Contributions to Navigation Under Unknown Input and Cyber-Physical Security

Ghadeer Shaaban

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ GRENOBLE ALPES

École doctorale : EEATS - Electronique, Electrotechnique, Automatique, Traitement du Signal
Spécialité : Automatique - Productique
Unité de recherche : Grenoble Images Parole Signal Automatique

Contributions à la navigation en présence d'entrées inconnues et à la sécurité cyber-physique

Contributions to Navigation Under Unknown Input and Cyber-Physical Security

Présentée par :

Ghadeer SHAABAN

Direction de thèse :

Alain KIBANGOU MAITRE DE CONFERENCES, UNIVERSITE GRENOBLE ALPES	Directeur de thèse
Christophe PRIEUR DIRECTEUR DE RECHERCHE, CNRS	Co-directeur de thèse
Hassen FOURATI Maitres de Conferences, UGA	Co-encadrant de thèse

Rapporteurs :

Subhrakanti DEY
FULL PROFESSOR, Uppsala Universitet
Tomas MENARD
PROFESSEUR DES UNIVERSITES, ENSICAEN

Thèse soutenue publiquement le **12 septembre 2025**, devant le jury composé de :

Gildas BESANÇON , PROFESSEUR DES UNIVERSITES, Grenoble INP - UGA	Président
Alain KIBANGOU, MAITRE DE CONFERENCES HDR, Université Grenoble Alpes	Directeur de thèse
Christophe PRIEUR, DIRECTEUR DE RECHERCHE, CNRS délégation Alpes	Co-directeur de thèse
Subhrakanti DEY, FULL PROFESSOR, Uppsala Universitet	Rapporteur
Tomas MENARD, PROFESSEUR DES UNIVERSITES, ENSICAEN	Rapporteur
Manon KOK, ASSOCIATE PROFESSOR, Delft University of Technology	Examinatrice

Invités :

Hassen FOURATI
MAITRE DE CONFERENCES, Université Grenoble Alpes

Acknowledgments

I am deeply grateful to have defended my PhD thesis on September 12, 2025, a date that holds special meaning for me. It marks exactly four years since I first arrived in France, on September 12, 2021, to begin my master's studies at Grenoble INP. That journey changed my life, and this day will forever remain in my memory.

I would first like to sincerely thank all the jury members for their time, effort, and presence. Your availability to attend the defense in person, read my thesis, and share your valuable feedback means a lot to me.

A special thanks goes to the jury members who traveled from outside Grenoble: **Professor Subhrakanti Dey** from Uppsala University, Sweden, whom I was very happy to meet earlier at the European Control Conference 2025 in Thessaloniki, where he attended my presentation and we had a wonderful discussion; **Professor Tomas Ménard** from ENSICAEN, Caen, whom I met during the SYNC-OBS Day in Paris in 2023; and **Associate Professor Manon Kok** from Delft University of Technology, the Netherlands.

To my supervisors **Alain Kibangou**, **Christophe Prieur**, and **Hassen Fourati**, my deepest gratitude. I will miss our Thursday afternoon meetings that shaped my PhD journey. Alain, I greatly admire your brilliant mind, your intelligence, and your ability to turn our discussions into innovative research ideas. Christophe, your remarkable ability to handle multiple tasks with calm precision has always inspired me. Hassen, you became not only a mentor but a true friend, I will always remember our many discussions beyond the meetings.

I would also like to thank all the professors at Grenoble INP and Université Grenoble Alpes. In particular, **Ahmad Hably**, who as the head of the MARS master's program, helped me obtain the MIAI scholarship that made it possible for me to study in France, a life-changing opportunity. **Lara Brinon-Arranz**, with whom I had the pleasure of teaching the Autonomous Systems course, and with whom I shared many enjoyable moments outside work, especially our hiking adventures in Grenoble. **Professor Gildas Besançon**, president of my PhD defense jury, for his professionalism and trust since the beginning. I will never forget when he invited me, even before starting my PhD, to teach the nonlinear control lab sessions for MARS students.

I am thankful to **MIAI** for funding my master's studies, to **CROUS** for providing affordable housing and meals during my master's, and to **GIPSA-DOC** for the great activities and community. I am proud to have served as its president during my second PhD year.

My appreciation also goes to everyone at **GIPSA-lab** for their smiles, kindness, and continuous support. To the administrative team, for their help with endless documents; and to **Madame Patricia**, responsible for the GIPSA library, for her daily kindness and our conversations that helped me improve my French.

I am also grateful to the **Mitacs Globalink Research Award** and the **University of Ottawa** for supporting my three-month research visit in summer 2024, and to **Assistant Professor Mohammad Pirani** for the fruitful collaboration.

To my office mates in room B231, **Sophie**, **Sylvain**, and **Paul**, thank you for the everyday discussions and for making the office such a pleasant place. To my colleagues **Saleh**, **Camel**, **Mathias**, **Matthieu**, and **Natalio**, thank you for your support and friendship.

To my Syrian friends in Grenoble, **Samara**, **Rand**, **Omar**, **Baraa**, **Anas**, **Hind**, and **Hassan**, your support and help have been endless. To my dear friend **Kostas**, who stood by me through every difficulty and celebration; meeting your family in Athens and your friends, including Eleni, was a joy. I am truly proud to have you as a friend.

To my GAOT friends, **Omran**, **Hashem**, and **Ihab**, our friendship is a treasure that will never end. Meeting Omran again in Canada after three years was one of the best moments of my PhD journey.

To my Lebanese friends, **Zakia**, **Borhan**, and **Wissam**, thank you for standing by me during my hardest moments, for the deep discussions, and for all the laughter we shared.

To the **Syrian Control Club**, thank you for your valuable feedback, especially during my PhD rehearsal. A special thanks to **Anas**, who founded this club and traveled from Munich to attend my defense. Thanks also to **Ghadeer**, **Ali**, **Fadi**, and **Sokrat** for the friendship and motivation.

Finally, to my **family**, who are the heart of everything I have achieved. At 30 years old, I still feel like a child when I talk to them. To my sisters **Reem** and **Nada**, who always recharge my spirit with their kindness; to my brothers-in-law **Ramzi** and **Ali**, who are truly like brothers; and to my nephews **Zain**, **Rani**, **Joud**, and my niece **Jouri**, who make me smile every time they call me *Uncle Ghadeer*.

To my **mother, Kafa**, whose voice always brings joy and peace, even in the hardest times. Every phone call with you ends with a smile. To my **father, Yousef**, whose entire life has been dedicated to his children's happiness. Since my childhood, he used to tell me, *I can work all day if it helps you in sport or science*. I am deeply happy and proud that he came to France to attend my defense, his first time ever flying on a plane. That moment will stay in my heart forever.

Contents

Symbols and Notation

This section summarizes the main symbols and notations used throughout this thesis. The notations are consistent across all chapters.

- Regular lower-case letters (e.g., m) denote scalars.
- Bold lower-case letters (e.g., $\mathbf{m}$) denote vectors.
- Bold upper-case letters (e.g., $\mathbf{M}$) denote matrices.
- $\mathbf{v}(i)$ denotes the i-th component of the vector $\mathbf{v}$.
- $\mathbf{v}(i:j)$ denotes a subvector of $\mathbf{v}$ containing components from i to j.
- $\mathbf{M}(i)$ denotes the i-th row of the matrix $\mathbf{M}$.
- $\mathbf{M}(i:j)$ denotes the submatrix of $\mathbf{M}$ containing rows from i to j.
- $\mathbf{I}_n$ denotes the identity matrix of order n.
- $\mathbf{0}$ denotes the all-zero matrix.
- $\mathbf{0}_n$ denotes the square zero matrix of order n.
- $\mathbb{R}$ denotes the field of real numbers.
- $\mathbb{C}$ denotes the field of complex numbers.
- $\mathbb{N}$ denotes the set of natural numbers.
- $\mathbf{E}(\cdot)$ denotes the expectation operator.
- $\mathbb{P}$ denotes the probability.
- $\det(\cdot)$ denotes the determinant of a matrix.
- $\mathrm{tr}(\cdot)$ denotes the trace of a matrix.
- $\mathcal{O}(\cdot)$ denotes higher-order terms neglected in an approximation.
- Δt denotes the sampling time.

Additionally, the following conventions and notes apply throughout the thesis.

- Throughout this thesis, the process noise covariance matrix is denoted by $\boldsymbol{\mathcal{Q}}$, the measurement noise covariance matrix by $\boldsymbol{\mathcal{R}}$, the output vector by $\mathbf{y}$, and the output measurement noise by $\mathbf{w}^y$. These notations are adopted consistently across all chapters to maintain clarity. However, the dimension and specific definition of each of these quantities depend on the estimation problem addressed in the corresponding chapter.
- For any vector $\mathbf{v}$, the subscript k is used to indicate its value at time step k, denoted as $\mathbf{v}_k$.
- Exceptionally, in Chapter 7, an uppercase letter M_z is used to denote a scalar representing the yaw moment of a ground vehicle. This choice is made to remain consistent with the notation commonly adopted in the literature on ground vehicle lateral dynamics.

List of Abbreviations

BCH	Baker–Campbell–Hausdorff
CG	Center of Gravity
CPS	Cyber-Physical System
CVXPY	Convex Optimization Python Package
DCCP	Disciplined Convex-Concave Programming
EA	External Acceleration
EKF	Extended Kalman Filter
EMI	Electromagnetic Interference
FDI	False Data Injection
FQA	Factored Quaternion Algorithm
GPS	Global Positioning System
IEKF	Invariant Extended Kalman Filter
IMU	Inertial Measurement Unit
KF	Kalman Filter
MARG	Magnetic, Angular Rate, and Gravity
MEMS	Micro-Electro-Mechanical Systems
MKF	Multiplicative Kalman Filter
MPC	Model Predictive Control
MUO	Misleading Unauthorized Observer
NED	North-East-Down
PVA	Position, Velocity, and Attitude
QUEST	QUaternion ESTimator

RMSE	Root Mean Square Error
RTSKF	Robust Two-Stage Kalman Filter
SDC	State-Dependent Coefficient
SO(3)	Special Orthogonal Group in 3D
SUV	Sport Utility Vehicle
TRIAD	Tri-axial Attitude Determination
UAV	Unmanned Aerial Vehicle
UIF	Unknown Input Filtering
UKF	Unscented Kalman Filter
UMV	Unbiased Minimum Variance
UWB	Ultra Wide Band

General Introduction

Context and Motivation

Modern engineering systems are becoming increasingly complex and interconnected, integrating sensing, computation, control, and communication to achieve advanced functionalities and efficiencies. Systems such as aerial robots and ground vehicles rely on actuator commands, such as motor inputs, and sensor measurements, such as Inertial Measurement Units (IMU), magnetometers, and Global Positioning Systems (GPS), for both control and state estimation. Those actuator commands and sensor measurements are the input and output of the system. They can be exposed to unknown physical components, missing or unavailable information, or even deliberately injected false data. Such unknown input may result from technical faults, physical phenomena, or external attacks.

Real-world incidents in which these malicious or unknown components can have a devastating impact have been reported. In 2008, a 1.4 billion USD aircraft crashed on take-off due to moisture in the air data sensors, which caused incorrect airspeed readings, where the moisture effectively acted as an unknown input to the sensors [37]. In 2009, false data from the speed sensors caused Air France Flight 447 to plunge into the Atlantic Ocean, killing all 228 people aboard [170]. In 2013, hackers disrupted communication between autonomous shuttles, causing a collision and extensive traffic delays [62]. In 2014, attackers remotely opened circuit breakers in a regional power grid, causing a power cut that left thousands of people without electricity [78]. In 2015, attackers crashed a Jeep Cherokee from ten miles away, demonstrating how injected false commands can override vehicle control systems [172]. In 2016, a team of hackers remotely controlled a Tesla Model S from twelve miles away, manipulating its brakes and steering [169]. Between 2023 and 2024, GPS spoofing incidents have caused significant disruptions to both civilian and military navigation systems. In the Baltic Sea region, over 46,000 flights experienced GPS spoofing, leading to navigation challenges and safety concerns for commercial aviation [171]. Similarly, in parts of the Middle East, widespread GPS spoofing affected users, with navigation applications misplacing their locations by hundreds of kilometers [8].

These events highlight the importance of secure and reliable operation, particularly in safety-critical applications where failures can lead to severe consequences. They also reveal a fundamental challenge: many widely used estimation and control algorithms assume that input-output signals are accurate and perturbed only by noise with known statistical properties. However, as these incidents demonstrate, such assumptions often break down in

real-world environments, where uncertainties are more complex and sometimes adversarial. While robust control methods address certain classes of model uncertainty and bounded disturbances, they may still fall short when dealing with the following two types of deviations examined in this thesis:

- **Unknown Input:** This category deals with situations where sensors' measurements and control commands are affected by unknown components. These can include: Unmodeled forces or disturbances acting on the system, unavailable or unreliable sensor measurements, internal system faults or parameter uncertainties.
- **Cyber-Physical Attacks:** This category involves deliberate actions by malicious adversaries targeting the system's sensors, actuators, or communication networks.

The main difference between an unknown input and a cyber-physical attack is that the latter is a deliberate action by an attacker. Although originating from different sources, both unknown input and cyber-physical attacks pose a similar fundamental challenge for state estimation and control algorithms: the estimator and controller process signals that are assumed to be correct, while in reality, they may contain unknown or incorrect terms. Addressing these challenges is essential for the safe operation of modern and interconnected systems.

Scope of this Thesis

Navigation systems, including ground and aerial vehicles, represent a particularly critical domain where failures due to unknown input or cyber-physical attacks are unacceptable. Incidents (mentioned earlier in this introduction) involving aircraft navigation errors [170] and ground vehicle intrusions [172] highlight the severity of such vulnerabilities, demonstrating the potential risks to property, mission success, and human lives. For this reason, this thesis concentrates its scope on developing security solutions specifically tailored to navigation-related applications.

In navigation systems, estimation of the attitude, or orientation, of a rigid body is essential. Reliable attitude estimation is crucial for stability, control, sensor data integration, and achieving overall system objectives. Incorrect or compromised attitude information can cause significant performance degradation and lead to critical system failures. Representing attitude mathematically is challenging because rotations have nonlinear properties and do not behave like standard vectors. Therefore, this thesis uses the Special Orthogonal Group SO(3) to represent rotations. The SO(3) representation avoids issues such as singularities and non-uniqueness that occur with simpler methods. This thesis focuses on developing secure attitude estimation on SO(3) methods capable of operating reliably when unknown input or cyber-physical attacks are present.

In many applications, attitude estimation relies on measurements from three sensors referred to as MARG sensors: **M**agnetic field, **A**ngular **R**ate, and **G**ravity. A three-axis magnetometer measures the magnetic field, a three-axis gyroscope measures the angular rate, and a three-axis accelerometer measures the sum of the Earth's gravitational acceleration and ex-

ternal acceleration (also referred to as linear acceleration). This thesis considers attitude estimation on SO(3) in the presence of unknown input, which reflect real-world challenges that degrade estimation performance and limit the reliability of navigation systems. In many practical scenarios, sensor data are incomplete, corrupted, or partially unavailable, making it essential to design estimators that remain reliable under such uncertainties. The work focuses on two representative forms of unknown input that affect attitude estimation. The first one corresponds to cases where angular rate measurements are unavailable or intentionally excluded, such as scenarios where the use of gyroscopes is limited due to energy, cost, or reliability constraints. The second is the external acceleration, which is not measured separately from Earth's gravity. In both cases, these quantities affect the estimation performance, motivating the need for reliable algorithms that account for such unknown input while preserving the geometric structure of SO(3).

In addition to the studies on attitude estimation on SO(3) under unknown input, this thesis addresses two security problems related to navigation applications against cyber-physical attacks: one concerning secure attitude estimation on SO(3), and the other involving ground vehicle dynamics. Furthermore, considering the security aspect, traditional defense mechanisms in CPS often focus on passive strategies: preventing attacks (e.g., encryption), detecting them (e.g., anomaly detection), or ensuring the system can withstand some impact (resilience). However, the security landscape can be viewed as a continuous game between attackers and defenders [147]. As defenders develop better passive strategies, attackers continue to improve their methods to bypass them. This creates constant competition, where the attacker always tries to stay ahead by designing attacks that are smart enough to avoid detection and defeat the protection methods of the defender. This competition motivates the current thesis to explore alternative and more active defense strategies. What if the defending system could take action against the attacker, rather than simply passively resisting? What would happen if this action was not detectable by the attacker? This thesis investigates such a concept, specifically focusing on misleading an attacker who is attempting unauthorized access to the system signals. Instead of simply blocking the attacker, the proposed strategy aims to feed them modified, seemingly correct data, causing them to build an inaccurate understanding of the state of the system. In this case, the attacker will believe that it is achieving its objective, while in reality it is not. This false confidence may discourage the attacker from improving its strategy, as it believes that the mission is already successful. Although this research is motivated by the security requirements of navigation systems, the proposed framework for active defense is formulated for general discrete-time linear systems, suggesting its applicability beyond navigation-related applications.

This research thus aims to advance the state of the art and contribute to the development of secure methods, with a particular focus on attitude estimation and navigation applications that address two primary challenges that violate standard assumptions: the presence of unknown inputs and the risk of cyber-physical attacks. The work provides specific solutions for attitude estimation on SO(3), analyzes vulnerabilities in vehicle dynamics, and introduces a new paradigm for active defense, collectively contributing to enhancing the security and reliability of these critical systems.

Contributions of the Thesis

This thesis consists of two parts. Part I focuses on attitude estimation on SO(3) under unknown input, and Part II focuses on the security of CPS. In the following, a brief explanation of the thesis contributions.

Part I contributions

Extensive research has focused on designing state estimation for linear and nonlinear systems with unknown input, where no prior information about the unknown input is available. This part of the thesis contributes to state estimation with unknown input for systems whose state lies on SO(3), which, unlike vector spaces, has a non-Euclidean structure. The motivation for using the SO(3) group is its structured framework for representing three-dimensional rotations. Three cases of attitude estimation on SO(3) based on MARG sensors under unknown input are addressed in this part, with each case solving a problem that remains open in the existing literature. These cases are categorized as follows: (i) the unknown input affects only the system dynamics, (ii) the unknown input affects only the output measurements, and (iii) the unknown input affects both the dynamics and the output. These cases are treated in Chapter 2, Chapter 3, and Chapter 4, respectively. The following paragraphs provide further explanation of the contributions made in each of these chapters.

Chapter 2 contribution: Due to the drawbacks associated with gyroscopes, such as relatively high power consumption, susceptibility to drift, and bias, extensive research has focused on developing angular motion estimation algorithms that enable attitude estimation without relying on a gyroscope. Chapter 2 designs two novel gyro-free attitude estimation algorithms, relying only on measurements from an accelerometer and a magnetometer, by considering angular velocity as an unknown input. The theoretical contribution of these two algorithms is the design of two state estimation algorithms for SO(3) with an unknown input affecting the system dynamics without direct feedthrough to the output, where the angular velocity appears only in the attitude dynamic model and not in the output function.

Chapter 3 contribution: A key challenge in MARG-based attitude estimation is the assumption that the acceleration is only gravity, ignoring external acceleration to satisfy the Wahba problem. Several solutions have been proposed in the literature, often involving additional sensors or imposing assumptions valid only under specific conditions. Chapter 3 presents a novel solution that treats external acceleration as an unknown input. The theoretical contribution is the design of an algorithm for state estimation on SO(3) with unknown input that has direct feedthrough to the output, without affecting the state dynamics.

Chapter 4 contribution: For a motion involving both rotational and translational movement, many applications require position and velocity estimation in addition to attitude. To ensure full state observability, a position sensor is used alongside MARG sensors. The external acceleration appears in the velocity kinematic equation and is multiplied by the rotation matrix, meaning that for position, velocity, and attitude estimation based on MARG and position measurements, the external acceleration affects both the dynamic model and the output function. Chapter 4 addresses the problem of position, velocity, and attitude

estimation by treating the external acceleration as an unknown input and designing a state estimator for systems on SO(3) $\times\mathbb{R}^3 \times \mathbb{R}^3$, where the unknown input affects both the dynamics and the output and is multiplicatively coupled with the state on SO(3).

Part II contributions

The integration of cyber and physical components in navigation systems makes these systems highly vulnerable to cyber-physical threats. Four main types of cyber-physical attacks have been explored in the literature: denial of service (DoS), replay, eavesdropping attack, and false data injection attacks (FDI).

Chapter 6 contribution: Secure state estimation under randomly occurring FDI attack has been widely studied. However, an important gap remains: no existing work addresses this problem when the state lies on SO(3). Chapter 6 designs a secure MARG sensor-based attitude estimation algorithm on SO(3), specifically for scenarios where accelerometer and magnetometer measurements are subject to randomly occurring FDI attacks.

Chapter 7 contribution: Ground vehicles represent another important application in navigation, and their security has received significant attention. The lateral model plays a critical role in maintaining stability and control during turns and maneuvers, making it a key focus of research in control, estimation, and observation. However, few studies have explored its security. One class of FDI attacks targeting system inputs is the zero dynamics attack, where an attacker exploits the system's invariant zeros to perform attacks that leave no trace in the system's outputs, making these attacks undetectable. Chapter 7 studies and analyzes the invariant zeros of the vehicle's lateral model and demonstrating how an attacker can exploit these zero dynamics to perform undetectable attacks. The motivation behind this work is not to create zero dynamics attacks but to evaluate vehicle security against them and enhance protection measures.

Chapter 8 contribution: Eavesdropping attacks compromise confidentiality by accessing private information. The unauthorized observer is an attacker who aims to perform remote state observation based on the knowledge of the system's model and eavesdropping on input-output signals. Traditional approaches to defending against unauthorized observation are similar to ones against eavesdropping attacks, which involve implementing passive defense strategies such as encrypting communication channels and using firewalls. Differently, Chapter 8 introduces the concept of active defense by misleading the unauthorized observer, the work is motivated by this example: if an attacker attempts to steal information from a system, but the system instead allows the attacker to steal modified data that appears correct, the attacker may falsely believe they have successfully obtained the information. This could discourage them from developing new methods for information theft. Our main result provides a strategy that makes attackers believe they are successfully completing their missions, while in fact, they are not.

Thesis organization

This thesis consists of two parts. Each part begins with an introductory chapter and includes three contributed chapters. Finally, a general conclusion summarizes the contributions of the thesis and outlines several perspectives for future work. Fig. 1 provides the overall organization of the thesis. An arrow from one chapter to another indicates that reading the first chapter is required for understanding the second.

This thesis is structured to present a coherent and, in many times, progressive development of the proposed methods. Therefore, it is recommended to read the chapters in sequence, from beginning to end, in order to fully understand the context and how the individual contributions are integrated. However, some chapters may still be read independently, taking into account the dependencies shown in Fig. 1.

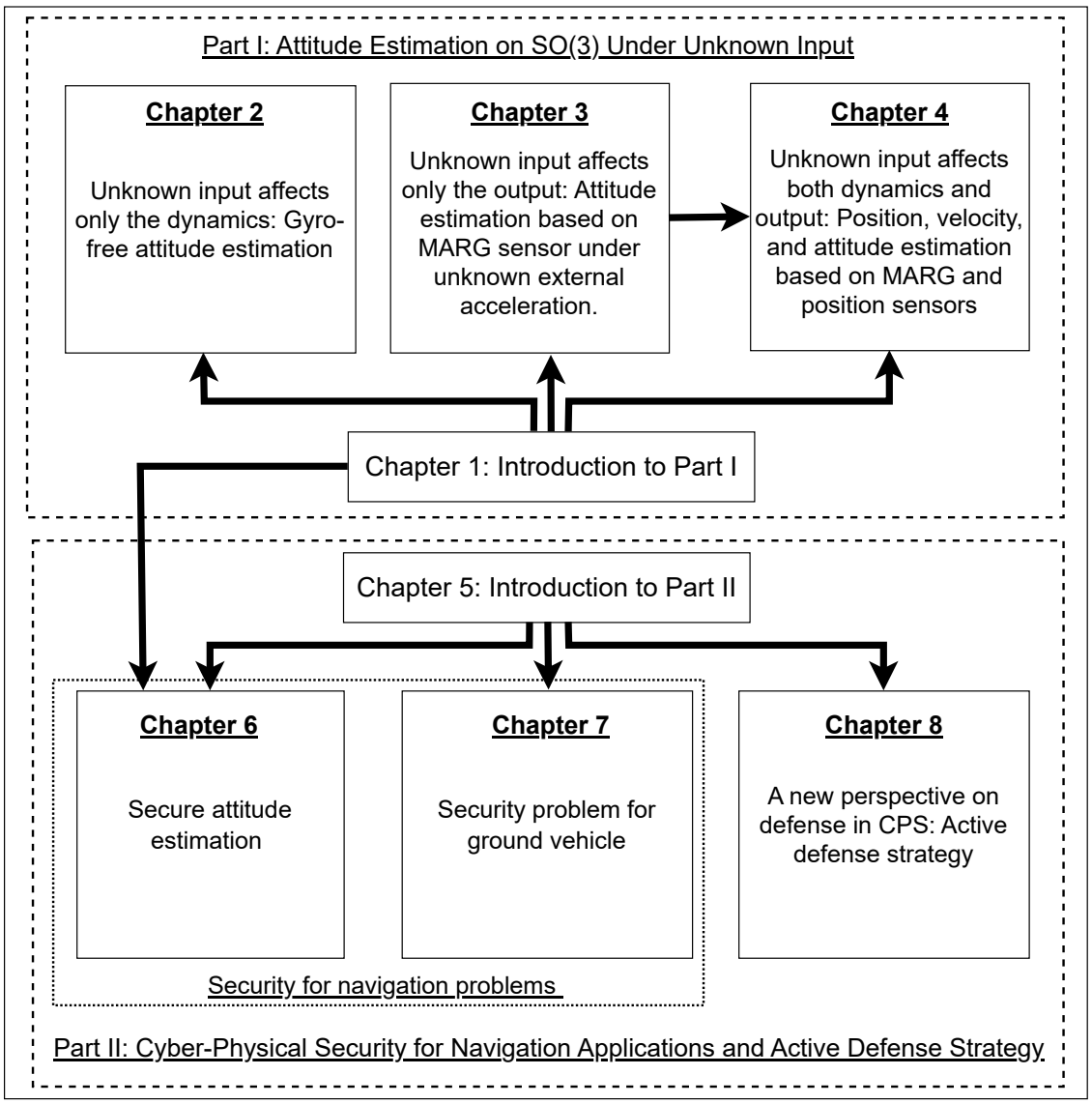

Figure 1: Thesis outline

Publications

The research conducted during this thesis has led to the following publications

Journals:

1. **G. Shaaban**, H. Fourati, A. Kibangou, and C. Prieur, "Active defense strategy in cyber-physical systems: Misleading unauthorized observers," IEEE Transactions on Control of Network Systems (TCNS), vol. 12, no. 3, pp. 2404-2415, Sept. 2025.
   DOI: 10.1109/TCNS.2025.3570931.

2. **G. Shaaban**, H. Fourati, A. Kibangou, and C. Prieur, "Attitude estimation on SO(3) with unknown input," International Journal of Robust and Nonlinear Control (IJRNC), accepted in July 2025.
   DOI: 10.1002/rnc.70060.

3. **G. Shaaban**, H. Fourati, A. Kibangou, C. Prieur, and M. Pirani, "Cyber-physical security of vehicles: Zero dynamics attacks against vehicle's lateral dynamics," European Journal of Control, accepted in July 2025.
   DOI: 10.1016/j.ejcon.2025.101316.

   Note 1: This work was accepted and presented at the 23rd European Control Conference (ECC), held in Thessaloniki, Greece, from 24 to 27 June 2025. It was subsequently invited and accepted for publication in the Special Issue of the European Journal of Control dedicated to the best papers of the 2025 European Control Conference.

   Note 2: This work was carried out during Ghadeer Shaaban's three-month research visit to the University of Ottawa (July–October 2024), in collaboration with Assistant Professor Mohammad Pirani, and was funded by the Mitacs Globalink Research Award.

4. **G. Shaaban**, H. Fourati, A. Kibangou, and C. Prieur, "Position, velocity and attitude estimation based on MARG and position measurements under unknown external acceleration," IEEE Control Systems Letters, vol. 9, pp. 1423-1428, June 2025.
   DOI: 10.1109/LCSYS.2025.3579402.

   Note: This work was jointly submitted to IEEE-LCSS and the IEEE Conference on Decision and Control (CDC) 2025. It was accepted for presentation at the CDC and will be presented at the conference, which will be held in Rio de Janeiro, Brazil, from 10 to 12 December 2025.

5. **G. Shaaban**, H. Fourati, A. Kibangou, and C. Prieur, "MARG sensor-based attitude estimation on SO(3) under unknown external acceleration," IEEE Control Systems Letters (L-CSS), vol. 7, pp. 3795–3800, December 2023.
   DOI: 10.1109/LCSYS.2023.3342855.

   Note: This work was jointly submitted to IEEE-LCSS and the American Control Conference (ACC) 2024. It was accepted for presentation at ACC and presented during the conference held in Toronto, Canada, 10-12 July 2024.

Conferences:

1. **G. Shaaban**, H. Fourati, A. Kibangou, and C. Prieur, "Secure MARG sensor-based attitude estimation on SO(3) under randomly occurring false data injection attacks," accepted in the 23rd European Control Conference (ECC), Thessaloniki, Greece, 24-27 June 2025.

2. **G. Shaaban**, H. Fourati, A. Kibangou, and C. Prieur, "Gyro-free Kalman filter with unknown inputs for SO(3)-based attitude estimation," in IEEE 13th International Conference Indoor Positioning and Indoor Navigation (IPIN), Nuremberg, Germany, 25-28 September 2023.
DOI: 10.1109/IPIN57070.2023.10332509.

In addition, part of the following work was completed during the thesis period, while the majority was conducted during the master's thesis of Ghadeer Shaaban, prior to the start of the PhD. The results from this work are not included in this thesis.

1. **G. Shaaban**, H. Fourati, C. Prieur, and A. Kibangou, Q-learning-based noise covariance matrices adaptation in Kalman filter for inertial navigation, IFAC-PapersOnLine, 58(21), 96-101, 2024.
DOI: 10.1016/j.ifacol.2024.10.150.

National conferences and workshops without Proceedings:

1. **G. Shaaban**, H. Fourati, A. Kibangou, and C. Prieur, "Attitude Estimation on SO(3) with Unknown Inputs," in the second edition of the Annual Société d'Automatique, de Génie Industriel et de Productique (SAGIP) Conference, Lyon, France, 29-31 May 2024.

2. **G. Shaaban**, H. Fourati, A. Kibangou, and C. Prieur, "MARG Sensors-based Attitude Estimation on SO(3) Under Unknown External Acceleration," in the Synchronisation – Observation Day, Paris, France, 6 December 2023.

Part I

Attitude Estimation on SO(3) Under Unknown Input

Chapter 1

Introduction

This chapter identifies the research gap addressed in this part and to prepare the reader for the three estimation problems considered in the following chapters. Section 1.1 reviews the unknown input filtering problem for systems with states belonging to a vector space. Section 1.2 reviews attitude estimation techniques based on MARG sensors and highlights the importance of attitude representation on the Special Orthogonal group SO(3). These two sections provide the necessary background to understand the research context. Based on these reviews, Section 1.3 identifies the research gap that motivates the contributions of this part, which is the problem of attitude estimation on SO(3) in the presence of unknown inputs. The remaining sections, from Section 1.4 to Section 1.7, present the mathematical tools, sensor models, and algorithmic frameworks required for the developments in the subsequent chapters. The next three chapters each address a distinct estimation problem, all formulated on SO(3) and involving unknown inputs.

1.1. Unknown Input Filtering

State estimation based on dynamic models and observations has long been of interest to scientists and engineers across various domains. One particular problem in this field is the estimation of the state in the presence of unknown input, where no prior information about the unknown input is available, also known as the unknown input filtering (UIF) problem. This problem finds applications in various areas, such as disturbance rejection [151], fault detection [140], weather forecasting [99], and bias compensation [61]. Early solutions addressed this problem by augmenting the state vector with the unknown input vector [61], assuming a known model for the unknown input dynamic. Subsequently, various approaches were developed to address the UIF problem. These include H∞ filtering, designed to maximize a predefined estimation performance criterion [185]; moving horizon estimation, which formulates the problem of state estimation in the presence of unknown input as an optimization task by minimizing a cost function over a finite prediction horizon [142]; and sliding mode observers, ensuring that the state converges to a predefined sliding surface while estimating the system states in the presence of unknown input [9].

Furthermore, extensive research has focused on designing state estimators for linear systems with unknown input, aiming to minimize the trace of the state estimation error covariance matrix while ensuring unbiasedness. Notably, several works have contributed to the linear UIF problem when the unknown input affects the state dynamics without direct feedthrough to the output, see [40, 65, 82, 99]. Extensions for linear systems with a full rank direct feedthrough matrix have also been proposed in [41, 66, 83, 160, 183]. A unified filter for linear systems was proposed in [182, 184] with no restriction on the direct feedthrough matrix. Researchers have made efforts to extend UIF algorithms to nonlinear systems. Inspired by nonlinear versions of the Kalman filter: the extended Kalman filter (EKF), and the unscented Kalman filter (UKF), the authors in [84, 86, 87] propose two distinct approaches for state estimation for nonlinear systems with unknown input. The first approach involves linearizing around the current state estimate, and the second involves generating a set of sample points, known as sigma points, and propagating them through the system dynamics. Several other extensions have been addressed in the literature, such as [52] inspired by the Bayesian estimation framework, [51, 53] inspired by the ensemble Kalman filter (EnKF), and [85] inspired by the state-dependent coefficient (SDC) factorization.

1.2. Attitude Estimation

Attitude represents the orientation of a rigid body, such as a drone, spacecraft, or robotic platform, relative to a fixed reference frame, commonly referred to as the navigation frame. Attitude estimation is fundamental for navigation and control across various domains, including aerospace, robotics, and autonomous systems. Since no sensors directly measure orientation, attitude is estimated based on sensor fusion techniques that integrate measurements from multiple sources [38]. A typical sensor combination for attitude estimation includes a three-axis magnetometer, which measures the magnetic field vector in the body frame; a three-axis gyroscope, which measures the angular velocity vector in the body frame; and a three-axis accelerometer, which measures the acceleration vector in the body frame, including the Earth's gravity. Together, these sensors form the Magnetic, Angular Rate, and Gravity (MARG) sensor.

A classical approach for attitude estimation relies on static algorithms that use two known non-collinear reference vectors in both the body and navigation frames. This problem is formally defined as Wahba's problem [58]. The reference vectors typically used are the Earth's gravity and magnetic field, both of which are known in the navigation frame and measured in the body frame using a three-axis accelerometer and a three-axis magnetometer, respectively, under the assumption that the only acceleration acting on the rigid body is the Earth's gravity and that no magnetic disturbances are present. Well-known solutions to Wahba's problem include the Factored Quaternion Algorithm (FQA) [187], the Three-Axis Attitude Determination (TRIAD) [156], and the Quaternion Estimation Algorithm (QUEST) [156].

To enhance attitude estimation accuracy, various algorithms incorporate angular velocity measurements in addition to acceleration and the magnetic field. Among these methods are complementary filters [116] and Kalman-like filters, such as EKF, where attitude is

represented using quaternions [146, 162]. One limitation of the EKF with quaternion is that it applies an additive correction to the quaternion, which requires normalization at each time step to preserve the unit-norm constraint. This normalization step may introduce inaccuracies in the estimated attitude. To address this issue, the Multiplicative Kalman Filter (MKF) [121] models the attitude error as a multiplicative correction, ensuring that the quaternion norm is maintained without the need for additional normalization. In addition to the normalization problem, quaternions present a structural drawback due to their double-cover property: each physical orientation corresponds to two opposite quaternions. This non-uniqueness can cause discontinuities in estimation and control algorithms, such as the unwinding phenomenon [13], where unnecessary full rotations may occur to reach a target orientation.

To overcome the limitations associated with quaternion-based approaches, several filtering techniques have been formulated on SO(3) for attitude estimation. These include the Invariant Kalman Filter (IEKF) [5] and UKF on Lie groups [20]. The use of SO(3) eliminates the need for quaternion normalization and avoids the non-uniqueness problem. This makes SO(3) an ideal choice for attitude representation in estimation and control applications [4, 5, 11, 116, 145]. A review of attitude estimation methods can be found in the survey [38].

1.3. Main problems

Despite the importance of both the unknown input filtering problem and attitude estimation on SO(3), where SO(3) is a group and not a vector space, no existing work has formally addressed unknown input filtering within the SO(3) framework. Some studies have considered attitude estimation on SO(3) in the presence of unknown disturbances and measurement biases, but these approaches remain limited in scope. For instance, the work in [177] focuses on attitude estimation under unknown dynamic disturbances. Similarly, several works [11, 69, 76, 96] have tackled the problem of angular velocity measurements affected by unknown biases, proposing observer-based techniques to compensate for such errors. However, while these studies provide valuable insights, they do not offer a formal framework for unknown input filtering on SO(3).

The first part of this thesis aims to bridge this gap by developing estimation algorithms that explicitly address the problem of unknown input in attitude estimation on SO(3). The proposed methods will contribute to solving two key problems that have been well-recognized in the literature. The first is attitude estimation without relying on gyroscopes, which is motivated by the drawbacks of gyroscopic sensors, such as high power consumption. This topic will be discussed in detail in Chapter 2. The second problem concerns the challenge that accelerometers measure both Earth's gravity and unknown external acceleration, making it difficult to separate the two effects for accurate attitude estimation. This issue will be addressed in Chapter 3 for attitude estimation and in Chapter 4 for position, velocity, and attitude estimation. By tackling these problems, this part of the thesis provides a comprehensive framework for attitude estimation on SO(3) under unknown inputs.

1.4. Mathematical Representations of Attitude and the SO(3) Framework

This section presents the mathematical formulations of Euler angles and quaternions, with an emphasis on their respective limitations, namely the singularity issue associated with Euler angles and the non-uniqueness of quaternions, where each orientation is represented by two equivalent quaternions. The relationship between these representations and the rotation matrix is also established. These limitations motivate the use of SO(3) for attitude representation. Accordingly, this section also introduces the mathematical framework of SO(3), which is required for the estimation algorithms developed in this thesis.

Euler Angles

Euler angles provide an intuitive way to represent attitude by decomposing a three-dimensional rotation into a sequence of three successive rotations about predefined axes. Their physical interpretability and minimal parameter count make them widely used in many applications. However, Euler angles suffer from a fundamental limitation known as singularity or gimbal lock, which leads to a loss of one degree of freedom in certain configurations [161].

Relation between Euler angles and rotation matrix, and singularity problem:

A set of Euler angles $[\phi, \theta, \psi]$, representing roll, pitch, and yaw, respectively, describes the three consecutive rotations. Several Euler angle conventions exist; in this thesis, the XYZ convention is adopted, as commonly used in the literature [146]. Under this convention, the rotation matrix $\mathbf{R}$ is expressed as [58, Chapter 3.3]:

$$\mathbf{R} = \mathbf{R}_z(\psi)\mathbf{R}_y(\theta)\mathbf{R}_x(\phi),$$

where $\mathbf{R}_x(\phi)$, $\mathbf{R}_y(\theta)$, and $\mathbf{R}_z(\psi)$ denote the elementary rotation matrices, defined as:

$$\mathbf{R}_x(\phi) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\phi) & -\sin(\phi) \\ 0 & \sin(\phi) & \cos(\phi) \end{pmatrix}, \quad \mathbf{R}_y(\theta) = \begin{pmatrix} \cos(\theta) & 0 & \sin(\theta) \\ 0 & 1 & 0 \\ -\sin(\theta) & 0 & \cos(\theta) \end{pmatrix},$$

$$\mathbf{R}_z(\psi) = \begin{pmatrix} \cos(\psi) & -\sin(\psi) & 0 \\ \sin(\psi) & \cos(\psi) & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The singularity problem associated with Euler angles can be explained by examining the relation between the body-frame angular velocity vector $\boldsymbol{\omega} = \begin{pmatrix} \omega_x & \omega_y & \omega_z \end{pmatrix}^\top$ and the derivatives of the Euler angles $\dot{\phi}$, $\dot{\theta}$, and $\dot{\psi}$. Following the XYZ convention, the angular velocity is

expressed as:

$$\begin{pmatrix} \omega_x \\ \omega_y \\ \omega_z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \dot{\psi} + \mathbf{R}_z(\psi) \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \dot{\theta} + \mathbf{R}_z(\psi)\mathbf{R}_y(\theta) \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \dot{\phi}.$$

In this formulation, $\dot{\psi}$ corresponds to a rotation about the z-axis, $\dot{\theta}$ corresponds to a rotation about the y-axis, transformed by $\mathbf{R}_z(\psi)$, and $\dot{\phi}$ corresponds to a rotation about the x-axis, transformed by $\mathbf{R}_z(\psi)\mathbf{R}_y(\theta)$. This shows that the angular velocity results from a combination of the three Euler angle rates, each affected by the current orientation.

By substituting the rotation matrices, the explicit relation between the angular velocity and the derivatives of the Euler angles is given by:

$$\begin{pmatrix} \omega_x \\ \omega_y \\ \omega_z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \dot{\psi} + \begin{pmatrix} -\sin\psi \\ \cos\psi \\ 0 \end{pmatrix} \dot{\theta} + \begin{pmatrix} \cos\psi\cos\theta \\ \sin\psi\cos\theta \\ -\sin\theta \end{pmatrix} \dot{\phi}.$$

The singularity occurs when $\theta = \pm\frac{\pi}{2}$, leading to:

$$\begin{pmatrix} \omega_x \\ \omega_y \\ \omega_z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \dot{\psi} + \begin{pmatrix} -\sin\psi \\ \cos\psi \\ 0 \end{pmatrix} \dot{\theta} + \begin{pmatrix} 0 \\ 0 \\ \mp 1 \end{pmatrix} \dot{\phi}.$$

At this configuration, the effects of $\dot{\psi}$ and $\dot{\phi}$ become indistinguishable, and it is no longer possible to uniquely express these variables in terms of the angular velocity components. This results in a loss of one degree of freedom and is referred to as singularity or gimbal lock, which limits the use of Euler angles in applications requiring global and continuous attitude representation.

Unit Quaternions

Quaternions provide an alternative representation of attitude by using four parameters, avoiding the singularity problem associated with Euler angles.

Relation between quaternions and rotation matrix, and non-uniqueness problem:

The unit quaternion $\mathbf{q}$ is defined as:

$$\mathbf{q} = \begin{pmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \end{pmatrix} = \begin{pmatrix} q_0 \\ \mathbf{q}_v \end{pmatrix},$$

where q_0 is the scalar part, and $\mathbf{q}_v = \begin{pmatrix} q_1 & q_2 & q_3 \end{pmatrix}^\top$ is the vector part. The unit quaternion satisfies the following norm constraint:

$$q_0^2 + q_1^2 + q_2^2 + q_3^2 = 1.$$

The corresponding rotation matrix is given by:

$$\mathbf{R}(\mathbf{q}) = \mathbf{I}_3 + 2q_0(\mathbf{q}_v)_\times + 2(\mathbf{q}_v)_\times^2,$$

where $(\mathbf{q}_v)_\times$ is the skew-symmetric matrix associated with $\mathbf{q}_v$:

$$(\mathbf{q}_v)_\times = \begin{pmatrix} 0 & -q_3 & q_2 \\ q_3 & 0 & -q_1 \\ -q_2 & q_1 & 0 \end{pmatrix}.$$

Expanding this equation yields the explicit form of $\mathbf{R}(\mathbf{q})$:

$$\mathbf{R}(\mathbf{q}) = \begin{pmatrix} 1 - 2(q_2^2 + q_3^2) & 2(q_1q_2 - q_0q_3) & 2(q_1q_3 + q_0q_2) \\ 2(q_1q_2 + q_0q_3) & 1 - 2(q_1^2 + q_3^2) & 2(q_2q_3 - q_0q_1) \\ 2(q_1q_3 - q_0q_2) & 2(q_2q_3 + q_0q_1) & 1 - 2(q_1^2 + q_2^2) \end{pmatrix}.$$

A fundamental property of quaternions is that both $\mathbf{q}$ and $-\mathbf{q}$ correspond to the same rotation matrix:

$$\mathbf{R}(\mathbf{q}) = \mathbf{R}(-\mathbf{q}).$$

This property leads to a non-uniqueness issue, as each physical orientation is represented by two equivalent quaternions.

This redundancy can introduce discontinuities in estimation and control algorithms. A significant consequence is the unwinding phenomenon, where the system unnecessarily performs a full 360-degree rotation even though a shorter rotation exists to reach the desired orientation. This issue arises when feedback controllers do not properly account for the fact that two distinct quaternions correspond to the same physical rotation, resulting in inefficient and energy-consuming trajectories [13].

The Special Orthogonal Group SO(3)

Mathematical formulation of SO(3) and its Lie algebra $\mathfrak{so}(3)$:

SO(3) consists of all 3×3 rotation matrices that preserve orientation and have a unit determinant:

$$\mathrm{SO}(3) = \left\{ \mathbf{R} \in \mathbb{R}^{3\times 3} \mid \mathbf{R}^T\mathbf{R} = \mathbf{I},\ \det(\mathbf{R}) = 1 \right\}.$$

Each element $\mathbf{R} \in \mathrm{SO}(3)$ represents a rotation in three-dimensional space. SO(3) is a manifold, meaning that the standard vector space operations do not apply. Instead, rotations evolve on a Lie group structure [1, 158], where smooth transformations between elements are governed by an associated Lie algebra. The Lie algebra $\mathfrak{so}(3)$ is the tangent space of SO(3) at the identity and consists of all skew-symmetric matrices:

$$\mathfrak{so}(3) = \left\{ (\boldsymbol{\xi})_\times \in \mathbb{R}^{3\times 3} \mid (\boldsymbol{\xi})_\times^T = -(\boldsymbol{\xi})_\times \right\}.$$

For any vector $\boldsymbol{\xi} = \begin{pmatrix} \xi_1 & \xi_2 & \xi_3 \end{pmatrix}^T \in \mathbb{R}^3$, the corresponding skew-symmetric matrix is given by:

$$(\boldsymbol{\xi})_\times = \begin{pmatrix} 0 & -\xi_3 & \xi_2 \\ \xi_3 & 0 & -\xi_1 \\ -\xi_2 & \xi_1 & 0 \end{pmatrix}.$$

The skew-symmetric matrix satisfies the anti-symmetry property, given by:

$$(\boldsymbol{\xi}_1)_\times \boldsymbol{\xi}_2 = -(\boldsymbol{\xi}_2)_\times \boldsymbol{\xi}_1. \tag{1.4.1}$$

A skew-symmetric matrix is rank-deficient by construction; this can be easily shown by computing its determinant, which is equal to zero. In the following, Lemma 1.4.1 provides the rank property of vertically concatenated two three-by-three skew-symmetric matrices.

Lemma 1.4.1. *Given two linearly independent vectors* $\mathbf{u}, \mathbf{w} \in \mathbb{R}^3$*, the matrix* $\begin{pmatrix} (\mathbf{u})_\times \\ (\mathbf{w})_\times \end{pmatrix}$ *has full column rank.*

Proof. Let us assume that the matrix $\begin{pmatrix} (\mathbf{u})_\times \\ (\mathbf{w})_\times \end{pmatrix}$ is not a full column rank. This means that there exists a vector $\mathbf{f} \in \mathbb{R}^3 \setminus \{\mathbf{0}\}$ such that $\begin{pmatrix} (\mathbf{u})_\times \\ (\mathbf{w})_\times \end{pmatrix} \mathbf{f} = \mathbf{0}$ then $(\mathbf{u})_\times \mathbf{f} = \mathbf{0}$ and $(\mathbf{w})_\times \mathbf{f} = \mathbf{0}$, which give us $\mathbf{u} \times \mathbf{f} = \mathbf{0}$ and $\mathbf{w} \times \mathbf{f} = \mathbf{0}$, and thus both $\mathbf{u}$ and $\mathbf{f}$ are linearly dependent, and similarly, both $\mathbf{w}$ and $\mathbf{f}$ are linearly dependent. Consequently, $\mathbf{w}$ and $\mathbf{u}$ are linearly dependent. Therefore, the initial assumption that the matrix $\begin{pmatrix} (\mathbf{u})_\times \\ (\mathbf{w})_\times \end{pmatrix}$ does not have a full-column rank, must be false. Hence, it indeed has a full-column rank. ■

The exponential map:

The exponential map maps elements from the Lie algebra $\mathfrak{so}(3)$ to the Lie group SO(3), as following:

$$\mathbf{R} = \exp((\boldsymbol{\xi})_\times).$$

The exponential map is expressed as a power series:

$$\exp_m(\boldsymbol{\xi}) = \exp\left((\boldsymbol{\xi})_\times\right) = \sum_{i=0}^{\infty} \frac{(\boldsymbol{\xi})_\times^i}{i!},$$

the normalized vector $\mathbf{u}$ is defined as $\mathbf{u} = \frac{\boldsymbol{\xi}}{\|\boldsymbol{\xi}\|}$ (when $\|\boldsymbol{\xi}\| \neq 0$). To derive an explicit expression for the exponential map, the powers of the skew-symmetric matrix of the normalized vector are written as:

$$(\mathbf{u})_\times^0 = \mathbf{I}, \quad (\mathbf{u})_\times^2 = \mathbf{u}\mathbf{u}^T - \mathbf{I}, \quad (\mathbf{u})_\times^3 = -(\mathbf{u})_\times.$$

Using these properties, the exponential map can be written as:

$$\exp_m(\boldsymbol{\xi}) = \mathbf{I} + \left(\|\boldsymbol{\xi}\| - \frac{\|\boldsymbol{\xi}\|^3}{3!} + \frac{\|\boldsymbol{\xi}\|^5}{5!} + \cdots\right)(\mathbf{u})_\times + \left(\frac{\|\boldsymbol{\xi}\|^2}{2!} - \frac{\|\boldsymbol{\xi}\|^4}{4!} + \frac{\|\boldsymbol{\xi}\|^6}{6!} + \cdots\right)(\mathbf{u})_\times^2.$$

The series expansions of $\sin(\|\boldsymbol{\xi}\|)$ and $\cos(\|\boldsymbol{\xi}\|)$ are recognized, yielding the following expression:

$$\begin{cases} \boldsymbol{\xi} = \mathbf{0}, & \exp_m(\boldsymbol{\xi}) = \mathbf{I}_3, \\ \forall \boldsymbol{\xi} \in \mathbb{R}^3 \setminus \{\mathbf{0}\}, & \exp_m(\boldsymbol{\xi}) = \mathbf{I}_3 + \frac{\sin(\|\boldsymbol{\xi}\|)}{\|\boldsymbol{\xi}\|}(\boldsymbol{\xi})_\times + 2\frac{\sin(\|\boldsymbol{\xi}\|/2)^2}{\|\boldsymbol{\xi}\|^2}(\boldsymbol{\xi})_\times^2, \end{cases} \tag{1.4.2}$$

The exponential map satisfies:

$$\exp_m(\boldsymbol{\xi}_1)^{-1} = \exp_m(-\boldsymbol{\xi}_1). \tag{1.4.3}$$

The exponential map has the following first-order approximations:

$$\exp_m(\boldsymbol{\xi}_1) = \mathbf{I}_3 + (\boldsymbol{\xi}_1)_\times + \mathcal{O}(||\boldsymbol{\xi}_1||^2), \tag{1.4.4}$$

$$\exp_m(\boldsymbol{\xi}_1)\exp_m(\boldsymbol{\xi}_2) = \exp_m\left(\boldsymbol{\xi}_1 + \boldsymbol{\xi}_2 + \mathcal{O}(||\boldsymbol{\xi}_1||^2, ||\boldsymbol{\xi}_2||^2)\right), \tag{1.4.5}$$

where $\mathcal{O}(.)$ denotes the higher-order terms beyond the considered approximation. Equation (1.4.5) represents the Baker-Campbell-Hausdorff (BCH) formula, which is widely used in the design of Kalman filters on SO(3) [16, 18].

Logarithm Map: From SO(3) to $\mathfrak{so}(3)$

The logarithm map is the inverse of the exponential map:

$$\log_m(\mathbf{R}) = \frac{\theta}{2\sin\theta}(\mathbf{R} - \mathbf{R}^T), \quad \theta = \cos^{-1}\left(\frac{\text{trace}(\mathbf{R}) - 1}{2}\right).$$

Error Representation on SO(3)

Let $\mathbf{R} \in \text{SO}(3)$ be the true rotation matrix and $\hat{\mathbf{R}} \in \text{SO}(3)$ its estimate. The estimation error on SO(3) is defined as:

$$\mathbf{R}_e = \hat{\mathbf{R}}^{-1}\mathbf{R} \in \mathrm{SO}(3), \tag{1.4.6}$$

where $\mathbf{R}_e$ represents the relative rotation between the estimated and true attitudes. This error can be mapped to a $\boldsymbol{\xi} \in \mathbb{R}^3$ using the logarithm map, where the corresponding Lie algebra element is given by:

$$\log_m(\mathbf{R}_e) = (\boldsymbol{\xi})_\times \in \mathfrak{so}(3). \tag{1.4.7}$$

Since $\boldsymbol{\xi}$ provides a minimal parameterization of the attitude error in $\mathbb{R}^3$, the error covariance matrix is naturally defined as:

$$\mathbf{P}^\xi = \mathbf{E}(\boldsymbol{\xi}\boldsymbol{\xi}^T). \tag{1.4.8}$$

This formulation ensures a consistent representation of uncertainty on SO(3), where the estimation error is handled in the Lie algebra through $(\boldsymbol{\xi})_\times$, while its minimal representation in $\mathbb{R}^3$ allows efficient computations.

1.5. MARG Sensor and Attitude Dynamic Model

In this thesis, and in the following sensor models, we do not consider sensor biases or magnetic field disturbances.

Three-Axis Gyroscope Model:

The three-axis gyroscope measures the angular velocity vector of the rigid body expressed in the body frame. The considered measurement model is given by:

$$\boldsymbol{\omega}^m = \boldsymbol{\omega} + \mathbf{w}^\omega, \tag{1.5.1}$$

where $\boldsymbol{\omega}^m \in \mathbb{R}^3$ is the measured angular velocity, $\boldsymbol{\omega} \in \mathbb{R}^3$ is the true angular velocity, and $\mathbf{w}^\omega \in \mathbb{R}^3$ is the measurement noise, which is assumed to be a zero-mean white noise signal.

Three-Axis Accelerometer Model:

The three-axis accelerometer measures the total acceleration vector of the rigid body expressed in the body frame, which includes the Earth's gravity and external acceleration. The considered measurement model is given by:

$$\mathbf{a}^m = \mathbf{R}^T\mathbf{g} + \mathbf{a}^{ext} + \mathbf{w}^a, \tag{1.5.2}$$

where $\mathbf{a}^m \in \mathbb{R}^3$ is the measured acceleration, $\mathbf{R} \in \mathrm{SO}(3)$ is the rotation matrix, $\mathbf{g} \in \mathbb{R}^3$ is the gravity vector expressed in the navigation frame, $\mathbf{a}^{ext} \in \mathbb{R}^3$ represents the external

acceleration expressed in the body frame, and $\mathbf{w}^a \in \mathbb{R}^3$ is the measurement noise, which is assumed to be a zero-mean white noise signal.

The Earth's gravity vector is expressed in the North-East-Down (NED) frame as $\mathbf{g} = \begin{pmatrix} 0 & 0 & g \end{pmatrix}^T$ m/s^2, with $g \approx 9.81$ m/s^2.

Three-Axis Magnetometer Model:

The three-axis magnetometer measures the Earth's magnetic field expressed in the body frame, assuming the absence of magnetic disturbances. The considered measurement model is given by:

$$\mathbf{b}^m = \mathbf{R}^T \mathbf{m}_e + \mathbf{w}^b, \tag{1.5.3}$$

where $\mathbf{b}^m \in \mathbb{R}^3$ is the measured magnetic field, $\mathbf{R} \in \mathrm{SO}(3)$ is the rotation matrix, $\mathbf{m}_e \in \mathbb{R}^3$ is the Earth's magnetic field expressed in the navigation frame, and $\mathbf{w}^b \in \mathbb{R}^3$ is the magnetometer noise, which is assumed to be a zero-mean white noise signal.

In this thesis, magnetometer measurements are expressed in Gauss (G) for numerical examples, as this unit is commonly used in practice.

The Earth's magnetic field varies slowly over geographic displacement, and can be considered locally constant. Based on the World Magnetic Model [36], the approximated value near Grenoble, France, expressed in the NED frame, is

$$\mathbf{m}_e = \begin{pmatrix} 0.23 & 0.01 & 0.41 \end{pmatrix}^T \text{ G}.$$

Attitude Dynamic Model:

The attitude of a rigid body evolves over time according to the following dynamics:

$$\dot{\mathbf{R}} = \mathbf{R}(\boldsymbol{\omega})_\times, \tag{1.5.4}$$

where $\mathbf{R} \in \mathrm{SO}(3)$ is the rotation matrix, and $(\boldsymbol{\omega})_\times$ is the skew-symmetric matrix of the angular velocity. This equation describes the continuous-time evolution of the attitude.

Discrete-Time Model:

To derive the discrete-time model, it is assumed that the angular velocity remains constant during the time interval $[t_k, t_{k+1}]$, with $\Delta t = t_{k+1} - t_k$. The solution to the differential equation over this interval can be obtained by integrating the dynamics using the matrix exponential:

$$\mathbf{R}(t_{k+1}) = \mathbf{R}(t_k) \exp\left((\boldsymbol{\omega}_k)_\times \Delta t\right),$$

This update ensures that $\mathbf{R}(t_{k+1}) \in \mathrm{SO}(3)$, preserving the group structure under discrete propagation. We thus obtain the discrete-time attitude dynamics:

$$\mathbf{R}_{k+1} = \mathbf{R}_k \exp_m(\boldsymbol{\omega}_k \Delta t). \tag{1.5.5}$$

By substituting the gyroscope model (1.5.1) into the attitude dynamic model (1.5.5), the resulting dynamic, in which angular velocity measurements serve as input, is given by:

$$\mathbf{R}_{k+1} = \mathbf{R}_k \exp_m \left((\boldsymbol{\omega}_k^m - \mathbf{w}_k^\omega) \Delta t \right). \tag{1.5.6}$$

The attitude dynamic model (1.5.5) will be used in Chapter 2, where the true angular velocity $\boldsymbol{\omega}_k$ is treated as an unknown input, while the attitude dynamic model (1.5.6) will be used in the remaining chapters, where the measured angular velocity by a gyroscope $\boldsymbol{\omega}_k^m$, is an input to the attitude dynamics.

1.6. TRIAD Algorithm

This section presents the TRIAD algorithm, a classical solution to Wahba's problem based on two non-collinear vector measurements. The TRIAD method will be used as a reference for comparison in Chapter 2, and also in the simulation setup described in Chapter 3 and Chapter 4.

The TRIAD algorithm computes an attitude estimate based on two known reference vectors in the navigation frame, and their corresponding measurements in the body frame. The method constructs two orthonormal bases, one in the navigation frame and one in the body frame, and computes the rotation matrix that aligns the two frames. In the context of this work, the two reference vectors are the Earth's gravity and magnetic field, measured respectively by a three-axis accelerometer and a three-axis magnetometer. This approach assumes the absence of external acceleration and magnetic field disturbances. Under this assumption, the accelerometer measurement model (1.5.2) and the magnetometer measurement model (1.5.3) simplify to the following forms, where the external acceleration term has been removed from the accelerometer model (1.5.2):

$$\begin{aligned} \mathbf{a}^m &= \mathbf{R}^T \mathbf{g} + \mathbf{w}^a, \\ \mathbf{b}^m &= \mathbf{R}^T \mathbf{m}_e + \mathbf{w}^b, \end{aligned}$$

The steps of the TRIAD algorithm are summarized in Algorithm 1.

