



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

Master's Thesis

석사 학위논문

UNKNOWN INPUT OBSERVER BASED RESILIENT CONTROL SYSTEM DESIGN

Dongmin Seo(서 동 민 徐 東 珉)

Department of Information and Communication Engineering

정보통신융합공학전공

DGIST

2017

Master's Thesis

석사 학위논문

Unknown Input Observer Based Resilient Control System Design

Dongmin Seo(서 동 민 徐 東 珉)

Department of Information and Communication Engineering

정보통신융합공학전공

DGIST

2017

Unknown Input Observer Based Resilient Control System Design

Advisor: Professor Yongsoon Eun
Co-advisor: Professor Hyungbo Shim

by

Dongmin Seo

Department of Information and Communication Engineering
DGIST

A thesis submitted to the faculty of DGIST in partial fulfillment of the requirements for the degree of Master of Science in the Department of Information and Communication Engineering. The study was conducted in accordance with Code of Research Ethics ¹

11. 22. 2016

Approved by

Professor Yongsoon Eun (Signature) 

Professor Hyungbo Shim (Signature) 

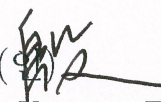

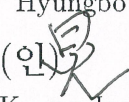
¹Declaration of Ethical Conduct in Research: I, as a graduate student of DGIST, hereby declare that I have not committed any acts that may damage the credibility of my research. These include, but are not limited to: falsification, thesis written by someone else, distortion of research findings or plagiarism. I affirm that my thesis contains honest conclusions based on my own careful research under the guidance of my thesis advisor.

Unknown Input Observer Based Resilient Control System Design

Dongmin Seo

Accepted in partial fulfillment of the requirements
for the degree of Master of Science.

11. 22. 2016

Head of Committee	<u>은 용 순</u> (인)  Prof. Yongsoon Eun
Committee Member	<u>심 형 보</u> (인)  Prof. Hyungbo Shim
Committee Member	<u>박 경 준</u> (인)  Prof. Kyung-Joon Park

MS/IC 서동민. Dongmin Seo. Unknown Input Observer Based Resilient Control
201522011 System Design. Department of Information and Communication Engineer-
ing. 2017. 95p. Advisor Prof. Yongsoon Eun. Co-Advisor Prof. Hyungbo
Shim

ABSTRACT

Resiliency of control systems means characteristics that a system operates well under malicious attacks on instrumentation. In this thesis, we propose Unknown Input Observer (UIO) based resilient control system design method for the case of simultaneous attacks on sensors and actuators.

We use an observer based Resilient State Estimation (RSE) method for protecting from sensor attack. Limitation of existing RSE method is that state estimation error is affected by disturbance and actuator attack. In order to supplement the drawback, we propose the UIO based RSE method. Proposed method provides superior state estimation performance regardless of the effect of disturbance and actuator attack. In addition, we suggest an algorithm that would be able to diagnose which sensors are attacked or broken.

In order to protect the system from actuator attack, we propose a method that would be able to estimate and reject the effect of actuator attack. Proposed method exploits UIO based RSE method. The proposed method provides a level of resiliency to the control system when disturbance and attack are slow varying.

Simulation and experiment are implemented on the magnetic levitation system platform so as to validate the effectiveness of proposed method. In addition, we compare the performance between existing method and proposed method.

Key words : Resiliency of Control Systems, Sensor Attack, Actuator Attack,
Resilient State Estimation, Unknown Input Observer

Contents

Abstract	i
List of Contents	vi
List of Figures	viii
Notation and Symbols	xi
1 Introduction	1
1.1 Significance of Resilient Control Systems	2
1.2 Motivation	2
1.3 Thesis Outline	4
2 Unknown Input Observer Based Resilient Control System Design	5
2.1 Problem Formulation	6
2.2 Unknown Input Observer Based Resilient State Estimation Method	11
2.2.1 Limitation of the Existing Resilient State Estimation Method . . .	11
2.2.2 Unknown Input Observer Based Resilient State Estimation Method Design	16
2.2.2.1 Unknown Input Observer Design	17
2.2.2.2 Median Operator	22
2.2.3 Analysis of State Estimation Error of Proposed RSE Method	23
2.2.4 Diagnosis Method of the System under Sensor Attack and Fault . .	37
2.3 Defense Approach Against Actuator Attack	40

3	Validation with Magnetic Levitation Platform	43
3.1	Modeling	44
3.2	Design of Resilient Control System Design	46
3.2.1	Existing Resilient State Estimation Method Using Median Operation	46
3.2.2	Proposed Resilient Control System Design	47
3.3	Scenarios	50
3.3.1	Scenario 1	50
3.3.2	Scenario 2	51
3.3.3	Scenario 3	51
3.4	Simulation Results	51
3.4.1	Simulation Results of Scenario 1	51
3.4.2	Simulation Results of Scenario 2	58
3.4.3	Simulation Results of Scenario 3	62
3.5	Experiment Results	67
3.5.1	Experiment Results of Scenario 1	67
3.5.2	Experiment Results of Scenario 2	71
3.5.3	Experiment Results of Scenario 3	78
4	Conclusion	83
A	MATLAB Code For Numerical Simulation	85
	Bibliography	97
	국문초록	99

List of Figures

2.1	Block diagram of the resilient control system.	6
2.2	Block diagram of the Defense methods against malicious attacks.	10
2.3	Block diagram of the proposed resilient state estimation method.	17
2.4	Structure of UIO.	18
2.5	Error between actual state and estimate when we set frequency to 100 rad/sec.	34
2.6	Error between actual state and estimate when we set frequency to 1000 rad/sec.	34
2.7	Error between actual state and estimate.	37
2.8	Block diagram of the diagnosis method under sensor attack.	38
2.9	Structure of an actuator attack estimation method using UIO based RSE method.	41
3.1	Magnetic Levitation System.	44
3.2	Sensor attack and actuator attack.	51
3.3	Estimate of Luenberger observer when using existing RSE method.	55
3.4	Actual state and estimate when using existing based RSE method.	56
3.5	State estimation error when using existing RSE method.	57
3.6	Estimate of UIO when using UIO based RSE method.	59
3.7	Actual state and estimate when using UIO based RSE method.	60
3.8	State estimation error when using UIO based RSE method.	61
3.9	Estimate of UIO when using UIO based RSE method and actuator attack estimator.	63

3.10	Actual state and estimate when using UIO based RSE method and actuator attack estimator.	64
3.11	State estimation error when using UIO based RSE method and actuator attack estimator.	65
3.12	Actuator attack and estimate of actuator attack.	66
3.13	Error of between Actuator attack and Estimate of actuator attack.	66
3.14	Estimate of Luenberger observer when using existing RSE method (Experiment results).	68
3.15	Actual state and estimate when using existing based RSE method (Experiment results).	69
3.16	State estimation error when using existing RSE method (Experiment results).	70
3.17	Estimate of UIO When using UIO based RSE method (Experiment results).	75
3.18	Actual state and estimate when using UIO based RSE method (Experiment results).	76
3.19	State estimation error when using UIO based RSE method (Experiment results).	77
3.20	Estimate of UIO when using UIO based RSE method and actuator attack estimator (Experiment results).	79
3.21	Actual state and estimate when using UIO based RSE method and actuator attack estimator (Experiment results).	80
3.22	State estimation error when using UIO based RSE method and actuator attack estimator (Experiment results).	81
3.23	Actuator attack and estimate of actuator attack (Experiment results).	82
3.24	Error of Actuator attack and Estimate of actuator attack (Experiment results).	82
A.1	Numerical_example.slx.	87
A.2	Magnetic_Levitation_System.slx.	90
A.3	Luenberger Observer.	92
A.4	Unknown Input Observer and Sensor Attack Diagnosis Method.	93

Notation and Symbols

\mathbb{R}	the set of all real numbers
\mathbb{R}^n	the n -dimensional Euclidean space
$\mathbb{R}^{n \times n}$	the space of $n \times n$ matrix with real entries
$\text{supp}(x)$	the indices that are not zero of x
$ \text{supp}(x) $	the total number of non-zero elements of x
A^+	the pseudo inverse of matrix A

1

Introduction

These days, computer technologies and communication systems have made remarkable development. Accordingly, control systems have become more sophisticated and complicated than before. There exists tons of systems that communicate wirelessly. But, a weak point of control systems has appeared in accordance with development of technologies.

In our society, there exist numerous control systems in the infrastructure such as nuclear plant, factory, power grid, transportation systems, and so on. It is evident that it would be catastrophic if control systems in the infrastructure were attacked. Actually, these kinds of thoughts and possibilities occur and these problems have received attention recently. Control researchers have tried how to protect control system from malicious attacks. They have focused on designing control system such that operates well under malicious attacks. In this section, we say why designing resilient control systems is important.

In section 1.1, we discuss the significance of the resilient control systems. The motivation of this thesis is explained in section 1.2. The outline of this thesis is presented in section 1.3.

1.1 Significance of Resilient Control Systems

Nowadays, there exist numerous control systems in infrastructure such as power grid, transportation, aircraft, chemical plant, nuclear plant, etc. With the remarkable technology development, systems have been more complex than in the past. Also, control systems have become vulnerable to malicious attacks. These issues have received a lot of attention. Many researchers have studied to improve resiliency of control systems. Also, its related works have been reported. Resiliency of control systems is characteristics that a system operates well despite of malicious attacks. If control systems cannot be protected from malicious attacks, it would result in catastrophe and social costs such as the biggest security threat and a terrible loss of human life. These apprehensions were realized.

Let we take an example of a car. These days, automobile is not simple transportation, but is the system equipped a state-of-the-art system. Internal systems of vehicle have become more vulnerable to malicious attacks than in the past. [2] and [9] imply possibilities of malicious attacks. [17] implies that it is possible for attacker to control the attack freely by interfering the magnetic field of magnetic-based wheel speed sensor of ABS (Anti-lock Braking System). Another example would be [10], [4], [8] and [12]. [10], [4], and [8] are about stuxnet virus and [12] is about analyzing attack on power grid.

In these examples, we are able to check that a malicious attack could bring about malfunction of control system. Cyber Physical Systems (CPS) will become more complex and vulnerable in the future. Thus, In order to protect systems from malicious attacks, we would like to emphasize that it is important improve the resiliency of control systems.

1.2 Motivation

Nowadays, much research on attack detection has been reported. [20] analyzed the weak points network of networked control systems in the presence of malicious attack. This paper proposed a method that would detect malicious attacks by using observer on the basis of attack scenarios. [15] analyzed an attack on CPS (Cyber Physical System) and proposed monitoring system. This paper proposed centralized and distributed attack detection method.

Many defense methods against sensor attack have been conducted. Mostly, many re-

searchers have tried to solve state reconstruction problem. It is essential to consider some assumptions in order to solve the problem. Assumptions are that system has multi-sensors and the number of attacked sensors are limited. This method is called as secure state reconstruction. [6], [5], [14], and [18] were studied in the beginning in the discrete-time system. [6] and [5] introduced the the optimization problem to solve the state reconstruction. [14] extended to bounded noises, disturbances, and modeling error. [18] extended to nonlinear systems and validated by using flat system.

[6], [5], [14], and [18] were to solve the optimization problem in order to reconstruct the state. Thus, these methods had the characteristics that need heavy computation effort. There are two methods [11], [7] that reduce the computation effort effectively. These two resilient state estimation methods are observer based approach. [11] proposed the finite set for solving optimization problem. Thus, computation effort is lower than existing methods. [7] is also resilient state estimation method using each observer and median operation. This method needs the design condition that the relation between system and all sensors should be observable. This method is more faster than [11].

There are a lot of studies related to defense approach against actuator attack. [6] and [5] proposed the optimization problem on the system having multiple inputs. [13] proposed outstanding attack detection method by using dual rate. [21] checked the resiliency by experiment so that the system continues operation even though some of the controllers are attacked and lose functionality. [16] proposed three resilient control algorithms inspired by disturbance observer in robust control design and the proposed methods of [16] provide a level of resiliency to the control system when attacks are composed of low frequencies. [19] is not about the attack, but is related to resiliency of control system. this paper proposed method that restores the performance by minimizing the performance loss when there exists fault on some of system input.

In this thesis, we consider actuator attack as well as sensor attack and disturbance. This thesis consists of two parts. The first part is concerned with malicious attacks on sensors. We use resilient state estimation method against sensor attack. Since there exist disturbance and actuator attack on system input, the accuracy of state estimation performance degrades. We adopt Unknown Input Observer (UIO) [3] in order to guarantee that estimate of UIO converges to actual state as time goes on despite of the effect of disturbance and actuator attack. The second part is concerned with attack on system input. So

as to reject the effect of disturbance and actuator attack, we exploit UIO mechanism [3].

1.3 Thesis Outline

We introduce this thesis in section 1. In section 2, we formulate the systems, assumptions and problems. Next, we discuss limitations of the existing method and introduce the compensate method. There are primary two methods against sensor attack and actuator attack respectively. The method protecting from sensor attack is to use the Unknown Input Observer and we will discuss the design the proposed method. Then, we introduce a diagnosis method that would be able to detect which sensors are attacked. The method protecting from actuator attack is to estimate and reject the effect of the actuator attack. We deal with basic principle of this method. In section 3, we discuss the result of experiment on magnetic levitation. In section 4, we conclude this thesis.

2

Unknown Input Observer Based Resilient Control System Design

In this thesis, we consider SIMO (Single Input Multiple Output) system under actuator attack as well as sensor attack, noise, and disturbance. Firstly, we use the existing Resilient State Estimation (RSE) method in order to enhance a resiliency of control system from sensor attacks. Since actuator is attacked, state estimation error occurs. In this chapter, we deal with a drawback of existing method. Then, we formulate the problems to solve. First Problem is to find a method that estimate error of RSE method converges to zero as time goes on despite of disturbance and actuator attack. Second problem is to find a method that would be able to estimate and reject a effect of disturbance and actuator attack. In this chapter, we will introduce proposed methods to solve problems. Plus, we will propose the diagnostic method that would be able to diagnose which sensors are attacked under sensor attack.

In section 2.1, we formulate a system considering sensor attack, noise, disturbance, and actuator attack. Then, we will assume a few things to solve the problem. Finally, we will define the problems and suggest solutions to problems. In section 2.2, we will deal with a solution to first problem and propose the UIO based RSE method. In section 2.2.1, we discuss the a limitation of existing observer based resilient state estimation method. Then, in section 2.2.2, we will discuss UIO based RSE method. In section 2.2.2.1, we will explain the UIO design method. In section 2.2.2.2, we discuss the median operator. Then, in section 2.2.3, we will analyze the state estimation error of proposed method. In section 2.2.4, we will propose a diagnostic method under the attack or the fault. Finally, in section 2.3, we will deal with a solution to second problem. We discuss a defense approach against actuator attack.

2.1 Problem Formulation

We consider a linear dynamical system given by

$$\begin{aligned}
 \dot{x}(t) &= Ax + B(u(t) + d(t) + a^a(t)), \\
 y(t) &= Cx(t) + \xi(t) + a^s(t), \\
 &= \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_i \\ \vdots \\ C_p \end{bmatrix} x(t) + \begin{bmatrix} \xi_1(t) \\ \xi_2(t) \\ \vdots \\ \xi_i(t) \\ \vdots \\ \xi_p(t) \end{bmatrix} + \begin{bmatrix} a_1^s(t) \\ a_2^s(t) \\ \vdots \\ a_i^s(t) \\ \vdots \\ a_p^s(t) \end{bmatrix}, \tag{2.1}
 \end{aligned}$$

where $x \in \mathbb{R}^n$ is the plant state, $u \in \mathbb{R}$ is control input, $d \in \mathbb{R}$ is external disturbance, $a^a \in \mathbb{R}$ is actuator attack, $y \in \mathbb{R}^p$ is the plant output, $\xi \in \mathbb{R}^p$ is sensor noise, and $a^s \in \mathbb{R}^p$ is sensor attack. The i -th sensor being attacked is represented by i th element of the vector $a^s(t)$, represented by $a_i^s(t)$. We consider SIMO (Single Input Multiple Output). The matrices A, B , and C are in appropriate dimensions.

In this thesis, an attack scenario that we consider differs from the scenario of existing studies. Existing scenarios only consider sensor attack, disturbance, and noise normally. We consider actuator attack as well as sensor attack and disturbance. The scenario considered in this study is shown in Figure 2.1.

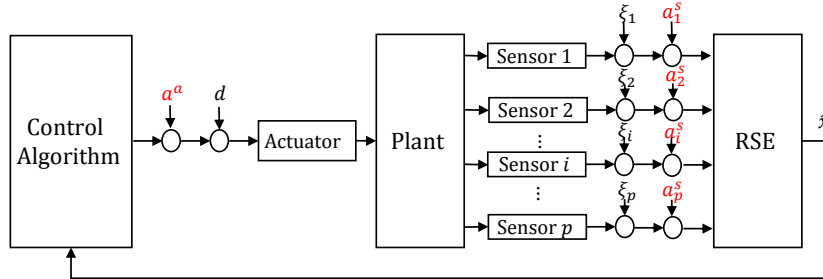


Figure 2.1: Block diagram of the resilient control system.

In this thesis, we consider sensor attack and actuator attack as false data injection attack. After injecting false data injection attack on actuator, values computed in controller and actuator attack are getting to be combined into the values that would be changed by attacker. In sensor attack case, sensor output and sensor attack are getting to be combined into any value that would be changed or destroyed by attacker. A system having multi-sensors can be considered largely divided into two cases. The first case is that multi-sensors measure the same physical quantity. The second case is that multi-sensors measure different physical quantities. we consider both.

Before we introduce a couple of assumptions, we explain the following notation so as to denote the set of sensors under attack. The support of the vector $a(t)$ is defined as

$$\text{supp}(a^s(t)) = \{i | a_i(t) \neq 0\}, \quad (2.2)$$

where $\text{supp}(a^s(t))$ are the indices of the attacked sensors. Also, the cardinality of the set $\text{supp}(a^s(t))$ is $|\text{supp}(a^s(t))|$. The $|\text{supp}(a(t))|$ is the total number of non-zero elements. In other words, it means the total number of non-attacked sensors.

We now introduce assumptions for the system of (2.1).

Assumption 2.1. The set $\text{supp}(a^s(t))$ satisfies the following inequality:

$$2|\text{supp}(a^s(t))| < p, \forall t. \quad (2.3)$$

Assumption 2.1 represents that the number of attacked sensors must be less than half the total number of the sensors for solve the problems. it is a necessary and sufficient condition for resilient state estimation problem to be solvable. This is the standard assumption for resilient state estimation technique [11], [7]. Assumption 2.1 is enough to be practical. The time and effort are needed for attacker to access all sensors practically.

Before explaining Assumption 2.2, Let we introduce the UIO Model:

$$\begin{aligned} \dot{g}_i(t) &= F_i g_i(t) + T_i B u(t) + K_i y_i(t), \quad i = 1, \dots, p, \\ z_i(t) &= g_i(t) + H_i y_i(t), \end{aligned} \quad (2.4)$$

where $g_i \in \mathbb{R}^n$ is i -th UIO state, $u \in \mathbb{R}$ is the system input, $y_i \in \mathbb{R}$ is i -th system output, and $z_i \in \mathbb{R}^n$ is i -th estimate of the UIO. The matrices F_i, T_i, K_i and H_i are UIO parameters are appropriate dimensions.

Assumption 2.2. System of (2.1) and each sensor satisfies the following design condition.

1. $\text{rank}(C_i B) = \text{rank}(B)$.
2. $(A - H_i C_i A, C_i)$ is detectable, where $H_i = B((C_i B)^T (C_i B))^{-1} (C_i B)^T$.

These two conditions are the necessary and sufficient condition for UIO based Resilient State Estimation method to be used. First condition is that rank of $C_i B$ must be the same with rank of B . Second condition is that $(A - H_i C_i A, C_i)$ must be detectable at least. Second condition depends on H_i . Thus, It is not always satisfied, and the condition may not be satisfied depending on system matrices A , C_i , and UIO matrix H_i . Design conditions that we consider differs from existing resilient state estimation technique [11], [7]. When design condition for existing RSE method is not satisfied, UIO based RSE method condition may be satisfied.

Assumption 2.3. The vectors $d(t), \xi(t)$, and $\dot{\xi}(t)$ satisfy

$$\begin{aligned} |d_i(t)| &\leq d_{max}, \quad i = 1, 2, \dots, n, \\ |\xi_i(t)| &\leq \xi_{max}, \quad i = 1, 2, \dots, p, \\ |\dot{\xi}_i(t)| &\leq \dot{\xi}_{max} := \bar{\xi}_{max}, \quad i = 1, 2, \dots, p. \end{aligned} \tag{2.5}$$

Assumption 2.3 states that external disturbance, noise and time derivative of noise are bounded.

Before formulating problems, we introduce the Resilient State Estimation (RSE) method briefly. Firstly, let consider that a system having multi-sensors are attacked only on some of sensors under assumption 2.1. Under this condition, RSE method is used for state reconstruction. It means estimate error of RSE method converges to zero as time goes infinity under sensor attack. Above all, we use the Observer based RSE method in order

to enhance the resiliency of control systems from sensor attack. By using one, the system is able to operate well under sensor attacks on some of sensors. we use the observer based RSE method such as combinatorial approach [11] and median approach [7]. But, there exist some limitations when using existing RSE method on system of (2.1). First drawback is that state estimation error degrades because of disturbance and actuator attack. We will deal with this drawback in section 2.2.1 in detail. Second limitation is that RSE method is not able to protect the system from the effect of disturbance and actuator attack. Also, disturbance and actuator attack would deteriorate control performance. Thus, we have to find a methods that would be able to enhance the resiliency against sensor attack, disturbance, and actuator attack.

Now, we formulate two problems.

Problem 2.1. Let Assumptions 2.1, 2.2 and 2.3 hold. Find a method of RSE whose output \hat{x} satisfies $\hat{x}(t) \rightarrow x(t)$ as $t \rightarrow \infty$, despite of disturbance and actuator attack.

As we mentioned before, we use observer based RSE method. State estimation performance deteriorates under disturbance and actuator attack. Then, state estimation problem (estimated state of RSE method converges to actual state as time goes on) can no longer be guaranteed. Thus, we have to find new method that would guarantee that estimated state converges to actual state as time goes on despite of disturbance and actuator attack. In order to solve problem 2.1, a method have to estimate the state correctly despite of disturbance and actuator attack. A solution to Problem 2.1 is to use the UIO as observer of RSE method instead of Luenberger observer. Advantage of UIO is that state estimation performance of UIO is not affected by disturbance and actuator attack. we will discuss the drawback of existing RSE method in section 2.2.1. Then, we will introduce UIO based RSE method and analyze performance of proposed method.

Problem 2.2. Let Assumptions 2.1, 2.2 and 2.3 hold. Find a method that would be able to estimate and reject the effect of disturbance and actuator attack.

By estimating state correctly, we are able to protect the system from sensor attack.

But, there still exists the effect of disturbance and actuator attack. This effect leads to deteriorate a control performance. Thus, we have to find a way to enhance the resiliency under the effect of disturbance and actuator attack. Solution is to estimate and reject the effect of disturbance and actuator attack by using proposed UIO based RSE method. Then, we are able to protect the system from the actuator attack. We will discuss basic principle in section 2.3.

Now, we illustrate system of (2.1), malicious attacks, and the solutions to problems in Figure 2.2. Solution to problem 2.1 is to use UIO based RSE method in order to estimate the state correctly despite of disturbance and actuator attack. Solution to problem 2.2 is to design a method that would be able to estimate and reject the effect of disturbance and actuator attack by exploiting UIO based RSE method. If the system of (2.1) is able to use the correct state by resilient state estimation method and eliminate the effect of disturbance and actuator attack, then, we are able to say that the system is resilient against malicious attack.

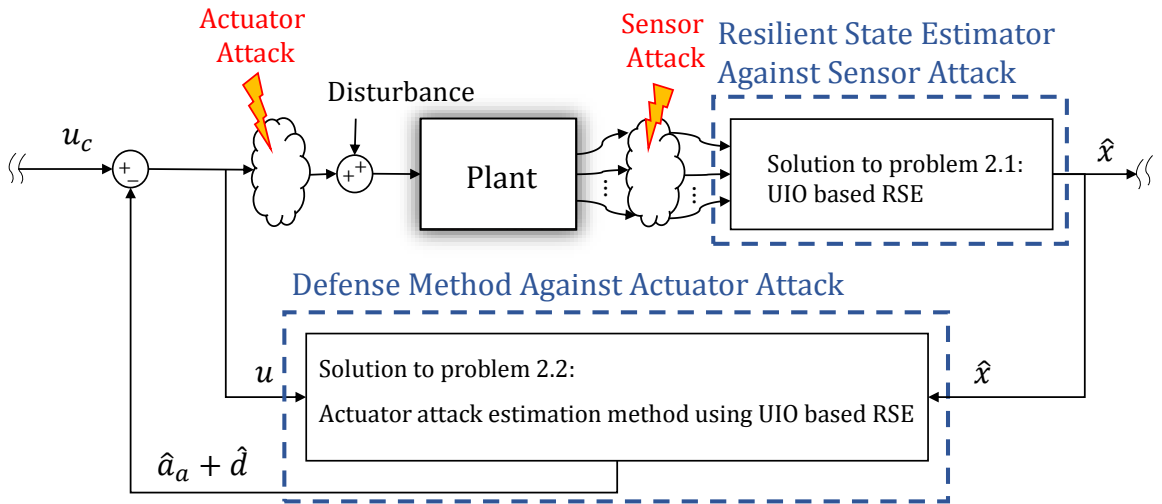


Figure 2.2: Block diagram of the Defense methods against malicious attacks.

2.2 Unknown Input Observer Based Resilient State Estimation Method

In this section, we mainly deal with the proposed UIO based resilient state estimation method. There are four main parts. Before introducing the proposed method, we analyze the limitation of existing observer based RSE method. Thus, we discuss the state estimation error of the system when using existing method. Next, we introduce the new resilient state estimation method whose state converges to real state despite of disturbance and actuator attack. The key component of proposed RSE method is UIO. We explain the UIO based RSE method and the design procedure. Then, we analyze the state estimation error of the system using UIO based RSE method. Finally, we introduce the diagnostic method in the presence of the sensor attack.

2.2.1 Limitation of the Existing Resilient State Estimation Method

In this section, we analyze the state estimation error of the system using the existing resilient state estimation method. There are two primary observer based state estimation methods [11], [7]. Two state reconstruction methods use commonly the Luenberger observer. When there exists the disturbance on the system input, the estimation performance of the Luenberger observer deteriorates. This is the main drawback. In this thesis, we only analyze the RSE method using median operation [7]. In accordance with the amplitude of disturbance and actuator attack, the state estimation error could be changed. The disturbance and actuator attack can make the state estimation error to be considerable when we use the existing RSE method.

Theorem 2.1. [7] *Suppose Assumption 2.1 and Assumption 2.3 hold. Also, the pair (C_i, A) is observable for $i = 1, 2, \dots, p$. Then, state estimation error of the system of (2.1) using existing RSE method exploiting median operation is written by*

$$\begin{aligned} \|\hat{x}(t) - x(t)\|_2 &\leq \nu \|\hat{x}(0) - x(0)\|_2 e^{-\lambda t} + \frac{\nu(\|B\|_2 d_{max} + \|L_i\|_2 \xi_{max})}{\lambda} \\ &\quad + n^{\frac{1}{2}} \left\| \int_0^t e^{(A-L_i C_i)(t-\tau)} (B a^a(\tau)) d\tau \right\|_2, \end{aligned} \quad (2.6)$$

where $\nu > 0$ and $\lambda > 0$ are constant, n is the number of system state, d_{max} is bounded disturbance, ξ_{max} is bounded noise, and a^a is actuator attack. B is system matrix and L_i

is i -th observer matrix.

◆

Note that the state estimation error of existing RSE method is bounded if the noise, disturbance, and effect of actuator attack are bounded. The state estimation error is related to disturbance and actuator attack as well as noise. If actuator attack and disturbance are considerable, the state estimation error would be large. Thus, it can no longer guarantee that estimate converges to real state ($\hat{x} \rightarrow x$) as time goes on ($t \rightarrow \infty$) because of the effect of disturbance and actuator attack. It may cause that control performance deteriorates. We would like to emphasize that it is a main drawback of the existing RSE method. Thus, it is important to design the RSE method whose estimate converges to actual state ($\hat{x} \rightarrow x$) as time goes on ($t \rightarrow \infty$) despite of the effect of disturbance and actuator attack. We will introduce the proposed RSE method later. The state estimation performance of the UIO based RSE method is not affected from disturbance and actuator attack.

