1

Introduction

1.1 Background and Motivation

With the rapid development of sensor technologies, and due to increased density in integrated circuits predicted by Moore's law, the autonomous vehicle has become a fruitful area blending robotics, automation, computer vision, and intelligent transportation technologies. It has been reported that traditional automobile companies and startups plan to get their autonomous driving systems ready in the 2020s [Ross, 2017].

The US Department of Transportation's National Highway Traffic Safety Administration (NHTSA) defined five levels of autonomous driving, from manual driving (level 0), to driver assistance (level 1), to fully autonomous driving (level 5) (https://www.sae.org/standards/content/j3016_202104). As an inspiring example, the Audi A8, launched in 2017, is claimed to be "the world's first production automobile conditional automated at level 3," according to Audi AG. Nevertheless, some pessimistic voices have emerged, claiming that fully autonomous cars will not be developed as quickly as expected or are even unlikely. One of the pacesetters in fully autonomous driving technologies, Waymo LLC, has received resident complaints due to conflicts in driving behaviors between humans and autonomous vehicles.

Although it is still a long way to level 5 autonomy, there is high demand for the development of autonomous vehicles so that tasks related to logistics, environmental cleanup, public security, and much more can be automated. Among all the functional blocks in autonomous vehicles, the navigation system plays an irreplaceable role since the vehicle needs to be literally "in motion" for any particular task. Multimodal perception and state estimation are two coadjutant modules for vehicle navigation. There have been extensive research outcomes on these two

Multimodal Perception and Secure State Estimation for Robotic Mobility Platforms, First Edition.
Xinghua Liu, Rui Jiang, Badong Chen, and Shuzhi Sam Ge.

topics in autonomous vehicle navigation, but a few challenges still exist, motivated by which the in-depth studies in this book have been carried out:

- A modern pose estimation system contains multiple sensors to achieve accuracy and robustness. Appropriate sensor configurations, which combine the advantages of each sensor to benefit the whole estimation system, are distinct depending on the specific applications and requirements. Based on a particular sensor configuration, new theories and ideas are required for multi-sensor pose estimation, where states, measurements, and constraints are represented in a unified fusion framework.
- Due to the stealthiness of attacks, system operators usually cannot discover attacks in time, which may lead to severe economic damage and even the loss of human lives. Such incidents indicate that enhancing the security of the system is an urgent issue. Researchers have studied how we can securely estimate the state of a dynamical system from the controller's point of view based on a set of noisy and maliciously corrupted sensor measurements. In particular, researchers have focused on linear dynamical systems and have tried to understand how the system dynamics can be leveraged for security guarantees.

This book discusses the pose estimation problem for robotic mobility platforms using information from multiple sensors. The first part discusses different sensor configurations and introduces new sensor fusion algorithms and frameworks to minimize pose estimation errors. Those concepts and methods are extensively used in current state-of-the-art autonomous vehicles, and extensive experimental results have been provided to verify the algorithm performance on real robotic platforms. The second part focuses on the secure estimation problem in multi-sensor fusion, where attacks are considered and explicitly modeled in algorithm design. As this is a new topic that is at the primary stage of research, theoretical analysis and simulation results are shown in the related chapters.

1.2 Multimodal Pose Estimation for Vehicle Navigation

1.2.1 Multi-Senor Pose Estimation

Multi-sensor fusion is a typical solution where system dynamics, measurements, and constraints are fused consistently to increase estimation performance in terms of accuracy and robustness [Borges and Aldon, 2002, Ye et al., 2015, Teixeira et al., 2018]. Essentially, pose estimation can be considered as state estimation within a state space with a problem-dependent topological structure. Let us assume the following discrete state equation and output equation:

$$\mathbf{x}_k = \mathbf{f}(\mathbf{x}_{k-1}, \mathbf{u}_{k-1}) + \mathbf{w}_{k-1} \tag{1.1}$$

$$\mathbf{z}_k = \mathbf{h}(\mathbf{x}_k) + \mathbf{v}_k \tag{1.2}$$

where $\mathbf{x}_k$, $\mathbf{u}_{k-1}$, $\mathbf{z}_k$ denote the state, control input, and measurement, respectively; $\mathbf{f}(\cdot)$ and $\mathbf{h}(\cdot)$ are the C^∞ state equation and output equation; and $\mathbf{w}_{k-1}$ and $\mathbf{v}_k$ represent process and measurement noise.