1.7. Invariant Extended Kalman Filter (IEKF) on SO(3)

This section presents IEKF on SO(3) for attitude estimation using MARG sensors, under the assumption of no external acceleration.

Dynamic Model and Output Function:

The discrete-time attitude dynamics and sensor output model are first recalled. The attitude dynamic model (1.5.6), along with the corresponding output consisting of the accelerometer measurements (1.5.2) (neglecting external acceleration) and the magnetometer

Algorithm 1 TRIAD Algorithm

Inputs: Reference vectors in navigation frame: $\mathbf{g}, \mathbf{m}_e$;
Corresponding measurements in body frame: $\mathbf{a}^m, \mathbf{b}^m$

▷ Construct TRIAD bases in navigation frame:

$\mathbf{x}_n = \frac{\mathbf{g}}{\|\mathbf{g}\|}$
$\mathbf{y}_n = \frac{\mathbf{x}_n \times \mathbf{m}_e}{\|\mathbf{x}_n \times \mathbf{m}_e\|}$
$\mathbf{z}_n = \mathbf{x}_n \times \mathbf{y}_n$

▷ Construct TRIAD bases in body frame:

$\mathbf{x}_b = \frac{\mathbf{a}^m}{\|\mathbf{a}^m\|}$
$\mathbf{y}_b = \frac{\mathbf{x}_b \times \mathbf{b}^m}{\|\mathbf{x}_b \times \mathbf{b}^m\|}$
$\mathbf{z}_b = \mathbf{x}_b \times \mathbf{y}_b$

▷ Form rotation matrix estimate:

$\mathbf{R}_n = (\mathbf{x}_n \ \mathbf{y}_n \ \mathbf{z}_n)$
$\mathbf{R}_b = (\mathbf{x}_b \ \mathbf{y}_b \ \mathbf{z}_b)$
$\hat{\mathbf{R}} = \mathbf{R}_n \mathbf{R}_b^T$
return $\hat{\mathbf{R}}$

measurements (1.5.3), are briefly recalled below:

$$\mathbf{R}_{k+1} = \mathbf{R}_k \exp_m (\boldsymbol{\omega}_k \Delta t), \tag{1.7.1}$$

$$\mathbf{y}_k = \mathbf{h}(\mathbf{R}_k) + \mathbf{w}_k^y, \tag{1.7.2}$$

where $\mathbf{R}_k \in \mathrm{SO}(3)$ denotes the rotation matrix at time step k, and $\boldsymbol{\omega}_k \in \mathbb{R}^3$ is the true angular velocity. The output measurement function $\mathbf{h}(\cdot)$ and the measurement noise $\mathbf{w}_k^y$ are defined as:

$$\mathbf{h}(\mathbf{R}) = \begin{pmatrix} \mathbf{R}^T \mathbf{g} \\ \mathbf{R}^T \mathbf{m}_e \end{pmatrix}, \qquad \mathbf{w}_k^y = \begin{pmatrix} \mathbf{w}_k^a \\ \mathbf{w}_k^b \end{pmatrix}, \tag{1.7.3}$$

where $\mathbf{g}$ is the Earth's gravity vector, $\mathbf{m}_e$ is the Earth's magnetic field, $\mathbf{w}_k^a$ is the accelerometer measurement noise, and $\mathbf{w}_k^b$ is the magnetometer measurement noise. The process noise $\mathbf{w}_k^\omega$ and the output measurement noise $\mathbf{w}_k^y$ are assumed to be uncorrelated and to have positive definite covariance matrices $\boldsymbol{\mathcal{Q}}_k$ and $\boldsymbol{\mathcal{R}}_k$, respectively.

Jacobian of the Output Function:

The Jacobian of the function $\mathbf{h}(\cdot)$ is derived in the following lemma. This result will be used throughout the remainder of the first part of this thesis, as the Jacobian is required in subsequent chapters.

Lemma 1.7.1. *Let $\mathbf{R} \in SO(3)$ and $\boldsymbol{\xi} \in \mathbb{R}^3$. The following relation holds:*

$$\left.\frac{\partial h\left(\hat{\mathbf{R}}_{k|k-1} \exp_m(\boldsymbol{\xi})\right)}{\partial \boldsymbol{\xi}}\right|_{\boldsymbol{\xi}=0} = \begin{pmatrix} \left(\hat{\mathbf{R}}^T \mathbf{g}\right)_\times \\ \left(\hat{\mathbf{R}}^T \mathbf{m}_e\right)_\times \end{pmatrix}. \tag{1.7.4}$$

Proof. For a general element $\mathbf{R} \in \mathrm{SO}(3)$ and a general perturbation $\boldsymbol{\xi} \in \mathbb{R}^3$, we compute:

$$\begin{aligned}
\mathbf{h}(\mathbf{R}\exp(\boldsymbol{\xi})) - \mathbf{h}(\mathbf{R}) &= \begin{pmatrix} (\mathbf{R}\exp(\boldsymbol{\xi}))^\top \mathbf{g} \\ (\mathbf{R}\exp(\boldsymbol{\xi}))^\top \mathbf{m}_e \end{pmatrix} - \begin{pmatrix} \mathbf{R}^\top \mathbf{g} \\ \mathbf{R}^\top \mathbf{m}_e \end{pmatrix}, \\
&= \begin{pmatrix} \exp(-\boldsymbol{\xi})\mathbf{R}^\top \mathbf{g} \\ \exp(-\boldsymbol{\xi})\mathbf{R}^\top \mathbf{m}_e \end{pmatrix} - \begin{pmatrix} \mathbf{R}^\top \mathbf{g} \\ \mathbf{R}^\top \mathbf{m}_e \end{pmatrix}, \\
&= \begin{pmatrix} (\exp(-\boldsymbol{\xi}) - \mathbf{I}_3)\mathbf{R}^\top \mathbf{g} \\ (\exp(-\boldsymbol{\xi}) - \mathbf{I}_3)\mathbf{R}^\top \mathbf{m}_e \end{pmatrix}.
\end{aligned}$$

Applying the first-order approximation (1.4.4), where $\boldsymbol{\xi}$ is close to zero, and the property (1.4.1) consequently gives:

$$\begin{aligned}
\mathbf{h}(\mathbf{R}\exp(\boldsymbol{\xi})) - \mathbf{h}(\mathbf{R}) &= \begin{pmatrix} -(\boldsymbol{\xi})_\times \mathbf{R}^\top \mathbf{g} \\ -(\boldsymbol{\xi})_\times \mathbf{R}^\top \mathbf{m}_e \end{pmatrix} + \mathcal{O}(\boldsymbol{\xi}^2), \\
&= \begin{pmatrix} (\mathbf{R}^\top \mathbf{g})_\times \\ (\mathbf{R}^\top \mathbf{m}_e)_\times \end{pmatrix} \boldsymbol{\xi} + \mathcal{O}(\boldsymbol{\xi}^2).
\end{aligned}$$

Therefore, the Jacobian is $\begin{pmatrix} (\mathbf{R}^\top \mathbf{g})_\times \\ (\mathbf{R}^\top \mathbf{m}_e)_\times \end{pmatrix}$. ■

IEKF on SO(3):

The IEKF on SO(3), used for attitude estimation based on MARG sensors, is presented in [5]. The inputs of the IEKF-SO(3) algorithm are the previously estimated attitude and its associated estimation error covariance matrix. The algorithm provides, as outputs, the estimated attitude along with the corresponding estimation error covariance matrix. Algorithm 2 presents the detailed steps of the recursive filter IEKF-SO(3).

The filter consists of two main stages: prediction and correction. In the prediction step, the attitude is propagated using the exponential map with the measured angular velocity $\boldsymbol{\omega}_{k-1}^m$. In the correction step, the innovation is computed using the difference between the measured output $\mathbf{y}_k$ and the expected output $\mathbf{h}(\hat{\mathbf{R}}_{k|k-1})$. The Jacobian $\mathbf{H}_k$ is constructed based on the predicted attitude and the known reference vectors. The Kalman gain $\mathbf{K}_k$ is then computed, and the attitude estimate is corrected using a right multiplication with the exponential of the correction term. The updated covariance is obtained using the standard Kalman update formula. The filter ensures that the attitude estimates remain on SO(3) at every step through the use of group operations based on the exponential map.

Algorithm 2 IEKF-SO(3)

Inputs: $\hat{\mathbf{R}}_{k-1}$, $\mathbf{P}^{\xi}_{k-1}$, $\boldsymbol{\omega}^{m}_{k-1}$, $\mathbf{y}_k = \begin{pmatrix} \mathbf{a}^{m}_{k} \\ \mathbf{b}^{m}_{k} \end{pmatrix}$

▷ Prediction:

$\hat{\mathbf{R}}_{k|k-1} = \hat{\mathbf{R}}_{k-1} \exp_m (\boldsymbol{\omega}^{m}_{k-1} \Delta t)$

$\mathbf{P}^{\xi}_{k|k-1} = \mathbf{P}^{\xi}_{k-1} + \Delta t^2 \boldsymbol{\mathcal{Q}}_{k-1}$

▷ Correction:

$\mathbf{H}_k = \begin{pmatrix} (\hat{\mathbf{R}}^{T}_{k|k-1}\mathbf{g})_{\times} \\ (\hat{\mathbf{R}}^{T}_{k|k-1}\mathbf{m}_e)_{\times} \end{pmatrix}$

$\tilde{\boldsymbol{\mathcal{R}}}_k = \mathbf{H}_k \mathbf{P}^{\xi}_{k|k-1} \mathbf{H}^{T}_{k} + \boldsymbol{\mathcal{R}}_k$

$\mathbf{K}_k = \mathbf{P}^{\xi}_{k|k-1} \mathbf{H}^{T}_{k} \tilde{\boldsymbol{\mathcal{R}}}^{-1}_{k}$

$\hat{\mathbf{R}}_k = \hat{\mathbf{R}}_{k|k-1} \exp_m \left(\mathbf{K}_k \left(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) \right) \right)$

$\mathbf{P}^{\xi}_{k} = (\mathbf{I} - \mathbf{K}_k \mathbf{H}_k) \mathbf{P}^{\xi}_{k|k-1}$

return $\hat{\mathbf{R}}_k$, $\mathbf{P}^{\xi}_{k}$

Remarks on the choice of comparison algorithm

The filter parameters play a central role in attitude estimation accuracy. In [26], experiments in nine scenarios, including three rotation rates and three commercial products, show that, when optimally tuned, no statistically significant differences are observed among different attitude estimation algorithms in all tested scenarios based on MARG sensors. These algorithms include the Madgwick filter [115], the Mahony filter [116], and Kalman-like filters.

A large number of studies aimed at comparatively evaluating different attitude estimation algorithms based on MARG sensors have reported contradictory results, which is not surprising given the previous discussion [50, 60, 70, 115, 120, 135, 148, 175, 186]. A summary of the results of these comparative studies is presented in [26]. The differences in results are likely due to not using the best parameters for the compared algorithms, which vary depending on the hardware, sensor noise, rotation rates, external acceleration, magnetic field disturbances, type of motion, and other factors.

Therefore, in this thesis, the proposed algorithms are compared with algorithms based on the IEKF-SO(3) to ensure a fair comparison. Since the new algorithms proposed in this thesis are also based on the IEKF-SO(3), the same parameters can be used for all comparative studies, ensuring a fair and consistent evaluation.

Chapter 2

Gyro-Free Attitude Estimation Based on a Three-Axis Accelerometer and a Three-Axis Magnetometer

This chapter starts with the introductory Section 2.1, which explains the attitude dynamics on SO(3) and the output measurements model, the motivation for avoiding the use of a gyroscope, and the existing solutions in the literature for attitude estimation without gyroscopes. It then presents the derivation of two new algorithms proposed in this chapter, based on treating the angular velocity as an unknown input affecting the system dynamics: UMV-SO(3) in Section 2.2, and RTSKF-SO(3) in Section 2.3. Section 2.4 provides an evaluation of both algorithms through simulation and experimental data. Finally, Section 2.5 concludes the chapter and prepares the reader for Chapter 3. [1]

2.1. Preliminaries and Problem Statement

This chapter addresses the problem of attitude estimation based solely on accelerometer and magnetometer measurements, along with the attitude dynamic model, without relying on gyroscope measurements. External acceleration and magnetic field disturbances are not considered in this chapter. The attitude dynamic model (1.5.5), along with the corresponding output consisting of the accelerometer measurements (1.5.2) (neglecting external acceleration) and the magnetometer measurements (1.5.3), are briefly recalled below:

$$\mathbf{R}_{k+1} = \mathbf{R}_k \exp_m (\boldsymbol{\omega}_k \Delta t), \tag{2.1.1}$$

$$\mathbf{y}_k = \mathbf{h}(\mathbf{R}_k) + \mathbf{w}_k^y, \tag{2.1.2}$$

where $\mathbf{R}_k \in \mathrm{SO}(3)$ denotes the rotation matrix at time step k, and $\boldsymbol{\omega}_k \in \mathbb{R}^3$ is the true angular velocity. The output measurement function $\mathbf{h}(\cdot)$ and the measurement noise $\mathbf{w}_k^y$ are

[1] Before reading this chapter, it is recommended to first read Chapter 1.

defined as:

$$\mathbf{h}(\mathbf{R}) = \begin{pmatrix} \mathbf{R}^T\mathbf{g} \\ \mathbf{R}^T\mathbf{m}_e \end{pmatrix}, \qquad \mathbf{w}_k^y = \begin{pmatrix} \mathbf{w}_k^a \\ \mathbf{w}_k^b \end{pmatrix}, \tag{2.1.3}$$

where $\mathbf{g}$ is the Earth's gravity vector, $\mathbf{m}_e$ is the Earth's magnetic field, $\mathbf{w}_k^a$ is the accelerometer measurement noise, and $\mathbf{w}_k^b$ is the magnetometer measurement noise. The output noise $\mathbf{w}_k^y$ has a positive definite covariance matrix $\boldsymbol{\mathcal{R}}_k$.

In the past, large, expensive, and power-consuming gyroscopes were developed for measuring the angular velocity. However, with the introduction of low-cost Micro-electro-mechanical Systems (MEMS), the size and cost of gyroscopes have significantly reduced [166]. Although MEMS gyroscopes offer advantages, they also have some drawbacks. One of the main drawbacks is that MEMS gyroscopes have a relatively high-power consumption compared to accelerometers and magnetometers, with MEMS accelerometers and magnetometers operating in the microampere range while MEMS gyroscopes typically require a few milliamperes [108, 117, 174]. Such high current consumption is unsuitable for applications requiring low-power consumption, such as smart devices (e.g., smartphones and tablets). Another important drawback of MEMS gyroscopes, especially in low-cost IMU, is their susceptibility to drift and bias [79]. Gyroscopes are also prone to noise, which tends to increase over time. Also, in order to use dynamic algorithms such as the IEKF-SO(3), introduced in Section 1.7, the covariance matrix of this noise should be known, which can be challenging and may not always be feasible.

To avoid the use of gyroscope, one existing solution consists in applying static attitude estimation algorithms, utilizing only observations from accelerometer and magnetometer sensors, without taking into account the history of measurements or the dynamic model, like TRIAD algorithm introduced in Section 1.6. In [118], a parsimonious use of the gyroscope is achieved by alternately turning the sensor on and off, in a manner that balances power consumption and attitude estimation accuracy. Additionally, there have been several studies in the literature that concentrate on developing angular motion estimation algorithms, to be able to achieve attitude estimation task without gyroscope. These algorithms are commonly known as gyro-free attitude estimation techniques [136, 165, 174]. Such algorithms rely on utilizing several accelerometers placed in specific spatial configurations. However, these works require knowledge of the sensors' exact positions and consider the measurements to be deterministic.

This chapter addresses the problem of gyro-free attitude estimation by treating the angular velocity measurements as unknown inputs. In the model (2.1.1)–(2.1.2), the angular velocity appears the system dynamics but does not have direct feedthrough to the output. Two recursive estimation algorithms are desinged in this chapter: UMV-SO(3), based on the Unbiased Minimum-Variance (UMV) algorithm [65], and RTSKF-SO(3), based on the Robust Two-Stage Kalman Filter (RTSKF) [82]. Both algorithms in [65, 82] were originally developed for linear systems in which unknown inputs affect the state dynamics but have no direct feedthrough to the output. While they address the same estimation problem, the two filters rely on different theoretical formulations and filtering strategies within the linear systems framework.

The primary focus is on the development of the UMV-SO(3) algorithm, in Section 2.2, which is presented with full theoretical details. In contrast, the derivation of RTSKF-SO(3), in Section 2.3, is presented more concisely. This is due to the structural similarity of several steps with those already developed for UMV-SO(3), allowing the use of shared intermediate results and avoiding unnecessary repetition. By including both algorithms, this chapter provides a broader perspective on filtering strategies for attitude estimation under unknown inputs. It illustrates how different methodologies from linear systems theory can be generalized to SO(3), enabling a structured comparison of their performance within the same estimation framework. The comparative analysis, presented later in the chapter, highlights the advantages of UMV-SO(3) in terms of estimation accuracy, as demonstrated through both simulation results and real experimental data in Section 2.4.

The main contributions of this chapter are:

- Development of two algorithms for state estimation on SO(3) with an unknown input affecting the dynamic model without direct feedthrough to the output.
- Design of two novel gyro-free attitude estimation algorithms based solely on accelerometer and magnetometer measurements, by treating the angular velocity as an unknown input.

The material presented in this chapter is based on the corresponding publications:

- *G. Shaaban, H. Fourati, A. Kibangou, and C. Prieur, "Attitude estimation on SO(3) with unknown input," International Journal of Robust and Nonlinear Control (IJRNC), accepted in July 2025.*
- *G. Shaaban, H. Fourati, A. Kibangou, and C. Prieur, "Gyro-free Kalman filter with unknown inputs for SO(3)-based attitude estimation," in IEEE 13th International Conference Indoor Positioning and Indoor Navigation (IPIN), Nuremberg, Germany, 2023.*

2.2. UMV-SO(3) Algorithm Derivation

For linear discrete-time systems with unknown input without having direct feedthrough to the output, the four-step Kalman filter was introduced in [65] for unbiased minimum variance state estimation. The first step gives a biased prediction of the state due to the unknown input, based on an unbiased state estimation in the previous time step and the dynamic model. The second step gives an unbiased minimum variance estimate of the unknown input using the measurements. The third step uses the unbiased estimate of the unknown input to obtain an unbiased prior estimation of the state. Finally, the fourth step minimizes the state estimation variance using a correction similar to the Kalman filter. Based on the same

principle, we propose the filter UMV-SO(3) based on the following equations:

$$\hat{\mathbf{R}}_{k|k-1} = \hat{\mathbf{R}}_{k-1} \tag{2.2.1}$$

$$\hat{\boldsymbol{\omega}}_{k-1} = \frac{1}{\Delta t}\mathbf{M}_k \left(\mathbf{y}_k - \mathbf{h}\left(\hat{\mathbf{R}}_{k|k-1}\right)\right) \tag{2.2.2}$$

$$\hat{\mathbf{R}}^*_k = \hat{\mathbf{R}}_{k|k-1} \exp_m\left(\hat{\boldsymbol{\omega}}_{k-1}\Delta t\right) \tag{2.2.3}$$

$$\hat{\mathbf{R}}_k = \hat{\mathbf{R}}^*_k \exp_m\left(\mathbf{K}_k \left(\mathbf{y}_k - \mathbf{h}\left(\hat{\mathbf{R}}^*_k\right)\right)\right) \tag{2.2.4}$$

where the matrices $\mathbf{M}_k \in \mathbb{R}^{3\times 6}$, and $\mathbf{K}_k \in \mathbb{R}^{3\times 6}$ are the gain matrices which have to be designed.

Main goal: *Considering $\hat{\mathbf{R}}_{k-1}$ as unbiased, the objective is to design $\mathbf{M}_k$ and $\mathbf{K}_k$ so that the first-order approximation-based estimators of $\hat{\boldsymbol{\omega}}_{k-1}$ and $\hat{\mathbf{R}}_k$ given by (2.2.2)-(2.2.4) are unbiased minimum variance (see Theorem 2.2.4 and Theorem 2.2.8).*

We define the prediction error $\exp_m(\boldsymbol{\xi}_{k|k-1}) = \hat{\mathbf{R}}^{-1}_{k|k-1}\mathbf{R}_k$, the prior estimation error $\exp_m(\boldsymbol{\xi}^*_k) = \hat{\mathbf{R}}^{*-1}_k\mathbf{R}_k$, and the estimation error $\exp_m(\boldsymbol{\xi}_k) = \hat{\mathbf{R}}^{-1}_k\mathbf{R}_k$, with the corresponding second-order moment $\mathbf{P}^{\xi}_{k|k-1} = \mathbf{E}(\boldsymbol{\xi}_{k|k-1}\boldsymbol{\xi}^T_{k|k-1})$, and covariance matrices $\mathbf{P}^{\xi*}_k = \mathbf{E}(\boldsymbol{\xi}^*_k\boldsymbol{\xi}^{*T}_k)$, and $\mathbf{P}^{\xi}_k = \mathbf{E}(\boldsymbol{\xi}_k\boldsymbol{\xi}^T_k)$, respectively. In the following, the steps of the algorithm are derived, starting with the prediction step (2.2.1), followed by the estimation of the unknown input (2.2.2), the prior state estimation (2.2.3), and the correction step (2.2.4). A summary of the complete algorithm is then provided.

Prediction:

The prediction error equation associated with (2.2.1) is formally derived in Lemma 2.2.1, which follows, and it is used in the subsequent algorithm derivation and implementation.

Lemma 2.2.1. *Let $\hat{\mathbf{R}}_{k-1}$ be unbiased, then the first-order approximation-based predictor (2.2.1) has prediction error*

$$\boldsymbol{\xi}_{k|k-1} = \boldsymbol{\xi}_{k-1} + \boldsymbol{\omega}_{k-1}\Delta t, \tag{2.2.5}$$

with expected value $\mathbf{E}(\boldsymbol{\xi}_{k|k-1}) = \boldsymbol{\omega}_{k-1}\Delta t$.

Proof. Starting with the prediction error equation $\exp_m(\boldsymbol{\xi}_{k|k-1}) = \hat{\mathbf{R}}^{-1}_{k|k-1}\mathbf{R}_k$, then employing the rotation dynamic (2.1.1) and the filter's first step (2.2.1) yields:

$$\begin{aligned}\exp_m(\boldsymbol{\xi}_{k|k-1}) &= \hat{\mathbf{R}}^{-1}_{k-1}\mathbf{R}_{k-1}\exp_m(\boldsymbol{\omega}_{k-1}\Delta t),\\ &= \exp_m(\boldsymbol{\xi}_{k-1})\exp_m(\boldsymbol{\omega}_{k-1}\Delta t).\end{aligned}$$

Applying the BCH approximation (1.4.5) gives:

$$\boldsymbol{\xi}_{k|k-1} = \boldsymbol{\xi}_{k-1} + \boldsymbol{\omega}_{k-1}\Delta t,$$

and yields $\mathbf{E}(\boldsymbol{\xi}_{k|k-1}) = \boldsymbol{\omega}_{k-1}\Delta t$, since $\mathbf{E}(\boldsymbol{\xi}_{k-1}) = \mathbf{0}$ (unbiased $\mathbf{R}_{k-1}$). ■

Unknown Input Estimation:

We define $\mathbf{H}_k$ which is the Jacobian of the output function $\mathbf{h}(.)$ with respect to the prediction error $\mathbf{H}_k = \frac{\partial \mathbf{h}\left(\hat{\mathbf{R}}_{k|k-1} \exp_m(\boldsymbol{\xi})\right)}{\partial \boldsymbol{\xi}}|_{\boldsymbol{\xi}=\mathbf{0}}$, it has the following value (see Lemma 1.7.1):

$$\mathbf{H}_k = \begin{pmatrix} (\hat{\mathbf{R}}_{k|k-1}^T \mathbf{g})_\times \\ (\hat{\mathbf{R}}_{k|k-1}^T \mathbf{m}_e)_\times \end{pmatrix}.$$

The matrix $\mathbf{H}_k$ is full column rank (see Lemma 1.4.1). We define variable $\tilde{\mathbf{e}}_k$:

$$\tilde{\mathbf{e}}_k = \mathbf{H}_k \boldsymbol{\xi}_{k-1} + \mathbf{w}_k^y. \tag{2.2.6}$$

The expected value of $\tilde{\mathbf{e}}_k$ is $\mathbf{E}(\tilde{\mathbf{e}}_k) = \mathbf{0}$ since $\mathbf{E}(\boldsymbol{\xi}_{k-1}) = \mathbf{0}$ (unbiased $\mathbf{R}_{k-1}$), and $\mathbf{E}(\mathbf{w}_k^y) = \mathbf{0}$ (zero mean measurement noise). The covariance matrix of $\tilde{\mathbf{e}}_k$ is given by:

$$\tilde{\boldsymbol{\mathcal{R}}}_k = \mathbf{E}(\tilde{\mathbf{e}}_k \tilde{\mathbf{e}}_k^T) = \mathbf{H}_k \mathbf{P}_{k-1}^\xi \mathbf{H}_k^T + \boldsymbol{\mathcal{R}}_k, \tag{2.2.7}$$

Sufficient conditions for the local optimality of the unknown input estimator (2.2.2) are established in Theorem 2.2.4, with the support of Lemma 2.2.2 and Lemma 2.2.3, all of which are presented below.

Lemma 2.2.2. *Let $\mathbf{R}_{k-1}$ be unbiased, then the innovation $\tilde{\mathbf{y}}_k = \mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1})$ found in the unknown input estimator (2.2.2) can be approximated as:*

$$\tilde{\mathbf{y}}_k = \mathbf{H}_k \boldsymbol{\omega}_{k-1} \Delta t + \tilde{\mathbf{e}}_k. \tag{2.2.8}$$

Proof. Substituting $\mathbf{y}_k$ (2.1.2) gives:

$$\begin{aligned} \tilde{\mathbf{y}}_k =& \mathbf{h}(\mathbf{R}_k) - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) + \mathbf{w}_k^y, \\ =& \mathbf{h}(\hat{\mathbf{R}}_{k|k-1} \exp_m(\boldsymbol{\xi}_{k|k-1})) - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) + \mathbf{w}_k^y, \end{aligned}$$

applying the first order approximation $\mathbf{h}(\hat{\mathbf{R}}_{k|k-1} \exp_m(\boldsymbol{\xi}_{k|k-1})) - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) = \mathbf{H}_k \boldsymbol{\xi}_{k|k-1} + \mathcal{O}(\boldsymbol{\xi}_{k|k-1})$ gives:

$$\tilde{\mathbf{y}}_k = \mathbf{H}_k \boldsymbol{\xi}_{k|k-1} + \mathbf{w}_k^y. \tag{2.2.9}$$

Lemma 2.2.1 holds, thus (2.2.5) is satisfied. Substituting (2.2.5) in (2.2.9), gives:

$$\begin{aligned} \tilde{\mathbf{y}}_k &= \mathbf{H}_k(\boldsymbol{\xi}_{k-1} + \boldsymbol{\omega}_{k-1} \Delta t) + \mathbf{w}_k^y, \\ &= \mathbf{H}_k \boldsymbol{\omega}_{k-1} \Delta t + \mathbf{H}_k \boldsymbol{\xi}_{k-1} + \mathbf{w}_k^y, \\ &= \mathbf{H}_k \boldsymbol{\omega}_{k-1} \Delta t + \tilde{\mathbf{e}}_k. \end{aligned}$$

■

Lemma 2.2.3. *Let $\mathbf{R}_{k-1}$ be unbiased, then the first-order approximation-based unknown input estimator (2.2.2) is unbiased if and only if the gain matrix $\mathbf{M}_k$ satisfies*

$$\mathbf{M}_k\mathbf{H}_k = \mathbf{I}_3, \tag{2.2.10}$$

and thus the unknown input estimation error is:

$$\boldsymbol{\omega}_{k-1} - \hat{\boldsymbol{\omega}}_{k-1} = -\frac{1}{\Delta t}\mathbf{M}_k\tilde{\mathbf{e}}_k. \tag{2.2.11}$$

Proof. Lemma 2.2.2 holds, thus (2.2.8) is satisfied, substituting it in the estimator (2.2.2) gives $\hat{\boldsymbol{\omega}}_{k-1} = \mathbf{M}_k\mathbf{H}_k\boldsymbol{\omega}_{k-1} + \frac{1}{\Delta t}\mathbf{M}_k\tilde{\mathbf{e}}_k$, and thus the expected value is $\mathbf{E}(\hat{\boldsymbol{\omega}}_{k-1}) = \mathbf{M}_k\mathbf{H}_k\boldsymbol{\omega}_{k-1}$ since $\mathbf{E}(\tilde{\mathbf{e}}_k) = \mathbf{0}$ (Lemma 2.2.2). Therefore we conclude that the condition $\mathbf{M}_k\mathbf{H}_k = \mathbf{I}_3$ is necessary and sufficient for $\mathbf{E}(\hat{\boldsymbol{\omega}}_{k-1}) = \boldsymbol{\omega}_{k-1}$. In this case, the unknown input estimate becomes $\hat{\boldsymbol{\omega}}_{k-1} = \boldsymbol{\omega}_{k-1} + \frac{1}{\Delta t}\mathbf{M}_k\tilde{\mathbf{e}}_k$. Finally, the unknown input estimation error is given by $\boldsymbol{\omega}_{k-1} - \hat{\boldsymbol{\omega}}_{k-1} = -\frac{1}{\Delta t}\mathbf{M}_k\tilde{\mathbf{e}}_k$. ■

Theorem 2.2.4. *Assume $\mathbf{R}_{k-1}$ is unbiased, and $\mathbf{M}_k = \left(\mathbf{H}_k^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{H}_k\right)^{-1}\mathbf{H}_k^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$, then the first-order approximation–based estimator (2.2.2) is unbiased minimum variance.*

Proof. Applying Lemma 2.2.2 enables us to use the approximated model (2.2.8), where $\tilde{\mathbf{e}}_k$ has a zero mean and a positive definite covariance matrix. The matrix $\mathbf{H}_k$ has full column rank, thus, the sufficient conditions for applying the Gauss-Markov Theorem [93, Chapter 3.4.2] are satisfied. Consequently, the first-order approximation-based estimator (2.2.2) is an unbiased minimum variance when $\mathbf{M}_k = \left(\mathbf{H}_k^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{H}_k\right)^{-1}\mathbf{H}_k^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$. ■

Prior State Estimation:

The prior state estimation error equation, used in the subsequent algorithm derivation, is established in Lemma 2.2.5, which follows.

Lemma 2.2.5. *Let $\mathbf{R}_{k-1}$ be unbiased, and the estimator (2.2.2) be unbiased, then the first-order approximation-based prior estimator (2.2.3) is unbiased, and*

$$\boldsymbol{\xi}_k^* = -\mathbf{M}_k\mathbf{w}_k^y. \tag{2.2.12}$$

Proof. Starting with the prior estimation error equation $\exp_m(\boldsymbol{\xi}_k^*) = \hat{\mathbf{R}}_k^{*-1}\mathbf{R}_k$, then employing the filter's third step (2.2.3) yields

$$\begin{aligned}\exp_m(\boldsymbol{\xi}_k^*) &= \exp_m(-\hat{\boldsymbol{\omega}}_{k-1}\Delta t)\hat{\mathbf{R}}_{k|k-1}^{-1}\mathbf{R}_k \\ &= \exp_m(-\hat{\boldsymbol{\omega}}_{k-1}\Delta t)\exp_m(\boldsymbol{\xi}_{k|k-1}).\end{aligned}$$

Applying the BCH approximation (1.4.5) gives $\boldsymbol{\xi}_k^* = -\hat{\boldsymbol{\omega}}_{k-1}\Delta t + \boldsymbol{\xi}_{k|k-1}$, and then substituting (2.2.5) gives:

$$\boldsymbol{\xi}_k^* = \boldsymbol{\omega}_{k-1}\Delta t - \hat{\boldsymbol{\omega}}_{k-1}\Delta t + \boldsymbol{\xi}_{k-1}. \tag{2.2.13}$$

Lemma 2.2.3 holds, thus (2.2.10) and (2.2.11) are satisfied. Substituting (2.2.11), (2.2.6), and (2.2.10) sequentially in (2.2.13) gives:

$$\begin{aligned}\boldsymbol{\xi}_k^* =& -\mathbf{M}_k\tilde{\mathbf{e}}_k + \boldsymbol{\xi}_{k-1},\\ =& -\mathbf{M}_k(\mathbf{H}_k\boldsymbol{\xi}_{k-1} + \mathbf{w}_k^y) + \boldsymbol{\xi}_{k-1},\\ =& -\mathbf{M}_k\mathbf{w}_k^y,\end{aligned}$$

and yields $\mathbf{E}(\boldsymbol{\xi}_k^*) = \mathbf{0}$, since $\mathbf{E}(\mathbf{w}_{k-1}^y) = \mathbf{0}$ (unbiased measurement noise). ■

Correction:

We define $\mathbf{H}_k^*$ which is the Jacobian of the observation function with respect to the prior estimation error $\mathbf{H}_k^* = \frac{\partial h\left(\hat{\mathbf{R}}_k^* \exp_m(\boldsymbol{\xi})\right)}{\partial \boldsymbol{\xi}}|_{\boldsymbol{\xi}=\mathbf{0}}$, it has the following value (see Lemma 1.7.1):

$$\mathbf{H}_k^* = \begin{pmatrix} (\hat{\mathbf{R}}_k^{*T}\mathbf{g})_\times \\ (\hat{\mathbf{R}}_k^{*T}\mathbf{m}_e)_\times \end{pmatrix},$$

The sufficient conditions for the local optimality of the estimator (2.2.4) are established in Theorem 2.2.8, with the support of Lemma 2.2.6 and Lemma 2.2.7, all of which are presented below.

Lemma 2.2.6. *Let $\mathbf{R}_{k-1}$ be unbiased, and the estimator (2.2.2) be unbiased, then the first-order approximation-based estimator (2.2.4) is unbiased, and*

$$\boldsymbol{\xi}_k = -\mathbf{M}_k\mathbf{w}_k^y + \mathbf{K}_k\mathbf{H}_k^*\mathbf{M}_k\mathbf{w}_k^y - \mathbf{K}_k\mathbf{w}_k^y. \tag{2.2.14}$$

Proof. Starting with the estimation error equation $\exp_m(\boldsymbol{\xi}_k) = \hat{\mathbf{R}}_k^{-1}\mathbf{R}_k$, then employing the filter's fourth step (2.2.4) yields

$$\begin{aligned}\exp_m(\boldsymbol{\xi}_k) &= \exp_m(-\mathbf{K}_k(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_k^*)))\hat{\mathbf{R}}_k^{*-1}\mathbf{R}_k\\ &= \exp_m(-\mathbf{K}_k(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_k^*)))\exp_m(\boldsymbol{\xi}_k^*).\end{aligned}$$

Applying the BCH approximation (1.4.5) gives $\boldsymbol{\xi}_k = \boldsymbol{\xi}_k^* - \mathbf{K}_k(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_k^*))$, and then substituting (2.1.2) gives:

$$\begin{aligned}\boldsymbol{\xi}_k =& \boldsymbol{\xi}_k^* - \mathbf{K}_k(\mathbf{h}(\mathbf{R}_k) - \mathbf{h}(\hat{\mathbf{R}}_k^*) + \mathbf{w}_k^y),\\ =& \boldsymbol{\xi}_k^* - \mathbf{K}_k(\mathbf{h}(\hat{\mathbf{R}}_k^*\exp_m(\boldsymbol{\xi}_k^*)) - \mathbf{h}(\hat{\mathbf{R}}_k^*) + \mathbf{w}_k^y),\\ =& \boldsymbol{\xi}_k^* - \mathbf{K}_k\mathbf{H}_k^*\boldsymbol{\xi}_k^* - \mathbf{K}_k\mathbf{w}_k^y.\end{aligned} \tag{2.2.15}$$

Lemma 2.2.5 holds, thus (2.2.12) is satisfied, substituting it in (2.2.15) gives:

$$\boldsymbol{\xi}_k = -\mathbf{M}_k\mathbf{w}_k^y + \mathbf{K}_k\mathbf{H}_k^*\mathbf{M}_k\mathbf{w}_k^y - \mathbf{K}_k\mathbf{w}_k^y.$$

and yields $\mathbf{E}(\boldsymbol{\xi}_k) = \mathbf{0}$, since $\mathbf{E}(\mathbf{w}_k^y) = \mathbf{0}$ (zero mean measurement noise). ■

We aim to minimize $\mathbf{E}(\|\boldsymbol{\xi}_k\|^2)$ which is equivalent to minimize the trace of the $\mathbf{P}_k^{\xi} = \mathbf{E}(\boldsymbol{\xi}_k\boldsymbol{\xi}_k^T)$. Given that $\boldsymbol{\xi}_{k-1}$ is unbiased, and the estimator (2.2.2) is unbiased, then we can utilize (2.2.14) (Lemma 2.2.6), thus the state estimation error covariance matrix $\mathbf{P}_k^{\xi} = \mathbf{E}(\boldsymbol{\xi}_k\boldsymbol{\xi}_k^T)$ has the following expression:

$$\begin{aligned}
\mathbf{P}_k^{\xi} =& \mathbf{E}((-\mathbf{M}_k\mathbf{w}_k^y + \mathbf{K}_k\mathbf{H}_k^*\mathbf{M}_k\mathbf{w}_k^y - \mathbf{K}_k\mathbf{w}_k^y)(-\mathbf{M}_k\mathbf{w}_k^y + \mathbf{K}_k\mathbf{H}_k^*\mathbf{M}_k\mathbf{w}_k^y - \mathbf{K}_k\mathbf{w}_k^y)^T),\\
=&(-\mathbf{M}_k - \mathbf{K}_k(\mathbf{I}_6 - \mathbf{H}_k^*\mathbf{M}_k))\mathbf{E}(\mathbf{w}_k^y\mathbf{w}_k^{yT})(-\mathbf{M}_k - \mathbf{K}_k(\mathbf{I}_6 - \mathbf{H}_k^*\mathbf{M}_k))^T,\\
=&(\mathbf{M}_k + \mathbf{K}_k(\mathbf{I}_6 - \mathbf{H}_k^*\mathbf{M}_k))\boldsymbol{\mathcal{R}}_k(\mathbf{M}_k + \mathbf{K}_k(\mathbf{I}_6 - \mathbf{H}_k^*\mathbf{M}_k))^T,\\
=&\mathbf{K}_k\left((\mathbf{I}_6 - \mathbf{H}_k^*\mathbf{M}_k)\boldsymbol{\mathcal{R}}_k(\mathbf{I}_6 - \mathbf{H}_k^*\mathbf{M}_k)^T\right)\mathbf{K}_k^T + \mathbf{M}_k\boldsymbol{\mathcal{R}}_k(\mathbf{I}_6 - \mathbf{H}_k^*\mathbf{M}_k)^T\mathbf{K}_k^T\\
&+ \mathbf{K}_k(\mathbf{I}_6 - \mathbf{H}_k^*\mathbf{M}_k)\boldsymbol{\mathcal{R}}_k\mathbf{M}_k^T + \mathbf{M}_k\boldsymbol{\mathcal{R}}_k\mathbf{M}_k^T. \qquad (2.2.16)
\end{aligned}$$

We define two variables $\boldsymbol{\mathcal{R}}_k^*$ and $\boldsymbol{\mathcal{S}}_k^*$ as follows:

$$\boldsymbol{\mathcal{R}}_k^* = (\mathbf{I}_6 - \mathbf{H}_k^*\mathbf{M}_k)\boldsymbol{\mathcal{R}}_k(\mathbf{I}_6 - \mathbf{H}_k^*\mathbf{M}_k)^T, \qquad (2.2.17)$$

$$\boldsymbol{\mathcal{S}}_k^* = \mathbf{M}_k\boldsymbol{\mathcal{R}}_k(\mathbf{I}_6 - \mathbf{H}_k^*\mathbf{M}_k)^T. \qquad (2.2.18)$$

Thus:

$$\mathbf{P}_k^{\xi} = \mathbf{K}_k\boldsymbol{\mathcal{R}}^*\mathbf{K}_k^T + \boldsymbol{\mathcal{S}}_k^*\mathbf{K}_k^T + \mathbf{K}_k\boldsymbol{\mathcal{S}}_k^{*T} + \mathbf{M}_k\boldsymbol{\mathcal{R}}_k\mathbf{M}_k^T. \qquad (2.2.19)$$

By utilizing the matrix derivatives [12, Propositions 10.7.2 and 10.7.4], we obtain:

$$\frac{dtr(\mathbf{P}_k^{\xi})}{d\mathbf{K}_k} = 2\mathbf{K}_k\boldsymbol{\mathcal{R}}_k^* + 2\boldsymbol{\mathcal{S}}_k^*.$$

Minimizing the trace $tr(\mathbf{P}_k^{\xi})$ means $\frac{dtr(\mathbf{P}_k^{\xi})}{d\mathbf{K}_k} = \mathbf{0}$, thus we aim to find $\mathbf{K}_k$ that satisfies:

$$\mathbf{K}_k\boldsymbol{\mathcal{R}}_k^* + \boldsymbol{\mathcal{S}}_k^* = \mathbf{0}. \qquad (2.2.20)$$

The matrix $\boldsymbol{\mathcal{R}}_k^* \in \mathbb{R}^{6\times 6}$, which is a real symmetric matrix, has no guarantee to be invertible. Let p_k be the rank of $\boldsymbol{\mathcal{R}}_k^*$, i.e $p_k \leq 6$. Consequently, there is no unique $\mathbf{K}_k$ that satisfies (2.2.20), we then propose $\mathbf{K}_k$ to be in the following form:

$$\mathbf{K}_k = \mathbf{K}_k^*\boldsymbol{\Gamma}_k, \qquad (2.2.21)$$

where $\boldsymbol{\Gamma}_k \in \mathbb{R}^{p_k\times 6}$ is a matrix that satisfies the invertibility of the matrix $\boldsymbol{\Gamma}_k\boldsymbol{\mathcal{R}}_k^*\boldsymbol{\Gamma}_k^T \in \mathbb{R}^{p_k\times p_k}$, and $\mathbf{K}_k^* \in \mathbb{R}^{3\times p_k}$ is designed to minimize the trace $tr(\mathbf{P}_k^{\xi})$. Lemma 2.2.7 proves that such $\boldsymbol{\Gamma}_k$ exists, and one solution is provided in the proof.

Lemma 2.2.7. *For a real symmetric matrix $\boldsymbol{\mathcal{R}}_k^* \in \mathbb{R}^{6\times 6}$ with rank $1 \leq p_k \leq 6$, there exsists a matrix $\boldsymbol{\Gamma}_k \in \mathbb{R}^{p_k\times 6}$ that satisfies the invertibility of $\boldsymbol{\Gamma}_k\boldsymbol{\mathcal{R}}_k^*\boldsymbol{\Gamma}_k^T$.*

Proof. The matrix $\boldsymbol{\mathcal{R}}_k^* \in \mathbb{R}^{6\times 6}$ is a real symmetric matrix. Thus it can be factored as $\boldsymbol{\mathcal{R}}_k^* = \boldsymbol{\Gamma}_k^*\boldsymbol{\Lambda}_k\boldsymbol{\Gamma}_k^{*T}$, where the columns of $\boldsymbol{\Gamma}_k^* = [\boldsymbol{\gamma}_{k1}\ \boldsymbol{\gamma}_{k2}...\boldsymbol{\gamma}_{kp_k}...\boldsymbol{\gamma}_{k6}]$ are an orthonormal set of 6 eigenvectors, the first p_k columns corresponding to the p_k nonzero eigenvalues $(\lambda_{ki})_{1\leq i\leq p_k}$, and $\boldsymbol{\Lambda}_k = diag(\lambda_{k1}, \lambda_{k2}, ...\lambda_{kp_k}, 0, ...0)$. Let $\boldsymbol{\Gamma}_k^T = [\boldsymbol{\gamma}_{k1}\ \boldsymbol{\gamma}_{k2}...\boldsymbol{\gamma}_{kp_k}]$, then $\boldsymbol{\Gamma}_k\boldsymbol{\mathcal{R}}_k^*\boldsymbol{\Gamma}_k^T = diag(\lambda_{k1}, \lambda_{k2}, ...\lambda_{kp_k})$, which is invertable. ■

Theorem 2.2.8. *Assume* $\mathbf{R}_{k-1}$ *is unbiased, the estimator (2.2.2) is unbiased, and the gain matrix* $\mathbf{K}_k$ *is*

$$\mathbf{K}_k = -\boldsymbol{\mathcal{S}}_k^* \boldsymbol{\Gamma}_k^T (\boldsymbol{\Gamma}_k \boldsymbol{\mathcal{R}}_k^* \boldsymbol{\Gamma}_k^T)^{-1} \boldsymbol{\Gamma}_k, \tag{2.2.22}$$

then the first-order approximation-based estimator (2.2.4) is unbiased minimum variance, and the estimation error covariance matrix is written as follows:

$$\mathbf{P}_k^{\xi} = \mathbf{K}_k \boldsymbol{\mathcal{S}}_k^{*T} + \mathbf{M}_k \boldsymbol{\mathcal{R}}_k \mathbf{M}_k^T. \tag{2.2.23}$$

Proof. Applying Lemma 2.2.6 proves the unbiasedness, then we rewrite the state estimation error covariance matrix (2.2.19) after substituting (2.2.21):

$$\mathbf{P}_k^{\xi} = \mathbf{K}_k^* \boldsymbol{\Gamma}_k \boldsymbol{\mathcal{R}}^* \boldsymbol{\Gamma}_k^T \mathbf{K}_k^{*T} + \boldsymbol{\mathcal{S}}_k^* \boldsymbol{\Gamma}_k^T \mathbf{K}_k^{*T} + \mathbf{K}_k^* \boldsymbol{\Gamma}_k \boldsymbol{\mathcal{S}}_k^{*T} + \mathbf{M}_k \boldsymbol{\mathcal{R}}_k \mathbf{M}_k^T, \tag{2.2.24}$$

using matrix derivatives:

$$\frac{dtr(\mathbf{P}_k^{\xi})}{d\mathbf{K}_k^*} = 2\mathbf{K}_k^* \boldsymbol{\Gamma}_k \boldsymbol{\mathcal{R}}_k^* \boldsymbol{\Gamma}_k^T + 2\boldsymbol{\mathcal{S}}_k^* \boldsymbol{\Gamma}_k^T, \tag{2.2.25}$$

the value $\mathbf{K}_k^* = -\boldsymbol{\mathcal{S}}_k^* \boldsymbol{\Gamma}_k^T (\boldsymbol{\Gamma}_k \boldsymbol{\mathcal{R}}_k^* \boldsymbol{\Gamma}_k^T)^{-1}$ satisfies

$$\frac{dtr(\mathbf{P}_k^{\xi})}{d\mathbf{K}_k^*} = 2\mathbf{K}_k^* \boldsymbol{\Gamma}_k \boldsymbol{\mathcal{R}}_k^* \boldsymbol{\Gamma}_k^T + 2\boldsymbol{\mathcal{S}}_k^* \boldsymbol{\Gamma}_k^T = \mathbf{0}.$$

Thus the gain $\mathbf{K}_k = \mathbf{K}_k^* \boldsymbol{\Gamma}_k = -\boldsymbol{\mathcal{S}}_k^* \boldsymbol{\Gamma}_k^T (\boldsymbol{\Gamma}_k \boldsymbol{\mathcal{R}}_k^* \boldsymbol{\Gamma}_k^T)^{-1} \boldsymbol{\Gamma}_k$ minimizes $\mathbf{E}(\|\boldsymbol{\xi}_k\|^2)$. Additionally, by substituting the value of the optimal $\mathbf{K}_k$ in (2.2.24) we can simplify the covariance equation as $\mathbf{P}_k^{\xi} = \mathbf{K}_k \boldsymbol{\mathcal{S}}_k^{*T} + \mathbf{M}_k \boldsymbol{\mathcal{R}}_k \mathbf{M}_k^T$. ■

UMV-SO(3) Algorithm Summary:

The inputs of the UMV-SO(3) algorithm are the previously estimated attitude and its associated covariance matrix, together with the acceleration and magnetic field measurements. The algorithm provides, as outputs, the estimated attitude along with the corresponding estimation error covariance matrix. The detailed steps of the proposed recursive filter UMV-SO(3) are summarized in Algorithm 3.

Algorithm 3 UMV-SO(3)

Input: $\hat{\mathbf{R}}_{k-1}$, $\mathbf{P}^{\xi}_{k-1}$, $\mathbf{y}_k = \begin{pmatrix} \mathbf{a}^m_k \\ \mathbf{b}^m_k \end{pmatrix}$

$\hat{\mathbf{R}}_{k|k-1} = \hat{\mathbf{R}}_{k-1}$

$\mathbf{H}_k = \begin{pmatrix} (\hat{\mathbf{R}}^T_{k|k-1}\mathbf{g})_\times \\ (\hat{\mathbf{R}}^T_{k|k-1}\mathbf{m}_e)_\times \end{pmatrix}$,

$\tilde{\boldsymbol{\mathcal{R}}}_k = \mathbf{H}_k \mathbf{P}^{\xi}_{k-1} \mathbf{H}^T_k + \boldsymbol{\mathcal{R}}_k$

$\mathbf{M}_k = \left(\mathbf{H}^T_k \tilde{\boldsymbol{\mathcal{R}}}^{-1}_k \mathbf{H}_k\right)^{-1} \mathbf{H}^T_k \tilde{\boldsymbol{\mathcal{R}}}^{-1}_k$

$\hat{\boldsymbol{\omega}}_{k-1} = \frac{1}{\Delta t}\mathbf{M}_k(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}))$

$\hat{\mathbf{R}}^*_k = \hat{\mathbf{R}}_{k|k-1} \exp_m(\hat{\boldsymbol{\omega}}_{k-1}\Delta t)$

$\mathbf{H}^*_k = \begin{pmatrix} (\hat{\mathbf{R}}^{*T}_k \mathbf{g})_\times \\ (\hat{\mathbf{R}}^{*T}_k \mathbf{m}_e)_\times \end{pmatrix}$,

$\boldsymbol{\mathcal{R}}^*_k = (\mathbf{I}_6 - \mathbf{H}^*_k\mathbf{M}_k)\boldsymbol{\mathcal{R}}_k(\mathbf{I}_6 - \mathbf{H}^*_k\mathbf{M}_k)^T$
$\boldsymbol{\mathcal{S}}^*_k = \mathbf{M}_k\boldsymbol{\mathcal{R}}_k(\mathbf{I}_6 - \mathbf{H}^*_k\mathbf{M}_k)^T$

$\boldsymbol{\Gamma}_k = [\boldsymbol{\gamma}_{k1}\, \boldsymbol{\gamma}_{k2} \ldots \boldsymbol{\gamma}_{kp_k}]^T$ ▷ where $(\boldsymbol{\gamma}_{ki})_{i\in\{1,\ldots,p_k\}}$ are the p_k lineary independent eigenvectors corresponding to the p_k non-zero eignvalues of the matrix $\boldsymbol{\mathcal{R}}^*_k$.

$\mathbf{K}_k = -\boldsymbol{\mathcal{S}}^*_k \boldsymbol{\Gamma}^T_k (\boldsymbol{\Gamma}_k \boldsymbol{\mathcal{R}}^*_k \boldsymbol{\Gamma}^T_k)^{-1} \boldsymbol{\Gamma}_k$

$\hat{\mathbf{R}}_k = \hat{\mathbf{R}}^*_k \exp_m\left(\mathbf{K}_k\left(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}^*_k)\right)\right)$

$\mathbf{P}^{\xi}_k = \mathbf{K}_k \boldsymbol{\mathcal{S}}^{*T}_k + \mathbf{M}_k \boldsymbol{\mathcal{R}}_k \mathbf{M}^T_k$

return $\hat{\mathbf{R}}_k$, $\mathbf{P}^{\xi}_k$

2.3. RTSKF-SO(3) Algorithm:

As mentioned in the introduction of this chapter, the derivation of the RTSKF-SO(3) algorithm is presented concisely in this section to avoid repetition of the detailed equations already provided in Section 2.2. The RTSKF algorithm [82] was originally developed for linear systems with unknown inputs that do not have direct feedthrough to the output.

In the context of this work, RTSKF-SO(3) is applied to the linearized error model of attitude, specifically utilizing the prediction equation (2.2.5) and the innovation equation (2.2.8). The detailed derivation steps are omitted here to avoid unnecessary repetition. For additional details, the reader is referred to [149].

The inputs of the RTSKF-SO(3) algorithm are the previously estimated attitude and its associated covariance matrix, together with the acceleration and magnetic field measurements. The algorithm provides, as outputs, the estimated attitude along with the corresponding estimation error covariance matrix. The steps of the proposed recursive filter RTSKF-SO(3) are summarized in Algorithm 4.

Algorithm 4 RTSKF-SO(3)

Input: $\hat{\mathbf{R}}_{k-1}$, $\mathbf{P}^{\xi}_{k-1}$, $\mathbf{y}_k = \begin{pmatrix} \mathbf{a}^m_k \\ \mathbf{b}^m_k \end{pmatrix}$

$\hat{\mathbf{R}}_{k|k-1} = \hat{\mathbf{R}}_{k-1}$

$\mathbf{H}_k = \begin{pmatrix} (\hat{\mathbf{R}}^T_{k|k-1}\mathbf{g})_\times \\ (\hat{\mathbf{R}}^T_{k|k-1}\mathbf{m}_e)_\times \end{pmatrix}$,

$\tilde{\boldsymbol{\mathcal{R}}}_k = \mathbf{H}_k \mathbf{P}^{\xi}_{k-1} \mathbf{H}^T_k + \boldsymbol{\mathcal{R}}_k$

$\mathbf{K}_k = \mathbf{P}^{\xi}_{k-1} \mathbf{H}^T_k \tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$

$\mathbf{R}^*_k = \hat{\mathbf{R}}_{k|k-1} \exp_m \left(\mathbf{K}_k \left(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) \right) \right)$

$\mathbf{P}^{\xi*}_k = (\mathbf{I} - \mathbf{K}_k \mathbf{H}_k) \mathbf{P}^{\xi}_{k-1}$

$\mathbf{M}_k = (\mathbf{H}^T_k \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \mathbf{H}_k)^{-1} \mathbf{H}_k{}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$

$\hat{\boldsymbol{\omega}}_k = \frac{1}{\Delta t} \mathbf{M}_k \left(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) \right)$

$\hat{\mathbf{R}}_k = \mathbf{R}^*_k \exp_m \left((\mathbf{I}_3 - \mathbf{K}_k \mathbf{H}_k) \hat{\boldsymbol{\omega}}_k \Delta t \right)$

$\mathbf{P}^{\xi}_k = \mathbf{P}^{\xi*}_k + (\mathbf{I}_3 - \mathbf{K}_k \mathbf{H}_k)(\mathbf{H}^T_k \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \mathbf{H}_k)^{-1} (\mathbf{I}_3 - \mathbf{K}_k \mathbf{H}_k)^T$

return $\hat{\mathbf{R}}_k$, $\mathbf{P}^{\xi}_k$

The main difference between RTSKF-SO(3) and UMV-SO(3) lies in the order of the unknown input estimation and the correction step. In UMV-SO(3), the unknown input is estimated first, and then incorporated into the state prediction before applying the correction step. In contrast, RTSKF-SO(3) performs the correction step before estimating and incorporating the unknown input, which results in a loss of local optimality.

Although UMV-SO(3) achieves better estimation accuracy, both algorithms are included to illustrate the extension of different linear-system-based methods to systems on SO(3). The two filters originate from distinct unknown input filtering approaches in the linear case, and their adaptation to the SO(3) framework offers a broader perspective on how various filtering strategies can be generalized to Lie groups.

2.4. Evaluation of UMV-SO(3) and RTSKF-SO(3)

This section aims to validate the effectiveness and demonstrate the performance of the two proposed algorithms: UMV-SO(3) and RTSKF-SO(3). Results are presented from both Monte Carlo simulations with 100 runs and real datasets to ensure a reliable evaluation of the proposed algorithms. The comparison is conducted between UMV-SO(3), RTSKF-SO(3), and the TRIAD algorithm introduced in Section 1.6. The reason for choosing the

static TRIAD algorithm for comparison is that there are no existing dynamic algorithms that rely solely on magnetometer and accelerometer measurements without using angular velocity data.

When showing the results, and in order to facilitate the interpretation of the results, the rotation matrices are converted into Euler angles using the XYZ convention and expressed in degrees.

Evaluation with Simulation

This subsection starts by explaining the simulation setup, and then the simulation results and discussions are presented in two parts. The first part includes figures that demonstrate the accuracy of attitude estimation and the convergence of the UMV-SO(3) algorithm, while the second part provides comparisons with RTSKF-SO(3) and TRIAD. Root Mean Square Error (RMSE) is calculated for each Monte Carlo run, and finally, the average is derived from the 100 runs.

Simulations setup

For every Monte Carlo run, the simulated data are generated for a duration of 100 s with a sampling time of $\Delta t = 0.01$ s. The Earth's gravity vector and the Earth's magnetic field are approximated by these two vectors written in NED (North-East-Down) frame in Grenoble, France: $\mathbf{g} = \begin{pmatrix} 0 & 0 & 9.81 \end{pmatrix}^T$ m/s^2 and $\mathbf{m}_e = \begin{pmatrix} 0.23 & 0.01 & 0.41 \end{pmatrix}^T$ G, respectively. The angular velocity ground truth is set as shown in Table 2.1. The standard deviations

Table 2.1: The true angular velocity used in simulation

	$0 \leq k\Delta t < 50$	$50 \leq k\Delta t \leq 100$
$\boldsymbol{\omega}_k(1)$	$0.8\cos(1.2k\Delta t)$	$-\cos(1.2k\Delta t)$
$\boldsymbol{\omega}_k(2)$	$-1.1\cos(0.5k\Delta t)$	$0.5\cos(0.8k\Delta t)$
$\boldsymbol{\omega}_k(3)$	$-0.4\cos(0.3k\Delta t)$	$-0.7\cos(0.7k\Delta t)$

for the accelerometer and magnetometer noises are assumed to be constants and set to be $\sigma_a = 0.01$ m/s^2 and $\sigma_m = 0.005$ G, respectively. The initial true rotation matrix is set to correspond to $(45°,\ 45°,\ 45°)$ in terms of Euler angles (Roll, Pitch, Yaw) using XYZ convention, and the initial estimation error covariance matrix is set to be identity.

For each Monte Carlo run, the initial estimate is generated randomly by setting it to correspond to Euler angles, where the three components are uniform random variables taking values between -180 and 180 degrees for roll and yaw, and between -90 and 90 degrees for pitch. These bounds for the uniform random variables cover the range of all possible rotations [58]. Additionally, the measurement noise realizations are generated independently for each run, meaning that each simulation has its own unique set of noise values, distinct from those of other runs, with common noise variances.

UMV-SO(3) theoretical estimation results

Fig. 2.1 plots the estimation error accuracy obtained with UMV-SO(3) for a single Monte Carlo run, where the initial estimate is set to the identity, corresponding to Euler angles with zero components. The left part of the figure represents the estimation error within the time range of $[0, 0.2]$ s, while the right part corresponds to the time range of $[0.2, 100]$ s. In the left part, UMV-SO(3) achieves convergence quickly, specifically in less than 0.05 s. In the right part, we observe that most of the time the roll error stays between $-0.3°$ and $0.3°$, the pitch error remains between $-0.12°$ and $0.12°$, and the yaw error is between $-2°$ and $2°$. The yaw angle error is notably larger due to its sole reliance on magnetometer measurements. This is because gravity, which has a strictly vertical direction, has no role in determining the yaw angle.

