} - \underline{\boldsymbol{M}}_k \boldsymbol{C}_k)(\boldsymbol{I} - \underline{\boldsymbol{L}}_k \boldsymbol{C}_k)\boldsymbol{A}_{k-1} \geq 0 \tag{6.32}$$

$$-(\boldsymbol{I} - \overline{\boldsymbol{M}}_k \boldsymbol{C}_k)\overline{\boldsymbol{L}}_k \geq 0 \tag{6.33}$$

$$-(\boldsymbol{I} - \underline{\boldsymbol{M}}_k \boldsymbol{C}_k)\underline{\boldsymbol{L}}_k \geq 0 \tag{6.34}$$

$$-\overline{\boldsymbol{L}}_k \geq 0 \tag{6.35}$$

$$-\underline{\boldsymbol{L}}_k \geq 0. \tag{6.36}$$

Proof: The upper bound of the error dynamics $\overline{\boldsymbol{e}}_k^x$ is given by

$$\begin{aligned}\overline{\boldsymbol{e}}_k^x =& \boldsymbol{A}_{k-1}\overline{\boldsymbol{e}}_{k-1}^x + \overline{\boldsymbol{e}}_{k-1}^g + \overline{\boldsymbol{e}}_{k-1}^w \overline{\boldsymbol{L}}_k(\boldsymbol{C}_k\boldsymbol{A}_{k-1}\overline{\boldsymbol{e}}_{k-1}^x + \boldsymbol{C}_k\overline{\boldsymbol{e}}_{k-1}^g + \boldsymbol{C}_k\overline{\boldsymbol{e}}_{k-1}^w + \overline{\boldsymbol{e}}_k^v) \\ =& (\boldsymbol{I} - \overline{\boldsymbol{L}}_k\boldsymbol{C}_k)\boldsymbol{A}_{k-1}\overline{\boldsymbol{e}}_{k-1}^x + (\boldsymbol{I} - \overline{\boldsymbol{L}}_k\boldsymbol{C}_k)\overline{\boldsymbol{e}}_{k-1}^g + (\boldsymbol{I} - \overline{\boldsymbol{L}}_k\boldsymbol{C}_k)\overline{\boldsymbol{e}}_{k-1}^w - \overline{\boldsymbol{L}}_k\overline{\boldsymbol{e}}_k^v.\end{aligned} \tag{6.37}$$

Plugging Equation (6.30) into Equation (6.37), we have

$$\begin{aligned}\overline{\boldsymbol{e}}_k^x =& (\boldsymbol{I} - \overline{\boldsymbol{L}}_k\boldsymbol{C}_k)\boldsymbol{A}_{k-1}\overline{\boldsymbol{e}}_{k-1}^x + (\boldsymbol{I} - \overline{\boldsymbol{L}}_k\boldsymbol{C}_k)\overline{\boldsymbol{e}}_{k-1}^g + (\boldsymbol{I} - \overline{\boldsymbol{L}}_k\boldsymbol{C}_k)\overline{\boldsymbol{e}}_{k-1}^w - \overline{\boldsymbol{L}}_k\overline{\boldsymbol{e}}_k^v \\ =& (\boldsymbol{I} - \overline{\boldsymbol{L}}_k\boldsymbol{C}_k)(\boldsymbol{I} - \overline{\boldsymbol{M}}_k\boldsymbol{C}_k)\boldsymbol{A}_{k-1}\overline{\boldsymbol{e}}_{k-1}^x \\ &+ (\boldsymbol{I} - \overline{\boldsymbol{L}}_k\boldsymbol{C}_k)(\boldsymbol{I} - \overline{\boldsymbol{M}}_k\boldsymbol{C}_k)\overline{\boldsymbol{e}}_{k-1}^w - (\boldsymbol{I} - \overline{\boldsymbol{L}}_k\boldsymbol{C}_k)\overline{\boldsymbol{M}}_k\overline{\boldsymbol{e}}_k^v - \overline{\boldsymbol{L}}_k\overline{\boldsymbol{e}}_k^v.\end{aligned} \tag{6.38}$$

We have $\overline{\boldsymbol{e}}_k^x \geq 0$ since the conditions in Equations (6.31), (6.33) and (6.35) hold. The statement $\underline{\boldsymbol{e}}_k^x \geq 0$ can be proven by a similar procedure. Therefore we have $\underline{\boldsymbol{x}}_k \leq \boldsymbol{x}_k \leq \overline{\boldsymbol{x}}_k \ \forall k \in \mathbb{Z}^+$. □

To ensure the error dynamics is a positive system, gain matrices should

be selected under the constraints stated in Lemma 6.3. On top of this, gain matrices $\overline{\boldsymbol{M}}_k$ and $\underline{\boldsymbol{M}}_k$ are selected such that the upper bound is minimized and the lower bound is maximized:

$$\begin{aligned} &\min_{\overline{\boldsymbol{M}}_k \leq 0} \|\overline{\boldsymbol{g}}_{k-1}\| \\ &\textit{subject to } (6.23), (6.25) \end{aligned} \tag{6.39}$$

$$\begin{aligned} &\max_{\underline{\boldsymbol{M}}_k \leq 0} \|\underline{\boldsymbol{g}}_{k-1}\| \\ &\textit{subject to } (6.24), (6.26). \end{aligned} \tag{6.40}$$

Likewise, given $\overline{\boldsymbol{M}}_k$ and $\underline{\boldsymbol{M}}_k$, the gain matrices $\overline{\boldsymbol{L}}_k$ and $\underline{\boldsymbol{L}}_k$ are selected such that the upper bound is minimized and the lower bound is maximized:

$$\begin{aligned} &\min_{\overline{\boldsymbol{L}}_k \leq 0} \|\overline{\boldsymbol{x}}_k\| \\ &\textit{subject to } (6.31), (6.33) \end{aligned} \tag{6.41}$$

$$\begin{aligned} &\max_{\underline{\boldsymbol{L}}_k \leq 0} \|\underline{\boldsymbol{x}}_k\| \\ &\textit{subject to } (6.32), (6.34). \end{aligned} \tag{6.42}$$

Optimization problems in Equations (6.39) to (6.42) are linear programming (LP) problems, which can be solved efficiently.