Filtering and optimization are two frequently used data fusion frameworks for pose estimation. Filtering approaches propagate state vectors with their joint probability distributions along with time. The Kalman filter models the state and noise as Gaussian, which is not suitable for non-Gaussian or multimodal distributions. The particle filter and its variants [Van Der Merwe et al., 2001, Nummiaro et al., 2003] have been proposed to deal with non-linear and non-Gaussian systems, and the computation load of updating particle states proliferates with the sample number. The optimization-based approaches retain historical measurement and estimation as a graph such that they can be used for bundle adjustment or simultaneous localization and mapping (SLAM) [Grisetti et al., 2010]. The two commonly used frameworks are elaborated here.

Filtering-Based Approaches As shown in related work [Janabi-Sharifi and Marey, 2010, Koval et al., 2015, Bloesch et al., 2017], filters provide a probabilistic solution on pose estimation, which can be divided into two steps. First, the “prediction” step predicts states without current measurement, according to the state equation

$$\mathbb{P}(\mathbf{x}_k|\mathbf{z}_{1:k-1}) = \int \mathbb{P}(\mathbf{x}_k|\mathbf{x}_{k-1})\mathbb{P}(\mathbf{x}_{k-1}|\mathbf{z}_{1:k-1})\mathrm{d}\mathbf{x}_{k-1} \tag{1.3}$$

where $\mathbb{P}(\cdot|\cdot)$ denotes the conditional distribution, and specifically $\mathbb{P}(\mathbf{x}_k|\mathbf{x}_{k-1})$ is obtained from (1.1). Then, the probability distribution of the update can be obtained in the “correction” step, based on the output equation

$$\mathbb{P}(\mathbf{x}_k|\mathbf{z}_{1:k}) = \frac{\mathbb{P}(\mathbf{z}_k|\mathbf{x}_k)\mathbb{P}(\mathbf{x}_k|\mathbf{z}_{1:k-1})}{\mathbb{P}(\mathbf{z}_k|\mathbf{z}_{1:k-1})} \tag{1.4}$$

where $\mathbb{P}(\mathbf{z}_k|\mathbf{x}_k)$ is obtained from (1.2), and the constant denominator is

$$\mathbb{P}(\mathbf{z}_k|\mathbf{z}_{1:k-1}) = \int \mathbb{P}(\mathbf{z}_k|\mathbf{x}_k)\mathbb{P}(\mathbf{x}_k|\mathbf{z}_{1:k-1})\mathrm{d}\mathbf{x}_k \tag{1.5}$$

Optimization-Based Approaches Instead of using the filtering-based approaches, some other research [Leutenegger et al., 2015, Huang et al., 2017, Parisotto et al., 2018, Wang et al., 2018a] aims to minimize the user-defined cost function $J(\mathbf{x})$ such that

$$\mathbf{x}^* = \arg\min_{\mathbf{x}} J(\mathbf{x}) = \arg\min_{\mathbf{x}} \sum_{C} \mathbf{e}(\mathbf{z},\mathbf{h}(\mathbf{x}))^\top \boldsymbol{\Omega}\ \mathbf{e}(\mathbf{z},\mathbf{h}(\mathbf{x})) \tag{1.6}$$

where C denotes the cost items to be considered; the information matrix $\boldsymbol{\Omega}$ indicates the degree of confidence in the corresponding measurement; and the error function $\mathbf{e}(\mathbf{z},\mathbf{h}(\mathbf{x}))$ measures the difference between the ideal and actual measurement.