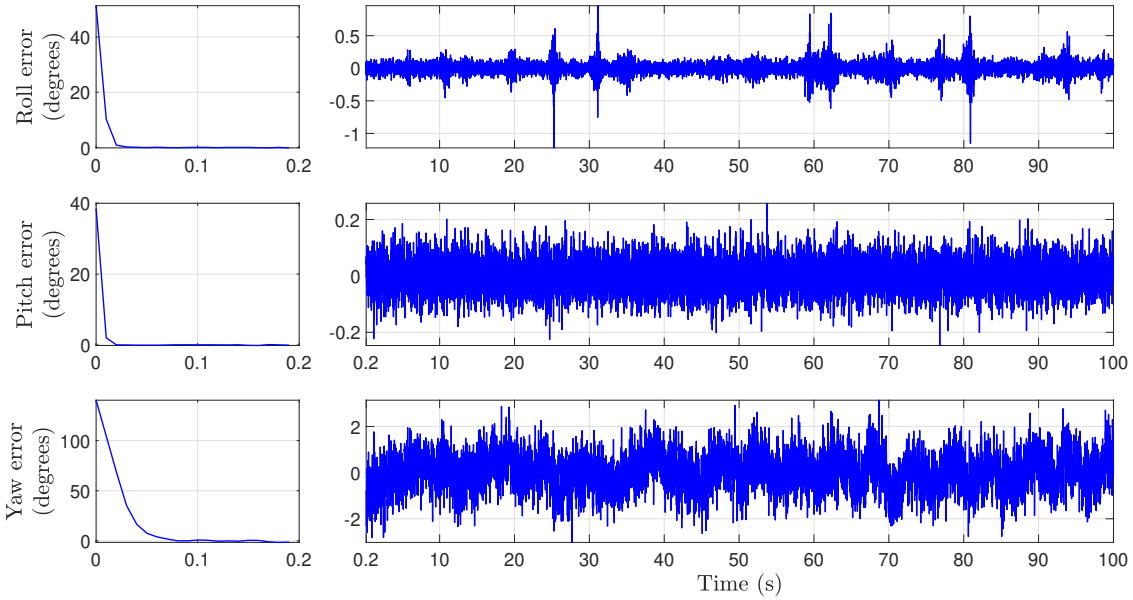

Figure 2.1: Attitude estimation error for UMV-SO(3)

Fig. 2.2 shows the convergence of the estimation error for 20 runs for UMV-SO(3), covering a wide range of initial estimates. These results demonstrate that convergence is achieved quickly across different initial estimates.

Comparison of UMV-SO(3) and RTSKF-SO(3) with TRIAD: Table 2.2 shows the RMSE for UMV-SO(3), RTSKF-SO(3), and TRIAD.

Table 2.2: RMSE (in degrees) for UMV-SO(3), RTSKF-SO(3), and TRIAD using Monte Carlo simulations

UMV-SO(3)	**RTSKF-SO(3)**	**TRIAD**
RMSE (degrees)	RMSE (degrees)	RMSE (degrees)
0.47	0.58	0.73

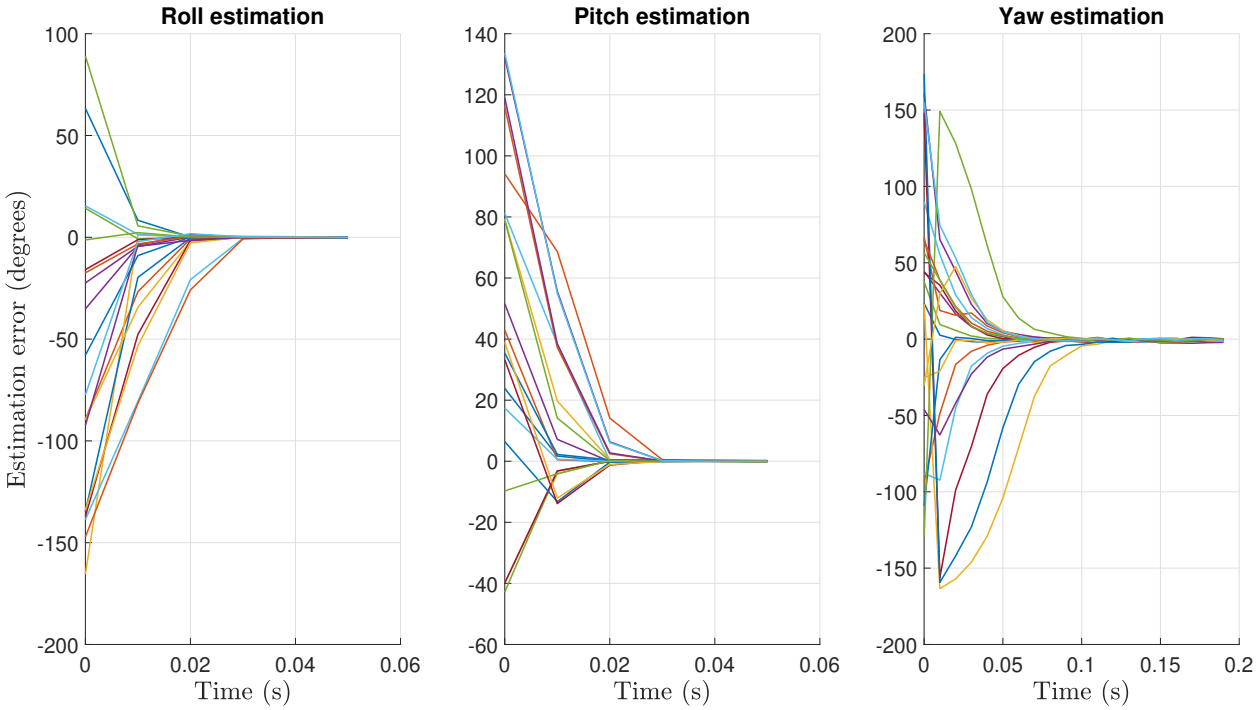

Figure 2.2: Attitude estimation error for UMV-SO(3), for 20 Monte Carlo runs.

UMV-SO(3) shows a 36% improvement in RMSE compared to the TRIAD algorithm, while RTSKF-SO(3) shows a 20% improvement in RMSE relative to TRIAD.

Evaluation with Real Data

To validate the effectiveness of both UMV-SO(3) and RTSKF-SO(3), we test them on real-world datasets obtained from previously conducted experiments. We use the dataset [25], which includes measurements from three commercial MIMU systems (Xsens-MTx, APDM-Opal, and Shimmer3) under different motion conditions (slow, medium, and fast rotation rates). Ground truth orientation is provided by a multi-camera stereo-photogrammetric (SP) system, ensuring high-accuracy reference data. This dataset is available on GitHub (accessible through [25]) and includes well-documented resources that facilitate its usage, along with experiment videos. In our comparison, we use the Xsens-MTx package with medium rotation rates. As shown in the experiment videos and confirmed by sensor measurement plots, the experiments consist of rest phases and moving phases. To ensure a fair comparison, we present results for a window where the system is in motion. Table 2.3 reports the RMSE for UMV-SO(3), RTSKF-SO(3), and TRIAD over the time window $[112, 130]$ s, corresponding to a moving phase. Additionally, Fig. 2.3 presents the ground truth and UMV-SO(3) attitude estimation for the same time window.

UMV-SO(3) shows a 20% improvement in RMSE compared to the TRIAD algorithm, while RTSKF-SO(3) shows a 18% improvement in RMSE compared to TRIAD. Both simulation and real data results confirm the improvement of UMV-SO(3) and RTSKF-SO(3) over the TRIAD algorithm.

Table 2.3: RMSE (in degrees) for UMV-SO(3), RTSKF-SO(3), and TRIAD using real dataset [25]

UMV-SO(3)	**RTSKF-SO(3)**	**TRIAD**
RMSE (degrees)	RMSE (degrees)	RMSE (degrees)
9.11	9.43	11.49

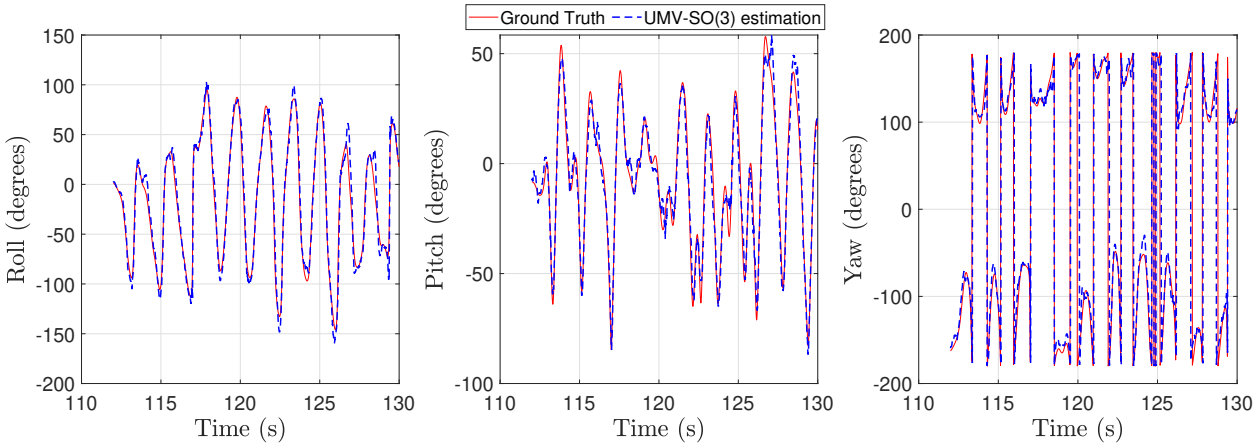

Figure 2.3: Experimental results: ground truth and UMV-SO(3) attitude estimation

Remark 2.4.1. *The improvement of UMV-SO(3) over TRIAD is* 36% *in simulation and* 20% *in real data. This difference in improvement can be attributed to assumption violations in real data. The UMV-SO(3) algorithm relies on certain assumptions, such as uncorrelated measurement noises, precise knowledge of covariance matrices, and minimal sensor biases. These assumptions are often met in simulations but may not hold in real-world scenarios, leading to suboptimal performance.*

Remark 2.4.2. *For each of the three algorithms individually, it can be observed that the estimation error with real data is much higher than in simulation. This is mainly due to the fact that all three algorithms rely on gravity and magnetic field measurements expressed in the body frame, while the accelerometer and magnetometer are affected by non-negligible external acceleration and magnetic field disturbances, respectively, in the real data. More details as follows: 1) By observing the acceleration measurements and reviewing the video of the experiment (available in the same repository), it is clear that the accelerometer is subject to significant external acceleration. The movement involves oscillatory translation: an accelerated motion in one direction followed by a short deceleration in the opposite direction. As a result, the external acceleration remains relatively high during several intervals and cannot be considered negligible compared to gravity. 2) Additionally, the experiment was conducted in a room containing several electronic devices, which caused magnetic field disturbances that affected the magnetometer readings.*

Remark 2.4.3. *UMV-SO(3) and RTSKF-SO(3) improve the estimation accuracy compared to the static algorithm TRIAD, although all three algorithms rely on the same sensor mea-*

surements. This improvement is attributed to the recursive estimation process employed by UMV-SO(3) and RTSKF-SO(3), which incorporates previous attitude estimates, their associated error covariance matrices, and the current accelerometer and magnetometer measurements along with their noise covariance matrices, while also exploiting the attitude dynamic model. In contrast, static algorithms such as TRIAD estimate the attitude at each time step based solely on the current measurements, without utilizing prior information or the system dynamics.

2.5. Conclusion

This chapter introduced two dynamic algorithms for attitude estimation on SO(3) using measurements from a three-axis accelerometer and a three-axis magnetometer, while treating the angular velocity as an unknown input affecting the attitude dynamic model. The two algorithms, UMV-SO(3) and RTSKF-SO(3), were evaluated through Monte Carlo simulations and real datasets, and their performance was compared with the static TRIAD algorithm. The results obtained from both simulations and real data demonstrated that UMV-SO(3) and RTSKF-SO(3) outperformed TRIAD. These findings confirm that the proposed algorithms provide an effective solution for attitude estimation in scenarios where gyroscope measurements are unreliable or unavailable.

In the formulation addressed in this chapter, the unknown input affects only the dynamic model, without direct feedthrough to the output, and the accelerometer measurements are assumed to contain only the gravity component, neglecting external acceleration. The next chapter addresses the problem of attitude estimation based on MARG sensor measurements in the presence of external acceleration, by considering it as an unknown input that directly affects the output function without affecting the dynamic model.

Chapter 3

Attitude Estimation Based on MARG Sensor Under Unknown External Acceleration

This chapter starts with the introductory Section 3.1, which explains the model of attitude dynamics on SO(3) and the output that considers the external acceleration, the challenges associated with external acceleration, and the existing solutions in the literature for attitude estimation using MARG sensors under external acceleration. Section 3.2 presents the derivation of the proposed UMV-SO(3)-EA algorithm. Section 3.3 evaluates the proposed algorithm through both simulation and experimental data. Finally, Section 3.4 concludes the chapter and prepares the reader for Chapter 4. [1]

3.1. Preliminaries and Problem Statement

This chapter addresses the problem of attitude estimation based on MARG sensors when the rigid body is subject to unknown external acceleration. The attitude dynamic model (1.5.6), along with the corresponding output consisting of the accelerometer measurements (1.5.2) and the magnetometer measurements (1.5.3), are briefly recalled below:

$$\mathbf{R}_{k+1} = \mathbf{R}_k \exp_m \left((\boldsymbol{\omega}_k^m - \mathbf{w}_k^\omega) \Delta t \right), \tag{3.1.1}$$

$$\mathbf{y}_k = \mathbf{h}(\mathbf{R}_k) + \mathbf{D}\mathbf{a}_k^{ext} + \mathbf{w}_k^y, \tag{3.1.2}$$

where $\mathbf{R}_k \in \mathrm{SO}(3)$ denotes the rotation matrix at time step k, $\boldsymbol{\omega}_k^m \in \mathbb{R}^3$ is the measured angular velocity, and $\mathbf{w}_k^\omega \in \mathbb{R}^3$ represents the gyroscope noise. The output measurement function $\mathbf{h}(.)$, the matrix $\mathbf{D} \in \mathbb{R}^{6\times 3}$, and the output noise $\mathbf{w}_k^y$ are given by:

[1] Before reading this chapter, it is recommended to first read Chapter 1.

$$\mathbf{h}(\mathbf{R}) = \begin{pmatrix} \mathbf{R}^T\mathbf{g} \\ \mathbf{R}^T\mathbf{m}_e \end{pmatrix}, \qquad \mathbf{D} = \begin{pmatrix} \mathbf{I}_3 \\ \mathbf{0}_3 \end{pmatrix}, \qquad \mathbf{w}_k^y = \begin{pmatrix} \mathbf{w}_k^a \\ \mathbf{w}_k^b \end{pmatrix}, \tag{3.1.3}$$

where $\mathbf{g}$ is the Earth's gravity vector, $\mathbf{m}_e$ is the Earth's magnetic field, $\mathbf{w}_k^a$ is the accelerometer measurement noise, $\mathbf{w}_k^b$ is the magnetometer measurement noise, and $\mathbf{a}_k^{ext} \in \mathbb{R}^3$ denotes the unknown external acceleration of the rigid body. The process noise $\mathbf{w}_k^\omega$ and the output measurement noise $\mathbf{w}_k^y$ are assumed to be uncorrelated and to have positive definite covariance matrices $\boldsymbol{\mathcal{Q}}_k$ and $\boldsymbol{\mathcal{R}}_k$, respectively.

The common solution for attitude estimation based on MARG sensors is to assume that the external acceleration $\mathbf{a}_k^{ext}$ is negligible compared to gravity [116, 122]. Under this assumption, the accelerometer is considered to measure only the projection of the gravity vector in the body frame. In this case, the accelerometer and magnetometer provide measurements of the gravity and magnetic field vectors expressed in the body frame, while their values in the navigation frame are known. This leads to a well-known Wahba problem [58]. Examples of works in the literature that adopt this assumption include the complementary filter in [116] and the invariant extended Kalman filter (IEKF) in [5], which is introduced in Section 1.7. However, this assumption becomes invalid in scenarios involving periods of accelerated motions, when the external acceleration is non-negligible compared to gravitational acceleration.

This problem has received the attention of numerous studies in the literature. The most popular approach is the threshold-based adaptive method, which involves computing the difference between the measured acceleration norm and the gravitational acceleration one. If the difference exceeds a predefined threshold, the algorithm considers the measured acceleration as unreliable [144, 146, 162]. This approach encounters a drawback during long-duration accelerated motion, as the algorithm completely ignores the measured acceleration, relying solely on magnetometer measurements in the correction step, making the attitude unobservable [146]. A second approach is based on an external acceleration model as illustrated in [103]. However, it is important to emphasize that these algorithms employ approximated models which are inaccurate in most scenarios. A third approach involves estimating the external acceleration through the double derivation of GPS measurements, as presented in [90]. A fourth approach, termed velocity-aided attitude observers, estimates the external acceleration through the derivation of velocity measurements from sources like air-data systems or Doppler radar as discussed in [88]. The last two approaches rely on extra measurements, which require additional sensors. A last approach assumes that the external acceleration displays high frequency [15]. However, this assumption is violated when dealing with situations involving constant or low-frequency external acceleration, leading to performance loss. From this literature review, one can conclude that no existing solution satisfies the following three conditions simultaneously: (1) the ability to handle long-duration accelerated motion, (2) no reliance on additional sensors, and (3) no prior information or assumptions on the external acceleration.

This chapter addresses this problem by considering the external acceleration as an unknown input that directly affects the output (measurement) function, where the unknown external

acceleration appears in the output model (3.1.2). Based on the unknown input filtering algorithm designed in [66] for a linear system with unknown input with direct feedthrough to the output, this chapter designs the algorithm UMV-SO(3)-EA for local Unbiased Minimum Variance attitude estimation on SO(3) under unknown External Acceleration.

The system (3.1.1)-(3.1.2) is left invertible (see [164, Def. 2.5]), meaning that the unknown input $\mathbf{a}_k^{ext}$ can be uniquely reconstructed given the outputs $(\mathbf{y}_i)_{i\in 0,1,\dots k}$, and the initial state $\mathbf{R}_0$. Moreover, the system is observable (see [164, Def. 2.4]), because the state $\mathbf{R}_k$ can be uniquely reconstructed given the inputs $(\mathbf{a}_i^{ext})_{i\in 0,1,\dots k}$ and the outputs $(\mathbf{y}_i)_{i\in 0,1,\dots k}$. Therefore, knowing the output sequence $(\mathbf{y}_i)_{i\in 0,1,\dots k}$ and the initial state $\mathbf{R}_0$ allows to uniquely reconstruct the unknown inputs $(\mathbf{a}_i^{ext})_{i\in 0,1,\dots k}$, and consequently the state $\mathbf{R}_k$.

Building on the previous discussion, this chapter designs a solution that assumes the availability of an unbiased initial estimate of attitude. The algorithm UMV-SO(3)-EA provides an unbiased minimum variance first-order approximation-based estimate of $\mathbf{R}_k$, using the unbiased estimate of $\mathbf{R}_{k-1}$, the known input $\boldsymbol{\omega}_{k-1}$, and the measurement $\mathbf{y}_k$. It is important to note that an unbiased and slightly perturbed initial estimate of the attitude can be obtained using static algorithms, such as the TRIAD method described in Section 1.6, which relies on the initial magnetometer and accelerometer measurements, where the external acceleration is known and equal to zero before the body starts moving.

The main contributions of this chapter are:

- Development of an algorithm for state estimation on SO(3) with an unknown input having direct feedthrough to the output without affecting the dynamic model.
- Design of a novel attitude estimation algorithm based on MARG sensor measurements under external acceleration, by treating the external acceleration as an unknown input.

The material presented in this chapter is based on the corresponding publication:

- *G. Shaaban, H. Fourati, A. Kibangou, and C. Prieur, "MARG sensor-based attitude estimation on SO(3) under unknown external acceleration," IEEE Control Systems Letters (L-CSS), vol. 7, pp. 3795–3800, 2023.*

3.2. UMV-SO(3)-EA Algorithm Derivation

For linear discrete-time systems with unknown input having direct linear feedthrough to the output, the three-step Kalman filter was introduced in [66] for unbiased minimum variance state and unknown input estimation. The three steps are as follows: (i) predict the state using the state dynamic model, (ii) estimate the unknown input using the predicted state and the measurements, (iii) correct the predicted state using the estimated unknown input and the measurements. Based on the same principle, we propose the filter UMV-SO(3)-EA

based on the following equations:

$$\hat{\mathbf{R}}_{k|k-1} = \hat{\mathbf{R}}_{k-1}\exp_{\mathrm{m}}(\boldsymbol{\omega}_{k-1}^{m}\Delta t), \tag{3.2.1}$$

$$\hat{\mathbf{a}}_{k}^{ext} = \mathbf{M}_k\left(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1})\right), \tag{3.2.2}$$

$$\hat{\mathbf{R}}_{k} = \hat{\mathbf{R}}_{k|k-1}\exp_{\mathrm{m}}\left(\mathbf{K}_k\left(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) - \mathbf{D}\hat{\mathbf{a}}_{k}^{ext}\right)\right), \tag{3.2.3}$$

where the matrices $\mathbf{M}_k \in \mathbb{R}^{3\times 6}$ and $\mathbf{K}_k \in \mathbb{R}^{3\times 6}$ are the gain matrices which have to be designed.

Main goal: *Considering $\hat{\mathbf{R}}_{k-1}$ as unbiased, the objective is to design $\mathbf{M}_k$ and $\mathbf{K}_k$ so that the first-order approximation-based estimators of $\mathbf{a}_k^{ext}$ and $\mathbf{R}_k$ given by (3.2.2)-(3.2.3) are unbiased minimum variance (see Theorem 3.2.3 and Theorem 3.2.5).*

We define the attitude estimation error $\exp_{\mathrm{m}}(\boldsymbol{\xi}_k) = \hat{\mathbf{R}}_k^{-1}\mathbf{R}_k$, and the attitude prediction error $\exp_{\mathrm{m}}(\boldsymbol{\xi}_{k|k-1}) = \hat{\mathbf{R}}_{k|k-1}^{-1}\mathbf{R}_k$, with the corresponding covariance matrices $\mathbf{P}_k^{\xi} = \mathbf{E}(\boldsymbol{\xi}_k\boldsymbol{\xi}_k^T)$, and $\mathbf{P}_{k|k-1}^{\xi} = \mathbf{E}(\boldsymbol{\xi}_{k|k-1}\boldsymbol{\xi}_{k|k-1}^T)$ respectively. In the following, the steps of the algorithm are derived, beginning with the prediction (3.2.1), followed by the estimation of the external acceleration (3.2.2), and then the correction (3.2.3). Finally, a summary of the complete algorithm is provided.

Prediction:

The prediction error and the corresponding covariance matrix associated with (3.2.1) are derived in Lemma 3.2.1, which follows, and are used in subsequent developments.

Lemma 3.2.1. *Let $\hat{\mathbf{R}}_{k-1}$ be an unbiased estimate. Then, the first-order approximation-based estimator (3.2.1) is also unbiased, and the prediction error is given by:*

$$\boldsymbol{\xi}_{k|k-1} = \boldsymbol{\xi}_{k-1} - \mathbf{w}_{k-1}^{\omega}\Delta t. \tag{3.2.4}$$

The corresponding prediction error covariance matrix is given by:

$$\mathbf{P}_{k|k-1}^{\xi} = \mathbf{E}(\boldsymbol{\xi}_{k|k-1}\boldsymbol{\xi}_{k|k-1}^T) = \mathbf{P}_{k-1}^{\xi} + \Delta t^2\boldsymbol{\mathcal{Q}}_{k-1}. \tag{3.2.5}$$

Proof. Starting with the equation of prediction error $\exp_{\mathrm{m}}(\boldsymbol{\xi}_{k|k-1}) = \hat{\mathbf{R}}_{k|k-1}^{-1}\mathbf{R}_k$, then employing the rotation dynamic (3.1.1) and the filter's first step (3.2.1) give:

$$\begin{aligned}\exp_{\mathrm{m}}(\boldsymbol{\xi}_{k|k-1}) =& \exp_{\mathrm{m}}(-\boldsymbol{\omega}_{k-1}^{m}\Delta t)\hat{\mathbf{R}}_{k-1}^{-1}\mathbf{R}_{k-1}\exp_{\mathrm{m}}\left((\boldsymbol{\omega}_{k-1}^{m} - \mathbf{w}_{k-1}^{\omega})\Delta t\right)\\ =& \exp_{\mathrm{m}}(-\boldsymbol{\omega}_{k-1}^{m}\Delta t)\exp_{\mathrm{m}}(\boldsymbol{\xi}_{k-1})\exp_{\mathrm{m}}\left((\boldsymbol{\omega}_{k-1}^{m} - \mathbf{w}_{k-1}^{\omega})\Delta t\right)\end{aligned}$$

Applying first-order approximation (1.4.5) gives:

$$\boldsymbol{\xi}_{k|k-1} = \boldsymbol{\xi}_{k-1} - \mathbf{w}_{k-1}^{\omega}\Delta t,$$

and yields $\mathbf{E}(\boldsymbol{\xi}_{k|k-1}) = \mathbf{E}(\boldsymbol{\xi}_{k-1}) - \Delta t\mathbf{E}(\mathbf{w}_{k-1}^{\omega}) = \mathbf{0}$ since $\mathbf{E}(\boldsymbol{\xi}_{k-1}) = \mathbf{0}$ and $\mathbf{E}(\mathbf{w}_{k-1}^{\omega}) = \mathbf{0}$. Computing the covariance matrix $\mathbf{E}(\boldsymbol{\xi}_{k|k-1}\boldsymbol{\xi}_{k|k-1}^T)$ confirms (3.2.5). ■

External Acceleration Estimation:

We define $\mathbf{H}_k$ which is the Jacobian of the output function $\mathbf{h}(.)$ with respect to the prediction error $\mathbf{H}_k = \frac{\partial \mathbf{h}\left(\hat{\mathbf{R}}_{k|k-1}\exp_m(\boldsymbol{\xi})\right)}{\partial \boldsymbol{\xi}}|_{\boldsymbol{\xi}=\mathbf{0}}$, it has the following value (see Lemma 1.7.1):

$$\mathbf{H}_k = \begin{pmatrix} (\hat{\mathbf{R}}_{k|k-1}^T \mathbf{g})_\times \\ (\hat{\mathbf{R}}_{k|k-1}^T \mathbf{m}_e)_\times \end{pmatrix},$$

and we define variable $\tilde{\mathbf{e}}_k$:

$$\tilde{\mathbf{e}}_k = \mathbf{H}_k \boldsymbol{\xi}_{k|k-1} + \mathbf{w}_k^y, \tag{3.2.6}$$

The expected value of $\tilde{\mathbf{e}}_k$ is $\mathbf{E}(\tilde{\mathbf{e}}_k) = \mathbf{0}$ since $\mathbf{E}(\boldsymbol{\xi}_{k|k-1}) = \mathbf{0}$ (unbiased $\mathbf{R}_{k-1}$ implies unbiased $\mathbf{R}_{k|k-1}$, see Lemma 3.2.1), and $\mathbf{E}(\mathbf{w}_k^y) = \mathbf{0}$ (zero mean measurement noise). The covariance matrix of $\tilde{\mathbf{e}}_k$ is given by:

$$\tilde{\boldsymbol{\mathcal{R}}}_k = \mathbf{E}(\tilde{\mathbf{e}}_k \tilde{\mathbf{e}}_k^T) = \mathbf{H}_k \mathbf{P}_{k|k-1}^{\xi} \mathbf{H}_k^T + \boldsymbol{\mathcal{R}}_k, \tag{3.2.7}$$

The sufficient conditions for the local optimality of the external acceleration estimator (3.2.2) are established in Theorem 3.2.3, with the support of Lemma 3.2.2, both of which are presented below.

Lemma 3.2.2. *Let $\hat{\mathbf{R}}_{k-1}$ be unbiased, then the difference $\tilde{\mathbf{y}}_k = \mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1})$ found in the filter's second step (3.2.2) can be approximated by*

$$\tilde{\mathbf{y}}_k = \mathbf{D}\mathbf{a}_k^{ext} + \tilde{\mathbf{e}}_k. \tag{3.2.8}$$

Proof. Substituting $\mathbf{y}_k$ (3.1.2) gives:

$$\tilde{\mathbf{y}}_k = \mathbf{h}(\mathbf{R}_k) - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) + \mathbf{D}\mathbf{a}_k^{ext} + \mathbf{w}_k^y,$$

applying the first order approximation $\mathbf{h}(\hat{\mathbf{R}}_{k|k-1}\exp_m(\boldsymbol{\xi}_{k|k-1})) - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) = \mathbf{H}_k\boldsymbol{\xi}_{k|k-1} + \mathcal{O}(\boldsymbol{\xi}_{k|k-1}^2)$ gives:

$$\begin{aligned} \tilde{\mathbf{y}}_k =& \mathbf{D}\mathbf{a}_k^{ext} + \mathbf{H}_k\boldsymbol{\xi}_{k|k-1} + \mathbf{w}_k^y, \\ \tilde{\mathbf{y}}_k =& \mathbf{D}\mathbf{a}_k^{ext} + \tilde{\mathbf{e}}_k. \end{aligned} \tag{3.2.9}$$

■

Theorem 3.2.3. *Let $\hat{\mathbf{R}}_{k-1}$ be unbiased and the gain matrix $\mathbf{M}_k$ be equal to*

$$\mathbf{M}_k = (\mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \mathbf{D})^{-1} \mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1}, \tag{3.2.10}$$

then the first-order approximation-based estimator of $\mathbf{a}_k^{ext}$ provided by (3.2.2) is unbiased minimum variance.

Proof. Applying Lemma 3.2.2 enables us to use the approximated model (3.2.9) which satisfies Gauss Markov conditions [93, Chapter 3.4.2], where the matrix $\mathbf{D}$ has full column rank and $\tilde{\boldsymbol{\mathcal{R}}}_k$ is positive definite, then the estimator (3.2.2) is unbiased and has minimum variance when the matrix gain $\mathbf{M}_k$ is equal to:

$$\mathbf{M}_k = (\mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \mathbf{D})^{-1} \mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1}.$$

This gain matrix satisfies $\mathbf{M}_k \mathbf{D} = \mathbf{I}_3$, we utilize this property after substituting (3.2.9) in (3.2.2):

$$\begin{aligned} \hat{\mathbf{a}}_k^{ext} =& \mathbf{M}_k \left(\mathbf{D}\mathbf{a}_k^{ext} + \tilde{\mathbf{e}}_k \right), \\ =& \mathbf{a}_k^{ext} + \mathbf{M}_k \tilde{\mathbf{e}}_k, \end{aligned}$$

and finally:

$$\mathbf{a}_k^{ext} - \hat{\mathbf{a}}_k^{ext} = -\mathbf{M}_k \tilde{\mathbf{e}}_k. \tag{3.2.11}$$

The corresponding covariance matrix is

$$\begin{aligned} \mathbf{P}_k^a =& \mathbf{E}(\mathbf{M}_k \tilde{\mathbf{e}}_k \tilde{\mathbf{e}}_k^T \mathbf{M}_k^T), \\ =& \mathbf{M}_k \tilde{\boldsymbol{\mathcal{R}}}_k \mathbf{M}_k^T, \\ =& (\mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \mathbf{D})^{-1} \mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \tilde{\boldsymbol{\mathcal{R}}}_k \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \mathbf{D} (\mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \mathbf{D})^{-1}, \\ =& (\mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \mathbf{D})^{-1}. \end{aligned}$$

■

Correction:

The sufficient conditions for the local optimality of the attitude estimator (3.2.3) are established in Theorem 3.2.5, with the support of Lemma 3.2.4, both of which are presented below.

Lemma 3.2.4. *Let $\hat{\mathbf{R}}_{k-1}$ be unbiased and the matrix gain $\mathbf{M}_k = (\mathbf{D}^T \tilde{\mathbf{R}}_k^{-1} \mathbf{D})^{-1} \mathbf{D}^T \tilde{\mathbf{R}}_k^{-1}$, then the first-order approximation-based estimator (3.2.3) is unbiased, and the estimation error equation is given by:*

$$\boldsymbol{\xi}_k = (\mathbf{I}_3 - \mathbf{K}_k (\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k)\boldsymbol{\xi}_{k|k-1} - \mathbf{K}_k (\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\mathbf{w}_k^y. \tag{3.2.12}$$

Proof. Lemma 3.2.2 and Theorem 3.2.3 hold, thus (3.2.9) and (3.2.11) are satisfied. We substitute (3.2.9) in (3.2.3) and then substitute (3.2.11):

$$\begin{aligned} \hat{\mathbf{R}}_k &= \hat{\mathbf{R}}_{k|k-1} \exp_{\mathrm{m}} \left(\mathbf{K}_k \left(\tilde{\mathbf{e}}_k + \mathbf{D} \left(\mathbf{a}_k^{ext} - \hat{\mathbf{a}}_k^{ext} \right) \right) \right), \\ &= \hat{\mathbf{R}}_{k|k-1} \exp_{\mathrm{m}} \left(\mathbf{K}_k \left(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k \right) \tilde{\mathbf{e}}_k \right). \end{aligned}$$

The estimation error:

$$\begin{aligned}\exp_{\mathrm{m}}(\boldsymbol{\xi}_k) =& \hat{\mathbf{R}}_k^{-1}\mathbf{R}_k,\\ =& \exp_{\mathrm{m}}(-\mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k)\hat{\mathbf{R}}_{k|k-1}^{-1}\mathbf{R}_k,\\ =& \exp_{\mathrm{m}}(-\mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k)\exp_{\mathrm{m}}(\boldsymbol{\xi}_{k|k-1}),\end{aligned}$$

applying the BCH approximation (1.4.5) gives

$$\boldsymbol{\xi}_k = -\mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k + \boldsymbol{\xi}_{k|k-1}.$$

Finally, substituting (3.2.6) gives:

$$\boldsymbol{\xi}_k = (\mathbf{I}_3 - \mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k)\boldsymbol{\xi}_{k|k-1} - \mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\mathbf{w}_k^y.$$

The expected value of $\boldsymbol{\xi}_k$ is $\mathbf{E}(\boldsymbol{\xi}_k) = \mathbf{0}$ since $\mathbf{E}(\boldsymbol{\xi}_{k|k-1}) = \mathbf{0}$ (See Lemma 3.2.1) and $\mathbf{E}(\mathbf{v}_k^y) = \mathbf{0}$ (zero mean measurement noise). ■

Theorem 3.2.5. *Let $\hat{\mathbf{R}}_{k-1}$ be unbiased. Given the gains $\mathbf{M}_k = (\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D})^{-1}\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$ and $\mathbf{K}_k = \mathbf{P}_{k|k-1}^{\xi}\mathbf{H}_k^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$, then the first-order approximation-based estimator (3.2.3) is unbiased minimum variance.*

Proof. Applying Lemma 3.2.4 proves that the estimator (3.2.3) is unbiased. Minimizing $\mathbf{E}(\|\boldsymbol{\xi}_k\|^2)$ is equivalent to minimizing the trace of the covariance matrix $\mathbf{P}_k^{\xi} = \mathbf{E}(\boldsymbol{\xi}_k\boldsymbol{\xi}_k^T)$. Then the aim is to prove that the proposed $\mathbf{K}_k$ satisfies $\frac{dtr(\mathbf{P}_k^{\xi})}{d\mathbf{K}_k} = \mathbf{0}$. We start by computing $\mathbf{P}_k^{\xi}$, where we replace $\boldsymbol{\xi}_k$ by (3.2.12):

$$\begin{aligned}\mathbf{P}_k^{\xi} =& \mathbf{E}(\boldsymbol{\xi}_k\boldsymbol{\xi}_k^T),\\ =& (\mathbf{I}_3 - \mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k)\,\mathbf{P}_{k|k-1}^{\xi}(\mathbf{I}_3 - \mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k)^T\\ &+ \mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\boldsymbol{\mathcal{R}}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)^T\mathbf{K}_k^T,\\ =& \mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)(\mathbf{H}_k\mathbf{P}_{k|k-1}^{\xi}\mathbf{H}_k^T + \boldsymbol{\mathcal{R}}_k)(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)^T\mathbf{K}_k^T\\ &- \mathbf{P}_{k|k-1}^{\xi}\mathbf{H}_k^T(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)^T\mathbf{K}_k^T - \mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k\mathbf{P}_{k|k-1}^{\xi} + \mathbf{P}_{k|k-1}^{\xi}.\end{aligned} \tag{3.2.13}$$

The term $\tilde{\boldsymbol{\mathcal{R}}}_k^* = (\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)(\mathbf{H}_k\mathbf{P}_{k|k-1}^{\xi}\mathbf{H}_k^T + \boldsymbol{\mathcal{R}}_k)(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)^T$ can be simplified, by substituting (3.2.7), which gives $\tilde{\boldsymbol{\mathcal{R}}}_k^* = (\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\tilde{\boldsymbol{\mathcal{R}}}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)^T$ and then substituting the value of $\mathbf{M}_k$, which gives $\tilde{\boldsymbol{\mathcal{R}}}_k^* = (\tilde{\boldsymbol{\mathcal{R}}}_k - \mathbf{D}(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D})^{-1}\mathbf{D}^T)(\mathbf{I}_6 - \mathbf{D}(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D})^{-1}\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1})^T$. The subterm $\mathbf{D}^T(\mathbf{I}_6 - \mathbf{D}(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D})^{-1}\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1})^T$ can be simplified as

$$(\mathbf{D} - \mathbf{D}(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D})^{-1}\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D})^T = (\mathbf{D} - \mathbf{D})^T = \mathbf{0},$$

thus $\tilde{\boldsymbol{\mathcal{R}}}_k^* = \tilde{\boldsymbol{\mathcal{R}}}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)^T$. Substituting this $\tilde{\boldsymbol{\mathcal{R}}}_k^*$ in (3.2.13) gives:

$$\begin{aligned}\mathbf{P}_k^{\xi} =& \mathbf{K}_k\tilde{\boldsymbol{\mathcal{R}}}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)^T\mathbf{K}_k^T\\ &- \mathbf{P}_{k|k-1}^{\xi}\mathbf{H}_k^T(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)^T\mathbf{K}_k^T\\ &- \mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k\mathbf{P}_{k|k-1}^{\xi}\\ &+ \mathbf{P}_{k|k-1}^{\xi},\end{aligned} \tag{3.2.14}$$

and utilizing the matrix derivatives from [12] (Propositions 10.7.2 and 10.7.4), leads to:

$$\begin{aligned}\frac{dtr(\mathbf{P}_k^{\xi})}{d\mathbf{K}_k} =& 2\mathbf{K}_k\tilde{\boldsymbol{\mathcal{R}}}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)^T \\ &- 2\mathbf{P}_{k|k-1}^{\xi}\mathbf{H}_k^T(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)^T,\end{aligned}$$

then direct substitution of $\mathbf{K}_k = \mathbf{P}_{k|k-1}^{\xi}\mathbf{H}_k^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$ concludes that $\frac{dtr(\mathbf{P}_k^{\xi})}{d\mathbf{K}_k} = \mathbf{0}$ and the estimator is minimum variance. Finally by applying the value of $\mathbf{K}_k$ in (3.2.14) gives $\mathbf{P}_k^{\xi} = \mathbf{P}_{k|k-1}^{\xi} - \mathbf{K}_k(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k\mathbf{P}_{k|k-1}^{\xi}$. ■

UMV-SO(3)-EA Algorithm Summary

The inputs of the UMV-SO(3)-EA algorithm are the previously estimated attitude and its associated covariance matrix, together with the MARG sensor measurements. The algorithm provides, as outputs, the estimated attitude along with the corresponding estimation error covariance matrix, as well as the estimated unknown external acceleration and its associated covariance matrix. The detailed steps of the proposed recursive filter UMV-SO(3)-EA are summarized in Algorithm 5.

Algorithm 5 UMV-SO(3)-EA

Input: $\hat{\mathbf{R}}_{k-1}$, $\mathbf{P}_{k-1}^{\xi}$, $\boldsymbol{\omega}_{k-1}^m$, $\mathbf{y}_k = \begin{pmatrix}\mathbf{a}_k^m \\ \mathbf{b}_k^m\end{pmatrix}$

▷ Prediction:

$\hat{\mathbf{R}}_{k|k-1} = \hat{\mathbf{R}}_{k-1}\exp_{\mathrm{m}}(\boldsymbol{\omega}_{k-1}^m\Delta t)$

$\mathbf{P}_{k|k-1}^{\xi} = \mathbf{P}_{k-1}^{\xi} + \Delta t^2\boldsymbol{\mathcal{Q}}_{k-1}$

▷ External acceleration estimation:

$\mathbf{H}_k = \begin{pmatrix}(\hat{\mathbf{R}}_{k|k-1}^T\mathbf{g})_\times \\ (\hat{\mathbf{R}}_{k|k-1}^T\mathbf{m}_e)_\times\end{pmatrix}$,

$\tilde{\boldsymbol{\mathcal{R}}}_k = \mathbf{H}_k\mathbf{P}_{k|k-1}^{\xi}\mathbf{H}_k^T + \boldsymbol{\mathcal{R}}_k$

$\mathbf{M}_k = \left(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D}\right)^{-1}\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$

$\hat{\mathbf{a}}_k^{ext} = \mathbf{M}_k\left(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1})\right)$

$\mathbf{P}_k^a = \left(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D}\right)^{-1}$

▷ Correction:

$\mathbf{K}_k = \mathbf{P}_{k|k-1}^{\xi}\mathbf{H}_k^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$

$\hat{\mathbf{R}}_k = \hat{\mathbf{R}}_{k|k-1}\exp_{\mathrm{m}}\left(\mathbf{K}_k\left(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) - \mathbf{D}\hat{\mathbf{a}}_k^{ext}\right)\right)$

$\mathbf{P}_k^{\xi} = \mathbf{P}_{k|k-1}^{\xi} - \mathbf{K}_k\left(\mathbf{I}_6 - \mathbf{D}\mathbf{M}_k\right)\mathbf{H}_k\mathbf{P}_{k|k-1}^{\xi}$

return $\hat{\mathbf{R}}_k$, $\mathbf{P}_k^{\xi}$, $\hat{\mathbf{a}}_k^{ext}$, $\mathbf{P}_k^a$

3.3. Evaluation of UMV-SO(3)-EA

This section aims to validate the algorithm's effectiveness in different scenarios. Results are presented from both Monte Carlo simulations with 100 runs and real datasets to ensure a reliable evaluation of the proposed algorithm. For the purpose of evaluation of the UMV-SO(3)-EA algorithm, we choose to compare it with the IEKF-SO(3) introduced in Section 1.7, and also with the IEKF-SO(3) coupled with the threshold-based adaptive approach [146], to compensate the effects of the external acceleration on the estimation accuracy. We selected the threshold-based adaptive approach due to its popularity in the literature, and its ability to run without prior information, specific assumptions about the external acceleration, or a mathematical model of external acceleration.

When showing the results, and in order to facilitate the interpretation of the results, the rotation matrices are converted into Euler angles using the XYZ convention and expressed in degrees.

Threshold-Based Adaptive Approach

The concept behind the threshold-based adaptive approach involves computing the difference between the norm of the accelerometer output and the gravity norm of 9.81 m/s^2, then comparing it to a predefined threshold value ϵ_a (we used $\epsilon_a = 0.2$ m/s^2 [146]). If the difference exceeds the threshold during the time interval, it implies the presence of external acceleration. Consequently, higher values of the acceleration measurements' variances are employed in the IEKF-SO(3) considering the accelerometer measurements as unreliable.

Evaluation with Simulation

This subsection starts by explaining the simulation setup, and then the results will be presented in two parts: the first part includes figures that demonstrate the accuracy of the attitude and external acceleration estimation of the UMV-SO(3)-EA algorithm; the second part involves a comparison with the IEKF-SO(3) to which we add the threshold-based adaptive approach. RMSE was calculated for each Monte Carlo run, and finally, the average was derived from the 100 runs.

Simulations setup

For every Monte Carlo run, the simulated data are generated for a duration of 100 s with a sampling time of $\Delta t = 0.01$ s. The Earth's gravity vector and the Earth's magnetic field are approximated by these two vectors written in NED (North-East-Down) frame in Grenoble, France: $\mathbf{g} = \begin{pmatrix} 0 & 0 & 9.81 \end{pmatrix}^T$ m/s^2 and $\mathbf{m}_e = \begin{pmatrix} 0.23 & 0.01 & 0.41 \end{pmatrix}^T$ G, respectively. The true values for body angular velocity and external acceleration are set as shown in Table 3.1. The gyroscope, accelerometer, and magnetometer noises are set to be zero-mean white noise signals with standard deviations of $\sigma_\omega = 0.01$ rad/s, $\sigma_a = 0.01$ m/s^2, and $\sigma_m = 0.005$ G, respectively. In order to have a fair comparison, the applied external acceleration shown in Table 3.1 is multiplied by a Bernoulli distributed white sequence taking values on $\{0, 1\}$ with

Table 3.1: The true angular velocity and external acceleration used in simulation

True angular velocity (rad/s)		True external acceleration (m/s^2)	
$\boldsymbol{\omega}_k(1)$	$2.0\cos(0.2\pi k\Delta t)$	$\mathbf{a}_k^{ext}(1)$	$2.0\sin(0.5\pi k\Delta t)\gamma_k$
$\boldsymbol{\omega}_k(2)$	$1.5\cos(0.6\pi k\Delta t)$	$\mathbf{a}_k^{ext}(2)$	$1.0\sin(0.2\pi k\Delta t)\gamma_k$
$\boldsymbol{\omega}_k(3)$	$1.0\cos(1.0\pi k\Delta t)$	$\mathbf{a}_k^{ext}(3)$	$0.5\sin(0.1\pi k\Delta t)\gamma_k$

probabilities:

$$\begin{cases} \mathbb{P}(\gamma_k = 1) = \bar{\gamma} \\ \mathbb{P}(\gamma_k = 0) = 1 - \bar{\gamma} \end{cases}$$

A higher value of $\bar{\gamma}$ (i.e. closer to 1) means the body has more instances with the presence of external acceleration, and lower values (i.e. closer to 0) mean more instances with rest.

For each Monte Carlo run, the measurement noise realizations are generated independently, meaning that each simulation has its own unique set of noise values, distinct from those of other runs, with common noise variances. The initial attitude estimate is determined by applying the TRIAD algorithm based on the initial accelerometer and magnetometer measurements, as described in Section 1.6.

UMV-SO(3)-EA theoretical estimation results

The estimation results of the UMV-SO(3)-EA algorithm are presented here for a single Monte Carlo run, under the considered external acceleration for the full duration i.e. $\bar{\gamma} = 1$. Fig. 3.1 illustrates the estimation error. The errors for the three angles generally remain below $0.3°$ most of the time. Although there are instances where the error exceeds $0.3°$, the algorithm demonstrates the ability to correct and achieve low-error estimation. Moreover, the UMV-SO(3)-EA algorithm effectively estimates the external acceleration, and the estimation error, depicted in Fig. 3.2, is mostly ranging between -0.05 m/s^2 and 0.05 m/s^2. Additionally, to illustrate the relative error in the external acceleration estimation, Fig. 3.3 presents both the ground truth and the UMV-SO(3)-EA estimate of the external acceleration. The RMSE (calculated for the 100 Monte-Carlo runs) is 0.04 m/s^2, aligning with the accelerometer's standard deviation range ($4\times\sigma_a$). These findings indicate that the UMV-SO(3)-EA performs well and provides good results even when exposed to the considered external acceleration.

Comparison with the IEKF-SO(3) coupled to the threshold-based adaptive approach

Table 3.2 shows the RMSE of UMV-SO(3)-EA algorithm, the IEKF-SO(3) with and without adaptation for several scenarios depending on the value of $\bar{\gamma}$, where $\bar{\gamma} = 1.0$, $\bar{\gamma} = 0.7$, $\bar{\gamma} = 0.55$, and $\bar{\gamma} = 0.3$ indicates 100%, 70%, 55%, and 30% of taking into account the external acceleration, respectively. In all scenarios, the IEKF-SO(3) with adaptation performs better than the IEKF-SO(3) without adaptation, because the latest relies on unreliable measurements. Across the same scenarios, UMV-SO(3)-EA demonstrates better performance to

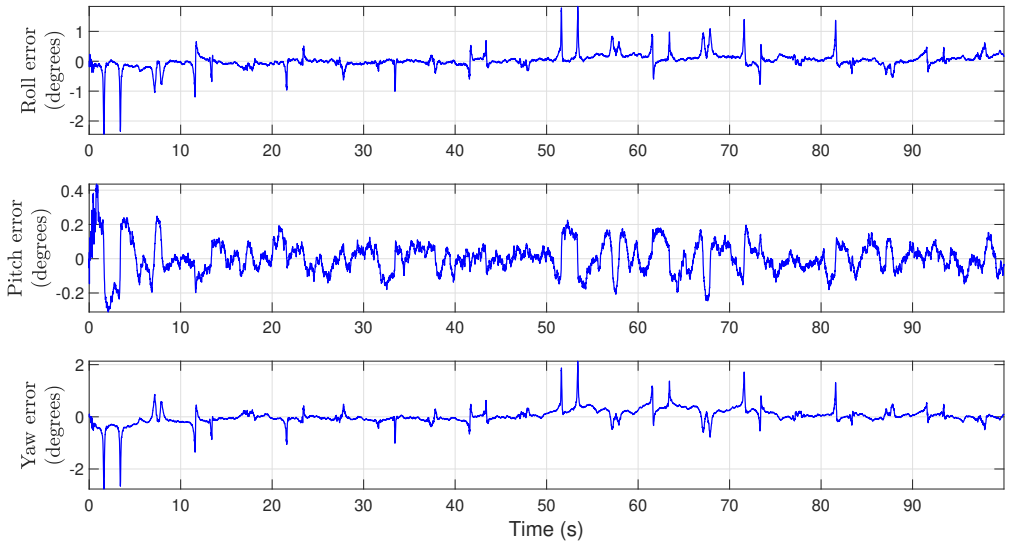

Figure 3.1: Attitude estimation error of UMV-SO(3)-EA represented as Euler angles

Table 3.2: RMSE (in degrees) for UMV-SO(3)-EA, IEKF-SO(3) with adaptation, and IEKF-SO(3) without adaptation in simulation

$\bar{\gamma}$	**UMV-SO(3)-EA**	**IEKF-SO(3) with adaptation**	**IEKF-SO(3)**
1.0	0.43	7.64	9.90
0.7	0.42	1.92	6.17
0.55	0.42	1.19	4.53
0.3	0.42	0.72	2.24

the IEKF-SO(3) with adaptation. This is because the IEKF-SO(3) with adaptation ignores acceleration measurements when detecting external acceleration. The accuracy of UMV-SO(3)-EA estimation is not affected significantly by a full or partial presence of external acceleration. In contrast, the accuracy of the IEKF-SO(3) with adaptation decreases when increasing the presence of external acceleration. This highlights that UMV-SO(3)-EA provides robust performance.

More realistic simulations for comparison: Presence of external acceleration modeled as a Markov chain

In the previous simulations, the presence of external acceleration was modeled by a Bernoulli distribution, meaning that at each time step the external acceleration may appear independently of the previous time step. This modeling is simple, but a more realistic approach is to use a temporally correlated model such as a two-state Markov chain, where the presence of external acceleration depends on its presence at the previous time step. For this purpose,

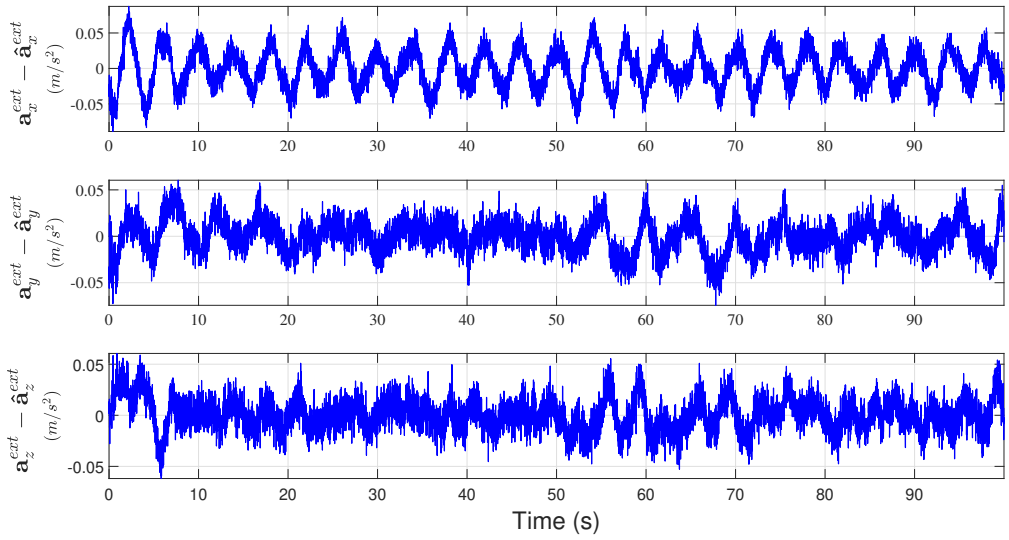

Figure 3.2: External acceleration estimation error $\mathbf{a}^{ext} - \hat{\mathbf{a}}^{ext}$ of UMV-SO(3)-EA

the variable γ_k is modeled as a Markov chain, where:

$$\begin{cases} \bar{\gamma_1^1} = \mathbb{P}(\gamma_k = 1 | \gamma_{k-1} = 1) = 1 - \mathbb{P}(\gamma_k = 0 | \gamma_{k-1} = 1), \\ \bar{\gamma_0^1} = \mathbb{P}(\gamma_k = 1 | \gamma_{k-1} = 0) = 1 - \mathbb{P}(\gamma_k = 0 | \gamma_{k-1} = 0). \end{cases} \tag{3.3.1}$$

The expected value is given by

$$\mathbf{E}(\gamma_k) = \frac{\bar{\gamma_0^1}}{1 - \bar{\gamma_1^1} + \bar{\gamma_0^1}}, \tag{3.3.2}$$

when $(\bar{\gamma_0^1}, \bar{\gamma_1^1}) \neq (0, 1)$. When $(\bar{\gamma_0^1}, \bar{\gamma_1^1}) = (0, 1)$, the sequence becomes constant and its value depends on the initial value.

In this simulation, pairs of $(\bar{\gamma_0^1}, \bar{\gamma_1^1})$ are chosen to obtain the same expected values of γ_k as in Table 3.2. Specifically, $(\bar{\gamma_0^1} = 0.25, \bar{\gamma_1^1} = 0.893)$, $(\bar{\gamma_0^1} = 0.25, \bar{\gamma_1^1} = 0.795)$, and $(\bar{\gamma_0^1} = 0.25, \bar{\gamma_1^1} = 0.417)$ correspond to expected values equal to 0.7, 0.55, and 0.3, respectively. Table 3.3 summarizes the comparison results, which confirm the findings obtained in Table 3.2.

A more realistic simulation is also presented in the next chapter, where alternating phases of presence and absence of external acceleration are implemented, and the duration of each phase is modeled by a uniform distribution.

Evaluation with Real Data

In this subsection, we show the comparison results using the BROAD benchmark datasets [102]. These datasets encompass various real movement scenarios, including rotation and translation, each stored in separate files identified by a trial ID. The datasets are thoroughly described in [102], providing details on sensors' noise variances and dataset characteristics.

For our comparison, we computed the RMSE over 50 s after the initiation of movement. Note that there is an initial rest phase of approximately 30 s, so each algorithm runs for around

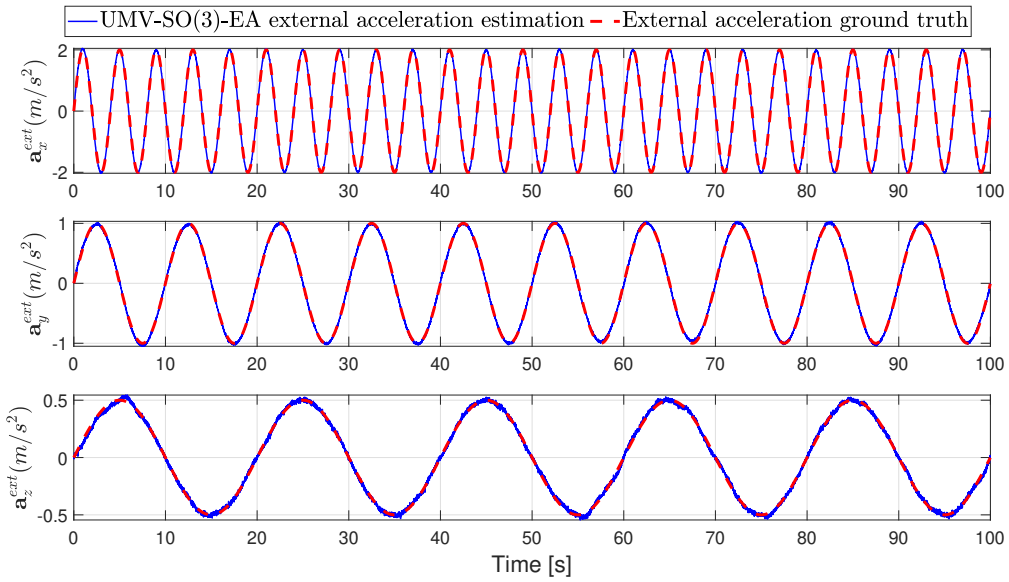

Figure 3.3: UMV-SO(3)-EA external acceleration estimation and ground truth.

Table 3.3: RMSE (in degrees) for UMV-SO(3)-EA, IEKF-SO(3) with adaptation, and IEKF-SO(3) without adaptation, in simulations where the presence of external acceleration is modeled as a Markov chain

$\bar{\gamma}_0^1$	$\bar{\gamma}_1^1$	$\mathbf{E}(\gamma_k)$	**UMV-SO(3)-EA**	**IEKF-SO(3)** with adaptation	**IEKF-SO(3)**
0.25	0.893	0.7	0.35	2.09	6.65
	0.795	0.55	0.37	1.57	5.16
	0.417	0.3	0.31	0.81	2.70

80 s for each scenario. We conducted this analysis for two different trials, numbered 16, and 23 with the results presented in Table 3.4. In trial 16, there is a significant external acceleration, with the measured acceleration norm reaching up to 10 times the Earth's gravity, persisting at a high value for most of the time. Trial 23, on the other hand, exhibits a lower acceleration norm, staying below 2 times the Earth's gravity, and having fewer instances with high measurement acceleration norms, mostly remaining close to the Earth's gravity. Our observations indicate that the UMV-SO(3)-EA consistently outperforms the IEKF-SO(3) with threshold-based adaptation. The improvement varies depending on the duration of external acceleration, and it is particularly significant during long periods of external acceleration. The accelerated motion duration of trial 16 is close to the simulated scenario with $\gamma = 0.55$. The IEKF-SO(3) with adaptation performs 2.8 times worse than UMV-SO(3)-EA in simulation, and around 1.5 times in real data. This difference could be due to several reasons, such as unmet assumptions regarding uncorrelated measurement noises, imprecise knowledge of covariance matrices, and sensor biases. Additionally, real magnetometer measurements

Table 3.4: RMSE (in degrees) for UMV-SO(3)-EA, IEKF-SO(3) with adaptation, and IEKF-SO(3) without adaptation when using real datasets

Trial ID in [102]	**UMV-SO(3)-EA**	**IEKF-SO(3) with adaptation**	**IEKF-SO(3)**
16	7.23	10.96	40.56
23	4.42	5.50	6.65

suffer from magnetic field disturbances, which are non-negligible.