Lemma 6.4 *Feasible sets for linear programming (LP) problems in Equations (6.39) to (6.42) are nonempty.*

We omit the proof of this lemma because it is trivial to show that the zero matrix is always in the feasible sets.

Algorithm 3 Interval estimation for uncertainty and state

Require: learning (GP) prediction $\overline{\boldsymbol{g}}_{k-1}^{p}$ and $\underline{\boldsymbol{g}}_{k-1}^{p}$, measurement $\boldsymbol{y}_k$

▷ State priori

1: Obtain $\overline{\boldsymbol{M}}_k$ and $\underline{\boldsymbol{M}}_k$ by solving LP problems in Equations (6.39) and (6.40);

2: $[\overline{\boldsymbol{x}}_k^p, \underline{\boldsymbol{x}}_k^p] \leftarrow$ STATE PRIORI as in Equation (6.17);

▷ Uncertainty posterior

3: $[\overline{\boldsymbol{g}}_{k-1}, \underline{\boldsymbol{g}}_{k-1}] \leftarrow$ UNCERTAINTY POSTERIOR as in Equation (6.16);

▷ State prediction

4: $[\overline{\boldsymbol{x}}_k^*, \underline{\boldsymbol{x}}_k^*] \leftarrow$ STATE PREDICTION as in Equation (6.18);

▷ State estimation

5: Obtain $\overline{\boldsymbol{L}}_k$ and $\underline{\boldsymbol{L}}_k$ by solving LP problems Equations (6.41) and (6.42);

6: $[\overline{\boldsymbol{x}}_k, \underline{\boldsymbol{x}}_k] \leftarrow$ STATE ESTIMATION as in Equation (6.19);

Remark 6.3 *It is worth to note that the proposed algorithm has a less restrictive assumption than that in [92], where there must be a set of observable states which are free of unknown inputs all the time.*

Remark 6.4 *Optimization problems in Equations (6.39) to (6.42) minimize the impact of external disturbances and the error propagation from the previous state estimate. The cost function is not unique. For example, we may choose $\ell_\infty - \ell_\infty$ observer which minimizes the impact of external disturbances $\boldsymbol{\omega}_k$ and $\boldsymbol{\nu}_k$ as in [93].*

Remark 6.5 *Positive systems constitute a remarkable class of systems and receive increasing attention and appear frequently in practical applications [88, 94, 95]. While we only assume the error dynamics to be a positive system, the original system does not need to be a positive system. But if it is a positive system, the LP problems in Equations (6.39) to (6.42) can be simplified, as in Chapter 6.4.4.*

6.4.4 Interval Estimation for Positive Systems

Given that the system (Equation (6.15)) is a positive system, i.e. $\boldsymbol{A}_k, \boldsymbol{B}_k, \boldsymbol{C}_k \geq 0$, Algorithm 3 can be simplified, as stated in the following Corollary 6.1.

Corollary 6.1 *Consider Assumption 6.2 and assume that* $\boldsymbol{A}_k, \boldsymbol{B}_k, \boldsymbol{C}_k \geq 0$. *Then the uncertainty* $\boldsymbol{g}_{k-1}$ *is bounded by Equation (6.16) and the state is bounded by Equation (6.19), i.e.*

$$\underline{\boldsymbol{g}}_{k-1} \leq \boldsymbol{g}_{k-1} \leq \overline{\boldsymbol{g}}_{k-1}$$
$$\underline{\boldsymbol{x}}_k \leq \boldsymbol{x}_k \leq \overline{\boldsymbol{x}}_k$$

for all $k \in \mathbb{Z}^+$, *if the following conditions hold*

$$\boldsymbol{I} - \overline{\boldsymbol{M}}_k \boldsymbol{C}_k \geq 0 \tag{6.43}$$
$$\boldsymbol{I} - \underline{\boldsymbol{M}}_k \boldsymbol{C}_k \geq 0 \tag{6.44}$$
$$-\overline{\boldsymbol{M}}_k \geq 0 \tag{6.45}$$
$$-\underline{\boldsymbol{M}}_k \geq 0 \tag{6.46}$$
$$\boldsymbol{I} - \overline{\boldsymbol{L}}_k \boldsymbol{C}_k \geq 0 \tag{6.47}$$
$$\boldsymbol{I} - \underline{\boldsymbol{L}}_k \boldsymbol{C}_k \geq 0 \tag{6.48}$$
$$-\overline{\boldsymbol{L}}_k \geq 0 \tag{6.49}$$
$$-\underline{\boldsymbol{L}}_k \geq 0. \tag{6.50}$$

Proof: Under the assumptions of this corollary, all the conditions in Lemmas 6.2 and 6.3 hold. By Lemma 6.3, the statement holds. □

In this case, the LP problems in Equations (6.39) to (6.42) are simplified

as follows:

$$\min_{\overline{\boldsymbol{M}}_k \leq 0} \overline{\boldsymbol{g}}_{k-1} \quad \textit{subject to } (6.43) \tag{6.51}$$

$$\max_{\underline{\boldsymbol{M}}_k \leq 0} \underline{\boldsymbol{g}}_{k-1} \quad \textit{subject to } (6.44) \tag{6.52}$$

$$\min_{\overline{\boldsymbol{L}}_k \leq 0} \overline{\boldsymbol{x}}_k \quad \textit{subject to } (6.47) \tag{6.53}$$

$$\max_{\underline{\boldsymbol{L}}_k \leq 0} \underline{\boldsymbol{x}}_k \quad \textit{subject to } (6.48). \tag{6.54}$$

Correspondingly, Lines 1 and 5 in Algorithm 3 can be replaced by the above stated simpler optimization problems in Equations (6.51) to (6.54).