Proof: Flow of proof of equation (2.6) is equal to the flow of [7]. However, the system considered is different each other. In this thesis, we consider actuator attack and not consider inner uncertainty. The Luenberger observer model is given by

$$\begin{aligned}\dot{z}^i(t) &= Az^i(t) + Bu(t) + L_i(y_i(t) - \hat{y}_i(t)), \\ \hat{y}^i(t) &= C_i z^i(t).\end{aligned}\tag{2.7}$$

We denote $\hat{x}_i = z^i$. The z^i implies the i -th state estimate. we also denote \tilde{z}^i as the estimation error from i -th sensor:

$$\tilde{z}^i(t) = x(t) - z^i(t).\tag{2.8}$$

The i -th estimation error dynamics is as follows:

$$\begin{aligned}\dot{\tilde{z}}^i(t) &= \dot{x}(t) - \dot{z}^i(t), \\ &= Ax(t) + Bu(t) + Ba^a(t) + Bd(t) - Az^i(t) - Bu(t) - L_i(y_i(t) - C_i z^i(t)), \\ &= (A - L_i C_i) \tilde{z}^i(t) + Ba^a(t) + Bd(t) - L_i \xi_i(t) - L_i a_i^s(t).\end{aligned}\tag{2.9}$$

The L_i is chosen so that the $A - L_i C_i$ is Hurwitz for all $i = 1, \dots, p$. the solution of above equation (2.9) is as follows.

$$\begin{aligned}\tilde{z}^i(t) &= e^{(A-L_i C_i)t} \tilde{z}^i(0) + \int_0^t e^{(A-L_i C_i)(t-\tau)} (B a^a(\tau) + B d(\tau) - L_i \xi_i(\tau) - L_i a_i^s(\tau)) d\tau, \\ &= e^{(A-L_i C_i)t} \tilde{z}^i(0) + \int_0^t e^{(A-L_i C_i)(t-\tau)} (B a^a(\tau)) d\tau + \int_0^t e^{(A-L_i C_i)(t-\tau)} (B d(\tau)) d\tau \\ &\quad - \int_0^t e^{(A-L_i C_i)(t-\tau)} (L_i \xi_i(\tau)) d\tau - \int_0^t e^{(A-L_i C_i)(t-\tau)} (L_i a_i^s(\tau)) d\tau.\end{aligned}\quad (2.10)$$

let denote the right-hand side part as the following:

$$\bar{e}^i(t) = e^{(A-L_i C_i)t} \tilde{z}^i(0), \quad (2.11)$$

$$\bar{a}^{ai}(t) = \int_0^t e^{(A-L_i C_i)(t-\tau)} (B a^a(\tau)) d\tau, \quad (2.12)$$

$$\bar{d}^i(t) = \int_0^t e^{(A-L_i C_i)(t-\tau)} (B d(\tau)) d\tau, \quad (2.13)$$

$$\bar{\xi}^i(t) = - \int_0^t e^{(A-L_i C_i)(t-\tau)} (L_i \xi_i(\tau)) d\tau, \quad (2.14)$$

$$\bar{a}^{si}(t) = - \int_0^t e^{(A-L_i C_i)(t-\tau)} (L_i a_i^s(\tau)) d\tau, \quad (2.15)$$

where $\bar{e}^i(t) \in \mathbb{R}^n$, $\bar{a}^{ai}(t) \in \mathbb{R}^m$, $\bar{d}^i(t) \in \mathbb{R}^m$, $\bar{\xi}^i \in \mathbb{R}$, $\bar{a}^{si}(t) \in \mathbb{R}$.

By using median operation, we can obtain the next equation:

$$\hat{x}_j = \text{med}(x_j + \bar{e}_j^i + \bar{a}_j^{ai} + \bar{d}_j^i + \bar{\xi}_j^i + \bar{a}_j^{si}, \dots, x_j + \bar{e}_j^p + \bar{a}_j^{ap} + \bar{d}_j^p + \bar{\xi}_j^p + \bar{a}_j^{sp}), j = 1, \dots, n. \quad (2.16)$$

Each the x_j , \bar{e}_j^i , \bar{a}_j^{ai} , \bar{d}_j^i , $\bar{\xi}_j^i$, and \bar{a}_j^{si} is the component of x , \bar{e}^i , \bar{a}^{ai} , \bar{d}^i , $\bar{\xi}^i$, and \bar{a}^{si} respectively.

If the $A - L_i C_i$ is Hurwitz for all i ($\forall i = 1, \dots, p$) for all time ($t \geq 0$), there exists the constant μ and λ satisfying the following inequality.

$$\|e^{(A-L_i C_i)t}\|_2 \leq \nu e^{-\lambda t}. \quad (2.17)$$

Each $\|\bar{e}^i(t)\|_2$, $\|\bar{a}^{ai}(t)\|_2$, $\|\bar{d}^i(t)\|_2$, and $\|\bar{\xi}^i(t)\|_2$ are bounded as follows

$$\begin{aligned} \|\bar{e}^i(t)\|_2 &= \|e^{(A-L_i C_i)t} \tilde{z}^i(0)\|_2, \\ &\leq \nu_e \|\tilde{z}^i(0)\|_2 e^{-\lambda_e t}, \\ &\leq \nu_e \|\hat{x}(0) - x(0)\|_2 e^{-\lambda_e t}, \end{aligned} \quad (2.18)$$

$$\|\bar{a}^{ai}(t)\|_2 = \left\| \int_0^t e^{(A-L_i C_i)(t-\tau)} (B a^a(\tau)) d\tau \right\|_2, \quad (2.19)$$

$$\begin{aligned} \|\bar{d}^i(t)\|_2 &= \left\| \int_0^t e^{(A-L_i C_i)(t-\tau)} (B d(\tau)) d\tau \right\|_2, \\ &\leq \|B\|_2 d_{max} \int_0^t \|e^{(A-L_i C_i)(t-\tau)}\|_2 d\tau = \|B\|_2 d_{max} \int_0^t \|e^{(A-L_i C_i)(\tau)}\|_2 d\tau, \\ &\leq \|B\|_2 d_{max} \frac{\nu_d}{\lambda_d} (1 - e^{-\lambda_d t}), \\ &\leq \frac{\nu_d \|B\|_2 d_{max}}{\lambda_d}, \end{aligned} \quad (2.20)$$

$$\begin{aligned} \|\bar{\xi}^i\|_2 &= - \int_0^t e^{(A-L_i C_i)(t-\tau)} (L_i \xi_i(\tau)) d\tau, \\ &\leq \|L_i\|_2 \xi_{max} \int_0^t \|e^{(A-L_i C_i)(t-\tau)}\|_2 d\tau = \|L_i\|_2 \xi_{max} \int_0^t \|e^{(A-L_i C_i)(\tau)}\|_2 d\tau, \\ &\leq \|L_i\|_2 \xi_{max} \frac{\nu_\xi}{\lambda_\xi} (1 - e^{-\lambda_\xi t}), \\ &\leq \frac{\nu_2 \|L_i\|_2 \xi_{max}}{\lambda_\xi}, \end{aligned} \quad (2.21)$$

where $\nu_e, \nu_a, \nu_d, \nu_\xi > 0$ and $\lambda_e, \lambda_a, \lambda_d, \lambda_\xi > 0$.

Since the $\bar{e}_j^i, \bar{a}_j^{ai}, \bar{d}_j^i$, and $\bar{\xi}_j^i$ belong to the $\bar{e}^i, \bar{a}^{ai}, \bar{d}^i$, and $\bar{\xi}^i$, the following inequalities are satisfied:

$$\begin{aligned} |\bar{e}_j^i| &\leq \|\bar{e}^i(t)\|_2, \\ |\bar{a}_j^{ai}| &\leq \|\bar{a}^{ai}(t)\|_2, \\ |\bar{d}_j^i| &\leq \|\bar{d}^i(t)\|_2, \\ |\bar{\xi}_j^i| &\leq \|\bar{\xi}^i(t)\|_2. \end{aligned} \quad (2.22)$$

Let $\bar{\eta}_j^i = \bar{e}_j^i + \bar{a}_j^{ai} + \bar{d}_j^i + \bar{\xi}_j^i, i = 1, \dots, p, j = 1, \dots, n$. By using Median operation, the following equation is satisfied:

$$\hat{x}_j = \text{med}(x_j + \bar{\eta}_j^1 + \bar{a}_j^{s1}, \dots, x_j + \bar{\eta}_j^p + \bar{a}_j^{sp}), j = 1, \dots, n. \quad (2.23)$$

The following inequality is satisfied:

$$|\hat{x}_j - x_j| \leq \max(|\bar{\eta}_j^i|), i = 1, \dots, p, j = 1, \dots, n. \quad (2.24)$$

The $\max(|\bar{\eta}_j^i|)$ is bounded as follows

$$\begin{aligned} \max(|\bar{\eta}_j^i|) &= \max|\bar{e}_j^i + \bar{a}_j^{ai} + \bar{d}_j^i + \bar{\xi}_j^i|, i = 1, \dots, p, j = 1, \dots, n, \\ &\leq \max(|\bar{e}_j^i|) + \max(|\bar{a}_j^{ai}|) + \max(|\bar{d}_j^i|) + \max(|\bar{\xi}_j^i|). \end{aligned} \quad (2.25)$$

We can see the $\|\hat{x}(t) - x(t)\|_2$ is

$$\begin{aligned} \|\hat{x}(t) - x(t)\|_2 &\leq n^{\frac{1}{2}} \max(|\hat{x}_j - x_j|, j = 1, \dots, n), \\ &\leq n^{\frac{1}{2}} (\max(|\bar{e}_j^i|) + \max(|\bar{a}_j^{ai}|) + \max(|\bar{d}_j^i|) + \max(|\bar{\xi}_j^i|)), \\ &\leq n^{\frac{1}{2}} (\nu_e \|\hat{x}(0) - x(0)\|_2 e^{\lambda_e t} + \frac{\nu_d \|B\|_2 d_{\max}}{\lambda_d} + \frac{\nu_n \|L_i\|_2 \xi_{\max}}{\lambda_n} \\ &\quad + \|\int_0^t e^{(A-L_i C_i)(t-\tau)} (B a^a(\tau)) d\tau\|_2). \end{aligned} \quad (2.26)$$

If we select the ν and λ satisfying the $\nu > n^{\frac{1}{2}} \max(\nu_e, \nu_d, \nu_\xi), 0 < \lambda < \min(\lambda_e, \lambda_\xi, \lambda_d)$, the following inequality can be written by

$$\begin{aligned} \|\hat{x}(t) - x(t)\|_2 &\leq \nu \|\hat{x}(0) - x(0)\|_2 e^{-\lambda t} + \frac{\nu(\|B\|_2 d_{max} + \|L_i\|_2 \xi_{max})}{\lambda} \\ &\quad + n^{\frac{1}{2}} \left\| \int_0^t e^{(A-L_i C_i)(t-\tau)} (B a^a(\tau)) d\tau \right\|_2. \end{aligned} \quad (2.27)$$

◇

2.2.2 Unknown Input Observer Based Resilient State Estimation Method Design

In section 2.2.1, we checked that the existing observer based resilient state estimation method had a drawback on system of (2.1). Luenberger observer is used in existing RSE method. We were able to check that state estimation performance would be deteriorated largely if the effect of disturbance and actuator attack is considerable. Note that the disturbance and actuator attack affect the state estimation performance. Then, the system become vulnerable. Thus, it is essential to estimate the state correctly despite of the effect of disturbance and actuator attack. Thus, in this section, we introduce a solution to problem 2.1. The solution is UIO based RSE method.

In this section, we mainly focus on the proposed UIO based RSE method. This method guarantees that estimate of this new method converges to actual state ($\hat{x} \rightarrow x$) as time goes on ($t \rightarrow \infty$) despite of the effect of disturbance and actuator attack. The key idea of the proposed method is illustrated in Figure 2.3. We are able to expand the proposed method from the existing RSE methods [7], [11]. Key point of the proposed method is to use the UIO [3] instead of the Luenberger Observer on RSE method. The UIO has characteristics that the state estimation performance of one is not affected by the effect of disturbance and actuator attack. The important thing is that the Median approach has higher computational efficiency compared to the combinatorial method. Thus, we mainly deal with the median approach.

In this section, There are two primary parts. the first part deal with the UIO design. This section includes with the UIO basic principle, the UIO design condition for system of (2.1), and UIO design procedure. The second part deals with median operation. In this section, we discuss the basic principle of the median operation.

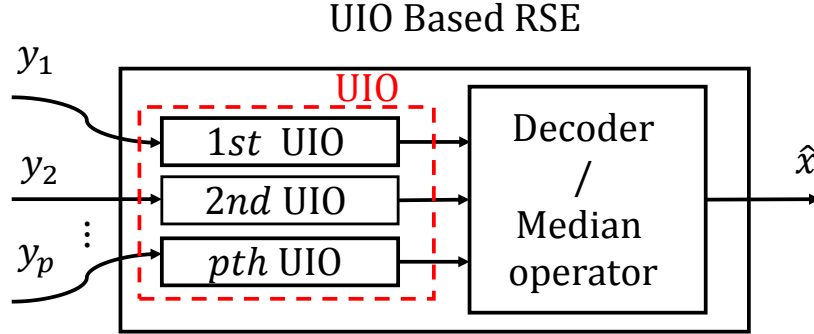


Figure 2.3: Block diagram of the proposed resilient state estimation method.

2.2.2.1 Unknown Input Observer Design

This subsection covers the UIO design condition and procedure of UIO design. Let us introduce the following UIO model:

$$\begin{aligned} \dot{g}_i(t) &= F_i g_i(t) + T_i B u(t) + K_i y_i(t), \quad i = 1, \dots, p, \\ z_i(t) &= g_i(t) + H_i y_i(t), \end{aligned} \quad (2.28)$$

where $g_i \in \mathbb{R}^n$ is i -th UIO state, $u \in \mathbb{R}$ is the system input, $y_i \in \mathbb{R}$ is i -th system output, and $z_i \in \mathbb{R}^n$ is i -th estimate of the UIO. The matrices F_i, T_i, K_i and H_i are UIO parameters that have appropriate dimensions. The system of (2.1) and the structure of the system of (2.1) and UIO is illustrated in Figure 2.4. In this Figure, The inner part in the dotted line stands for i -th UIO. System input and i -th output are needed for the UIO design. There exist particular conditions for designing the UIO.

A difference value between The system state and estimate of the i -th UIO is described as follows

$$\tilde{z}_i(t) := x(t) - z_i(t). \quad (2.29)$$

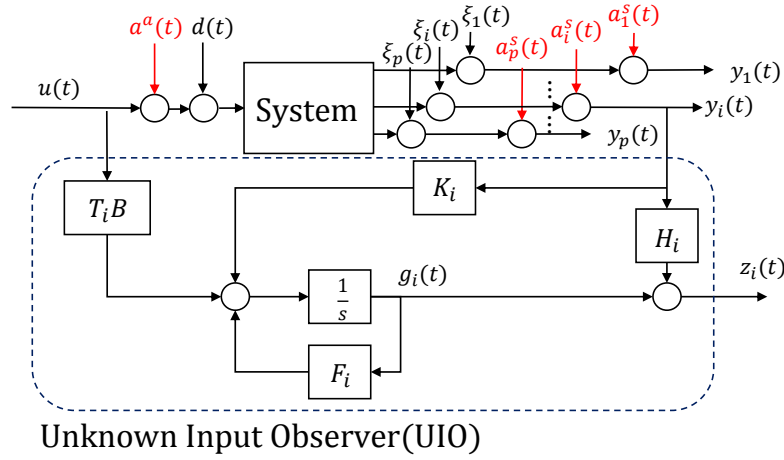


Figure 2.4: Structure of UIO.

Estimation error dynamics of (2.28) is

$$\begin{aligned}
\tilde{z}_i(t) &= \dot{x}(t) - \dot{z}_i(t) \\
&= Ax(t) + Bu(t) + Bd(t) + Ba^a(t) - \dot{g}_i(t) - H_i \dot{y}_i(t) \\
&= Ax(t) + Bu(t) + Bd(t) + Ba^a(t) - F_i g_i(t) - T_i Bu(t) - K_i y_i(t) - H_i (C_i \dot{x}(t) + \dot{\xi}_i(t) + \dot{a}_i^a(t)) \\
&= Ax(t) + Bu(t) + Bd(t) + Ba^a(t) - F_i g_i(t) - T_i Bu(t) - K_i y_i(t) \\
&\quad - H_i C_i (Ax(t) + Bu(t) + Bd(t) + Ba^a(t)) - H_i \dot{\xi}_i(t) - H_i \dot{a}_i^a(t) \\
&= Ax(t) + Bu(t) + Bd(t) + Ba^a(t) - F_i g_i(t) - T_i Bu(t) - K_i^1 y_i(t) - K_i^2 y_i(t) - H_i C_i Ax(t) \\
&\quad - H_i C_i Bu(t) - H_i C_i Bd(t) - H_i C_i Ba^a(t) - H_i \dot{\xi}_i(t) - H_i \dot{a}_i^s(t) \\
&= (A - H_i C_i A - K_i^1 C_i) x(t) + (A - H_i C_i A - K_i^1 C_i) (z_i(t) - z_i(t)) + (I - T_i - H_i C_i) Bu(t) \\
&\quad + (I - H_i C_i) (Bd(t) + Ba^a(t)) - F_i g_i(t) - K_i^2 y_i(t) \\
&\quad + (A - H_i C_i A - K_i^1 C_i) (H_i y_i(t) - H_i y_i(t)) - H_i \dot{\xi}_i(t) - K_i^1 \xi_i(t) - H_i \dot{a}_i^s(t) - K_i^1 a_i^s(t) \\
&= (A - H_i C_i A - K_i^1 C_i) (x(t) - z_i(t)) + (A - H_i C_i A - K_i^1 C_i) (z_i(t) - H_i y_i(t)) \\
&\quad + ((I - H_i C_i) - T_i) Bu(t) + (I - H_i C_i) (Bd(t) + Ba^a(t)) - F_i g_i(t) - K_i^2(t) y_i(t) \\
&\quad - (A - H_i C_i A - K_i^1 C_i) H_i y_i(t) - H_i \dot{\xi}_i(t) - K_i^1 \xi_i(t) - H_i \dot{a}_i^s(t) - K_i^1 a_i^s(t) \\
&= (A - H_i C_i A - K_i^1 C_i) (x(t) - z_i(t)) + (F_i - (A - H_i C_i A - K_i^1 C_i)) g_i(t) \\
&\quad - (T_i - (I - H_i C_i)) Bu(t) - (H_i C_i - I) (Bd(t) + Ba^a(t)) \\
&\quad - (K_i^2 - (A - H_i C_i A - K_i^1 C_i) H_i) y_i(t) - H_i \dot{\xi}_i(t) - K_i^1 \xi_i(t) - H_i \dot{a}_i^s(t) - K_i^1 a_i^s(t).
\end{aligned} \tag{2.30}$$

Then, error dynamics of equation (2.29) is as follows:

$$\begin{aligned}\dot{\tilde{z}}_i(t) = & (A - H_i C_i A - K_i^1 C_i)(x(t) - z_i(t)) + (F_i - (A - H_i C_i A - K_i^1 C_i))g_i(t) \\ & - (T_i - (I - H_i C_i))Bu(t) - (H_i C_i - I)(Bd(t) + Ba^a(t)) \\ & - (K_i^2 - (A - H_i C_i A - K_i^1 C_i)H_i)y_i(t) - H_i \dot{\xi}_i(t) - K_i^1 \xi_i(t) - H_i \dot{a}_i^s(t) - K_i^1 a_i^s(t).\end{aligned}\quad (2.31)$$

If the following conditions are satisfied,

$$(H_i C_i - I)B = 0, \quad (2.32)$$

$$T_i = I - H_i C_i, \quad (2.33)$$

$$F_i = A - H_i C_i A - K_i^1 C_i, \quad (2.34)$$

$$K_i^2 = F_i H_i. \quad (2.35)$$

Then, the state estimation error dynamics is

$$\dot{\tilde{z}}_i(t) = F_i \tilde{z}_i(t) - H_i \dot{\xi}_i(t) - K_i^1 \xi_i(t) - H_i \dot{a}_i^s(t) - K_i^1 a_i^s(t). \quad (2.36)$$

In order to facilitate an interpretation, we assume that i -th sensor attack is zero ($a_i^s = 0$). Also, we assume that noise is very small and time derivative of noise also very small. Then, equation of (2.36) become $\dot{\tilde{z}}_i(t) \approx F_i \tilde{z}_i(t)$. The objective of UIO is that $\tilde{z}_i(t)$ asymptotically converges to 0 as time goes on. In other words, it is the objective of UIO for estimate to follows actual state despite of the effect of disturbance and actuator attack. If the F_i of equation of (2.36) is Hurwitz, the $\tilde{z}_i(t)$ will asymptotically converge to zero. So as to achieve this goal, the two conditions have to be satisfied. One is to satisfy equation (2.32-2.35), making all eigenvalues of F is the second condition. Therefore, the two conditions are the essential design condition for UIO. We will explain the detailed description later. Before explaining the design condition, let us introduce two important lemmas. Lemma 2.1, lemma 2.2 and Theorem 2.2 are excerpt from [3].

Lemma 2.1. [3] *If the following equation (2.37) is satisfied, the equation (2.32) is solvable.*

$$\text{rank}(C_i B) = \text{rank}(B). \quad (2.37)$$

Then, The H_i has the special solution. it is

$$H_i^* = B((C_i B)^T (C_i B))^{-1} (C_i B)^T. \quad (2.38)$$

◆

Lemma 2.2. [3] *Let:*

$$C_i^1 = \begin{bmatrix} C_i \\ C_i A \end{bmatrix}. \quad (2.39)$$

Then, the detectability of the pair (C_i^1, A) equals to one of the pair (C_i, A) .

◆

Now, let us introduce the UIO design condition [3].

Theorem 2.2. [3] *If the following two conditions are satisfied, the UIO can be designed for the system of (2.1).*

1. *the rank of $(C_i B)$ equals to the rank of B .*
2. *The pair $(A - H_i C_i A, C_i)$ is detectable, where $H_i = B((C_i B)^T (C_i B))^{-1} (C_i B)^T$.*

◆

These two conditions are the necessary and sufficient condition in order to design the UIO. First condition is that rank of $C_i B$ must be the same with rank of B . Second condition is $(A - H_i C_i A, C_i)$ must be detectable at least. Second condition depends on H_i . Thus, It is not always satisfied, and the condition may not be satisfied depending on system matrices A , C_i , and UIO matrix H_i . Design conditions that we consider differ from existing resilient state estimation methods [11], [7]. When design condition for existing RSE method is not satisfied, UIO based RSE method condition may be satisfied.

Now, we discuss the design procedure. As we mentioned before, the first step is to check the first condition of Theorem 2.2. If the first condition is not fulfill, then we can no

longer design any UIO. Let assume that the first condition is satisfied. Then, we obtain the special solution of H_i and also T_i . Next, we focus on the second condition of Theorem 2.2. We have to check the condition such that The pair $(C_i, H_i C_i A)$ is detectable. If it is observable, We can obtain the K_i^1 so that $F_i = A - H_i C_i A - K_i^1 C_i$ is Hurwitz. Finally, we are able to get the F_i as follows

$$K_i = K_i^1 + K_i^2 = K_i^1 + F_i H_i. \quad (2.40)$$

If the pair $(C_i, H_i C_i A)$ is not observable, let's perform the observable canonical decomposition to the system pair $(C_i, H_i C_i A)$. The pair $(C_i, H_i C_i A)$ performed the coordination transformation is as follows

$$(P_i A P_i^{-1}) = \begin{bmatrix} A_i^{11} & 0 \\ A_i^{21} & A_i^{22} \end{bmatrix}, A_i^{11} \in R^{n_0 \times n_0}, \quad (2.41)$$

$$(C_i P^{-1}) = \begin{bmatrix} C_i^* & 0 \end{bmatrix}, C_i^* \in R^{m \times n_0}, \quad (2.42)$$

where n_0 is the rank of the observability matrix of the pair $(C_i, H_i C_i A)$ and the pair (C_i^*, A_i^{11}) is observable. Key point is to check whether all eigenvalues of A_i^{22} is stable. If one of the A_i^{22} 's eigenvalues is unstable, we can no longer design the UIO. If all of the eigenvalues of A_i^{22} is stable, the system pair $(C_i, H_i C_i A)$ is detectable. Plus, F_i can be described as follows by using the transformation matrix P_i :

$$\begin{aligned} F_i &= A - H_i C_i A - K_i^1 C_i, \\ &= P_i^{-1} [P_i (A - H_i C_i A) P_i^{-1} - P_i K_i^1 C_i P_i^{-1}] P_i, \\ &= P_i^{-1} \left\{ \begin{bmatrix} (A - H_i C_i A)^{11} & 0 \\ (A - H_i C_i A)^{21} & (A - H_i C_i A)^{22} \end{bmatrix} - \begin{bmatrix} \widetilde{K}_i^1 \\ \widetilde{K}_i^2 \end{bmatrix} \begin{bmatrix} C_i^* & 0 \end{bmatrix} \right\} P_i, \\ &= P_i^{-1} \begin{bmatrix} (A - H_i C_i A)^{11} - \widetilde{K}_i^1 C_i^* & 0 \\ (A - H_i C_i A)^{21} - \widetilde{K}_i^2 C_i^* & A_i^{22} \end{bmatrix}, \end{aligned} \quad (2.43)$$

where $\widetilde{K}_i = P_i K_i^1 = \begin{bmatrix} \widetilde{K}_i^1 \\ \widetilde{K}_i^2 \end{bmatrix}$ Total eigenvalues added between one of the A_i^{22} and one of the $(A - H_i C_i A)^{11} - \widetilde{K}_i^1 C_i^*$ equals the all eigenvalues of the F_i . Then, we have to determine \widetilde{K}_i^1 so that $(A - H_i C_i A)^{11} - \widetilde{K}_i^1 C_i^*$ is stable. The matrix \widetilde{K}_i^2 is determined as the arbitrary matrix. Thus, by using \widetilde{K}_i^1 and \widetilde{K}_i^2 , we can obtain K_i^1 , F_i , and K_i .

2.2.2.2 Median Operator

The section 2.2.1.1 covered UIO properties and the UIO design procedure. This section focus on a median operation. Median operation is used in order to choose the estimate that is not affected by sensor attacks. The outputs of each UIO are used as inputs of median operator. Median operator selects median value that is not affected from sensor attacks among UIO outputs. Thus, the selected value is the state of the system that is not attacked. By using obtained value from median operation, the control system can maintain normal operating condition despite of the sensor attack. i -th output is as follows

$$z_i(t) = \begin{bmatrix} z_i^1(t) \\ z_i^2(t) \\ \vdots \\ z_i^n(t) \end{bmatrix}. \quad (2.44)$$

The number of the multiplier of z_i is the number of system state. $z_i^1(t)$, $z_i^2(t)$, and $z_i^n(t)$ are the estimate of $x_i^1(t)$, $x_i^2(t)$, and $x_i^n(t)$. In other words, the i of z_i^j means the number of sensor, j is the number of the state. Median operation is as follows using each UIO output:

$$\hat{x} = \begin{bmatrix} \hat{x}^1 \\ \hat{x}^2 \\ \vdots \\ \hat{x}^n \end{bmatrix} = \begin{bmatrix} \text{median}(z_1^1, z_2^1, z_3^1, \dots, z_p^1) \\ \text{median}(z_1^2, z_2^2, z_3^2, \dots, z_p^2) \\ \vdots \\ \text{median}(z_1^n, z_2^n, z_3^n, \dots, z_p^n) \end{bmatrix}. \quad (2.45)$$

where median of the p values is given by

If p is odd,

$$\text{median}(w_1, w_2, \dots, w_p) = \left(\frac{P+1}{2}\right)^{th}. \quad (2.46)$$

If p is even,

$$\text{median}(w_1, w_2, \dots, w_p) = 0.5\left(\frac{p}{2}\right)^{th} + 0.5\left(\frac{p}{2} + 1\right)^{th}. \quad (2.47)$$

On the basis of the Assumption 2.1, UIO based RSE method is able to estimate system state correctly despite of malicious sensor attacks by using median operator. Median operation algorithm is faster and more simple than other methods. Thus, we can save the operating time for the system having tons of sensors.

2.2.3 Analysis of State Estimation Error of Proposed RSE Method

In this section, we mainly analysis the state estimation error of the proposed UIO based RSE method. The state estimation performance of the UIO based RSE method is excellent regardless of the effect of disturbance and actuator attack. In other words, the state estimation error of the UIO based RSE method is not affected by the effect of disturbance and actuator attack.

Theorem 2.3. *Suppose Assumption 2.1, 2.2, and 2.3 hold. Then, state estimation error of the system of (2.1) using UIO based RSE method is written by*

$$\|\hat{x}(t) - x(t)\|_2 \leq \nu \|\hat{x}(0) - x(0)\|_2 e^{-\lambda t} + \frac{\nu(\|K_i^1\|_2 \xi_{max} + \|H_i\|_2 \bar{\xi}_{max})}{\lambda}, \quad (2.48)$$

where $\nu > 0$ and $\lambda > 0$ are constant, n is the number of system state, ξ_{max} is bounded noise, and $\bar{\xi}_{max}$ is bounded time derivative of noise. K_i^1 and L_i are i -th UIO matrices.

◆

We would like to emphasize that state estimation error of proposed UIO based RSE method can no longer be affected by the effect of disturbance and actuator attack. The state estimation error only depends on the effect of noise and time derivative of noise even if actuator attack is considerable. The state estimation error is related to two terms.

The term $(\|\hat{x}(0) - x(0)\|_2 e^{-\lambda t})$ diminishes as time goes on. Note that inequality (2.48) implies that the state estimation error is bounded if noise and time derivative of noise are bounded.

Theorem 2.3 is proved assuming that time derivative of noise is bounded. That is, if value of time derivative of noise becomes large, it looks like that the maximum bounded state estimation error will be increased. However, when considering the sine wave with small amplitude as noise, it is confirmed through simulations that the state estimation value of UIO does not increase continuously even if the frequency is increased (This is analyzed in the mini section after the proof of Theorem 2.3). Further research is needed on how the noise differential affects the estimation error of UIO. That is, there is a need for a method that can accurately prove the maximum bounded value of the state estimation error for Theorem 2.3.

After the proof of Theorem 2.3, we analyzed how noise and time derivative of noise affect state estimation error of UIO when considering second-order system. In this case, noise is considered as a sine wave having a small amplitude and a large frequency. And then, we analyzed through the simple example how the influence of the sensor attack on the UIO state estimation error when considering the sine wave with small amplitude and high frequency as sensor attack.