1.2.2 Pose Estimation with Constraints

Constraints[1] in pose estimation are helpful in increasing algorithm robustness and accuracy. For example, we may consider *motion constraints* (1.1), that limit the vehicle's pose change with time, and *road constraints*, which require the vehicle to stay on the road. Constraints in practical issues are mostly considered as soft to allow modeling errors and noise. We discuss constrained pose estimation from two perspectives.

Incorporating Constraints into Filtering Given the constraints $\mathbf{c}(\mathbf{x}_k) = \breve{\mathbf{c}}(\mathbf{x}_k) + \breve{\mathbf{z}}_k = \mathbf{0}$, where $\breve{\mathbf{z}}_k$ is a constant vector, the augmented output equation can be obtained to incorporate the constraints into measurements [Mourikis and Roumeliotis, 2007, Simon, 2010, Boada et al., 2017, Ramezani et al., 2017, Yang et al., 2017a, Shen et al., 2017]:

$$\begin{bmatrix} \mathbf{z}_k \\ \breve{\mathbf{z}}_k \end{bmatrix} = \begin{bmatrix} \mathbf{h}(\mathbf{x}_k) \\ -\breve{\mathbf{c}}(\mathbf{x}_k) \end{bmatrix} + \begin{bmatrix} \mathbf{v}_k \\ \breve{\mathbf{v}}_k \end{bmatrix} \tag{1.7}$$

where the covariance matrix of $\breve{\mathbf{v}}_k$ indicates the confidence in the soft constraints. With a prediction that remains the same, the correction step can be achieved by applying the augmented output equation.

In addition, we may first obtain the estimate without constraints $\hat{\mathbf{x}}_k$ and then project the unconstrained estimates toward the constraint states to get the final estimate $\hat{\mathbf{x}}_k^*$

$$\hat{\mathbf{x}}_k^* = \arg\min_{\mathbf{x}} \left[\mathbf{x} \ominus \hat{\mathbf{x}}_k\right]^\top \mathbf{W} \left[\mathbf{x} \ominus \hat{\mathbf{x}}_k\right] \text{ s.t. } \mathbf{c}(\mathbf{x}_k) \approx \mathbf{0} \tag{1.8}$$

where $\ominus$ is an operator indicating the difference between states and $\mathbf{W}$ is a positive-definite weighting matrix. For linear systems under linear constraints, if $\mathbf{x} \in \mathbb{R}^n$, the ordinary vector subtraction is selected as $\ominus$, leading to analytical solutions. Numerical methods are required to generalize the projection method to non-linear systems or with non-linear constraints. For particle filters, particle weights can be adjusted to reduce the influence of estimation results that do not satisfy the constraints.

Incorporating Constraints into Optimization For hard constraints, the method of Lagrange multipliers can be used to construct the corresponding non-constrained optimization problem. For soft constraints, one naive but effective way is to add

---

[1] Note that the constraints in this book, which are derived from physical principles or engineering assumptions, should be differentiated from the measurements, which are obtained from sensors.

the penalty functions to the cost function $J(\mathbf{x})$, such that

$$\mathbf{x}^* = \arg\min_{\mathbf{x}} \left(J(\mathbf{x}) + \sum_{C} \mathbf{c}^i(\mathbf{x})^\top \boldsymbol{\Omega}^i \mathbf{c}^i(\mathbf{x}) \right) \tag{1.9}$$

where $\mathbf{c}^i(\mathbf{x})$ denotes the i-th constraint to be considered; $\boldsymbol{\Omega}^i$ indicates the degree of confidence in the i-th constraint. Examples of related work can be found in [Estrada et al., 2005, Levinson et al., 2007, Lu et al., 2017, Hoang et al., 2017].