Chapter 7

Conclusions and Future Research

This dissertation studied a framework for cyber-physical systems (CPS) that allows safe operation under significant uncertainties, such as malicious attacks, unforeseen environments, and model uncertainties. Chapter 2 introduced a case study of GPS spoofing attacks. We proposed a safety constrained control framework that adapts the UAV at a path re-planning level to support resilient state estimation against GPS spoofing attacks. Using the estimates of the attacker' s location obtained by the UKF with sliding window outputs, an optimal escape controller is designed based on the constrained MPC such that the UAV escapes from the effective range of the spoofing device within a safe time. The framework has been extended to multi-UAV systems for time-critical coordination tasks. In Chapter 3, we designed a constrained attack-resilient estimation algorithm (`CARE`) that can simultaneously estimate the compromised system states and attack signals. The proposed `CARE` has improved estimation accuracy and attack detection performance after projection induced by inequality constraints. To the best of our knowledge, we are the first to investigate the stability of the estimation algorithm with inequality constraints and prove that the estimation errors are practically exponentially stable in mean square. In Chapter 4, we developed a proactive robust adaptive control architecture for autonomous vehicles' lane-keeping control problems to deal with unforeseen environments in advance. The data center estimates an environmental factor by synthesiz-

ing weather forecasts and measurements from anonymous vehicles through FRRF, a spatio-temporal filter. The estimates contribute in Chapter 5, where we provided the systematic proactive-design procedure for the $\mathcal{L}_1$ robust adaptive controller for lateral vehicle control and nominal longitudinal velocity design for proactive adaptation to each area of interest. Chapter 6 presented a novel interval state estimation method. The bounds can be efficiently found through a linear programming formulation. We empirically showed the performance of the proposed interval state estimation algorithm by comparing it to others. We extended the method to a class of systems with a large uncertainty setup. We have investigated several resilient estimation algorithms, including resilient state estimation, UKF with sliding window outputs, resilient interval estimation, constrained attack-resilient estimation, and fixed rank resilient filter. Then we utilized these resilient estimation algorithms to support safe control designs for autonomous vehicles.

While the research in this dissertation attempts to achieve safe operation for CPS under significant uncertainties by integrating resilient estimation and safe control, many open questions are left for further research and development. We list possible extensions and future directions as follows.

- In Chapter 3, we proposed a constrained attack-resilient estimation algorithm that induces improved attack detection performance in terms of false negative rate. Due to the improved estimation accuracy, a better false positive rate is also expected. Providing rigorous analysis of the false positive rate is one of the possible extensions. The algorithm is designed for linear time-varying stochastic systems subject to linear inequality constraints. If the target system is nonlinear, the linearization of the system is required. One needs to investigate how linearization errors affect estimation and attack detection performances. Furthermore,

we are interested in developing another constrained attack-resilient estimation algorithm for nonlinear systems. One possible approach is to deal with the nonlinearity through sample-based filtering techniques.

- The proactive control architecture proposed in Chapter 5 enables a good tracking performance by designing the heading angle and nominal longitudinal velocity. However, regenerating the reference trajectory for the $\mathcal{L}_1$ controller to follow might be necessary since the road condition has changed. Extending the current proactive control architecture with a high-level motion planner would be practical. The tentative approach could be i) at the proactive level, developing a model predictive controller based on the future road conditions estimated by FRRF; ii) at the reactive level, designing the $\mathcal{L}_1$ controller to compensate for the measured errors resulting from the proactive level.
- Recent years have seen tremendous efforts in integrating artificial intelligence (AI) with control theory to establish unified frameworks for safe CPS. The interval resilient estimation method proposed in Chapter 6 can be extended to a machine learning framework. Learning errors can destabilize the system, and unexpected system behaviors may also affect the performance of learning. The resilient interval estimation can be utilized to correct the prediction from learning [96]. The proposed estimation and machine learning framework will open various new research directions: i) the machine learning-based reachability audit for backup model predictive control ([97]), ii) the spatio-temporal filtering on vehicle-to-cloud (V2C) communication and proactive control framework (proposed in Chapters 4 and 5) for adversarial cloud data [98], and iii) robust AI-based perception certificates for obstacle detection in bad weather with uncertainty quantification.

References

[1] R. M. Lee, M. J. Assante, and T. Conway, "German steel mill cyber attack," *Industrial Control Systems*, vol. 30, p. 22, 2014.

[2] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," in *Springer International Conference on Eritical Infrastructure Protection*, pp. 73–82, 2007.

[3] R. Langner, "Stuxnet: Dissecting a cyber warfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[4] S. Peterson and P. Faramarzi, "Iran hijacked US drone, says Iranian engineer," *Christian Science Monitor*, vol. 15, 2011.

[5] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, *et al.*, "Experimental security analysis of a modern automobile," in *IEEE Symposium on Security and Privacy*, pp. 447–462, 2010.

[6] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *USENIX Security Symposium*, vol. 4, pp. 447–462, 2011.

[7] P. P. Marra, C. J. Dove, R. Dolbeer, N. F. Dahlan, M. Heacker, J. F. Whatton, N. E. Diggs, C. France, and G. A. Henkes, "Migratory Canada geese cause crash of US airways flight 1549," *Frontiers in Ecology and the Environment*, vol. 7, no. 6, pp. 297–301, 2009.

[8] J. Raiyn, "A survey of cyber attack detection strategies," *International Journal of Security and Its Applications*, vol. 8, no. 1, pp. 247–256, 2014.

[9] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *28th International Conference on Distributed Computing Systems Workshops*, pp. 495–500, 2008.

[10] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[11] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proceedings of the 1st international conference on High Confidence Networked Systems*, pp. 55–64, 2012.

[12] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[13] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, "Robustness of attack-resilient state estimators," in *ACM/IEEE International Conference on Cyber-Physical Systems*, pp. 163–174, 2014.

[14] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[15] M. Pajic, I. Lee, and G. J. Pappas, "Attack-resilient state estimation for noisy dynamical systems," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 82–92, 2017.