Limitation and proposed solutions of UMV-SO(3)-EA

In both simulation and real data, UMV-SO(3)-EA performs better than existing algorithms in the literature. However, these simulation and real-data tests may not cover all scenarios that could occur in practice. The algorithm assumes that the system is left-invertible, which introduces a limitation. For example, if the gyroscope provides incorrect measurements at certain moments due to an internal fault, this will lead to an incorrect prediction. Since the prediction error covariance matrix does not account for such unexpected faults, this will consequently result in incorrect estimation of both the external acceleration and the attitude.

To address this, an additional correction step can be added to the algorithm. At each moment, the external acceleration is checked. This is done by comparing the norm of the measured acceleration with the gravity magnitude. If the difference between the two is sufficiently small, it can be considered an indicator that the external acceleration is zero. In this case, the algorithm can enforce the external acceleration estimate to be zero. An algorithm such as IEKF-SO(3) can then be run during these periods, while UMV-SO(3)-EA remains active during periods when external acceleration is present.

Additionally, gyro bias is not considered in this algorithm. An important direction for future work is to extend the method to account for gyro bias. This could be done by designing a new algorithm that treats both gyro bias and external acceleration as unknown inputs, applying the unknown input filtering methods presented in this thesis, or by augmenting the gyro bias into the state. Both extensions deserve dedicated investigation.

3.4. Conclusion

This chapter presented a novel attitude estimation algorithm in the presence of external acceleration, using measurements from MARG sensors, by considering the external acceleration as an unknown input affecting the output function. The proposed UMV-SO(3)-EA was evaluated through Monte Carlo simulations and real datasets, and it was compared to the IEKF-SO(3), with a threshold-based adaptation technique. The results, with both simulated and real data, showed that the UMV-SO(3)-EA performed precise and robust attitude estimation under significant external acceleration, and also outperformed the IEKF-SO(3) with threshold-based adaptation. The results showed also accurate external acceleration

estimation of UMV-SO(3)-EA.

The next chapter extends this framework to the estimation of position, velocity, and attitude based on MARG and position measurements, also under unknown external acceleration, that affects both dynamic model and output function. This problem introduces additional theoretical challenges, such as the coupling between translational and rotational dynamics and the influence of unknown acceleration on both motion components. These challenges are addressed through a new estimation strategy developed in the next chapter.

Chapter 4

Position, Velocity, and Attitude Estimation Based on MARG and Position Sensors

This chapter starts with the introductory Section 4.1, which extends the model employed in Chapter 3 to include position and velocity in the dynamics and position sensor measurements in the output, and explains existing solutions in the literature for position, velocity, and attitude estimation based on MARG and position sensors. Section 4.2 presents the derivation of the proposed PVA-SO(3) algorithm. Section 4.3 evaluates the proposed algorithm through simulations. Finally, Section 4.4 concludes the chapter and prepares the reader for Chapter 6, which is the bridge between the two parts. [1]

4.1. Preliminaries and Problem Statement

This chapter addresses the problem of position, velocity, and attitude estimation based on MARG and position measurements. The position can be directly measured using GPS [68], or computed from other sensors such as range measurements [7] and Ultra Wide-Band (UWB) radio technology [75].

Velocity is the time derivative of position, and the external acceleration (i.e., the translational acceleration) expressed in the navigation frame is the time derivative of velocity. The discrete-time position and velocity dynamic model is given by:

$$\mathbf{v}_{k+1} = \mathbf{v}_k + \mathbf{a}_k^{ext,n}\Delta t, \tag{4.1.1}$$

$$\mathbf{p}_{k+1} = \mathbf{p}_k + \mathbf{v}_k\Delta t, \tag{4.1.2}$$

where $\mathbf{v}_k$ and $\mathbf{p}_k$ denote the velocity and position at time step k, and $\mathbf{a}_k^{ext,n}$ is the external acceleration expressed in the navigation frame. The output measurement model is the

[1] Before reading this chapter, it is recommended to first read Chapter 1 and Chapter 3.

position measurements:

$$\mathbf{p}_k^m = \mathbf{p}_k + \mathbf{w}_k^p, \tag{4.1.3}$$

where $\mathbf{p}_k^m$ is the measured position and $\mathbf{w}_k^p$ is the position measurement noise.

This position and velocity dynamic model (4.1.1)-(4.1.2), with the external acceleration $\mathbf{a}_k^{ext,n}$ as input and the position measurements as output, defines a linear state-space system in which both position and velocity are observable. However, the external acceleration is not directly measured. As explained in the previous chapter, the external acceleration is measured in the body frame, together with the gravity component. Some approaches estimate the external acceleration by differentiating velocity measurements obtained from air-data systems or Doppler radar, or by computing the second derivative of position measurements [88, 90]. However, these methods are sensitive to noise amplification.

In the cascaded approach [191] adopted in the literature, the external acceleration is typically expressed in terms of accelerometer measurements and attitude. Specifically, the external acceleration in the navigation frame is written as $\mathbf{a}_k^{ext,n} = \mathbf{R}_k \mathbf{a}_k^{ext}$, where $\mathbf{R}_k \in \mathrm{SO}(3)$ is the rotation matrix representing the attitude, and $\mathbf{a}_k^{ext}$ is the external acceleration expressed in the body frame. This body-frame external acceleration is further expressed as $\mathbf{a}_k^{ext} = \mathbf{a}_k^m - \mathbf{R}_k^\top \mathbf{g} - \mathbf{w}_k^a$, where $\mathbf{a}_k^m$ is the accelerometer measurement, $\mathbf{g}$ is the gravity vector, and $\mathbf{w}_k^a$ denotes the accelerometer measurement noise (see (1.5.2)). Consequently, the velocity model used in this approach is given by $\mathbf{v}_{k+1} = \mathbf{v}_k + (\mathbf{R}_k(\mathbf{a}_k^m - \mathbf{w}_k^a) - \mathbf{g})\,\Delta t$. This model requires knowledge of the attitude $\mathbf{R}_k$, which is typically replaced by an estimate obtained from MARG sensor measurements. As discussed in Chapter 3, attitude estimation based on MARG sensors is affected by the presence of external acceleration.

Chapter 3 proposed to address this issue by considering the external acceleration as an unknown input affecting the output function. In the present chapter, this formulation is extended to jointly estimate position, velocity, and attitude. In this case, the unknown external acceleration affects not only the output function but also the dynamic model, specifically appearing in the velocity dynamics.

To have a complete state space representation, the position (4.1.2), velocity (4.1.1), and attitude (1.5.6) dynamic models, along with the output consisting of the accelerometer measurements (1.5.2), the magnetometer measurements (1.5.3), and the position measurements (4.1.3), are recalled below.

$$\mathbf{R}_{k+1} = \mathbf{R}_k \exp_m\left((\boldsymbol{\omega}_k^m - \mathbf{w}_k^\omega)\Delta t\right), \tag{4.1.4}$$
$$\mathbf{v}_{k+1} = \mathbf{v}_k + \mathbf{R}_k \mathbf{a}_k^{ext} \Delta t, \tag{4.1.5}$$
$$\mathbf{p}_{k+1} = \mathbf{p}_k + \mathbf{v}_k \Delta t, \tag{4.1.6}$$

$$\mathbf{y}_k = \mathbf{h}^+(\mathbf{R}_k, \mathbf{p}_k) + \mathbf{D}\mathbf{a}_k^{ext} + \mathbf{w}_k^y, \tag{4.1.7}$$

where $\boldsymbol{\omega}_k^m \in \mathbb{R}^3$ is the measured angular velocity, and $\mathbf{w}_k^\omega \in \mathbb{R}^3$ represents the gyroscope noise. The function $\mathbf{h}^+(\cdot)$, the matrix $\mathbf{D} \in \mathbb{R}^{9\times 3}$ and the measurement noise $\mathbf{w}_k^y \in \mathbb{R}^9$ are

given by:

$$\mathbf{h}^{+}(\mathbf{R},\mathbf{p}) = \begin{pmatrix} \mathbf{R}^{\top}\mathbf{g} \\ \mathbf{R}^{\top}\mathbf{m}_e \\ \mathbf{p} \end{pmatrix}, \quad \mathbf{D} = \begin{pmatrix} \mathbf{I}_3 \\ \mathbf{0}_3 \\ \mathbf{0}_3 \end{pmatrix}, \quad \mathbf{w}_k^{y} = \begin{pmatrix} \mathbf{w}_k^{a} \\ \mathbf{w}_k^{b} \\ \mathbf{w}_k^{p} \end{pmatrix},$$

where $\mathbf{m}_e$ and $\mathbf{w}_k^b$ are the Earth's magnetic field and magnetometer measurement noise, respectively. The noises $\mathbf{w}_k^{\omega}$ and $\mathbf{w}_k^{y}$ are assumed to be uncorrelated, zero-mean white random signals with positive definite covariance matrices $\boldsymbol{\mathcal{Q}}_k$ and $\boldsymbol{\mathcal{R}}_k$, respectively.

Similar to Chapter 3, this chapter designs a solution that assumes the availability of an unbiased initial estimate of attitude. The proposed algorithm in this chapter, named PVA-SO(3), provides an unbiased minimum variance first-order approximation-based estimator for Position $\mathbf{p}_k$, Velocity $\mathbf{v}_k$, Attitude $\mathbf{R}_k \in \mathrm{SO}(3)$, and the external acceleration $\mathbf{a}_k^{ext}$, based on unbiased estimates of $\mathbf{R}_{k-1}$, $\mathbf{v}_{k-1}$, $\mathbf{p}_{k-1}$, and $\mathbf{a}_{k-1}^{ext}$, and the measurements $\boldsymbol{\omega}_{k-1}^{m}$ and $\mathbf{y}_k$.

As explained in Chapter 3, obtaining an unbiased and slightly perturbed initial attitude estimate is possible using static algorithms, such as the TRIAD method described in Section 1.6, which relies on the initial magnetometer and accelerometer measurements, where the external acceleration is known and equal to zero before the body starts moving.

The main contributions of this chapter are:

- Development of an estimator for systems on $\mathrm{SO}(3)\times\mathbb{R}^3\times\mathbb{R}^3$, with an unknown input affecting both the dynamics and the output, and multiplicatively coupled with the state on SO(3).
- Design of a novel estimation algorithm for position, velocity, attitude, and external acceleration based on measurements from MARG and position sensors.

The material presented in this chapter is based on the corresponding publication, currently under review:

- *G. Shaaban, H. Fourati, A. Kibangou, and C. Prieur, "Position, velocity and attitude estimation based on MARG and position measurements under unknown external acceleration," IEEE Control Systems Letters, vol. 9, pp. 1423-1428, June 2025.*

4.2. PVA-SO(3) Algorithm Derivation

The current chapter adopts the three-step procedure as Chapter 3. The three steps are: (i) state prediction based on the dynamic model and previous estimates, (ii) external acceleration estimation based on the state prediction and measurements, and (iii) state estimation correction using the state prediction, external acceleration estimation, and measurements. The proposed PVA-SO(3) filter has the following structure:

▷ Prediction:

$$\hat{\mathbf{R}}_{k|k-1} = \hat{\mathbf{R}}_{k-1} \exp_m(\boldsymbol{\omega}_{k-1}^m \Delta t), \tag{4.2.1}$$
$$\hat{\mathbf{v}}_{k|k-1} = \hat{\mathbf{v}}_{k-1} + \hat{\mathbf{R}}_{k-1} \hat{\mathbf{a}}_{k-1}^{ext} \Delta t, \tag{4.2.2}$$
$$\hat{\mathbf{p}}_{k|k-1} = \hat{\mathbf{p}}_{k-1} + \hat{\mathbf{v}}_{k-1} \Delta t. \tag{4.2.3}$$

▷ External acceleration estimation:

$$\hat{\mathbf{a}}_k^{ext} = \mathbf{M}_k \left(\mathbf{y}_k - \mathbf{h}^+(\hat{\mathbf{R}}_{k|k-1}, \hat{\mathbf{p}}_{k|k-1}) \right). \tag{4.2.4}$$

▷ Correction:

$$\boldsymbol{\delta}_k = \mathbf{K}_k \left(\mathbf{y}_k - \mathbf{h}^+(\hat{\mathbf{R}}_{k|k-1}, \mathbf{p}_{k|k-1}) - \mathbf{D}\hat{\mathbf{a}}_k^{ext} \right), \tag{4.2.5}$$
$$\hat{\mathbf{R}}_k = \hat{\mathbf{R}}_{k|k-1} \exp_m(\boldsymbol{\delta}_k(1:3)), \tag{4.2.6}$$
$$\hat{\mathbf{v}}_k = \hat{\mathbf{v}}_{k|k-1} + \boldsymbol{\delta}_k(4:6), \tag{4.2.7}$$
$$\hat{\mathbf{p}}_k = \hat{\mathbf{p}}_{k|k-1} + \boldsymbol{\delta}_k(7:9), \tag{4.2.8}$$

where the matrices $\mathbf{M}_k \in \mathbb{R}^{3\times 9}$ and $\mathbf{K}_k \in \mathbb{R}^{3\times 9}$ are the gain matrices which have to be designed.

Main goal: *Considering* $\hat{\mathbf{R}}_{k-1}$, $\hat{\mathbf{v}}_{k-1}$, $\hat{\mathbf{p}}_{k-1}$, *and* $\hat{\mathbf{a}}_{k-1}^{ext}$ *are unbiased, the objective is to design* $\mathbf{M}_k$ *and* $\mathbf{K}_k$ *so that the first-order approximation-based estimators of* $\hat{\mathbf{R}}_k$, $\hat{\mathbf{v}}_k$, $\hat{\mathbf{p}}_k$, *and* $\hat{\mathbf{a}}_k^{ext}$ *provided by* (4.2.6), (4.2.7), (4.2.8), *and* (4.2.4), *respectively, are unbiased minimum variance (see Lemma 4.2.2, Theorem 4.2.4 and Theorem 4.2.8).*

The current chapter presents three main challenges beyond Chapter 3. First, the state includes two additional vectors in $\mathbb{R}^3$, along with the attitude, which belongs to SO(3). Second, in contrast to Chapter 3, where the unknown external acceleration affects only the measurements, the current chapter involves it affecting both the dynamic model and the measurements, creating a coupling between state prediction and external acceleration estimation. Third, the dynamic model involves a multiplication of the rotation matrix with the unknown external acceleration, making the derivation of the prediction error transition matrix, which is essential for deriving the prediction covariance matrix, challenging.

We denote the state estimation error by $\mathbf{e}_k = \begin{pmatrix} \boldsymbol{\xi}_k \\ \mathbf{e}_k^v \\ \mathbf{e}_k^x \end{pmatrix}$, and the external acceleration estimation error by $\mathbf{e}_k^a = \mathbf{a}_k^{ext} - \hat{\mathbf{a}}_k^{ext}$, where $\exp_{\mathrm{m}}(\boldsymbol{\xi}_k) = \hat{\mathbf{R}}_k^{-1}\mathbf{R}_k$, $\mathbf{e}_k^v = \mathbf{v}_k - \hat{\mathbf{v}}_k$, and $\mathbf{e}_k^x = \mathbf{p}_k - \hat{\mathbf{p}}_k$ are the attitude, velocity, and position estimation error, respectively. We define the corresponding covariance matrics: $\mathbf{P}_k^e = \mathbf{E}(\mathbf{e}_k\mathbf{e}_k^T)$, $\mathbf{P}_k^a = \mathbf{E}(\mathbf{e}_k^a\mathbf{e}_k^{aT})$, and $\mathbf{P}_k^{ae} = (\mathbf{P}_k^{ea})^T = \mathbf{E}(\mathbf{e}_k^a\mathbf{e}_k^T)$. In the following, the steps of the algorithm are derived, beginning with the prediction, followed by the estimation of the external acceleration, and then the correction. Finally, a summary of the complete algorithm is provided.

Prediction:

A key contribution of this chapter is presented in Lemma 4.2.1, which is given below. It establishes the estimation error for the product of two estimates: one belonging to SO(3) and the other to $\mathbb{R}^3$.

Lemma 4.2.1. *Consider two elements, $\mathbf{R} \in SO(3)$ and $\mathbf{a} \in \mathbb{R}^3$, with their respective estimations $\hat{\mathbf{R}} \in SO(3)$ and $\hat{\mathbf{a}} \in \mathbb{R}^3$, and their respective estimation errors $\exp_m(\boldsymbol{\xi}) = \hat{\mathbf{R}}^{-1}\mathbf{R}$ and $\mathbf{e}^a = \mathbf{a} - \hat{\mathbf{a}}$. The following equation holds:*

$$\mathbf{R}\mathbf{a} - \hat{\mathbf{R}}\hat{\mathbf{a}} = -\hat{\mathbf{R}}(\hat{\mathbf{a}})_\times \boldsymbol{\xi} + \hat{\mathbf{R}}\mathbf{e}^a + \mathcal{O}(||\boldsymbol{\xi}||^2, ||\boldsymbol{\xi}||.||\mathbf{e}^a||)) \tag{4.2.9}$$

Proof.

$$\begin{aligned}\mathbf{R}\mathbf{a} =& \hat{\mathbf{R}} \exp_m(\boldsymbol{\xi})(\hat{\mathbf{a}} + \mathbf{e}^a),\\ =& \hat{\mathbf{R}}(\mathbf{I}_3 + (\boldsymbol{\xi})_\times + \mathcal{O}(||\boldsymbol{\xi}||^2))(\hat{\mathbf{a}} + \mathbf{e}^a),\\ =& \hat{\mathbf{R}}\hat{\mathbf{a}} + \hat{\mathbf{R}}(\boldsymbol{\xi})_\times \hat{\mathbf{a}} + \hat{\mathbf{R}}\mathbf{e}^a + \mathcal{O}(||\boldsymbol{\xi}||^2) + \hat{\mathbf{R}}(\boldsymbol{\xi})_\times \mathbf{e}^a,\end{aligned}$$

thus:

$$\mathbf{R}\mathbf{a} - \hat{\mathbf{R}}\hat{\mathbf{a}} = -\hat{\mathbf{R}}(\hat{\mathbf{a}})_\times \boldsymbol{\xi} + \hat{\mathbf{R}}\mathbf{e}^a + \mathcal{O}(||\boldsymbol{\xi}||^2, ||\boldsymbol{\xi}||.||\mathbf{e}^a||)).$$

■

The prediction step is addressed in Lemma 4.2.2, which is presented below. It provides the expression for the prediction error covariance matrix used in the subsequent algorithm derivation.

Lemma 4.2.2. *Let $\hat{\mathbf{R}}_{k-1}$, $\hat{\mathbf{v}}_{k-1}$, $\hat{\mathbf{p}}_{k-1}$, and $\hat{\mathbf{a}}^{ext}_{k-1}$ be unbiased, then the attitude, velocity and position predictions provided by (4.2.1), (4.2.2), and (4.2.3) are unbiased, and the prediction error covariance matrix is given by:*

$$\mathbf{P}^e_{k|k-1} = \begin{pmatrix} \mathbf{A}_{k-1} & \mathbf{B}_{k-1} \end{pmatrix} \begin{pmatrix} \mathbf{P}^e_{k-1} & \mathbf{P}^{ea}_{k-1} \\ \mathbf{P}^{ae}_{k-1} & \mathbf{P}^a_{k-1} \end{pmatrix} \begin{pmatrix} \mathbf{A}^T_{k-1} \\ \mathbf{B}^T_{k-1} \end{pmatrix} + \mathbf{G}\boldsymbol{\mathcal{Q}}_{k-1}\mathbf{G}^T, \tag{4.2.10}$$

where:

$$\mathbf{A}_{k-1} = \begin{pmatrix} \mathbf{I}_3 & \mathbf{0}_3 & \mathbf{0}_3 \\ -\hat{\mathbf{R}}_{k-1}(\hat{\mathbf{a}}^{ext}_{k-1})_\times \Delta t & \mathbf{I}_3 & \mathbf{0}_3 \\ \mathbf{0}_3 & \mathbf{I}_3\Delta t & \mathbf{I}_3 \end{pmatrix}, \quad \mathbf{B}_{k-1} = \begin{pmatrix} \mathbf{0}_3 \\ \hat{\mathbf{R}}_{k-1}\Delta t \\ \mathbf{0}_3 \end{pmatrix}, \quad \mathbf{G} = \begin{pmatrix} \mathbf{I}_3\Delta t \\ \mathbf{0}_3 \\ \mathbf{0}_3 \end{pmatrix},$$

Proof. The attitude prediction error is

$$\begin{aligned}\exp_m(\boldsymbol{\xi}_{k|k-1}) =& \hat{\mathbf{R}}^T_{k|k-1}\mathbf{R}_k,\\ =& \exp_m(-\boldsymbol{\omega}^m_{k-1}\Delta t)\hat{\mathbf{R}}^T_{k-1}\mathbf{R}_{k-1}\exp_m(\boldsymbol{\omega}^m_{k-1}\Delta t - \mathbf{w}^\omega_{k-1}\Delta t),\\ =& \exp_m(-\boldsymbol{\omega}^m_{k-1}\Delta t)\exp_m(\boldsymbol{\xi}_{k-1})\exp_m(\boldsymbol{\omega}^m_{k-1}\Delta t - \mathbf{w}^\omega_{k-1}\Delta t),\end{aligned}$$

Applying BCH formula (1.4.5) gives

$$\boldsymbol{\xi}_{k|k-1} = \boldsymbol{\xi}_{k-1} - \mathbf{w}^{\omega}_{k-1}\Delta t. \tag{4.2.11}$$

The velocity prediction error is:

$$\begin{aligned}\mathbf{e}^{v}_{k|k-1} =& \mathbf{v}_k - \hat{\mathbf{v}}_{k|k-1},\\ =& \mathbf{v}_{k-1} + \mathbf{R}_{k-1}\mathbf{a}^{ext}_{k-1}\Delta t - \hat{\mathbf{v}}_{k-1} - \hat{\mathbf{R}}_{k-1}\hat{\mathbf{a}}^{ext}_{k-1}\Delta t,\\ =& \mathbf{e}^{v}_{k-1} + \left(\mathbf{R}_{k-1}\mathbf{a}^{ext}_{k-1} - \hat{\mathbf{R}}_{k-1}\hat{\mathbf{a}}^{ext}_{k-1}\right)\Delta t.\end{aligned}$$

Applying first order approximation of Lemma 4.2.1 on the term $\mathbf{R}_{k-1}\mathbf{a}^{ext}_{k-1}$ we obtain:

$$\mathbf{e}^{v}_{k|k-1} = \mathbf{e}^{v}_{k-1} - \hat{\mathbf{R}}_{k-1}(\hat{\mathbf{a}}^{ext}_{k-1})_{\times}\boldsymbol{\xi}_{k-1}\Delta t + \hat{\mathbf{R}}_{k-1}\mathbf{e}^{a}_{k-1}\Delta t. \tag{4.2.12}$$

The position prediction error is

$$\begin{aligned}\mathbf{e}^{x}_{k|k-1} =& \mathbf{p}_k - \hat{\mathbf{p}}_{k|k-1},\\ =& \mathbf{p}_{k-1} + \mathbf{v}_{k-1}\Delta t - \hat{\mathbf{p}}_{k-1} - \hat{\mathbf{v}}_{k-1}\Delta t,\\ =& \mathbf{e}^{x}_{k-1} + \mathbf{e}^{v}_{k-1}\Delta t.\end{aligned} \tag{4.2.13}$$

Concatinating the prediction error equations (4.2.11), (4.2.12), and (4.2.13) gives:

$$\begin{aligned}\mathbf{e}_{k|k-1} =& \begin{pmatrix} \mathbf{I}_3 & \mathbf{0}_3 & \mathbf{0}_3 \\ -\hat{\mathbf{R}}_{k-1}(\hat{\mathbf{a}}^{ext}_{k-1})_{\times}dt & \mathbf{I}_3 & \mathbf{0}_3 \\ \mathbf{0}_3 & \mathbf{I}_3 dt & \mathbf{I}_3 \end{pmatrix}\mathbf{e}_{k-1} + \begin{pmatrix} \mathbf{0}_3 \\ \hat{\mathbf{R}}_{k-1}dt \\ \mathbf{0}_3 \end{pmatrix}\mathbf{e}^{a}_{k-1} - \begin{pmatrix} \mathbf{I}_3 dt \\ \mathbf{0}_3 \\ \mathbf{0}_3 \end{pmatrix}\mathbf{w}^{\omega}_{k-1},\\ =& \begin{pmatrix} \mathbf{A}_{k-1} & \mathbf{B}_{k-1} \end{pmatrix}\begin{pmatrix} \mathbf{e}_{k-1} \\ \mathbf{e}^{a}_{k-1} \end{pmatrix} - \mathbf{G}\mathbf{w}^{\omega}_{k-1}.\end{aligned} \tag{4.2.14}$$

Thus, $\mathbf{E}(\mathbf{e}_{k|k-1}) = \mathbf{0}$ follows from the unbiasedness of $\mathbf{e}_{k-1}$, $\mathbf{e}^{a}_{k-1}$ and $\mathbf{w}^{\omega}_{k-1}$. Finally, computing the covariance matrix $\mathbf{E}(\mathbf{e}_{k|k-1}\mathbf{e}^{T}_{k|k-1})$ confirms the prediction covariance matrix (4.2.10). ■

External Acceleration Estimation:

The sufficient conditions for the local optimality of the external acceleration estimator (4.2.4) are established in Theorem 4.2.4, with the support of Lemma 4.2.3, both of which are presented below.

Lemma 4.2.3. *Let $\mathbf{e}_{k|k-1}$ be unbiased, then the term $\tilde{\mathbf{y}}_k = \mathbf{y}_k - \mathbf{h}^{+}(\hat{\mathbf{R}}_{k|k-1}, \hat{\mathbf{p}}_{k|k-1})$ has first order approximation*

$$\tilde{\mathbf{y}}_k = \mathbf{D}\mathbf{a}^{ext}_k + \tilde{\mathbf{e}}_k,$$

where

$$\tilde{\mathbf{e}}_k = \mathbf{H}^{+}_k\mathbf{e}_{k|k-1} + \mathbf{w}^{y}_k, \tag{4.2.15}$$

the matrix $\mathbf{H}_k^+$ *is defined as follows:*

$$\mathbf{H}_k^+ = \begin{pmatrix} (\hat{\mathbf{R}}_{k|k-1}^T \mathbf{g})_\times & \mathbf{0}_3 & \mathbf{0}_3 \\ (\hat{\mathbf{R}}_{k|k-1}^T \mathbf{m}_e)_\times & \mathbf{0}_3 & \mathbf{0}_3 \\ \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{I}_3 \end{pmatrix}, \tag{4.2.16}$$

and the random variable $\tilde{\mathbf{e}}_k$ *has zero mean and positive definite covariance matrix*

$$\tilde{\boldsymbol{\mathcal{R}}}_k = \mathbf{H}_k^+ \mathbf{P}_{k|k-1}^e \mathbf{H}_k^{+T} + \boldsymbol{\mathcal{R}}_k. \tag{4.2.17}$$

Proof. $\tilde{\mathbf{y}}_k = \mathbf{h}^+(\hat{\mathbf{R}}_k, \hat{\mathbf{p}}_k) - \mathbf{h}^+(\hat{\mathbf{R}}_{k|k-1}, \hat{\mathbf{p}}_{k|k-1}) + \mathbf{D}\mathbf{a}_k^{ext} + \mathbf{w}_k^y$. We simplify the term

$$\begin{aligned} \tilde{\mathbf{h}} =& \mathbf{h}^+(\hat{\mathbf{R}}_k, \hat{\mathbf{p}}_k) - \mathbf{h}^+(\hat{\mathbf{R}}_{k|k-1}, \hat{\mathbf{p}}_{k|k-1}), \\ =& \begin{pmatrix} \mathbf{R}_k^T \mathbf{g} \\ \mathbf{R}_k^T \mathbf{m}_e \\ \mathbf{p}_k \end{pmatrix} - \begin{pmatrix} \mathbf{R}_{k|k-1}^T \mathbf{g} \\ \mathbf{R}_{k|k-1}^T \mathbf{m}_e \\ \mathbf{p}_{k|k-1} \end{pmatrix}, \\ =& \begin{pmatrix} (\exp_m(-\boldsymbol{\xi}_{k|k-1}) - \mathbf{I}_3)\mathbf{R}_{k|k-1}^T \mathbf{g} \\ (\exp_m(-\boldsymbol{\xi}_{k|k-1}) - \mathbf{I}_3)\mathbf{R}_{k|k-1}^T \mathbf{m}_e \\ \mathbf{e}_{k|k-1}^x \end{pmatrix}, \end{aligned}$$

by applying (1.4.4), we obtain:

$$\tilde{\mathbf{h}} = \begin{pmatrix} -(\boldsymbol{\xi}_{k|k-1})_\times \hat{\mathbf{R}}_{k|k-1}^T \mathbf{g} \\ -(\boldsymbol{\xi}_{k|k-1})_\times \hat{\mathbf{R}}_{k|k-1}^T \mathbf{m}_e \\ \mathbf{e}_{k|k-1}^x \end{pmatrix} = \begin{pmatrix} (\hat{\mathbf{R}}_{k|k-1}^T \mathbf{g})_\times \boldsymbol{\xi}_{k|k-1} \\ (\hat{\mathbf{R}}_{k|k-1}^T \mathbf{m}_e)_\times \boldsymbol{\xi}_{k|k-1} \\ \mathbf{e}_{k|k-1}^x \end{pmatrix} = \mathbf{H}_k^+ \mathbf{e}_{k|k-1}.$$

Substituting it gives

$$\begin{aligned} \tilde{\mathbf{y}}_k =& \mathbf{D}\mathbf{a}_k^{ext} + \mathbf{H}_k^+ \mathbf{e}_{k|k-1} + \mathbf{w}_k^y, \\ =& \mathbf{D}\mathbf{a}_k^{ext} + \tilde{\mathbf{e}}_k. \end{aligned}$$

Also, $\mathbf{E}(\tilde{\mathbf{e}}_k) = \mathbf{0}$ follows from the unbiasedness of $\mathbf{e}_{k|k-1}$ and $\mathbf{w}_k^y$. Finally, computing the covariance matrix $\tilde{\boldsymbol{\mathcal{R}}}_k = \mathbf{E}(\tilde{\mathbf{e}}_k \tilde{\mathbf{e}}_k^T)$ confirms (4.2.17). ■

Theorem 4.2.4. *Let* $\mathbf{e}_{k|k-1}$ *be unbiased, and the matrix gain* $\mathbf{M}_k$ *has the following value:*

$$\mathbf{M}_k = \left(\mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \mathbf{D}\right)^{-1} \mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1}, \tag{4.2.18}$$

then the first order approximation-based estimator of $\mathbf{a}_k^{ext}$ *given by* (4.2.4) *is unbiased minimum variance, the estimation error is given by:*

$$\mathbf{e}_k^a = \mathbf{a}_k^{ext} - \hat{\mathbf{a}}_k^{ext} = -\mathbf{M}_k\tilde{\mathbf{e}}_k, \tag{4.2.19}$$

and its covariance matrix is equal to:

$$\mathbf{P}_k^a = \left(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D}\right)^{-1}. \tag{4.2.20}$$

Proof. Lemma 4.2.3 holds, thus $\tilde{\mathbf{y}}_k = \mathbf{D}\mathbf{a}_k^{ext} + \tilde{\mathbf{e}}_k$, where $\tilde{\mathbf{e}}_k$ is a random variable with zero mean and positive definite covariance matrix $\tilde{\boldsymbol{\mathcal{R}}}_k$, and the matrix $\mathbf{D}$ is full column rank, thus we can apply Gauss-Markov Theorem on $\tilde{\mathbf{y}}_k$ [93, Chapter 3.4.2], and the gain matrix $\mathbf{M}_k$ defined in (4.2.18) is making the first order based estimator of (4.2.4) unbiased minimum variance. This gain matrix satisfies $\mathbf{M}_k\mathbf{D} = \mathbf{I}_3$, applying it in the estimator of $\mathbf{a}_k^{ext}$ (after substituting $\tilde{\mathbf{y}}_k$), we obtain $\hat{\mathbf{a}}_k^{ext} = \mathbf{M}_k\left(\ \mathbf{D}\mathbf{a}_k^{ext} + \tilde{\mathbf{e}}_k\ \right) = \mathbf{a}_k^{ext} + \mathbf{M}_k\tilde{\mathbf{e}}_k$, thus $\mathbf{e}_k^a = \mathbf{a}_k^{ext} - \hat{\mathbf{a}}_k^{ext} = -\mathbf{M}_k\tilde{\mathbf{e}}_k$. Finally, computing the covariance matrix $\mathbf{P}_k^a = E(\mathbf{e}_k^a\mathbf{e}_k^{aT})$ confirms (4.2.20). ■

Correction:

The sufficient conditions for the local optimality of the attitude (4.2.6), velocity (4.2.7), and position estimator (4.2.8) are established in Theorem 4.2.8, with the support of Lemma 4.2.5 and Lemma 4.2.6. In addition, the covariance matrix $\mathbf{P}_k^{ea}$ is derived in Lemma 4.2.7. All of these results are presented below.

Lemma 4.2.5. *Let* $\mathbf{e}_{k|k-1}$ *be unbiased, then the first-order approximation of the attitude, velocity, and position estimation error given by* (4.2.6), (4.2.7), *and* (4.2.8) *is as follows:*

$$\mathbf{e}_k = \left(\mathbf{I}_9 - \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k^+\right)\mathbf{e}_{k|k-1} - \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\mathbf{w}_k^y. \tag{4.2.21}$$

Proof. Lemma 4.2.3 and Theorem 4.2.4 hold, thus

$$\begin{aligned}\mathbf{y}_k - \mathbf{h}^+(\hat{\mathbf{R}}_{k|k-1}, \mathbf{p}_{k|k-1}) - \mathbf{D}\hat{\mathbf{a}}_k^{ext} =& \mathbf{D}\mathbf{a}_k^{ext} + \tilde{\mathbf{e}}_k - \mathbf{D}\hat{\mathbf{a}}_k^{ext},\\ =& \mathbf{D}\mathbf{e}_k^a + \tilde{\mathbf{e}}_k,\\ =& (\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k.\end{aligned}$$

We define $\mathbf{K}_k^\xi = \mathbf{K}_k(1:3)$, $\mathbf{K}_k^v = \mathbf{K}_k(4:6)$, and $\mathbf{K}_k^x = \mathbf{K}_k(7:9)$, thus the correction steps (4.2.6), (4.2.7), and (4.2.8) can be written as follows:

$$\begin{aligned}\hat{\mathbf{R}}_k &= \hat{\mathbf{R}}_{k|k-1}\exp_m(\mathbf{K}_k^\xi\,(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\,\tilde{\mathbf{e}}_k),\\ \hat{\mathbf{v}}_k &= \hat{\mathbf{v}}_{k|k-1} + \mathbf{K}_k^v(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k,\\ \hat{\mathbf{p}}_k &= \hat{\mathbf{p}}_{k|k-1} + \mathbf{K}_k^x(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k.\end{aligned}$$

Attitude estimation error is given by

$$\begin{aligned}\exp_m(\boldsymbol{\xi}_k) =& \hat{\mathbf{R}}_k^{-1}\mathbf{R}_k,\\ =& \exp_m(-\mathbf{K}_k^\xi(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k)\hat{\mathbf{R}}_{k|k-1}^{-1}\mathbf{R}_k,\\ =& \exp_m(-\mathbf{K}_k^\xi(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k)\exp_m(\boldsymbol{\xi}_{k|k-1}),\end{aligned}$$

applying BCH formula (1.4.5) gives

$$\boldsymbol{\xi}_k = -\mathbf{K}_k^{\xi}(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k + \boldsymbol{\xi}_{k|k-1}. \tag{4.2.22}$$

Velocity estimation error is given by:

$$\begin{aligned}\mathbf{e}_k^v =& \mathbf{v}_k - \hat{\mathbf{v}}_k,\\ =& \mathbf{v}_k - \hat{\mathbf{v}}_{k|k-1} - \mathbf{K}_k^v(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k,\\ =& \mathbf{e}_{k|k-1}^v - \mathbf{K}_k^v(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k,\end{aligned} \tag{4.2.23}$$

and the similar calculation for position gives

$$\mathbf{e}_k^x = \mathbf{e}_{k|k-1}^x - \mathbf{K}_k^x(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k. \tag{4.2.24}$$

By vertically concatenating the three estimation errors (4.2.22), (4.2.23), (4.2.24) we obtain

$$\mathbf{e}_k = \mathbf{e}_{k|k-1} - \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\mathbf{e}}_k.$$

By substituting $\tilde{\mathbf{e}}_k = \mathbf{H}_k^{+}\mathbf{e}_{k|k-1} + \mathbf{w}_k^y$ (see Lemma 4.2.3) the proof is established. ■

Lemma 4.2.6. *The terms* $(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\boldsymbol{\mathcal{R}}}_k\mathbf{M}_k^T$ *and* $\mathbf{M}_k\tilde{\boldsymbol{\mathcal{R}}}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)^T$ *are both zero.*

Proof. The two terms are transposes of each other. Thus, proving that one is zero directly implies that the other is also zero.

$$\boldsymbol{\mathcal{R}}_k^* = (\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\boldsymbol{\mathcal{R}}}_k\mathbf{M}_k^T = \tilde{\boldsymbol{\mathcal{R}}}_k\mathbf{M}_k^T - \mathbf{D}\mathbf{M}_k\tilde{\boldsymbol{\mathcal{R}}}_k\mathbf{M}_k^T,$$

substitute $\mathbf{M}_k$ from (4.2.18) gives:

$$\begin{aligned}\boldsymbol{\mathcal{R}}_k^* =& \tilde{\boldsymbol{\mathcal{R}}}_k\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D}(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D})^{-1} - \mathbf{D}(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D})^{-1}\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\tilde{\boldsymbol{\mathcal{R}}}_k\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D}(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D})^{-1},\\ =& \mathbf{D}(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D})^{-1} - \mathbf{D}(\mathbf{D}^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\mathbf{D})^{-1} = \mathbf{0}.\end{aligned}$$

■

Lemma 4.2.7. *Let* $\mathbf{e}_{k|k-1}$ *be unbiased, then*

$$\mathbf{P}_k^{ea} = \mathbf{E}(\mathbf{e}_k\mathbf{e}_k^{aT}) = -\mathbf{P}_{k|k-1}^e\mathbf{H}_k^{+T}\mathbf{M}_k^T. \tag{4.2.25}$$

Proof. We compute the covarinace matrix $\mathbf{P}_k^{ea}$ employing (4.2.15), (4.2.19), and (4.2.21):

$$\begin{aligned}\mathbf{P}_k^{ea} =& \mathbf{E}(\mathbf{e}_k\mathbf{e}_k^{aT})\\ =& \mathbf{E}(((\mathbf{I}_9 - \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k^{+})\mathbf{e}_{k|k-1} - \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\mathbf{w}_k^y)(-\mathbf{M}_k\mathbf{H}_k^{+}\mathbf{e}_{k|k-1} - \mathbf{M}_k\mathbf{w}_k^y)^T),\\ =& -(\mathbf{I}_9 - \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k^{+})\mathbf{P}_{k|k-1}^e\mathbf{H}_k^{+T}\mathbf{M}_k^T + \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\boldsymbol{\mathcal{R}}_k\mathbf{M}_k^T,\\ =& -\mathbf{P}_{k|k-1}^e\mathbf{H}_k^{+T}\mathbf{M}_k^T + \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\left(\mathbf{H}_k^{+}\mathbf{P}_{k|k-1}^e\mathbf{H}_k^{+T} + \boldsymbol{\mathcal{R}}_k\right)\mathbf{M}_k^T,\\ =& -\mathbf{P}_{k|k-1}^e\mathbf{H}_k^{+T}\mathbf{M}_k^T + \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\boldsymbol{\mathcal{R}}}_k\mathbf{M}_k^T,\end{aligned}$$

we apply Lemma 4.2.6 and we conclude $\mathbf{P}_k^{ea} = -\mathbf{P}_{k|k-1}^e\mathbf{H}_k^{+T}\mathbf{M}_k^T$. ■

Theorem 4.2.8. *Let* $\mathbf{e}_{k|k-1}$ *and* $\mathbf{e}_k^a$ *be unbiased, then the state estimates* (4.2.22), (4.2.23), (4.2.24) *are unbiased minimum variance, and the state estimation covariance matrix is given by:*

$$\mathbf{P}_k^e = \mathbf{P}_{k|k-1}^e - \mathbf{K}_k \left(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k\right) \mathbf{H}_k^+ \mathbf{P}_{k|k-1}^e. \tag{4.2.26}$$

Proof. Lemma 4.2.5 holds, thus (4.2.21) is satisfied, and $\mathbf{E}(\mathbf{e}_k) = \mathbf{0}$ follows from the unbiasedness of $\mathbf{e}_{k|k-1}$ and $\mathbf{w}_k^y$. $\mathbf{E}(\|\mathbf{e}_k\|^2) = tr(\mathbf{P}_k^e)$, thus our goal is to find the matrix gain $\mathbf{K}_k$ that satisfies $\frac{dtr(\mathbf{P}_k^e)}{d\mathbf{K}_k} = \mathbf{0}$. First we compute $\mathbf{P}_k^e$:

$$\begin{aligned}
\mathbf{P}_k^e =& \mathbf{E}(\mathbf{e}_k \mathbf{e}_k^T), \\
=& \left(\mathbf{I}_9 - \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k^+\right) \mathbf{P}_{k|k-1}^e (\mathbf{I}_9 - \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k^+)^T \\
&+ \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\boldsymbol{\mathcal{R}}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)^T\mathbf{K}_k^T, \\
=& \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\tilde{\boldsymbol{\mathcal{R}}}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)^T\mathbf{K}_k^T - \mathbf{P}_{k|k-1}^e \mathbf{H}_k^{+T}(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)^T\mathbf{K}_k^T \\
&- \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k^+ \mathbf{P}_{k|k-1}^e + \mathbf{P}_{k|k-1}^e.
\end{aligned} \tag{4.2.27}$$

Applying Lemma 4.2.6 gives:

$$\begin{aligned}
\mathbf{P}_k^e =& \mathbf{K}_k \tilde{\boldsymbol{\mathcal{R}}}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)^T\mathbf{K}_k^T - \mathbf{P}_{k|k-1}^e \mathbf{H}_k^{+T}(\mathbf{I}_9 - \\
& \mathbf{D}\mathbf{M}_k)^T\mathbf{K}_k^T - \mathbf{K}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)\mathbf{H}_k^+ \mathbf{P}_{k|k-1}^e + \mathbf{P}_{k|k-1}^e,
\end{aligned} \tag{4.2.28}$$

implementing matrix derivatives leads to

$$\frac{dtr(\mathbf{P}_k^e)}{d\mathbf{K}_k} = 2\mathbf{K}_k \tilde{\boldsymbol{\mathcal{R}}}_k(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)^T - 2\mathbf{P}_{k|k-1}^e \mathbf{H}_k^{+T}(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k)^T,$$

the matrix gain $\mathbf{K}_k = \mathbf{P}_{k|k-1}^e \mathbf{H}_k^{+T} \tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$ satisfies $\frac{dtr(\mathbf{P}_k^e)}{d\mathbf{K}_k} = \mathbf{0}$. Substituting this $\mathbf{K}_k$ in (4.2.28) confirms the covariance matrix (4.2.26). ■

PVA-SO(3) Algorithm Summary

The inputs of the PVA-SO(3) algorithm are the previously estimated state and external acceleration, along with their corresponding covariance matrices, together with the MARG and position measurements. The algorithm provides, as outputs, the estimated state and external acceleration at the current time step, along with their corresponding estimation error covariance matrices. The detailed steps of the proposed recursive filter PVA-SO(3) are summarized in Algorithm 6.

Algorithm 6 PVA-SO(3)

Inputs: $\hat{\mathbf{R}}_{k-1}$, $\hat{\mathbf{v}}_{k-1}$, $\hat{\mathbf{p}}_{k-1}$, $\hat{\mathbf{a}}^{ext}_{k-1}$, $\mathbf{P}^{e}_{k-1}$, $\mathbf{P}^{a}_{k-1}$, $\mathbf{P}^{ea}_{k-1}$, $\boldsymbol{\omega}^{m}_{k-1}$, $\mathbf{y}_k = \begin{pmatrix} \mathbf{a}^m_k \\ \mathbf{b}^m_k \\ \mathbf{p}^m_k \end{pmatrix}$.

▷ State prediction:

$\hat{\mathbf{R}}_{k|k-1} = \hat{\mathbf{R}}_{k-1} \exp_m (\boldsymbol{\omega}^m_{k-1} \Delta t)$

$\hat{\mathbf{v}}_{k|k-1} = \hat{\mathbf{v}}_{k-1} + \hat{\mathbf{R}}_{k-1} \hat{\mathbf{a}}^{ext}_{k-1} \Delta t$

$\hat{\mathbf{p}}_{k|k-1} = \hat{\mathbf{p}}_{k-1} + \hat{\mathbf{v}}_{k-1} \Delta t$

$$\mathbf{A}_{k-1} = \begin{pmatrix} \mathbf{I}_3 & \mathbf{0}_3 & \mathbf{0}_3 \\ -\hat{\mathbf{R}}_{k-1}(\hat{\mathbf{a}}^{ext}_{k-1})_\times \Delta t & \mathbf{I}_3 & \mathbf{0}_3 \\ \mathbf{0}_3 & \mathbf{I}_3 \Delta t & \mathbf{I}_3 \end{pmatrix}, \quad \mathbf{B}_{k-1} = \begin{pmatrix} \mathbf{0}_3 \\ \hat{\mathbf{R}}_{k-1} \Delta t \\ \mathbf{0}_3 \end{pmatrix}, \quad \mathbf{G} = \begin{pmatrix} \mathbf{I}_3 \Delta t \\ \mathbf{0}_3 \\ \mathbf{0}_3 \end{pmatrix},$$

$$\mathbf{P}^{e}_{k|k-1} = \begin{pmatrix} \mathbf{A}_{k-1} & \mathbf{B}_{k-1} \end{pmatrix} \begin{pmatrix} \mathbf{P}^{e}_{k-1} & \mathbf{P}^{ea}_{k-1} \\ \mathbf{P}^{ae}_{k-1} & \mathbf{P}^{a}_{k-1} \end{pmatrix} \begin{pmatrix} \mathbf{A}^T_{k-1} \\ \mathbf{B}^T_{k-1} \end{pmatrix} + \mathbf{G} \boldsymbol{\mathcal{Q}}_{k-1} \mathbf{G}^T$$

▷ External acceleration estimation:

$$\mathbf{H}^{+}_{k} = \begin{pmatrix} (\hat{\mathbf{R}}^T_{k|k-1} \mathbf{g})_\times & \mathbf{0}_3 & \mathbf{0}_3 \\ (\hat{\mathbf{R}}^T_{k|k-1} \mathbf{m}_e)_\times & \mathbf{0}_3 & \mathbf{0}_3 \\ \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{I}_3 \end{pmatrix}$$

$\tilde{\boldsymbol{\mathcal{R}}}_k = \mathbf{H}^{+}_{k} \mathbf{P}^{e}_{k|k-1} \mathbf{H}^{+T}_{k} + \boldsymbol{\mathcal{R}}_k$

$\mathbf{M}_k = \left(\mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \mathbf{D} \right)^{-1} \mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$

$\hat{\mathbf{a}}^{ext}_{k} = \mathbf{M}_k \left(\mathbf{y}_k - \mathbf{h}^{+}(\hat{\mathbf{R}}_{k|k-1}, \hat{\mathbf{p}}_{k|k-1}) \right)$

$\mathbf{P}^{a}_{k} = \left(\mathbf{D}^T \tilde{\boldsymbol{\mathcal{R}}}_k^{-1} \mathbf{D} \right)^{-1}$

▷ Correction:

$\mathbf{K}_k = \mathbf{P}^{e}_{k|k-1} \mathbf{H}^{+T}_{k} \tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$

$\boldsymbol{\delta}_k = \mathbf{K}_k \left(\mathbf{y}_k - \mathbf{h}^{+}(\hat{\mathbf{R}}_{k|k-1}, \mathbf{p}_{k|k-1}) - \mathbf{D} \hat{\mathbf{a}}^{ext}_{k} \right)$

$\hat{\mathbf{R}}_k = \hat{\mathbf{R}}_{k|k-1} \exp_m (\boldsymbol{\delta}_k(1:3))$

$\hat{\mathbf{v}}_k = \hat{\mathbf{v}}_{k|k-1} + \boldsymbol{\delta}_k(4:6)$

$\hat{\mathbf{p}}_k = \hat{\mathbf{p}}_{k|k-1} + \boldsymbol{\delta}_k(7:9)$

$\mathbf{P}^{ea}_{k} = -\mathbf{P}^{e}_{k|k-1} \mathbf{H}^{+T}_{k} \mathbf{M}^T_k$

$\mathbf{P}^{e}_{k} = \mathbf{P}^{e}_{k|k-1} - \mathbf{K}_k \left(\mathbf{I}_9 - \mathbf{D}\mathbf{M}_k \right) \mathbf{H}^{+}_{k} \mathbf{P}^{e}_{k|k-1}$

return $\hat{\mathbf{R}}_k$, $\hat{\mathbf{v}}_k$, $\hat{\mathbf{p}}_k$, $\hat{\mathbf{a}}^{ext}_{k}$, $\mathbf{P}^{e}_{k}$, $\mathbf{P}^{a}_{k}$, $\mathbf{P}^{ea}_{k}$

4.3. Evaluation of PVA-SO(3)

This section aims to validate the effectiveness and demonstrate the performance of the proposed algorithm under different scenarios. Monte Carlo simulations are carried out with 100 runs for each scenario. The performance of the proposed algorithm is compared with two reference algorithms, which are briefly described below. The simulation setup and the corresponding results are then presented.

When showing the results, and in order to facilitate the interpretation of the results, the rotation matrices are converted into Euler angles using the XYZ convention and expressed in degrees. RMSE is calculated for each Monte Carlo run, and finally, the average is derived from the 100 runs.

Comparison Algorithms

PVA-SO(3) is compared with two algorithms, both based on cascaded approaches [191]. First, the attitude is estimated using MARG sensors, then, it is used to compute the external acceleration based on the accelerometer measurement model (1.5.2). This computed acceleration serves as an input to a Kalman filter applied to the velocity and position dynamics (4.1.1)-(4.1.2), with position measurements as the output (4.1.3).

The first algorithm uses IEKF-SO(3), explained in Section 1.7, for attitude estimation, assuming that the accelerometer measures only gravity, ignoring external acceleration. The second uses IEKF-SO(3) combined with a threshold-based adaptive method [146], which adjusts the measurement noise covariance matrix. Specifically, when external acceleration is detected, a higher acceleration measurement noise covariance matrix is assigned, reducing the algorithm's reliance on accelerometer measurements. External acceleration is detected when the difference between the norm of the accelerometer output and the gravity norm exceeds a threshold ϵ_a. We set $\epsilon_a = 0.2$ m/s^2 following [146]. In the remainder of this chapter, we refer to these two algorithms as cascaded-IEKF and cascaded-IEKF with adaptation, respectively.

Simulation Setup

For every Monte Carlo run, the simulated data are generated for a duration of 100 s with a sampling time of $\Delta t = 0.01$ s. The Earth's gravity vector and the Earth's magnetic field are approximated by these two vectors written in NED (North-East-Down) frame in Grenoble, France: $\mathbf{g} = \begin{pmatrix} 0 & 0 & 9.81 \end{pmatrix}^T$ m/s^2 and $\mathbf{m}_e = \begin{pmatrix} 0.23 & 0.01 & 0.41 \end{pmatrix}^T$ G, respectively. The true values for body angular velocity and external acceleration are set as shown in Table 4.1. The gyroscope, accelerometer, magnetometer, and position noises are set as zero-mean white Gaussian signals with standard deviations of $\sigma_\omega = 0.01$ rad/s, $\sigma_a = 0.01$ m/s^2, $\sigma_m = 0.005$ G, and $\sigma_p = 0.5$ m, respectively.

To ensure a fair comparison, the applied external acceleration shown in Table 4.1 at each time step k is scaled by α_k, which can take 0 (no external acceleration) or 1 (with external acceleration). The sequence $(\alpha_k)_{0\leq k}$ is generated as alternating phases of zeros and ones.

Table 4.1: The true angular velocity and external acceleration

True angular velocity (rad/s)		True external acceleration (m/s^2)	
$\boldsymbol{\omega}_k(1)$	$2.0\cos(0.2\pi k\Delta t)$	$\mathbf{a}_k^{ext}(1)$	$2.0\sin(0.5\pi k\Delta t)\alpha_k$
$\boldsymbol{\omega}_k(2)$	$1.5\cos(0.6\pi k\Delta t)$	$\mathbf{a}_k^{ext}(2)$	$1.0\sin(0.2\pi k\Delta t)\alpha_k$
$\boldsymbol{\omega}_k(3)$	$1.0\cos(1.0\pi k\Delta t)$	$\mathbf{a}_k^{ext}(3)$	$0.5\sin(0.1\pi k\Delta t)\alpha_k$

Each phase is generated to have a random duration following a uniform distribution in the range $[0, 1-\bar{\alpha}]$ seconds for the zero phase, and $[0, \bar{\alpha}]$ seconds for the one phase. The closer $\bar{\alpha}$ is to 1, the more external acceleration is present. Conversely, as $\bar{\alpha}$ approaches 0, the presence of external acceleration decreases.

Each Monte Carlo run has a different noise sequence and different initial estimates for position and velocity. The measurement noise realizations are generated independently, meaning that each simulation has its own unique set of noise values, distinct from those of other runs, with common noise variances. The initial attitude estimates for all three algorithms are obtained using a slightly perturbed rotation estimate, computed via the static attitude algorithm TRIAD, explained in Section 1.6, based on the first accelerometer and magnetometer readings. The initial velocity and position estimates are set as uniform distributions in the ranges $[-10, 10]$ m/s and $[-100, 100]$ m for each component, respectively.

Simulation Results

Table 4.2 presents the RMSE of position, velocity, attitude, and external acceleration estimation, for the three algorithms across three scenarios of external acceleration presence, corresponding to $\bar{\alpha} = 1$, $\bar{\alpha} = 0.6$, and $\bar{\alpha} = 0.3$. In all scenarios, PVA-SO(3) outperforms the cascaded IEKF with and without adaptation and remains unaffected by the presence of external acceleration, unlike the cascaded IEKF approaches. In every scenario, the cascaded-IEKF with adaptation consistently outperforms the cascaded-IEKF without adaptation. This is because the latter relies on unreliable acceleration measurements during the correction step when external acceleration is present, while the former neglects these measurements when detecting external acceleration. On the other hand, PVA-SO(3) demonstrates even better performance than the cascaded-IEKF with adaptation, as it fully exploits all available measurements, even in the presence of external acceleration. Fig. 4.1 and Fig. 4.2 show a comparison of velocity and position estimation, respectively, for a single simulation run, presenting the estimates from the three algorithms and the ground truth. These figures are appropriately zoomed in for better visualization. Both figures are consistent with the RMSE-based comparison shown in Table 4.2. Fig. 4.3 and Fig. 4.4 show the achieved convergence of the position and velocity estimation error for 10 runs when $\bar{\alpha} = 1$, respectively, covering a wide range of initial estimates.

Table 4.2: RMSE for the rotation (in degree), velocity (in m/s), position (in m), and the external acceleration (in m/s^2), for the three algorithms, over three $\bar{\alpha}$ cases.

$\bar{\alpha}$	**State**	**PVA-SO(3)**	**cascaded-IEKF with adaptation**	**cascaded-IEKF**
1.0	Rotation	0.39	7.64	9.90
	Velocity	0.06	1.01	1.82
	Position	0.08	2.55	7.30
	External acceleration	0.02	0.54	0.69
0.6	Rotation	0.39	1.87	6.40
	Velocity	0.06	0.34	1.09
	Position	0.08	1.36	4.30
	External acceleration	0.02	0.20	0.48
0.3	Rotation	0.39	1.15	3.78
	Velocity	0.06	0.17	0.51
	Position	0.08	0.66	2.06
	External acceleration	0.02	0.12	0.28

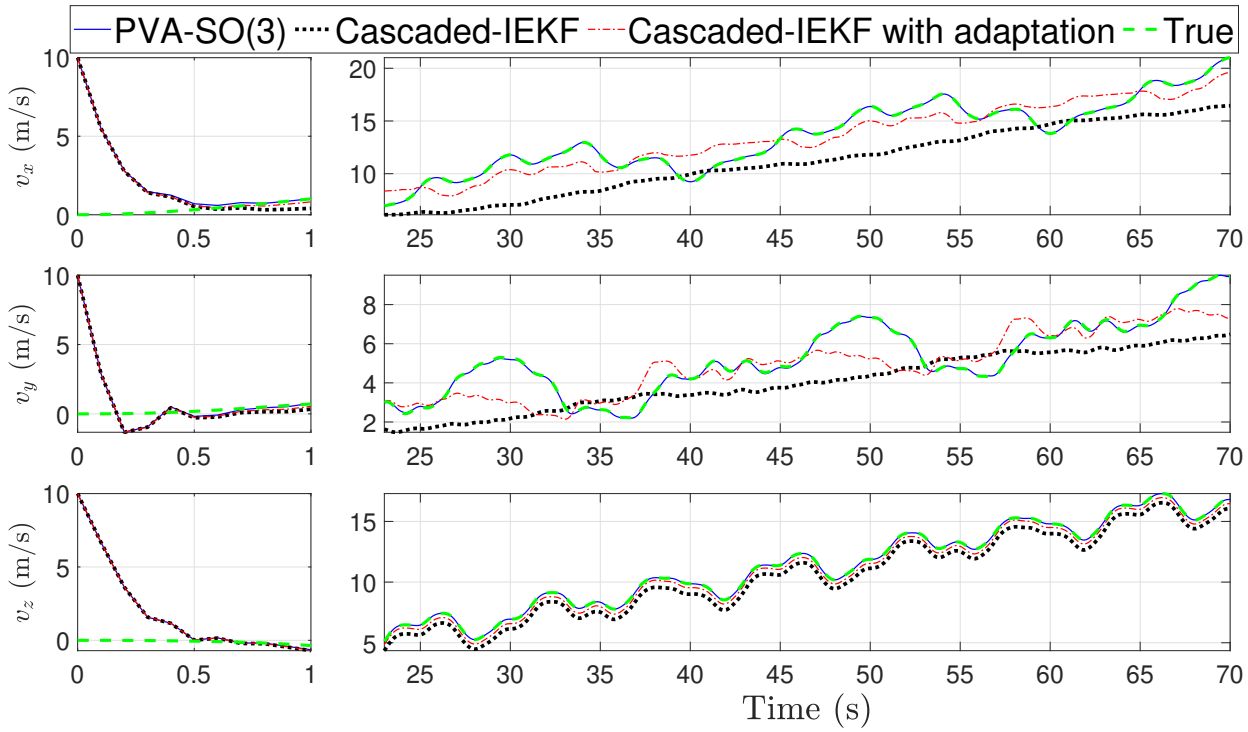

Figure 4.1: Velocity estimation comparison.