Proof: Let denote \tilde{z} as state estimation error. In other words, we set that i -th state estimation error is \tilde{z}_i ($\tilde{z}_i(t) := x(t) - z_i(t)$). When the UIO model of (2.28) is applied to the system of (2.1), the state estimation error dynamics is written by

$$\begin{aligned}
\dot{\tilde{z}}_i(t) &= \dot{x}(t) - \dot{z}_i(t), \\
&= (A - H_i C_i A - K_i^1 C_i)(x(t) - z_i(t)) - (F_i - (A - H_i C_i A - K_i^1 C_i))g_i(t) \\
&\quad - (T_i - (I - H_i C_i))Bu(t) - (H_i C_i - I)(Bd(t) + Ba^a(t)) \\
&\quad - (K_i^2 - (A - H_i C_i A - K_i^1 C_i)H_i)y_i(t) - K_i^1 \xi_i(t) - H_i \dot{\xi}_i(t) - K_i^1 a_i^s(t) - H_i \dot{a}_i^s(t).
\end{aligned} \tag{2.49}$$

Since Assumption 2.2 hold, the followings are satisfied:

$$\begin{aligned}
(H_i C_i - I)B &= 0, \\
T_i &= I - H_i C_i, \\
F_i &= A - H_i C_i A - K_i^1 C_i, \\
K_i^2 &= F_i H_i, \\
K_i &= K_i^1 + K_i^2.
\end{aligned} \tag{2.50}$$

The i -th estimation error dynamics is

$$\dot{\tilde{z}}_i(t) = (A_i^1 - K_i^1 C_i)\tilde{z}_i(t) - K_i^1 \xi_i(t) - H_i \dot{\xi}_i(t) - K_i^1 a_i^s(t) - H_i \dot{a}_i^s(t). \tag{2.51}$$

The solution of equation (2.51) is as follows

$$\begin{aligned}
\tilde{z}_i(t) &= e^{(A_i^1 - K_i^1 C_i)t} \tilde{z}_i(0) + \int_0^t e^{(A_i^1 - K_i^1 C_i)(t-\tau)} (-K_i^1 \xi_i(\tau) - H_i \dot{\xi}_i(\tau) - K_i^1 a_i^s(\tau) - H_i \dot{a}_i^s(\tau)) d\tau \\
&= e^{(A_i^1 - K_i^1 C_i)t} \tilde{z}_i(0) - \int_0^t e^{(A_i^1 - K_i^1 C_i)(t-\tau)} (K_i^1 \xi_i(\tau)) d\tau - \int_0^t e^{(A_i^1 - K_i^1 C_i)(t-\tau)} (H_i \dot{\xi}_i(\tau)) d\tau \\
&\quad - \int_0^t (K_i^1 a_i^s(\tau)) d\tau - \int_0^t (H_i \dot{a}_i^s(\tau)) d\tau.
\end{aligned} \tag{2.52}$$

Denote each part in the right-hand side of (2.52) by $\bar{e}^i(t) \in \mathbb{R}^n$, $\bar{\xi}^i(t) \in \mathbb{R}$, $\bar{\xi}^i(t) \in \mathbb{R}$, $\bar{a}^i \in \mathbb{R}$, and $\bar{a}^i \in \mathbb{R}$ respectively:

$$\bar{e}^i(t) = e^{(A_i^1 - K_i^1 C_i)t} \tilde{z}_i(0), \tag{2.53}$$

$$\bar{\xi}^i(t) = - \int_0^t e^{(A_i^1 - K_i^1 C_i)(t-\tau)} (K_i^1 \xi_i(\tau)) d\tau, \tag{2.54}$$

$$\bar{\xi}^i(t) = - \int_0^t e^{(A_i^1 - K_i^1 C_i)(t-\tau)} (H_i \dot{\xi}_i(\tau)) d\tau, \tag{2.55}$$

$$\bar{a}^i(t) = - \int_0^t e^{(A_i^1 - K_i^1 C_i)(t-\tau)} (K_i^1 a_i^s(\tau)) d\tau, \tag{2.56}$$

$$\bar{a}^i(t) = - \int_0^t e^{(A_i^1 - K_i^1 C_i)(t-\tau)} (H_i \dot{a}_i^s(\tau)) d\tau. \quad (2.57)$$

Then, output of the median operator is

$$\begin{aligned} \hat{x}_j(t) = \text{med}(x_j(t) + \bar{e}_j^i(t) + \bar{\xi}_j^i(t) + \bar{\xi}_j^i(t) + \bar{a}_j^i(t) + \bar{a}_j^i(t), \dots, \\ x_j(t) + \bar{e}_j^p(t) + \bar{\xi}_j^p(t) + \bar{\xi}_j^p(t) + \bar{a}_j^p(t) + \bar{a}_j^p(t)), \quad j = 1, \dots, n. \end{aligned} \quad (2.58)$$

Each $x_j(t)$, $\bar{e}_j^p(t)$, $\bar{\xi}_j^p(t)$, $\bar{\xi}_j^p(t)$, $\bar{a}_j^p(t)$, and $\bar{a}_j^p(t)$ is the component of $x(t)$, \bar{e}^i , $\bar{\xi}^i$, $\bar{\xi}^i$, \bar{a}^i , and \bar{a}^i respectively. Since $(A - L_i C_i)$ is designed so that $(A - L_i C_i)$ is Hurwitz, there always exist the constant ν and λ for all time as follows

$$\|e^{(A_i^1 - K_i^1 C_i)t}\|_2 \leq \nu e^{-\lambda t}. \quad (2.59)$$

Each quantity of $\|\bar{e}^i(t)\|_2$, $\|\bar{\xi}^i(t)\|_2$, and $\|\bar{\xi}^i(t)\|_2$ is bounded as

$$\begin{aligned} \|\bar{e}^i\|_2 &\leq \|e^{(A_i^1 - K_i^1 C_i)t} \tilde{z}^i(0)\|_2, \\ &\leq \nu_e \|\tilde{z}^i(0)\|_2 e^{-\lambda_e t}, \\ &\leq \nu_e \|\hat{x}(0) - x(0)\|_2 e^{-\lambda_e t}. \end{aligned} \quad (2.60)$$

where $\nu_e > 0$ and $\lambda_e > 0$,

$$\begin{aligned} \|\bar{\xi}^i(t)\|_2 &\leq \left\| - \int_0^t e^{(A_i^1 - K_i^1 C_i)(t-\tau)} (K_i^1 \xi_i(\tau)) d\tau \right\|_2, \\ &\leq \|K_i^1\|_2 \xi_{max} \int_0^t \|e^{(A_i^1 - K_i^1 C_i)(t-\tau)}\|_2 d\tau, \\ &= \|K_i^1\|_2 \xi_{max} \int_0^t \|e^{(A_i^1 - K_i^1 C_i)(\tau)}\|_2 d\tau, \\ &\leq \|K_i^1\|_2 \xi_{max} \frac{\nu_\xi}{\lambda_\xi} (1 - e^{-\lambda_\xi t}), \\ &\leq \|K_i^1\|_2 \xi_{max} \frac{\nu_\xi}{\lambda_\xi}, \end{aligned} \quad (2.61)$$

where $\nu_\xi > 0$ and $\lambda_\xi > 0$,

$$\begin{aligned}
\|\bar{\xi}^i(t)\|_2 &\leq \left\| - \int_0^t e^{(A_i^1 - K_i^1 C_i)(t-\tau)} (H_i \dot{\xi}_i(\tau)) d\tau \right\|_2, \\
&\leq \|H_i\|_2 \bar{\xi}_{max} \int_0^t \|e^{(A_i^1 - K_i^1 C_i)(t-\tau)}\|_2 d\tau, \\
&= \|H_i\|_2 \bar{\xi}_{max} \int_0^t \|e^{(A_i^1 - K_i^1 C_i)(\tau)}\|_2 d\tau, \\
&\leq \|H_i\|_2 \bar{\xi}_{max} \frac{\nu_{\bar{\xi}}}{\lambda_{\bar{\xi}}} (1 - e^{-\lambda_{\bar{\xi}} t}), \\
&\leq \|H_i\|_2 \bar{\xi}_{max} \frac{\nu_{\bar{\xi}}}{\lambda_{\bar{\xi}}},
\end{aligned} \tag{2.62}$$

where $\nu_{\bar{\xi}} > 0$ and $\lambda_{\bar{\xi}} > 0$.

The $\bar{e}_j^i, \bar{\xi}_j^i$, and $\bar{\xi}_j^i$ belong to the $\bar{e}^i, \bar{\xi}^i$, and $\bar{\xi}^i$ respectively. It satisfies the followings:

$$|\bar{e}_j^i| \leq \|\bar{e}^i(t)\|_2, \tag{2.63}$$

$$|\bar{\xi}_j^i| \leq \|\bar{\xi}^i(t)\|_2, \tag{2.64}$$

$$|\bar{\xi}_j^i| \leq \|\bar{\xi}^i(t)\|_2. \tag{2.65}$$

Let $\bar{\eta}_j^i = \bar{e}_j^i + \bar{\xi}_j^i + \bar{\xi}_j^i$, $i = 1, \dots, p$, $j = 1, \dots, n$.

By using Median operation, we can express the \hat{x}_j as follows

$$\hat{x}_j = med(x_j + \bar{\eta}_j^1 + \bar{a}_j^1 + \bar{a}_j^1, \dots, x_j + \bar{\eta}_j^p + \bar{a}_j^p + \bar{a}_j^p), \quad j = 1, \dots, n. \tag{2.66}$$

Also,

$$|\hat{x}_j - x_j| \leq max(|\bar{\eta}_j^i|), \quad i = 1, \dots, p, \quad j = 1, \dots, n. \tag{2.67}$$

The $max(|\bar{\eta}_j^i|)$ is bounded as follows

$$\begin{aligned} \max(|\bar{\eta}_j^i|) &= \max|\bar{e}_j^i + \bar{\xi}_j^i + \bar{\xi}_j^i| \quad i = 1, \dots, p, \quad j = 1, \dots, n, \\ &\leq \max(|\bar{e}_j^i|) + \max(|\bar{\xi}_j^i|) + \max(|\bar{\xi}_j^i|). \end{aligned} \quad (2.68)$$

Then,

$$\begin{aligned} \|\hat{x}(t) - x(t)\|_2 &\leq n^{\frac{1}{2}} \max(|\hat{x}_j - x_j|, \quad j = 1, \dots, n), \\ &\leq n^{\frac{1}{2}} (\max(|\bar{e}_j^i|) + \max(|\bar{\xi}_j^i|) + \max(|\bar{\xi}_j^i|)), \\ &\leq n^{\frac{1}{2}} (\nu_e \|\hat{x}(0) - x(0)\|_2 e^{-\lambda_e t} + \frac{\nu_\xi \|K_i^1\|_2 \xi_{\max}}{\lambda_\xi} + \frac{\nu_{\bar{\xi}} \|H_i\|_2 \bar{\xi}_{\max}}{\lambda_{\bar{\xi}}}). \end{aligned} \quad (2.69)$$

If we choose $\nu > n^{\frac{1}{2}} \max(\nu_e, \nu_\xi, \nu_{\bar{\xi}})$ and $0 < \lambda < \min(\lambda_e, \lambda_\xi, \lambda_{\bar{\xi}})$, we can express the equation (2.69) as follows

$$\|\hat{x}(t) - x(t)\|_2 \leq \nu \|\hat{x}(0) - x(0)\|_2 e^{-\lambda t} + \frac{\nu (\|K_i^1\|_2 \xi_{\max} + \|H_i\|_2 \bar{\xi}_{\max})}{\lambda}. \quad (2.70)$$

◇

Now, we discuss the effect of noise and time derivative of noise. We made a mini section in order to analyze the effect of noise and time derivative of noise. The state estimation error dynamics of system of (2.1) is as follows

$$\dot{\tilde{z}}_i(t) = F_i \tilde{z}_i(t) - K_i^1 \xi_i(t) - H_i \dot{\xi}_i(t) - K_i^1 a_i^s(t) - H_i \dot{a}_i^s(t). \quad (2.71)$$

In order to facilitate an interpretation, we assume that i -th sensor attack is zero ($a_i^s = 0$). Only in this mini section (analysis of the effect of noise and time derivative of noise), we consider second order system having single input ($\tilde{z}_i \in \mathbb{R}^2$, $\xi_i \in \mathbb{R}$, $F_i \in \mathbb{R}^{2 \times 2}$, $H_i \in \mathbb{R}^{2 \times 1}$, and $K_i^1 \in \mathbb{R}^{2 \times 1}$). Then,

$$\dot{\tilde{z}}_i(t) = F_i \tilde{z}_i(t) - K_i^1 \xi_i(t) - H_i \dot{\xi}_i(t). \quad (2.72)$$

Solution of error dynamics is written by

$$\tilde{z}_i(t) = e^{F_i(t)}\tilde{z}(0) - \int_0^t e^{F_i(t-\tau)} K_i^1 \xi_i(\tau) d\tau - \int_0^t e^{F_i(t-\tau)} H_i \dot{\xi}_i(\tau) d\tau. \quad (2.73)$$

Since F_i is Hurwitz, $e^{F_i(t)}\tilde{z}(0)$ converges to zero as time goes on. But, noise and time derivative of noise affect state estimation error. we consider sine wave as noise:

$$\begin{aligned} \xi_i(t) &= \varepsilon \sin(\omega t), \\ \dot{\xi}_i(t) &= \varepsilon \omega \sin(\omega t), \end{aligned} \quad (2.74)$$

where ε is amplitude of sine wave and ω is frequency of sine wave. We will check whether error becomes large if ω is large (noise commonly has a high frequency). Firstly, we check the effect of noise. Denote the effect of noise by $\bar{n}(t)$. Then,

$$\begin{aligned} \bar{n}_i(t) &= \begin{bmatrix} \bar{n}_{i(1,1)}(t) \\ \bar{n}_{i(2,1)}(t) \end{bmatrix}, \\ &:= \int_0^t e^{F_i(t-\tau)} K_i^1 \xi(\tau) d\tau, \\ &= \int_0^t e^{F_i(t-\tau)} K_i^1 \varepsilon \sin(\omega \tau) d\tau, \end{aligned} \quad (2.75)$$

where $\bar{n}_i \in \mathbb{R}^2$. Let we calculate above equation by using MATLAB. Then,

$$\begin{aligned} \bar{n}_{i(1,1)}(t) &= [-V_{i(1,1)}^{-1} V_{i(1,1)} K_{i(1,1)}^1 \varepsilon \lambda_{i(1)} \sin(\omega t) + V_{i(1,1)}^{-1} V_{i(1,1)} K_{i(1,1)}^1 \varepsilon \omega e^{\lambda_{i(1)} t} \\ &\quad + V_{i(1,1)}^{-1} V_{i(1,1)} K_{i(1,1)}^1 \varepsilon \cos(\omega t)] / (\lambda_{i(1)}^2 + \omega^2) \\ &\quad [-V_{i(1,2)}^{-1} V_{i(1,1)} K_{i(2,1)}^1 \varepsilon \lambda_{i(1)} \sin(\omega t) + V_{i(1,2)}^{-1} V_{i(1,1)} K_{i(2,1)}^1 \varepsilon \omega e^{\lambda_{i(1)} t} \\ &\quad + V_{i(1,2)}^{-1} V_{i(1,1)} K_{i(2,1)}^1 \varepsilon \cos(\omega t)] / (\lambda_{i(1)}^2 + \omega^2) \\ &\quad [-V_{i(2,1)}^{-1} V_{i(1,2)} K_{i(1,1)}^1 \varepsilon \lambda_{i(2)} \sin(\omega t) + V_{i(2,1)}^{-1} V_{i(1,2)} K_{i(1,1)}^1 \varepsilon \omega e^{\lambda_{i(2)} t} \\ &\quad + V_{i(2,1)}^{-1} V_{i(1,2)} K_{i(1,1)}^1 \varepsilon \cos(\omega t)] / (\lambda_{i(2)}^2 + \omega^2) \\ &\quad [-V_{i(2,2)}^{-1} V_{i(1,2)} K_{i(2,1)}^1 \varepsilon \lambda_{i(2)} \sin(\omega t) + V_{i(2,2)}^{-1} V_{i(1,2)} K_{i(2,1)}^1 \varepsilon \omega e^{\lambda_{i(2)} t} \\ &\quad + V_{i(2,2)}^{-1} V_{i(1,2)} K_{i(2,1)}^1 \varepsilon \cos(\omega t)] / (\lambda_{i(2)}^2 + \omega^2), \end{aligned} \quad (2.76)$$

$$\begin{aligned}
\bar{n}_{i(2,1)}(t) = & [-V_{i(1,1)}^{-1}V_{i(2,1)}K_{i(1,1)}^1\varepsilon\lambda_{i(1)}\sin(\omega t) + V_{i(1,1)}^{-1}V_{i(2,1)}K_{i(1,1)}^1\varepsilon\omega e^{\lambda_{i(1)}t} \\
& + V_{i(1,1)}^{-1}V_{i(2,1)}K_{i(1,1)}^1\varepsilon\cos(\omega t)]/(\lambda_{i(1)}^2 + \omega^2) \\
& [-V_{i(1,2)}^{-1}V_{i(2,1)}K_{i(2,1)}^1\varepsilon\lambda_{i(1)}\sin(\omega t) + V_{i(1,2)}^{-1}V_{i(2,1)}K_{i(2,1)}^1\varepsilon\omega e^{\lambda_{i(1)}t} \\
& + V_{i(1,2)}^{-1}V_{i(2,1)}K_{i(2,1)}^1\varepsilon\cos(\omega t)]/(\lambda_{i(1)}^2 + \omega^2) \\
& [-V_{i(2,1)}^{-1}V_{i(2,2)}K_{i(1,1)}^1\varepsilon\lambda_{i(2)}\sin(\omega t) + V_{i(2,1)}^{-1}V_{i(2,2)}K_{i(1,1)}^1\varepsilon\omega e^{\lambda_{i(2)}t} \\
& + V_{i(2,1)}^{-1}V_{i(2,2)}K_{i(1,1)}^1\varepsilon\cos(\omega t)]/(\lambda_{i(2)}^2 + \omega^2) \\
& [-V_{i(2,2)}^{-1}V_{i(2,2)}K_{i(2,1)}^1\varepsilon\lambda_{i(2)}\sin(\omega t) + V_{i(2,2)}^{-1}V_{i(2,2)}K_{i(2,1)}^1\varepsilon\omega e^{\lambda_{i(2)}t} \\
& + V_{i(2,2)}^{-1}V_{i(2,2)}K_{i(2,1)}^1\varepsilon\cos(\omega t)]/(\lambda_{i(2)}^2 + \omega^2),
\end{aligned} \tag{2.77}$$

where V_i is a matrix whose columns are eigenvectors of F_i , $V_{i(j,k)}$ is a j -th row and k -th column of a matrix V_i , $\lambda_{i(j)}$ is j -th eigenvalue of F_i , and $K_{i(j,k)}^1$ is a j -th row and k -th column of a matrix K_i^1 .

If $\omega \rightarrow \infty$,

$$\bar{n}_{i(1,1)}(t) \approx 0, \tag{2.78}$$

$$\bar{n}_{i(2,1)}(t) \approx 0. \tag{2.79}$$

Thus, the effect of noise is very small if frequency of noise (sine wave) is large. Secondly, we check the effect of time derivative of noise. Denote the effect of time derivative of noise by $\bar{\psi}_i(t)$. Then,

$$\begin{aligned}
\bar{\psi}_i(t) &= \begin{bmatrix} \bar{\psi}_{i(1,1)}(t) \\ \bar{\psi}_{i(2,1)}(t) \end{bmatrix}, \\
&:= \int_0^t e^{F_i(t-\tau)} H_i \xi(\tau) d\tau, \\
&= \int_0^t e^{F_i(t-\tau)} H_i \varepsilon \omega \cos(\omega \tau) d\tau,
\end{aligned} \tag{2.80}$$

where $\bar{n}_i \in \mathbb{R}^2$. Let we calculate above equation by using MATLAB. Then,

$$\begin{aligned}
\bar{\psi}_{i(1,1)}(t) = & [V_{i(1,1)}^{-1} V_{i(1,1)} H_{i(1,1)} \varepsilon \omega^2 \sin(\omega t) + V_{i(1,1)}^{-1} V_{i(1,1)} H_{i(1,1)} \varepsilon \omega \lambda_{i(1)} e^{\lambda_{i(1)} t} \\
& - V_{i(1,1)}^{-1} V_{i(1,1)} H_{i(1,1)} \varepsilon \omega \lambda_{i(1)} \cos(\omega t)] / (\lambda_{i(1)}^2 + \omega^2) \\
& [V_{i(1,2)}^{-1} V_{i(1,1)} H_{i(2,1)} \varepsilon \omega^2 \sin(\omega t) + V_{i(1,2)}^{-1} V_{i(1,1)} H_{i(2,1)} \varepsilon \omega \lambda_{i(1)} e^{\lambda_{i(1)} t} \\
& - V_{i(1,2)}^{-1} V_{i(1,1)} H_{i(2,1)} \varepsilon \omega \lambda_{i(1)} \cos(\omega t)] / (\lambda_{i(1)}^2 + \omega^2) \\
& [V_{i(2,1)}^{-1} V_{i(1,2)} H_{i(1,1)} \varepsilon \omega^2 \sin(\omega t) + V_{i(2,1)}^{-1} V_{i(1,2)} H_{i(1,1)} \varepsilon \omega \lambda_{i(2)} e^{\lambda_{i(2)} t} \\
& - V_{i(2,1)}^{-1} V_{i(1,2)} H_{i(1,1)} \varepsilon \omega \lambda_{i(2)} \cos(\omega t)] / (\lambda_{i(2)}^2 + \omega^2) \\
& [V_{i(2,2)}^{-1} V_{i(1,2)} H_{i(2,1)} \varepsilon \omega^2 \sin(\omega t) + V_{i(2,2)}^{-1} V_{i(1,2)} H_{i(2,1)} \varepsilon \omega \lambda_{i(2)} e^{\lambda_{i(2)} t} \\
& - V_{i(2,2)}^{-1} V_{i(1,2)} H_{i(2,1)} \varepsilon \omega \lambda_{i(2)} \cos(\omega t)] / (\lambda_{i(2)}^2 + \omega^2),
\end{aligned} \tag{2.81}$$

$$\begin{aligned}
\bar{\psi}_{i(2,1)}(t) = & [V_{i(1,1)}^{-1} V_{i(2,1)} H_{i(1,1)} \varepsilon \omega^2 \sin(\omega t) + V_{i(1,1)}^{-1} V_{i(2,1)} H_{i(1,1)} \varepsilon \omega \lambda_{i(1)} e^{\lambda_{i(1)} t} \\
& - V_{i(1,1)}^{-1} V_{i(2,1)} H_{i(1,1)} \varepsilon \omega \lambda_{i(1)} \cos(\omega t)] / (\lambda_{i(1)}^2 + \omega^2) \\
& [V_{i(1,2)}^{-1} V_{i(2,1)} H_{i(2,1)} \varepsilon \omega^2 \sin(\omega t) + V_{i(1,2)}^{-1} V_{i(2,1)} H_{i(2,1)} \varepsilon \omega \lambda_{i(1)} e^{\lambda_{i(1)} t} \\
& - V_{i(1,2)}^{-1} V_{i(2,1)} H_{i(2,1)} \varepsilon \omega \lambda_{i(1)} \cos(\omega t)] / (\lambda_{i(1)}^2 + \omega^2) \\
& [V_{i(2,1)}^{-1} V_{i(2,2)} H_{i(1,1)} \varepsilon \omega^2 \sin(\omega t) + V_{i(2,1)}^{-1} V_{i(2,2)} H_{i(1,1)} \varepsilon \omega \lambda_{i(2)} e^{\lambda_{i(2)} t} \\
& - V_{i(2,1)}^{-1} V_{i(2,2)} H_{i(1,1)} \varepsilon \omega \lambda_{i(2)} \cos(\omega t)] / (\lambda_{i(2)}^2 + \omega^2) \\
& [V_{i(2,2)}^{-1} V_{i(2,2)} H_{i(2,1)} \varepsilon \omega^2 \sin(\omega t) + V_{i(2,2)}^{-1} V_{i(2,2)} H_{i(2,1)} \varepsilon \omega \lambda_{i(2)} e^{\lambda_{i(2)} t} \\
& - V_{i(2,2)}^{-1} V_{i(2,2)} H_{i(2,1)} \varepsilon \omega \lambda_{i(2)} \cos(\omega t)] / (\lambda_{i(2)}^2 + \omega^2),
\end{aligned} \tag{2.82}$$

where V_i is a matrix whose columns are eigenvectors of F_i , $V_{i(j,k)}$ is a j -th row and k -th column of a matrix V_i , $\lambda_{i(j)}$ is j -th eigenvalue of F_i , and $H_{i(j,k)}$ is a j -th row and k -th column of a matrix H_i .

If $\omega \rightarrow \infty$,

$$\begin{aligned}
\bar{\psi}_{i(1,1)}(t) &\approx \frac{V_{i(1,1)}^{-1} V_{i(1,1)} H_{i(1,1)} \varepsilon \omega^2 \sin(\omega t)}{\lambda_{i(1)}^2 + \omega^2} + \frac{V_{i(1,2)}^{-1} V_{i(1,1)} H_{i(2,1)} \varepsilon \omega^2 \sin(\omega t)}{\lambda_{i(1)}^2 + \omega^2} \\
&\quad + \frac{V_{i(2,1)}^{-1} V_{i(1,2)} H_{i(1,1)} \varepsilon \omega^2 \sin(\omega t)}{\lambda_{i(1)}^2 + \omega^2} + \frac{V_{i(2,2)}^{-1} V_{i(1,2)} H_{i(2,1)} \varepsilon \omega^2 \sin(\omega t)}{\lambda_{i(1)}^2 + \omega^2}, \quad (2.83) \\
&\approx (V_{i(1,1)}^{-1} V_{i(1,1)} H_{i(1,1)} + V_{i(1,2)}^{-1} V_{i(1,1)} H_{i(2,1)} + V_{i(2,1)}^{-1} V_{i(1,2)} H_{i(1,1)} \\
&\quad + V_{i(2,2)}^{-1} V_{i(1,2)} H_{i(2,1)}) \varepsilon \sin(\omega t),
\end{aligned}$$

$$\begin{aligned}
\bar{\psi}_{i(2,1)}(t) &\approx \frac{V_{i(1,1)}^{-1} V_{i(2,1)} H_{i(1,1)} \varepsilon \omega^2 \sin(\omega t)}{\lambda_{i(1)}^2 + \omega^2} + \frac{V_{i(1,2)}^{-1} V_{i(2,1)} H_{i(2,1)} \varepsilon \omega^2 \sin(\omega t)}{\lambda_{i(1)}^2 + \omega^2} \\
&\quad + \frac{V_{i(2,1)}^{-1} V_{i(2,2)} H_{i(1,1)} \varepsilon \omega^2 \sin(\omega t)}{\lambda_{i(1)}^2 + \omega^2} + \frac{V_{i(2,2)}^{-1} V_{i(2,2)} H_{i(2,1)} \varepsilon \omega^2 \sin(\omega t)}{\lambda_{i(1)}^2 + \omega^2}, \quad (2.84) \\
&\approx (V_{i(1,1)}^{-1} V_{i(2,1)} H_{i(1,1)} + V_{i(1,2)}^{-1} V_{i(2,1)} H_{i(2,1)} + V_{i(2,1)}^{-1} V_{i(2,2)} H_{i(1,1)} \\
&\quad + V_{i(2,2)}^{-1} V_{i(2,2)} H_{i(2,1)}) \varepsilon \sin(\omega t).
\end{aligned}$$

Since ω^2 is canceled each other if ω is large, the effect of time derivative of noise has a bounded value. In other words, even if frequency of noise increases continuously, the part affected by time derivative of noise does not increase continuously but has a bounded value.

Example 1: In this example, we check the effect of noise and time derivative of noise by using simulation. Let consider the following model:

$$\begin{aligned}
\dot{x}(t) &= Ax(t) + Bu(t), \\
y(t) &= Cx(t) + \xi(t),
\end{aligned} \quad (2.85)$$

where $A = \begin{bmatrix} -3 & 4 \\ 3 & 2 \end{bmatrix}$, $B = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 1 \end{bmatrix}$, initial state $x(0)=0$, and $\xi(t) = \varepsilon \sin(\omega t)$.