Besides the constraints discussed previously (so-called *state constraints* in the literature), *measurement constraints* can be seen in practice. One example would be the constant norm constraint on measurement vectors for translationally static but rotating magnetometers. Unfortunately, the current literature pays less attention to measurement constraints than state constraints. In Chapters 4 and 5, by presenting a unified representation containing state space and measurement space, both state constraints and measurement constraints are considered in the proposed geometric pose estimation framework.

1.2.3 Research Focus in Multimodal Pose Estimation

In the first part of this book, we focus primarily on two topics in designing new frameworks of multimodal pose estimation.

Toward Drift Reduction in Visual Odometry As low-cost sensors with abundant visual information, cameras are frequently seen in ground vehicles, where visual odometry (VO) has been widely used for autonomous vehicle pose estimation thanks to its constantly improving performance. However, several challenges still need to be resolved. Error accumulation or the so-called drift issue is a challenge preventing VO from being used in long-range navigation. The existing solutions for enhancing VO performance involve (i) improving VO components including feature detection, matching, outlier removal, and pose optimization; and (ii) seeking assistance from other approaches or databases [Shen et al., 2014] such as LIDAR [Zhang and Singh, 2015], global positioning systems (GPSs) [Agrawal and Konolige, 2006], digital maps [Jiang et al., 2017, Alonso et al., 2012], and inertial navigation systems (INS) [Bloesch et al., 2015, Mourikis and Roumeliotis, 2007, Lobo and Dias, 2003, Wang et al., 2014, Falquez et al., 2016, Leutenegger et al., 2015, Lupton and Sukkarieh, 2012, Forster et al., 2017, Piniés et al., 2007, Li and Mourikis, 2013, Santoso et al., 2017]. Benefiting from the self-contained property, many visual-inertial odometry (VIO) schemes have been proposed to reduce drift in VO. Loosely coupled methods [Mourikis and Roumeliotis, 2007, Falquez et al., 2016] fuse data at a higher level, where data from the inertial measurement unit (IMU) and VO are fused after being obtained; tightly coupled methods, which consider not only poses but features as state variables in estimation, generally achieve greater precision but also suffer from higher computational costs. There are two main streams in tightly coupled VIO: on the one hand, a filter-based method is proposed to estimate egomotion, camera extrinsic parameters, and the additive IMU biases in Bloesch et al. (2015). On the other hand, with optimization-based methods, pose estimation can be formulated as a non-linear least-square optimization problem that aims to minimize a cost function containing inertial error terms and reprojection error simultaneously. Leutenegger et al. (2015) have proposed an integration framework where the concepts of keyframes and marginalization are introduced to ensure real-time operation. In Forster et al. (2017), a preintegration scheme of inertial measurement between keyframes has been proposed, where a fused measurement model and error propagation expression have been derived such that the optimization could be achieved directly on-manifold. Yang and Shen (2017) have addressed the initialization and calibration problems on the fly for monocular VIO. Unfortunately, the existing methods still suffer from drift issues, which motivates us to eliminate rotation drift by introducing an absolute heading in pose estimation.

As for the deployment of orientations as supplementary information, gravity has been used as a vertical reference for vision and inertial sensor cooperation in structure from motion (SfM) methods, where the image horizon line can be determined [Lobo and Dias, 2003]. Saurer et al. (2017) have further proposed an egomotion estimation approach, where fewer point correspondences for relative motion estimation are needed by utilizing the gravity direction. To the best of the authors' knowledge, Chapter 2 of this book serves as the first attempt to discuss the heading reference-assisted pose estimation problem for ground vehicles.