[16] M. Naghnaeian, N. H. Hirzallah, and P. G. Voulgaris, "Security via multirate control in cyber–physical systems," *Systems & Control Letters*, vol. 124, pp. 12–18, 2019.

[17] N. H. Hirzallah, P. G. Voulgaris, and N. Hovakimyan, "On the estimation of signal attacks: A dual rate SD control framework," in *IEEE European Control Conference (ECC)*, pp. 4380–4385, 2019.

[18] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 21–32, 2011.

[19] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *47th Annual Allerton Conference on Communication, Control, and Computing*, pp. 911–918, 2009.

[20] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, 2014.

[21] S. Z. Yong, M. Zhu, and E. Frazzoli, "Resilient state estimation against switching attacks on stochastic cyber-physical systems," in *IEEE Conference on Decision and Control (CDC)*, pp. 5162–5169, 2015.

[22] N. Forti, G. Battistelli, L. Chisci, and B. Sinopoli, "A Bayesian approach to joint attack detection and resilient state estimation," in *IEEE Conference on Decision and Control (CDC)*, pp. 1192–1198, 2016.

[23] H. Kim, P. Guo, M. Zhu, and P. Liu, "Simultaneous input and state estimation for stochastic nonlinear systems with additive unknown inputs," *Automatica*, vol. 111, p. 108588, 2020.

[24] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *IEEE Conference on Decision and Control (CDC)*, pp. 5991–5998, 2010.

[25] D. Simon and T. L. Chia, "Kalman filtering with state equality constraints," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 38, no. 1, pp. 128–136, 2002.

[26] S. Ko and R. R. Bitmead, "State estimation for linear systems with state equality constraints," *Automatica*, vol. 43, no. 8, pp. 1363–1368, 2007.

[27] D. Simon, "Kalman filtering with state constraints: A survey of linear and nonlinear algorithms," *IET Control Theory & Applications*, vol. 4, no. 8, pp. 1303–1318, 2010.

[28] H. Kong, M. Shan, S. Sukkarieh, T. Chen, and W. X. Zheng, "Kalman filtering under unknown inputs and norm constraints," *Automatica*, vol. 133, p. 109871, 2021.

[29] A. I. Mourikis and S. I. Roumeliotis, "A multi-state constraint Kalman filter for vision-aided inertial navigation," in *IEEE International Conference on Robotics and Automation (ICRA)*, pp. 3565–3572, 2007.

[30] L.-S. Wang, Y.-T. Chiang, and F.-R. Chang, "Filtering method for nonlinear systems with constraints," *IEEE Proceedings-Control Theory and Applications*, vol. 149, no. 6, pp. 525–531, 2002.

[31] S. Z. Yong, M. Zhu, and E. Frazzoli, "Simultaneous input and state estimation of linear discrete-time stochastic systems with input aggregate information," in *IEEE Conference on Decision and Control (CDC)*, pp. 461–467, 2015.

[32] S. H. Kafash, J. Giraldo, C. Murguia, A. A. Cardenas, and J. Ruths, "Constraining attacker capabilities through actuator saturation," in *IEEE American Control Conference (ACC)*, pp. 986–991, 2018.

[33] S. M. Djouadi, A. M. Melin, E. M. Ferragut, J. A. Laska, J. Dong, and A. Drira, "Finite energy and bounded actuator attacks on cyber-physical systems," in *IEEE European Control Conference (ECC)*, pp. 3659–3664, 2015.

[34] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, 2020.

[35] C. Constantinides and P. Parkinson, "Security challenges in uav development," in *2008 IEEE/AIAA 27th Digital Avionics Systems Conference*, pp. 1–C, IEEE, 2008.

[36] G. de Carvalho Bertoli, L. A. Pereira, and O. Saotome, "Classification of denial of service attacks on Wi-Fi-based unmanned aerial vehicle," in *2021 10th Latin-American Symposium on Dependable Computing (LADC)*, pp. 1–6, IEEE, 2021.

[37] E. Deligne, "Ardrone corruption," *Journal in Computer Virology*, vol. 8, no. 1, pp. 15–27, 2012.

[38] T. Krajník, V. Vonásek, D. Fišer, and J. Faigl, "AR-drone as a platform for robotic research and education," in *International conference on research and education in robotics*, pp. 172–186, Springer, 2011.

[39] P. Paganini, "A hacker developed Maldrone, the first malware for drones," *Securityaffairs. co (cit. 2020-11-1)*, 2015.

[40] E. McMilin, D. S. De Lorenzo, T. Walter, T. H. Lee, and P. Enge, "Single antenna GPS spoof detection that is simple, static, instantaneous and backwards compatible for aerial applications," in *Proceedings of the 27th international technical meeting of the satellite division of the institute of navigation, Tampa, FL*, pp. 2233–2242, Citeseer, 2014.

[41] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proceedings of the International Technical Meeting of The Institute of Navigation*, pp. 124–130, 2009.

[42] J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," *Journal of applied research and technology*, vol. 13, no. 1, pp. 45–57, 2015.

[43] Y.-H. Chen, "A study of geometry and commercial off-the-shelf (COTS) antennas for controlled reception pattern antenna (CRPA) arrays," in *Proceedings of ION GNSS*, pp. 907–914, 2012.

[44] Y.-H. Chen, S. Lo, D. M. Akos, D. S. De Lorenzo, and P. Enge, "Validation of a controlled reception pattern antenna (CRPA) receiver built from inexpensive general-purpose elements during several live-jamming test campaigns," in *Proceedings of the International Technical Meeting of The Institute of Navigation, San Diego, California*, pp. 154–163, 2013.

[45] K. Jansen and C. Pöpper, "Advancing attacker models of satellite-based localization systems: the case of multi-device attackers," in *Proceedings*

of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 156–159, 2017.

[46] H. T. Friis, "A note on a simple transmission formula," *Proceedings of the IRE*, vol. 34, pp. 254–256, May 1946.