We set ε and ω are 0.1 and 1000 rad/sec respectively. UIO model is

$$\begin{aligned}
\dot{g}(t) &= Fg(t) + TBu(t) + Ky(t), \\
\hat{x}(t) &= g(t) + Hy(t),
\end{aligned} \quad (2.86)$$

where $F = \begin{bmatrix} -8 & 5 \\ -2 & -5 \end{bmatrix}$, $T = \begin{bmatrix} 0.3333 & -0.6667 \\ -0.3333 & 0.6667 \end{bmatrix}$, $H = \begin{bmatrix} 0.6667 \\ 0.3333 \end{bmatrix}$, $K = \begin{bmatrix} -2 \\ 2 \end{bmatrix}$, $K^1 = \begin{bmatrix} 5 \\ 5 \end{bmatrix}$, and initial state $g(0)=0$. We consider that $(\tilde{z} := x - \hat{x})$. Then, error dynamics is

$$\dot{\tilde{z}}(t) = F\tilde{z}(t) - K^1\xi(t) - H\dot{\xi}(t). \quad (2.87)$$

Solution of above equation is as follows

$$\tilde{z}(t) = e^{Ft}\tilde{z}(0) + \bar{n}(t) + \bar{\psi}(t), \quad (2.88)$$

where $\bar{n}(t) := \int_0^t e^{F(t-\tau)} K^1 \xi(\tau) d\tau$ and $\bar{\psi}(t) := \int_0^t e^{F(t-\tau)} H \dot{\xi}(\tau) d\tau$. Since we consider that initial state is zero, above equation is written by

$$\tilde{z}(t) = \bar{n}(t) + \bar{\psi}(t). \quad (2.89)$$

Firstly, let we check the effect of $\bar{n}(t)$. Refer to equations of (2.78)-(2.79). Since ω is 1000 rad/sec, $\bar{n}(t)$ is

$$\bar{n}_{(1,1)}(t) \approx 0, \quad (2.90)$$

$$\bar{n}_{(2,1)}(t) \approx 0, \quad (2.91)$$

where $\bar{n}_{(j,1)}$ is j -th row element of matrix \bar{n} . Secondly, let we check the effect of $\bar{\psi}(t)$. Refer to equations of (2.83)-(2.84). Since ω is 1000 rad/sec, $\bar{\psi}(t)$ is

$$\begin{aligned} \bar{\psi}_{(1,1)}(t) &\approx (V_{(1,1)}^{-1}V_{(1,1)}H_{(1,1)} + V_{(1,2)}^{-1}V_{(1,1)}H_{(2,1)} + V_{(2,1)}^{-1}V_{(1,2)}H_{(1,1)} \\ &\quad + V_{(2,2)}^{-1}V_{(1,2)}H_{(2,1)})\varepsilon \sin(\omega t), \\ &= 0.6667\varepsilon \sin(1000t), \\ &= 0.06667\sin(1000t), \end{aligned} \quad (2.92)$$

$$\begin{aligned} \bar{\psi}_{(2,1)}(t) &\approx (V_{(1,1)}^{-1}V_{(2,1)}H_{(1,1)} + V_{(1,2)}^{-1}V_{(2,1)}H_{(2,1)} + V_{(2,1)}^{-1}V_{(2,2)}H_{(1,1)} \\ &\quad + V_{(2,2)}^{-1}V_{(2,2)}H_{(2,1)})\varepsilon \sin(\omega t), \\ &= 0.3333\varepsilon \sin(1000t), \\ &= 0.03333\sin(1000t), \end{aligned} \quad (2.93)$$

where V is a matrix whose columns are eigenvectors of F , $V_{(j,k)}$ is a j -th row and k -th column of a matrix V , and $H_{(j,k)}$ is a j -th row and k -th column of a matrix H . Even if frequency is very large, we are able to calculate the bounded values affected by time derivative of noise. Let us check a simulation. We see that error does not get large even if ω increases. Also, we can figure out that the amplitudes of (2.92)-(2.93) nearly equal to simulation results.

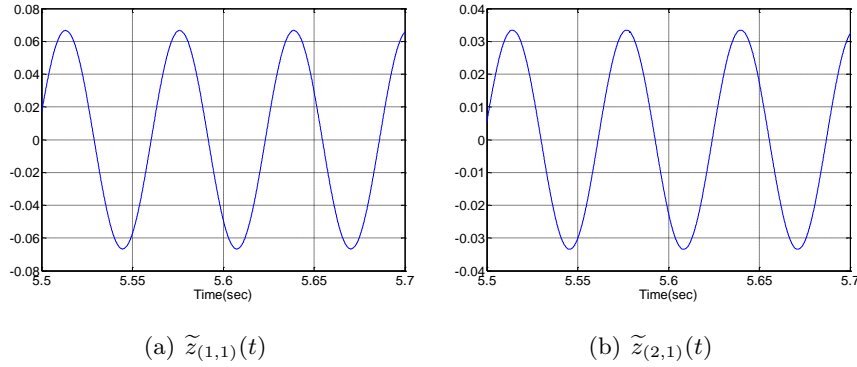


Figure 2.5: Error between actual state and estimate when we set frequency to 100 rad/sec.

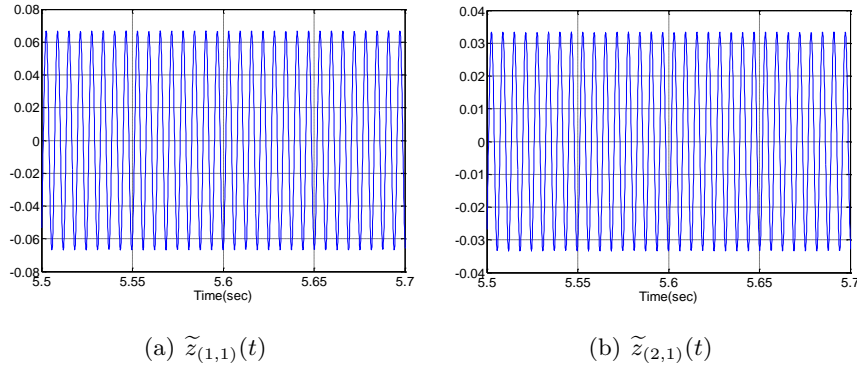


Figure 2.6: Error between actual state and estimate when we set frequency to 1000 rad/sec.

Finally, we consider the following equation as a sensor attack similar to the above case. In this case, we consider that ε is small and ω is very large. We will analyze whether the following sensor attack affects the state estimation performance of UIO with one example.

$$a^s(t) = \varepsilon \sin(\omega t) \quad (2.94)$$

Example 2: We consider numerical example.

$$\begin{aligned}\dot{x}(t) &= \begin{bmatrix} 2.1 & 3.5 \\ 1.3 & -2.5 \end{bmatrix} x(t) + \begin{bmatrix} 0.75 \\ 2.8 \end{bmatrix} u(t), \\ y(t) &= \begin{bmatrix} 1 & 1 \end{bmatrix} x(t) + a^s(t),\end{aligned}\tag{2.95}$$

where $a^s(t) = \varepsilon \sin(\omega t)$ and initial state is zero. We set ε and ω are 0.01 and 3000 rad/sec respectively. UIO model is

$$\begin{aligned}\dot{g}(t) &= Fg(t) + TBu(t) + Ky(t), \\ \hat{x}(t) &= g(t) + Hy(t),\end{aligned}\tag{2.96}$$

where $F = \begin{bmatrix} -3.6183 & -1.7113 \\ -6.3817 & -8.2887 \end{bmatrix}$, $T = \begin{bmatrix} 0.7887 & -0.2113 \\ -0.7887 & 0.2113 \end{bmatrix}$, $H = \begin{bmatrix} 0.2113 \\ 0.7887 \end{bmatrix}$, $K = \begin{bmatrix} 2.8858 \\ -2.8858 \end{bmatrix}$, $K^1 = \begin{bmatrix} 5 \\ 5 \end{bmatrix}$, and initial state $g(0)=0$. We consider that ($\tilde{z} := x - \hat{x}$). Then, error dynamics is as follows

$$\dot{\tilde{z}}(t) = F\tilde{z}(t) - K^1 a^s(t) - H\dot{a}^s(t).\tag{2.97}$$

Solution of above equation is

$$\tilde{z}(t) = e^{Ft}\tilde{z}(0) + \int_0^t e^{F(t-\tau)} K^1 a^s(\tau) d\tau + \int_0^t e^{F(t-\tau)} H \dot{a}^s(\tau) d\tau.\tag{2.98}$$

Denote $\bar{a}^s(t) := \int_0^t e^{F(t-\tau)} K^1 a^s(\tau) d\tau$ and $\bar{\psi}^s(t) := \int_0^t e^{F(t-\tau)} H \dot{a}^s(\tau) d\tau$. Then,

$$\tilde{z}(t) = e^{Ft}\tilde{z}(0) + \bar{a}^s(t) + \bar{\psi}^s(t).\tag{2.99}$$

Since we consider that initial condition is zero, above equation is written by

$$\tilde{z}(t) = \bar{a}^s(t) + \bar{\psi}^s(t).\tag{2.100}$$

Firstly, let we check the effect of $\bar{a}^s(t)$. Refer to equations of (2.78)-(2.79). Since ω is very large, $\bar{a}^s(t)$ can be approximated. $\bar{a}^s(t)$ is

$$\bar{a}_{(1,1)}^s(t) \approx 0, \quad (2.101)$$

$$\bar{a}_{(2,1)}^s(t) \approx 0, \quad (2.102)$$

where $\bar{a}_{(j,1)}^s$ is j -th row element of matrix \bar{n} . Secondly, let we check the effect of $\bar{\psi}^s(t)$. Refer to equations of (2.81)-(2.82). Since ω is very large, $\bar{\psi}^s(t)$ can be approximated. $\bar{\psi}^s(t)$ is

$$\begin{aligned} \bar{\psi}_{(1,1)}^s(t) &\approx (V_{(1,1)}^{-1}V_{(1,1)}H_{(1,1)} + V_{(1,2)}^{-1}V_{(1,1)}H_{(2,1)} + V_{(2,1)}^{-1}V_{(1,2)}H_{(1,1)} \\ &\quad + V_{(2,2)}^{-1}V_{(1,2)}H_{(2,1)})\varepsilon\sin(\omega t), \\ &= 0.2113\varepsilon\sin(3000t), \\ &= 0.002113\sin(3000t), \end{aligned} \quad (2.103)$$

$$\begin{aligned} \bar{\psi}_{(2,1)}^s(t) &\approx (V_{(1,1)}^{-1}V_{(2,1)}H_{(1,1)} + V_{(1,2)}^{-1}V_{(2,1)}H_{(2,1)} + V_{(2,1)}^{-1}V_{(2,2)}H_{(1,1)} \\ &\quad + V_{(2,2)}^{-1}V_{(2,2)}H_{(2,1)})\varepsilon\sin(\omega t), \\ &= 0.7887\varepsilon\sin(3000t), \\ &= 0.007887\sin(3000t), \end{aligned} \quad (2.104)$$

where V is a matrix whose columns are eigenvectors of F , $V_{(j,k)}$ is a j -th row and k -th column of a matrix V , and $H_{(j,k)}$ is a j -th row and k -th column of a matrix H . Now, let we check a simulation. We illustrate error between actual state and estimate in Figure 2.7. We can see that the amplitudes of (2.103)-(2.104) nearly equal to simulation results.

Equations of (2.103)-(2.104) and simulations show that the sinusoidal attack, which is very small in amplitude and large in frequency, does not significantly affect the state estimation performance of UIO. That is, this type of attack does not have a significant impact on the system that uses UIO state values.

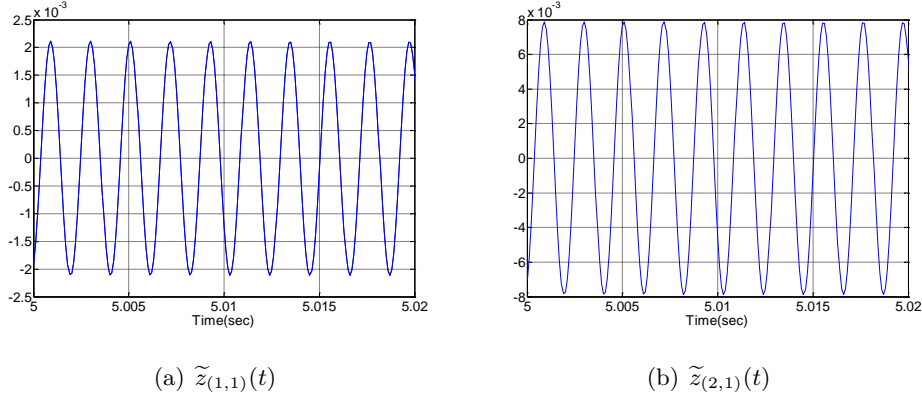


Figure 2.7: Error between actual state and estimate.

2.2.4 Diagnosis Method of the System under Sensor Attack and Fault

In this section, we explain the diagnostic algorithm in the presence of attack or fault. The proposed UIO based Resilient State Estimation method is used for the diagnosis. The objective of the proposed diagnostic method is to notify which sensors are attacked or have a break down. The Figure 2.8 shows the block diagram of the diagnosis method under attack. Basic principle is to subtract each state obtained by UIO from estimate state obtained by Median operation. If there exist sensor attacks on some of sensors and the absolute value of $(\hat{x} - z_i)$ is smaller than the residual value, the system regarded as normal. If the absolute value of $(\hat{x} - z_i)$ is larger than the residual value, the alarm is triggered. Then, the system is able to know which sensors are influenced by attack or the fault. By using this diagnosis method, we are able to check the condition of each sensor in real time. Also, By using this method, we are able to use the sensor that is not attacked.

Now, we discuss how to set residual value. In this section, we only focus on the case of having sensors that measures same physical quantity. A case of considering sensors that measure different physical quantity is future work. We assume that Assumption 2.1-2.3 are hold and each UIO has same design condition. Considering the case of no attack, i -th UIO model is given by

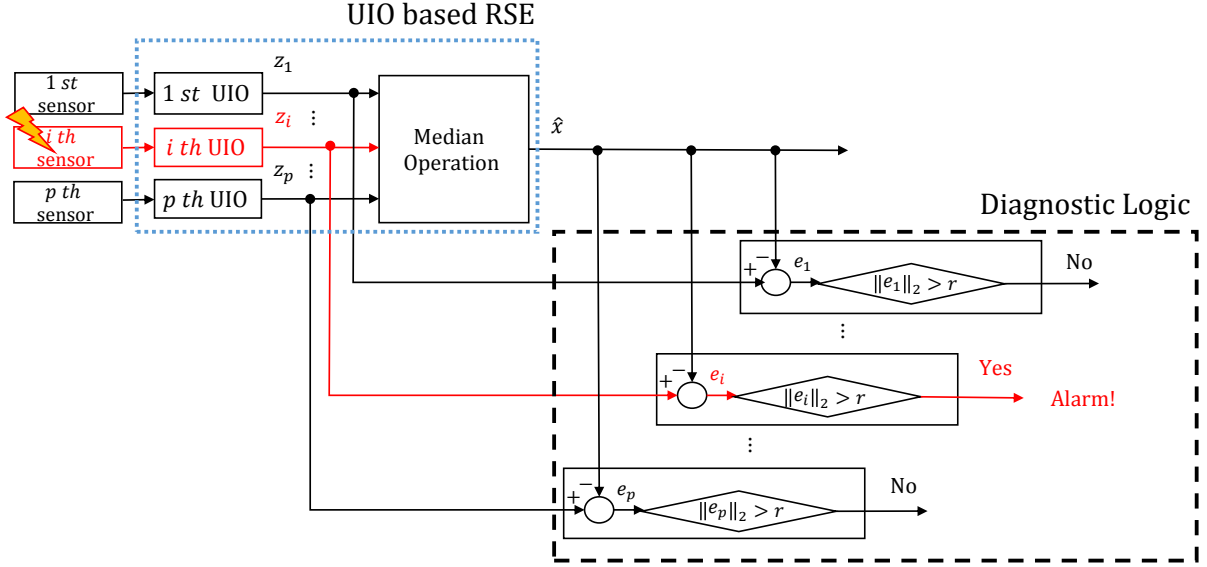


Figure 2.8: Block diagram of the diagnosis method under sensor attack.

$$\begin{aligned}
 \dot{g}_i(t) &= F_i g_i(t) + T_i B u(t) + K_i y_i(t), \\
 &= F_i g_i(t) + T_i B u(t) + K_i C_i x(t) + K_i \xi_i(t), \\
 z_i(t) &= g_i(t) + H_i y_i(t), \\
 &= g_i(t) + H_i C_i x(t) + H_i \xi_i(t),
 \end{aligned} \tag{2.105}$$

where $g_i \in \mathbb{R}^n$ is i -th UIO state, $u \in \mathbb{R}$ is system input, $y_i \in \mathbb{R}$ is i -th system output, $x \in \mathbb{R}^n$ is system state, $\xi_i \in \mathbb{R}$ is i -th sensor noise, and $z_i \in \mathbb{R}^n$ is output of i -th UIO ($\hat{x} := z_i$). F_i , T_i , K_i , and H_i are UIO matrices. Dynamics of g_i is

$$\begin{aligned}
 g_i(t) &= e^{F_i t} g_i(0) + \int_0^t e^{F_i(t-\tau)} T_i B u(\tau) d\tau \\
 &\quad + \int_0^t e^{F_i(t-\tau)} K_i C_i x(\tau) d\tau + \int_0^t e^{F_i(t-\tau)} K_i \xi_i(\tau) d\tau.
 \end{aligned} \tag{2.106}$$

Then, i -th estimate is

$$\begin{aligned}
z_i(t) = & e^{F_i t} g_i(0) + \int_0^t e^{F_i(t-\tau)} T_i B u(\tau) d\tau \\
& + \int_0^t e^{F_i(t-\tau)} K_i C_i x(\tau) d\tau + \int_0^t e^{F_i(t-\tau)} K_i \xi_i(\tau) d\tau + H_i C_i x(t) + H_i \xi_i(t).
\end{aligned} \tag{2.107}$$

Let the state (\hat{x}) selected by the median operation is z_m . $(z_m - z_i)$ can be written by

$$z_m(t) - z_i(t) = \int_0^t e^{F_m(t-\tau)} K_m \xi_m(\tau) d\tau - \int_0^t e^{F_i(t-\tau)} K_i \xi_i(\tau) d\tau + H_m \xi_m(t) - H_i \xi_i(t). \tag{2.108}$$

Then, $\|(z_m - z_i)\|_2$ is

$$\begin{aligned}
\|(z_m - z_i)\|_2 & \leq \left\| \int_0^t e^{F_m(t-\tau)} K_m \xi_m(\tau) d\tau \right\|_2 + \left\| \int_0^t e^{F_i(t-\tau)} K_i \xi_i(\tau) d\tau \right\|_2 \\
& \quad + \|H_m \xi_m(t)\|_2 + \|H_i \xi_i(t)\|_2, \\
& \leq \|K_m\|_2 \xi_{max} \int_0^t \|e^{F_m(t-\tau)}\|_2 d\tau + \|K_i\|_2 \xi_{max} \int_0^t \|e^{F_i(t-\tau)}\|_2 d\tau \\
& \quad + \|H_m\|_2 \xi_{max} + \|H_i\|_2 \xi_{max}, \\
& = 2\|K_m\|_2 \xi_{max} \int_0^t \|e^{F_m(t-\tau)}\|_2 d\tau + 2\|H_m\|_2 \xi_{max}.
\end{aligned} \tag{2.109}$$

The F_m and the F_i are designed such that F_m and F_i are Hurwitz for all time. Then, there exists constant ν_ξ and λ_ξ satisfying the following inequality:

$$\|e^{(A-L_i C_i)t}\|_2 \leq \nu_\xi e^{-\lambda_\xi t}, \tag{2.110}$$

where $\nu_\xi > 0$ and $\lambda_\xi > 0$.

Then, $\|(z_m - z_i)\|_2$ can be written by

$$\begin{aligned}
\|(z_m - z_i)\|_2 & = 2\|K_m\|_2 \xi_{max} \frac{\nu_\xi}{\lambda_\xi} (1 - e^{-\lambda_\xi t}) + \|H_m\|_2 \xi_{max}, \\
& \leq 2\|K_m\|_2 \xi_{max} \frac{\nu_\xi}{\lambda_\xi} + \|H_m\|_2 \xi_{max},
\end{aligned} \tag{2.111}$$

where $\nu_\xi > 0$ and $\lambda_\xi > 0$.

Thus, the residual value r is set to $(\|K_m\|_2 \xi_{max} \frac{\nu_\xi}{\lambda_\xi} + \|H_m\|_2 \xi_{max})$ in order to detect sensor attack. If 2 norm of the difference ($\|e_i\|_2 = \|\hat{x} - z_i\|_2$) between the output value of each UIO and the output of the median operation are larger than the residual value, The i -th sensor is considered to be attacked. Then, alarm is triggered.

2.3 Defense Approach Against Actuator Attack

In this section, we mainly deal with an actuator attack estimation method using UIO based RSE method. The problem 2.2 that we discussed in section 2.1 was to find a method that would be able to estimate and reject the effect of disturbance and actuator attack. We introduce a actuator attack estimation method using RSE method. The objective of this method is to estimate and reject the bad effect caused by disturbance and actuator attack. This method uses a system input and the estimated state that is obtained by UIO based RSE method. Proposed method provides a level of resiliency to the control system when disturbance and actuator attack are slow varying. The system of (2.1) can be expressed by

$$\dot{x}(t) - Ax(t) - Bu(t) = B(d(t) + a^a(t)). \quad (2.112)$$

The above equation can be written as

$$\hat{d}(t) + \hat{a}^a(t) = B^+(\dot{\hat{x}}(t) - A\hat{x}(t) - Bu(t)). \quad (2.113)$$

The B^+ represents the pseudo inverse of the B . The structure of this method is shown in Figure 2.9. In Figure 2.9, the blue box is expressed as the equation of (2.113). In order to estimate the disturbance and actuator attack correctly, we have to use the system input and actual state. The state needs to be accurate despite of disturbance and actuator attack. In order to obtain the correct state, we use the the estimated state by using UIO based RSE method. The filter $(\frac{s}{\tau s + 1})$ commonly is used as time derivative. The estimate and estimate performance depend on the τ . Mostly, disturbance and actuator attack are estimated and rejected in the low frequency ranges. By using proposed actuator attack estimation method, we can estimate and reject the effect of disturbance and actuator attack in the low frequency ranges.

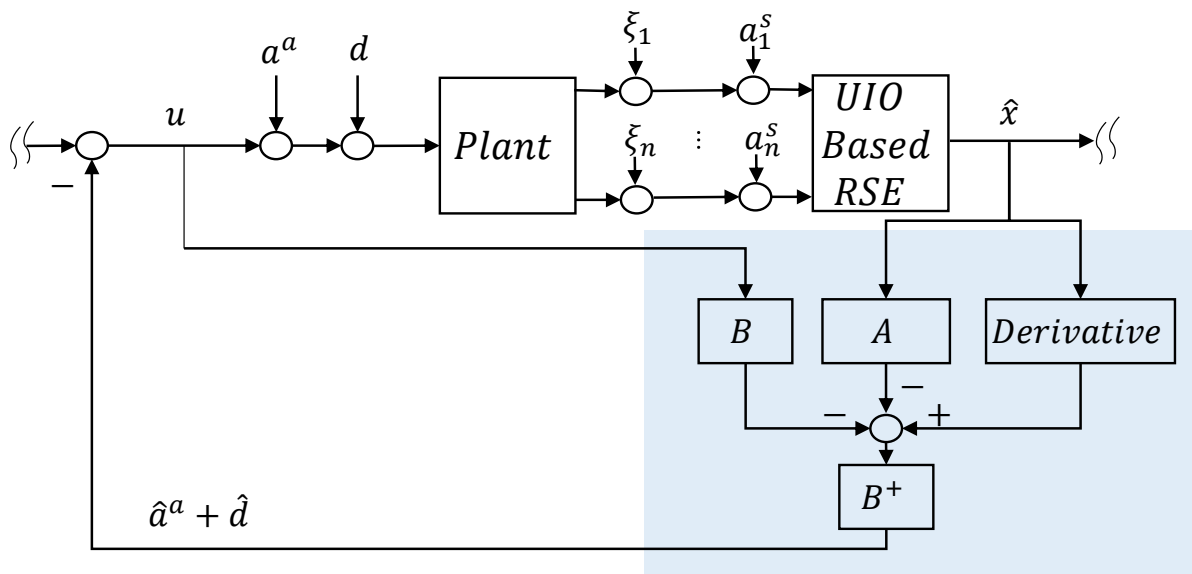


Figure 2.9: Structure of an actuator attack estimation method using UIO based RSE method.

3

Validation with Magnetic Levitation Platform

In order to validate the proposed method, we conducted simulations and experiments on magnetic levitation system. The objective of system is to levitate the position that we want. By adding an virtual sensor on system in Simulink, we made an SIMO (Single Input Multiple Output) system. we considered the case of sensor attack and actuator attack simultaneously.

In this chapter, we firstly describe the modeling of the magnetic levitation system. Then, we explain the design method of existing method and proposed method. Next, we discuss three attack scenarios. Finally, we analyze the results of simulations and experiments.

3.1 Modeling

In order to validate the proposed resilient control method against malicious attack, we used a magnetic levitation system [1] as shown in Figure 4.1. A magnetic levitation system can float the steel ball in its magnetic field. The control purpose is to lift the ball to a certain height. The upper part is coiled by a solenoid coil with a steel core. The post provides initial conditions for control system performance evaluation. MATLAB software tool played the role of the controller. The magnetic levitation system is a nonlinear system described by

$$\begin{aligned}\dot{x}_1 &= x_2, \\ \dot{x}_2 &= g - \frac{K_m I^2}{M_b(x_1)^2}, \\ y &= x_1,\end{aligned}\tag{3.1}$$

where x_1 is the ball position measured by infrared sensor, x_2 is the ball velocity, g is the gravitational constant, I is input signal that is coil current of system of (3.1), K_m is the electromagnet force constant, and M_b is the mass of the metal ball. The parameters of g, K_m , and M_b is specified in [1].



Figure 3.1: Magnetic Levitation System.

we are able to linearize the equation of (3.1) at operating point. To get the equilibrium point, solve equations

$$\begin{aligned} 0 &= x_2, \\ 0 &= g - \frac{K_m I^2}{M_b (x_1)^2}. \end{aligned} \quad (3.2)$$

The equilibrium point of coil current I where equilibrium point of ball position $x_{10} = 6mm$ is written by

$$\begin{aligned} I_0 &= x_{10} \sqrt{\frac{2gM_b}{K_m}} \\ &\approx 1. \end{aligned} \quad (3.3)$$

Denote the deviations of the input and state from the equilibrium point by

$$\begin{aligned} \tilde{I}(t) &= I(t) - I_0 = I(t) - 1, \\ \tilde{x}(t) &= x(t) - x_0 = \begin{bmatrix} x_1(t) - 0.006 \\ x_2(t) \end{bmatrix}. \end{aligned} \quad (3.4)$$

Now, the linearized model of the deviation variables is

$$\begin{aligned} \dot{\tilde{x}}(t) &= A\tilde{x}(t) + B\tilde{I}(t), \\ &= \begin{bmatrix} 0 & 1 \\ \frac{K_m I_0^2}{M_b x_{10}^3} & 0 \end{bmatrix} \tilde{x}(t) + \begin{bmatrix} 0 \\ -\frac{K_m I_0}{M_b x_{10}^2} \end{bmatrix} \tilde{I}(t). \end{aligned} \quad (3.5)$$

By putting in the parameters, then we can obtain the following equation as

$$\dot{\tilde{x}}(t) = \begin{bmatrix} 0 & 1 \\ 3270 & 0 \end{bmatrix} \tilde{x}(t) + \begin{bmatrix} 0 \\ -26.67 \end{bmatrix} \tilde{I}(t). \quad (3.6)$$

The sensor of Magnetic levitation system only measures the position of the steel ball. In order to implement the proposed resilient control method, we virtually made the additional

position sensor and the velocity sensor in MATLAB Simulink. The Magnetic levitation output equation can be written as

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix}, \quad (3.7)$$

where $C_1 = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $C_2 = \begin{bmatrix} 1 & 1 \end{bmatrix}$, and $C_3 = \begin{bmatrix} 0 & 1 \end{bmatrix}$. we injected the actuator attack and sensor attack by using MATLAB Simulink. The equation considering actuator attack and sensor attack can be written by

$$\begin{aligned} \dot{\tilde{x}}(t) &= \begin{bmatrix} 0 & 1 \\ 3270 & 0 \end{bmatrix} \tilde{x}(t) + \begin{bmatrix} 0 \\ -26.67 \end{bmatrix} (\tilde{I}(t) + d(t) + a^a(t)), \\ \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} &= \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \tilde{x}(t) + \begin{bmatrix} a_1^s(t) \\ a_2^s(t) \\ a_3^s(t) \end{bmatrix}, \end{aligned} \quad (3.8)$$

where d is a disturbance, a^a is the actuator attack, and a^s is the sensor attack.

3.2 Design of Resilient Control System Design

3.2.1 Existing Resilient State Estimation Method Using Median Operation

Luenberger observer is used in existing RSE method. i -th Luenberger observer is given by

$$\begin{aligned} \dot{z}^i(t) &= Az^i(t) + B\tilde{I}(t) + L_i(y_i(t) - \hat{y}^i(t)), \\ \hat{y}^i(t) &= C_i z^i(t). \end{aligned} \quad (3.9)$$

where z^i is i -th estimated state, y_i is i -th system output, \hat{y}_i is i -th estimated system output, and L_i is i -th observer gain. Each L_i is obtained such that $(A - L_i C_i)$ is Hurwitz. The observer gains are $L_1 = \begin{bmatrix} 1.0564 & 370.4436 \end{bmatrix}^T$, $L_2 = \begin{bmatrix} 1.0564 & 370.4436 \end{bmatrix}^T$, and $L_3 = \begin{bmatrix} 1.1697 & 371.5 \end{bmatrix}^T$.

Then, perform median operation using each Luenberger observer output value, $\hat{\hat{x}}$ is computed by

$$\begin{aligned}\hat{\hat{x}}_1 &= \text{med}(z_1^1, z_1^2, z_1^3), \\ \hat{\hat{x}}_2 &= \text{med}(z_2^1, z_2^2, z_2^3).\end{aligned}\tag{3.10}$$

So far, this is a method of designing the existing RSE method.