Map-Aided Visual Dead-Reckoning Stereo visual odometry (SVO) and monocular visual odometry (MVO) are two popular forms of visual dead-reckoning in practice. The motion estimated from SVO drifts in six degrees of freedom, while the motion estimated from MVO drifts in seven degrees of freedom, with an additional scale drift. To correct the drift, loop closure detection, followed by a global bundle adjustment or graph optimization [Strasdat et al., 2010] step, is widely used, and impressive results have been achieved [Mur-Artal et al., 2015a]. Unfortunately, loops do not necessarily exist in practical driving conditions. But when loops do exist, the corrected motion is still a largely delayed result for the route before loop closure. Thus, the loop-closing method is not appropriate for applications where instantaneous decisions are desired, such as autonomous vehicles.

For MVO, another challenge is how to obtain the metric scale of the motion estimated from a monocular system. The most straightforward approach is to fuse information from the IMU, GPS, or other sensors [Nützi et al., 2011], which of course will increase the cost and complexity of the system. Another popular method to estimate the metric scale assumes that the camera is moving at a known fixed height over the ground [Song and Chandraker, 2014]. However, the result of this kind of method relies heavily on the accuracy of ground plane detection. Some other researchers propose to use objects with known sizes to give the absolute scale of monocular results [Davison, 2003]. Nevertheless, it is difficult to ensure that the objects appear and are detected in all frames.

To solve the drift and scale ambiguity challenge, we turn to freely available maps (such as OpenStreetMap [OSM] and Google Maps), which have plenty of information that can be used for localization. On the one hand, since street segments and the connectivity of roads can be intuitively expressed as nodes and edges of a graph model, a map can be represented by a directed graph, which is much simpler to work within a localization problem. In Brubaker et al. (2013), a graph-based representation of the map was defined, and a probabilistic map localization approach was proposed. They achieved an accuracy of 3 meters within a city-level road map by using VO measurements and OSM data as the only inputs. To reduce the high computational cost, a simplified approach that used wheel speed odometry instead of VO was proposed in Merriaux et al. (2015), and real-time performance was achieved. On the other hand, the geometric shape of road networks can be considered as a constraint to assist with position estimation. Senlet and Elgammal (2012) succeeded in localizing a mobile robot on sidewalks by using a combination of SVO and satellite map matching. Top-view images generated from stereo frames were matched with satellite maps to correct incremental drift. The shape-matching method was utilized to evaluate the alignment of different trajectories to the map in Floros et al. (2013), and a shape-matching process was considered as the measurement model of the Monte Carlo localization framework. Similarly, shape matching is also used in Chapter 3. However, there is a difference: we focus on monocular camera localization, while they worked on the stereo case. Thus, not only motion drift but also scale ambiguity are considered in Chapter 3.

1.3 Secure Estimation

1.3.1 Secure State Estimation under Cyber Attacks

Cyber attacks reduce the reliability of the system primarily by destroying the availability and integrity of sensor or actuator data. A deception attack is a typical network attack that is more difficult to be detected because an adversary can keep the attack hidden from an anomaly detector. A false data injection attack is a specific type of deception attack when the system model is known to the adversary. It is mentioned that an alternative way to achieve secure estimation is to treat the false data injection attack signal as unknown input. Although classical methods on unknown input can be used to solve some secure estimation problems, when the system suffers from an attack and unknown input simultaneously, there seem to be some limitations. The main reason is that the existing literature considers the two unknown inputs in the system model (state equation and measurement equation) are the same. Once two identical unknown inputs are set as different signals, the analysis of filter gain and stability needs to be reconsidered. Therefore, based on existing results about unknown input, how to solve the secure estimation problem for systems in the presence of random attacks and unknown input remains a challenge and serves as the main motivation of our book.

Networked-embedded sensors are ubiquitous in monitoring dynamical systems due to their low cost and ease of installation. However, they are also vulnerable to attackers owing to their limited capacity and sparse spatial deployment. Attackers might gain access to sensors and arbitrarily manipulate sensor measurements or break the communication links between sensors and system operators to inject faked information. Therefore, the secure state estimation problem of linear dynamical systems under sparse sensor attacks has been extensively studied in the past few years. In the problem setting, it is usually assumed that a group of sensors are deployed to monitor the system's dynamics, of which a subset of sensors might be compromised and their measurements arbitrarily tampered with. The problem of interest is to determine the conditions under which the system states can be reliably estimated and to design secure estimators to generate reliable estimates.