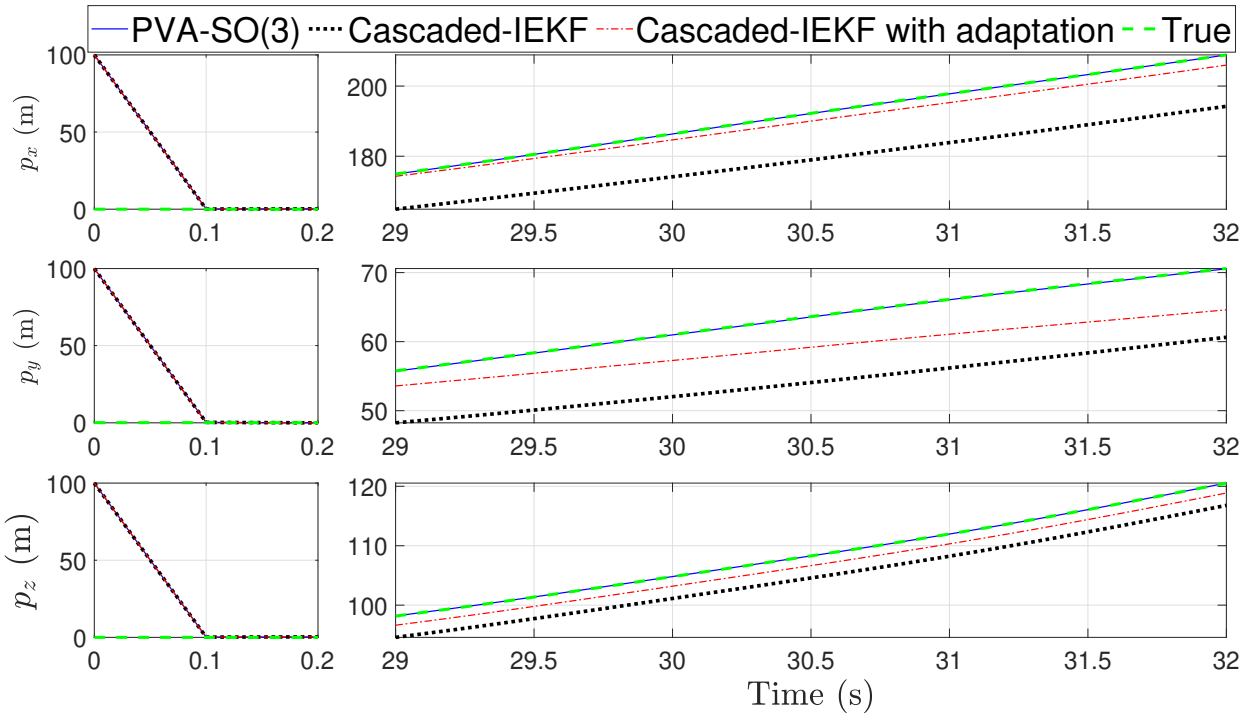

Figure 4.2: Position estimation comparison.

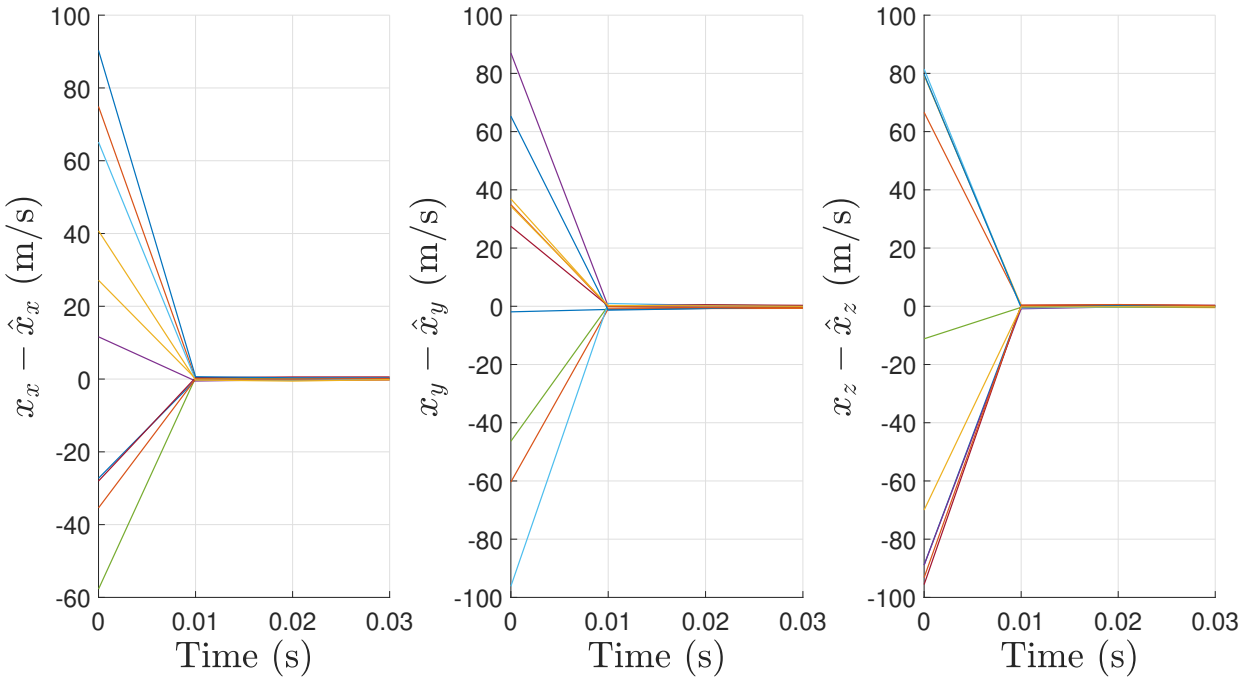

Figure 4.3: Position estimation error for PVA-SO(3), for 10 Monte Carlo runs.

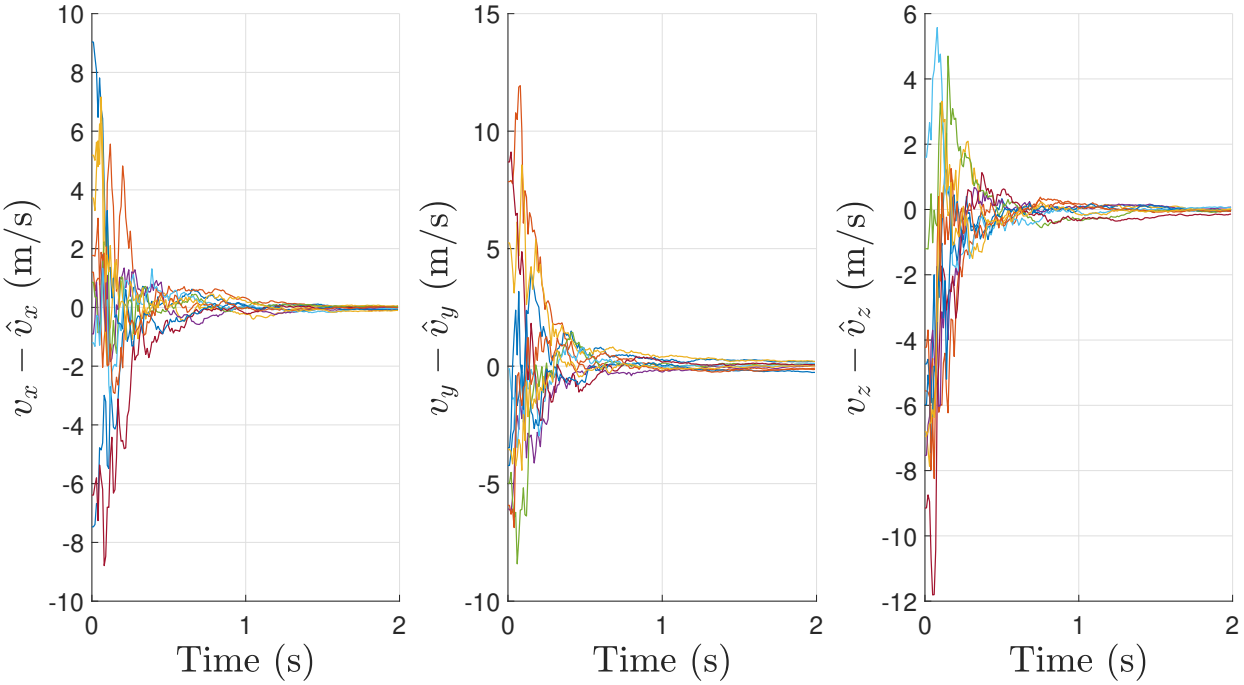

Figure 4.4: Velocity estimation error for PVA-SO(3) for 10 Monte Carlo runs.

4.4. Conclusion

This chapter proposed a novel algorithm, PVA-SO(3), for estimating the position, velocity, and attitude of a rigid body using position and MARG sensor measurements. PVA-SO(3) treats external acceleration, which is measured by the accelerometer along with gravity and appears in the kinematic equation of velocity, as an unknown input affecting both the dynamic model and the output function. The effectiveness of PVA-SO(3) is demonstrated through Monte Carlo simulations and compared with a cascaded approach, where attitude is first estimated using the IEKF-SO(3), and an IEKF-SO(3) integrated with threshold-based adaptation, then used for position and velocity estimation. Simulation results showed that PVA-SO(3) outperforms the cascaded methods.

This part of the thesis consists of three chapters, each addressing the problem of state estimation on SO(3) in the presence of unknown inputs. In Chapter 2, the unknown input affects the dynamic model without direct feedthrough to the output. In Chapter 3, the unknown input affects only the output function. In the current chapter, the unknown input affects both the dynamic model and the output function. Each of these frameworks addresses a practical estimation problem. In the first framework, the unknown input corresponds to the gyroscope measurements, and the proposed solution is applicable when gyroscope measurements are unavailable or unreliable. In the second and third frameworks, the unknown input corresponds to the external acceleration affecting the rigid body.

It is worth noting that MARG sensors can also be subject to other types of unknown inputs, such as cyber-physical attacks. The next part of this thesis focuses on the problem of

cyber-physical security. It begins with the design of an attitude estimation algorithm based on MARG sensor measurements, in the presence of randomly occurring FDI attacks. The objective is to minimize the estimation error under such cyber-physical attacks.

Part II

Cyber-Physical Security for Navigation Applications and Active Defense Strategy

Chapter 5

Introduction

This introductory chapter presents the fundamental categories of cyber-physical attacks and defense strategies, identifies the research gap addressed in this part, and prepares the reader for the problems investigated in the subsequent chapters. It does not aim to provide a comprehensive literature review but rather a focused overview to support the understanding of the problems addressed in this part.

It begins by presenting the main categories of cyber-physical attacks in Section 5.1, followed by an overview of existing defense strategies in Section 5.2. Section 5.3 discusses the vulnerabilities of navigation systems, including ground vehicles and aerial robots, and highlights the importance of securing their estimation and control processes. It also presents two specific problems that will be addressed in this part: one related to the security of attitude estimation, and the other to the protection of vehicle's lateral dynamics. Section 5.4 introduces a different viewpoint on how to defend cyber-physical systems and motivates new directions for protection beyond conventional methods.

5.1. Cyber-Physical Attack Categories

Research in CPS security has primarily focused on four major categories of cyber-physical attacks: denial of service (DoS) attacks, replay attacks, false data injection (FDI) attacks, and eavesdropping attacks.

DoS Attacks

In a DoS attack, the attacker blocks the transmission of input or output signals, disrupting the system's operation [42]. This type of attack assumes that the attacker has the capability to write to the input-output signals transmission lines.

Replay Attacks

In a replay attack, the adversary records a sequence of measurement data and replays it later in place of current measurements [125]. This type of attack is difficult to detect, as the replayed sequence may correspond to a legitimate measurement pattern [57]. This type of attack assumes that the attacker has the capability to read from and write to the input-output signals transmission lines.

FDI Attacks

In an FDI attack, the attacker injects false signals into the input and/or output channels to degrade the control system's performance [33, 126, 127, 137] or to degrade the system's state estimation performance [72, 73].

In the CPS security literature, spoofing and deception attacks are commonly used terms for attacks that are, in essence, FDI attacks, as both involve feeding false information into the system. A spoofing attack typically refers to falsifying the identity of a sensor's data source, leading to incorrect measurements, such as spoofed GPS signals using fake satellites [178], or electromagnetic interference on magnetic sensors [132]. In some literature, the term "deception attack"is used instead of "FDI attack" [72, 137]. However, the term "deception"originates from military studies, where it refers to altered representations of reality [39].

An FDI attack is considered undetectable against a specific detector, where this detector is based on a signal produced by the system, if this signal, in the presence of FDI attacks, is identical to the signal produced in its absence.

Zero dynamics attacks: An undetectable attack is achieved by injecting false data solely into the input channels, where the attacker exploits the invariant zeros of the system to perform attacks leaving no trace on the system's outputs, thus, it is called a zero dynamics attack [138, 139]. This type of attack assumes that the attacker has the capability to write to the input signal transmission lines. Additionally, the attacker is assumed to have knowledge of the system model.

A detailed mathematical formulation of the zero dynamics attack is presented in Section 7.3 of Chapter 7.

Covert attacks: An undetectable attack is achieved in [100, 101] by injecting false data into both inputs and outputs, and known as covert attack [157]. This type of attack assumes that the attacker has the capability to read from and write to the input-output signals transmission lines. Additionally, the attacker is assumed to have knowledge of the system model.

Eavesdropping Attacks

In an eavesdropping attack, the adversary passively accesses communication channels to extract sensitive information without modifying system behavior [34]. Eavesdropping attacks are classified as passive cyber-physical attacks [113, 134], where unauthorized access is obtained without directly affecting the system's functionality.

Cyber-Physical Attack Space

To better understand the resource requirements of the aforementioned attack types, the cyber-physical attack space, introduced in [167], is frequently used in the literature [34, 147, 168]. Figure 5.1 shows the three-dimensional cyber-physical attack space, with the location of each attack type, the three dimensions are:

1. disclosure resources quantify the attacker's access to read the transmitted data,
2. disruption resources quantify the attacker's access to modify the transmitted data,
3. the model knowledge refers to how much the attacker knows about the system model.

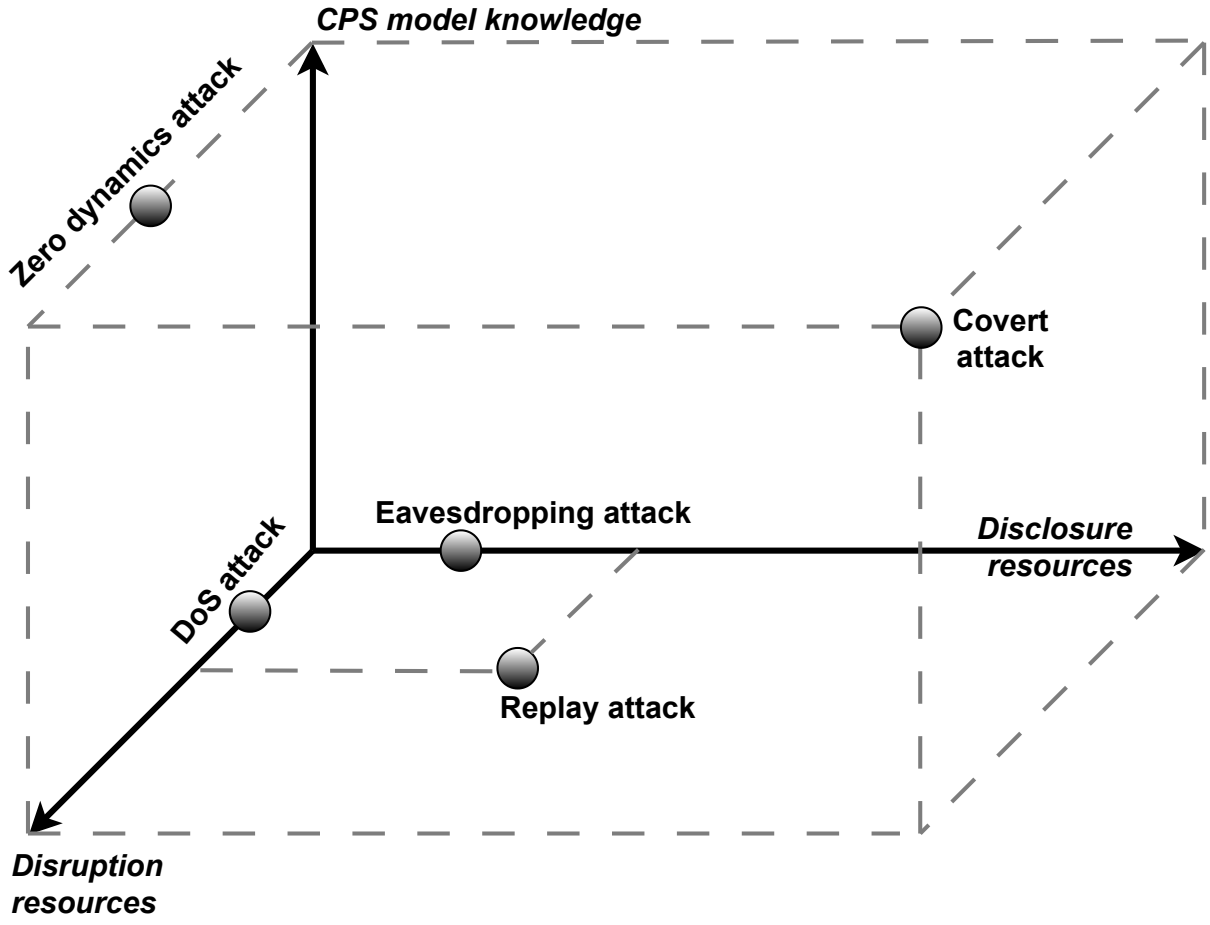

Figure 5.1: The cyber-physical attack space.

5.2. Defense Mechanisms Against Cyber-Physical Attacks

The second major focus in CPS security is the development of defense mechanisms. Defense strategies are commonly categorized into three approaches: prevention, detection, and

resilience [34, 44].

Prevention

Prevention aims to reduce the likelihood of successful attacks by securing communication and access. This includes encryption, firewalls [55, 95, 114], and masking protocols [27, 32].

Detection

Detection involves determining whether an attack has occurred, typically using statistical tests on some resulting signal of the system; examples of these tests are χ^2 [23], cumulative sum [67], and Euclidean detector [119].

Another detection method involves physical watermarking, where known signals are embedded in the data. Any alteration or absence of these signals can indicate an attack [128].

Resilience

Resilience refers to the system's ability to continue functioning correctly under attack, particularly in terms of secure control and state estimation. Various approaches have been proposed in the literature.

For example, under observability conditions and bounds on the number of compromised sensors, secure state estimation can be achieved through majority voting among a bank of observers [35, 180, 181]. Other methods solve optimization problems to minimize the total residuals from each sensor [56, 155].

Remote state estimation in the presence of randomly occurring FDI attacks, modeled by Bernoulli distributions, has also been studied. These approaches aim to maintain bounded estimation errors and minimize these bounds [105, 109].

Several techniques have been proposed in the literature to defend against passive eavesdroppers. These methods aim to degrade the estimation performance of the eavesdroppers, while still allowing the legitimate estimator to maintain acceptable performance. One strategy is transmission scheduling and data omission, where the sensor intentionally withholds some transmissions [104]. Another approach is to inject randomness or dummy data into the transmissions [71, 192].

5.3. Cyber-Physical Security of Navigation Systems

The purpose of this section is to explain how and why navigation systems, specifically in ground vehicles and aerial robots, are vulnerable to cyber-physical attacks. It then presents relevant studies on securing such systems and finally introduces two specific problems that remain unexplored, which will be addressed in Chapter 6 and Chapter 7.

Navigation systems rely heavily on the integrity of both sensor measurements and control commands, as these signals are fundamental to state estimation and closed-loop control.

This tight integration makes them vulnerable to cyber-physical attacks. In practical scenarios, attackers may compromise communication channels that transmit sensor or actuator data [91], leading to degraded system performance or unsafe behavior. Furthermore, sensor failures may mimic the behavior of randomly occurring FDI attacks, leading to estimation errors or control instability.

Additionally, inertial and magnetic sensors, which are essential for navigation in both ground vehicles and aerial robots, are vulnerable to several types of cyber-physical attacks. In acoustic attacks, the attacker emits sound waves near the sensor's resonant frequency to distort its readings without physical contact. This method has been used to disrupt gyroscope and accelerometer measurements, leading to drone crashes and hijacked motion in ground platforms [159, 173]. Electromagnetic interference (EMI) attacks, which introduce malicious electromagnetic signals, have been shown to corrupt IMU outputs and significantly degrade UAV navigation performance [17]. In addition, deep learning-based stealthy attacks can generate false IMU values that mimic valid measurements, allowing the system to deviate from its mission objectives without triggering anomaly detectors [98]. Similarly, magnetometers can be spoofed through controlled magnetic fields. In [132], a coil-based attack was designed to manipulate magnetometer readings by injecting artificial magnetic fields, resulting in incorrect heading estimates.

Such vulnerabilities highlight the critical need to secure navigation systems, particularly ground vehicles and aerial robots. Hereafter, relevant studies are presented that address two key challenges in this context: the security of ground vehicles and the secure estimation of attitude, the primary state in navigation systems, particularly in aerial robots.

Secure Attitude Estimation

Limited research has focused on securing attitude estimation against FDI attacks. In [89], a secure attitude estimation method for AVs systems is proposed, which involves preprocessing the compromised measurements prior to their use in attitude estimation. In [107] a secure quaternion estimation is designed, where both the state and measurements are represented as quaternions, and the state dynamics and output functions are linear.

Ground Vehicle Security

Some researchs have already studied securing vehicles against DoS attacks [2], and reply attacks [150]. In [14, 92, 163], the FDI attacks against connected vehicles are studied, where the attacks occur on the transmitted signals between vehicles, rather than within the individual vehicle. In [80, 141, 154], FDI and spoofing attacks against vehicle sensors attacks are studied.

Some attacks specifically target the vehicle's lateral control. The work [106] addresses lateral control for connected vehicles under cyber-physical attacks, where the attack targets sensor measurements and control inputs, utilizing a fuzzy-model-based control approach. Attacks that modify sensor signals to cause damage in the lateral control have been proposed in [54]. In [133], security measures are proposed to protect against attackers who aim to infer the

values of lateral controller gains. In [129, 130], the lateral model is compromised by attacking the braking system and continuously varying the longitudinal slip of the wheels.

Addressing Two Problems in the Security of Navigation Systems

In this part, two specific gaps in the field of cyber-physical security for navigation systems are addressed.

Although the attitude state plays a major role in navigation, and despite the advantages of SO(3) as detailed in Section 1.2, no prior work has addressed secure attitude estimation on SO(3) under FDI attacks. Chapter 6 fills this gap by proposing a secure estimation algorithm that remains resilient when accelerometer and magnetometer measurements are affected by randomly occurring FDI attacks. While this is a specific problem, it is hoped that this work will encourage further research into securing attitude estimation on SO(3).

The second gap concerns the security of ground vehicles. Chapter 7 investigates the vulnerability of the vehicle's lateral dynamics to zero dynamics attacks. Although lateral dynamics are essential for maintaining vehicle stability during maneuvers, their protection against such attacks has not been explored in the literature. This work addresses that gap by analyzing the lateral dynamics model and proposing structural conditions to detect and mitigate potential threats.

5.4. A New Perspective on Defense in CPS

Defense strategies proposed in the CPS literature are passive, aiming to avoid, detect, or reduce the impact of attacks without taking action against the attacker, as discussed in Section 5.2. This thesis proposes an active defense strategy, where the defending system takes an action against the attacker.

Existing studies generally assume that eavesdropping attacks have access to the input-output signals without incorporating knowledge of the system model. However, assuming model knowledge is common in the context of CPS security, such as in the case of FDI attacks [147]. This thesis introduces a new type of attack, referred to as unauthorized observation, in which the attacker observes the input-output signals and has knowledge of the system model.

In Chapter 8, an active defense strategy is developed to mislead the unauthorized observer by modifying the input-output signals in a way that remains undetected by existing detection methods. In this case, the unauthorized observer will believe it is achieving its objective, while in reality it is not. This false confidence may discourage the attacker from improving its strategy, as it believes the mission is already successful. This approach shares conceptual similarities with strategies developed in military deception, where altered representations of reality are used to create a strategic advantage [39]. It is also related to the idea that "*the best defense is a good offense*" [179]. Although such ideas have been widely explored in military and strategic contexts, they remain undeveloped in the field of CPS security. Investigating these concepts introduces new directions for CPS security research. It reflects a shift from traditional passive defense methods toward strategies in which the system can

actively influence, mislead, or counter adversarial actions. This may lead to more defense mechanisms. The proposed framework for active defense is formulated for general discrete-time linear systems, suggesting its applicability beyond navigation-related applications.

Chapter 6

Attitude Estimation Based on MARG Sensor Under Randomly Occurring False Data Injection Attacks

This chapter starts with the introductory Section 6.1, which explains the attitude dynamics on SO(3), the output measurements including the attack term, the attack model, and provides a literature review on how the problem of secure estimation under randomly occurring FDI attacks is addressed in the literature for systems whose state belongs to vector spaces. Section 6.2 and Section 6.3 present the derivation of the proposed secure-IEKF-SO(3) algorithm .Section 6.4 evaluates the proposed algorithm through simulations. Finally, Section 6.5 concludes the chapter and prepares the reader for Chapter 7. [1]

6.1. Preliminaries and Problem Statement

This chapter addresses the problem of attitude estimation based on MARG sensors when the accelerometer and magnetometer are subject to randomly occurring FDI attacks. This chapter assumes the absence of external acceleration. The attitude dynamic model (1.5.6), along with the corresponding output consisting of the accelerometer measurements (1.5.2) (neglecting external acceleration) and the magnetometer measurements (1.5.3), are briefly recalled below, with the addition of a cyber-physical attack term:

$$\mathbf{R}_{k+1} = \mathbf{R}_k \exp_m \left((\boldsymbol{\omega}_k^m - \mathbf{w}_k^\omega) \Delta t \right), \tag{6.1.1}$$

$$\mathbf{y}_k = \mathbf{h}(\mathbf{R}_k) + \mathbf{w}_k^y + \gamma_k \boldsymbol{\delta}_k, \tag{6.1.2}$$

where $\mathbf{R}_k \in \mathrm{SO}(3)$ denotes the rotation matrix at time step k, $\boldsymbol{\omega}_k^m \in \mathbb{R}^3$ is the measured angular velocity, and $\mathbf{w}_k^\omega \in \mathbb{R}^3$ represents the gyroscope noise. The output measurement function $\mathbf{h}(.)$ and the output noise $\mathbf{w}_k^y$ are given by:

[1] Before reading this chapter, it is recommended to first read Chapter 1 and Chapter 5.

$$\mathbf{h}(\mathbf{R}) = \begin{pmatrix} \mathbf{R}^T\mathbf{g} \\ \mathbf{R}^T\mathbf{m}_e \end{pmatrix}, \qquad \mathbf{w}_k^y = \begin{pmatrix} \mathbf{w}_k^a \\ \mathbf{w}_k^b \end{pmatrix}, \tag{6.1.3}$$

where $\mathbf{g} \in \mathbb{R}^3$ is the Earth's gravity vector, $\mathbf{m}_e \in \mathbb{R}^3$ is the Earth's magnetic field, $\mathbf{w}_k^a \in \mathbb{R}^3$ is the accelerometer measurement noise, and $\mathbf{w}_k^b \in \mathbb{R}^3$ is the magnetometer measurement noise. The random variable γ_k takes the value zero in the absence of the attack and one when an attack occurs. The vector $\boldsymbol{\delta}_k \in \mathbb{R}^6$ denotes the unknown false signal injected during the attack; it is assumed to be bounded, and more precisely, there exists a known matrix $\bar{\boldsymbol{\Delta}}$ i.e.

$$\boldsymbol{\delta}_k \boldsymbol{\delta}_k^T \leq \bar{\boldsymbol{\Delta}}. \tag{6.1.4}$$

This is a realistic assumption, as attackers generally aim to remain undetectable; thus, larger false injected signals are more likely to be detected. The process noise $\mathbf{w}_k^\omega$ and the output measurement noise $\mathbf{w}_k^y$ are assumed to be uncorrelated and to have positive definite covariance matrices $\boldsymbol{\mathcal{Q}}_k$ and $\boldsymbol{\mathcal{R}}_k$, respectively. The random variables $\mathbf{w}_k^\omega$, $\mathbf{w}_k^y$ and γ_k are assumed to be uncorrelated.

The design of secure state estimation against randomly occurring FDI attacks, where the occurrence of the attack follows a Bernoulli distribution, has been studied in various works [3, 45, 112, 190]. The Bernoulli distribution is used to describe the occurrence of FDI attacks because, at each time step, the attack may or may not succeed, depending on whether the protection mechanisms effectively block the attack or not. The Bernoulli distribution is characterized by the probability of occurrence, which represents the attack's success rate. This makes it an effective model for capturing the random nature of the attack's occurrence over time. Thus, in this chapter, the random variable γ_k is considered to be independent Bernoulli distributed white sequences taking values in $\{0, 1\}$ with probabilities:

$$\begin{cases} \mathbb{P}(\gamma_k = 1) = \bar{\gamma} \\ \mathbb{P}(\gamma_k = 0) = 1 - \bar{\gamma} \end{cases}$$

where $\bar{\gamma} \in [0, 1]$, and it is assumed to be known.

Secure state estimation against randomly occurring FDI attacks on the output with occurrence represented by Bernoulli distribution is done for linear systems in [105] by modifying the Kalman gain in the Kalman filter taking into account the attack on the output. The gain design in the secure Kalman filter aims to minimize the upper bound of the estimation error second-order moment matrix. Based on the same principle, several works extended to nonlinear systems, e.g. secure-EKF [110, 112], secure-UKF [111], and secure high-degree cubature Kalman filter [190].

Based on the same principle, this chapter proposes a novel Kalman gain design within the IEKF-SO(3) framework, thus, we call it secure-IEKF-SO(3). This algorithm provides an estimation along with an upper bound for the estimation error second-order moment matrix, and this upper bound is locally minimal among filters with the same form of IEKF-SO(3). This chapter first treats the attack signal $\boldsymbol{\delta}_k$ as a deterministic signal, as in the

literature [105, 110, 111, 112, 190], and then develops and discusses the case of a stochastic signal in Section 6.3.

The main contributions of this chapter are:

- Development of a secure state estimation algorithm on SO(3) under randomly occurring FDI attacks on the output,
- Design of a secure MARG sensor-based attitude estimation framework, where accelerometer and magnetometer measurements are affected by randomly occurring FDI attacks.

The material presented in this chapter is based on the corresponding publication:

- *G. Shaaban, H. Fourati, A. Kibangou, and C. Prieur, "Secure MARG sensor-based attitude estimation on SO(3) under randomly occurring false data injection attacks," accepted in the 23rd European Control Conference (ECC), Thessaloniki, Greece 2025.*

6.2. Secure-IEKF-SO(3) Algorithm Derivation

For systems under FDI attacks on the output, with randomly occurring presented by Bernoulli distribution, the works in [105, 110, 112] design secure state estimation algorithms based on modifying the Kalman gain in KF (for linear systems), and EKF and UKF (for nonlinear systems), respectively. The modified Kalman gain is designed to minimize the upper bound of the state estimation error second-order moment matrix.

Based on the same principle, we propose secure-IEKF-SO(3) that gives an estimate of the attitude on SO(3) in the presence of a false injected signal to the output, based on modifying the Kalman gain in the IEKF-SO(3), to minimize the upper bound of the attitude estimation error second-order moment matrix. Secure-IEKF-SO(3) consists of two steps, as in IEKF-SO(3), prediction and correction. The prediction follows the dynamic model with noise set to zero. The correction is applied using the exponential map of the Kalman gain multiplied by the difference between the output and the predicted output. The two steps are as follows:

$$\hat{\mathbf{R}}_{k|k-1} = \hat{\mathbf{R}}_{k-1} \exp_m (\boldsymbol{\omega}_{k-1}^m \Delta t), \tag{6.2.1}$$

$$\hat{\mathbf{R}}_{k} = \hat{\mathbf{R}}_{k|k-1} \exp_m \left(\mathbf{K}_k \left(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) \right) \right), \tag{6.2.2}$$

where $\mathbf{K}_k$ is the Kalman gain.

Main goal: *The objective is to design the Kalman gain $\mathbf{K}_k$ to minimize the upper bound of the estimation error second-order moment matrix, taking into account the randomly occurring FDI attacks on the output.*

The prediction error and the corresponding second-order moment matrix are denoted by $\exp_m(\boldsymbol{\xi}_{k|k-1}) = \hat{\mathbf{R}}_{k|k-1}^{-1}\mathbf{R}_k$ and $\mathbf{P}_{k|k-1}^{\xi} = \mathbf{E}(\boldsymbol{\xi}_{k|k-1}\boldsymbol{\xi}_{k|k-1}^T)$, respectively. Similarly, the estimation error and its corresponding second-order moment matrix are denoted by $\exp_m(\boldsymbol{\xi}_k) =$

$\hat{\mathbf{R}}_k^{-1}\mathbf{R}_k$ and $\mathbf{P}_k^{\xi} = \mathbf{E}(\boldsymbol{\xi}_k\boldsymbol{\xi}_k^T)$, respectively. The following lemma will be used in the derivation of the algorithm.

Lemma 6.2.1. *[112] For any dimension-compatible matrices* $\mathbf{M}, \mathbf{W}$*, and a scalar* $\varepsilon > 0$*, the following inequality holds:*

$$\mathbf{M}\mathbf{W} + \mathbf{W}^\top\mathbf{M}^\top \leq \varepsilon\mathbf{M}\mathbf{M}^\top + \varepsilon^{-1}\mathbf{W}\mathbf{W}^\top$$

In the following, the steps of the algorithm are derived, followed by a summary of the algorithm and a discussion on its parameters.

Prediction:

Employing the attitude dynamic (6.1.1), and the prediction (6.2.1) in the prediction error $\exp_m(\boldsymbol{\xi}_{k|k-1})$ gives:

$$\begin{aligned}\exp_{\mathrm{m}}(\boldsymbol{\xi}_{k|k-1}) =& \exp_{\mathrm{m}}(-\boldsymbol{\omega}_{k-1}^m\Delta t)\hat{\mathbf{R}}_{k-1}^{-1}\mathbf{R}_{k-1}\exp_{\mathrm{m}}\left((\boldsymbol{\omega}_{k-1}^m - \mathbf{w}_{k-1}^{\omega})\Delta t\right),\\ =& \exp_{\mathrm{m}}(-\boldsymbol{\omega}_{k-1}^m\Delta t)\exp_m(\boldsymbol{\xi}_{k-1})\exp_{\mathrm{m}}\left((\boldsymbol{\omega}_{k-1}^m - \mathbf{w}_{k-1}^{\omega})\Delta t\right).\end{aligned}$$

Applying the first-order approximation (1.4.5) gives:

$$\boldsymbol{\xi}_{k|k-1} = \boldsymbol{\xi}_{k-1} - \mathbf{w}_{k-1}^{\omega}\Delta t. \tag{6.2.3}$$

Then the prediction error second-order moment matrix is

$$\mathbf{P}_{k|k-1}^{\xi} = \mathbf{E}(\boldsymbol{\xi}_{k|k-1}\boldsymbol{\xi}_{k|k-1}^T) = \mathbf{P}_{k-1}^{\xi} + \Delta t^2\boldsymbol{\mathcal{Q}}_{k-1}.$$

The prediction error second-order moment matrix in the previous time step is upper bounded by $\boldsymbol{\Pi}_{k-1}$, i.e. $\mathbf{P}_{k-1}^{\xi} \leq \boldsymbol{\Pi}_{k-1}$, thus $\mathbf{P}_{k|k-1}^{\xi} \leq \boldsymbol{\Pi}_{k-1} + \Delta t^2\boldsymbol{\mathcal{Q}}_{k-1}$, and the upper bound of the prediction error second-order moment matrix is given by:

$$\boldsymbol{\Pi}_{k|k-1} = \boldsymbol{\Pi}_{k-1} + \Delta t^2\boldsymbol{\mathcal{Q}}_{k-1}. \tag{6.2.4}$$

Correction:

The estimation error is given by $\exp_m(\boldsymbol{\xi}_k) = \hat{\mathbf{R}}_k^{-1}\mathbf{R}_k$, employing the correction equation (6.2.2) gives:

$$\begin{aligned}\exp_m(\boldsymbol{\xi}_k) =& \exp_m(-\mathbf{K}_k(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1})))\hat{\mathbf{R}}_{k|k-1}^{-1}\mathbf{R}_k,\\ =& \exp_m(-\mathbf{K}_k(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1})))\exp_m(\boldsymbol{\xi}_{k|k-1}).\end{aligned}$$

Applying first-order approximation (1.4.5) gives:

$$\begin{aligned}\boldsymbol{\xi}_k &= -\mathbf{K}_k\left(\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1})\right) + \boldsymbol{\xi}_{k|k-1},\\ &= -\mathbf{K}_k\left(\mathbf{h}(\mathbf{R}_k) - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) + \gamma_k\boldsymbol{\delta}_k + \mathbf{w}_k^y\right) + \boldsymbol{\xi}_{k|k-1}.\end{aligned} \tag{6.2.5}$$

Note that applying (1.4.5) relies on the assumption that the vector $\mathbf{y}_k - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1})$ is sufficiently small. Although this condition is not theoretically guaranteed at all time steps due to the potential presence of cyber-physical attacks, simulation results indicate that the approximation remains valid and leads to accurate estimation performance in practice.

Applying the first order approximation $\mathbf{h}(\hat{\mathbf{R}}_{k|k-1}\exp_m(\boldsymbol{\xi}_{k|k-1})) - \mathbf{h}(\hat{\mathbf{R}}_{k|k-1}) = \mathbf{H}_k\boldsymbol{\xi}_{k|k-1} + \mathcal{O}(\boldsymbol{\xi}^2_{k|k-1})$ (see Lemma 1.7.1) gives:

$$\begin{aligned}\boldsymbol{\xi}_k &= -\mathbf{K}_k\left(\mathbf{H}_k\boldsymbol{\xi}_{k|k-1} + \gamma_k\boldsymbol{\delta}_k + \mathbf{w}^y_k\right) + \boldsymbol{\xi}_{k|k-1},\\ &= \left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\boldsymbol{\xi}_{k|k-1} - \gamma_k\mathbf{K}_k\boldsymbol{\delta}_k - \mathbf{K}_k\mathbf{w}^y_k,\end{aligned} \tag{6.2.6}$$

where $\mathbf{H}_k = \begin{pmatrix}(\hat{\mathbf{R}}^T_{k|k-1}\mathbf{g})_\times\\ (\hat{\mathbf{R}}^T_{k|k-1}\mathbf{m}_e)_\times\end{pmatrix}$. Now, we calculate $\mathbf{P}^\xi_k = \mathbf{E}(\boldsymbol{\xi}_k\boldsymbol{\xi}^T_k)$:

$$\begin{aligned}\mathbf{P}^\xi_k =& \left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\mathbf{E}(\boldsymbol{\xi}_{k|k-1}\boldsymbol{\xi}^T_{k|k-1})\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)^T + \mathbf{E}(\gamma^2_k)\mathbf{K}_k\boldsymbol{\delta}_k\boldsymbol{\delta}^T_k\mathbf{K}^T_k + \mathbf{K}_k\mathbf{E}(\mathbf{w}^y_k\mathbf{w}^{yT}_k)\mathbf{K}^T_k\\ &- \mathbf{E}(\gamma_k)\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\mathbf{E}(\boldsymbol{\xi}_{k|k-1})\boldsymbol{\delta}^T_k\mathbf{K}^T_k - \mathbf{E}(\gamma_k)\mathbf{K}_k\boldsymbol{\delta}_k\mathbf{E}(\boldsymbol{\xi}^T_{k|k-1})\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)^T\\ &- \left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\mathbf{E}(\boldsymbol{\xi}_{k|k-1})\mathbf{E}(\mathbf{w}^{yT}_k)\mathbf{K}^T_k - \mathbf{K}_k\mathbf{E}(\mathbf{w}^y_k)\mathbf{E}(\boldsymbol{\xi}^T_{k|k-1})\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)^T\\ &+ \mathbf{E}(\gamma_k)\mathbf{K}_k\boldsymbol{\delta}_k\mathbf{E}(\mathbf{w}^{yT}_k)\mathbf{K}^T_k + \mathbf{E}(\gamma_k)\mathbf{K}_k\mathbf{E}(\mathbf{w}^y_k)\boldsymbol{\delta}^T_k\mathbf{K}^T_k,\end{aligned} \tag{6.2.7}$$

employing $\mathbf{P}^\xi_{k|k-1} = \mathbf{E}(\boldsymbol{\xi}_{k|k-1}\boldsymbol{\xi}^T_{k|k-1})$, $\mathbf{E}(\mathbf{w}^y_k) = \mathbf{0}$, $\mathbf{E}(\mathbf{w}^y_k\mathbf{w}^{yT}_k) = \boldsymbol{\mathcal{R}}_k$, $\mathbf{E}(\gamma_k) = \bar{\gamma}$, $\mathbf{E}(\gamma^2_k) = \bar{\gamma}$ gives:

$$\begin{aligned}\mathbf{P}^\xi_k =& \left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\mathbf{P}^\xi_{k|k-1}\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)^T + \bar{\gamma}\mathbf{K}_k\boldsymbol{\delta}_k\boldsymbol{\delta}^T_k\mathbf{K}^T_k + \mathbf{K}_k\boldsymbol{\mathcal{R}}_k\mathbf{K}^T_k\\ &- \bar{\gamma}\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\mathbf{E}(\boldsymbol{\xi}_{k|k-1})\boldsymbol{\delta}^T_k\mathbf{K}^T_k - \bar{\gamma}\mathbf{K}_k\boldsymbol{\delta}_k\mathbf{E}(\boldsymbol{\xi}^T_{k|k-1})\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)^T.\end{aligned}$$

Applying Lemma 6.2.1 on $-\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\mathbf{E}(\boldsymbol{\xi}_{k|k-1})$ and $\mathbf{K}_k\boldsymbol{\delta}_k$, and applying these properties $\boldsymbol{\delta}_k\boldsymbol{\delta}^T_k \leq \bar{\boldsymbol{\Delta}}$, $\mathbf{E}^2(.) \leq \mathbf{E}(.^2)$, and $\mathbf{P}^\xi_{k|k-1} \leq \boldsymbol{\Pi}_{k|k-1}$ give:

$$\mathbf{P}^\xi_k \leq \boldsymbol{\Pi}_k = (1+\bar{\gamma}\epsilon)\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\boldsymbol{\Pi}_{k|k-1}\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)^T + (\epsilon^{-1}+1)\bar{\gamma}\mathbf{K}_k\bar{\boldsymbol{\Delta}}\mathbf{K}^T_k + \mathbf{K}_k\boldsymbol{\mathcal{R}}_k\mathbf{K}^T_k, \tag{6.2.8}$$

we rearrange it for easier trace derivation later:

$$\begin{aligned}\boldsymbol{\Pi}_k =& \mathbf{K}_k((1+\bar{\gamma}\epsilon)\mathbf{H}_k\boldsymbol{\Pi}_{k|k-1}\mathbf{H}^T_k + (\epsilon^{-1}+1)\bar{\gamma}\bar{\boldsymbol{\Delta}} + \boldsymbol{\mathcal{R}}_k)\mathbf{K}^T_k\\ &- (1+\bar{\gamma}\epsilon)\mathbf{K}_k\mathbf{H}_k\boldsymbol{\Pi}_{k|k-1}\\ &- (1+\bar{\gamma}\epsilon)\boldsymbol{\Pi}_{k|k-1}\mathbf{H}^T_k\mathbf{K}^T_k\\ &+ (1+\bar{\gamma}\epsilon)\boldsymbol{\Pi}_{k|k-1}.\end{aligned} \tag{6.2.9}$$

In order to minimize the trace of $\boldsymbol{\Pi}_k$, we find $\mathbf{K}_k$ that satisfies $\frac{\partial tr(\boldsymbol{\Pi}_k)}{\partial \mathbf{K}_k} = \mathbf{0}$. Utilizing the matrix derivatives from [12] (Propositions 10.7.2 and 10.7.4), leads to $\frac{\partial tr(\boldsymbol{\Pi}_k)}{\partial \mathbf{K}_k} =$

$2\mathbf{K}_k\left((1+\bar{\gamma}\epsilon)\mathbf{H}_k\mathbf{\Pi}_{k|k-1}\mathbf{H}_k^T+(\epsilon^{-1}+1)\bar{\gamma}\bar{\mathbf{\Delta}}+\boldsymbol{\mathcal{R}}_k\right)-2(1+\bar{\gamma}\epsilon)\mathbf{\Pi}_{k|k-1}\mathbf{H}_k^T$, thus the following gain minimizes the trace of $\mathbf{\Pi}_k$:

$$\mathbf{K}_k=(1+\bar{\gamma}\epsilon)\,\mathbf{\Pi}_{k|k-1}\mathbf{H}_k^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}, \tag{6.2.10}$$

where

$$\tilde{\boldsymbol{\mathcal{R}}}_k=(1+\bar{\gamma}\epsilon)\,\mathbf{H}_k\mathbf{\Pi}_{k|k-1}\mathbf{H}_k^T+\bar{\gamma}(\epsilon^{-1}+1)\bar{\mathbf{\Delta}}+\boldsymbol{\mathcal{R}}_k. \tag{6.2.11}$$

By applying this gain in (6.2.9), we obtain:

$$\mathbf{\Pi}_k=(1+\bar{\gamma}\epsilon)\,(\mathbf{I}-\mathbf{K}_k\mathbf{H}_k)\,\mathbf{\Pi}_{k|k-1}. \tag{6.2.12}$$

Secure-IEKF-SO(3) Algorithm Summary

The inputs of the Secure-IEKF-SO(3) algorithm are the previously estimated attitude and the upper bound of its estimation error second-order moment matrix, together with the MARG sensor measurements. The algorithm provides, as outputs, the estimated attitude along with the upper bound of the corresponding estimation error second-order moment matrix. The detailed steps of the proposed recursive filter Secure-IEKF-SO(3) are summarized in Algorithm 7.

Algorithm 7 Secure-IEKF-SO(3)

Input: $\hat{\mathbf{R}}_{k-1}$, $\mathbf{\Pi}_{k-1}$, $\boldsymbol{\omega}_{k-1}^m$, $\mathbf{y}_k=\begin{pmatrix}\mathbf{a}_k^m\\ \mathbf{b}_k^m\end{pmatrix}$

▷ Prediction:

1: $\hat{\mathbf{R}}_{k|k-1}=\hat{\mathbf{R}}_{k-1}\exp_m(\boldsymbol{\omega}_{k-1}^m\Delta t)$

2: $\mathbf{\Pi}_{k|k-1}=\mathbf{\Pi}_{k-1}+\Delta t^2\boldsymbol{\mathcal{Q}}_{k-1}$

▷ Correction:

3: $\mathbf{H}_k=\begin{pmatrix}(\hat{\mathbf{R}}_{k|k-1}^{-1}\mathbf{g})_\times\\ (\hat{\mathbf{R}}_{k|k-1}^{-1}\mathbf{m}_e)_\times\end{pmatrix}$

4: $\tilde{\boldsymbol{\mathcal{R}}}_k=(1+\bar{\gamma}\epsilon)\,\mathbf{H}_k\mathbf{\Pi}_{k|k-1}\mathbf{H}_k^T+\bar{\gamma}(\epsilon^{-1}+1)\bar{\mathbf{\Delta}}+\boldsymbol{\mathcal{R}}_k$

5: $\mathbf{K}_k=(1+\bar{\gamma}\epsilon)\,\mathbf{\Pi}_{k|k-1}\mathbf{H}_k^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}$

6: $\hat{\mathbf{R}}_k=\hat{\mathbf{R}}_{k|k-1}\exp_m\left(\mathbf{K}_k\left(\mathbf{y}_k-\mathbf{h}(\hat{\mathbf{R}}_{k|k-1})\right)\right)$

7: $\mathbf{\Pi}_k=(1+\bar{\gamma}\epsilon)\,(\mathbf{I}-\mathbf{K}_k\mathbf{H}_k)\,\mathbf{\Pi}_{k|k-1}$

8: **return** $\hat{\mathbf{R}}_k$, $\mathbf{\Pi}_k$

Remark 6.2.2. *The steps of Secure-IEKF-SO(3), presented in Algorithm 7, are identical to those of IEKF-SO(3), presented in Algorithm 2, except for Steps 4, 5, and 7. When $\bar{\gamma}=0$, i.e., when there is no attack on the output, Algorithm 7 becomes identical to Algorithm 2.*

Discussion on Filter Parameters:

Selection of ϵ: According to Lemma 6.2.1, any real positive value greater than zero can be chosen for ϵ. However, in practice, selecting a very large or very small value for ϵ may

degrade estimation performance. Therefore, this parameter serves as a tunable parameter of the algorithm.

The effect of $\bar{\boldsymbol{\Delta}}$: Increasing $\bar{\boldsymbol{\Delta}}$ leads to increasing $\tilde{\boldsymbol{\mathcal{R}}}_k$, and thus decreasing $\mathbf{K}_k$, giving less weight to the correction step. This result is expected, because increasing the upper bound of the false injected signal to the output makes the output unreliable, and making the estimator depends less on the output to perform the correction.

Remark 6.2.3. *The upper bound on the false data injected term is assumed to be known; however, in practice, this may be unknown and is therefore treated as a tuning parameter. From Step 4 of Algorithm 7, increasing $\bar{\boldsymbol{\Delta}}$ beyond the smallest value that still upper-bounds the signal increases the innovation second-order moment matrix $\tilde{\boldsymbol{\mathcal{R}}}_k$. As a result, the algorithm relies less on the output when it could actually make more use of it, thus depending less on the correction step and giving more weight to the prediction. On the other hand, choosing a smaller value decreases $\tilde{\boldsymbol{\mathcal{R}}}_k$ and causes the algorithm to depend more on the correction step, which also means relying more on attacked measurements. Therefore, selecting $\bar{\boldsymbol{\Delta}}$ in the algorithm is critical and should be tuned carefully so that it is neither much higher nor much lower than the actual upper bound of the attack signal.*

6.3. Secure Estimation Under Stochastic Signal Injection

The injection attack signal $\boldsymbol{\delta}_k$ is considered to be deterministic in the algorithm derivation in Section 6.2, and this signal is bounded, i.e., $\boldsymbol{\delta}_k\boldsymbol{\delta}_k^T \leq \bar{\boldsymbol{\Delta}}$. This could be unrealistic in practice, as a deterministic attack signal can be detected through a spectrum analysis of the output signal if the defending system has access to the spectrum of the benign signals. In such a case, any extra components that appear in the spectrum could indicate the presence of the deterministic attack. Therefore, it is important to also consider the case where the attack signals are stochastic.

In this section, the injection signal $\boldsymbol{\delta}_k$ is considered to be a stochastic signal, defined as a white random variable with known second-order moment, i.e., the injection signal energy

$$\mathbf{E}(\boldsymbol{\delta}_k\boldsymbol{\delta}_k^T) = \bar{\bar{\boldsymbol{\Delta}}}.$$

We consider that the injection signal $\boldsymbol{\delta}_k$ is independent of the variable γ_k, and of the process and measurement noises. We start the derivation from the estimation error (6.2.6):

$$\boldsymbol{\xi}_k = (\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k)\,\boldsymbol{\xi}_{k|k-1} - \gamma_k\mathbf{K}_k\boldsymbol{\delta}_k - \mathbf{K}_k\mathbf{w}_k^y,$$

We calculate $\mathbf{P}_k^{\xi} = \mathbf{E}(\boldsymbol{\xi}_k\boldsymbol{\xi}_k^T)$:

$$\begin{aligned}\mathbf{P}_k^{\xi} = {} & (\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k)\,\mathbf{E}(\boldsymbol{\xi}_{k|k-1}\boldsymbol{\xi}_{k|k-1}^T)\,(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k)^T + \mathbf{E}(\gamma_k^2)\mathbf{K}_k\mathbf{E}(\boldsymbol{\delta}_k\boldsymbol{\delta}_k^T)\mathbf{K}_k^T + \mathbf{K}_k\mathbf{E}(\mathbf{w}_k^y\mathbf{w}_k^{yT})\mathbf{K}_k^T \\ & - \mathbf{E}(\gamma_k)\,(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k)\,\mathbf{E}(\boldsymbol{\xi}_{k|k-1})\mathbf{E}(\boldsymbol{\delta}_k^T)\mathbf{K}_k^T - \mathbf{E}(\gamma_k)\mathbf{K}_k\mathbf{E}(\boldsymbol{\delta}_k)\mathbf{E}(\boldsymbol{\xi}_{k|k-1}^T)\,(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k)^T \\ & - (\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k)\,\mathbf{E}(\boldsymbol{\xi}_{k|k-1})\mathbf{E}(\mathbf{w}_k^{yT})\mathbf{K}_k^T - \mathbf{K}_k\mathbf{E}(\mathbf{w}_k^y)\mathbf{E}(\boldsymbol{\xi}_{k|k-1}^T)\,(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k)^T \\ & + \mathbf{E}(\gamma_k)\mathbf{K}_k\mathbf{E}(\boldsymbol{\delta}_k)\mathbf{E}(\mathbf{w}_k^{yT})\mathbf{K}_k^T + \mathbf{E}(\gamma_k)\mathbf{K}_k\mathbf{E}(\mathbf{w}_k^y)\mathbf{E}(\boldsymbol{\delta}_k^T)\mathbf{K}_k^T,\end{aligned}$$

Employing $\mathbf{P}^{\xi}_{k|k-1} = \mathbf{E}(\boldsymbol{\xi}_{k|k-1}\boldsymbol{\xi}^T_{k|k-1})$, $\mathbf{E}(\mathbf{w}^y_k) = \mathbf{0}$, $\mathbf{E}(\mathbf{w}^y_k \mathbf{w}^{yT}_k) = \boldsymbol{\mathcal{R}}_k$, $\mathbf{E}(\gamma_k) = \bar{\gamma}$, $\mathbf{E}(\gamma^2_k) = \bar{\gamma}$, and $\mathbf{E}(\boldsymbol{\delta}_k \boldsymbol{\delta}^T_k) = \bar{\bar{\boldsymbol{\Delta}}}$ gives:

$$\begin{aligned}\mathbf{P}^{\xi}_k = &\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\mathbf{P}^{\xi}_{k|k-1}\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)^T + \bar{\gamma}\mathbf{K}_k\bar{\bar{\boldsymbol{\Delta}}}\mathbf{K}^T_k + \mathbf{K}_k\boldsymbol{\mathcal{R}}_k\mathbf{K}^T_k \\ &- \bar{\gamma}\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\mathbf{E}(\boldsymbol{\xi}_{k|k-1})\mathbf{E}(\boldsymbol{\delta}_k)^T\mathbf{K}^T_k - \bar{\gamma}\mathbf{K}_k\mathbf{E}(\boldsymbol{\delta}_k)\mathbf{E}(\boldsymbol{\xi}^T_{k|k-1})\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)^T. \quad (6.3.1)\end{aligned}$$

Applying Lemma 6.2.1 on $-\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\mathbf{E}(\boldsymbol{\xi}_{k|k-1})$ and $\mathbf{K}_k\mathbf{E}(\boldsymbol{\delta}_k)$, and applying the properties $\mathbf{E}^2(.) \leq \mathbf{E}(.^2)$ and $\mathbf{P}^{\xi}_{k|k-1} \leq \boldsymbol{\Pi}_{k|k-1}$ gives:

$$\mathbf{P}^{\xi}_k \leq \boldsymbol{\Pi}_k = (1+\bar{\gamma}\epsilon)\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)\boldsymbol{\Pi}_{k|k-1}\left(\mathbf{I}_3 - \mathbf{K}_k\mathbf{H}_k\right)^T + (\epsilon^{-1}+1)\bar{\gamma}\mathbf{K}_k\bar{\boldsymbol{\Delta}}\mathbf{K}^T_k + \mathbf{K}_k\boldsymbol{\mathcal{R}}_k\mathbf{K}^T_k, \quad (6.3.2)$$

Which is similar to (6.2.8), with $\bar{\boldsymbol{\Delta}}$ replaced by $\bar{\bar{\boldsymbol{\Delta}}}$. Thus, the remaining derivation follows the same steps as in the deterministic case, and Algorithm 7 is also valid for the stochastic attack signal, where the second-order moment (i.e., signal energy) is used instead of the upper bound required in the deterministic case.

Remark 6.3.1. *In this section, it is considered that there is no knowledge of the first-order moment (mean) of the attack signal. If the mean is known, the upper bound term in the algorithm derivation can be minimized by incorporating the mean, instead of upper-bounding the square of its expectation by the expectation of its square. More specifically, in the derivation steps after (6.3.1), this part of the derivation is omitted.*

6.4. Evaluation of Secure-IEKF-SO(3)

This section aims to validate the effectiveness and demonstrate the performance of the proposed algorithm. Monte Carlo simulations are carried out with 100 runs. The performance of the proposed algorithm is compared with IEKF-SO(3), explained in Section 1.7, which does not consider the attack.

When showing the results, and to facilitate interpretation, the rotation matrices are converted into Euler angles using the XYZ convention and expressed in degrees. RMSE is calculated for each Monte Carlo run, and finally, the average is derived from the 100 runs.

Simulation Setup

For every Monte Carlo run, the simulated data are generated for a duration of 100 s with a sampling time of $\Delta t = 0.01$ s. The Earth's gravity vector and the Earth's magnetic field are approximated by these two vectors written in NED (North-East-Down) frame in Grenoble, France: $\mathbf{g} = \begin{pmatrix}0 & 0 & 9.81\end{pmatrix}^T$ m/s^2 and $\mathbf{m}_e = \begin{pmatrix}0.23 & 0.01 & 0.41\end{pmatrix}^T$ G, respectively. The true value of the body's angular velocity is

$$\boldsymbol{\omega}_k = \begin{pmatrix}0.8\cos\left(1.2\Delta t k\right) & -1.1\cos\left(0.5\Delta t k\right) & -0.4\cos\left(0.3\Delta t k\right)\end{pmatrix}^T.$$

The gyroscope, accelerometer, and magnetometer noises were set to be zero-mean white Gaussian noise signals with standard deviations of $\sigma_\omega = 0.05$ rad/s, $\sigma_a = 0.1\text{m/s}^2$, and $\sigma_m = 0.01$ G, respectively. The false data injected signal is set to $\boldsymbol{\delta}_k = \sin(t)\boldsymbol{\delta}_{max}$, where $\boldsymbol{\delta}_{max} = \begin{pmatrix} 3 & 3 & 3 & 0.2 & 0.2 & 0.2 \end{pmatrix}^T$. Inspired by [112], we set $\epsilon = 0.001$. The initial true rotation matrix was set to correspond to $[45°, 45°, 45°]$ in terms of Euler angles, while the initial estimation error second-order moment matrix is set to the all-ones matrix, respectively.

For each Monte Carlo run, the initial attitude estimate is randomly generated, with roll and yaw uniformly sampled from $[-180°, 180°]$, and pitch from $[-90°, 90°]$, covering the full range of possible rotations [58]. Additionally, each run has different noise sequences for sensor measurements and different Bernoulli sequences for the attack occurrence. All runs share the same measurement noise standard deviation and attack success rate.