[47] H.-J. Yoon, W. Wan, H. Kim, N. Hovakimyan, L. Sha, and P. G. Voulgaris, "Towards resilient UAV: Escape time in GPS denied environment with sensor drift," *IFAC-PapersOnLine*, vol. 52, no. 12, pp. 423–428, 2019.

[48] S. J. Julier and J. K. Uhlmann, "New extension of the Kalman filter to nonlinear systems," in *Signal processing, sensor fusion, and target recognition VI*, vol. 3068, pp. 182–193, International Society for Optics and Photonics, 1997.

[49] E. A. Wan and R. Van Der Merwe, "The unscented Kalman filter for nonlinear estimation," in *IEEE Adaptive Systems for Signal Processing, Communications, and Control Symposium (Cat. No. 00EX373)*, pp. 153–158, 2000.

[50] D. Van Hessem and O. Bosgra, "A conic reformulation of model predictive control including bounded and stochastic disturbances under state and input constraints," in *IEEE Conference on Decision and Control (CDC)*, vol. 4, pp. 4643–4648, 2002.

[51] J. Köhler, R. Soloperto, M. A. Müller, and F. Allgöwer, "A computationally efficient robust model predictive control framework for uncertain nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 66, no. 2, pp. 794–801, 2020.

[52] H. Schlüter and F. Allgöwer, "A constraint-tightening approach to nonlinear stochastic model predictive control for systems under general disturbances," *arXiv preprint arXiv:1912.01946*, 2019.

[53] S. S. Ge and Y. J. Cui, "New potential functions for mobile robot path planning," *IEEE Transactions on robotics and automation*, vol. 16, no. 5, pp. 615–620, 2000.

[54] R. Olfati-Saber, "Flocking for multi-agent dynamic systems: algorithms and theory," *IEEE Transactions on Automatic Control*, vol. 51, no. 3, pp. 401–420, 2006.

[55] H. M. Choset, S. Hutchinson, K. M. Lynch, G. Kantor, W. Burgard, L. E. Kavraki, and S. Thrun, *Principles of robot motion: theory, algorithms, and implementation*. MIT press, 2005.

[56] M. T. Wolf and J. W. Burdick, "Artificial potential functions for highway driving with collision avoidance," in *IEEE International Conference on Robotics and Automation*, pp. 3731–3736, 2008.

[57] I. Dunning, J. Huchette, and M. Lubin, "Jump: A modeling language for mathematical optimization," *SIAM Review*, vol. 59, no. 2, pp. 295–320, 2017.

[58] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[59] M. Mesbahi and M. Egerstedt, *Graph Theoretic Methods in Multiagent Networks*, vol. 33. Princeton University Press, 2010.

[60] R. H. Bartels, J. C. Beatty, and B. A. Barsky, *An Introduction to Splines for Use in Computer Graphics and Geometric Modelling*. Morgan Kaufmann, 1995.

[61] S. Z. Yong, M. Zhu, and E. Frazzoli, "A unified filter for simultaneous input and state estimation of linear discrete-time stochastic systems," *Automatica*, vol. 63, pp. 321–329, 2016.

[62] H. Kim, P. Guo, M. Zhu, and P. Liu, "Attack-resilient estimation of switched nonlinear cyber-physical systems," in *IEEE American Control Conference (ACC)*, pp. 4328–4333, 2017.

[63] P. Guo, H. Kim, N. Virani, J. Xu, M. Zhu, and P. Liu, "Roboads: Anomaly detection against sensor and actuator misbehaviors in mobile robots," in *48th Annual IEEE/IFIP international conference on dependable systems and networks (DSN)*, pp. 574–585, 2018.

[64] B. O. Teixeira, J. Chandrasekar, L. A. Tôrres, L. A. Aguirre, and D. S. Bernstein, "State estimation for linear and non-linear equality-constrained systems," *International Journal of Control*, vol. 82, no. 5, pp. 918–936, 2009.

[65] B. D. Anderson and J. B. Moore, "Detectability and stabilizability of time-varying discrete-time linear-systems," *SIAM Journal on Control and Optimization*, vol. 19, no. 1, pp. 20–32, 1981.

[66] S. Kluge, K. Reif, and M. Brokate, "Stochastic stability of the extended Kalman filter with intermittent observations," *IEEE Transactions on Automatic Control*, vol. 55, no. 2, pp. 514–518, 2010.

[67] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*. Tata McGraw-Hill Education, 2002.

[68] D. J. Tylavsky and G. R. Sohie, "Generalization of the matrix inversion lemma," *Proceedings of the IEEE*, vol. 74, no. 7, pp. 1050–1052, 1986.

[69] R. Rajamani, *Vehicle dynamics and control*. Springer Science & Business Media, 2011.

[70] C. K. Law, D. Dalal, and S. Shearrow, "Robust model predictive control for autonomous vehicles/self driving cars," *arXiv preprint arXiv:1805.08551*, 2018.

[71] T. L. Lai, "Sequential changepoint detection in quality control and dynamical systems," *Journal of the Royal Statistical Society. Series B (Methodological)*, pp. 613–658, 1995.

[72] G. Evensen, *Data assimilation: the ensemble Kalman filter*. Springer Science & Business Media, 2009.

[73] B. R. Hunt, E. J. Kostelich, and I. Szunyogh, "Efficient data assimilation for spatiotemporal chaos: A local ensemble transform Kalman filter," *Physica D: Nonlinear Phenomena*, vol. 230, no. 1-2, pp. 112–126, 2007.

[74] N. Cressie, T. Shi, and E. L. Kang, "Fixed rank filtering for spatio-temporal data," *Journal of Computational and Graphical Statistics*, vol. 19, no. 3, pp. 724–745, 2010.

[75] H. Nguyen, M. Katzfuss, N. Cressie, and A. Braverman, "Spatio-temporal data fusion for very large remote sensing datasets," *Technometrics*, vol. 56, no. 2, pp. 174–185, 2014.