3.2.2 Proposed Resilient Control System Design

Firstly, we deal with design of UIO based RSE method. Then, we will discuss the design of a method that would be able to estimate and reject the effect of disturbance and actuator attack. So as to design UIO based RSE method, we consider the UIO. In order to design the UIO firstly, we have to check the condition for using UIO. Since $\text{rank}(C_1B) = \text{rank}(B)$, $\text{rank}(C_2B) = \text{rank}(B)$, and $\text{rank}(C_3B) = \text{rank}(B)$, the first condition is satisfied. Each UIO dynamics is given by

$$\begin{aligned}\dot{g}_i(t) &= F_i g_i(t) + T_i B u(t) + K_i y_i(t), \\ z^i(t) &= g_i(t) + H_i y_i(t),\end{aligned}\tag{3.11}$$

where $i = 1, 2, 3$ is the index for the i -th sensor, g_i is the i -th observer state, u is the system input, y_i is the i -th system output, z_i is the estimate of the system state. The matrices F_i, T_i, K_i and H_i are UIO parameters. The UIO matrices are obtained next:

$$\begin{aligned}H_i &= B((C_i B)^T (C_i B))^{-1} (C_i B)^T, \\ H_1 &= \begin{bmatrix} 0 \\ 1 \end{bmatrix}, H_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, H_3 = \begin{bmatrix} 0 \\ 1 \end{bmatrix},\end{aligned}\tag{3.12}$$

$$\begin{aligned}T_i &= I - H_i C_i, \\ T_1 &= \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}, T_2 = \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}, T_3 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},\end{aligned}\tag{3.13}$$

$$A - H_i C_i A = T_i A, \\ A - H_1 C_1 A = \begin{bmatrix} 0 & 1 \\ 0 & -1 \end{bmatrix}, A - H_2 C_2 A = \begin{bmatrix} 0 & 1 \\ 0 & -1 \end{bmatrix}, A - H_3 C_3 A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}. \quad (3.14)$$

Next, we need to consider the second UIO design condition. Thus, the observability of the pair of the pair $(A - H_i C_i A, C_i)$ must be checked. If the observability of this pair $(A - H_i C_i A, C_i)$ is full rank, then we can apply pole placement so that error dynamics is Hurwitz. Each observability matrices is

$$W_0^i := \begin{bmatrix} C_i \\ C_i(A - H_i C_i A) \\ \vdots \\ C_i(A - H_i C_i A)^{n-1} \end{bmatrix}, \quad (3.15)$$

$$\text{rank}(W_0^1) = 1, \text{rank}(W_0^2) = 1, \text{rank}(W_0^3) = 1.$$

Since each rank of the observability matrices is not full rank, we should find a transformation matrix P_i by using the observable canonical decomposition.

$$P_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, P_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, P_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (3.16)$$

Apply an observable canonical decomposition on each pair $(A - H_i C_i A, C_i)$.

$$P_1(A - H_1 C_1 A)P_1^{-1} = \begin{bmatrix} A_{11}^1 & 0 \\ A_{21}^1 & A_{22}^1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & -1 \end{bmatrix}, \quad (3.17)$$

$$P_2(A - H_2 C_2 A)P_2^{-1} = \begin{bmatrix} A_{11}^2 & 0 \\ A_{21}^2 & A_{22}^2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & -1 \end{bmatrix}, \quad (3.18)$$

$$P_3(A - H_3 C_3 A)P_3^{-1} = \begin{bmatrix} A_{11}^3 & 0 \\ A_{21}^3 & A_{22}^3 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & -1 \end{bmatrix}, \quad (3.19)$$

$$C_1 P_1^{-1} = \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad (3.20)$$

$$C_2 P_2^{-1} = \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad (3.21)$$

$$C_3 P_3^{-1} = \begin{bmatrix} 1 & -1 \end{bmatrix}. \quad (3.22)$$

Then, we need to check the detectability of the pair $(A - H_i C_i A, C_i)$. Since each A_{22} is stable, each pair is detectable. Now, we can obtain K_i^1 using pole placement in order to place the observer pole at $[-1001]$. Next, the K_i^2 can be any matrix. Compute K_i .

$$\begin{aligned} \widetilde{K}_i &= P_i^{-1} \begin{bmatrix} (K_i^1)^T & (K_i^2)^T \end{bmatrix}^T \\ \widetilde{K}_1 &= \begin{bmatrix} 1001 \\ 0 \end{bmatrix}, \widetilde{K}_2 = \begin{bmatrix} 1001 \\ 0 \end{bmatrix}, \widetilde{K}_3 = \begin{bmatrix} 0 \\ 1001 \end{bmatrix}. \end{aligned} \quad (3.23)$$

The UIO matrices F_i and K_i can be obtained:

$$\begin{aligned} F_i &= A - H_i C_i A - \widetilde{K}_i C_i, \\ F_1 &= \begin{bmatrix} -1001 & -1000 \\ 0 & -1 \end{bmatrix}, F_2 = \begin{bmatrix} -1001 & -1000 \\ 0 & -1 \end{bmatrix}, F_3 = \begin{bmatrix} 0 & 1 \\ 0 & -1002 \end{bmatrix}, \end{aligned} \quad (3.24)$$

$$\begin{aligned} K_i &= \widetilde{K}_i + F_i H_i, \\ K_1 &= \begin{bmatrix} 1 \\ -1 \end{bmatrix}, K_2 = \begin{bmatrix} 1 \\ -1 \end{bmatrix}, K_3 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}. \end{aligned} \quad (3.25)$$

Then, perform median operation using each UIO output value, $\widehat{\widehat{x}}$ is computed by

$$\begin{aligned} \widehat{\widehat{x}}_1 &= med(z_1^1, z_1^2, z_1^3), \\ \widehat{\widehat{x}}_2 &= med(z_2^1, z_2^2, z_2^3). \end{aligned} \quad (3.26)$$

So far, this is a method of designing the UIO based RSE method.

Now, we deal with the actuator attack estimation method that would be able to estimate and reject the effect of disturbance and actuator attack. In order to protect the system from actuator attack, we will design the actuator attack estimation method using UIO based RSE method. The system of (3.8) can be expressed as follows.

$$\dot{\tilde{x}}(t) - A\tilde{x}(t) - Bu(t) = B(d(t) + a^a(t)). \quad (3.27)$$

The above equation can be written as

$$\hat{d}(t) + \hat{a}^a(t) = B^+(\dot{\hat{x}}(t) - A\hat{x}(t) - Bu(t)), \quad (3.28)$$

where B^+ is the pseudo inverse of the B , and \hat{x} is the estimate of state using UIO based RSE method. we use a filter $(\frac{s}{\tau+s})$ for a time derivative. We set the τ to 40 in simulation and experiment. By using correct estimate of state, system input, A , B , and B^+ , we are able to estimate and reject the effect of disturbance and actuator attack.

3.3 Scenarios

We consider three scenarios. Simulation and experiment are based on three scenarios. In each scenarios, we consider same attack scenarios where third output and plant input are compromised by adversaries simultaneously. A sensor attack and actuator attack is shown in Figure 3.2. We consider sensor attack as square wave and third output is attacked at 10 seconds. We consider actuator attack as step waveform that is filtered by low-pass filter. Actuator attack is injected on system input at 12 seconds. Reference is $0.006m$. In section 3.3.1-3.3.3, we explain three scenarios in detail.

3.3.1 Scenario 1

In order to show a limitation of existing RSE method under sensor attack and actuator attack simultaneously, we made scenario 1. In this scenario 1, We used existing Luenberger observer based RSE method using Median operation [7]. In these conditions, two primary limitations occur. The first is state estimation performance and the second is effect of actuator attack. In scenario 1, we are able to check two limitations.

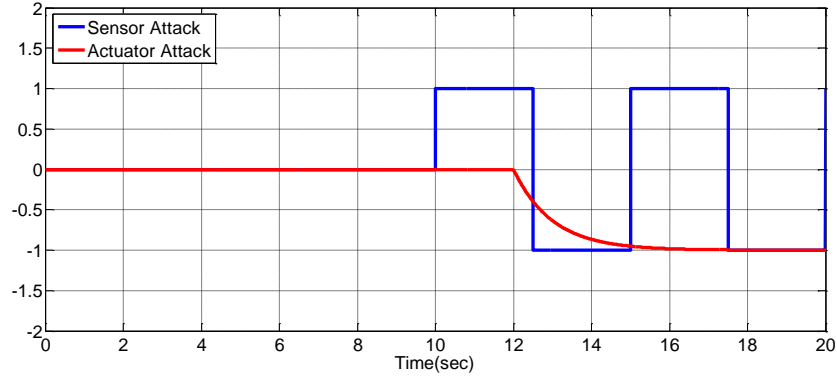


Figure 3.2: Sensor attack and actuator attack.

3.3.2 Scenario 2

In order to validate solution to problem 1 (problem 1 was to find a method of RSE whose state estimation error converges to zero despite of actuator attack), we made scenario 2. In this scenario 2, we only used proposed UIO based RSE method. Since there still exists effect of actuator attack, control performance deteriorates. In scenario 2, we are able to check superior estimation performance and effect of actuator attack.

3.3.3 Scenario 3

So as to validate solution to problem 2 (problem 2 was to find a method that would be able to estimate and reject the effect of actuator attack), we made scenario 3. In this scenario 3, we used UIO based method as well as proposed UIO based RSE method. In scenario 3, we are able to check that proposed method would be able to estimate of effect of actuator attack.

3.4 Simulation Results

3.4.1 Simulation Results of Scenario 1

As we mentioned before in section 3.3.1, we used existing RSE method using median operation. Sensor attack is injecting on third sensor at 10 seconds and actuator attack is injecting on system input at 12 seconds.

Existing Luenberger observer based RSE method exploits three observer outputs. Then, estimated states are obtained by using median operation. We illustrate three observer output in Figure 3.3. First state is shown in (a) of Figure 3.3. Second state is shown in (b) of Figure 3.3. Blue dots, green dashed line, and red line are first, second, and third observer output respectively. We see that third observer output is affected by sensor attack.

By using median operation, existing RSE method is able to estimate state. Estimated state by median operation is shown in Figure 3.4. Also, state estimation error of existing RSE method is illustrated in Figure 3.5. In Figure 3.4, red dashed line is estimated state and gray line is actual state. We see that existing RSE method is able to protect system from sensor attack. When only sensor attack is considered from 10 seconds to 12 seconds, we can confirm that RSE method estimates the correct value even in the presence of a sensor attack.

Now, we discuss limitations of existing method. First limitation is estimation performance. After injecting actuator attack, we see that estimation error occur. We are able to check that state estimation performance of existing method deteriorates by actuator attack from 12 seconds to 20seconds in Figure 3.4 and 3.5. Second limitation is the effect of actuator attack. we see that control performance is weakened by actuator attack in Figure 3.4.

Lastly, we deal with a interesting phenomenon. In Figure 3.4, first real state seems to move differently from reference. But, second real state seems to return to reference. Second real state seems to have no impact on actuator attack. This phenomenon is caused by system characteristics. That is, This phenomenon may occur differently in accordance with each system and observer. Now, let we explain the reason. Error of i -th Luenberger observer is $\tilde{z}^i := x^i - \hat{x}^i$. Error dynamics of i -th Luenberger observer is given by

$$\dot{\tilde{z}}^i(t) = (A - L_i C_i) \tilde{z}^i(t) + B a^a(t). \quad (3.29)$$

A solution of equation of (3.27) is

$$\tilde{z}^i(t) = e^{(A-L_i C_i)(t-t_0)} \tilde{z}^i(0) + \int_{t_0}^t (e^{(A-L_i C_i)(t-\tau)} B a^a(\tau)) d\tau. \quad (3.30)$$

We assume that $a^a(t)$ is constant and t_0 is zero. Then,

$$\tilde{z}^i(t) = e^{(A-L_iC_i)(t)}\tilde{z}^i(0) + \int_0^t (e^{(A-L_iC_i)(t-\tau)}Ba^a)d\tau. \quad (3.31)$$

In this scenario, we consider that third output is attacked by actuator attack. Thus, the output of first output of observer or second output of observer is chosen by median operation. First $(A - L_1C_1)$ and second $(A - L_2C_2)$ are

$$A - L_1C_1 = A - L_2C_2 = \begin{bmatrix} -1.1 & -0.1 \\ 2899.6 & -370.4 \end{bmatrix}. \quad (3.32)$$

Since $(A - L_1C_1)$ and $(A - L_2C_2)$ are nonsingular, 1-st and 2-nd error solution of equation (3.29) is

$$\tilde{z}^1(t) = e^{(A-L_1C_1)(t)}\tilde{z}^1(0) + (A - L_1C_1)^{-1}(e^{(A-L_1C_1)t} - I)Ba^a, \quad (3.33)$$

$$\tilde{z}^2(t) = e^{(A-L_2C_2)(t)}\tilde{z}^2(0) + (A - L_2C_2)^{-1}(e^{(A-L_2C_2)t} - I)Ba^a. \quad (3.34)$$

We assume that t is converge to infinity in order to facilitate interpretation. Then,

$$\tilde{z}^1(t) = (A - L_1C_1)^{-1}(-I)Ba^a, \quad (3.35)$$

$$\tilde{z}^2(t) = (A - L_2C_2)^{-1}(-I)Ba^a. \quad (3.36)$$

The $(A - L_1C_1)^{-1}$ and the $(A - L_2C_2)^{-1}$ are given by

$$(A - L_1C_1)^{-1} = (A - L_2C_2)^{-1} = \begin{bmatrix} -0.6675 & 0.0001 \\ -5.2244 & -0.0019 \end{bmatrix}. \quad (3.37)$$

Then, equation (3.31) and (3.32) is as follows:

$$\begin{aligned}
\tilde{z}^1(t) &= \begin{bmatrix} 0.6675 & -0.0001 \\ 5.2244 & 0.0019 \end{bmatrix} \begin{bmatrix} 0 \\ -26.67 \end{bmatrix} a^a, \\
&= \begin{bmatrix} 0.0018 \\ 0.0340 \end{bmatrix} a^a, \\
\tilde{z}^2(t) &= \begin{bmatrix} 0.0018 \\ 0.0340 \end{bmatrix} a^a,
\end{aligned} \tag{3.38}$$

where $\tilde{z}^1(t) = \begin{bmatrix} x_1 - \hat{x}_1^1 \\ x_2 - \hat{x}_2^1 \end{bmatrix}$ and $\tilde{z}^2(t) = \begin{bmatrix} x_1 - \hat{x}_1^2 \\ x_2 - \hat{x}_2^2 \end{bmatrix}$.

In this simulation, we consider a_a is negative value. Thus, we are able to explain why this phenomenon happens. If i -th $(A - L_i C_i)$ is nonsingular, state estimation performance depend on $(A - L_i C_i)^{-1} B$. That is, This phenomenon may occur differently in accordance with each system and observer.

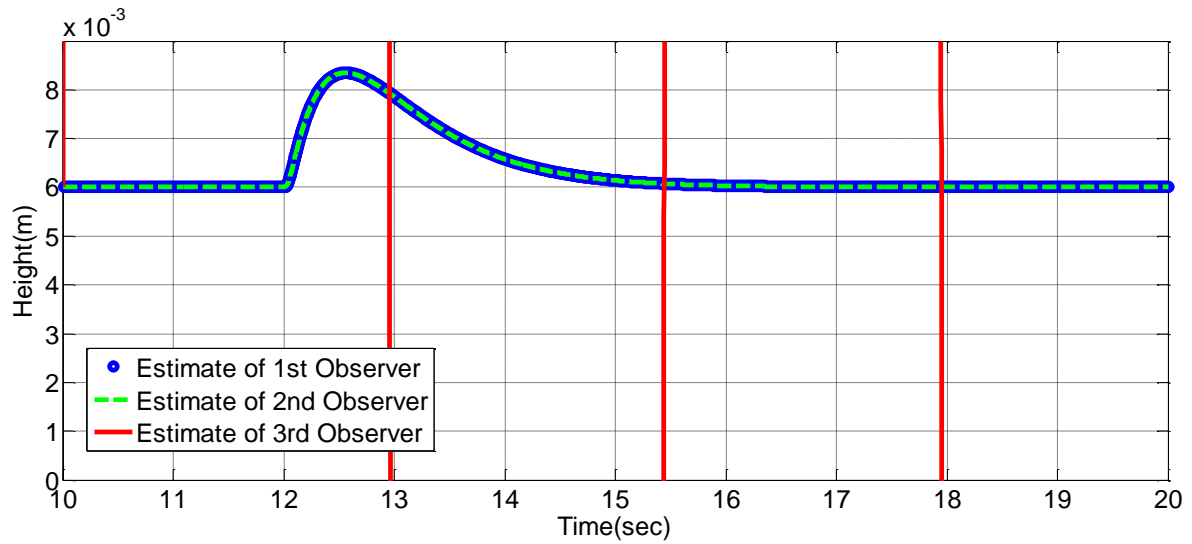
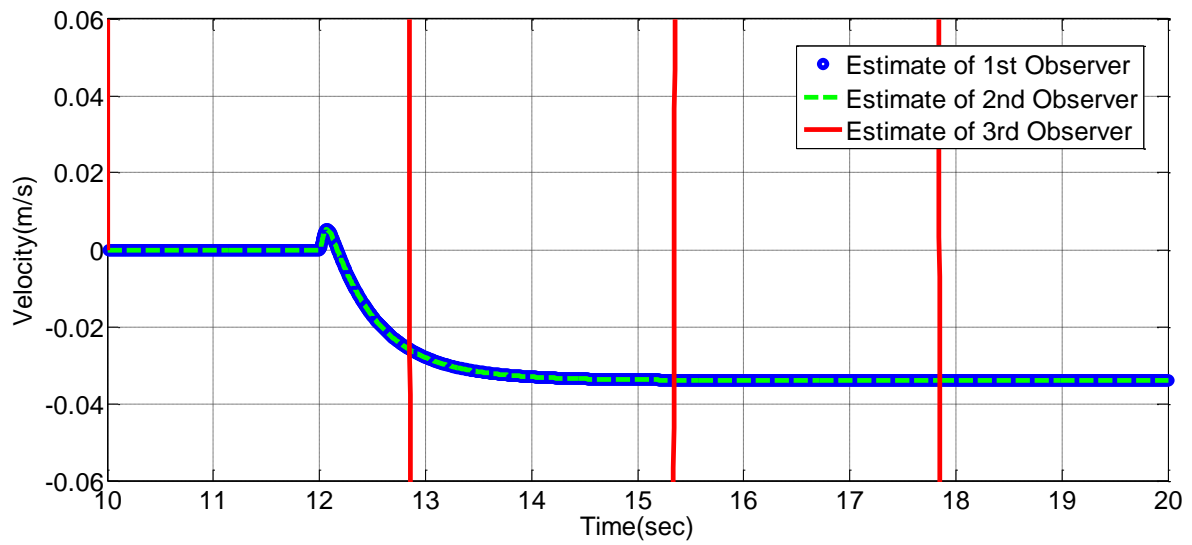
(a) Estimate of first state (x_1)(b) Estimate of second state (x_2)

Figure 3.3: Estimate of Luenberger observer when using existing RSE method.

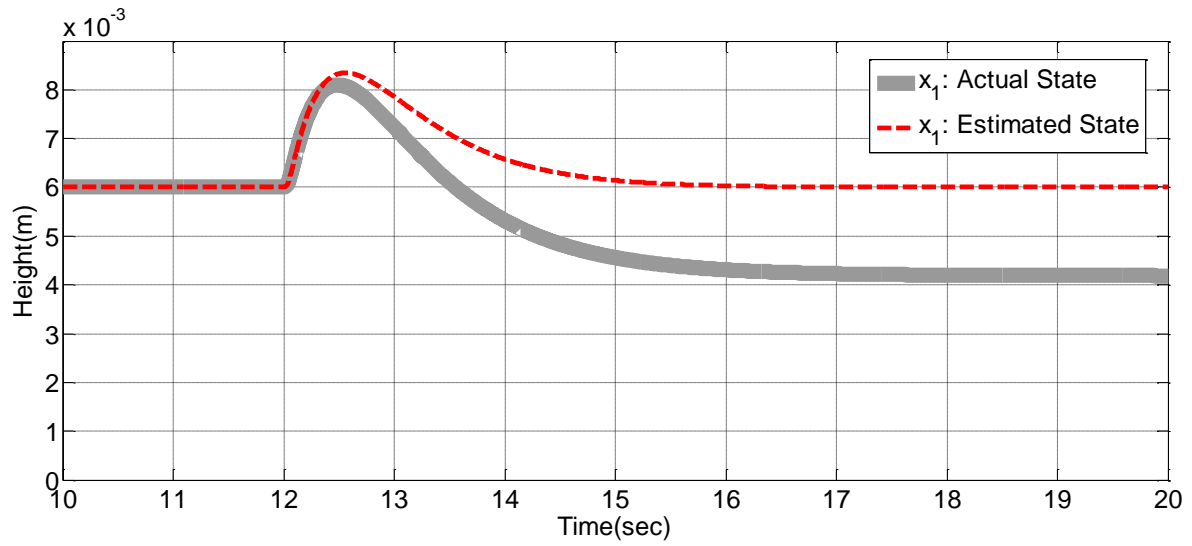
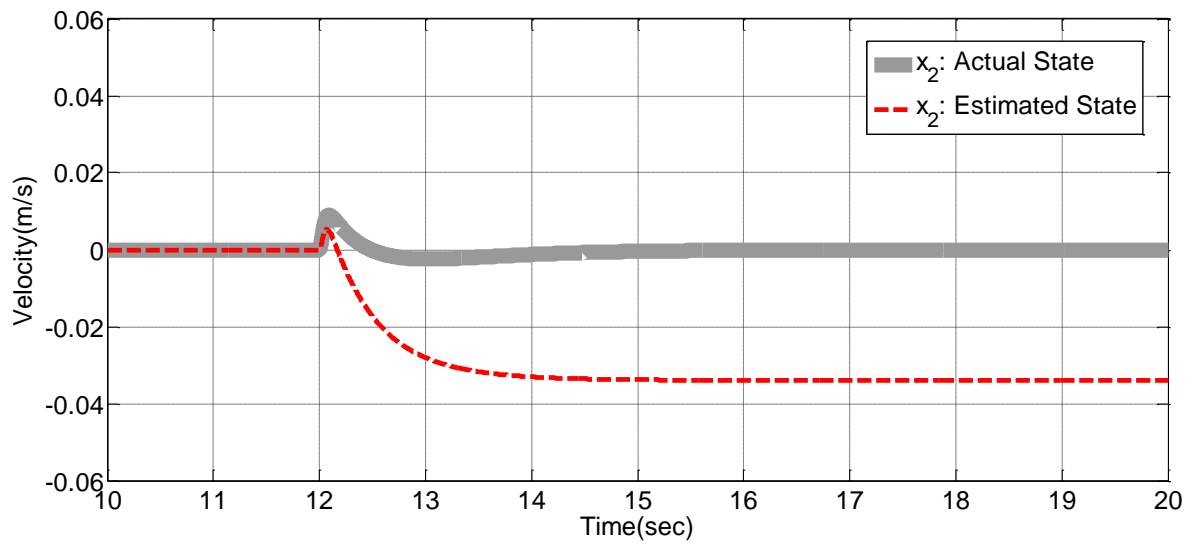
(a) First state (x_1)(b) Second state (x_2)

Figure 3.4: Actual state and estimate when using existing based RSE method.

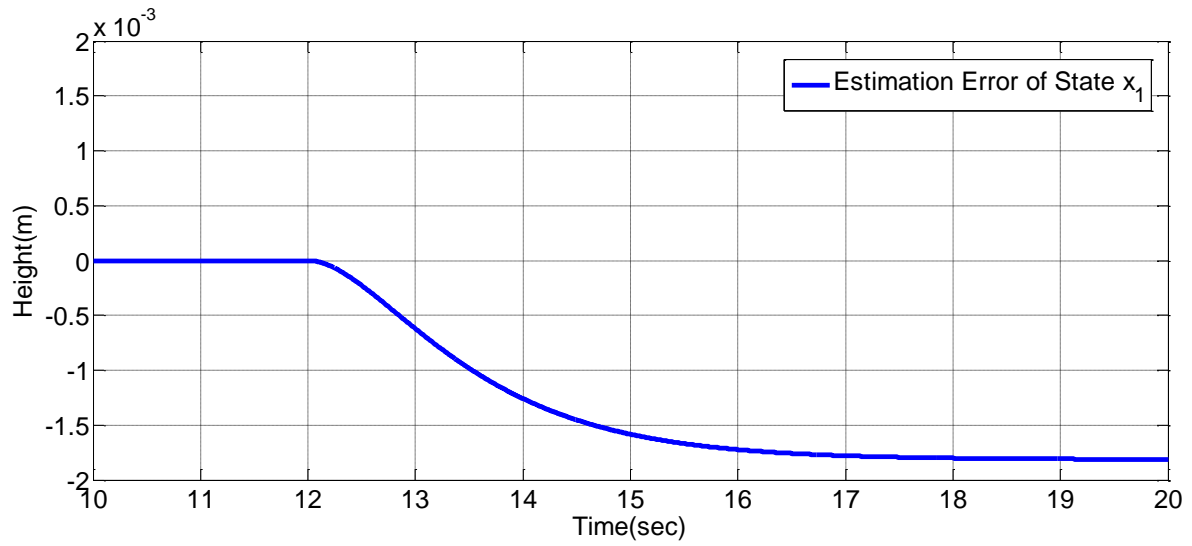
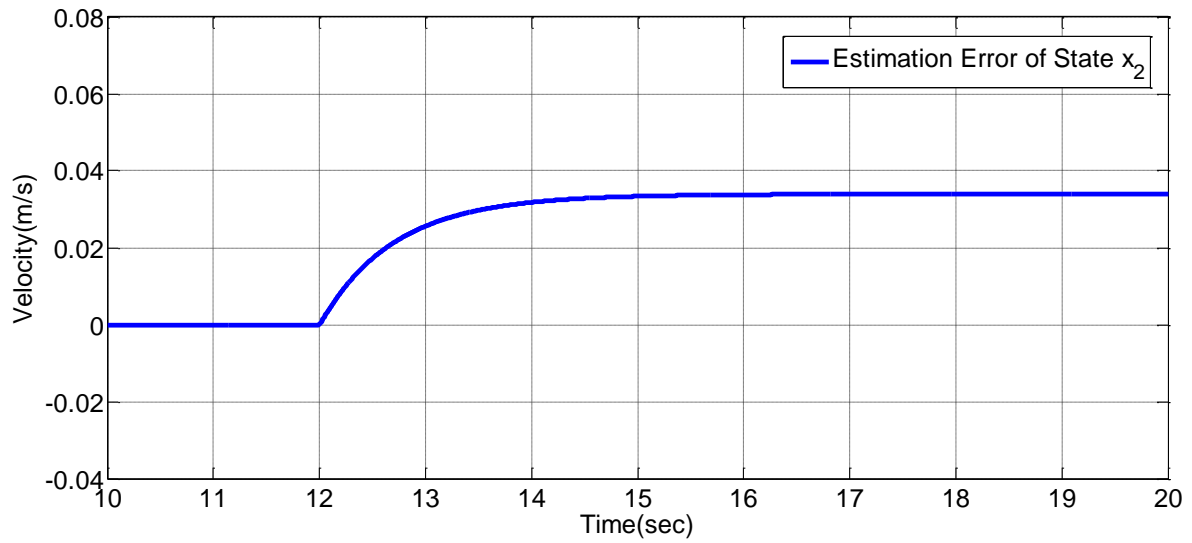
(a) State estimation error of first state (x_1)(b) State estimation error of second state (x_2)

Figure 3.5: State estimation error when using existing RSE method.

3.4.2 Simulation Results of Scenario 2

Scenario 2 was created to validate the solution to problem 1. In other words, in this section, we will check the state estimation performance. The solution to first problem was to use UIO based RSE method in order to guarantee estimation performance under actuator attack. Thus, we used UIO based RSE method in scenario 2. As we mentioned before, we were injecting sensor attack to the third output at 10 seconds and actuator attack at 12 seconds as shown in Figure 3.2.

In figure 3.6-3.8, (a) is first state (x_1) and (b) is second state (x_2). We illustrate three UIO output in Figure 3.6. blue dot, green dashed line, and led line are first, second, and third output of UIO. we see that third output is attacked. By using median operation, RSE method can accurately estimate system state despite of sensor attack. The state estimate after the median operation is shown in Figure 3.7. Gray line is actual state and red dashed line are estimate. Also, state estimation error is shown in Figure 3.8. We see that state estimation error of UIO based RSE method is smaller than one of existing method. We are able to check that estimation performance of UIO based RSE method is superior to existing method. Thus, UIO based RSE method is the method whose output \hat{x} satisfies $\hat{x}(t) \rightarrow x(t)$ as time goes infinity despite of actuator attack.

But, there still exists the effect of actuator attack. In figure 3.7, we can see that state is rapidly rising in 12 seconds and then descending. This phenomenon is caused by actuator attack. Thus, we see that actuator attack deteriorates the control performance. In scenario 3, we will validate a method that would be able to estimate and reject the effect of actuator attack.