Secure-IEKF-SO(3) Theoretical Estimation Results

In this subsection, simulation results are presented for the case $\bar{\gamma} = 0.7$, based on a single run with an initial estimated rotation matrix corresponding to Euler angles $[-45°, -20°, -15°]$. Fig. 6.1 plots the estimation error accuracy obtained with the proposed algorithm, showing how the estimation error converges. After convergence, the error is less than 0.5 degrees for each Euler angle, for most of the time. To validate the upper bound of the estimation error second-order moment matrix, which applies to the estimation error on SO(3) mapped to vector space, we calculate the estimation error in this mapped space and plot it alongside the ± 3 times the standard deviation, derived from the diagonal of the upper bound second-order moment matrix. The ± 3 times the standard deviation contains 95% of the signal for a Gaussian distribution, though it is important to note that, due to first-order approximation, the resulting estimation error is not Gaussian. Fig. 6.2 shows that the ± 3 times the standard deviation bounds the estimation error.

6.4.1 Comparison with IEKF-SO(3)

Table 6.1 shows the RMSE of the proposed secure-IEKF-SO(3) and IEKF-SO(3) for several scenarios of $\bar{\gamma}$. Both algorithms give the same accuracy when $\bar{\gamma} = 0$ because the secure-IEKF-

Table 6.1: RMSE (in degrees) for Secure-IEKF-SO(3) and IEKF-SO(3)

$\bar{\gamma}$	**Secure-IEKF-SO(3)** RMSE (degrees)	**IEKF-SO(3)** RMSE (degrees)
0	0.228	0.228
0.5	0.255	8.68
0.7	0.259	12.4

SO(3) algorithm is identical to IEKF-SO(3) when $\bar{\gamma} = 0$, as discussed in the previous section. As $\bar{\gamma}$ increases, the estimation performance of the IEKF-SO(3) degrades because it treats

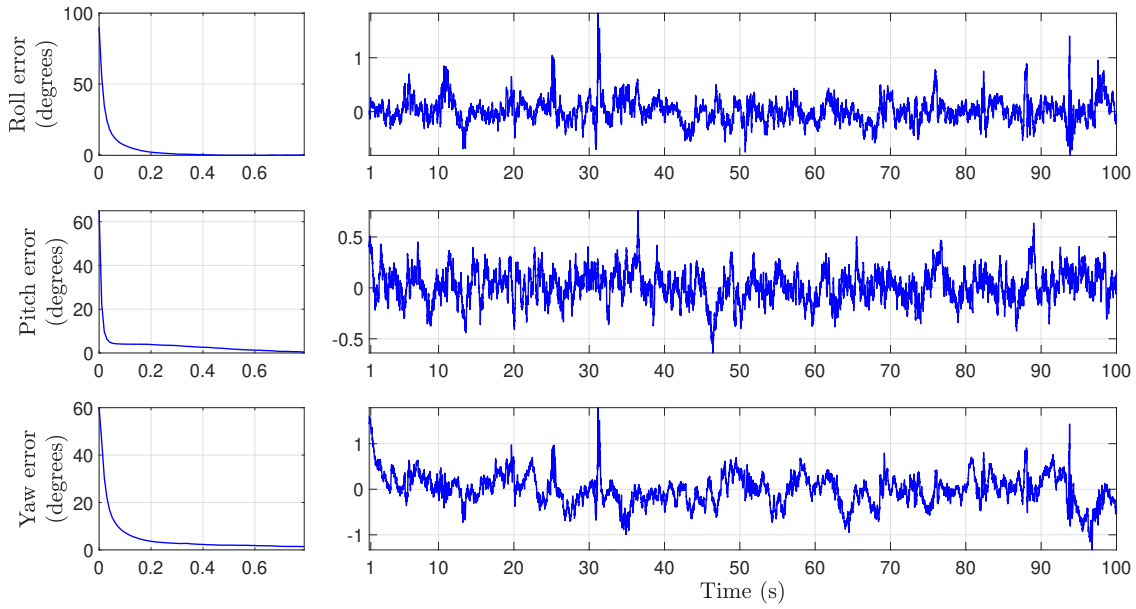

Figure 6.1: Secure-IEKF-SO(3) attitude estimation error

the measurements as benign, whereas the secure-IEKF-SO(3)'s estimation performance is not affected much, as it takes into account the possibility of attacks and their characteristics ($\bar{\gamma}$ and its upper bound).

6.5. Conclusion

This chapter presented a secure attitude estimation approach on SO(3) based on MARG measurements, where the accelerometer and magnetometer sensors are subject to randomly occurring FDI attacks characterized by a Bernoulli distribution. The proposed algorithm, secure-IEKF-SO(3), was designed with a novel Kalman gain of IEKF, with the goal of minimizing the upper bound of the estimation error second-order moment matrix. Simulations demonstrated the algorithm's convergence and effectiveness in attitude estimation, as well as the validation of the upper bound on the estimation error second-order moment matrix. Additionally, Monte Carlo simulations showed that the performance of the standard IEKF-SO(3) degrades as the frequency of randomly occurring FDI attacks increases, while the secure-IEKF-SO(3) remains relatively unaffected.

The FDI attack considered in this chapter targets only the output, specifically the measurements from the three-axis accelerometer and the three-axis magnetometer. An attack on the input, represented by the three-axis gyroscope measurements, is not considered here. One possible direction for future work is to extend the framework to include FDI attacks on the gyroscope measurements.

This chapter is the first to address secure state estimation on SO(3), with the aim of encouraging further research in this direction, as attitude represents a fundamental state in navigation problems, particularly for aerial robots. The next chapter focuses on another

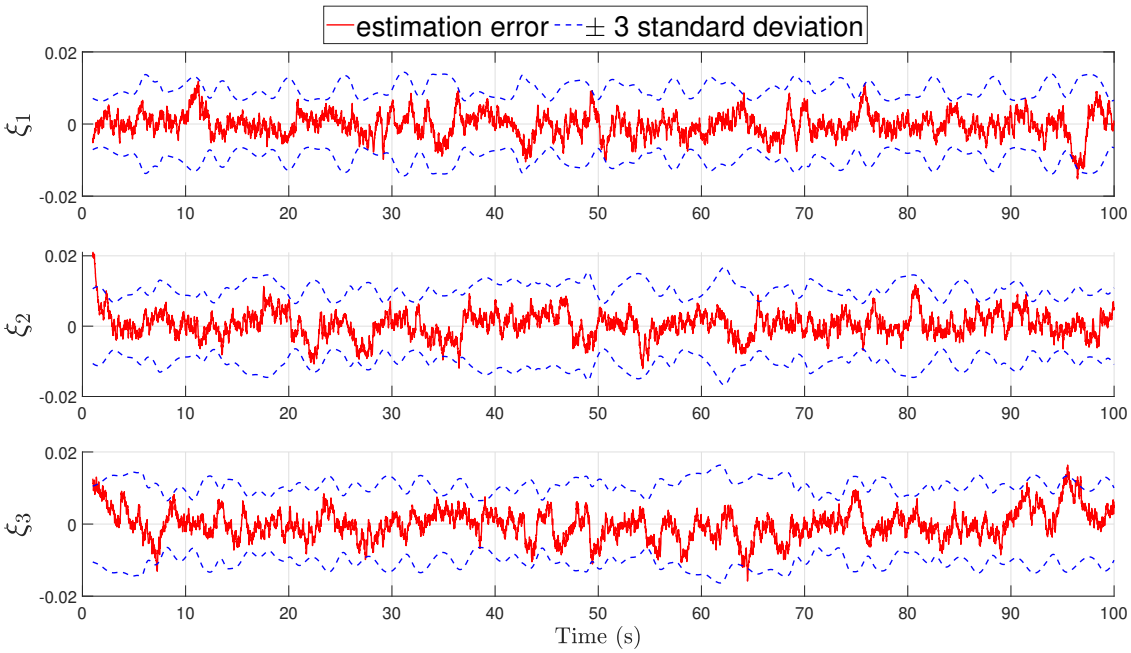

Figure 6.2: Secure-IEKF-SO(3) estimation error on SO(3) mapped to vector space alongside the ± 3 times the standard deviation.

important navigation application, namely ground vehicles. It presents a security analysis of the lateral dynamics of ground vehicles under zero dynamics attacks.

Chapter 7

Zero Dynamics Attacks Against Vehicle's Lateral Dynamics

This chapter starts with the introductory Section 7.1, which explains the importance of the vehicle lateral dynamics, and introduces the problem addressed in this chapter. Section 7.2 explains the vehicle's linear lateral model. Section 7.3 explains the zero dynamics attacks. Section 7.4 studies and analyzes the zero dynamics attacks against the vehicle's lateral dynamics and provides suggestions for securing systems against such attacks. Section 7.5 illustrates the findings through simulations. Section 7.6 concludes the chapter and prepares the reader for Chapter 8. [1]

7.1. Introduction

Fundamental vehicle dynamics are the lateral dynamics, which describe the vehicle's lateral movement. These dynamics have been widely studied in academic and industrial domains [64, 143]. Lateral dynamics involve the lateral velocity and yaw rate dynamics, with two inputs: the steering angle, which is an input by the driver, and the yaw moment, which can be generated by independent in-wheel motors. The yaw moment plays a vital role in enhancing vehicle stability and controllability. The yaw rate can be directly measured by IMU sensors, but lateral velocity lacks direct measurement. Instead, it is estimated based on the dynamic model, inputs and other sensors' measurements, such as yaw rate measurements [97, 131], lateral acceleration measurements [46], or a combination of both [30, 31]. Due to the importance of lateral dynamics, extensive research has focused on control methods [28, 74, 188, 189], as well as on estimation and observation techniques for the lateral model [46, 47, 97, 131].

In this chapter, we study and analyze the invariant zeros of the vehicle's lateral model, and show how the attacker can exploit these zero dynamics to perform undetectable attacks, leaving no trace to the system's outputs, namely lateral acceleration and yaw rate. This

[1] Before reading this chapter, it is recommended to first read Chapter 5.

kind of FDI attack is referred to as a zero dynamics attack, which was defined previously in this part in Section 5.1. We study three cases of output, when the output consists only of yaw rate measurements, when it consists only of lateral acceleration measurements, and when it consists of a combination of both. Additionally, we exploit the relationship between the system's invariant zeros and its strong observability and detectability properties to analyze these characteristics in the lateral dynamics model. Our motivation for this work is not to create zero dynamics attacks but to evaluate vehicle security against them and improve protection measures.

This chapter analyzes the security of the lateral dynamics model under zero dynamics attacks. Since neither the model nor the attack has been formally introduced in this thesis so far, the next two sections provide the necessary background. Section 7.2 presents the linear lateral dynamics model of the vehicle, and Section 7.3 introduces the concept of zero dynamics attacks. The security analysis is then presented in Section 7.4.

The main contributions of this chapter are:

1. **Attacks Design:** Study the existence of invariant zeros of the vehicle's lateral dynamics, design zero dynamics attacks.
2. **Attacks Prevention:** Suggest measures to protect the vehicle's lateral dynamics against zero dynamics attacks.
3. **Observability Under Attacks:** Investigate the strong observability and detectability properties of the lateral dynamics model by examining its invariant zeros.

The material presented in this chapter is based on the corresponding publication:

- *G. Shaaban, H. Fourati, A. Kibangou, C. Prieur, and M. Pirani, "Cyber-physical security of vehicles: Zero dynamics attacks against vehicle's lateral dynamics," European Journal of Control, accepted in July 2025.*

7.2. Vehicle's Linear Lateral Model

The two-degrees-of-freedom *bicycle model* is a widely used approach for analyzing vehicle lateral dynamics, describing the dynamics of lateral velocity, v_y, and yaw rate, $r = \dot{\psi}$ [64, 143], where ψ is the vehicle's yaw (heading) angle. The vehicle's bicycle model with front-wheel steering is shown in Fig. 7.1. The body frame which is attached to the vehicle, has its origin in the vehicle's center of gravity (CG), its x-axis and y-axis are aligned with the longitudinal and lateral axes, respectively. The distances from CG to the front and rear axles are denoted by a and b, respectively. The steering angle, which is a command by the driver is denoted by δ. In addition to the steering angle δ, a control input M_z, representing the yaw moment, is designed to stabilize the lateral motion. The following linear state space model describes the vehicle lateral motion dynamics [64, 143]:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}M_z + \mathbf{B}^{\delta}\delta, \tag{7.2.1}$$

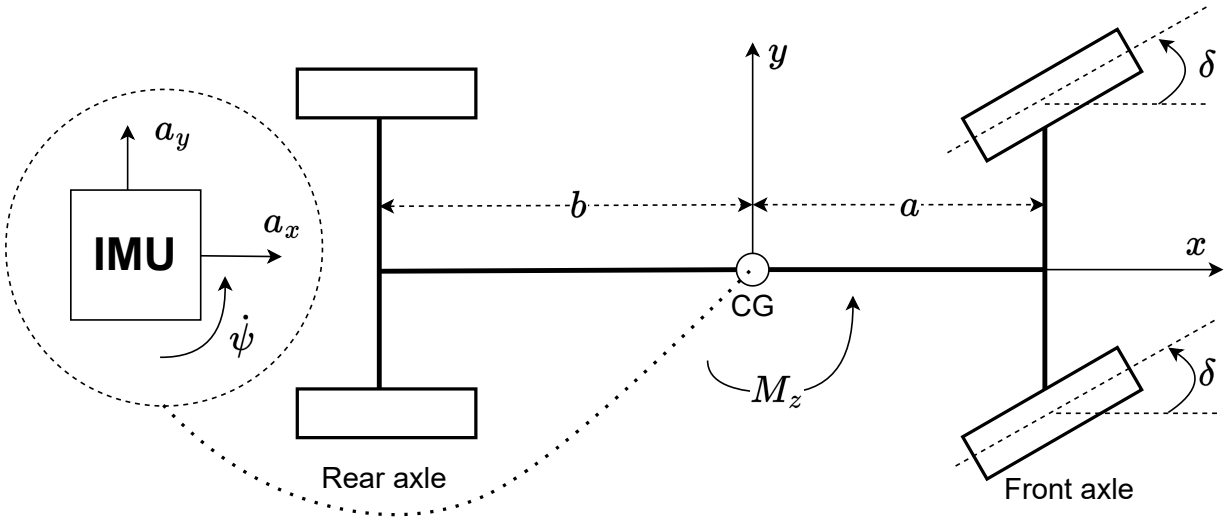

Figure 7.1: Plan view of vehicle dynamics model.

where $\mathbf{x} = (v_y \; r)^T$ is the state vector, and the matrices $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{B}^\delta$ are the state matrix, the input matrix for the yaw moment, and the input matrix for the steering angle, respectively, and have the following forms:

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \; \mathbf{B} = \begin{pmatrix} 0 \\ b_2 \end{pmatrix}, \; \mathbf{B}^\delta = \begin{pmatrix} b_1^\delta \\ b_2^\delta \end{pmatrix}, \tag{7.2.2}$$

and $a_{11} = -2\frac{C_f + C_r}{v_x m}$, $a_{12} = 2\frac{bC_r - aC_f}{v_x m} - v_x$, $a_{21} = 2\frac{bC_r - aC_f}{v_x I_z}$, $a_{22} = -2\frac{a^2 C_f + b^2 C_r}{v_x I_z}$, $b_2 = \frac{1}{I_z}$, $b_1^\delta = \frac{2C_f}{m}$ and $b_2^\delta = \frac{2aC_f}{I_z}$. The parameters C_f, C_r, v_x, m, I_z are the front and rear wheels' cornering stiffness, the vehicle's longitudinal velocity, the vehicle's total mass, and the vehicle's moment of inertia around z-axis, respectively.

Remark 7.2.1. *Although the bicycle model is relatively simple and relies on certain assumptions to yield a linear representation of the system, it effectively captures key lateral vehicle dynamics. Its effectiveness in practical applications validates its use in control design and analysis [64, 143].*

There is no direct measurement of the vehicle's lateral velocity, and it is estimated using the dynamic model (7.2.1) and knowledge of the system inputs M_z and δ, and measurement of yaw rate [97, 131], lateral acceleration [46], or both [30, 31]. These measurements are feasible by using an IMU. We describe hereafter the output model in each case of measurements. The first case concerns yaw rate as output, thus $y_1 = r$, the output matrix is:

$$\mathbf{C}_1 = (0 \; 1)\,. \tag{7.2.3}$$

The second case concerns lateral acceleration as output, thus $y_2 = a_y = \dot{v}_y + v_x r$. From the dynamic model (7.2.1) we have $y_2 = a_{11} v_y + a_{12} r + b_1^\delta \delta + v_x r = \begin{pmatrix} a_{11} & a_{12} + v_x \end{pmatrix} \mathbf{x} + b_1^\delta \delta$, the output matrix is:

$$\mathbf{C}_2 = \begin{pmatrix} a_{11} & a_{12} + v_x \end{pmatrix}. \tag{7.2.4}$$

In the third case, the output consists of the two measurements, and the output model is given by $\mathbf{y}_3 = (r \;\; a_y)^T = \mathbf{C}_3\mathbf{x} + \begin{pmatrix}0 & b_1^\delta\end{pmatrix}^T \delta$, where the output matrix $\mathbf{C}_3$ is:

$$\mathbf{C}_3 = \begin{pmatrix} 0 & 1 \\ a_{11} & a_{12} + v_x \end{pmatrix}. \tag{7.2.5}$$

The following equation summarizes the output model for the three cases of measurements:

$$\mathbf{y}_i = \mathbf{C}_i\mathbf{x} + \mathbf{D}_i^\delta\delta, \tag{7.2.6}$$

where $i \in \{1, 2, 3\}$, $\mathbf{D}_1^\delta = 0$, $\mathbf{D}_2^\delta = b_1^\delta$, and $\mathbf{D}_3^\delta = (0 \;\; b_1^\delta)^T$.

7.3. Zero Dynamics Attacks

This section defines the undetectable attack [138, 139], and its relation with the existence of invariant zeros. It further presents the connection between zero dynamics attacks and strong observability and detectability properties.

Undetectable zero dynamics attacks

We adapt the definition of undetectable attacks which is defined in [138, 139] for the vehicle lateral model. Recalling the linear vehicle lateral dynamics (7.2.1) and the output model (7.2.6):

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{A}\mathbf{x} + \mathbf{B}M_z + \mathbf{B}^\delta\delta, \\ \mathbf{y}_i &= \mathbf{C}_i\mathbf{x} + \mathbf{D}_i^\delta\delta. \end{aligned} \tag{7.3.1}$$

We assume that the attacker injects signal M_z^a to the input M_z, without altering the input δ as it is a mechanical command by the driver.

Definition 7.3.1. *[Undetectable attacks [138, 139]] Consider the linear system (7.3.1), and let $\mathbf{y}_i\left(\mathbf{x}^\alpha(t_0), M_z^a, t\right)$ be the system's output at time $t \geq t_0$, given an initial state $\mathbf{x}^\alpha(t_0)$ and the presence of an injection of attack signal M_z^a, the attacks are considered undetectable if there exists an initial state $\mathbf{x}^\beta(t_0)$ such that*

$$\forall t \geq t_0, \quad \mathbf{y}_i\left(\mathbf{x}^\alpha(t_0), M_z^a, t\right) = \mathbf{y}_i\left(\mathbf{x}^\beta(t_0), 0, t\right).$$

Note that, because of the linearity of (7.3.1), the attack undetectability condition as presented in Definition 7.3.1 is equivalent to finding initial condition $\mathbf{x}(t_0)$ resulting:

$$\forall t \geq t_0, \quad \mathbf{y}_i(\mathbf{x}(t_0), M_z^a, t) = \mathbf{0},$$

specifically $\mathbf{x}(t_0) = \mathbf{x}^\alpha(t_0) - \mathbf{x}^\beta(t_0)$, for the following model:

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{A}\mathbf{x} + \mathbf{B}M_z^a, \\ \mathbf{y}_i &= \mathbf{C}_i\mathbf{x}. \end{aligned} \tag{7.3.2}$$

The resulting dynamics of (7.3.2) after applying the attack signal M_z^a, which makes the output equal to zero, is called zero dynamics, and the attack signal is called zero dynamics attacks. By applying Laplace transformation on (7.3.2) and setting the output to zero, we get:

$$\begin{aligned} s\mathbf{x} &= \mathbf{A}\mathbf{x} + \mathbf{B}M_z^a, \\ \mathbf{0} &= \mathbf{C}_i\mathbf{x}, \end{aligned}$$

thus:

$$\begin{pmatrix} s\mathbf{I} - \mathbf{A} & -\mathbf{B} \\ \mathbf{C} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{x} \\ M_z^a \end{pmatrix} = \mathbf{0}.$$

The matrix $\mathbf{P}(s) = \left(\begin{smallmatrix} s\mathbf{I}-\mathbf{A} & -\mathbf{B} \\ \mathbf{C} & \mathbf{0} \end{smallmatrix}\right)$ is called the Rosenbrock matrix associated with the system (7.3.2). The complex values $s_0 \in \mathbb{C}$ satisfying $Rank\left(\mathbf{P}(s_0)\right) < \dim\left(\begin{smallmatrix} \mathbf{x} \\ M_z^a \end{smallmatrix}\right) = 3$ are called invariant zeros. The following lemma presents necessary and sufficient conditions for the existence of zero dynamics for the model (7.3.2).

Lemma 7.3.2. *[139] Consider the linear state space model (7.3.2), the system has zero dynamics if and only if it has invariant zeros, i.e. there exist complex value $s_0 \in \mathbb{C}$ satisfying $Rank\left(\mathbf{P}(s_0)\right) < \dim\left(\begin{smallmatrix} \mathbf{x} \\ M_z^a \end{smallmatrix}\right) = 3$.*

Definition 7.3.3. *[Disruptive zero dynamics attack [153]] The zero dynamics attacks are called disruptive if the associated invariant zero is unstable, i.e. the resulting zero dynamics is unstable.*

Remark 7.3.4. *The undetectable attack defined in Definition 7.3.1 applies to attacks that target the system input, where the attacker aims to remain undetectable by injecting false data into the input (modifying the input), that leaves no trace on the output. However, undetectable modifications on both the input and output channels are defined in the next chapter, Chapter 8, specifically in Definition 8.4.1.*

Connection with strong observability and detectability properties

The existence of invariant zeros is related to the properties of strong observability (see [164, Def. 2.6]) and detectability (see [164, Def. 2.9]) in linear systems, as explained in the following theorem.

Theorem 7.3.5. *[164] A linear dynamic system is strongly observable if and only if it has no invariant zeros, and it is strongly detectable if and only if all its invariant zeros are stable.*

The zero dynamics attacks are injection attacks into the input, and this injection is unknown to the system.

Case 1: If the system is strongly observable, it means that the system can uniquely reconstruct the state based on the output, without having any information about the unknown attack signal. Therefore, the attacker cannot perform zero dynamics attacks on a strongly observable system.

Case 2: If the system is not strongly observable, it means that there can be two different states for the same output, specifically, one state belongs to a system under zero dynamics attacks and one state belongs to an attack-free system. The system which is not strongly observable can be strongly detectable (Case 2.1) or not (Case 2.2).

Case 2.1: If the system is strongly detectable, the attacked system's state will converge to the attack-free system's state over time.

Case 2.2: If the system is not strongly detectable, the attacker can perform zero dynamics attacks that cause the state to diverge while the output is identical to an attack-free system.

7.4. Security Analysis of Zero Dynamics Attacks Against Vehicle's Lateral Dynamics

Main goal: *The objective is to answer the following questions:*

- *Do the linear lateral dynamics have invariant zeros?*
- *How can an attacker exploit these invariant zeros to perform zero dynamics attacks?*
- *Are these attacks disruptive?*

These questions are addressed in Propositions 7.4.1, 7.4.3, and 7.4.6, each considering one of the following output scenarios: yaw rate, lateral acceleration, and their combination. For each scenario, the existence of invariant zeros and the feasibility of zero dynamics attacks are examined, followed by an analysis of the system behavior under attack. Finally, this section proposes countermeasures to protect the vehicle's lateral dynamics from zero dynamics attacks.

Exclusive Yaw Rate Output

Proposition 7.4.1. *Consider the linear state space model (7.3.2), with an output containing only yaw rate, the system has invariant zero $s_0 = a_{11}$, and the zero dynamics attacks $M_z^a = -\frac{a_{21}}{b_2} v_y$ excite this invariant zero, resulting in stable zero dynamics:*

$$\dot{v}_y = a_{11} v_y. \tag{7.4.1}$$

Proof. For the case where the output is only the yaw rate, the output matrix is given by (7.2.3). The Rosenbrock matrix in this case is given by:

$$\begin{pmatrix} s\mathbf{I} - \mathbf{A} & -\mathbf{B} \\ \mathbf{C}_1 & \mathbf{0} \end{pmatrix} = \begin{pmatrix} s - a_{11} & -a_{12} & 0 \\ -a_{21} & s - a_{22} & -b_2 \\ 0 & 1 & 0 \end{pmatrix},$$

which is a square matrix with a determinant of $b_2(s - a_{11})$, thus the Rosenbrock matrix is rank-deficient when $s = a_{11}$. Therefore, $s_0 = a_{11}$ is an invariant zero of the system. Note

that $a_{11} = -2\frac{C_f+C_r}{v_x m}$ is negative and the invariant zero is stable. Now we find the input that excites the zero dynamics, the output is zero for any $t > t_0$, where t_0 is the onset of the attacks, thus $\forall t > t_0$, $r = 0$ and $\dot{r} = 0$. Substituting in the dynamics of (7.3.2) gives:

$$\begin{pmatrix} \dot{v}_y \\ \dot{r} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} v_y \\ r \end{pmatrix} + \begin{pmatrix} 0 \\ b_2 \end{pmatrix} M_z^a,$$
$$\begin{pmatrix} \dot{v}_y \\ 0 \end{pmatrix} = \begin{pmatrix} a_{11} v_y \\ a_{21} v_y + b_2 M_z^a \end{pmatrix},$$

thus the attack signal $M_z^a = -\frac{a_{21}}{b_2} v_y$ excites the invariant zero of the system, and the system dynamics become $\dot{v}_y = a_{11} v_y$. ■

Remark 7.4.2. *The zero dynamics (7.4.1) shows that under zero dynamics attacks, the vehicle experiences lateral sliding without any rotational motion. These zero dynamics are stable dynamics, where the invariant zero a_{11} is stable. Consequently, based on Theorem 7.3.5, the system is not strongly observable but is strongly detectable; this means that although the output remains identically zero, the state is not zero but converges to zero over time. As a result, zero dynamics attacks exist, and these attacks are not disruptive, i.e. the resulting zero dynamics are stable. Although the lateral velocity converges to zero over time, it can still be dangerous for the system to have lateral movement without being observed. For instance, the system may believe that the vehicle is moving forward, while lateral movement is occurring.*

Exclusive Lateral Acceleration Output

Proposition 7.4.3. *Consider the linear state space model (7.3.2), with an output containing only lateral acceleration, the system has invariant zero $s_0 = \frac{a_{11} v_x}{a_{12}+v_x}$, and the zero dynamics attack*

$$M_z^a = -\frac{1}{b_2(a_{12}+v_x)} \left((a_{11}^2 + a_{21}(a_{12}+v_x)) v_y + (a_{11}a_{12} + (a_{12}+v_x)a_{22}) r \right),$$

excites this invariant zero, resulting in the following zero dynamics:

$$\begin{aligned} \dot{v}_y &= \frac{a_{11} v_x}{a_{12}+v_x} v_y = s_0 v_y, \\ \dot{r} &= \frac{a_{11} v_x}{a_{12}+v_x} r = s_0 r, \end{aligned} \tag{7.4.2}$$

which are stable if and only if $aC_f - bC_r < 0$.

Proof. For the case where the output is only the lateral acceleration, the output matrix is given by (7.2.4). The Rosenbrock matrix becomes in this case:

$$\begin{pmatrix} s\mathbf{I} - \mathbf{A} & -\mathbf{B} \\ \mathbf{C}_2 & \mathbf{0} \end{pmatrix} = \begin{pmatrix} s - a_{11} & -a_{12} & 0 \\ -a_{21} & s - a_{22} & -b_2 \\ a_{11} & a_{12} + v_x & 0 \end{pmatrix},$$

which is a square matrix with a determinant of $b_2\left((a_{12}+v_x)s - a_{11}v_x\right)$, thus the Rosenbrock matrix is rank-deficient when $s = \frac{a_{11}v_x}{a_{12}+v_x}$. Therefore, $s_0 = \frac{a_{11}v_x}{a_{12}+v_x}$ is an invariant zero of the system. Substituting $a_{11} = -2\frac{C_f+C_r}{v_x m}$, and $a_{12} = 2\frac{bC_r - aC_f}{v_x m} - v_x$, gives:

$$s_0 = \frac{C_f + C_r}{aC_f - bC_r} v_x. \tag{7.4.3}$$

The sign of s_0, i.e. the stability of the invariant zero, is determined by the sign of the term $aC_f - bC_r$. Generally, the stability of matrix $\mathbf{A}$ does not impose a condition on the sign of this term. The stability condition of the matrix $\mathbf{A}$, ensuring the eigenvalues of $\mathbf{A}$ have negative real parts, is [64, 77]:

$$(a+b)^2 - \frac{m(aC_f - bC_r)}{C_r C_f} v_x^2 > 0. \tag{7.4.4}$$

The term $aC_f - bC_r$ could be positive while the condition (7.4.4) is still satisfied. Now we find the input that excites the zero dynamics, the output (the lateral acceleration) is zero thus $a_y = a_{11}v_y + (a_{12}+v_x)r = 0$, and the initial conditions r_0 and v_{y0} should satisfy $a_{11}v_{y0} + (a_{12}+v_x)r_0 = 0$, and the derivatives $\dot{v}_y$ and $\dot{r}$ should satisfy $a_{11}\dot{v} + (a_{12}+v_x)\dot{r} = 0$, substituting the dynamics $\dot{v}_y$ and $\dot{r}$:

$$a_{11}(a_{11}v_y + a_{12}r) + (a_{12}+v_x)(a_{21}v_y + a_{22}r + b_2 M_z^a) = 0,$$

thus, the attack signal that excites the invariant zero is:

$$M_z^a = -\frac{1}{b_2(a_{12}+v_x)}\left((a_{11}^2 + a_{21}(a_{12}+v_x))v_y + (a_{11}a_{12} + (a_{12}+v_x)a_{22})r\right),$$

and the output is identical to zero $a_{11}v_y + (a_{12}+v_x)r = 0$, thus $r = -\frac{a_{11}v_y}{a_{12}+v_x}$, substituting in the dynamics $\dot{v}_y = a_{11}v_y + a_{12}r$ gives $\dot{v}_y = \frac{a_{11}v_x}{a_{12}+v_x}v_y = s_0 v_y$, thus $\dot{r} = \frac{a_{11}v_x}{a_{12}+v_x}r = s_0 r$, which concludes the proof of the proposition. ■

Fig. 7.2 presents the phase plane illustrating the system's behavior under zero dynamics attacks, the state evolves along the zero-output manifold: 1) The state follows the green dashed line when the attacks target the yaw rate, setting it to zero; the invariant zero is stable, and the state converges to zero. 2) The state follows the blue closed-dots line when the attacks target the lateral acceleration, setting it to zero with a stable invariant zero, leading to convergence. 3) The state follows the red dotted line when the attacks target the lateral acceleration, setting it to zero with an unstable invariant zero, causing the state to diverge.

Remark 7.4.4. *The zero dynamics (7.4.2) show that under zero dynamics attacks, the vehicle experiences lateral and rotational motion. According to Proposition 7.4.3, the invariant zero could be stable or unstable depending on the sign of the term $aC_f - bC_r$. Based on Theorem 7.3.5, the system is not strongly observable, and it could be not strongly detectable if $aC_f - bC_r > 0$, in such case, the state diverges to infinity while the output remains at zero. There are threats associated with zero dynamics attacks, and we impose the condition*

$$aC_f - bC_r < 0 \tag{7.4.5}$$

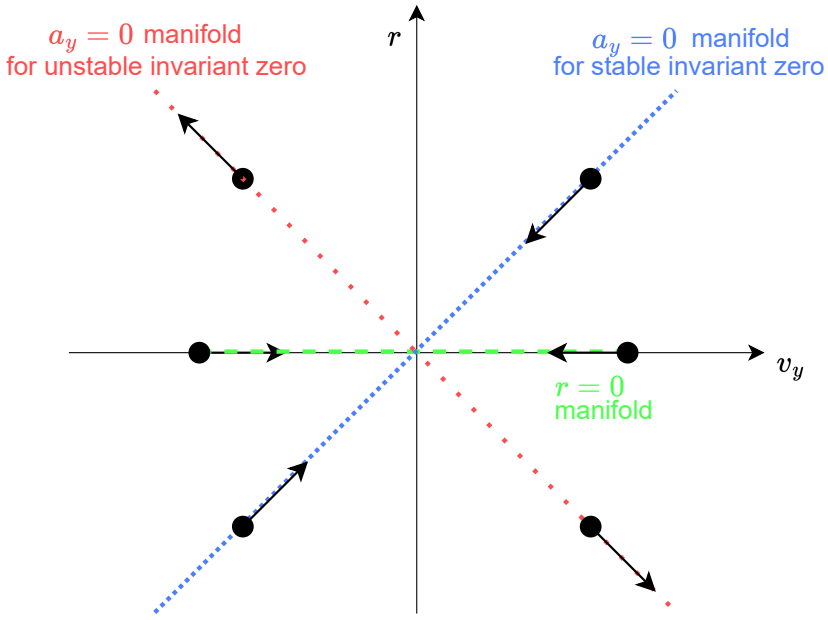

Figure 7.2: System behavior under zero dynamics attacks for three cases: when the output is the yaw rate (the state lies on the green dashed line), when the output is the lateral acceleration with a stable invariant zero (the state lies on the blue closed-dots line), and when the output is the lateral acceleration with an unstable invariant zero (the state lies on the red dotted line).

to prevent them, making the system strongly detectable, and thus ensuring the zero dynamics attacks are not disruptive.

Remark 7.4.5. ***Zero dynamics attacks can be detected using lateral and longitudinal acceleration.*** *The attacker performs zero dynamics attacks making the lateral acceleration (the output) equal to zero, thus* $a_y = a_{11}v_y + (a_{12} + v_x)r = 0$*, while both lateral velocity and yaw rate are nonzero. The longitudinal acceleration,* a_x *is given by* $a_x = \dot{v}_x - v_y r$*, which under the assumption of constant longitudinal velocity becomes* $a_x = -v_y r$*. Note that, for a time window, the longitudinal acceleration can not be equal to zero while both* v_y *and* r *are nonzero. Thus, longitudinal acceleration measurements serve as a detector for zero dynamics attacks that target the lateral acceleration output.*

Output Combines Both Yaw Rate and Lateral Acceleration

Proposition 7.4.6. *Consider the linear state space model (7.3.2), with an output that combines both yaw rate and lateral acceleration, the system has no invariant zeros.*

Proof. For the case where the output includes both yaw rate and lateral acceleration, the

output matrix is given by (7.2.5). The Rosenbrock matrix becomes in this case:

$$\begin{pmatrix} s\mathbf{I}-\mathbf{A} & -\mathbf{B} \\ \mathbf{C}_3 & \mathbf{0} \end{pmatrix} = \begin{pmatrix} s-a_{11} & -a_{12} & 0 \\ -a_{21} & s-a_{22} & -b_2 \\ 0 & 1 & 0 \\ a_{11} & a_{12}+v_x & 0 \end{pmatrix},$$

the three columns of the Rosenbrock matrix are linearly independent regardless of the value of s, thus the matrix has a rank of 3 and the system has no invariant zeros. This can be seen also by trying to set the output to zero:

$$\begin{pmatrix} r \\ a_y \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ a_{11} & a_{12}+v_x \end{pmatrix} \begin{pmatrix} v_y \\ r \end{pmatrix},$$

$$\mathbf{0} = \begin{pmatrix} 0 \\ a_{11}v_y \end{pmatrix},$$

thus, both r and v_y (along with their derivatives) are zero, resulting in no zero dynamics. ■

Remark 7.4.7. *Proposition 7.4.6 indicates that there is no threat of zero dynamics attacks when the output combines both yaw rate and lateral acceleration. Based on Theorem 7.3.5, the system is strongly observable, indicating that the system's states can be fully reconstructed from the output.*

Summary of Findings

When the output consists of yaw rate, the system exhibits a stable invariant zero, allowing the attacker to perform undetectable but non-disruptive attacks. In the case where the output contains lateral acceleration, the system may have a stable or un unstable invariant zero. A new condition (7.4.5) is proposed to ensure a stable invariant zero. When the invariant zero is unstable, the attacker can perform disruptive and undetectable attacks. Also, this paper proposes to measure the longitudinal acceleration and use it as a detector for zero dynamics attacks. Finally, when the output includes both yaw rate and lateral acceleration, the system has no invariant zeros, eliminating the possibility of zero dynamics attacks. This paper recommends using sensors measuring both yaw rate and lateral acceleration to enhance the security of vehicle lateral dynamics against such attacks. Table 7.1 shows summarizes these findings.

Discussion on Model Validity and Attack Objectives

Under normal driving conditions, a vehicle's tire side slip angle, defined as the angle between the tire's orientation and its actual trajectory, remains small. Under this condition, tire lateral forces increase approximately linearly with respect to the tire's side slip angle. This

Table 7.1: Summary of findings. The sign ✓ means the existence, while × means the non-existence

Output measurements	Additional condition	Threat of zero dynamics attack?	Disruptive attack?
r	-	✓	×
a_y	$aC_f - bC_r > 0$	✓	✓
a_y	$aC_f - bC_r < 0$	✓	×
a_y, a_x	-	×	×
r, a_y	-	×	×

linear relationship yields the lateral dynamics model used in this study [64, 143]. The linear tire behaviour holds in the linear region of operation, which corresponds to everyday maneuvers where tire grip is not pushed to its limit. Moreover, it is worth noting that, thanks to modern active safety systems and advanced traction and brake control technologies, vehicles typically operate within the linear force-slip region, rarely reaching tire saturation [64, 143]. This further justifies and motivates the focus on zero dynamics attack analysis within the linear region. Once instability occurs, the abnormal behaviour becomes evident, but the attacker has already succeeded. Using both yaw rate and lateral acceleration measurements ensures strong observability in the linear region, effectively preventing such attacks before instability occurs.

7.5. Illustration of the Analysis Through Simulations

We demonstrate through simulations how zero dynamics attacks can go undetected, leaving no trace in the output. The simulations cover two cases: one where the output is the yaw rate r and another where it is the lateral acceleration a_y, as there is no invariant zero when both outputs are combined. The vehicle's parameters used in these simulations are real parameters belonging to a Sports Utility Vehicle (SUV) [77], as shown in Table 7.2.

Exclusive Yaw Rate Output

Firstly, we consider zero dynamics attacks that aim to maintain r equal to zero, as stated in Proposition 7.4.1. For this simulation, we assume longitudinal velocity v_x is equal to 25 m/s and that the attacks occur at the initial time when lateral velocity v_y is equal to 5 m/s. Fig. 7.3 shows v_y and r for a duration of 1 second. r remains equal to zero while v_y is not. These attacks are undetectable but not disruptive, as v_y converges to zero.

Secondly, we consider zero dynamics attacks that aim to perform undetectable attacks i.e. the output is identical to the output of an attack-free case, while the lateral velocities have different trajectories. For this simulation, we assume $v_x = 25$ m/s for both the attack and

Table 7.2: SUV paremeters

Parameter	Value	Description
m	2270 kg	Vehicle mass
I_z	4600 kg.m^2	Moment of inertia
a	1.421 m	Front axle to CG
b	1.438 m	Rear axle to CG
C_{α_f}	69800 N/rad	Front cornering stiffness
C_{α_r}	69600 N/rad	Rear cornering stiffness

attack-free cases. The attacks occur at the initial time, with the lateral velocity being 5 m/s in the attack case trajectory, and -5 m/s in the attack-free case trajectory. We consider the following steering angle input for both attack and attack-free cases:

$$\delta(t) = \begin{cases} 0 & t <= 0.1, \\ \sin(10t) & t > 0.1. \end{cases}$$

Fig. 7.4 shows the lateral velocity and the yaw rate for a duration of 1 second. Both attack-case trajectory and attack-free case trajectory have the same output, but different lateral velocities, however, the attack-case lateral velocity converges to the attack-free one.

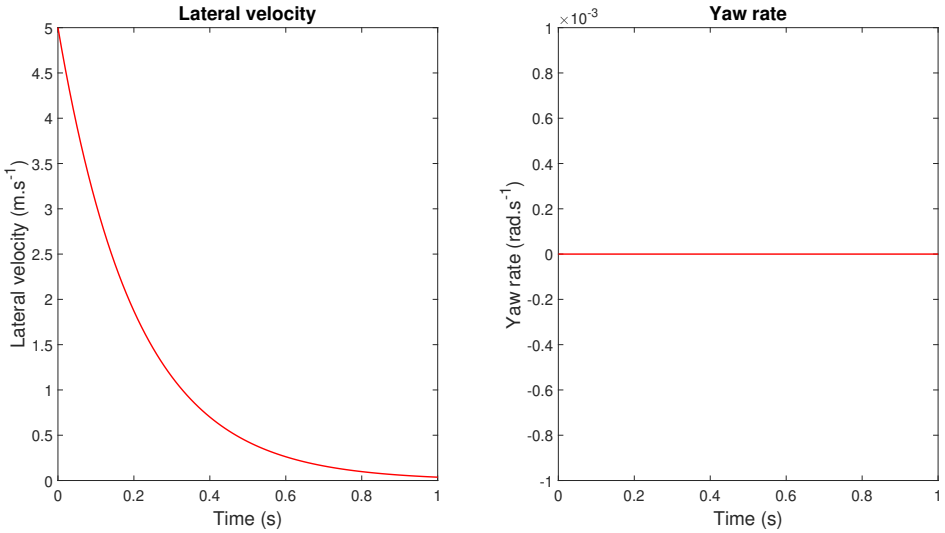

Figure 7.3: Lateral velocity v_y and yaw rate r when the zero dynamics attacks aim to maintain r equal to zero.

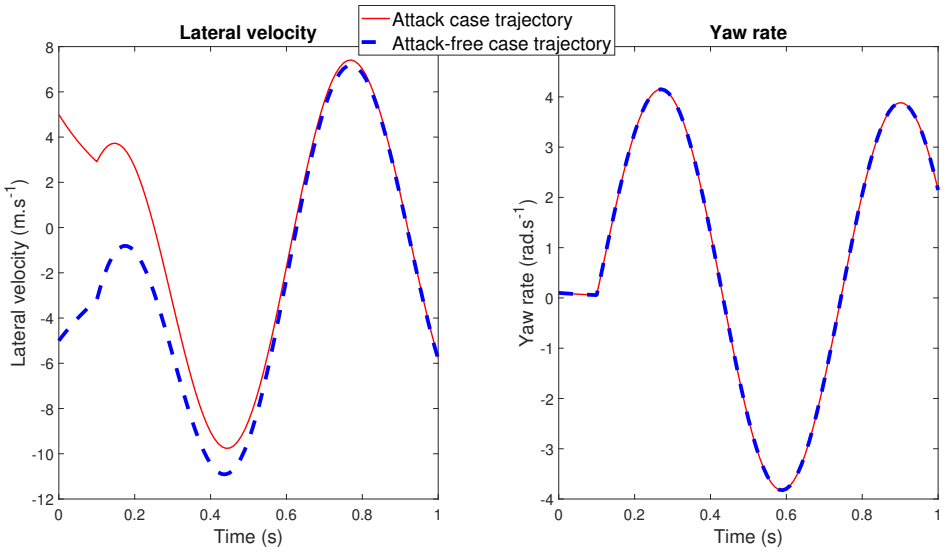

Figure 7.4: Lateral velocity v_y and yaw rate r when the zero dynamics attacks aim to perform undetectable attacks i.e. the output is identical to the one of an attack-free case, while the lateral velocities have different trajectories.

Remark 7.5.1. *Although the attacks are not disruptive, i.e. the lateral velocity is converging, having a lateral movement that is not observed by the system can still be dangerous in practical situations, on the highway for instance.*

Exclusive lateral acceleration output

We consider zero dynamics attacks that aim to maintain a_y equal to zero, as stated in Proposition 7.4.3. The invariant zero, given in (7.4.3) has large value considering the parameters in Table 7.2, thus we consider longitudinal velocity 5 m/s, and the value of the invariant zero, in this case, is $s_0 = -775.3$ 1/s, which is stable and causes the zero dynamics to converge quickly. For this simulation, we assume that the attacks occur at the initial time when the yaw rate is equal to 1 rad/s and the lateral velocity is equal to 6.4×10^{-3} m/s. Fig. 7.5 shows the lateral velocity, yaw rate, and lateral acceleration. The lateral acceleration remains zero while the lateral velocity and yaw rate are not, however, they converge to zero.

Now, we consider a vehicle where the condition (7.4.5) is not satisfied, e.g. the front axle to CG distance is $a = 1.521\ m$, the invariant zero will have the value $s_0 = 114.6$ 1/s, which is unstable; while the eigenvalues of the matrix $\mathbf{A}$, in this case, are $(-23.5, -27.6)$, indicating its stability. Fig. 7.6 shows that the lateral acceleration remains zero, while the lateral velocity and yaw rate diverge. It is important to mention that, the linear model is not guaranteed to be valid when the vehicle enters the unstable mode.

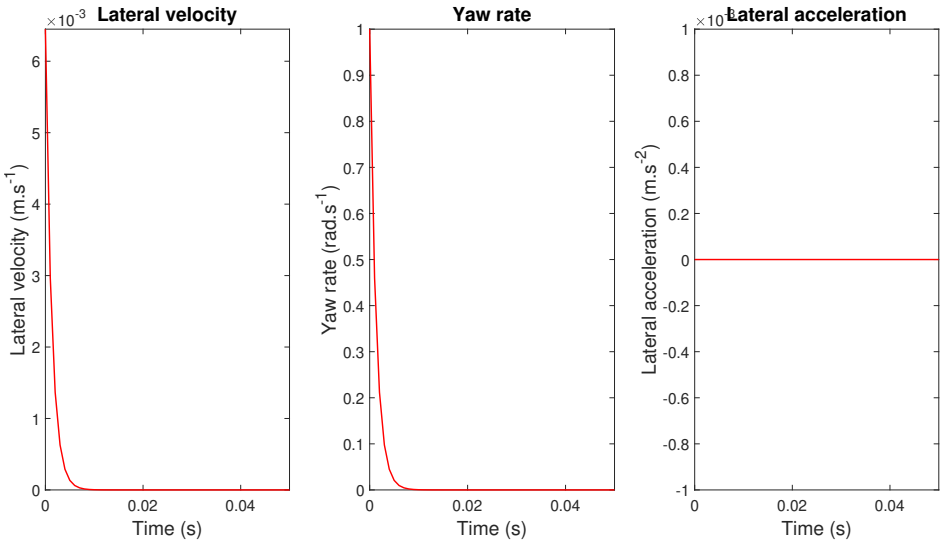

Figure 7.5: Lateral velocity v_y, yaw rate r, and lateral acceleration a_y when the zero dynamics attacks aim to maintain a_y equal to zero, in the case of stable invariant zero.

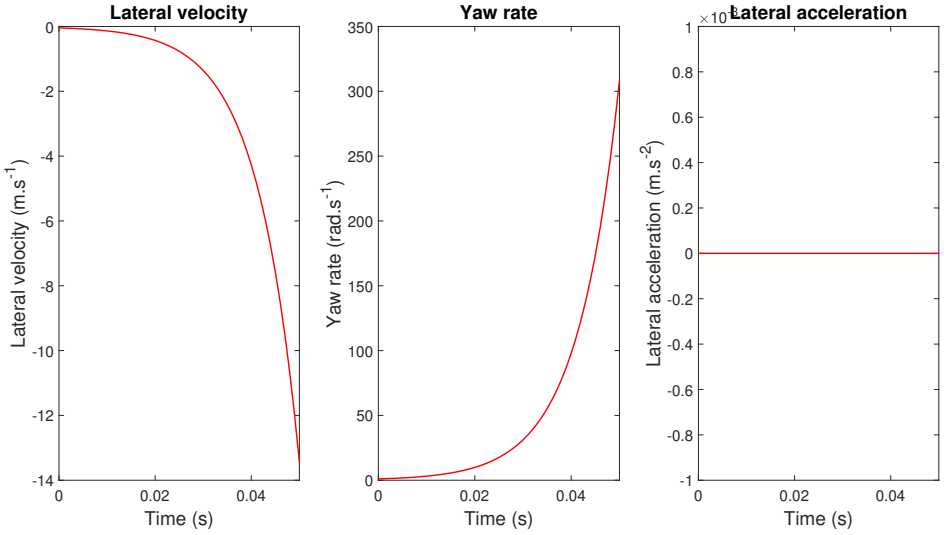

Figure 7.6: Lateral velocity v_y, yaw rate r, and lateral acceleration a_y when the zero dynamics attacks aim to maintain a_y equal to zero, in the case of unstable invariant zero.

7.6. Conclusion

This chapter studied the linear vehicle lateral dynamics and identified the three types of outputs. It demonstrated how zero dynamics attacks can exploit the invariant zeros of a linear system to perform undetectable attacks. For each case of the lateral model output, the system's invariant zeros were studied and analyzed. This chapter recommended that the output consists of both yaw rate and lateral acceleration to prevent zero dynamics attacks, and it recommended using longitudinal acceleration measurements as a detector for zero dynamics attacks when only accelerometers are available.

This chapter and the previous one addressed two different navigation problems under FDI attacks. In the previous chapter, the secure attitude estimation on SO(3) aimed to minimize the estimation error caused by randomly occurring FDI attacks, and thus followed a resilience-based defense strategy. The current chapter recommends that the output include a combination of sensors to prevent zero dynamics attacks, which corresponds to a prevention-based defense strategy. In both chapters, the defense strategies are passive, as is typical of the defense strategies found in the literature. The next chapter introduces a new type of defense strategy, an active defense strategy, targeting unauthorized observation.

Chapter 8

Active Defense Strategy: Misleading Unauthorized Observers

This chapter starts with the introductory Section 8.1, which introduces the unauthorized observer and motivates the problem of misleading such attackers. Section 8.2 explains the system model and the legitimate observer. Section 8.3 mathematically defines the unauthorized observer and locates it among other types of attacks. Section 8.4 defines the MUO strategy mathematically. Section 8.5 provides the structure of the two possible scenarios in which the proposed MUO can effectively defend against an unauthorized observer. Section 8.6 presents conditions under which the misleading injections are undetectable by the unauthorized observer. Section 8.7 provides the system properties required for the existence of an MUO defense strategy. Section 8.8 proposes a method for designing misleading injections to maximize the unauthorized observer's estimation error while ensuring that the injections remain undetectable. Section 8.9 illustrates the findings through simulations. Finally, Section 8.10 concludes the chapter. [1]

8.1. Introduction

In this thesis, we introduce the term "unauthorized observation"as an attack in which the attacker aims to perform remote state observation based on the knowledge of the system model and eavesdropping on input-output signals. The unauthorized observation attack extends beyond traditional eavesdropping by incorporating knowledge of the system model. Addressing this type of attack is crucial, as knowledge of the CPS model is common for attackers [147], and has been studied for other types of attack, like FDI attacks, but not for eavesdropping attacks.

The defense against an unauthorized observation can be similar to defenses against eavesdropping attacks, such as using encryption and firewalls, which prevent the unauthorized observer from accessing input-output signals. However, these conventional defenses might

[1] Before reading this chapter, it is recommended to first read Chapter 5.

motivate the attackers to improve themselves, attempting to bypass encryption or firewalls. Also, the defense can be based on data omission [104] or injecting randomness into the transmissions [71, 192]. However, these methods also affect the performance of the legit observer, and the unauthorized observer may detect that the data have been modified. To address this, we propose defense strategy that leave no trace and remain undetectable to the unauthorized observer as a potential solution. The proposed defense strategy can be used independently or in conjunction with encryption and firewalls, ensuring that the system remains protected even if the attacker bypasses them.

The objective of this chapter is then to design a smart defense strategy against an unauthorized observer, called Misleading Unauthorized Observer (MUO), by modifying the input-output signals before being read by the unauthorized observer. These modifications involve smart additional terms we call them misleading injections, ensuring that the modified input-output signals remain consistent with each other and with the history of estimations. In other words, within the framework of Kalman filter theory, these modifications are undetectable by innovation or residual-based methods. This defense strategy is an active defense, which involves misleading the unauthorized observer, making it believe that it is accurately monitoring the system. In addition to testing the consistency between input-output signals and the history of estimation, it is important to consider the possibility that the unauthorized observer may also verify that the obtained input-output signals fall within certain bounds and satisfy other characteristics defined by the physical nature of these signals. For example, in an autonomous vehicle system, the acceleration and velocity signals must not exceed the mechanical limits of the vehicle. Similarly, in power grid systems, voltage and current measurements need to stay within the operational limits. Another example of a characteristic that should be verified in some applications is the smooth evolution of the signal. In the case of a moving vehicle, the position and velocity signals should change gradually, without abrupt jumps. For example, a car's position should not show sudden, unrealistic jumps from one location to another. These bounds and other characteristics impose conditions on the modified input-output signals, which can be represented mathematically as constraints.

An important concern is that the defending system might not only aim to introduce errors in the unauthorized observer's state estimation but also to deliberately mislead it by steering the estimation along a specific trajectory. For instance, if the unauthorized observer is observing the system state, and wants to make an action, i.e., physical attack, if it observes the system state outside a specific safe area, then the defending system aims to mislead the unauthorized observer making it believe that the system is still inside the safe area while the system is outside.

Additionally, in order to consider the input-output signals bounds and characteristics, we propose to design the misleading injections as solutions to an optimization problem, where the objective is to maximize the unauthorized observer's estimation error, subject to undetectability conditions and constraints on the modified input-output signals.

The main contributions of this chapter are:

- Define a new type of cyber-physical attack, which is the unauthorized observation, where the attacker aims to perform a remote state observation based on the knowledge of the system model and eavesdropping on input-output signals.
- Introduce the concept of active defense by misleading the unauthorized observer, which differs from the traditional passive defense in cyber-physical systems.
- Formulate the conditions for undetectability by the residual and innovation-based detectors as a dynamic model of the estimation error caused by the misleading injections. These constraints can be utilized within an optimization problem.
- State properties that the system must have and find stronger properties required for the system to mislead the unauthorized observer's estimation into following a specific trajectory.

The material presented in this chapter is based on the corresponding publication:

- *G. Shaaban, H. Fourati, A. Kibangou, and C. Prieur, "Active defense strategy in cyber-physical systems: Misleading unauthorized observers," accepted to the IEEE Transactions on Control of Network Systems (TCNS), 2025.*

8.2. System Model and Legit Observer

System Model

Consider the following discrete-time linear system model $\mathbf{\Sigma}$, which is commonly adopted in the literature for CPS modelling [33, 123, 124, 147]:

$$\mathbf{x}_k = \mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{w}^x_{k-1}, \tag{8.2.1}$$
$$\mathbf{y}_k = \mathbf{C}\mathbf{x}_k + \mathbf{w}^y_k, \tag{8.2.2}$$

where for any time step $k \in \mathbb{N}$, $\mathbf{x}_k \in \mathbb{R}^{n_x}$, $\mathbf{u}_k \in \mathbb{R}^{n_u}$, and $\mathbf{y}_k \in \mathbb{R}^{n_y}$ are the system state, the system input, and the system output, respectively. The matrices $\mathbf{A} \in \mathbb{R}^{n_x \times n_x}$, $\mathbf{B} \in \mathbb{R}^{n_x \times n_u}$, and $\mathbf{C} \in \mathbb{R}^{n_y \times n_x}$ are the state, input, and output matrices, respectively. The process noise $\mathbf{w}^x_k \in \mathbb{R}^{n_x}$, and the measurement noise $\mathbf{w}^y_k \in \mathbb{R}^{n_y}$ are assumed to be uncorrelated zero-mean white random Gaussian signals with positive definite covariance matrices $\boldsymbol{\mathcal{Q}}_k$ and $\boldsymbol{\mathcal{R}}_k$, respectively. Since unauthorized observation attacks concern system observation, we assume that the system described in (8.2.1)-(8.2.2) is observable.

Assumption 8.2.1. *The pair* $(\mathbf{A}, \mathbf{C})$ *is observable.*

Legit Observer

The legit observer estimates the system state based on the input-output signals. We consider the case of the Kalman filter, as it is optimal in the sense of minimum mean square error

for linear systems with uncorrelated zero-mean white process and measurement noises [94], which is the case of system (8.2.1)-(8.2.2).

Kalman filter

At each time step, the Kalman filter performs prediction and correction. The prediction uses the dynamic model and the input signal:

$$\begin{aligned}\hat{\mathbf{x}}_{k|k-1} =& \mathbf{A}\hat{\mathbf{x}}_{k-1} + \mathbf{B}\mathbf{u}_{k-1},\\ \mathbf{P}_{k|k-1} =& \mathbf{A}\mathbf{P}_{k-1}\mathbf{A}^T + \boldsymbol{\mathcal{Q}}_{k-1},\end{aligned}$$

where $\hat{\mathbf{x}}_{k|k-1}$ and $\mathbf{P}_{k|k-1}$ are the predicted state and the prediction error covariance matrix, respectively, while $\hat{\mathbf{x}}_{k-1}$ and $\mathbf{P}_{k-1}$ are the previous estimated state and the estimation error covariance matrix. The correction uses the output function and the output signal:

$$\begin{aligned}\mathbf{K}_k =& \mathbf{P}_{k|k-1}\mathbf{C}^T(\mathbf{C}\mathbf{P}_{k|k-1}\mathbf{C}^T + \boldsymbol{\mathcal{R}}_k)^{-1},\\ \tilde{\mathbf{y}}_k =& \mathbf{y}_k - \mathbf{C}\hat{\mathbf{x}}_{k|k-1},\\ \hat{\mathbf{x}}_k =& \hat{\mathbf{x}}_{k|k-1} + \mathbf{K}_k\tilde{\mathbf{y}}_k,\\ \mathbf{P}_k =& \mathbf{P}_{k|k-1} - \mathbf{K}_k\mathbf{C}\mathbf{P}_{k|k-1},\\ \tilde{\mathbf{r}}_k =& \mathbf{y}_k - \mathbf{C}\hat{\mathbf{x}}_k,\end{aligned}$$

where $\hat{\mathbf{x}}_k$ is the estimation, $\mathbf{K}_k$ is the Kalman gain, $\tilde{\mathbf{y}}_k$ is the innovation, which is the difference between the actual output and the predicted output, and $\tilde{\mathbf{r}}_k$ is the residual, which is the difference between the actual and the estimated outputs. The legit observer can be summarized as follows:

$$[\hat{\mathbf{x}}_k, \mathbf{P}_k, \tilde{\mathbf{y}}_k, \tilde{\mathbf{r}}_k] = KF\left((\mathbf{u}_i)_{i<k}, (\mathbf{y}_i)_{i\leq k}, \boldsymbol{\Sigma}, \hat{\mathbf{x}}_0, \mathbf{P}_0\right), \tag{8.2.3}$$

where $KF(.)$ stands for the Kalman filter, $\hat{\mathbf{x}}_0$ is the initial estimate, and $\mathbf{P}_0$ is the initial estimate covariance matrix.

In the Kalman filter, two types of resulting signals can serve as input for detectors: the innovation [29, 72], and the residual [63, 119].

Detection Scheme

The concept of innovation-based or residual-based detectors involves performing statistical tests on the innovation or residual signals. In the absence of input-output signals modifications, the innovation and residual are equal to the one of the legit observer described in Section 8.2. Thus, we explain hereafter the innovation and residual-based detectors applied to the resulting signals of the legit observer.