[76] S. Gillijns and B. De Moor, "Unbiased minimum-variance input and state estimation for linear discrete-time systems," *Automatica*, vol. 43, no. 1, pp. 111–116, 2007.

[77] W. Wan, H. Kim, N. Hovakimyan, and P. G. Voulgaris, "Attack-resilient estimation for linear discrete-time stochastic systems with input and state constraints," in *IEEE Conference on Decision and Control (CDC)*, pp. 5107–5112, 2019.

[78] W. Wan, H. Kim, N. Hovakimyan, and P. Voulgaris, "Constrained attack-resilient estimation of stochastic cyber-physical systems," *arXiv preprint arXiv:2109.12255*, 2021.

[79] K. Reif, S. Gunther, E. Yaz, and R. Unbehauen, "Stochastic stability of the discrete-time extended Kalman filter," *IEEE Transactions on Automatic control*, vol. 44, no. 4, pp. 714–728, 1999.

[80] S. Bonnabel and J.-J. Slotine, "A contraction theory-based analysis of the stability of the deterministic extended Kalman filter," *IEEE Transactions on Automatic Control*, vol. 60, no. 2, pp. 565–569, 2014.

[81] M. K. Kwong and P. P. Tang, "W-matrices, nonorthogonal multiresolution analysis, and finite signals of arbitrary length," Tech. Rep. No. ANL/MCS/CP-84114; CONF-9407170-1, Argonne National Lab., IL, 1994.

[82] P. Falcone, F. Borrelli, J. Asgari, H. E. Tseng, and D. Hrovat, "Predictive active steering control for autonomous vehicle systems," *IEEE Transactions on Control Systems Technology*, vol. 15, no. 3, pp. 566–580, 2007.

[83] A. Carvalho, Y. Gao, S. Lefevre, and F. Borrelli, "Stochastic predictive control of autonomous vehicles in uncertain environments," in *12th International Symposium on Advanced Vehicle Control*, pp. 712–719, 2014.

[84] N. Hovakimyan and C. Cao, $\mathcal{L}_1$ *Adaptive Control Theory: Guaranteed Robustness with Fast Adaptation*. SIAM, 2010.

[85] D. Li, N. Hovakimyan, C. Cao, and K. Wise, "Filter design for feedback-loop trade-off of $\mathcal{L}_1$ adaptive controller: A linear matrix inequality approach," in *AIAA Guidance, Navigation and Control Conference and Exhibit*, p. 6280, 2008.

[86] C. Cao and N. Hovakimyan, "Design and analysis of a novel $\mathcal{L}_1$ adaptive control architecture with guaranteed transient performance," *IEEE Transactions on Automatic Control*, vol. 53, no. 2, pp. 586–591, 2008.

[87] M. M. Shirazi and A. B. Rad, "$\mathcal{L}_1$ adaptive control of vehicle lateral dynamics," *IEEE Transactions on Intelligent Vehicles*, vol. 3, no. 1, pp. 92–101, 2017.

[88] T. Kaczorek, *Positive 1D and 2D systems*. Springer Science & Business Media, 2012.

[89] D. Efimov and T. Raïssi, "Design of interval observers for uncertain dynamical systems," *Automation and Remote Control*, vol. 77, no. 2, pp. 191–225, 2016.

[90] W. Tang, Z. Wang, Y. Wang, T. Raïssi, and Y. Shen, "Interval estimation methods for discrete-time linear time-invariant systems," *IEEE Transactions on Automatic Control*, vol. 64, no. 11, pp. 4717–4724, 2019.

[91] M. Buciakowski, M. Witczak, M. Mrugalski, and D. Theilliol, "A quadratic boundedness approach to robust dc motor fault estimation," *Control Engineering Practice*, vol. 66, pp. 181–194, 2017.

[92] E. I. Robinson, J. Marzat, and T. Raïssi, "Interval observer design for unknown input estimation of linear time-invariant discrete-time systems," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 4021–4026, 2017.

[93] C. Briat and M. Khammash, "Interval peak-to-peak observers for continuous-and discrete-time systems with persistent inputs and delays," *Automatica*, vol. 74, pp. 206–213, 2016.

[94] R. Shorten, F. Wirth, and D. Leith, "A positive systems model of tcp-like congestion control: asymptotic results," *IEEE/ACM transactions on networking*, vol. 14, no. 3, pp. 616–629, 2006.

[95] L. Farina and S. Rinaldi, *Positive linear systems: theory and applications*, vol. 50. John Wiley & Sons, 2011.

[96] W. Wan, H. Kim, and N. Hovakimyan, "Towards trustworthy autonomy: Reliable and efficient interval estimation and learning for robust model predictive control," *AAAI Conference on Artificial Intelligence Workshop on Trustworthy Autonomous Systems Engineering*, 2022.

[97] H. Kim, H. Yoon, W. Wan, N. Hovakimyan, L. Sha, and P. Voulgaris, "Backup plan constrained model predictive control," in *IEEE Conference on Decision and Control (CDC)*, pp. 289–294, 2021.

[98] J. Yang, H. Kim, W. Wan, N. Hovakimyan, and Y. Vorobeychik, "Certified robust control under adversarial perturbations," in *IEEE American Control Conference (ACC)*, 2023 (Submitted).

[99] A. H. Sayed, *Fundamentals of adaptive filtering*. John Wiley & Sons, 2003.