1.3.2 Secure Pose Estimation for Autonomous Vehicles

Autonomous vehicles (AVs) have recently attracted significant attention from both the academic and industrial domains. Today, many automobile manufacturers and IT companies have implemented active programs to develop AV technologies. Before AV technologies become mature and ultimately available for massive usage, their security problems should be well addressed. In 2015, hackers took control of a Jeep Cherokee and crashed it into a ditch by remotely breaking into its dashboard computer from 10 miles away. Therefore, security is always one of the most critical issues in all kinds of vehicle applications for both AVs and traditional vehicles.

AVs with a small form factor, quick responses, and the ability to operate remotely in a difficult and challenging environment have wide applications. To accomplish an autonomous task, the vehicle should have the capability to determine its pose using sensors mounted on the vehicle. Accurate pose estimation of the AV still remains a significant challenge, especially in GPS-denied environments. Small vehicles like micro aerial vehicles (MAVs) have major constraints, including limited payload carrying capacity. Therefore, a wise selection of sensor(s) and processing unit is important. Equally important is an online, real-time estimation of the pose of the vehicle. For AVs, this book aims to develop a resilient and efficient run-time estimation algorithm that provides a performance guarantee in the presence of malicious sensor attacks.

1.4 Contributions and Organization

Chapters 2 to **5** focus on multi-sensor pose estimation for ground vehicles, while **Chapters 6** to **9** formulate secure dynamic state estimation for mobile robots. Finally, **Chapter 10** concludes the book and provides several perspectives for future work. The primary contributions in the book are summarized and highlighted as follows:

- In order to suppress VO rotation drift in pose estimation, the absolute heading is used to assist VO in **Chapter 2** [Wang et al., 2018a]. By utilizing the coupling characteristics between rotation and translation in VO, the heading measurement can be cost-effectively used to benefit both rotation and translation estimation in ground vehicles. With the absolute heading, a sensor fusion framework is introduced to incorporate heading measurements into VO. In the framework, a heading reference is abstracted as a vertex in the graph model, based on which the problem is formulated as a graph optimization such that off-the-shelf back-end libraries can be utilized effortlessly. To demonstrate the effectiveness of the heading reference-assisted approach, extensive experiments have been conducted based on the KITTI dataset and self-collected data. The results are compared and discussed between pure VO and the proposed approach.
- In addition to the drift issue, the scale ambiguity of MVO is considered as a measurement uncertainty and incorporated into a unified probability distribution. A uniform Gaussian distribution (UGD) is introduced in **Chapter 3** [Jiang et al., 2017, Yang et al., 2017b] to describe measurement uncertainties in VO. The UGD model is used to generate particles representing either SVO or MVO measurements that contain drift and scale ambiguity. A parameter estimation scheme is then presented to refine the probability distribution according to sample particles. The parameter estimation result is used to generate particles iteratively, similar to the Monte Carlo localization framework. Combined with particle *saliency* representing VO measurement certainty degree and particle *consistency* denoting accordance with the map, a map-assisted localization framework is introduced to reduce the drift and scale ambiguity of VO.
- In **Chapter 4** [Jiang et al., 2018], we present a fusion approach to localize urban vehicles by integrating VO, a low-cost GPS, and a two-dimensional digital road map. Distinguished from conventional sensor fusion methods, two types of

potential functions (i.e. potential wells and potential trenches) are introduced to represent measurements and constraints, respectively. By choosing different potential functions according to data properties, data from various sensors can be integrated with intuitive understanding, while no extra map matching is required. The minimum of the fused potential, which is regarded as a position estimation, is confined such that fast minimum searching can be achieved. Experiments under realistic conditions have been conducted to validate satisfactory positioning accuracy and robustness compared to pure VO and map-matching methods.