Innovation-based detector

The general idea of the innovation-based detector is that the detector triggers an alarm when a remarkable difference in the innovation happens. The innovation of the legit observer is:

$$\begin{aligned}\tilde{\mathbf{y}}_k =&\mathbf{y}_k - \mathbf{C}\hat{\mathbf{x}}_{k|k-1},\\ =&\mathbf{C}\mathbf{x}_k + \mathbf{w}_k^y - \mathbf{C}\hat{\mathbf{x}}_{k|k-1},\\ =&\mathbf{C}\left(\mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{w}_{k-1}^x\right) + \mathbf{w}_k^y - \mathbf{C}\left(\mathbf{A}\hat{\mathbf{x}}_{k-1} + \mathbf{B}\mathbf{u}_{k-1}\right),\\ =&\mathbf{C}\mathbf{A}\mathbf{e}_{k-1} + \mathbf{C}\mathbf{w}_{k-1}^x + \mathbf{w}_k^y,\end{aligned} \tag{8.2.4}$$

where $\mathbf{e}_{k-1} = \mathbf{x}_{k-1} - \hat{\mathbf{x}}_{k-1}$ is the estimation error in the previous time step.

To illustrate the idea, we explain one innovation-based detector, which is the $\boldsymbol{\chi}^2$ detector, as it is the most used in the literature. The innovation (8.2.4) is zero mean Gaussian signal with known covariance matrix $\tilde{\boldsymbol{\mathcal{R}}}_k = \mathbf{C}\mathbf{A}\mathbf{P}_{k-1}\mathbf{A}^T\mathbf{C}^T + \mathbf{C}\boldsymbol{\mathcal{Q}}_{k-1}\mathbf{C}^T + \boldsymbol{\mathcal{R}}_k$. The signal $s_k = \tilde{\mathbf{y}}_k^T\tilde{\boldsymbol{\mathcal{R}}}_k^{-1}\tilde{\mathbf{y}}_k$ follows a $\boldsymbol{\chi}^2$ distribution with n_y degree of freedom, i.e. $\mathbf{E}(s_k) = n_y$. At each time step, the signal s_k is compared with a predefined threshold s^{th}, this threshold defines the probability of the false alarm [23]. If it exceeds this threshold, it indicates that the input-output signals have been modified. The $\boldsymbol{\chi}^2$ detector is summarized as follows:

$$\begin{cases}\text{Alarm not triggered} & \text{if,} \quad s_k \leq s^{th},\\ \text{Alarm triggered} & \text{if,} \quad s_k > s^{th}.\end{cases}$$

Residual-based detector

The idea is similar to the case of innovation-based detectors, the detector triggers an alarm when a remarkable difference in the residual happens. The residual of the legit observer is:

$$\begin{aligned}\tilde{\mathbf{r}}_k =&\mathbf{y}_k - \mathbf{C}\hat{\mathbf{x}}_k,\\ =&\mathbf{C}\mathbf{x}_k + \mathbf{w}_k^y - \mathbf{C}\hat{\mathbf{x}}_k,\\ =&\mathbf{C}\mathbf{e}_k + \mathbf{w}_k^y,\end{aligned} \tag{8.2.5}$$

this residual is a zero mean Gaussian signal, with a covariance matrix $\boldsymbol{\mathcal{S}}_k = \mathbf{E}(\tilde{\mathbf{r}}_k\tilde{\mathbf{r}}_k^T)$:

$$\boldsymbol{\mathcal{S}}_k = \mathbf{C}\mathbf{P}_k\mathbf{C}^T + \boldsymbol{\mathcal{R}}_k + \mathbf{C}\mathbf{E}(\mathbf{e}_k\mathbf{w}_k^{yT}) + \mathbf{E}(\mathbf{w}_k^y\mathbf{e}_k^T)\mathbf{C}^T. \tag{8.2.6}$$

The estimation error $\mathbf{e}_k$ is given by:

$$\begin{aligned}\mathbf{e}_k =&\mathbf{x}_k - \hat{\mathbf{x}}_k,\\ =&\mathbf{x}_k - \hat{\mathbf{x}}_{k|k-1} - \mathbf{K}_k\tilde{\mathbf{y}}_k,\end{aligned}$$

we substitute the dynamic model and the prediction, in addition to the innovation from (8.2.4):

$$\begin{aligned}\mathbf{e}_k =&\mathbf{x}_k - \hat{\mathbf{x}}_k,\\ =&\mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{w}_{k-1}^x - \mathbf{A}\hat{\mathbf{x}}_{k-1} - \mathbf{B}\mathbf{u}_{k-1} - \mathbf{K}_k\left(\mathbf{C}\left(\mathbf{A}\mathbf{e}_{k-1} + \mathbf{w}_{k-1}^x\right) + \mathbf{w}_k^y\right),\\ =&\left(\mathbf{I} - \mathbf{K}_k\mathbf{C}\right)\left(\mathbf{A}\mathbf{e}_{k-1} + \mathbf{w}_{k-1}^x\right) - \mathbf{K}_k\mathbf{w}_k^y,\end{aligned} \tag{8.2.7}$$

thus, $\mathbf{E}(\mathbf{e}_k \mathbf{w}_k^{yT}) = -\mathbf{K}_k \boldsymbol{\mathcal{R}}_k$, we substitute in (8.2.6):

$$\boldsymbol{\mathcal{S}}_k = \mathbf{C}\mathbf{P}_k\mathbf{C}^T + \boldsymbol{\mathcal{R}}_k - \mathbf{C}\mathbf{K}_k\boldsymbol{\mathcal{R}}_k - \boldsymbol{\mathcal{R}}_k\mathbf{K}_k^T\mathbf{C}^T. \tag{8.2.8}$$

Finally, the signal $z_k = \tilde{\mathbf{r}}_k^T \boldsymbol{\mathcal{S}}_k^{-1} \tilde{\mathbf{r}}_k$ follows a $\boldsymbol{\chi}^2$ distribution with n_y degree of freedom, i.e. $\mathbf{E}(z_k) = n_y$. At each time step, the signal z_k is compared with a predefined threshold z^{th}. If it exceeds this threshold, it indicates that a fault has occurred.

8.3. Unauthorized Observer

The unauthorized observer remotely estimates the system state based on the input-output signals obtained through a network, denoted by $\mathbf{u}_k^m$ and $\mathbf{y}_k^m$, respectively. The unauthorized observer is assumed to implement a Kalman filter equipped with a detector based on innovation or residual. The use of the Kalman filter is widely adopted in the CPS literature, even under possible input-output signals modifications (e.g., those caused by FDI attacks), which result in a loss of its optimality [33, 123, 124, 147].

Remark 8.3.1. *The innovation or residual signals indicate the consistency between the input-output signals and the system model. If signals modifications preserve this consistency, i.e., they pass the innovation, or residual-based detectors, they are likely, intuitively, to pass other types of detectors as well.*

Additionally, the unauthorized observer may verify that the input-output signals are within some bounds and satisfy other characteristics defined by the physical nature of these signals. Mathematically, this can be expressed by general constraint functions:

$$\begin{aligned} \mathbf{g}_k^{min} \leq \mathbf{g}_k(\mathbf{u}_k^m) \leq \mathbf{g}_k^{max}, \\ \mathbf{h}_k^{min} \leq \mathbf{h}_k(\mathbf{y}_k^m) \leq \mathbf{h}_k^{max}, \end{aligned} \tag{8.3.1}$$

where $\mathbf{g}_k$ and $\mathbf{h}_k$ are bounded functions. One basic and essential constraint is that any physical signal has minimum and maximum bounds, in this case, the constraint function in (8.3.1) can be written as:

$$\begin{aligned} \mathbf{u}_k^{min} \leq \mathbf{u}_k^m \leq \mathbf{u}_k^{max}, \\ \mathbf{y}_k^{min} \leq \mathbf{y}_k^m \leq \mathbf{y}_k^{max}. \end{aligned} \tag{8.3.2}$$

If some of these constraints are not satisfied, it indicates to the unauthorized observer that the input-output signals have been compromised.

The worst-case attack scenario is commonly considered in the CPS literature [147], as successfully defending against such scenarios ensures the system's ability to defend against less severe cases. This approach is further inspired by Shannon's maxim (1948), *"The enemy knows the system,"* which is a restatement of Kerckhoffs's principle in military ciphers (1883)[176]. Accordingly, we adopt Assumptions 8.3.2, 8.3.3, and 8.3.4 to address the worst-case security problem.

Assumption 8.3.2. *The unauthorized observer has perfect knowledge of the system model* $\boldsymbol{\Sigma}$*, i.e. it knows the system matrices* $\mathbf{A}$*,* $\mathbf{B}$*, and* $\mathbf{C}$*, and the noises covariance matrices* $\boldsymbol{\mathcal{Q}}_k$ *and* $\boldsymbol{\mathcal{R}}_k$*.*

Assumption 8.3.3. *The unauthorized observer knows the initial estimate* $\hat{\mathbf{x}}_0$ *and its estimation error covariance matrix* $\mathbf{P}_0$*, which are used by the legit observer.*

Assumption 8.3.4. *The unauthorized observer has knowledge of the physical bounds, i.e,* $\mathbf{u}_k^{min}, \mathbf{u}_k^{max}, \mathbf{y}_k^{min}, \mathbf{y}_k^{max}$ *expressed in* (8.3.2)*, and other characteristics of the input-output signals of the system, i.e,* $\mathbf{g}_k(.), \mathbf{h}_k(.)$ *and their bounds* $\mathbf{g}_k^{min}, \mathbf{g}_k^{max}, \mathbf{h}_k^{min}, \mathbf{h}_k^{max}$ *expressed in* (8.3.1)*.*

Assumption 8.3.2 indicates that the unauthorized observer knows the system dynamics and the noise covariance matrices. This is widely adopted in the literature of CPS [147]. Regarding Assumption 8.3.3, as the system is observable, in the absence of signals modifications, both the unauthorized and legit observers' estimates will converge to the true state, and the covariance matrices will converge to the same value. Thus, this assumption represents the worst-case scenario. Finally, the resulting signals of the unauthorized observer can be summarized as follows:

$$[\hat{\mathbf{x}}_k^m, \mathbf{P}_k^m, \tilde{\mathbf{y}}_k^m, \tilde{\mathbf{r}}_k^m] = KF\left((\mathbf{u}_i^m)_{i<k}, (\mathbf{y}_i^m)_{i\leq k}, \mathbf{\Sigma}, \hat{\mathbf{x}}_0, \mathbf{P}_0\right), \tag{8.3.3}$$

Assumption 8.3.4 is justified by the fact that the characteristics and bounds of input-output signals often stem from physical properties, which are not confidential.

In order to locate the unauthorized observer among other types of attacks, we use the cyber-physical attack space. The unauthorized observer has access to read all input-output signals and has the knowledge of the system model, as illustrated in Fig. 8.1.

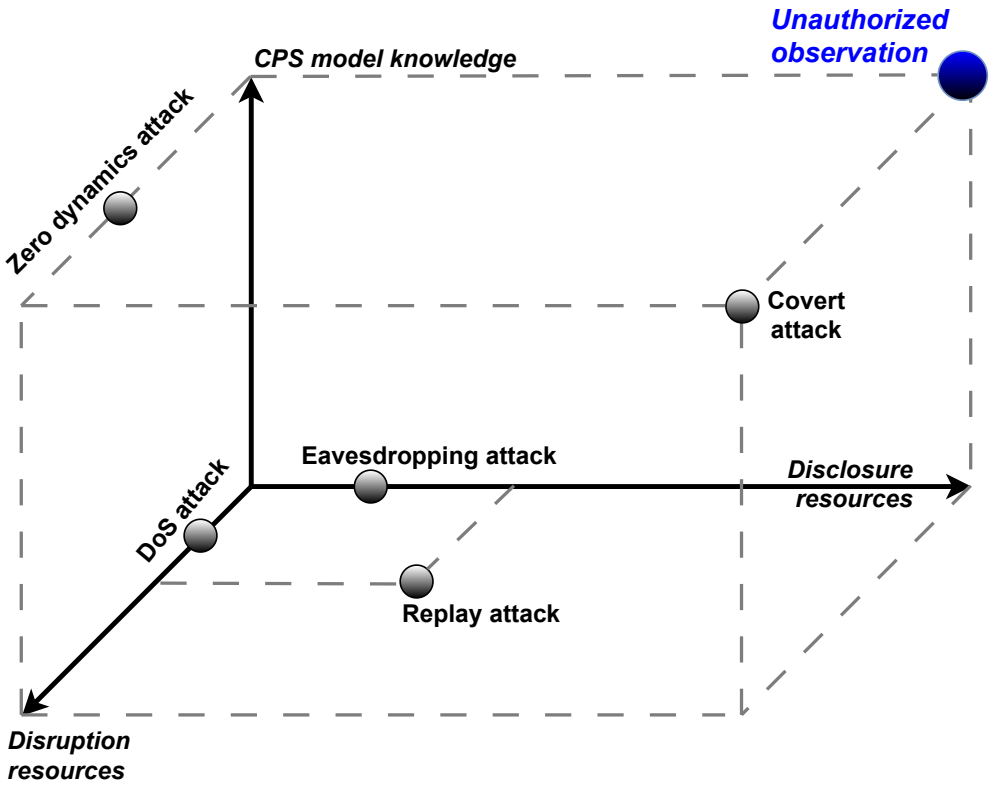

Figure 8.1: Unauthorized observation in the cyber-physical attack space.

8.4. Misleading Unauthorized Observers

The defending system is assumed to be able to modify the input-output signals that the unauthorized observer is receiving, specifically, for time step k:

$$\mathbf{u}_k^m = \mathbf{u}_k + \boldsymbol{\zeta}_k^u, \tag{8.4.1}$$
$$\mathbf{y}_k^m = \mathbf{y}_k + \boldsymbol{\zeta}_k^y, \tag{8.4.2}$$

where $\boldsymbol{\zeta}_k^u$ and $\boldsymbol{\zeta}_k^y$ are misleading injections to input-output signals, respectively.

The unauthorized observer estimation error caused by input-output signals modifications is denoted by $\mathbf{e}_k^m$, i.e. $\hat{\mathbf{x}}_k - \hat{\mathbf{x}}_k^m = \mathbf{e}_k^m$. In the following, we define the undetectable input-output signals modifications and the Misleading Unauthorized Observer (MUO) in Definitions 8.4.1 and 8.4.3, respectively. More specific types of MUO are defined in Definitions 8.4.4, 8.4.5, and 8.4.6.

Definition 8.4.1. *[Undetectable input-output signals modifications] The input-output signals modifications are considered undetectable if the resulting innovation $\tilde{\mathbf{y}}_k^m$ and residual $\tilde{\mathbf{r}}_k^m$ of the unauthorized observer's Kalman filter (8.3.3), which are inputs to the innovation-based and residual-based detectors, are identical to the ones of the legit observer's Kalman filter (8.2.3), i.e. $\tilde{\mathbf{y}}_k = \tilde{\mathbf{y}}_k^m$ and $\tilde{\mathbf{r}}_k = \tilde{\mathbf{r}}_k^m$.*

Remark 8.4.2. *Definition 8.4.1 considers that the modifications are undetectable if both the residual and innovation signals of the unauthorized observer are identical to those of the legit observer. This is a strong condition and represents the worst-case scenario for the security problem. There is also a weaker condition, known as stealthy modification, where the innovation and residual are not the same, but the statistical test (e.g., $\boldsymbol{\chi}^2$) does not raise an alarm [34]. However, if the modifications are undetectable, this implies that they are also stealthy.*

If the unauthorized observer does not know the exact parameters used by the legit observer, it will use a stealth detector with a higher threshold. If this detector gives an alarm for the designed undetectable modified signals, it will also give false alarms for the original (true) signal.

Definition 8.4.3. *[MUO] The defending system is considered to be performing an MUO defense strategy by input-output signals modifications, if these modifications are undetectable (see Definition 8.4.1) and degrades the unauthorized observer state estimation, i.e. for $k \geq 0$, $\tilde{\mathbf{y}}_k = \tilde{\mathbf{y}}_k^m$, $\tilde{\mathbf{r}}_k = \tilde{\mathbf{r}}_k^m$, and $\mathbf{e}_k^m \neq \mathbf{0}$.*

Definition 8.4.4. *[State-i MUO] An MUO is called to be state-i MUO if, for any time step $k \geq n_x$, the defending system is able to achieve $\mathbf{e}_k^m(i) \neq 0$.*

Definition 8.4.5. *[State-i strongly MUO] A state-i MUO is called to be state-i strongly MUO if for any time step $k \geq n_x$, and any desired estimation error $e_k^{d,i} \in \mathbb{R} \setminus \{0\}$, the defending system is able to achieve $\mathbf{e}_k^m(i) = e_k^{d,i}$.*

Definition 8.4.6. *[Strongly MUO] An MUO is called to be strongly MUO if $\forall i \in \{1, 2, ..., n\}$, it is State-i strongly MUO.*

Remark 8.4.7. *In Definitions 8.4.5 and 8.4.6, the strongly misleading case assumes that the unauthorized observer uses the same parameters as the legit observer. If this is not the case, the definitions are still valid. The difference between the unauthorized observer's estimate and the legit observer's estimate will be close to the desired error defined in the strongly MUO case, and will converge to it as the parameter differences tend to zero, assuming that the unauthorized observer uses an unbiased estimator.*

Main objectives *The first objective is to design* $(\boldsymbol{\zeta}_k^u)_{k\in\mathbb{N}}$ *and* $(\boldsymbol{\zeta}_k^y)_{k\in\mathbb{N}}$ *in order to perform an MUO defense strategy, and study and analyze the property that the system should have to enable the different kinds of MUO listed in Definitions 8.4.4, 8.4.6, and 8.4.5. The first objective is achieved in Section 8.7. The second objective is to design* $(\boldsymbol{\zeta}_k^u)_{k\in\mathbb{N}}$ *and* $(\boldsymbol{\zeta}_k^y)_{k\in\mathbb{N}}$ *so that the unauthorized observer estimation error is maximized while these injections are undetectable, and the modified input-output signals satisfy the input-output signals bounds and characteristics. The second objective is achieved in Section 8.8. Conditions for undetectable input-output modifications are derived in Section 8.6. The architecture of the MUO defense strategy is presented in Section 8.5.*

8.5. MUO Architecture

There are two possible scenarios in which the proposed MUO can be effective in defending against an unauthorized observer.

The first scenario occurs when the unauthorized observer gains unauthorized access to the input-output signals transmission lines connecting the sensors and actuators on one side and the control unit on the other side. The control unit is responsible for state estimation (the legit observer) and computing control commands. An example of this scenario is a vehicle, where all sensors, actuators, and the control unit are connected through Controller Area Network (CAN) bus [49]. The defending system operates similarly to an encryption/decryption method [55], where the system encrypts the message before transmission and decrypts it upon arrival. In this case, however, instead of encrypting, the defending system injects misleading terms into the transmitted signals and subtracts them upon arrival. This ensures that the communication between the sensors, actuators, and control unit remains secure, while the obtained signals by the unauthorized observer are modified. It is worth noting that the injection and subtraction of misleading terms can be performed separately when the misleading error trajectory is designed in advance and known by both components of the defending system. The design of misleading injections depends solely on the misleading error trajectory and is independent of the true trajectory or the input/output data, as illustrated in (8.6.1) in Theorem 8.6.1. This first scenario is illustrated in Fig. 8.2.

The second scenario occurs when the unauthorized observer installs hidden sensors on the system at an earlier time with the purpose of tracking it. These sensors transmit measured signals using a transmitter installed alongside them. For example, an unauthorized observer might install a GPS sensor on a moving car to track its position. Once the system detects these unauthorized sensors, the defending system modifies the transmitted signals received by the unauthorized observer. In this scenario, the system does not necessarily use these

measurements for its own observation or control. The second scenario is illustrated in Fig. 8.3.

The architecture of the MUO defense strategy, including the legit observer and the unauthorized observer, is depicted in Fig. 8.4. This diagram is intended to clarify the overall problem and solution, rather than representing a real-world scenario. Note that the legit observer may be a conceptual observer introduced to illustrate the idea, as the system might use different sensor measurements than those accessed by the unauthorized observer, as explained in the second scenario earlier.

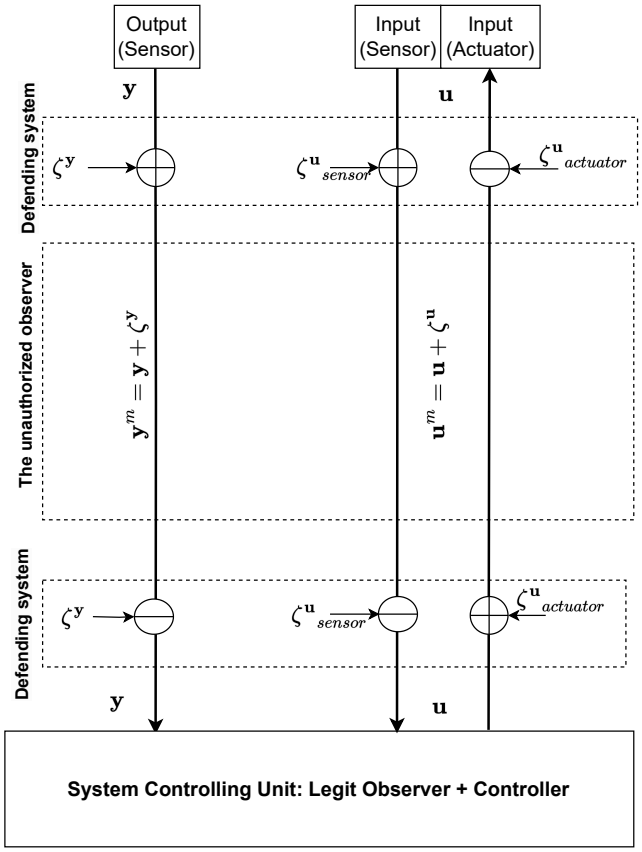

Figure 8.2: The first scenario of MUO defense: the input $\mathbf{u}$ represents either sensor measurements or actuator commands, while the output $\mathbf{y}$ always represents sensor measurements. The defending system injects misleading terms into the signals before transmission and subtracts them upon arrival. The authorized observer receives the modified signals through the network.

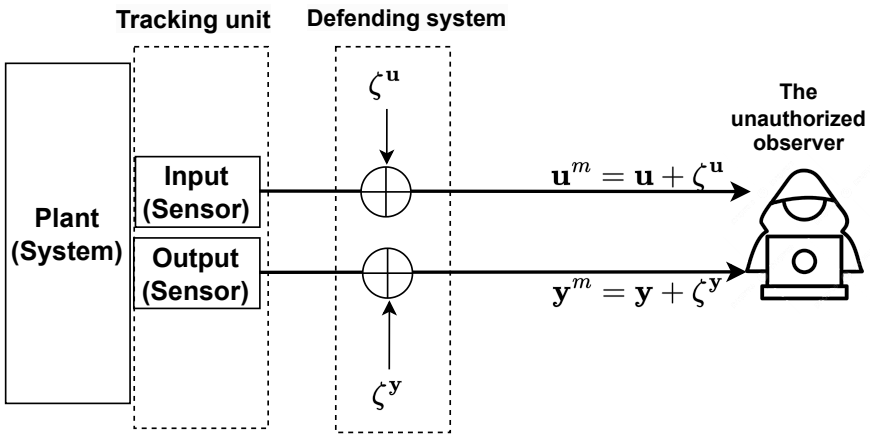

Figure 8.3: The second scenario of MUO defense: the input and output signals are sensor measurements. The defending system injects misleading terms into the signals before they are transmitted to the unauthorized observer.

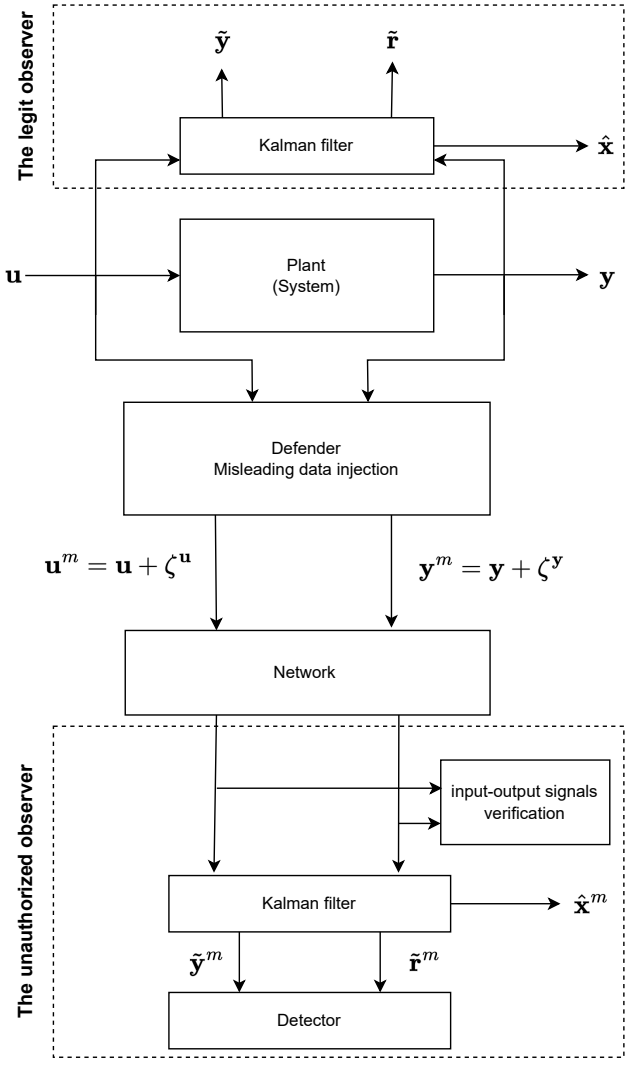

Figure 8.4: Architecture of a MUO defense strategy: The defending system injects misleading data $\boldsymbol{\zeta}^u$ and $\boldsymbol{\zeta}^y$, into the input and output signals, respectively, which are read by the unauthorized observer. The unauthorized observer uses a Kalman filter for remote state estimation and applies two detection steps: first, by verifying that the obtained input-output signals satisfy certain characteristics; and second, by using innovation-based or residual-based detectors.

8.6. Undetectable Misleading Injections

Theorem 8.6.1 states the sufficient and necessary conditions to make modifications to the input-output signals undetectable by innovation and residual-based detectors.

Theorem 8.6.1. *Consider the discrete-time linear system model defined by (8.2.1)-(8.2.2) being subject to an unauthorized observer through eavesdropping on its input-output signals, and the defending system aims to mislead the unauthorized observer by modifying the received input-output signals as in (8.4.1)- (8.4.2). The misleading injections $(\boldsymbol{\zeta}_k^u)_{k\geq 0}$ and $(\boldsymbol{\zeta}_k^y)_{k\geq 0}$ in (8.4.1)- (8.4.2) are undetectable by innovation-based and residual-based detectors if and only if they satisfy the following conditions:*

$$\begin{aligned} \mathbf{e}_{k+1}^m =& \mathbf{A}\mathbf{e}_k^m - \mathbf{B}\boldsymbol{\zeta}_k^u, \\ \boldsymbol{\zeta}_k^y =& -\mathbf{C}\mathbf{e}_k^m, \end{aligned} \tag{8.6.1}$$

for all $k \geq 0$.

Proof. The unauthorized observer applies the Kalman filter for state estimation based on the modified input-output signals. Thus the prediction step is as follows:

$$\begin{aligned} \hat{\mathbf{x}}_{k|k-1}^m =& \mathbf{A}\hat{\mathbf{x}}_{k-1}^m + \mathbf{B}\mathbf{u}_{k-1}^m, \\ =& \mathbf{A}\hat{\mathbf{x}}_{k-1}^m + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{B}\boldsymbol{\zeta}_{k-1}^u. \end{aligned}$$

The innovation in the presence of the misleading injections is as follows:

$$\begin{aligned} \tilde{\mathbf{y}}_k^m =& \mathbf{y}_k^m - \mathbf{C}\hat{\mathbf{x}}_{k|k-1}^m = \mathbf{y}_k + \boldsymbol{\zeta}_k^y - \mathbf{C}\hat{\mathbf{x}}_{k|k-1}^m, \\ =& \mathbf{C}\mathbf{x}_k + \mathbf{w}_k^y + \boldsymbol{\zeta}_k^y - \mathbf{C}\left(\mathbf{A}\hat{\mathbf{x}}_{k-1}^m + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{B}\boldsymbol{\zeta}_{k-1}^u\right), \\ =& \mathbf{C}\left(\mathbf{A}\left(\mathbf{x}_{k-1} - \hat{\mathbf{x}}_{k-1}^m\right) + \mathbf{w}_{k-1}^x\right) + \mathbf{w}_k^y + \boldsymbol{\zeta}_k^y - \mathbf{C}\mathbf{B}\boldsymbol{\zeta}_{k-1}^u, \end{aligned} \tag{8.6.2}$$

the term $\mathbf{x}_{k-1} - \hat{\mathbf{x}}_{k-1}^m$ is the estimation error in the previous time step, we can rewrite it as follows: $\mathbf{x}_{k-1} - \hat{\mathbf{x}}_{k-1}^m = \mathbf{x}_{k-1} - \hat{\mathbf{x}}_{k-1} + \hat{\mathbf{x}}_{k-1} - \hat{\mathbf{x}}_{k-1}^m = \mathbf{e}_{k-1} + \mathbf{e}_{k-1}^m$, we remind that $\mathbf{e}_{k-1}$ is the estimation error of the legit observer, substituting in the innovation (8.6.2):

$$\tilde{\mathbf{y}}_k^m = \mathbf{C}\left(\mathbf{A}\mathbf{e}_{k-1} + \mathbf{w}_{k-1}^x\right) + \mathbf{w}_k^y + \boldsymbol{\zeta}_k^y - \mathbf{C}\mathbf{B}\boldsymbol{\zeta}_{k-1}^u + \mathbf{C}\mathbf{A}\mathbf{e}_{k-1}^m, \tag{8.6.3}$$

by comparing the innovation equations of the unauthorized observer (8.6.3) with the one of the legit observer (8.2.4), we find $\tilde{\mathbf{y}}_k^m = \tilde{\mathbf{y}}_k + \boldsymbol{\zeta}_k^y - \mathbf{C}\mathbf{B}\boldsymbol{\zeta}_{k-1}^u + \mathbf{C}\mathbf{A}\mathbf{e}_{k-1}^m$ and we conclude that the misleading injections are not detectable by the innovation-based detector i.e. $\tilde{\mathbf{y}}_k^m = \tilde{\mathbf{y}}_k$ if and only if the following condition is satisfied:

$$\boldsymbol{\zeta}_k^y - \mathbf{C}\mathbf{B}\boldsymbol{\zeta}_{k-1}^u + \mathbf{C}\mathbf{A}\mathbf{e}_{k-1}^m = \mathbf{0}. \tag{8.6.4}$$

To find the term $\mathbf{e}_{k-1}^m$, we start by writing the equation of the state estimation after the correction step, assuming that the condition (8.6.4) is satisfied, and we substitute it in (8.6.3), thus we obtain $\tilde{\mathbf{y}}_k^m = \mathbf{C}\left(\mathbf{A}\mathbf{e}_{k-1} + \mathbf{w}_{k-1}^x\right) + \mathbf{w}_k^y$, then we find the estimation after correction:

$$\begin{aligned} \hat{\mathbf{x}}_k^m =& \hat{\mathbf{x}}_{k|k-1}^m + \mathbf{K}_k\tilde{\mathbf{y}}_k^m, \\ =& \mathbf{A}\hat{\mathbf{x}}_{k-1}^m + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{B}\boldsymbol{\zeta}_{k-1}^u + \mathbf{K}_k\left(\mathbf{C}\left(\mathbf{A}\mathbf{e}_{k-1} + \mathbf{w}_{k-1}^x\right) + \mathbf{w}_k^y\right), \end{aligned}$$

and the estimation error:

$$\begin{aligned}\mathbf{x}_k - \hat{\mathbf{x}}_k^m =& \mathbf{A}\mathbf{x}_{k-1} + \mathbf{B}\mathbf{u}_{k-1} + \mathbf{w}_{k-1}^x - \mathbf{A}\hat{\mathbf{x}}_{k-1}^m - \mathbf{B}\mathbf{u}_{k-1} - \mathbf{B}\boldsymbol{\zeta}_{k-1}^u \\ & - \mathbf{K}_k \left(\mathbf{C}\left(\mathbf{A}\mathbf{e}_{k-1} + \mathbf{w}_{k-1}^x\right) + \mathbf{w}_k^y\right) \\ =& \mathbf{A}\left(\mathbf{x}_{k-1} - \hat{\mathbf{x}}_{k-1}^m\right) + \mathbf{w}_{k-1}^x - \mathbf{B}\boldsymbol{\zeta}_{k-1}^u - \mathbf{K}_k \left(\mathbf{C}\left(\mathbf{A}\mathbf{e}_{k-1} + \mathbf{w}_{k-1}^x\right) + \mathbf{w}_k^y\right) \\ & + \mathbf{A}\mathbf{e}_{k-1}^m - \mathbf{B}\boldsymbol{\zeta}_{k-1}^u, \end{aligned} \tag{8.6.5}$$

we substitute (8.2.7):

$$\mathbf{x}_k - \hat{\mathbf{x}}_k^m = \mathbf{e}_k + \mathbf{A}\mathbf{e}_{k-1}^m - \mathbf{B}\boldsymbol{\zeta}_{k-1}^u, \tag{8.6.6}$$

thus we conclude:

$$\mathbf{e}_k^m = \mathbf{A}\mathbf{e}_{k-1}^m - \mathbf{B}\boldsymbol{\zeta}_{k-1}^u, \tag{8.6.7}$$

by comparing (8.6.4) and (8.6.7), we conclude:

$$\boldsymbol{\zeta}_k^y = -\mathbf{C}\mathbf{e}_k^m, \tag{8.6.8}$$

thus the conditions (8.6.1) are sufficient and necessary conditions for the undetectable misleading injections by the innovation-based detector. Now we prove that these misleading injections are undetectable by the residual-based detector. The residual of the unauthorized observer's Kalman filter is:

$$\begin{aligned}\tilde{\mathbf{r}}_k^m =& \mathbf{y}_k^m - \mathbf{C}\hat{\mathbf{x}}_k^m, \\ =& \mathbf{C}\mathbf{x}_k + \mathbf{w}_k^y + \boldsymbol{\zeta}_k^y - \mathbf{C}\hat{\mathbf{x}}_k^m, \\ =& \mathbf{C}\mathbf{e}_k + \mathbf{w}_k^y + \boldsymbol{\zeta}_k^y + \mathbf{C}\mathbf{e}_k^m, \end{aligned} \tag{8.6.9}$$

substituting the condition (8.6.7):

$$\tilde{\mathbf{r}}_k^m = \mathbf{C}\mathbf{e}_k + \mathbf{w}_k^y,$$

which is identical to the residual of the legit observer (8.2.5), thus, these injections are undetectable by the residual-based detector. ■

Remark 8.6.2. *Conditions (8.6.1) represent a linear state-space model of the unauthorized observer's estimation error, where its input corresponds to the misleading injections to the system input, and its output corresponds to the misleading injections to the system output. These injections can be designed to cause estimation errors based on the system properties addressed in Theorem 8.7.1 and Theorem 8.7.2 in Section 8.7. These conditions can also be incorporated into an optimization problem, as outlined in Proposition 7.4.1 in Section 8.8, making the conditions effective for designing the misleading injections.*

8.7. System Properties for Existence of an MUO Defense Strategy

The purpose of this section is to study and analyze the properties that a system must possess to be defended against unauthorized observers through misleading injections (8.6.1) in the three defenses strategies: state-i MUO, strongly MUO and state-i strongly MUO.

Theorem 8.7.1. *The defending system is able to perform state-i MUO defense strategy on a system defined by (8.2.1)-(8.2.2), if and only if the i^{th} row of the controllability matrix $\boldsymbol{\mathcal{C}} = [\mathbf{A}^{n_x-1}\mathbf{B} \ ... \ \mathbf{AB} \ \mathbf{B}]$ differs from zero.*

Proof. At time step $k \geq n_x$, the unauthorized observer estimation error caused by misleading injections (see (8.6.1)):

$$\begin{aligned}\mathbf{e}_k^m =& \mathbf{A}\mathbf{e}_{k-1}^m - \mathbf{B}\boldsymbol{\zeta}_{k-1}^u,\\ =& \mathbf{A}^2\mathbf{e}_{k-2}^m - \mathbf{AB}\boldsymbol{\zeta}_{k-2}^u - \mathbf{B}\boldsymbol{\zeta}_{k-1}^u,\\ =& -\begin{bmatrix}\mathbf{A}^{k-1}\mathbf{B} \ ... \ \mathbf{AB} \ \mathbf{B}\end{bmatrix}\begin{bmatrix}\boldsymbol{\zeta}_0^u\\ \vdots\\ \boldsymbol{\zeta}_{k-2}^u\\ \boldsymbol{\zeta}_{k-1}^u\end{bmatrix},\end{aligned}$$

Note that $\mathbf{e}_0^m = \mathbf{0}$, as the unauthorized observer knows the initial estimate of the legit observer $\hat{\mathbf{x}}_0$, as stated in Assumption 8.3.3. We denote the matrix $\begin{bmatrix}\mathbf{A}^{k-1}\mathbf{B} \ ... \ \mathbf{AB} \ \mathbf{B}\end{bmatrix}$ by $\boldsymbol{\mathcal{C}}_k$ (which is equal to the controllability matrix $\boldsymbol{\mathcal{C}}$ when $k = n_x$), its i^{th} row by $\boldsymbol{\mathcal{C}}_k(i)$, and the vector $\begin{bmatrix}\boldsymbol{\zeta}_0^{u\,T} \ ... \ \boldsymbol{\zeta}_{k-2}^{u\,T} \ \boldsymbol{\zeta}_{k-1}^{u\,T}\end{bmatrix}^T$ by $\boldsymbol{\zeta}_{<k}^u$, thus $\mathbf{e}_k^m(i) = \boldsymbol{\mathcal{C}}_k(i)\boldsymbol{\zeta}_{<k}^u$. We analyze two cases, if $\boldsymbol{\mathcal{C}}_k(i) = \mathbf{0}$, then $\mathbf{e}_k^m(i) = 0$ regardless of the value of $\boldsymbol{\zeta}_{<k}^u$. Conversely, if $\boldsymbol{\mathcal{C}}_k(i) \neq \mathbf{0}$, then we can find $\boldsymbol{\zeta}_{<k}^u$ so that $\mathbf{e}_k^m(i) \neq 0$.
We prove that, $\forall k \geq n_x$, $\boldsymbol{\mathcal{C}}_k(i) = \mathbf{0}$ if and only if $\boldsymbol{\mathcal{C}}(i) = \mathbf{0}$, where $\boldsymbol{\mathcal{C}}(i)$ is the i^{th} row of the controllability matrix $\boldsymbol{\mathcal{C}}$. The first implication is straightforward: if $\boldsymbol{\mathcal{C}}(i) \neq \mathbf{0}$, then $\boldsymbol{\mathcal{C}}_k(i) \neq \mathbf{0}$. Conversely, if $\boldsymbol{\mathcal{C}}(i) = \mathbf{0}$, it means that all i^{th} rows of the terms $\mathbf{A}^l\mathbf{B}$ are zeros for all $l < n_x$. Applying the Cayley–Hamilton theorem [81, Section 2.4.3] to the square matrix $\mathbf{A}$, we can express $\mathbf{A}^l$ for $l \geq n_x$ as a linear combination of $\mathbf{I}, \mathbf{A}, \ldots, \mathbf{A}^{n_x-1}$. Consequently, the term $\mathbf{A}^l\mathbf{B}$ for $l \geq n_x$ can be expressed as a linear combination of $\mathbf{B}, \mathbf{AB}, \ldots, \mathbf{A}^{n_x-1}\mathbf{B}$, which have the i^{th} rows equal to zero. Thus, the terms $\mathbf{A}^l\mathbf{B}$ have the i^{th} rows equal to zero for all $l \geq n_x$, thereby proving the second implication. ■

Theorem 8.7.2. *A defending system can perform a strongly MUO by misleading data injections on a system defined by (8.2.1)-(8.2.2) if and only if the pair $(\mathbf{A}, \mathbf{B})$ is controllable. Otherwise, it can perform a state-i strongly MUO defense if the state component i belongs to the controllable subspace of the system.*

Proof. Given (8.6.1), the error dynamics is a system driven by $\boldsymbol{\zeta}_k^u$ with controllability depending on the pair $(\mathbf{A}, \mathbf{B})$. From Definition 8.4.6, driving the error $\mathbf{e}_k^m$ to arbitrary trajectory

$\mathbf{e}_k^d$, means controlling e_k^m, the state of system (8.6.1). This is achieved if and only if $(\mathbf{A}, \mathbf{B})$ is controllable. Otherwise, based on the notions of controllable supscases [48], state-i strongly MUO is achieved if the i^{th} component of the state belongs to the controllable subspace. ■

The importance of strongly MUO (discussed in Theorem 8.7.2) comes from a crucial point that the defending system may not only need to introduce an error in the unauthorized observer's estimation (even if the error is large), but it may have the purpose of directing the unauthorized observer's estimation along a specific trajectory. For instance, in the case of a moving car, the defending system might aim to mislead the unauthorized observer into believing that the car is following a trajectory inside a specific area while the car is outside this area. In such situations, causing an estimation error (even if it is large) without imposing a specific trajectory may not satisfy this purpose.

Theorem 8.7.1 is important for uncontrollable systems, where even if some states are not controllable, the defending system is still able to cause error in the unauthorized observer estimation for these states. For example, for the system model defined by (8.2.1)-(8.2.2), where its matrices are:

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \mathbf{C} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix},$$

the observability matrix is:

$$\boldsymbol{\mathcal{O}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

the observability matrix has the rank of 3, and the system is observable, satisfying Assumption 8.2.1. The controllability matrix is:

$$\boldsymbol{\mathcal{C}} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

it has a rank of 1, thus the pair $(\mathbf{A}, \mathbf{B})$ is not controllable, and the defending system can not mislead the unauthorized observer to follow a specific trajectory. However, all rows of the controllability matrix differ from zeros, thus the defending system by misleading injections (8.6.1) can cause unauthorized observer estimation error for all states, and this error could be unbounded (and still undetectable by residual and innovation-based detectors), for instance by choosing $\boldsymbol{\zeta}_k^u = 1$ for all k, and the injections on output $\boldsymbol{\zeta}_k^y$ satisfy (8.6.1).

8.8. Design of Misleading Injections for an Optimal MUO Defense Strategy

In Proposition 8.8.1, a solution is proposed to design the misleading injections so that the unauthorized observer estimation error is maximized while these injections are undetectable, and the modified input-output signals satisfy the input-output signals characteristics.

Proposition 8.8.1. *Consider the discrete-time linear system model defined by (8.2.1)-(8.2.2), subject to an unauthorized observer through eavesdropping on its input-output signals, and the defending system is able to modify the received input-output signals as in (10)-(11). The defending system misleads the unauthorized observer by injecting $\boldsymbol{\zeta}_k^u$ and $\boldsymbol{\zeta}_{k+1}^y$ which are the solution of the following optimization problem:*

$$
\begin{aligned}
&\max_{\boldsymbol{\zeta}_k^u,\dots,\boldsymbol{\zeta}_{k+N-1}^u,\boldsymbol{\zeta}_{k+1}^y,\dots,\boldsymbol{\zeta}_{k+N}^y} \sum_{i=1}^{N} \mathbf{e}_{k+i}^{mT}\mathbf{W}\mathbf{e}_{k+i}^{m} \\
&\textit{s.t.} \\
&\mathbf{e}_{k+i+1}^{m} = \mathbf{A}\mathbf{e}_{k+i}^{m} - \mathbf{B}\boldsymbol{\zeta}_{k+i}^{u}, && i = 0,\dots,N-1 \\
&\boldsymbol{\zeta}_{k+i}^{y} = -\mathbf{C}\mathbf{e}_{k+i}^{m}, && i = 1,\dots,N \\
&\mathbf{g}_{k+i}^{min} \leq \mathbf{g}_{k+i}(\mathbf{u}_{k+i}^{m}) \leq \mathbf{g}_{k+i}^{max}, && i = 0,\dots,N-1 \\
&\mathbf{h}_{k+i}^{min} \leq \mathbf{h}_{k+i}(\mathbf{y}_{k+i}^{m}) \leq \mathbf{h}_{k+i}^{max}. && i = 1,\dots,N
\end{aligned}
\tag{8.8.1}
$$

where $\mathbf{W}$ is a weight matrix, and N is the time window on which the optimization problem is solved.

The optimization problem (8.8.1) involves maximizing a quadratic convex function subject to constraints. The quadratic cost function is commonly used in the literature for expressing estimation error, e.g. it aligns with the properties of the optimal Kalman filter [94].

The first two constraint equations are the sufficient and necessary conditions to ensure that the input-output signals modifications remains undetectable by innovation-based and residual-based detectors, these conditions are stated in Theorem 8.6.1 in Section 8.6. The third and fourth constraints aim that the modified input-output signals satisfy the input-output signals characteristics. In order to illustrate the concept of misleading unauthorized observer, and more specifically Proposition 8.8.1, Section 8.9 shows a study case where the defending system applies Proposition 8.8.1 in order to mislead the unauthorized observer. For a general and in-depth understanding of optimization theory and its applications, see [19].

8.9. Illustration of MUO Through Simulations

In this section, simulations demonstrate how the defending system can mislead the unauthorized observer and maximize the corresponding estimation error by implementing Proposition 8.8.1. The defending system is a moving body in the XY plane, capable of free movement in both X and Y directions. The system is equipped with two sensors: a GPS to measure the position and an accelerometer to measure the acceleration. This scenario

illustrates an interesting case where the moving body seeks to defend itself by misleading the unauthorized observer, while the unauthorized observer believes that the body is being accurately monitored. This example illustrates both scenarios where the MUO defense can protect against the unauthorized observer, as explained in Section 8.5. In both cases, the input consists of acceleration measurements, and the output consists of GPS measurements. In the first scenario, the unauthorized observer gains access to the system network, as illustrated in Fig. 8.5. In the second scenario, the unauthorized observer has previously installed a GPS and an accelerometer, which the system later detects and modifies, as illustrated in Fig. 8.6. In the second scenario, the legit observer is a conceptual observer.

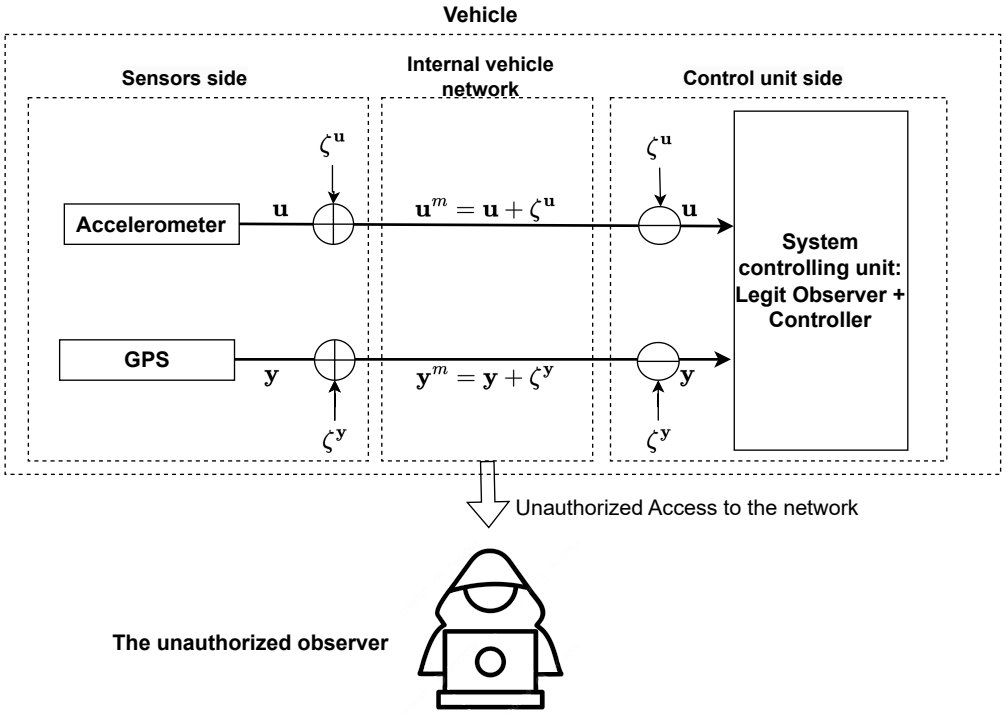

Figure 8.5: First scenario: The unauthorized observer has unauthorized access to the internal network of the vehicle, which transmits modified accelerometer and GPS measurements.

The system state consists of four components, the position on X and Y axes, and the velocity on X and Y axes, i.e. $\mathbf{x}_k = [p_k^x, p_k^y, v_k^x, v_k^y]^T$. The output vector is the GPS measurement vector, i.e. $\mathbf{y}_k = \left[p_k^{x,GPS}, p_k^{y,GPS}\right]^T$. The input vector is the acceleration measurement vector on X and Y axes, i.e. $\mathbf{u}_k = [a_k^x, a_k^y]^T$. The system's discrete-time model is given as follows:

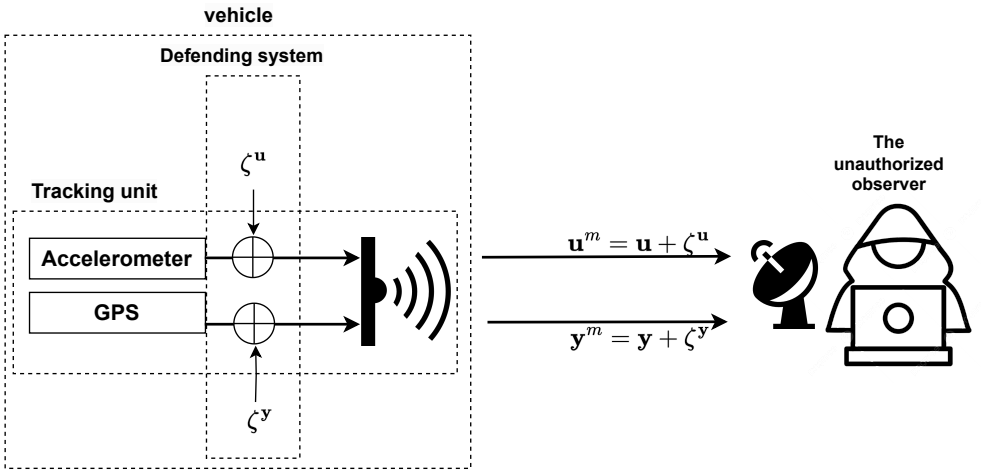

Figure 8.6: Second scenario: The unauthorized observer installs a tracking unit containing an accelerometer and GPS, equipped with a transmitter. The defending system detects this tracking unit and, instead of removing or damaging it, modifies its measurements to mislead the unauthorized observer.

$$\mathbf{x}_k = \begin{pmatrix} 1 & 0 & \Delta t & 0 \\ 0 & 1 & 0 & \Delta t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mathbf{x}_{k-1} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ \Delta t & 0 \\ 0 & \Delta t \end{pmatrix} \mathbf{u}_{k-1} + \mathbf{w}_{k-1}, \tag{8.9.1}$$

$$\mathbf{y}_k = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \mathbf{x}_k + \mathbf{w}_k^y, \tag{8.9.2}$$

where Δt is the sampling time, $\mathbf{w}_k = \left[0, 0, w_k^{a_x}\Delta t, w_k^{a_y}\Delta t\right]^T$, and $\mathbf{w}_k^y = \left[v_k^{x,GPS}, v_k^{y,GPS}\right]^T$. The noises $w_k^{a_x}, w_k^{a_y}$ are the accelerometer measurements noise, and $v_k^{x,GPS}, v_k^{y,GPS}$ are the GPS measurements noise. All of these noises are assumed to be uncorrelated zero-mean white random Gaussian signals with known covariance matrices.

8.9.1 Simulation Setup

The simulation is done for sampling time $\Delta t = 0.1$ s, and for $N^s = 100$ discrete time steps. We assume a circular true trajectory for one turn, by considering these true accelerations:

$$\begin{aligned} a_k^x &= 30\cos(\frac{2\pi}{N^s}k), \\ a_k^y &= 30\sin(\frac{2\pi}{N^s}k). \end{aligned}$$

The true state is calculated using the dynamic model while setting the noises to zero and starting from initial state $\mathbf{x}_0 = \left[-30\left(\frac{N^s\Delta t}{2\pi}\right)^2, 0, 0, -30\frac{N^s\Delta t}{2\pi}\right]^T$ in order to have a circular trajectory. We assume the worst-case security scenario, where the initial state is known by the unauthorized observer. The process noise comes from the accelerometer noise, which is set to have a standard deviation of 0.1 m/s^2, and the measurement noise comes from the GPS, which is set to have a standard deviation of 4 m.

In this simulation, the signals modifications start in the middle of simulation time, to show how the unauthorized observer correctly estimates the state until the mid-time and then starts to diverge. The optimization problem is solved with undetectability constraints, ensuring that the signals modifications are not detectable by innovation-based or residual-based detectors, and includes input-output signals verifications. Two types of input-output signals verifications are performed in the following subsections.

The optimization problem (8.8.1) involves maximizing a quadratic convex function subject to linear constraints. Therefore, instead of using a general nonlinear solver, we employ disciplined convex-concave programming (DCCP) [152], which is built on top of CVXPY, a domain-specific language for convex optimization embedded in Python [43]. The weight matrix is chosen to be identity $\mathbf{W} = \mathbf{I}$, in order to have the same weight for all states. The defender solves the optimization problem for a time window of $N = 20$, we choose this value inspired by the literature of the MPC, e.g. [10].

8.9.2 Bounds Verification Constraints

In this subsection, the defender adds constraints on the bounds of the accelerometer measurements. We assume that both the defender and the unauthorized observer know that the moving body can not have acceleration more than 30 m/s^2 in any direction, thus, these constraints are added when solving the optimization problem:

$$-30 \leq a_k^x \leq 30,$$
$$-30 \leq a_k^y \leq 30.$$

The results of this simulation are shown in Figs. 8.7, 8.8, 8.9, and 8.10. Fig. 8.7 shows the received (the modified) acceleration measurements by the unauthorized observer, where these measurements respect the acceleration bounds, and the modifications start at the midpoint of simulation time. Fig. 8.8 shows the true trajectory and the estimated trajectory by the unauthorized observer in the XY plane. The unauthorized observer can estimate the first half of the trajectory before the defending system begins signals modifications. Afterward, the observer's estimations start to diverge, achieving the goal of the defending system. Fig. 8.9 shows the true and estimated velocity estimation, demonstrating that the unauthorized observer correctly estimates the velocity in the first half of the time, and diverges after activating the defense system. We consider in this simulation that the unauthorized observer is using a $\boldsymbol{\chi}^2$ detector, and based on the innovation. Fig. 8.10 shows the $\boldsymbol{\chi}^2$ signal and the 99% confidence interval used as a threshold to decide if there are signals modifications. The value of the confidence interval can be found in $\boldsymbol{\chi}^2$ tables by locating the desired confidence level corresponding to the degrees of freedom [23], where our simulation, the $\boldsymbol{\chi}^2$ signal has

2 degrees of freedom (output dimension). Fig. 8.10 shows that the χ^2 signal does not exceed the threshold, thus the detector does not trigger an alarm. Moreover, the χ^2 signal has the same behaviour before and after starting signals modifications. This χ^2 signal corresponds to one realization; in another simulation, the signal will differ but maintain the same distribution characteristics. This variation occurs because each simulation run involves different realizations of sensors' noises. We observe non-smooth velocity estimates in Fig. 8.9, and discontinuities in the acceleration measurements at the midpoint in Fig. 8.7, which may indicate unusual behaviour. Therefore, in the next subsection, additional constraints on the evolution of the modified accelerometer measurements are incorporated into the optimization problem.

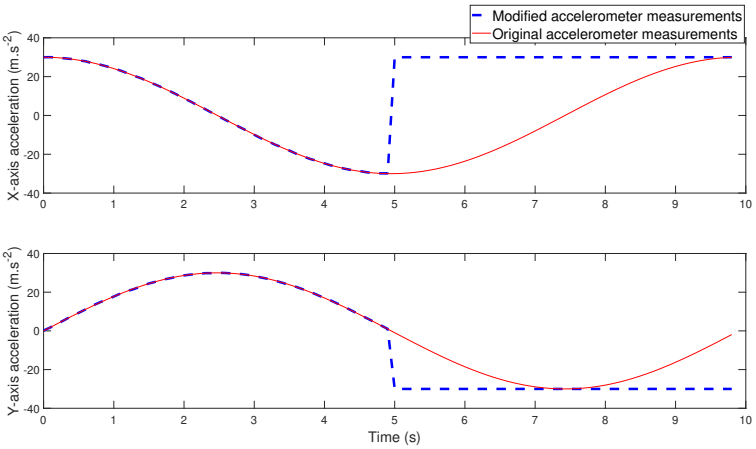

Figure 8.7: The modified accelerometer measurements, with bound constraints.

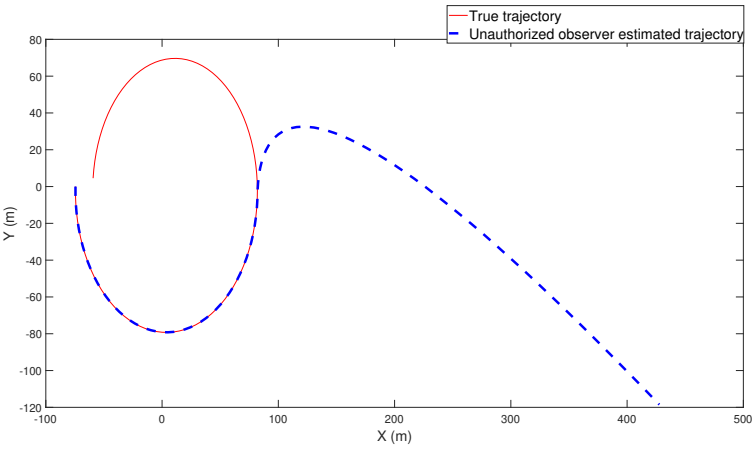

Figure 8.8: True trajectory and estimated trajectory by the unauthorized observer in the XY plane. The misleading injections are undetectable with bound constraints on the modified accelerometer measurements.

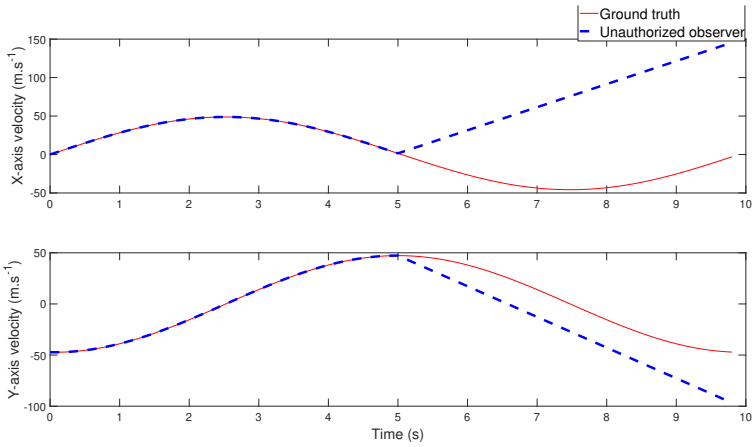

Figure 8.9: True velocity and estimated velocity by the unauthorized observer. The misleading injections are undetectable with bound constraints on the modified accelerometer measurements.