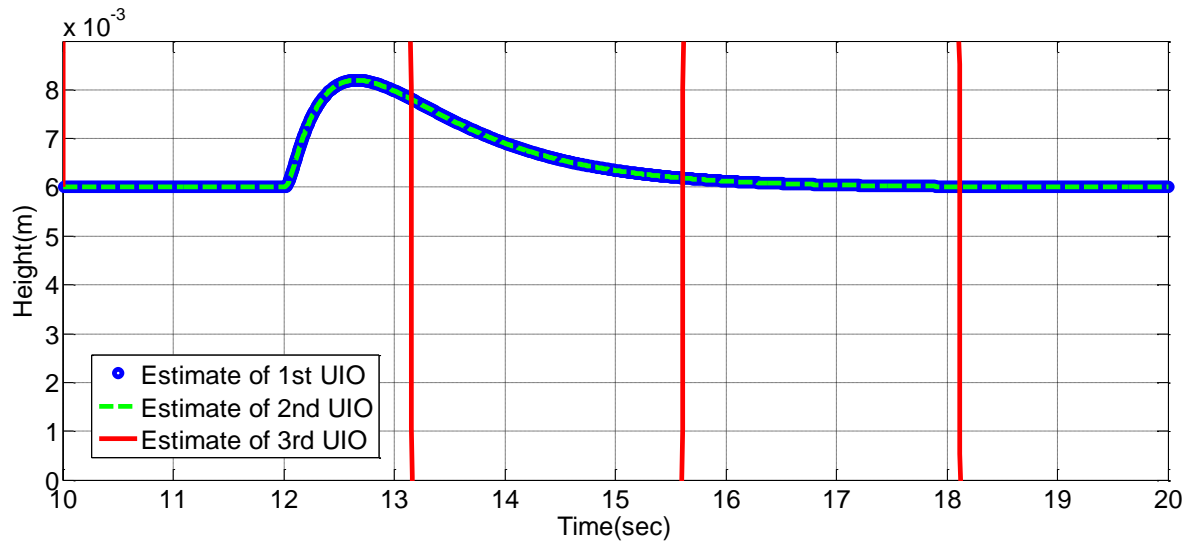
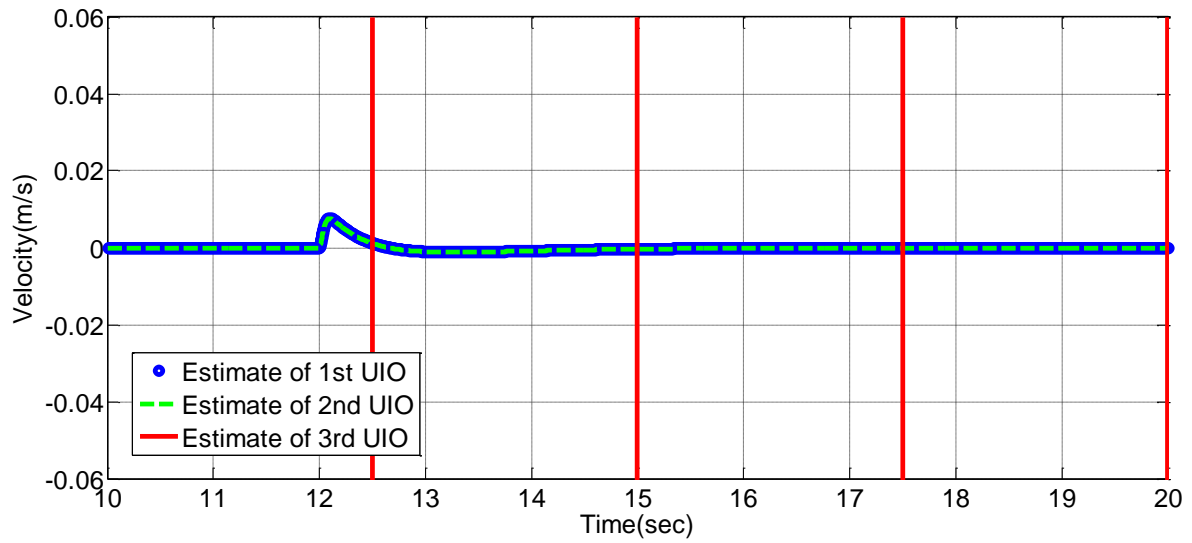
(a) Estimate of first state (x_1)(b) Estimate of second state (x_2)

Figure 3.6: Estimate of UIO when using UIO based RSE method.

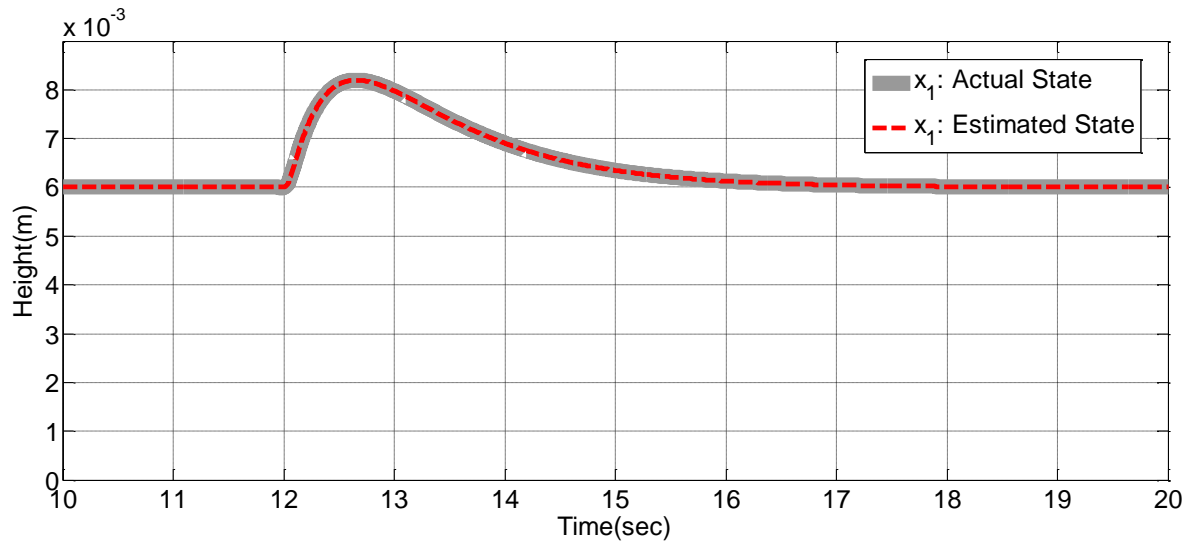
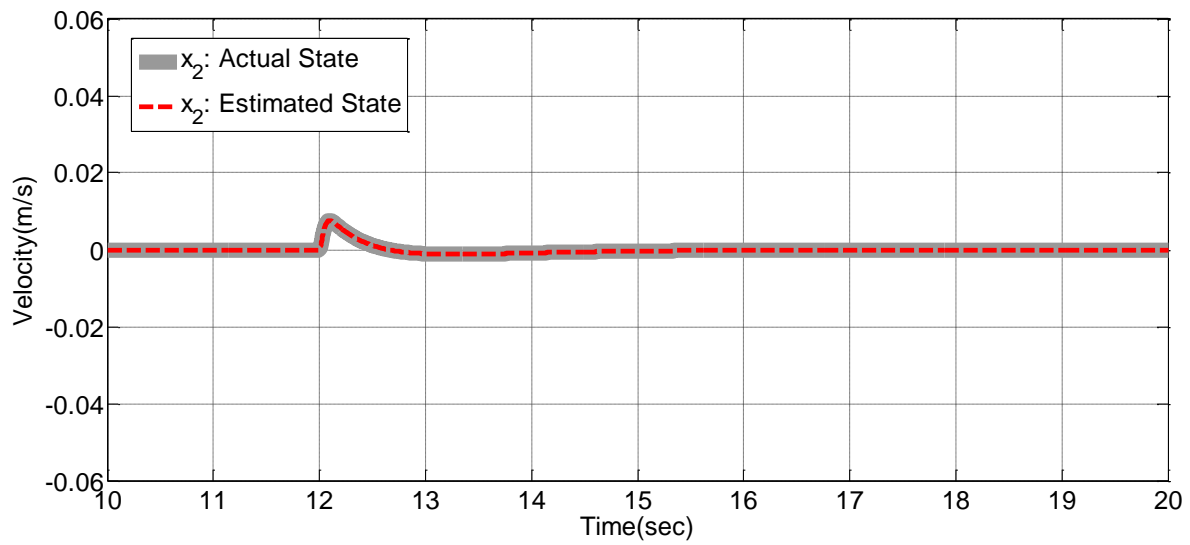
(a) First state (x_1)(b) Second state (x_2)

Figure 3.7: Actual state and estimate when using UIO based RSE method.

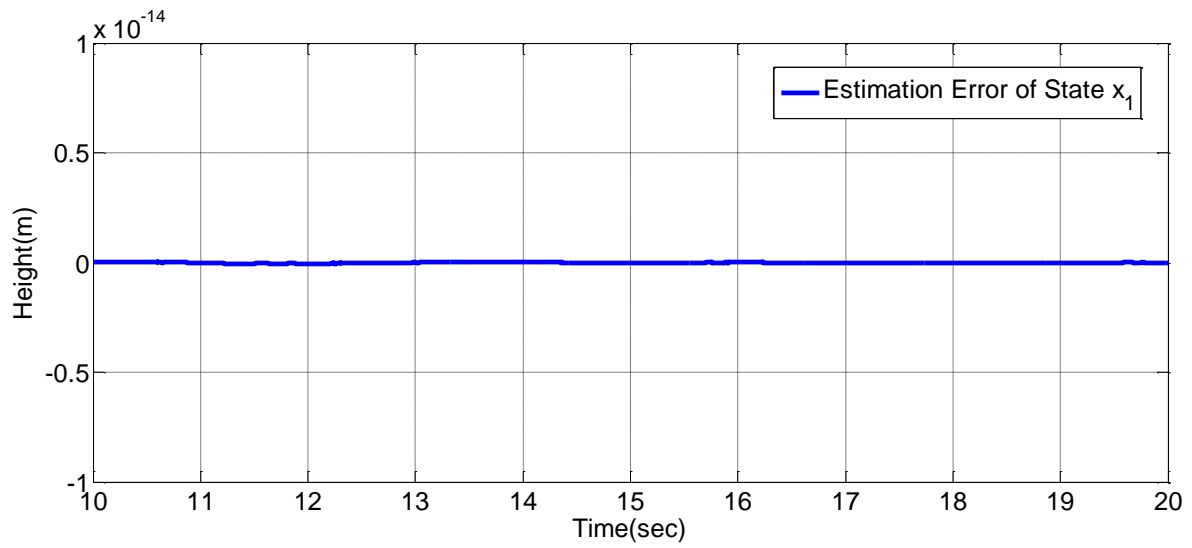
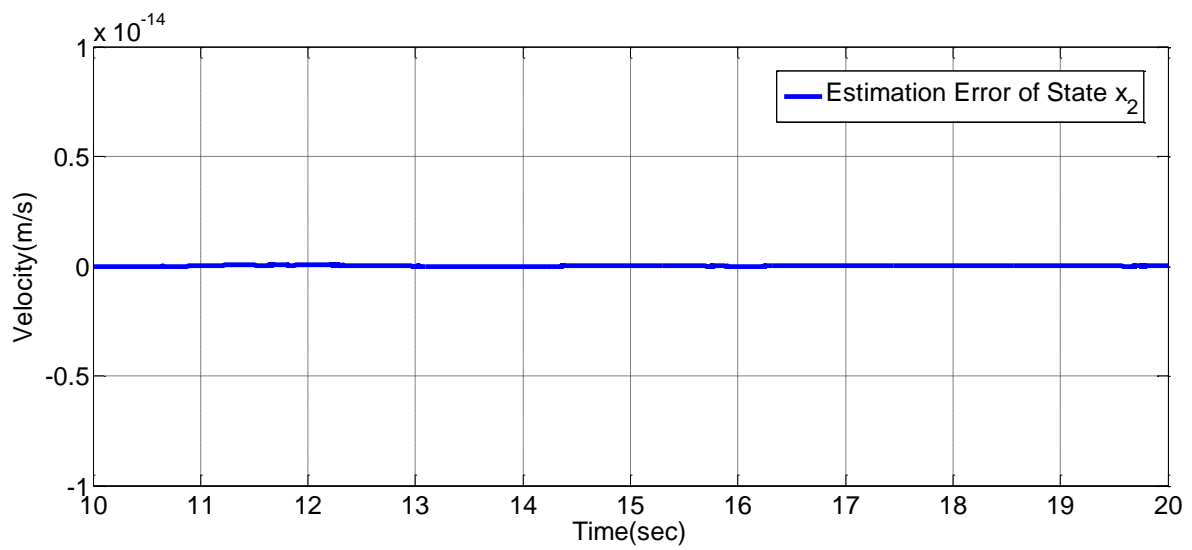
(a) State estimation error of first state (x_1)(b) State estimation error of second state (x_2)

Figure 3.8: State estimation error when using UIO based RSE method.

3.4.3 Simulation Results of Scenario 3

Scenario 3 was created to validate the solution to problem 2. In other words, in this section, we will check whether proposed method can estimate and reject the effect of actuator attack well. The solution to second problem was to use the actuator attack estimation method exploiting UIO based RSE method. Thus, in this scenario 3, we used actuator attack estimation method as well as UIO based RSE method together. As we mentioned before, we were injecting sensor attack to third output at 10 seconds and actuator attack at 12 seconds as shown in Figure 3.2.

In figure 3.9-3.11, (a) is first state (x_1) and (b) is second state (x_2). We illustrate three UIO output in Figure 3.10. blue dot, green dashed line, and led line are first, second, and third output of UIO. We see that third output is compromised by adversary. By using median operation, RSE method can accurately estimate system state despite of sensor attack. The state estimate after the median operation is shown in Figure 3.10. Gray line is actual state and red dashed line is estimate. Also, state estimation error is shown in Figure 3.11. In scenario 2 and 3, the state estimate performance is the same each other. In scenario 2, we checked that state is rapidly rising in 12 seconds and then descending. In this scenario 3, we can check that the effect of actuator attack is greatly reduced. In Figure 3.12, we illustrate actual actuator attack and estimate. Gray line is real actuator attack and led dashed line is estimate. Figure 3.13 is error of two values (actuator attack-estimate). Thus, we can check that the proposed method (solution to problem 2) would be able to estimate and reject the effect of actuator attack well.

Therefore, by using UIO based RSE method and actuator attack estimation method using UIO based, the system is able to improve the resiliency under restrictive sensor attacks and actuator attack that is composed of low frequency.

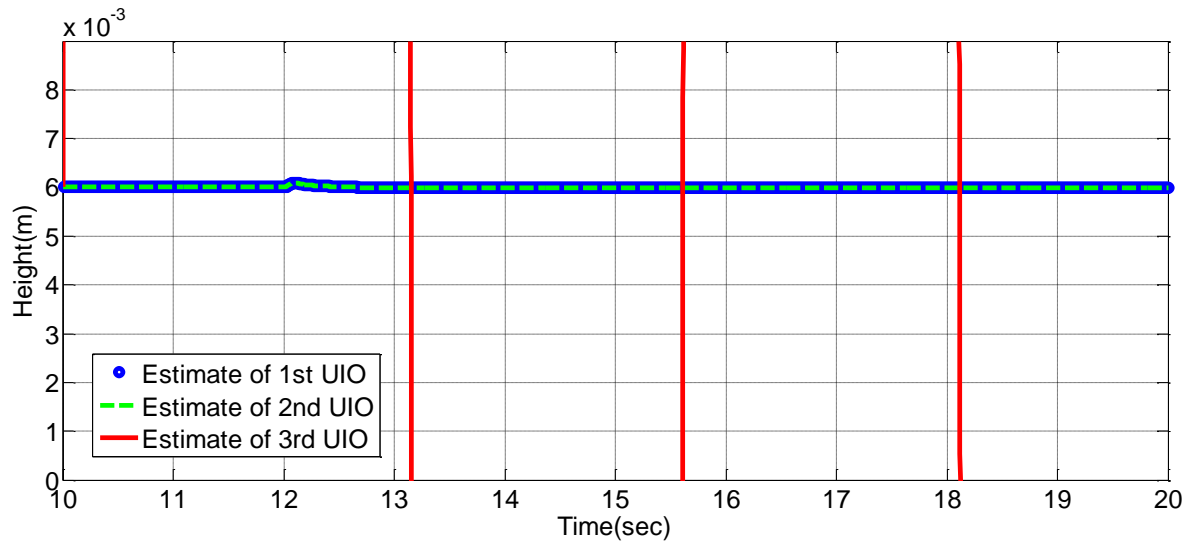
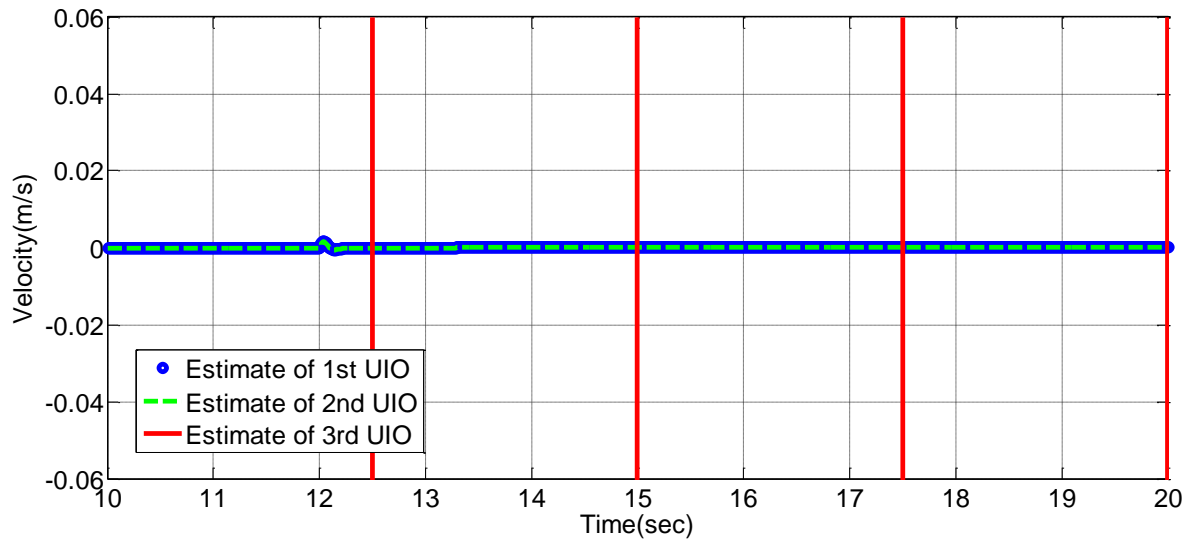
(a) Estimate of first state (x_1)(b) Estimate of second state (x_2)

Figure 3.9: Estimate of UIO when using UIO based RSE method and actuator attack estimator.

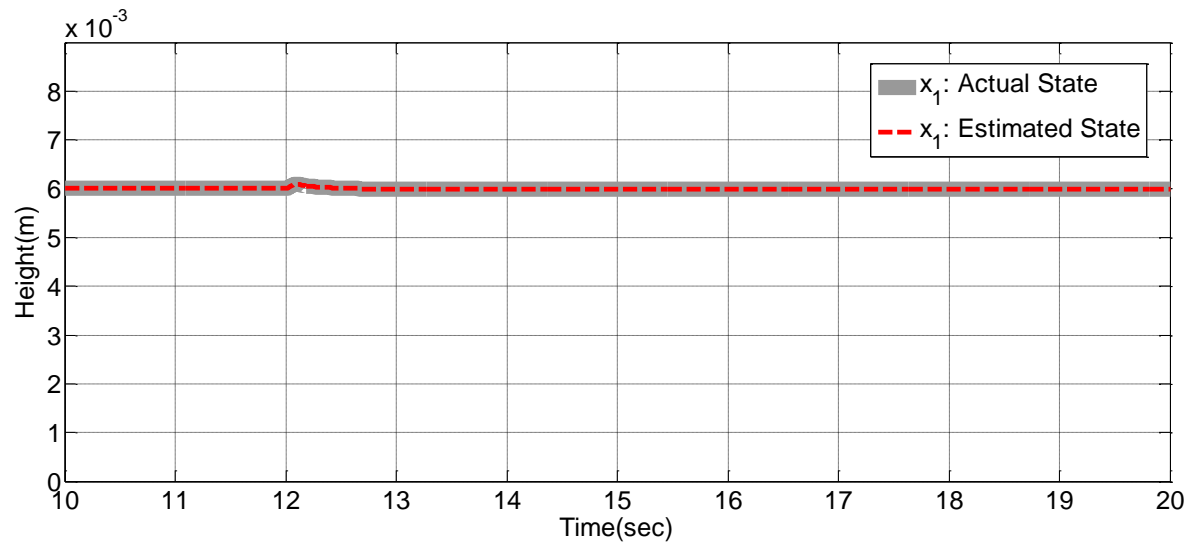
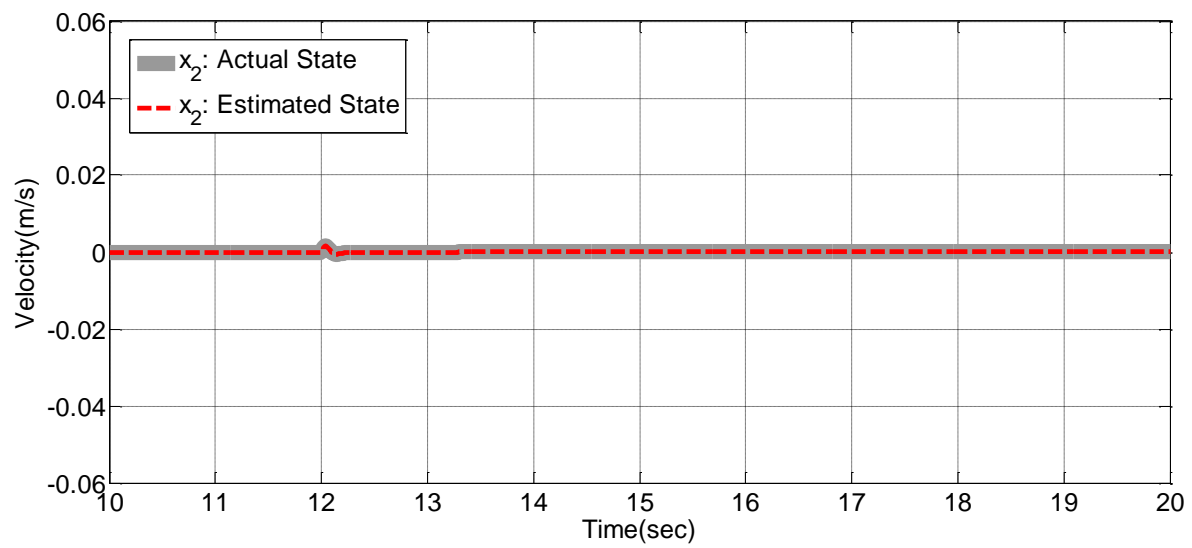
(a) First state (x_1)(b) Second state (x_2)

Figure 3.10: Actual state and estimate when using UIO based RSE method and actuator attack estimator.

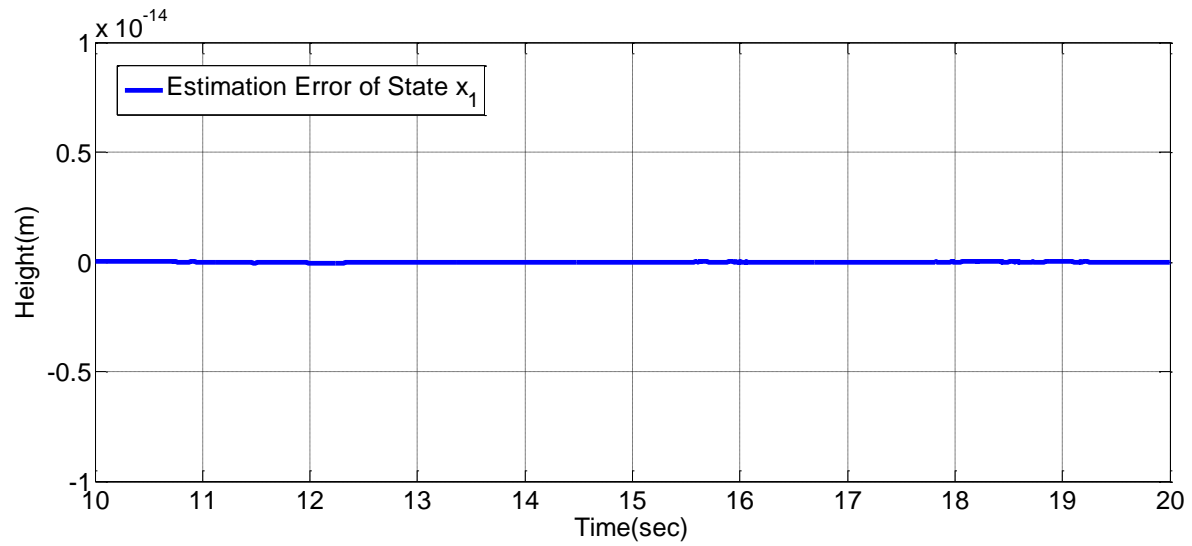
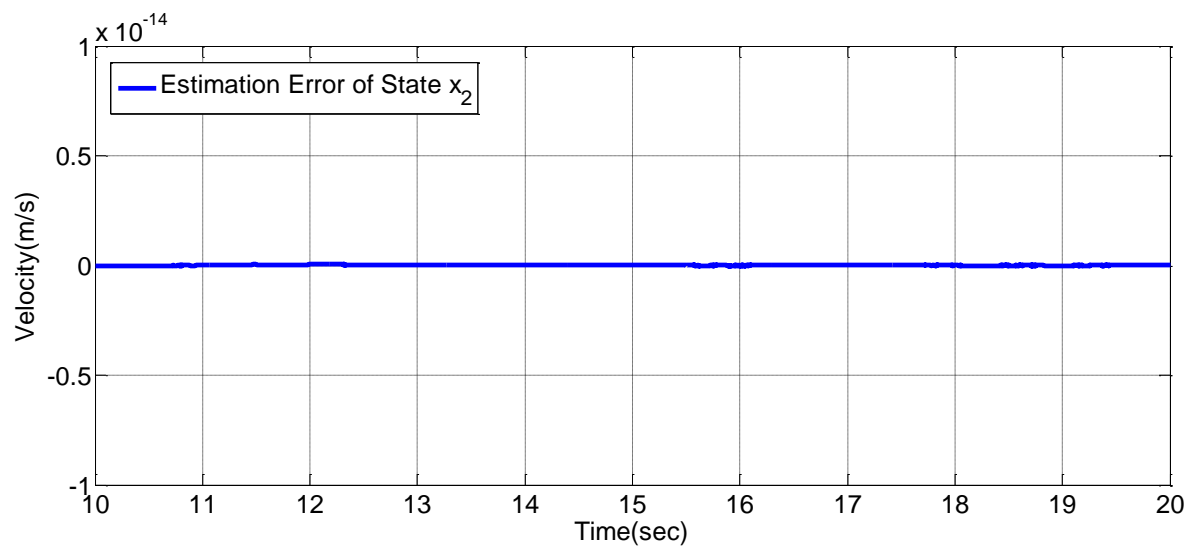
(a) State estimation error of first state (x_1)(b) State estimation error of second state (x_2)

Figure 3.11: State estimation error when using UIO based RSE method and actuator attack estimator.

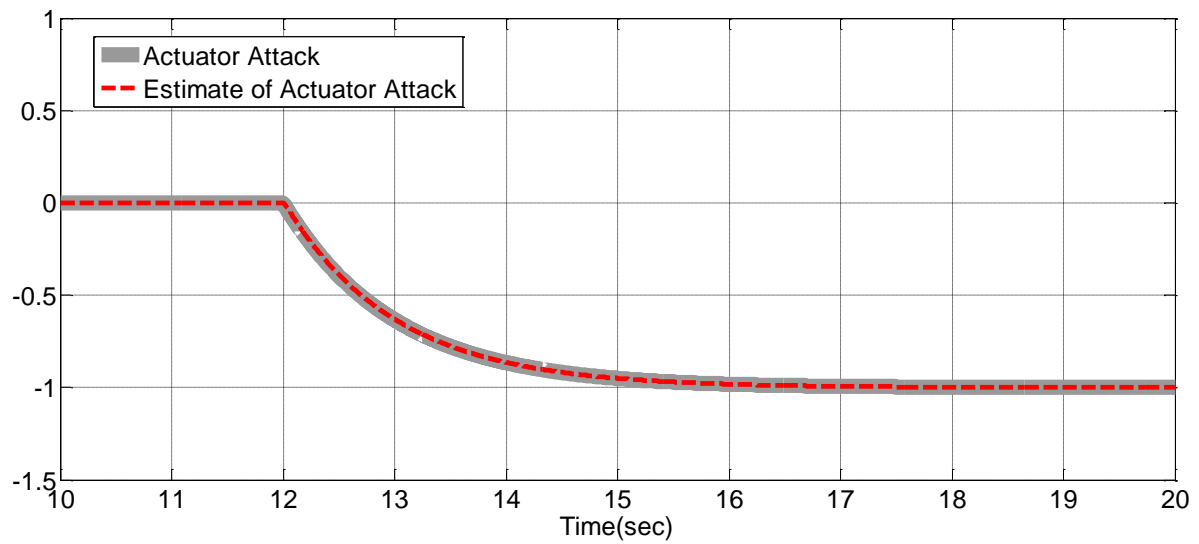


Figure 3.12: Actuator attack and estimate of actuator attack.