Appendix A

Chi-square Tests for Attack Detection

χ^2 test. The χ^2 test is widely used in attack detection for stochastic systems [24, 20]. Given a sample of Gaussian random variable $\hat{\boldsymbol{\sigma}}_k$ with unknown mean $\boldsymbol{\sigma}_k$ and known covariance $\boldsymbol{\Sigma}_k$, the χ^2 test provides statistical evidence of whether $\boldsymbol{\sigma}_k = 0$ or not. In particular, the sample $\hat{\boldsymbol{\sigma}}_k$ is being normalized by $\hat{\boldsymbol{\sigma}}_k^\top \boldsymbol{\Sigma}_k^{-1} \hat{\boldsymbol{\sigma}}_k$, and we compare the normalized value with $\chi^2_{df}(\alpha)$, where $\chi^2_{df}(\alpha)$ is the χ^2 value with degree of freedom df and statistical significance level α. We reject the null hypothesis H_0: $\boldsymbol{\sigma}_k = 0$, if $\hat{\boldsymbol{\sigma}}_k^\top \boldsymbol{\Sigma}_k^{-1} \hat{\boldsymbol{\sigma}}_k > \chi^2_{df}(\alpha)$, and accept alternative hypothesis H_1: $\boldsymbol{\sigma}_k \neq 0$, i.e., there is significant statistical evidence that $\boldsymbol{\sigma}_k$ is non-zero. Otherwise, we accept H_0, i.e., there is no significant evidence that $\boldsymbol{\sigma}_k$ is non-zero.

False negative rate. Given a set of vectors $\{\boldsymbol{\sigma}_k\}$, the false negative rate of the χ^2 test is defined as the ratio of the number of false negative test results N_{neg} and the number of non-zero vectors in the given set $N_{\boldsymbol{\sigma}_k \neq 0}$

$$F_{neg}(\{\hat{\boldsymbol{\sigma}}_k\}, \{\boldsymbol{\Sigma}_k\}) \triangleq \frac{N_{neg}}{N_{\boldsymbol{\sigma}_k \neq 0}} = \frac{\sum_k (\mathbf{1}_k)}{N_{\boldsymbol{\sigma}_k \neq 0}}, \tag{A.1}$$

where

$$\mathbf{1}_k \triangleq \begin{cases} 1, & \textit{if } \hat{\boldsymbol{\sigma}}_k^\top \boldsymbol{\Sigma}_k^{-1} \hat{\boldsymbol{\sigma}}_k \leq \chi^2_{df}(\alpha) \textit{ and } \boldsymbol{\sigma}_k \neq 0 \\ 0, & \textit{otherwise} \end{cases}. \tag{A.2}$$

Appendix B

UKF with Sliding Window Outputs

Algorithm Derivation. Without losing the generality, we consider the following partially nonlinear systems

$$\boldsymbol{x}_{k+1} = \boldsymbol{A}_k \boldsymbol{x}_k + \boldsymbol{w}_k \tag{B.1a}$$

$$\boldsymbol{y}_k = f(\boldsymbol{x}_k) + \boldsymbol{v}_k, \tag{B.1b}$$

where f is a nonlinear function of the system state $\boldsymbol{x}_k$. The noise signals $\boldsymbol{w}_k$ and $\boldsymbol{v}_k$ are assumed to be independent and identically distributed Gaussian random variables with zero means and covariances $\mathbb{E}[\boldsymbol{w}_k(\boldsymbol{w}_k)^\top] = \boldsymbol{\Sigma}_w \geq 0$ and $\mathbb{E}[\boldsymbol{v}_k \boldsymbol{v}_k^\top] = \boldsymbol{\Sigma}_v > 0$.

Prediction. Given the previous state estimate $\hat{\boldsymbol{x}}_{k-1}$ and system model Equation (B.1), the current state can be predicted as

$$\hat{\boldsymbol{x}}_{k|k-1} = \boldsymbol{A}_{k-1} \hat{\boldsymbol{x}}_{k-1}.$$

Its error covariance matrix is

$$\begin{aligned} \boldsymbol{P}_{k|k-1} &\triangleq \mathbb{E}[(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_{k|k-1})(\boldsymbol{x}_k - \hat{\boldsymbol{x}}_{k|k-1})^\top] \\ &= \boldsymbol{A}_{k-1} \boldsymbol{P}_{k-1} \boldsymbol{A}_{k-1}^\top + \boldsymbol{\Sigma}_w, \end{aligned}$$

where $\boldsymbol{P}_{k-1} \triangleq \mathbb{E}[(\boldsymbol{x}_{k-1} - \hat{\boldsymbol{x}}_{k-1})(\boldsymbol{x}_{k-1} - \hat{\boldsymbol{x}}_{k-1})^\top]$ is the state estimation error covariance matrix.

Sigma Points Generation. We define a sigma points array

$$\mathcal{X}_k \triangleq \{\hat{\boldsymbol{x}}_{k|k-1} \pm (\sqrt{n\boldsymbol{P}_{k|k-1}})_i^\top, i = 1, \cdots, n\},$$

where $\sqrt{n\boldsymbol{P}_{k|k-1}}$ is the matrix square root such that $\sqrt{n\boldsymbol{P}_{k|k-1}}^\top \sqrt{n\boldsymbol{P}_{k|k-1}} = n\boldsymbol{P}_{k|k-1}$, and the matrix operator $(\cdot)_i$ gives the i^{th} row of the matrix.

Measurement Update. Given the sliding window size M, the nonlinear measurement equation $f(\cdot)$ is used to transform the sigma points into predicted measurement vectors

$$\begin{aligned}
\hat{\boldsymbol{y}}_k^i &= f(\mathcal{X}_k^i) \\
\hat{\boldsymbol{y}}_{k-1}^i &= f(\boldsymbol{A}_{k-1}^{-1}\mathcal{X}_k^i) \\
&\vdots \\
\hat{\boldsymbol{y}}_{k-N+1}^i &= f(\boldsymbol{A}_{k-1}^{-M+1}\mathcal{X}_k^i).
\end{aligned}$$

We define $\hat{\mathbf{y}}_k^i \triangleq [\hat{\boldsymbol{y}}_k^i, \cdots, \hat{\boldsymbol{y}}_{k-M+1}^i]^\top$, then the approximated mean of the measurements is

$$\bar{\mathbf{y}}_k \triangleq \sum_{i=0}^{2n} \boldsymbol{W}_k^i \hat{\mathbf{y}}_k^i,$$

where $\boldsymbol{W}_k^i$ are the weighting coefficients.