- In **Chapter 5** [Jiang et al., 2019c], to fuse information from multiple sensors and constraints in pose estimation, non-Euclidean state space and measurement space are presented as background spaces in which states and measurements are points while constraints are subsets. With the distance defined on connected Riemannian manifolds, dynamic potential fields (DPFs) are designed accordingly to represent states, measurements, and constraints such that system noise, measurement noise, and constraint softness are modeled. Based on the DPF formulation, an information fusion scheme called Geometric Pose Estimation (Geo-PE) is presented, in which the state equation and output equation are considered mappings between state-sourced and measurement-sourced DPFs with clear probabilistic implications; the state-sourced and measurement-sourced DPFs are then projected to constraints along the derivative of constraint-sourced DPF. Constraints are thus inherently considered compared to conventional sensor fusion approaches. The approximated version of Geo-PE is then presented, catering to various systems without explicit analytic expression. Geo-PE has been developed for ground vehicles equipped with SVO, an attitude and heading reference system, and OSM so that the pose transformation from dead-reckoning, heading in the East-North-Up frame, and road map in the East-North plane are incorporated for estimating the vehicle pose without rotation drift. Experiments have been conducted based on public KITTI sequences and self-collected Nanyang Technological University (NTU) dataset to validate the performance of the proposed approach.
- In **Chapter 6** [Liu et al., 2019b], we present a filter-based secure dynamic pose estimation approach such that the vehicle pose can be resilient under possible sensor attacks. Our estimator coincides with the conventional Kalman filter when all sensors on AVs are benign. If less than half of the measurement states are compromised by randomly occurring deception attacks, it still gives stable estimates of the pose states: i.e. an upper bound is guaranteed for the estimation error covariance. The pose estimation results with single and multiple attacks on the testing route validate the effectiveness and robustness of the proposed approach.

- In **Chapter 7** [Liu et al., 2021], we introduce a pose estimation approach for ground vehicles under randomly occurring deception attacks. By modeling attacks as signals added to measurements with a certain probability, the attack model is presented and incorporated into the existing process and measurement equations of ground vehicle pose estimation based on multi-sensor fusion. An unscented Kalman filter (UKF)-based secure pose estimator is then established to generate a stable estimate of the vehicle pose states; i.e. an upper bound is guaranteed for the estimation error covariance. The simulation and experiments are conducted on a simple but effective single-input-single-output dynamic system and the ground vehicle model to show the effectiveness of UKF-based secure pose estimation.
- In **Chapter 8** [Liu et al., 2017], we consider the problem of estimating the state of a linear time-invariant Gaussian system in the presence of sparse integrity attacks. The attacker can control p out of m sensors and arbitrarily change the measurements. Under mild assumptions, we can decompose the optimal Kalman estimate as a weighted sum of local state estimates, each of which is derived using only the measurements from a single sensor. Furthermore, we introduce a convex optimization-based approach, instead of the weighted sum approach, to combine the local estimate into a more secure state estimate. It is shown that our proposed estimator coincides with the Kalman estimator with a certain probability when all sensors are benign, and we provide a sufficient condition under which the estimator is stable against the (p, m)-sparse attack when p sensors are compromised. A numerical example is provided to illustrate the performance of the state estimation scheme.
- In **Chapter 9** [Jiang et al., 2019a], we focus on the problem of secure attitude estimation for AVs. Based on the established attitude and heading reference system (AHRS) measuring model and the attack model, we have decomposed the optimal Kalman estimate into a linear combination of local state estimates. We then introduce a convex optimization-based approach, instead of the weighted sum approach, to combine the local estimate into a more secure estimate. It is shown that the secure estimator coincides with the Kalman estimator with a certain probability when there is no attack and can be stable when p elements of the model state are compromised. Simulations have been conducted to validate the secure filter under single and multiple measurement attacks.