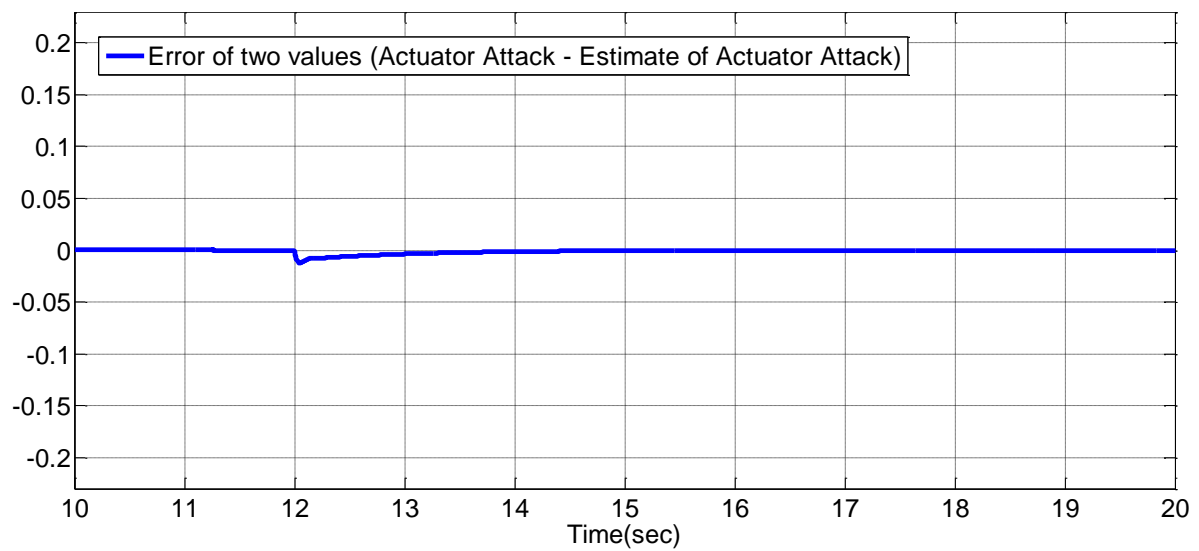


Figure 3.13: Error of between Actuator attack and Estimate of actuator attack.

3.5 Experiment Results

3.5.1 Experiment Results of Scenario 1

As we mentioned before, Scenario 1 is created to check the limitation of existing RSE method. There are two limitations. The first is state performance and the second is the effect of actuator attack. Actuator attack is injecting on third output at 10 seconds and actuator attack is injecting on system input at 12 seconds.

In Figure 3.14-3.16, (a) is first state (x_1) and (b) is second state (x_2). Figure 3.14 shows three UIO output of first state and second state. Blue dot, green dashed line, and led line are first, second, and third output of UIO. We see that third output is attacked. Overall, the experimental results of first state are similar to the simulation results of scenario 1. Results are similar to the simulation results except for some variation. Experimental results of second state shows big variation. Probably, noise would have affected. Also, we can check that existing RSE method can estimate state under sensor attack from 10 seconds to 12 seconds. The state estimate after median operation is shown in Figure 3.15. Gray line is actual state and red dashed line is estimate. State estimation error is shown in Figure 3.16. We can check two limitations of existing RSE method. The first is related to state estimation performance. In experiment, there exists the disturbance in Input. Thus, we see that state estimation error is not zero from 10 seconds to 12 seconds. In (a) of Figure 3.15, estimate is below the actual state from 10 seconds to 12 seconds. But, in (b) of Figure 3.16, estimate is over the actual state from 10 seconds to 12 seconds. The cause of this phenomenon is probably due to disturbance. After injecting actuator attack, we see that state estimation performance degrades from 12 seconds to 20 seconds. These are consistent with the simulation results. The second limitation is related to the effect of disturbance and actuator attack. we are able to see that system state is rapidly rising and then descending. In experiment results of scenario 2 and 3, we will check validation of solutions to problem 1 and 2 respectively.

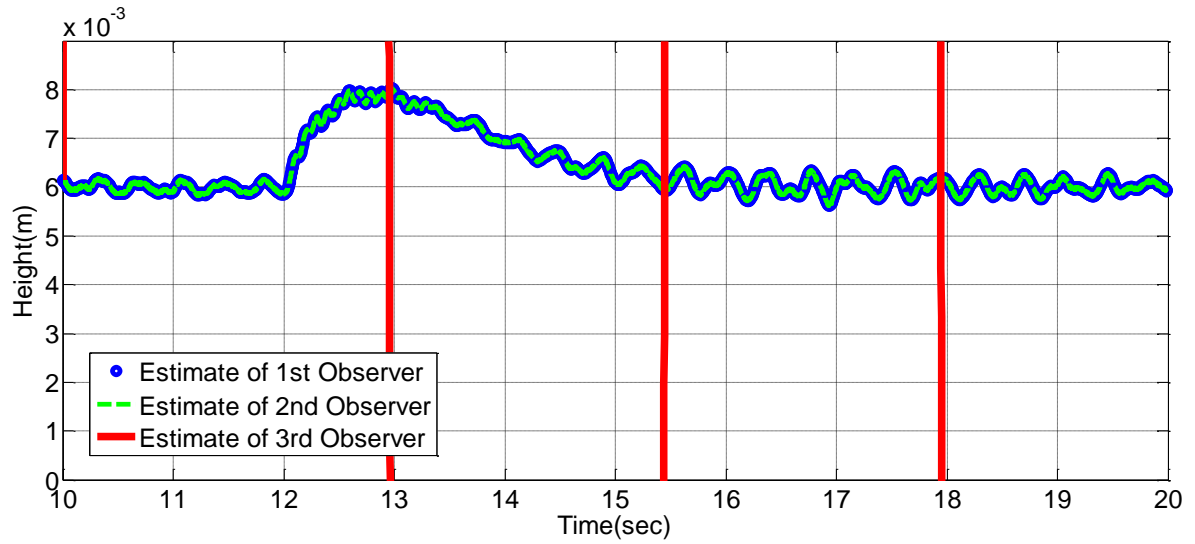
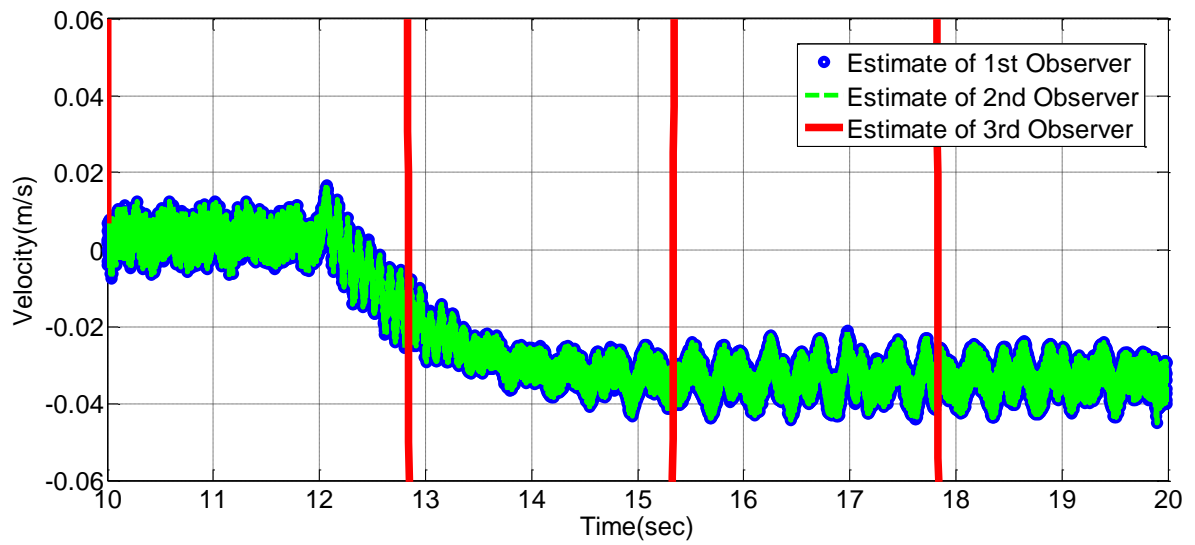
(a) Estimate of first state (x_1)(b) Estimate of second state (x_2)

Figure 3.14: Estimate of Luenberger observer when using existing RSE method (Experiment results).

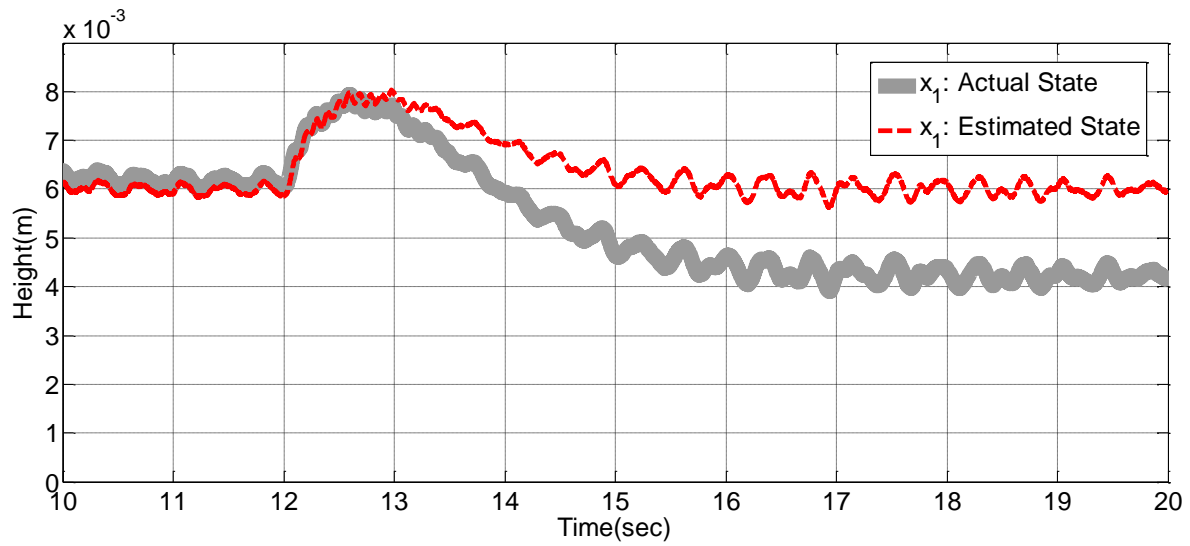
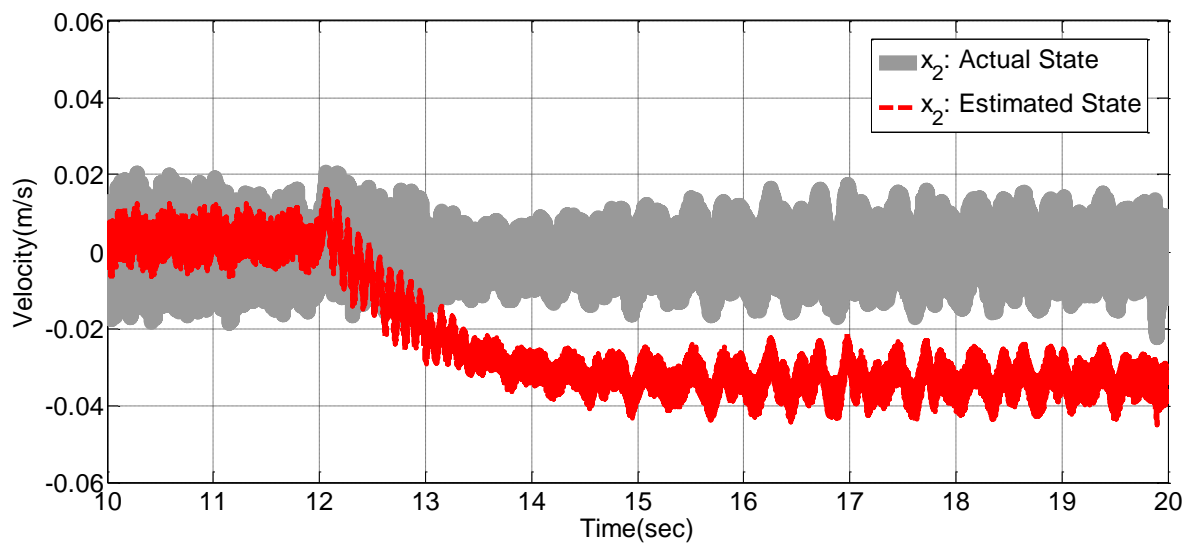
(a) First state (x_1)(b) Second state (x_2)

Figure 3.15: Actual state and estimate when using existing based RSE method (Experiment results).

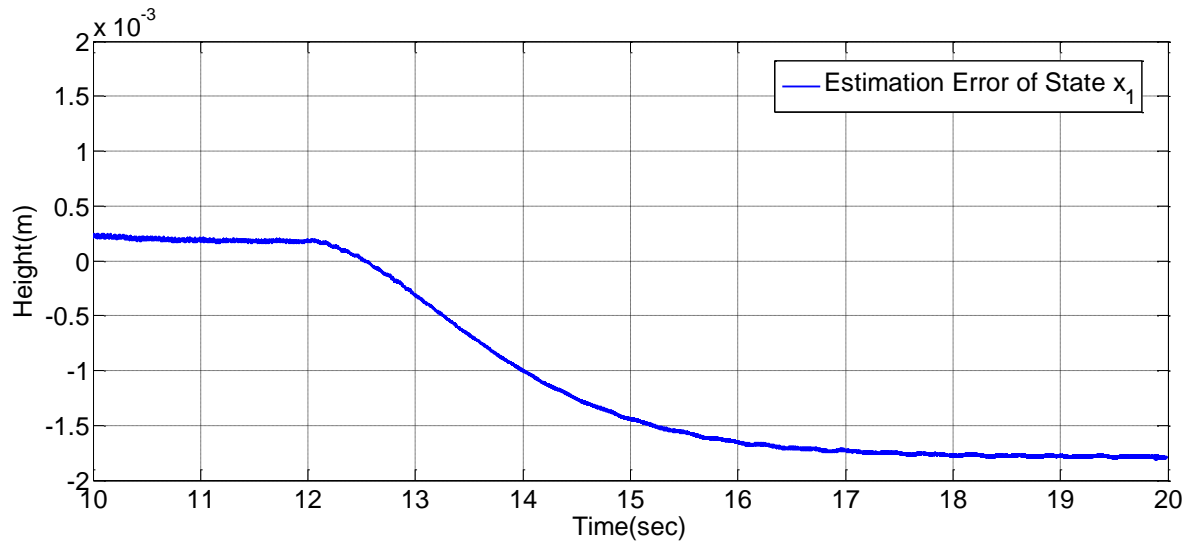
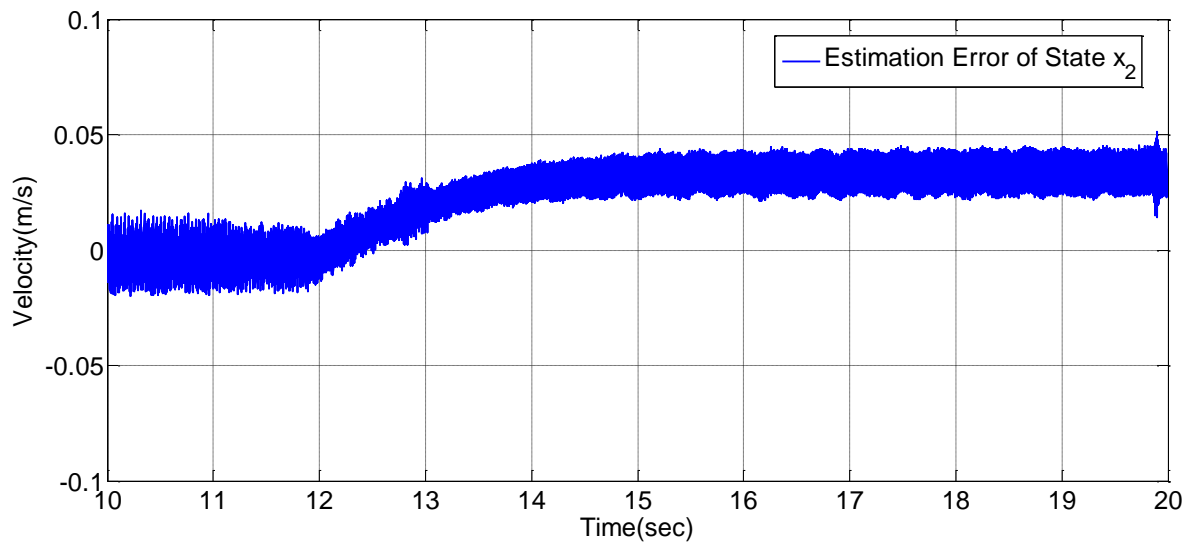
(a) State estimation error of first state (x_1)(b) State estimation error of second state (x_2)

Figure 3.16: State estimation error when using existing RSE method (Experiment results).

3.5.2 Experiment Results of Scenario 2

As we mentioned before, scenario 2 was created to validate the solution to problem 1. The solution to first problem was to use UIO based RSE method. Thus, we used UIO based RSE method in scenario 2. we were injecting sensor attack to the third output 10 seconds and actuator attack at 12 seconds as shown in Figure 3.2.

Overall, the experimental results are similar to the simulation results of scenario 2. In figure 3.17-3.19, (a) is first state (x_1) and (b) is second state (x_2). Figure 3.17 shows three UIO output of first state and second state. Blue dot, green dashed line, and led line are first, second, and third output of UIO. Results are similar to the simulation results except for some variation. Figure 3.18 shows state estimate and plant state. Gray line is actual state and red dashed line is estimate. State estimation error is shown in Figure 3.19. Compared with the experimental results of scenario 1, we can see that state estimation performance of UIO based RSE method is superior to existing RSE method. State estimation performance of UIO based RSE method is not affected by disturbance and actuator attack. Thus, we are able to check that UIO based RSE method is the method whose estimate $\hat{x}(t)$ converges to $x(t)$ as time goes on despite of disturbance and actuator attack.

But, disturbance and actuator attack may affect control performance. In figure (a) of Figure 3.18, we see that system state is rapidly rising and then descending at 12 seconds. It suggests that control performance may degrade. Unfortunately, in figure (b) of Figure 3.18, we cannot find out whether state is changed after injecting actuator attack. In simulation of scenario 2, we were able to find out that second state is varying after actuator attack. Probably in the experiment, it seems that the change of the second state is big and it is not confirmed well.

Lastly, we discuss a uncertainty. The real system always has uncertainty. Since UIO is a model based observer, if the model is not correct, it will have an estimation error for uncertainty. Bu, in Figure 3.7, it does not look like that. Thus, the uncertainty of the magnetic levitation platform and the estimation error of UIO will be analyzed. The i -th

error dynamics of UIO and system model is as follows.

$$\begin{aligned}\dot{\tilde{z}}_i(t) = & (A - H_i C_i A - K_i^1 C_i)(x(t) - z_i(t)) + (F_i - (A - H_i C_i A - K_i^1 C_i))g_i(t) \\ & - (T_i - (I - H_i C_i))Bu(t) - (H_i C_i - I)(Bd(t) + Ba^a(t)) \\ & - (K_i^2 - (A - H_i C_i A - K_i^1 C_i)H_i)y_i(t) - H_i \dot{\xi}_i(t) - K_i^1 \xi_i(t) - H_i \dot{a}_i^s(t) - K_i^1 a_i^s(t).\end{aligned}\quad (3.39)$$

Here, the method to check whether the state estimation error of the UIO increases when having model uncertainty is to check how the equation of $(A - H_i C_i A - K_i C_i)$ changes and to check whether the following two equations always satisfy 0.

$$(T_i - (I - H_i C_i))B = 0, \quad (3.40)$$

$$(H_i C_i - I)B = 0. \quad (3.41)$$

In order, we will check how the above equations change even though we have model uncertainty. Firstly, each $(A - H_i C_i A - K_i C_i)$ of from 1-st to 3-rd is as follows.

$$\begin{aligned}A - H_1 C_1 A - K_1^1 C_1 &= \begin{bmatrix} 0 & 1 \\ \frac{K_m I_0^2}{M_b x_{10}^3} & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ \frac{K_m I_0^2}{M_b x_{10}^3} & 1 \end{bmatrix} - \begin{bmatrix} 500 & 500 \\ 500 & 500 \end{bmatrix}, \\ &= \begin{bmatrix} 0 & 1 \\ 3270 + \Delta_A & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 3270 + \Delta_A & 1 \end{bmatrix} - \begin{bmatrix} 500 & 500 \\ 500 & 500 \end{bmatrix},\end{aligned}\quad (3.42)$$

$$\begin{aligned}A - H_2 C_2 A - K_2^1 C_2 &= \begin{bmatrix} 0 & 1 \\ \frac{K_m I_0^2}{M_b x_{10}^3} & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ \frac{K_m I_0^2}{M_b x_{10}^3} & 1 \end{bmatrix} - \begin{bmatrix} 500 & 500 \\ 500 & 500 \end{bmatrix}, \\ &= \begin{bmatrix} 0 & 1 \\ 3270 + \Delta_A & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 3270 + \Delta_A & 1 \end{bmatrix} - \begin{bmatrix} 500 & 500 \\ 500 & 500 \end{bmatrix},\end{aligned}\quad (3.43)$$

$$\begin{aligned}A - H_3 C_3 A - K_3^1 C_3 &= \begin{bmatrix} 0 & 1 \\ \frac{K_m I_0^2}{M_b x_{10}^3} & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ \frac{K_m I_0^2}{M_b x_{10}^3} & 1 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 1000 \end{bmatrix}, \\ &= \begin{bmatrix} 0 & 1 \\ 3270 + \Delta_A & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 3270 + \Delta_A & 1 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 1000 \end{bmatrix},\end{aligned}\quad (3.44)$$

where Δ_A means uncertainty. In above equations, we can see that a part having uncertainty in A matrix is canceled with each other. And it can be confirmed that it does not affect the state estimation error. Then, let we check equation of (3.40). Each $(T_i - (I - H_i C_i))B$ of from 1-st to 3-rd is as follows

$$\begin{aligned} (T_1 - (I - H_1 C_1))B &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -\frac{K_m I_0}{M_b x_{10}^2} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -26.67 + \Delta_B \end{bmatrix} \\ &= \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \end{aligned} \quad (3.45)$$

$$\begin{aligned} (T_2 - (I - H_2 C_2))B &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -\frac{K_m I_0}{M_b x_{10}^2} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -26.67 + \Delta_B \end{bmatrix} \\ &= \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \end{aligned} \quad (3.46)$$

$$\begin{aligned} (T_3 - (I - H_3 C_3))B &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -\frac{K_m I_0}{M_b x_{10}^2} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -26.67 + \Delta_B \end{bmatrix} \\ &= \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \end{aligned} \quad (3.47)$$

where Δ_B means uncertainty. In above equations, we see that $(T_i - (I - H_i C_i))$ is zero. Thus, it can be seen that even if the B matrix has uncertainty, it does not affect the state estimation. Lastly, let we check equation of (3.41). Each $(H_i C_i - I)B$ of from 1-st to 3-rd is as follows

$$\begin{aligned} (H_1 C_1 - I)B &= \begin{bmatrix} -1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -\frac{K_m I_0}{M_b x_{10}^2} \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -26.67 + \Delta_B \end{bmatrix} \\ &= \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \end{aligned} \quad (3.48)$$

$$\begin{aligned}
(H_2C_2 - I)B &= \begin{bmatrix} -1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -\frac{K_m I_0}{M_b x_{10}^2} \end{bmatrix} == \begin{bmatrix} -1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -26.67 + \Delta_B \end{bmatrix} \\
&= \begin{bmatrix} 0 \\ 0 \end{bmatrix},
\end{aligned} \tag{3.49}$$

$$\begin{aligned}
(H_3C_3 - I)B &= \begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -\frac{K_m I_0}{M_b x_{10}^2} \end{bmatrix} == \begin{bmatrix} -1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ -26.67 + \Delta_B \end{bmatrix} \\
&= \begin{bmatrix} 0 \\ 0 \end{bmatrix},
\end{aligned} \tag{3.50}$$

where Δ_B means uncertainty. In above equations, we see that each $(H_iC_i - I)B$ is zero even if B has uncertainty. Thus, it can be seen that even if the B matrix has uncertainty, it does not affect the state estimation. In summary, when the magnetic levitation platform is modeled as Equation of (3.8), the uncertainty of the actual system does not affect the estimation performance of the UIO. Nevertheless, it is thought that the reason for the slight estimation error is the influence of the influence of time derivative of noise and noise. For other systems, it can not be guaranteed that uncertainty does not affect the estimated performance of the UIO. For other systems, uncertainty may or may not affect estimation error of UIO. This effect can be seen through analysis of error dynamics.

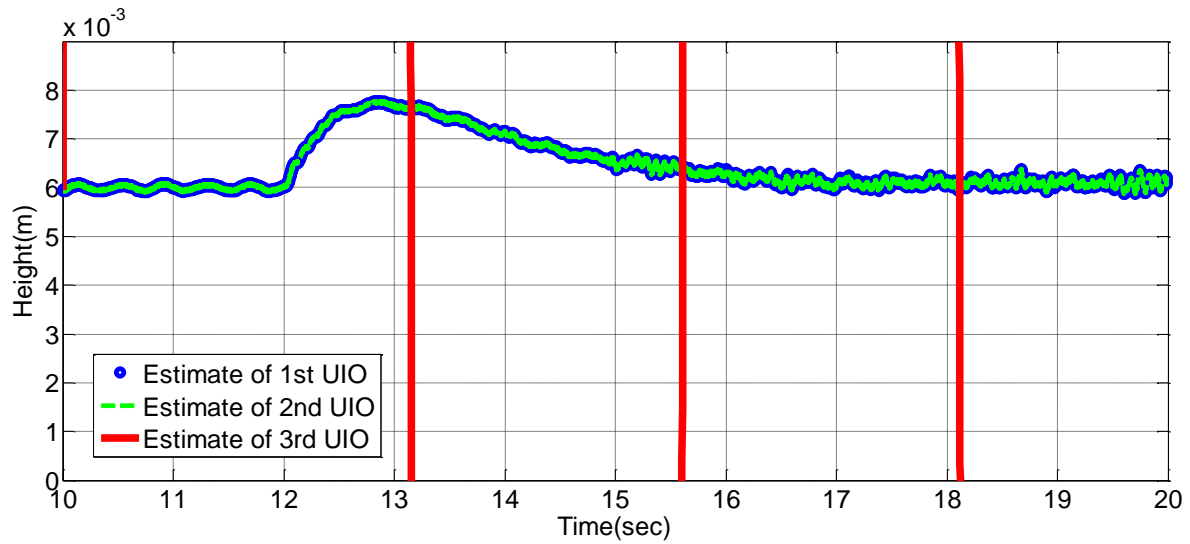
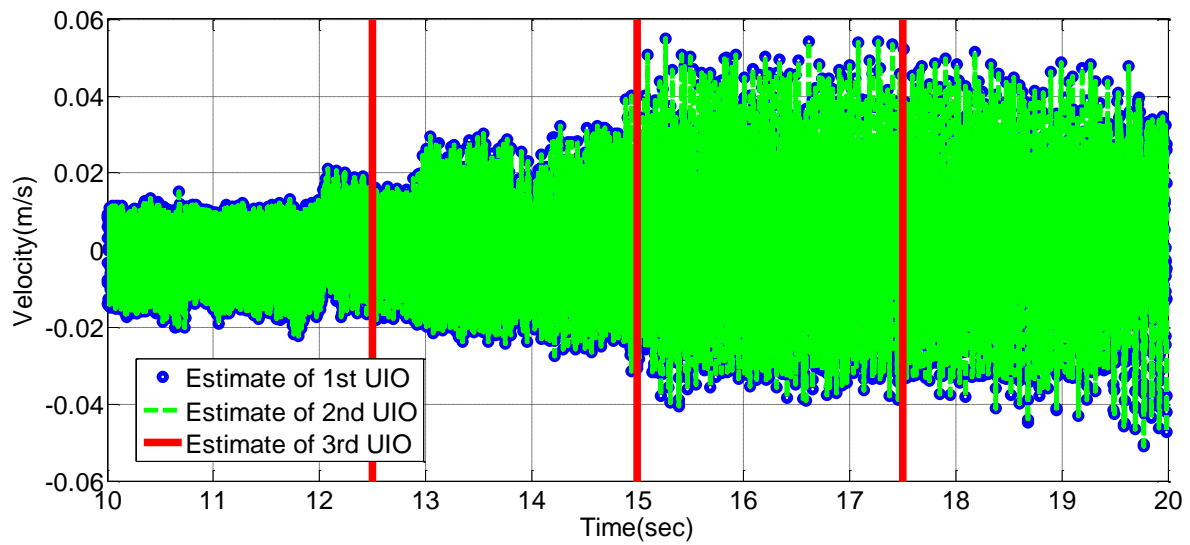
(a) Estimate of first state (x_1)(b) Estimate of second state (x_2)

Figure 3.17: Estimate of UIO When using UIO based RSE method (Experiment results).