By taking the measurement noise into account, the estimated covariance of the predicted measurements is given by:

$$\mathbf{P}_k^y \triangleq \sum_{i=0}^{2n} \boldsymbol{W}_k^i (\hat{\mathbf{y}}_k^i - \bar{\mathbf{y}}_k)(\hat{\mathbf{y}}_k^i - \bar{\mathbf{y}}_k)^\top + \boldsymbol{\Sigma}_{\boldsymbol{v}},$$

where $\boldsymbol{\Sigma}_{\boldsymbol{v}} = \text{diag}\{\boldsymbol{\Sigma}_v, \cdots, \boldsymbol{\Sigma}_v\}$ is the diagonal matrix.

The cross covariance between the state prediction and predicted measure-

ments is

$$\mathbf{P}_k^{xy} = \sum_{i=0}^{2n} \boldsymbol{W}_k^i (\mathcal{X}_k^i - \hat{\boldsymbol{x}}_{k|k-1})(\hat{\mathbf{y}}_k^i - \bar{\mathbf{y}}_k)^\top,$$

where $\mathcal{X}_k^i$ denotes the i^{th} element in $\mathcal{X}_k$.

The measurement $\mathbf{y}_k \triangleq [\boldsymbol{y}_k, \cdots, \boldsymbol{y}_{k-M+1}]^\top$ is used to update the prediction $\hat{x}_{k|k-1}$ as

$$\hat{\boldsymbol{x}}_k = \hat{\boldsymbol{x}}_{k|k-1} + \boldsymbol{K}_k(\mathbf{y}_k - \bar{\mathbf{y}}_k).$$

The covariance matrix of the state estimation error is

$$\boldsymbol{P}_k = \boldsymbol{P}_{k|k-1} - \boldsymbol{K}_k(\mathbf{P}_k^{xy})^\top - \mathbf{P}_k^{xy}\boldsymbol{K}_k^\top + \boldsymbol{K}_k\mathbf{P}_k^y\boldsymbol{K}_k^\top.$$

The gain matrix $\boldsymbol{K}_k$ is chosen by minimizing the trace norm of $\boldsymbol{P}_k$, i.e. $\min_{\boldsymbol{K}_k} \operatorname{tr}(\boldsymbol{P}_k)$. The solution of the program is given by $\boldsymbol{K}_k = \mathbf{P}_k^{xy}(\mathbf{P}_k^y)^{-1}$. Note that the prediction step does not need unscented transformation because the dynamic system Equation (B.1a) is linear. The UKF with sliding window outputs algorithm is summarized in Algorithm 4.

Algorithm 4 UKF with sliding window outputs

▷ Prediction

$\hat{\boldsymbol{x}}_{k|k-1} = \boldsymbol{A}_{k-1}\hat{\boldsymbol{x}}_{k-1}$;

$\boldsymbol{P}_{k|k-1} = \boldsymbol{A}_{k-1}\boldsymbol{P}_{k-1}\boldsymbol{A}_{k-1}^{\top} + \boldsymbol{\Sigma}_w$;

▷ Sigma points generation

$\mathcal{X}_k = \{\hat{\boldsymbol{x}}_{k|k-1} \pm (\sqrt{n\boldsymbol{P}_{k|k-1}})_i^{\top}\},\ i \in \{1, \cdots, n\}$;

▷ Measurement Update

for $i = 1 : 2n$ **do**

$$\hat{\mathbf{y}}_k^i \triangleq [\hat{\boldsymbol{y}}_k^i, \hat{\boldsymbol{y}}_{k-1}^i, \cdots, \hat{\boldsymbol{y}}_{k-M+1}^i]^{\top} = [f(\mathcal{X}_k^i), f(\boldsymbol{A}_{k-1}^{-1}\mathcal{X}_k^i), \cdots, f(\boldsymbol{A}_{k-1}^{-M+1}\mathcal{X}_k^i)]^{\top};$$

end for

$\bar{\mathbf{y}}_k = \sum_{i=0}^{2n} \boldsymbol{W}_k^i \hat{\mathbf{y}}_k^i$;

$\mathbf{P}_k^y = \sum_{i=0}^{2n} \boldsymbol{W}_k^i (\hat{\mathbf{y}}_k^i - \bar{\mathbf{y}}_k)(\hat{\mathbf{y}}_k^i - \bar{\mathbf{y}}_k)^{\top} + \boldsymbol{\Sigma}_{\boldsymbol{v}}$;

$\mathbf{P}_k^{xy} = \sum_{i=0}^{2n} \boldsymbol{W}_k^i (\mathcal{X}_k^i - \hat{\boldsymbol{x}}_{k|k-1})(\hat{\mathbf{y}}_k^i - \bar{\mathbf{y}}_k)^{\top}$;

$\boldsymbol{K}_k = \mathbf{P}_k^{xy}(\mathbf{P}_k^y)^{-1}$;

$\hat{\boldsymbol{x}}_k = \hat{\boldsymbol{x}}_{k|k-1} + \boldsymbol{K}_k(\mathbf{y}_k - \bar{\mathbf{y}}_k)$;

$\boldsymbol{P}_k = \boldsymbol{P}_{k|k-1} - \boldsymbol{K}_k \mathbf{P}_k^y \boldsymbol{K}_k^{\top}$;

Appendix C

Gauss-Markov Theorem

Theorem C.1 (Gauss-Markov Theorem [99]) *Given the linear model* $\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{v}$*, where* $\boldsymbol{v}$ *is a zero-mean random variable with positive-definite covariance matrix* $\boldsymbol{R}_v$ *and* $\boldsymbol{H}$ *is full rank* $m \times n$ *matrix with* $m \geq n$*, the minimum-variance-unbiased linear estimator of* $\boldsymbol{x}$ *given* $\boldsymbol{y}$ *is*

$$\hat{\boldsymbol{x}} = (\boldsymbol{H}^* \boldsymbol{R}_v^{-1} \boldsymbol{H})^{-1} \boldsymbol{H}^* \boldsymbol{R}_v^{-1} \boldsymbol{y}.$$