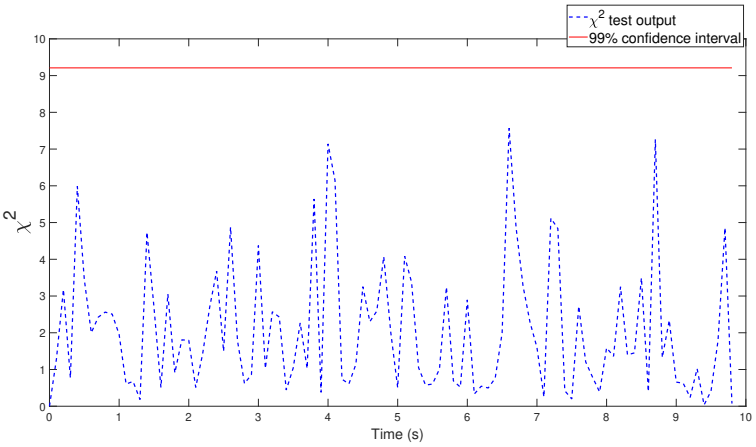

Figure 8.10: χ^2 test output for one realization. The misleading injections are undetectable with bound constraints on the modified accelerometer measurements.

8.9.3 Bounds and Evolution Verification Constraints

In this subsection, the defender adds constraints on both bounds and the evolution of accelerometer measurements. The additional constraints are:

$$-3 \leq a_{k+1}^x - a_k^x \leq 3,$$
$$-3 \leq a_{k+1}^y - a_k^y \leq 3.$$

The results of this simulation are shown in Figs. 8.11, 8.12, 8.13, and 8.14. These results demonstrate that adding constraints on the evolution of modified acceleration ensures the unauthorized observer's velocity estimates remain smooth and the received acceleration data remains continuous. Additionally, the undetectability criterion is still satisfied by the χ^2 detector, as shown in Fig. 8.14. These results demonstrate the benefits of solving the optimization problem for signals modifications. Constraints can be added to address any undesired behaviour in the modified input-output data. Additionally, the defending system can prioritize misleading the unauthorized observer about specific states by assigning more weight to those states.

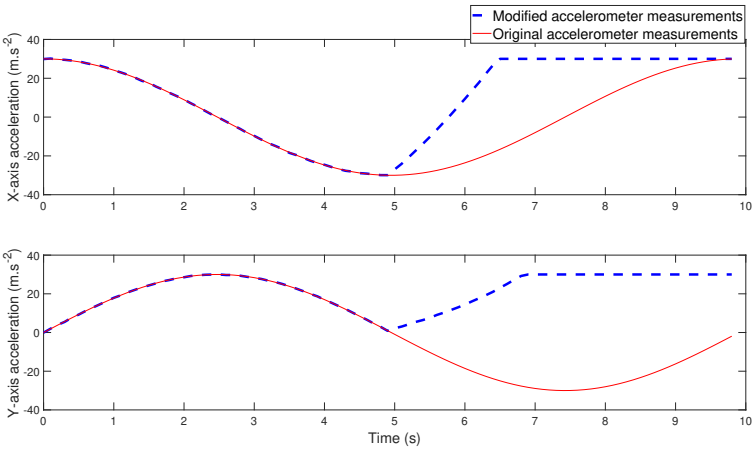

Figure 8.11: The modified accelerometer measurements, with bound and evolution constraints.

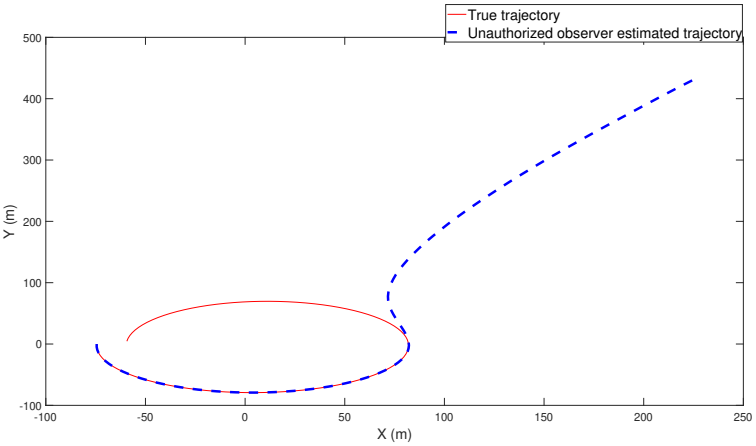

Figure 8.12: True trajectory and estimated trajectory by the unauthorized observer in the XY plane. The misleading injections are undetectable with bound and evolution constraints on the modified accelerometer measurements.

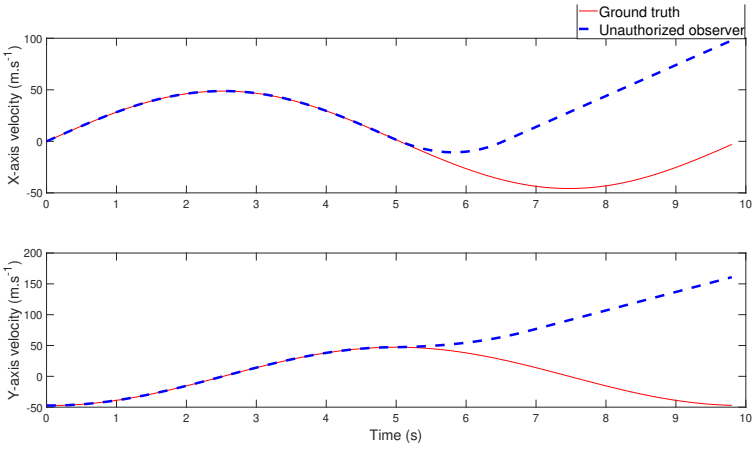

Figure 8.13: True velocity state and estimated velocity state by the unauthorized observer. The misleading injections are undetectable with bound and evolution constraints on the modified accelerometer measurements.

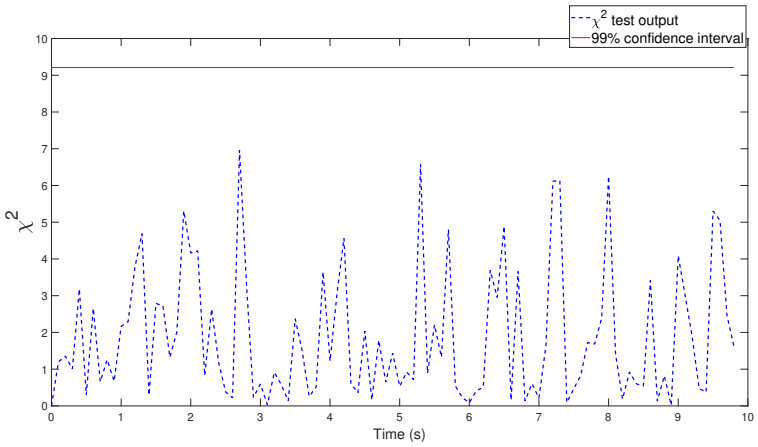

Figure 8.14: χ^2 test output for one realization. The misleading injections are undetectable with bound and evolution constraints on the modified accelerometer measurements.

Remark 8.9.1. *The purpose of the simulations in subsections 8.9.2 and 8.9.3 is to show how additional constraints can be incorporated into the optimization problem so that the modified input–output signals are less likely to appear as modified signals. The modified signals in subsection 8.9.3 are more natural than those in subsection 8.9.2, as a constraint is added on the evolution of the acceleration, avoiding a sudden jump in its value. As shown in Fig. 8.11, the acceleration gradually increases until it reaches the maximum bound, which is a natural behaviour. However, remaining constant at the maximum bound for a period of time may not appear very natural. This could be improved by adding further constraints or by designing a predefined trajectory and then finding the input–output data that leads the estimation to follow that trajectory. We do not go further into this study, as it is closer to trajectory planning and falls outside the scope of this work. The purpose of this simulation is to illustrate the concept of misleading.*

8.10. Conclusion

This chapter addressed the challenge of securing CPS against unauthorized observers who aim to estimate system states by eavesdropping on input-output signals. An active defense strategy is proposed, that involves modifications to input-output signals in order to mislead the unauthorized observer. The modifications should remain undetectable by innovation or residual-based detectors. Additionally, this chapter addressed the properties that the system must have to perform three specific types of misleading unauthorized observers: state-i misleading unauthorized observer, strongly misleading unauthorized observer, and state-i strongly misleading unauthorized observer. The modifications were found as solutions to an optimization problem constrained by the conditions that the modifications are undetectable and that the input-output signals received by the unauthorized observer are within certain bounds and satisfy the physical characteristics of these signals. The proposed solution was validated through simulations involving a moving body in the XY plane. The simulation results demonstrated that the defending system can successfully mislead the unauthorized observer, thereby enhancing the security of CPS against such threats.

This research opens new directions for developing active defense approaches against cyber-physical attacks, rather than relying solely on passive methods. Defending cyber-physical

systems will remain a crucial and growing area of research. It is therefore important that new defense methods are developed faster than new attack techniques.

Chapter 9

Conclusion and Perspectives

9.1. Summary of Contributions

This thesis investigated the challenges of state estimation and CPS security in systems subject to unknown input and cyber-physical attacks. The focus was primarily on navigation applications, where the reliability of sensor measurements and control signals is critical. Through a structured exploration of both attitude estimation under unknown input and defense against cyber-physical attacks, this work presented novel algorithms and theoretical insights aimed at enhancing the reliability and security of such systems. The results were organized into two complementary parts: the first addressed attitude estimation on SO(3) under unknown input, and the second focused on cyber-physical security for two navigation applications and active defense strategies.

Part I: Attitude Estimation on SO(3) Under Unknown Input. This part addressed the problem of attitude estimation on SO(3) under unknown input in three cases: 1) the unknown input affects only the state dynamics, 2) it affects only the output, and 3) it affects both. Each case corresponds to a problem with recognized significance in navigation applications.

- **Chapter 2** addressed the case where the unknown input affects only the state dynamics without direct feedthrough to the output. Two algorithms were developed, RTSKF-SO(3) and UMV-SO(3), for gyro-free attitude estimation, where the two algorithms treat the angular velocity as unknown input. Monte Carlo simulations and experimental data using a publicly available dataset validated the effectiveness of both algorithms, showing that both algorithms outperformed the static algorithm TRIAD.
- **Chapter 3** addressed the case where the unknown input affects only the output. The algorithm UMV-SO(3)-EA was developed for attitude estimation based on MARG sensors under unknown external acceleration. Monte Carlo simulations and experimental data using a publicly available dataset validated the effectiveness of UMV-SO(3)-EA, showing that it outperformed IEKF-SO(3) with adaptation.
- **Chapter 4** addressed the case where the unknown input affects both the state dy-

namics and the output. This chapter extended the scope of Chapter 3 to the joint estimation of position, velocity, and attitude based on MARG and position sensors. Monte Carlo simulations validated the algorithm, showing that PVA-SO(3) outperformed cascaded approaches.

Together, these contributions provided a comprehensive framework for attitude estimation on SO(3) under various unknown input scenarios.

Part II: Cyber-Physical Security for Navigation Applications and Active Defense Strategy. This part addressed the security of two different navigation problems and presented a novel concept in CPS security, the active defense strategy.

- **Chapter 6** addressed secure attitude estimation on SO(3) using MARG sensor under randomly occurring FDI attacks on accelerometer and magnetometer measurements. Monte Carlo simulations validated the effectiveness of secure-IEKF-SO(3), showing that it outperformed the standard IEKF-SO(3).
- **Chapter 7** studied the invariant zeros of ground vehicle lateral dynamics and analyzed the vulnerability to zero dynamics attacks. This chapter recommended that the output include both yaw rate and lateral acceleration to prevent such attacks.
- **Chapter 8** introduced the novel concept in CPS security, the active defense strategy. It proposed the MUO strategy, which aims to mislead an unauthorized observer. The defense strategy was formulated for general discrete-time linear systems and illustrated through a case study in ground vehicle dynamics.

9.2. Perspectives

Building on the contributions of this thesis, several research directions are possible. Three main directions for future work are presented below, with an explanation of their importance and the main challenges they present:

1. **Perspectives considering the generalization of the algorithms in Part I to more general group structures:** The algorithms presented in Part I are designed for attitude estimation on SO(3), which is a special case of Lie groups [1, 158]. An interesting direction for future work would be to extend these algorithms to more general Lie groups, allowing estimation under various types of unknown inputs. Thus, exploring estimation on Lie groups with unknown input. The unknown input could be the angular velocity, external acceleration, and potentially other unknown inputs that could be explored for practical applications. Here are some example of Lie groups that can be direct application when exploring estimation on general Lie groups:
    - SO(2) represents 2D rotations.
    - SE(2) represents 2D rotation and translation.
    - SE(3) represents 3D poses, including both translation and rotation.

- $\mathrm{SE}_2(3)$ is an extension of SE(3) that includes attitude, position, and velocity, as in [6].
- $\mathrm{SE}_\mathrm{p}(3)$ is a further extension, including $p-2$ landmark positions, which can be estimated from vision data, as described in [21].
- In [24], the state is represented on a Lie group that includes attitude, velocity, position, and magnetic field.

Therefore, extending the unknown input filtering problem to general Lie groups could lead to a wide range of applications. This generalization presents challenges related to the complexity of Lie group operations and their associated Lie algebras.

2. **Perspectives considering secure attitude estimation on SO(3):** While a very specific case was addressed in Chapter 6, which considered secure attitude estimation on SO(3) under randomly occurring FDI attacks on accelerometer and magnetometer measurements, several perspectives can be considered. It is hoped that this work will serve as a starting point for an important research direction on secure estimation on SO(3), due to the importance of attitude estimation in critical navigation applications such as aerial vehicles. The security of systems lying on SO(3) has not been addressed in the literature before. Possible perspectives are:
   - Designing secure estimation algorithms on SO(3) for cases where FDI attacks occur on gyroscope measurements.
   - Considering different types of attack, not only randomly occurring FDI attacks.
   - Investigate the possibility of undetectable attacks on systems lying on SO(3), such as covert and zero dynamics attacks.

   The main challenge in this direction is that the current literature on CPS security generally assumes that the system state belongs to a vector space. Extending these methods to SO(3) is challenging because the operators and structure on SO(3) differ significantly from those of vector spaces.

3. **Perspective on active defense strategies:** Traditional defenses in CPS often focus on passive strategies, such as preventing attacks (e.g., encryption), detecting them (e.g., anomaly detection), or ensuring the system can tolerate their effects (resilience). An important direction for future research lies in the development of active defense strategies. Chapter 8 explored one such approach against an unauthorized observer, namely the MUO strategy. Future work could consider different active defense mechanisms tailored to various types of attacks, based on taking actions rather than relying solely on passive responses. This aligns with the idea that "the best defense is a good offense" [179]. While such concepts have been widely studied in military and strategic domains, they remain underexplored in the context of CPS security. It is hoped that MUO will open the door for further research on active defense strategies.

   Developing active defense strategies in CPS presents several challenges, as this is new explored concept in this context. It involves not only theoretical development but also a deeper understanding of real-world incidents in industrial systems. Inspiration may

need to be drawn from other domains where active defense is more common, such as cybersecurity in information technology and strategic studies.

In addition to the previous perspectives, which involve significant challenges, several other directions represent more straightforward extensions of this thesis and are of practical importance. These aspects were not addressed in this thesis primarily due to time constraints related to their development and implementation. Nevertheless, we believe that the algorithms and studies developed in this thesis provide a solid foundation that makes these extensions relatively easy to achieve.

1. **Perspectives considering the attitude estimation on SO(3) under unknown input:**

   - The gyro-free attitude estimation algorithms in Chapter 2 can be extended to different types of output, such as vision data from a camera. The vision data are used for the correction step for attitude estimation in some works, like [20, 21, 22].
   - Extending the MARG sensor models to include sensor biases is an important direction for future work. Bias estimation can be solved by applying the UIF techniques adopted in Part I. Another approach is to augment the state with the sensor biases, assuming these biases are approximately constant between steps with some process noise, as proposed in [59, 146, 162].
   - Considering different types of unknown input, such as magnetic disturbances, which can exist in many environments, such as industrial ones. In this case, the derivation may follow a similar structure to the one used for external accelerations in Chapter 3.
   - In the work presented in [24], the magnetic field is included as part of the state, alongside the position, velocity, and attitude states. The magnetic field dynamics in this approach include the magnetic field gradient as a known input. A possible direction for future work is to extend the PVA-SO(3) framework in Chapter 4 to include the magnetic field in the state, while treating the gradient as an unknown input.

2. **Perspective considering ground vehicle security:** In Chapter 7, the analysis addressed zero dynamics attacks against lateral dynamics, where the attacker injects undetectable terms into the input of the system. Two straightforward perspectives are:

   - Investigate zero dynamics attacks against other vehicle dynamics, like the longitudinal dynamics.
   - Investigate the case where the attacker tries to design undetectable attacks by injecting both input and output signals, such as covert attacks.

Bibliography

[1] H. Abbaspour and M. Moskowitz. *Basic Lie Theory*. World Scientific, 2007. DOI: 10.1142/6462.

[2] Z. Abdollahi Biron, S. Dey, and P. Pisu. "Real-time detection and estimation of denial of service attack in connected vehicle systems". In: *IEEE Transactions on Intelligent Transportation Systems* 19.12 (2018), pp. 3893–3902.

[3] S. Amin, G. A. Schwartz, and S. Shankar Sastry. "Security of interdependent and identical networked control systems". In: *Automatica* 49.1 (2013), pp. 186–192.

[4] F. Aslam and M. F. Haydar. "Nonlinear H ∞ filtering on the special orthogonal group SO(3) using vector directions". In: *IEEE Control Systems Letters* 6 (2022), pp. 2599–2604.

[5] A. Barrau and S. Bonnabel. "Intrinsic filtering on Lie groups with applications to attitude estimation". In: *IEEE Transactions on Automatic Control* 60.2 (2015), pp. 436–449.

[6] A. Barrau and S. Bonnabel. "The invariant extended Kalman filter as a stable observer". In: *IEEE Transactions on Automatic Control* 62.4 (2017), pp. 1797–1812.

[7] P. Batista. "GES long baseline navigation with unknown sound velocity and discrete-time range measurements". In: *IEEE Transactions on Control Systems Technology* 23.1 (2015), pp. 219–230.

[8] BBC News. *GPS jamming and spoofing: Why is my location wrong?* 2024. URL: https://www.bbc.com/news/world-middle-east-68734689.

[9] F. Bejarano, L. Fridman, and A. Poznyak. "Exact state estimation for linear systems with unknown inputs based on hierarchical super-twisting algorithm". In: *International Journal of Robust and Nonlinear Control* 17.18 (2007), pp. 1734–1753.

[10] A. Bemporad, M. Morari, V. Dua, and E. N. Pistikopoulos. "The explicit linear quadratic regulator for constrained systems". In: *Automatica* 38.1 (2002), pp. 3–20.

[11] S. Berkane, A. Abdessameud, and A. Tayebi. "Hybrid attitude and gyro-bias observer design on SO(3)". In: *IEEE Transactions on Automatic Control* 62.11 (2017), pp. 6044–6050.

[12] D. Bernstein. *Matrix mathematics: theory, facts, and formulas*. 2. ed. Princeton University Press, 2009.

[13] S. P. Bhat and D. S. Bernstein. "A topological obstruction to continuous global stabilization of rotational motion and the unwinding phenomenon". In: *Systems & Control Letters* 39.1 (2000), pp. 63–70.

[14] R. A. Biroon, Z. A. Biron, and P. Pisu. "False data injection attack in a platoon of CACC: real-time detection and isolation with a PDE approach". In: *IEEE Transactions on Intelligent Transportation Systems* 23.7 (2022), pp. 8692–8703.

[15] T. Bonargent, T. Menard, E. Pigeon, and O. Gehan. "Observer and first-order low-pass filter based attitude estimation for rigid bodies subject to external acceleration". In: *IEEE 58th Conference on Decision and Control (CDC)*. Nice, France, 2019, pp. 629–634.

[16] S. Bonnabel and A. Barrau. "The geometry of navigation problems". In: *IEEE Transactions on Automatic Control* 68.2 (2023), pp. 689–704.

[17] I. Boukabou, N. Kaabouch, and D. Rupanetti. "Cybersecurity challenges in UAV systems: IEMI attacks targeting inertial measurement units". In: *Drones* 8.12 (2024), p. 738.

[18] G. Bourmaud, R. Mégret, M. Arnaudon, and A. Giremus. "Continuous-discrete extended Kalman filter on matrix Lie groups using concentrated Gaussian distributions". In: *Journal of Mathematical Imaging and Vision* 51.1 (2015), pp. 209–228.

[19] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[20] M. Brossard, S. Bonnabel, and J.-P. Condomines. "Unscented Kalman filtering on Lie groups". In: *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. Vancouver, BC, 2017, pp. 2485–2491.

[21] M. Brossard, S. Bonnabel, and A. Barrau. "Invariant Kalman filtering for visual inertial SLAM". In: *IEEE 21st International Conference on Information Fusion (FUSION)*. Cambridge, 2018, pp. 2021–2028.

[22] M. Brossard, S. Bonnabel, and A. Barrau. "Unscented Kalman filter on Lie groups for visual inertial odometry". In: *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. Madrid, 2018, pp. 649–655.

[23] B. Brumback and M. Srinath. "A Chi-square test for fault-detection in Kalman filters". In: *IEEE Transactions on Automatic Control* 32.6 (1987), pp. 552–554.

[24] D. Caruso, A. Eudes, M. Sanfourche, D. Vissiere, and G. L. Besnerais. "Magneto-visual-inertial dead-reckoning: improving estimation consistency by invariance". In: *IEEE 58th Conference on Decision and Control (CDC)*. Nice, France, 2019, pp. 7923–7930.

[25] M. Caruso, A. M. Sabatini, M. Knaflitz, M. Gazzoni, U. D. Croce, and A. Cereatti. "Orientation estimation through magneto-inertial sensor fusion: a heuristic approach for suboptimal parameters tuning". In: *IEEE Sensors Journal* 21.3 (2021), pp. 3408–3419.

[26] M. Caruso, A. M. Sabatini, D. Laidig, T. Seel, M. Knaflitz, U. Della Croce, and A. Cereatti. "Analysis of the accuracy of ten algorithms for orientation estimation using inertial and magnetic sensing under optimal conditions: one size does not fit all". In: *Sensors* 21.7 (2021), p. 2543.

[27] A. Cecilia, D. Astolfi, G. Casadei, R. Costa-Castelló, and D. Nešić. "A masking protocol for private communication and attack detection in nonlinear observers". In: *IEEE 62nd Conference on Decision and Control (CDC)*. Singapore, Singapore, 2023, pp. 7495–7500.

[28] X.-H. Chang, Y. Liu, and M. Shen. "Resilient control design for lateral motion regulation of intelligent vehicle". In: *IEEE/ASME Transactions on Mechatronics* 24.6 (2019), pp. 2488–2497.

[29] A. Chattopadhyay and U. Mitra. "Security against false data-injection attack in cyber-physical systems". In: *IEEE Transactions on Control of Network Systems* 7.2 (2020), pp. 1015–1027.

[30] F. Cheli, E. Sabbioni, M. Pesce, and S. Melzi. "A methodology for vehicle sideslip angle identification: comparison with experimental data". In: *Vehicle System Dynamics* 45.6 (2007), pp. 549–563.

[31] B.-C. Chen and F.-C. Hsieh. "Sideslip angle estimation using extended Kalman filter". In: *Vehicle System Dynamics* 46.sup1 (2008), pp. 353–364.

[32] T. Chen, A. Cecilia, D. Astolfi, L. Wang, Z. Liu, and H. Su. "Chaotic masking protocol for secure communication and attack detection in remote estimation of cyber-physical systems". In: *4th Conference on Modelling, Identification and Control of Nonlinear Systems (MICNON)*. Lyon, France, 2024.

[33] Y. Chen, S. Kar, and J. M. F. Moura. "Optimal attack strategies subject to detection constraints against cyber-physical systems". In: *IEEE Transactions on Control of Network Systems* 5.3 (2018), pp. 1157–1168.

[34] M. S. Chong, H. Sandberg, and A. M. Teixeira. "A tutorial introduction to security and privacy for cyber-physical systems". In: *IEEE 18th European Control Conference (ECC)*. Naples, Italy, 2019, pp. 968–978.

[35] M. S. Chong, M. Wakaiki, and J. P. Hespanha. "Observability of linear systems under adversarial attacks". In: *IEEE American Control Conference (ACC)*. Chicago, IL, USA, 2015, pp. 2439–2444.

[36] A. Chulliat, W. Brown, P. Alken, C. Beggan, M. Nair, G. Cox, A. Woods, S. Macmillan, B. Meyer, and M. Paniccia. *The US/UK World Magnetic Model for 2020–2025: Technical Report*. Tech. rep. NOAA National Centers for Environmental Information (NCEI), 2020.

[37] CNN News. *Air Force: Moisture caused $1.4 billion bomber crash*. 2008. URL: https://web.archive.org/web/20080610054520/http://www.cnn.com/2008/US/06/06/crash.ap/index.html.

[38] J. L. Crassidis, F. L. Markley, and Y. Cheng. "Survey of nonlinear attitude estimation methods". In: *Journal of Guidance, Control, and Dynamics* 30.1 (2007), pp. 12–28.

[39] D. C. Daniel and K. L. Herbig. "Propositions on military deception". In: *Journal of Strategic Studies* 5.1 (1982), pp. 155–177.

[40] M. Darouach and M. Zasadzinski. "Unbiased minimum variance estimation for systems with unknown exogenous inputs". In: *Automatica* 33.4 (1997), pp. 717–719.

[41] M. Darouach, M. Zasadzinski, and M. Boutayeb. "Extension of minimum variance estimation for systems with unknown inputs". In: *Automatica* 39.5 (2003), pp. 867–876.

[42] C. De Persis and P. Tesi. "Input-to-state stabilizing control under denial-of-service". In: *IEEE Transactions on Automatic Control* 60.11 (2015), pp. 2930–2944.

[43] S. Diamond and S. Boyd. "CVXPY: A Python-embedded modeling language for convex optimization". In: *Journal of Machine Learning Research* 17.83 (2016), pp. 1–5.

[44] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty. "A systems and control perspective of CPS security". In: *Annual Reviews in Control* 47 (2019), pp. 394–411.

[45] D. Ding, Z. Wang, Q.-L. Han, and G. Wei. "Security control for discrete-time stochastic nonlinear systems subject to deception attacks". In: *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 48.5 (2018), pp. 779–789.

[46] P. Dixon, M. Best, and T. Gordon. "An extended adaptive Kalman filter for real-time state estimation of vehicle handling dynamics". In: *Vehicle System Dynamics* 34.1 (2000), pp. 57–75.

[47] M. Doumiati, A. C. Victorino, A. Charara, and D. Lechner. "Onboard real-time estimation of vehicle lateral tire–road forces and sideslip angle". In: *IEEE/ASME Transactions on Mechatronics* 16.4 (2011), pp. 601–614.

[48] E. Evangelisti, ed. *Controllability and observability*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

[49] F. Fakhfakh, M. Tounsi, and M. Mosbah. "Cybersecurity attacks on CAN bus based vehicles: a review and open challenges". In: *Library Hi Tech* 40.5 (2022), pp. 1179–1203.

[50] B. Fan, Q. Li, and T. Liu. "Improving the accuracy of wearable sensor orientation using a two-step complementary filter with state machine-based adaptive strategy". In: *Measurement Science and Technology* 29.11 (2018), p. 115104.

[51] H. Fang, R. De Callafon, and J. Cortés. "Simultaneous input and state estimation for nonlinear systems with applications to flow field estimation". In: *Automatica* 49.9 (2013), pp. 2805–2812.

[52] H. Fang, R. De Callafon, and P. Franks. "Smoothed estimation of unknown inputs and states in dynamic systems with application to oceanic flow field reconstruction". In: *International Journal of Adaptive Control and Signal Processing* 29.10 (2015), pp. 1224–1242.

[53] H. Fang, T. Srivas, R. De Callafon, and M. Haile. "Ensemble-based simultaneous input and state estimation for nonlinear dynamic systems with application to wildfire data assimilation". In: *Control Engineering Practice* 63 (2017), pp. 104–115.

[54] F. Farivar, M. S. Haghighi, A. Jolfaei, and S. Wen. "Covert attacks through adversarial learning: study of lane keeping attacks on the safety of autonomous vehicles". In: *IEEE/ASME Transactions on Mechatronics* 26.3 (2021), pp. 1350–1357.

[55] F. Farokhi, I. Shames, and N. Batterham. "Secure and private control using semi-homomorphic encryption". In: *Control Engineering Practice* 67 (2017), pp. 13–20.

[56] H. Fawzi, P. Tabuada, and S. Diggavi. "Secure estimation and control for cyber-physical systems under adversarial attacks". In: *IEEE Transactions on Automatic Control* 59.6 (2014), pp. 1454–1467.

[57] R. M. Ferrari and A. M. Teixeira. "Detection and isolation of replay attacks through sensor watermarking". In: *IFAC-PapersOnLine* 50.1 (2017), pp. 7363–7368.

[58] H. Fourati and D. Belkhiat, eds. *Multisensor attitude estimation: fundamental concepts and applications*. CRC Press, 2016.

[59] H. Fourati, N. Manamanni, L. Afilal, and Y. Handrich. "Posture and body acceleration tracking by inertial and magnetic sensing: Application in behavioral analysis of free-

ranging animals". en. In: *Biomedical Signal Processing and Control* 6.1 (2011), pp. 94–104.

[60] H. Fourati, N. Manamanni, L. Afilal, and Y. Handrich. "Complementary observer for body segments motion capturing by inertial and magnetic sensors". In: *IEEE/ASME Transactions on Mechatronics* 19.1 (2014), pp. 149–157.

[61] B. Friedland. "Treatment of bias in recursive filtering". In: *IEEE Transactions on Automatic Control* 14.4 (1969), pp. 359–367.

[62] R. M. Gerdes, C. Winstead, and K. Heaslip. "CPS: an efficiency-motivated attack against autonomous vehicular transportation". In: *29th Annual Computer Security Applications Conference*. New Orleans Louisiana USA: ACM, 2013, pp. 99–108.

[63] M. Ghaderi, K. Gheitasi, and W. Lucia. "A blended active detection strategy for false data injection attacks in cyber-physical systems". In: *IEEE Transactions on Control of Network Systems* 8.1 (2021), pp. 168–176.

[64] T. Gillespie. *Fundamentals of vehicle dynamics, 2nd edition*. 2nd. Warrendale: SAE Internationals, 2021.

[65] S. Gillijns and B. De Moor. "Unbiased minimum-variance input and state estimation for linear discrete-time systems". In: *Automatica* 43.1 (2007), pp. 111–116.

[66] S. Gillijns and B. De Moor. "Unbiased minimum-variance input and state estimation for linear discrete-time systems with direct feedthrough". In: *Automatica* 43.5 (2007), pp. 934–937.

[67] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell. "A survey of physics-based attack detection in cyber-physical systems". In: *ACM Computing Surveys* 51.4 (2019), pp. 1–36.

[68] M. S. Grewal, L. R. Weill, and A. P. Andrews. *Global positioning systems, inertial navigation, and integration*. 1st ed. Wiley, 2007.

[69] H. F. Grip, T. I. Fossen, T. A. Johansen, and A. Saberi. "Attitude estimation using biased gyro and vector measurements with time-varying reference vectors". In: *IEEE Transactions on Automatic Control* 57.5 (2012), pp. 1332–1338.

[70] S. Guo, J. Wu, Z. Wang, and J. Qian. "Novel MARG-sensor orientation estimation algorithm using fast Kalman filter". In: *Journal of Sensors* 2017 (2017), pp. 1–12.

[71] X. Guo, A. S. Leong, and S. Dey. "Distortion outage minimization in distributed estimation with estimation secrecy outage constraints". In: *IEEE Transactions on Signal and Information Processing over Networks* 3.1 (2017), pp. 12–28.

[72] Z. Guo, D. Shi, K. H. Johansson, and L. Shi. "Optimal linear cyber-attack on remote state estimation". In: *IEEE Transactions on Control of Network Systems* 4.1 (2017), pp. 4–13.

[73] Z. Guo, D. Shi, K. H. Johansson, and L. Shi. "Worst-case innovation-based integrity attacks with side information on remote state estimation". In: *IEEE Transactions on Control of Network Systems* 6.1 (2019), pp. 48–59.

[74] Haiping Du, Nong Zhang, and Guangming Dong. "Stabilizing vehicle lateral dynamics with considerations of parameter uncertainties and control saturation through robust yaw control". In: *IEEE Transactions on Vehicular Technology* 59.5 (2010), pp. 2593–2597.

[75] M. Hamer and R. D'Andrea. "Self-calibrating ultra-wideband network supporting multi-robot localization". In: *IEEE Access* 6 (2018), pp. 22292–22304.

[76] R. Hamrah, R. R. Warier, and A. K. Sanyal. "Finite-time stable estimator for attitude motion in the presence of bias in angular velocity measurements". In: *Automatica* 132 (2021), p. 109815.

[77] E. Hashemi, M. Pirani, A. Khajepour, and A. Kasaiezadeh. "A comprehensive study on the stability analysis of vehicle dynamics with pure/combined-slip tyre models". In: *Vehicle System Dynamics* 54.12 (2016), pp. 1736–1761.

[78] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, and K. C. Sou. "Efficient computations of a security index for false data attacks in power networks". In: *IEEE Transactions on Automatic Control* 59.12 (2014), pp. 3194–3208.

[79] T. Hiller, Z. Pentek, J.-T. Liewald, A. Buhmann, and H. Roth. "Origins and mechanisms of bias instability noise in a three-axis mode-matched MEMS gyroscope". In: *Journal of Microelectromechanical Systems* 28.4 (2019), pp. 586–596.

[80] Z. Hong, X. Li, Z. Wen, L. Zhou, H. Chen, and J. Su. "ESP spoofing: covert Acoustic attack on MEMS gyroscopes in vehicles". In: *IEEE Transactions on Information Forensics and Security* 17 (2022), pp. 3734–3747.

[81] R. Horn and C. Johnson. *Matrix Analysis*. Cambridge University Press, 2012.

[82] C.-S. Hsieh. "Robust two-stage Kalman filters for systems with unknown inputs". In: *IEEE Transactions on Automatic Control* 45.12 (2000), pp. 2374–2378.

[83] C.-S. Hsieh. "Extension of unbiased minimum-variance input and state estimation for systems with unknown inputs". In: *Automatica* 45.9 (2009), pp. 2149–2153.

[84] C.-S. Hsieh. "A unified framework for state estimation of nonlinear stochastic systems with unknown inputs". In: *IEEE 9th Asian Control Conference (ASCC)*. Istanbul, Turkey, 2013, pp. 1–6.

[85] C.-S. Hsieh. "State estimation for nonlinear systems with unknown inputs using SDC factorization". In: *IEEE Region 10 International Conference (TENCON)*. Macao, 2015, pp. 1–6.

[86] C.-S. Hsieh and D.-C. Liaw. "Unknown input filtering for nonlinear systems and its application to traffic state estimation". In: *7th IEEE Conference on Industrial Electronics and Applications (ICIEA)*. Singapore, Singapore, 2012, pp. 1847–1852.

[87] C.-S. Hsieh. "State estimation for nonlinear systems with unknown inputs". In: *7th IEEE Conf. on Industrial Electronics and Applications (ICIEA)*. Singapore, Singapore, 2012, pp. 1533–1538.

[88] M.-D. Hua, P. Martin, and T. Hamel. "Stability analysis of velocity-aided attitude observers for accelerated vehicles". In: *Automatica* 63 (2016), pp. 11–15.

[89] R. Jiang, X. Liu, H. Wang, and S. S. Ge. "Secure estimation for attitude and heading reference systems under sparse attacks". In: *IEEE Sensors Journal* 19.2 (2019), pp. 641–649.

[90] T. A. Johansen, J. M. Hansen, and T. I. Fossen. "Nonlinear observer for tightly integrated inertial navigation aided by pseudo-range measurements". In: *Journal of Dynamic Systems, Measurement, and Control* 139.1 (2017), p. 011007.

[91] I. Jovanov and M. Pajic. "Sporadic data integrity for secure state estimation". In: *IEEE 56th Annual Conference on Decision and Control (CDC)*. Melbourne, Australia, 2017, pp. 163–169.

[92] Z. Ju, H. Zhang, X. Li, X. Chen, J. Han, and M. Yang. "A survey on attack detection and resilience for connected and automated vehicles: from vehicle dynamics

and control perspective". In: *IEEE Transactions on Intelligent Vehicles* 7.4 (2022), pp. 815–837.
[93] T. Kailath, A. Sayed, and B. Hassibi. *Linear estimation*. Prentice Hall, 2000.
[94] R. E. Kalman. "A new approach to linear filtering and prediction problems". In: *Journal of Basic Engineering* 82.1 (1960), pp. 35–45.
[95] A. Khazraei and M. Pajic. "Attack-resilient state estimation with intermittent data authentication". In: *Automatica* 138 (2022), p. 110035.
[96] A. Khosravian, J. Trumpf, R. Mahony, and C. Lageman. "Observers for invariant systems on Lie groups with biased input measurements and homogeneous outputs". In: *Automatica* 55 (2015), pp. 19–26.
[97] U. Kiencke and A. Daiß. "Observation of lateral vehicle dynamics". In: *Control Engineering Practice* 5.8 (1997), pp. 1145–1150.
[98] K. H. Kim, D. Kara, V. Paruchuri, S. Mohan, G. Kimberly, D. Osipychev, J. H. Kim, J. D. Eckhardt, and M. Pajic. "Insights on using deep learning to spoof inertial measurement units for stealthy attacks on uavs". In: *IEEE Military Communications Conference (MILCOM)*. IEEE. 2022, pp. 1065–1069.
[99] P. Kitanidis. "Unbiased minimum-variance linear state estimation". In: *Automatica* 23.6 (1987), pp. 775–778.
[100] C. Kwon, W. Liu, and I. Hwang. "Analysis and design of stealthy cyber attacks on unmanned aerial systems". In: *Journal of Aerospace Information Systems* 11.8 (2014), pp. 525–539.
[101] C. Kwon, S. Yantek, and I. Hwang. "Real-time safety assessment of unmanned aircraft systems against stealthy cyber attacks". In: *Journal of Aerospace Information Systems* 13.1 (2016), pp. 27–45.
[102] D. Laidig, M. Caruso, A. Cereatti, and T. Seel. "BROAD—A benchmark for robust inertial orientation estimation". In: *Data* 6.7 (2021), p. 72.
[103] J. K. Lee, E. J. Park, and S. N. Robinovitch. "Estimation of attitude and external acceleration using inertial sensor measurement during various dynamic conditions". In: *IEEE Transactions on Instrumentation and Measurement* 61.8 (2012), pp. 2262–2273.
[104] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey. "Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper". In: *IEEE Transactions on Automatic Control* 64.9 (2019), pp. 3732–3739.
[105] L. Li, H. Yang, Y. Xia, and H. Yang. "State estimation for linear systems with unknown input and random false data injection attack". In: *IET Control Theory & Applications* 13.6 (2019), pp. 823–831.
[106] Z. Lian, P. Shi, C.-C. Lim, and X. Yuan. "Fuzzy-model-based lateral control for networked autonomous vehicle systems under hybrid cyber-attacks". In: *IEEE Transactions on Cybernetics* 53.4 (2023), pp. 2600–2609.
[107] D. Lin, Q. Zhang, X. Chen, J. Qian, W. Yan, and S. Wang. "Quaternion Kalman filter for false data injection attacks". In: *IEEE Transactions on Circuits and Systems II: Express Briefs* 71.3 (2024), pp. 1501–1505.
[108] Q. Liu, J. Williamson, K. Li, W. Mohrman, Q. Lv, R. Dick, and L. Shang. "Gazelle: energy-efficient wearable analysis for running". In: *IEEE Transactions on Mobile Computing* 16.9 (2017), pp. 2531–2544.

[109] S. Liu, G. Wei, Y. Song, and Y. Liu. "Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks". In: *Neurocomputing* 207 (2016), pp. 708–716.
[110] S. Liu, G. Wei, Y. Song, and Y. Liu. "Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks". In: *Neurocomputing* 207 (2016), pp. 708–716.
[111] X. Liu, D. Bai, Y. Lv, R. Jiang, and S. S. Ge. "UKF-based vehicle pose estimation under randomly occurring deception attacks". In: *Security and Communication Networks* 2021 (2021). Ed. by S. Cimato, pp. 1–12.
[112] X. Liu, R. Jiang, H. Wang, and S. S. Ge. "Filter-based secure dynamic pose estimation for autonomous vehicles". In: *IEEE Sensors Journal* 19.15 (2019), pp. 6298–6308.
[113] Y. Liu and Y. Morgan. "Security against passive attacks on network coding system – A survey". In: *Computer Networks* 138 (2018), pp. 57–76.
[114] Y. Lu and M. Zhu. "Privacy preserving distributed optimization using homomorphic encryption". In: *Automatica* 96 (2018), pp. 314–325.
[115] S. O. H. Madgwick, A. J. L. Harrison, and R. Vaidyanathan. "Estimation of IMU and MARG orientation using a gradient descent algorithm". In: *2011 IEEE International Conference on Rehabilitation Robotics*. Zurich: IEEE, 2011, pp. 1–7.
[116] R. Mahony, T. Hamel, and J.-M. Pflimlin. "Nonlinear complementary filters on the special orthogonal group". In: *IEEE Transactions on Automatic Control* 53.5 (2008), pp. 1203–1218.
[117] A. Makni, H. Fourati, and A. Y. Kibangou. "Energy-aware adaptive attitude estimation under external acceleration for pedestrian navigation". In: *IEEE/ASME Transactions on Mechatronics* 21.3 (2016), pp. 1366–1375.
[118] A. Makni, H. Fourati, and A. Kibangou. "Adaptive Kalman filter for MEMS-IMU based attitude estimation under external acceleration and parsimonious use of gyroscopes". In: *IEEE European Control Conference (ECC)*. Strasbourg, France, 2014, pp. 1379–1384.
[119] K. Manandhar, X. Cao, F. Hu, and Y. Liu. "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter". In: *IEEE Transactions on Control of Network Systems* 1.4 (2014), pp. 370–379.
[120] P. Marantos, Y. Koveos, and K. J. Kyriakopoulos. "UAV state estimation using adaptive complementary filters". In: *IEEE Transactions on Control Systems Technology* 24.4 (2016), pp. 1214–1226.
[121] F. L. Markley. "Multiplicative vs. additive filtering for spacecraft attitude determination". In: *Dynamics and Control of Systems and Structures in Space* 467-474 (2004), p. 48.
[122] P. Martin and E. Salaün. "Design and implementation of a low-cost observer-based attitude and heading reference system". In: *Control Engineering Practice* 18.7 (2010), pp. 712–722.
[123] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada. "Secure state estimation against sensor attacks in the presence of noise". In: *IEEE Transactions on Control of Network Systems* 4.1 (2017), pp. 49–59.

[124] Y. Mo, R. Chabukswar, and B. Sinopoli. "Detecting integrity attacks on SCADA systems". In: *IEEE Transactions on Control Systems Technology* 22.4 (2014), pp. 1396–1407.

[125] Y. Mo and B. Sinopoli. "Secure control against replay attacks". In: *IEEE 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. Monticello, IL, USA, 2009, pp. 911–918.

[126] Y. Mo and B. Sinopoli. "False data injection attacks in control systems". In: *Preprints of the 1st workshop on Secure Control Systems*. Vol. 1. 2010.

[127] Y. Mo and B. Sinopoli. "On the performance degradation of cyber-physical systems under stealthy integrity attacks". In: *IEEE Transactions on Automatic Control* 61.9 (2016), pp. 2618–2624.

[128] Y. Mo, S. Weerakkody, and B. Sinopoli. "Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs". In: *IEEE Control Systems* 35.1 (2015), pp. 93–109.

[129] A. Mohammadi and H. Malik. "Vehicle lateral motion stability under wheel lockup attacks". In: *Proceedings Fourth International Workshop on Automotive and Autonomous Vehicle Security*. San Diego, CA, USA: Internet Society, 2022.

[130] A. Mohammadi, H. Malik, and M. Abbaszadeh. "Vehicle lateral motion dynamics under braking/ABS cyber-physical attacks". In: *IEEE Transactions on Information Forensics and Security* 18 (2023), pp. 4100–4115.

[131] K. Nam, S. Oh, H. Fujimoto, and Y. Hori. "Estimation of sideslip and roll angles of electric vehicles using lateral tire force sensors through RLS and Kalman filter approaches". In: *IEEE Transactions on Industrial Electronics* 60.3 (2013), pp. 988–1000.

[132] S. Narain, A. Ranganathan, and G. Noubir. "Security of GPS/INS based on-road location tracking systems". In: *2019 IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA, USA: IEEE, 2019, pp. 587–601.

[133] E. Nekouei, M. Pirani, H. Sandberg, and K. H. Johansson. "A randomized filtering strategy against inference attacks on active steering control systems". In: *IEEE Transactions on Information Forensics and Security* 17 (2022), pp. 16–27.

[134] J. Ning, J. Xu, K. Liang, F. Zhang, and E.-C. Chang. "Passive attacks against searchable encryption". In: *IEEE Transactions on Information Forensics and Security* 14.3 (2019), pp. 789–802.

[135] A. Olivares, J. Górriz, J. Ramírez, and G. Olivares. "Using frequency analysis to improve the precision of human body posture algorithms based on Kalman filters". In: *Computers in Biology and Medicine* 72 (2016), pp. 229–238.

[136] A. J. Padgaonkar, K. W. Krieger, and A. I. King. "Measurement of angular acceleration of a rigid body using linear accelerometers". In: *Journal of Applied Mechanics* 42.3 (1975), pp. 552–556.

[137] Z.-H. Pang, G.-P. Liu, D. Zhou, F. Hou, and D. Sun. "Two-channel false data injection attacks against output tracking control of networked systems". In: *IEEE Transactions on Industrial Electronics* 63.5 (2016), pp. 3242–3251.

[138] F. Pasqualetti, F. Dorfler, and F. Bullo. "Attack detection and identification in cyber-physical systems". In: *IEEE Transactions on Automatic Control* 58.11 (2013), pp. 2715–2729.

[139] F. Pasqualetti, F. Dorfler, and F. Bullo. "Control-theoretic methods for cyberphysical security: geometric principles for optimal cross-layer resilient control systems". In: *IEEE Control Systems* 35.1 (2015), pp. 110–127.

[140] R. Patton, P. Frank, and R. Clark, eds. *Fault diagnosis in dynamic systems: theory and application*. Prentice Hall, 1989.

[141] Z. Peng, Y. Zhang, G. Wen, J. Wang, and T. Huang. "Security analysis for autonomous ground vehicle under stealthy sensor attacks". In: *IEEE Transactions on Vehicular Technology* (2024), pp. 1–12.

[142] L. Pina and M. Botto. "Simultaneous state and input estimation of hybrid systems with unknown inputs". In: *Automatica* 42.5 (2006), pp. 755–762.

[143] R. Rajamani. *Vehicle dynamics and control*. 2nd ed. Mechanical engineering series. New York: Springer, 2012.

[144] H. Rehbinder and X. Hu. "Drift-free attitude estimation for accelerated rigid bodies". In: *Automatica* 40.4 (2004), pp. 653–659.

[145] "Rigid-body attitude control". In: *IEEE Control Systems* 31.3 (2011), pp. 30–51.

[146] A. M. Sabatini. "Quaternion-based extended Kalman filter for determining orientation by inertial and magnetic sensing". In: *IEEE Transactions on Biomedical Engineering* 53.7 (2006), p. 11.

[147] H. Sandberg, V. Gupta, and K. H. Johansson. "Secure networked control systems". In: *Annual Review of Control, Robotics, and Autonomous Systems* 5.1 (2022), pp. 445–464.

[148] T. Seel and S. Ruppin. "Eliminating the effect of magnetic disturbances on the inclination estimates of inertial sensors". In: *IFAC-PapersOnLine* 50.1 (2017), pp. 8798–8803. (Visited on 08/13/2025).

[149] G. Shaaban, H. Fourati, A. Kibangou, and C. Prieur. "Gyro-free Kalman filter with unknown inputs for SO(3)-based attitude estimation". In: *IEEE 13th International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. Nuremberg, Germany, 2023, pp. 1–6.

[150] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. M. Hamdi. "Review of prevention schemes for replay attack in vehicular Ad hoc networks (VANETs)". In: *IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP)*. Shanghai, China, 2020, pp. 394–398.

[151] J.-H. She, H. Kobayashi, Y. Ohyama, and X. Xin. "Disturbance estimation and rejection - an equivalent input disturbance estimator approach". In: *IEEE 43rd Conference on Decision and Control (CDC)*. Nassau, Bahamas, 2004, 1736–1741 Vol.2.

[152] X. Shen, S. Diamond, Y. Gu, and S. Boyd. "Disciplined convex-concave programming". In: *IEEE 55th Conference on Decision and Control (CDC)*. Las Vegas, NV, USA, 2016, pp. 1009–1014.

[153] H. Shim, J. Back, Y. Eun, G. Park, and J. Kim. "Zero-dynamics attack, variations, and countermeasures". In: *Security and Resilience of Control Systems: Theory and Applications*. Ed. by H. Ishii and Q. Zhu. Cham: Springer International Publishing, 2022, pp. 31–61.

[154] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava. "Non-invasive spoofing attacks for anti-lock braking systems". In: *Cryptographic Hardware and Embedded Systems -*

CHES. Ed. by G. Bertoni and J.-S. Coron. Vol. 8086. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 55–72.

[155] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada. "Secure state estimation for cyber-physical systems under sensor attacks: a satisfiability modulo theory approach". In: *IEEE Transactions on Automatic Control* 62.10 (2017), pp. 4917–4932.

[156] M. D. Shuster and S. D. Oh. "Three-axis attitude determination from vector observations". In: *Journal of Guidance, Control, and Dynamics* 4.1 (1981), pp. 70–77.

[157] R. S. Smith. "A decoupled feedback structure for covertly appropriating networked control systems". In: *IFAC Proceedings Volumes* 44.1 (2011), pp. 90–95.

[158] J. Sola, J. Deray, and D. Atchuthan. "A micro Lie theory for state estimation in robotics". In: *arXiv preprint arXiv:1812.01537* (2018).

[159] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim. "Rocking drones with intentional sound noise on gyroscopic sensors". In: *24th USENIX security symposium (USENIX Security 15)*. 2015, pp. 881–896.

[160] X. Song and W. Zheng. "A Kalman-filtering derivation of input and state estimation for linear discrete-time systems with direct feedthrough". In: *Automatica* 161 (2024), p. 111453.

[161] J. Stuelpnagel. "On the parametrization of the three-dimensional rotation group". In: *SIAM Review* 6.4 (1964), pp. 422–430.

[162] Y. S. Suh. "Orientation estimation using a quaternion-based indirect Kalman filter with adaptive estimation of external acceleration". In: *IEEE Transactions on Instrumentation and Measurement* 59.12 (2010), pp. 3296–3305.

[163] X. Sun, F. R. Yu, and P. Zhang. "A survey on cyber-security of connected and autonomous vehicles (CAVs)". In: *IEEE Transactions on Intelligent Transportation Systems* 23.7 (2022), pp. 6240–6259.

[164] S. Sundaram. *Fault-tolerant and secure control systems*. Univ. Waterloo, Waterloo, ON, Canada, Lecture Notes, 2012. 2012.

[165] C.-W. Tan, S. Park, K. Mostov, and P. Varaiya. "Design of gyroscope-free navigation systems". In: *ITSC 2001. 2001 IEEE Intelligent Transportation Systems. Proceedings (Cat. No.01TH8585)*. Oakland, CA, USA, 2001, pp. 286–291.

[166] D. Tazartes. "An historical perspective on inertial navigation systems". In: *2014 International Symposium on Inertial Sensors and Systems (ISISS)*. Laguna Beach, CA, USA: IEEE, 2014, pp. 1–5.

[167] 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*. Beijing China: ACM, 2012, pp. 55–64.

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

[169] The Guardian. *Team of hackers take remote control of Tesla Model S from 12 miles away*. 2016. URL: https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes.

[170] The Guardian. *Air France could face trial over 2009 crash of Rio–Paris flight*. 2019. URL: https://www.theguardian.com/world/2019/jul/17/air-france-could-face-trial-over-2009-crash-of-rio-paris-flight.

[171] The Guardian. *Thousands of flights to and from Europe affected by suspected GPS jamming*. 2024. URL: https://www.theguardian.com/business/2024/apr/22/thousands-of-flights-to-and-from-europe-affected-by-suspected-russian-jamming.

[172] The Telegraph. *Hacker remotely crashes Jeep from 10 miles away*. 2015. URL: https://www.telegraph.co.uk/news/worldnews/northamerica/usa/11754089/Hacker-remotely-crashes-Jeep-from-10-miles-away.html.

[173] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu. "Walnut: waging doubt on the integrity of mems accelerometers with acoustic injection attacks". In: *2017 IEEE European symposium on security and privacy (EuroS&P)*. IEEE. 2017, pp. 3–18.

[174] Y.-L. Tsai, T.-T. Tu, H. Bae, and P. Chou. "EcoIMU: a dual triaxial-accelerometer inertial measurement unit for wearable applications". In: *International Conference on Body Sensor Networks (BSN)*. Singapore, Singapore: IEEE, 2010, pp. 207–212.

[175] R. Valenti, I. Dryanovski, and J. Xiao. "Keeping a good attitude: A quaternion-based orientation filter for IMUs and MARGs". In: *Sensors* 15.8 (2015), pp. 19302–19330.

[176] H. C. A. Van Tilborg and S. Jajodia, eds. *Encyclopedia of Cryptography and Security*. Boston, MA: Springer US, 2011.

[177] N. Wang, R. Hamrah, A. K. Sanyal, and M. N. Glauser. "Geometric extended state observer on TSE(3) with fast finite-time stability: Theory and validation on a multi-rotor vehicle". In: *Aerospace Science and Technology* 155 (2024), p. 109596.

[178] J. S. Warner and R. G. Johnston. "GPS spoofing countermeasures". In: *Homeland Security Journal* 25.2 (2003), pp. 19–27.

[179] G. Washington. *The papers of George Washington. 4: 5. Retirement series April - December 1799 / W. W. Abbot, ed.* 1. publ. Charlottesville, Va: Univ. Press of Virginia, 1999.

[180] T. Yang, C. Murguia, M. Kuijper, and D. Nesic. "An unknown input multiobserver approach for estimation and control under adversarial attacks". In: *IEEE Transactions on Control of Network Systems* 8.1 (2021), pp. 475–486.

[181] T. Yang, C. Murguia, M. Kuijper, and D. Nešić. "A multi-observer based estimation framework for nonlinear systems under sensor attacks". In: *Automatica* 119 (2020), p. 109043.

[182] L. Yin, W. Xie, S. Wang, and V. Sreeram. "Simultaneous input and state estimation: From a unified least-squares perspective". In: *Automatica* 171 (2025), p. 111906.

[183] S. Yong, M. Zhu, and E. Frazzoli. "Simultaneous input and state estimation for linear discrete-time stochastic systems with direct feedthrough". In: *IEEE 52nd Conference on Decision and Control (CDC)*. Firenze, 2013, pp. 7034–7039.

[184] S. Yong, M. Zhu, and E. Frazzoli. "A unified filter for simultaneous input and state estimation of linear discrete-time stochastic systems". In: *Automatica* 63 (2016), pp. 321–329.

[185] F.-Q. You, F.-L. Wang, and S.-P. Guan. "Hybrid estimation of state and input for linear discrete time-varying systems: a game theory approach". In: *Acta Automatica Sinica* 34.6 (2008), pp. 665–669.

[186] A. Young. "Comparison of orientation filter Algorithms for realtime wireless inertial posture tracking". In: *2009 Sixth International Workshop on Wearable and Implantable Body Sensor Networks*. Berkeley, CA: IEEE, 2009, pp. 59–64.

[187] X. Yun, E. R. Bachmann, and R. B. McGhee. “A simplified quaternion-based algorithm for orientation estimation from Earth gravity and magnetic field measurements”. In: *IEEE Transactions on Instrumentation and Measurement* 57.3 (2008), pp. 638–650.

[188] H. Zhang and J. Wang. “Vehicle lateral dynamics control through AFS/DYC and robust gain-scheduling approach”. In: *IEEE Transactions on Vehicular Technology* 65.1 (2016), pp. 489–494.

[189] H. Zhang, X. Zhang, and J. Wang. “Robust gain-scheduling energy-to-peak control of vehicle lateral dynamics stabilisation”. In: *Vehicle System Dynamics* 52.3 (2014), pp. 309–340.

[190] X. Zhang, Z. Yan, and Y. Chen. “High-degree cubature Kalman filter for nonlinear state estimation with missing measurements”. In: *Asian Journal of Control* 24.3 (2022), pp. 1261–1272.

[191] Z. Zhou and J. Wu. “Cascaded indirect Kalman filters for land-vehicle attitude estimation with MARG sensors and GNSS observations”. In: *IEEE Transactions on Vehicular Technology* 70.4 (2021), pp. 3267–3282.

[192] J. Zou, H. Liu, C. Liu, X. Ren, and X. Wang. “Optimal privacy-preserving transmission schedule against eavesdropping attacks on remote state estimation”. In: *IEEE Control Systems Letters* 8 (2024), pp. 538–543.

Contributions to Navigation Under Unknown Input and Cyber-Physical Security

Abstract

This thesis contributes to state estimation on the special orthogonal group SO(3) under unknown input and to cyber-physical systems (CPS) security. Two challenges related to unknown input are addressed. The first is attitude estimation without relying on the gyroscope, due to its drawbacks such as high-power consumption. The second is the separation of Earth gravity and external acceleration from accelerometer measurements, as the former is needed for attitude estimation and the latter for position and velocity. Additionally, two security problems related to navigation applications are addressed: secure attitude estimation on SO(3) under randomly occurring false data injection attacks, and security analysis of the ground vehicle lateral model under zero dynamics attacks. Finally, the thesis proposes an active defense strategy called "misleading unauthorized observers", which targets attackers attempting unauthorized remote state estimation. This strategy introduces a new direction in CPS security based on active rather than traditional passive defenses.

Keywords: Navigation, Attitude/velocity/position estimation, Unknown input filtering, SO(3) group, Cyber-physical security, Active defense.

Résumé

Cette thèse contribue à l'estimation d'état sur le groupe spécial orthogonal SO(3) en présence d'entrées inconnues, et à la sécurité des systèmes cyber-physiques. Deux défis liés aux entrées inconnues sont abordés. Le premier concerne l'estimation de l'attitude sans gyroscope, notamment en raison d'inconvénients tels qu'une consommation énergétique élevée. Le second concerne la séparation entre la gravité terrestre, nécessaire à l'estimation de l'attitude, et l'accélération externe, nécessaire à l'estimation de la position et de la vitesse. Ces données sont issues de mesures d'accéléromètre. En outre, deux problématiques de sécurité liées aux applications de navigation sont étudiées : l'estimation sécurisée de l'attitude sur SO(3) en présence d'attaques par injection aléatoire de fausses données, et l'analyse de la sécurité du modèle latéral d'un véhicule terrestre en cas d'attaques liées aux zéros dynamiques. Enfin, cette thèse propose une stratégie de défense active, appelée « tromper les observateurs non autorisés », qui cible les attaquants tentant d'estimer sans autorisation l'état du système à distance. Cette approche introduit une nouvelle direction en matière de sécurité des systèmes cyber-physiques, fondée sur des mécanismes de défense actifs plutôt que passifs.

Mots-clés : Navigation, Estimation d'attitude/vitesse/position, Filtrage avec entrées inconnues, Groupe SO(3), Sécurité cyber-physique, Défense active.