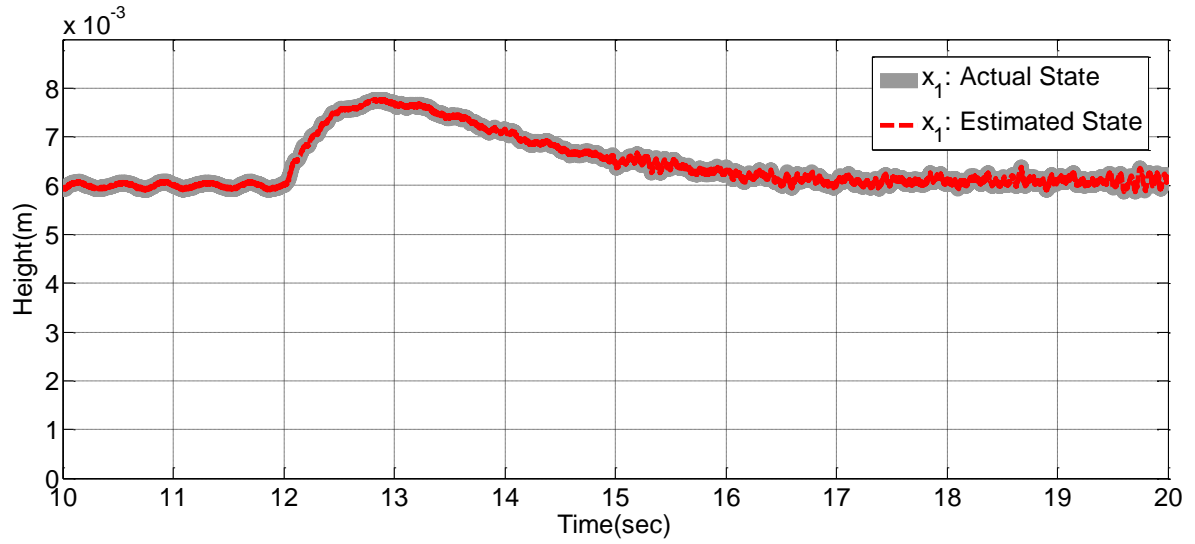
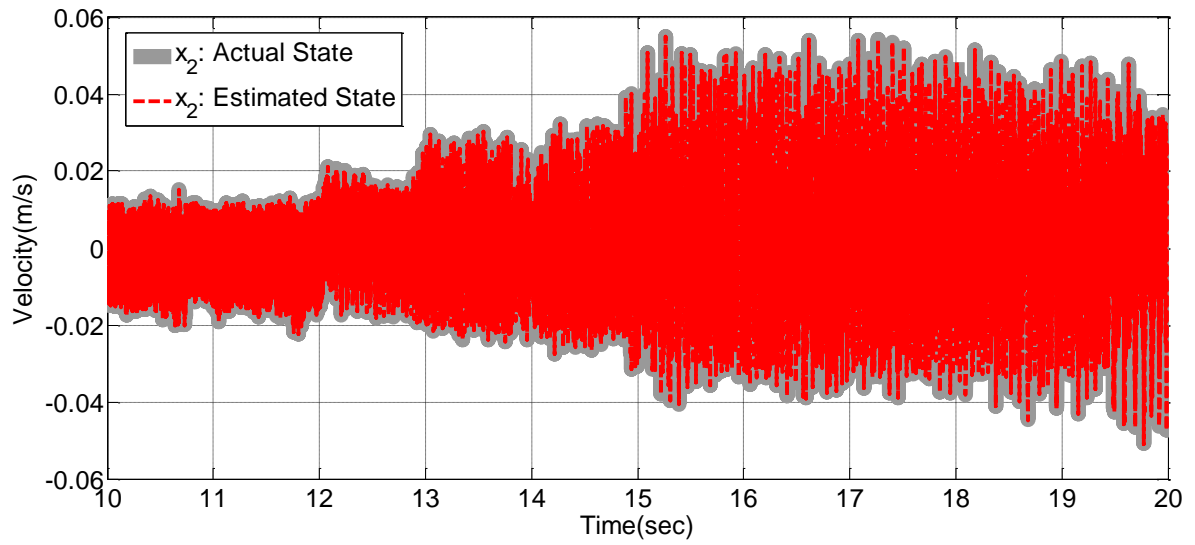
(a) First state (x_1)(b) Second state (x_2)

Figure 3.18: Actual state and estimate when using UIO based RSE method (Experiment results).

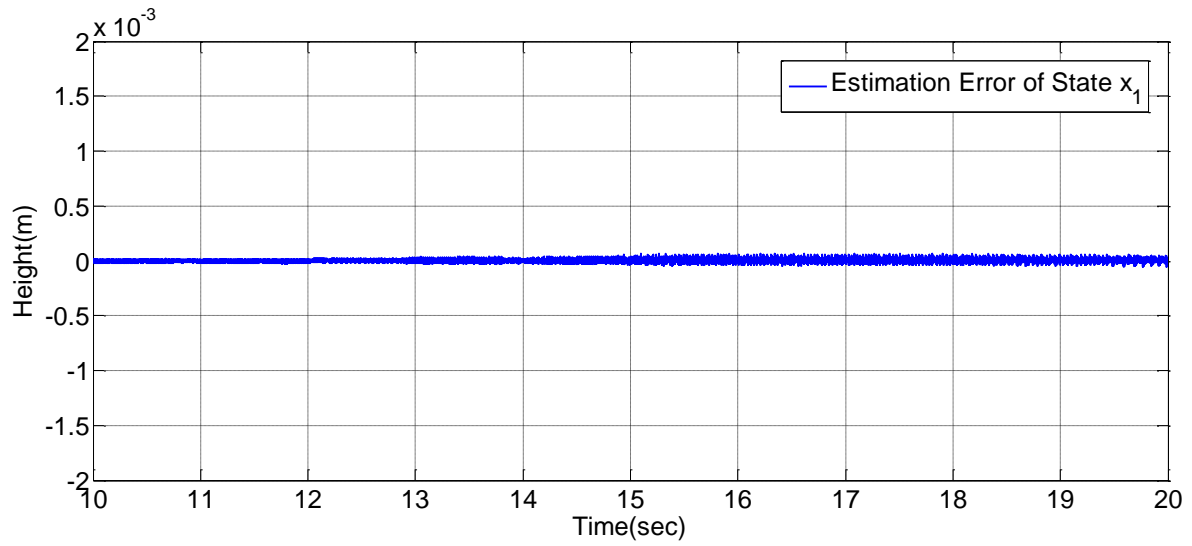
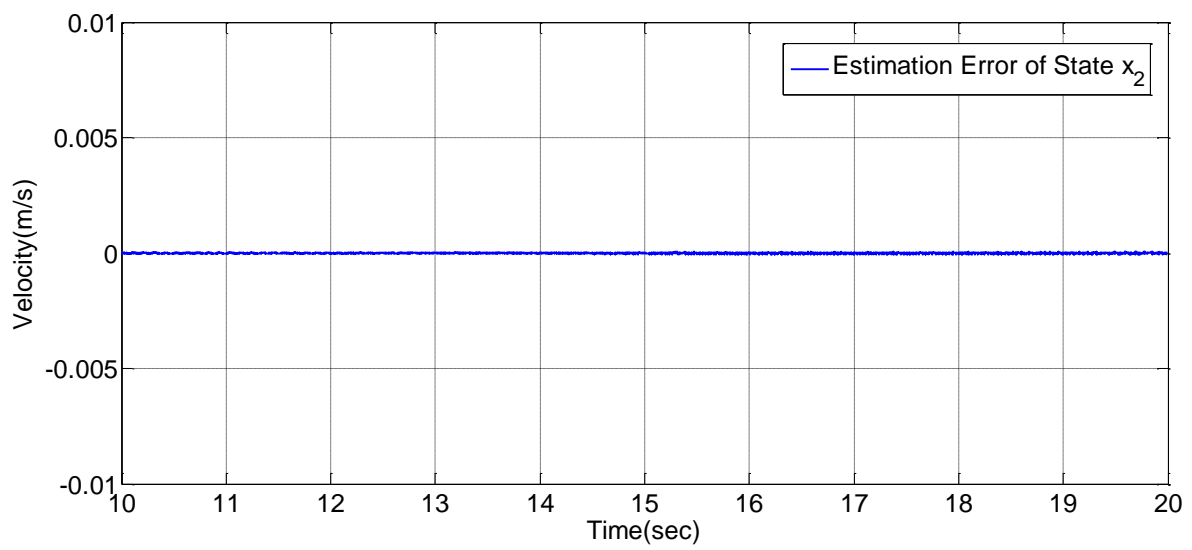
(a) State estimation error of first state (x_1)(b) State estimation error of second state (x_2)

Figure 3.19: State estimation error when using UIO based RSE method (Experiment results).

3.5.3 Experiment Results of Scenario 3

As we mentioned before, scenario 3 was created to validate the solution to problem 3. The solution to second problem was to use the actuator attack estimation method exploiting UIO based RSE method. Thus, in this scenario 3, we used UIO based RSE method and actuator attack estimation method together. we were injecting sensor attack to third output at 10 seconds and actuator attack at 12 seconds as shown in Figure 3.2.

In Figure 3.20-3.22, (a) is first state (x_1) and (b) is second state (x_2). Figure 3.20 shows estimate of each UIO. We can see that third output is attacked. Figure 3.21 shows the output of UIO based RSE method. Figure 3.22 is state estimation error. In experimental result of second state has a big variation unlike simulation. Thus, it is hard for using second state to analyze the phenomenon. We only focus on first state. In experiment results of scenario 2, we were able to checked that first state is rapidly rising and then descending after actuator attack. But, in (a) of Figure 3.21, we can see that effect of actuator attack is reduced considerably. This is because actuator attack estimation method well estimated and removed from the effects of disturbance and actuator attack. Figure 3.23 shows real actuator attack and estimate. Figure 3.24 is error of two values between real actuator attack and estimate. we can see that there is error between two values in Figure 3.23. The error of the two values is considered to be a disturbance in the system input, since actuator attack estimation estimate the effect of disturbance and actuator attack together.

In short, we are able to check the effectiveness of proposed method. UIO based RSE method has superior state estimation performance under sensor attack and actuator attack than existing RSE method. Also, actuator attack estimation method would be able to estimate and reject the effect of disturbance and actuator attack. Therefore, by using UIO based RSE method and actuator attack estimation method using UIO based, the system is able to improve the resiliency under restrictive sensor attacks and actuator attack.

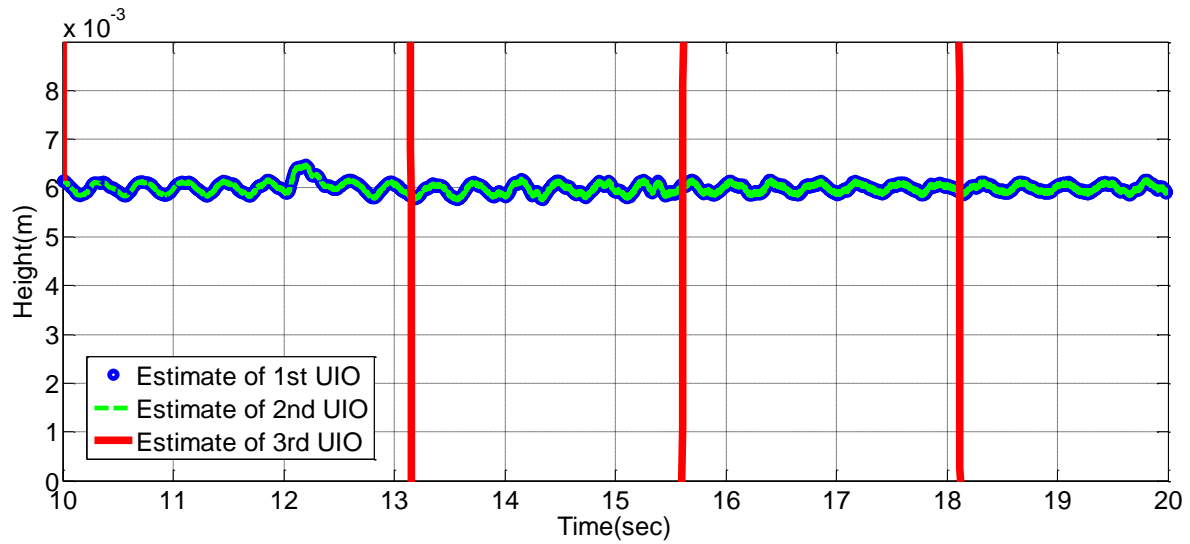
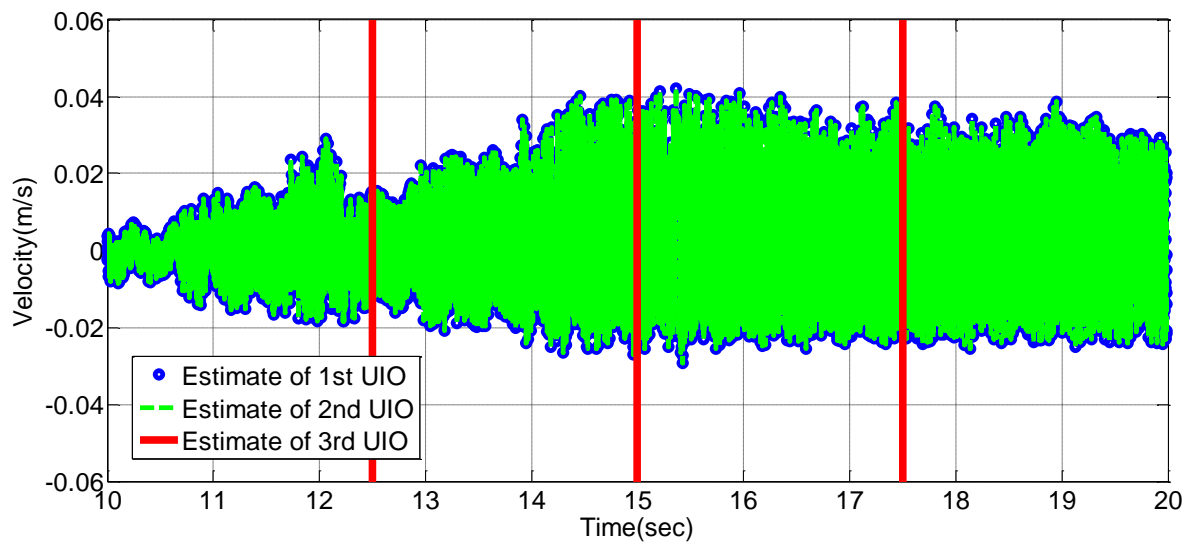
(a) Estimate of first state (x_1)(b) Estimate of second state (x_2)

Figure 3.20: Estimate of UIO when using UIO based RSE method and actuator attack estimator (Experiment results).

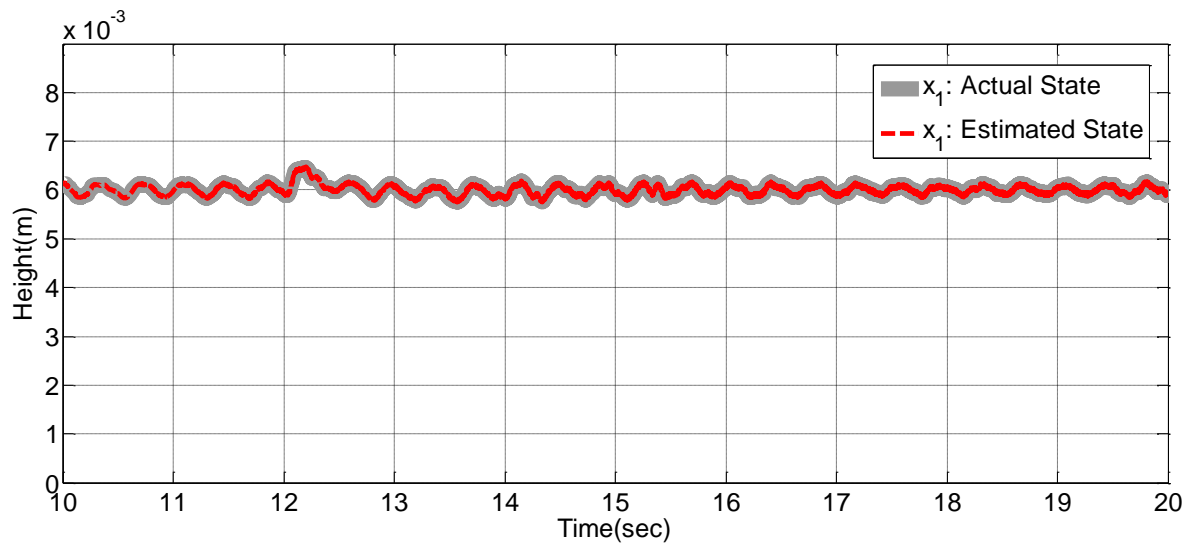
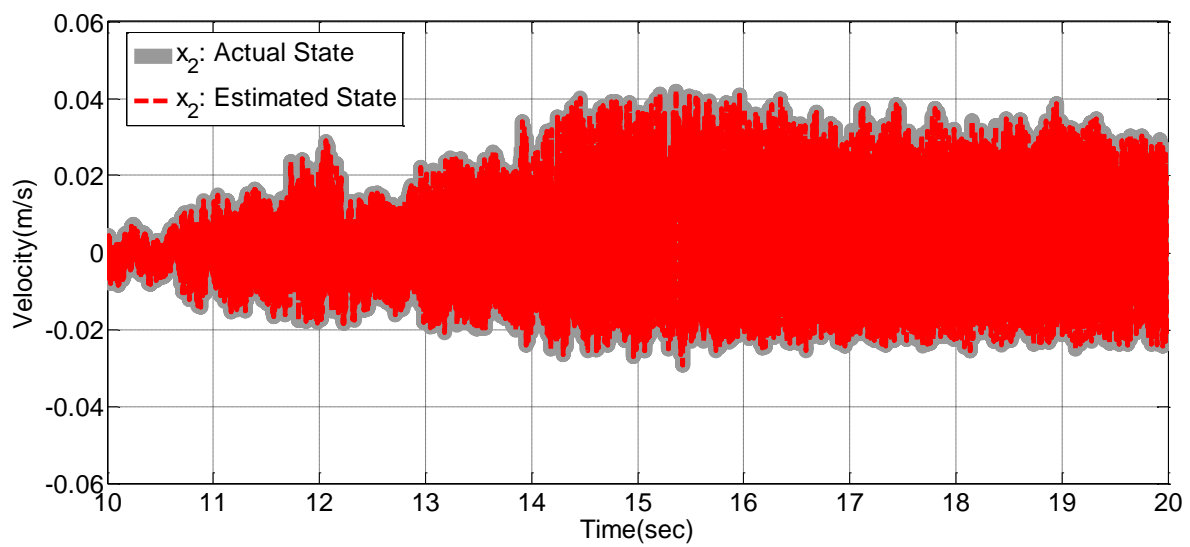
(a) First state (x_1)(b) Second state (x_2)

Figure 3.21: Actual state and estimate when using UIO based RSE method and actuator attack estimator (Experiment results).

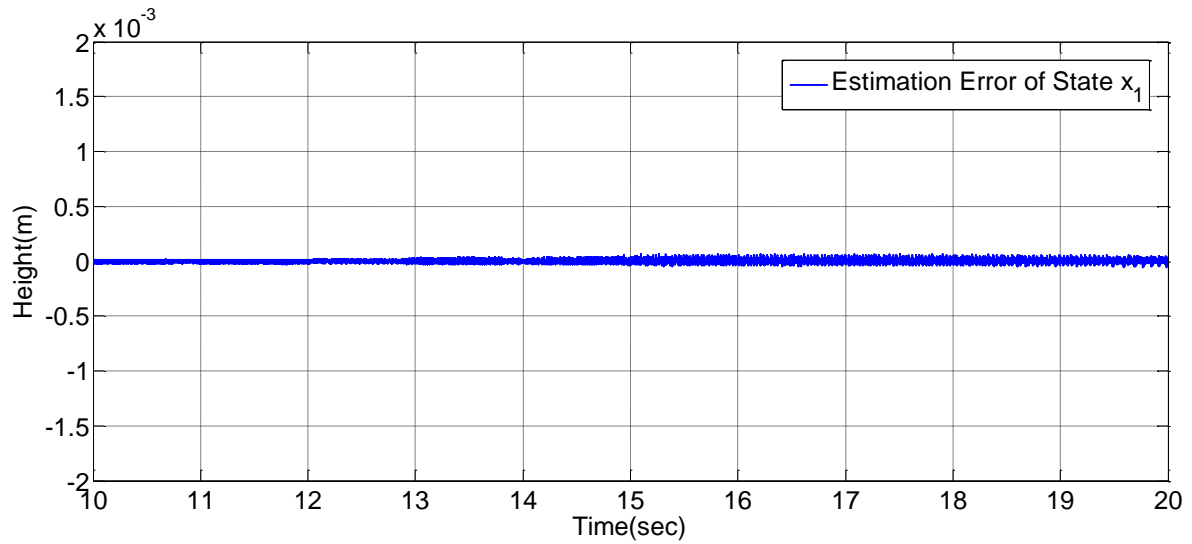
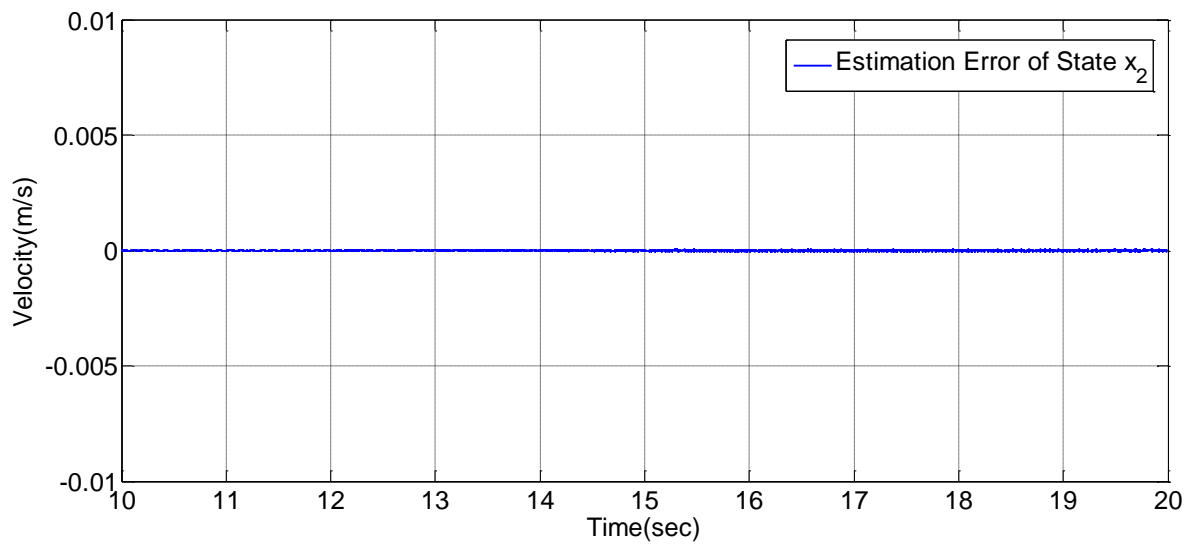
(a) State estimation error of first state (x_1)(b) State estimation error of second state (x_2)

Figure 3.22: State estimation error when using UIO based RSE method and actuator attack estimator (Experiment results).

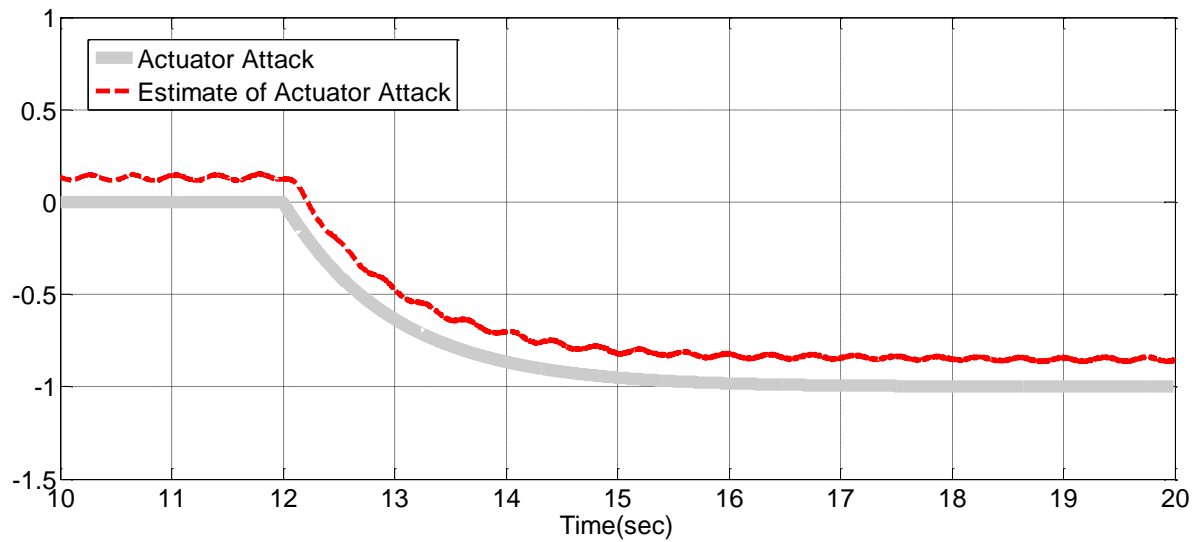


Figure 3.23: Actuator attack and estimate of actuator attack (Experiment results).

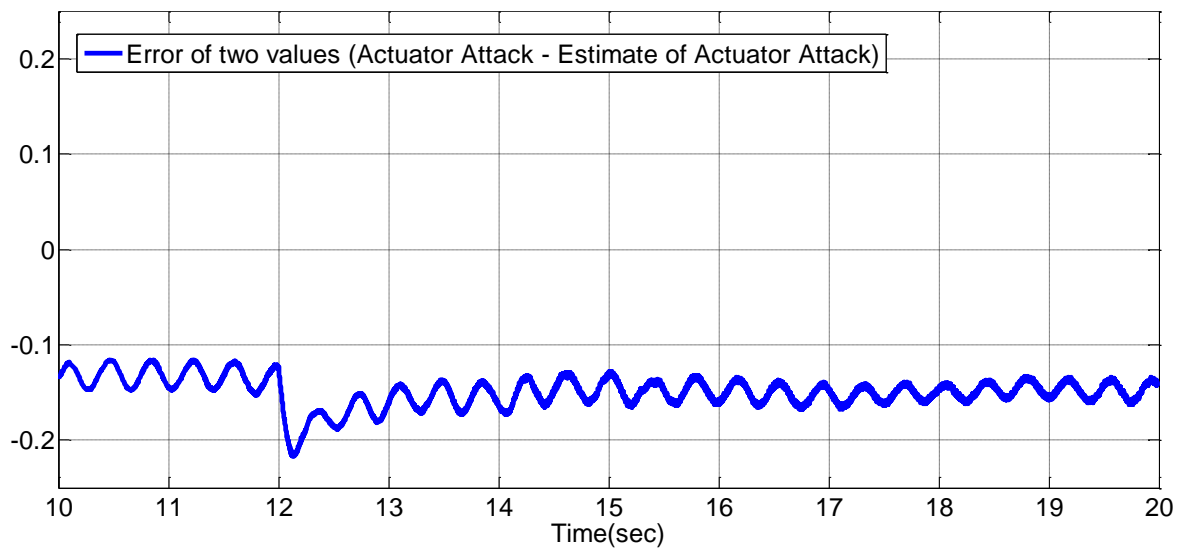


Figure 3.24: Error of Actuator attack and Estimate of actuator attack (Experiment results).

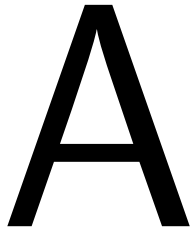
4

Conclusion

In this thesis, we proposed resilient control system design method under sensor attack, disturbance and actuator attack.

In order to protect the system from sensor attack, we consider observer based resilient state estimation method. existing method is to use the Luenberger observer as observer of state estimator. In this case, disturbance and actuator attack affect the state estimation error. In this thesis, we prove the state estimation error when using existing method. Proposed method is to exploit Unknown Input Observer as observer of state estimation method. The state estimation error of proposed method is superior regardless of disturbance and actuator. We also prove state estimation error in detail. In addition, we suggest a algorithm that is able to diagnose which sensors are attacked or broken by exploiting proposed UIO based RSE method. In order to protect the system from actuator attack, we propose a method that would be able to estimate and reject the effect of disturbance and actuator attack. This method also use the proposed UIO based RSE method.

So as to validate the effectiveness of proposed method, We made three scenarios. Simulations and experiments are implemented on the magnetic levitation system platform. We showed that existing method has two limitations. Then, we showed that UIO based RSE method has superior state estimation performance to existing RSE method and the effect of disturbance and actuator attack is rejected by using actuator attack estimation method. We would like to emphasize that system would be resilient by designing proposed UIO based resilient control system regardless of malicious attacks.



MATLAB Code For Numerical Simulation

Analysis_of_time_derivative_of_noise_and_noise.m

```
1
2
3 clc
4 clear
5 syms t F tau w eta H
6 f=exp(F*(t-tau))*H*eta*w*cos(tau*w)
7 int(f,tau,0,t)
8
9 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
10 clc
11 clear
12 syms F11 F12 F21 F22
13 syms F
14 F=[F11 F12;F21 F22]
15 syms H11 H21
16 syms H
17 H=[H11;H21]
18 syms t tau eta w a
19 f=exp([F11 F12;F21 F22]*(t-tau))*[H11;H21]*eta*w*cos(w*tau)
20 SOL=int(f,tau,0,t)
21 tt=exp(F)
22
23 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
24 clc
25 clear
26 syms F11 F12 F21 F22
27 syms F
28 F=[F11 F12;F21 F22]
29 syms DI11 DI12 DI21 DI22
30 syms DI
31 DI=[DI11 DI12;DI21 DI22]
32 syms D11 D12 D21 D22
33 syms D
34 D=[D11 D12;D21 D22]
35 syms eig1 eig2
36 syms H11 H21
37 syms H
38 H=[H11;H21]
39 syms t tau eta w a
40 f=DI*[exp(eig1*(t-tau)) 0;0 exp(eig2*(t-tau))]*D * [H11;H21]*eta*w*cos(w*tau)
41 SOL=int(f,tau,0,t)
42
```

Numerical_example.m

```
1
2  clc
3  clear
4
5  A=[2.1 3.5;1.3 -2.5]
6  B=[0.75;2.8]
7  C=[1 1]
8  initial_state=[0 0]
9  Ts=1e-4
10 %% state feedback controller
11 K=place(A,B,[-11 -12])
12 p=1/(C*(A+B*K)^-1*B)
13 eigv=eig(A-B*K)
14 %% UI0
15 % step 1
16 rank(B)
17 rank(C*B)
18 H=B*inv((C*B)'*(C*B))*(C*B)'
19 T=eye(2)-H*C
20 A1=T*A
21 RANK=rank(observ(A1,C))
22 [A1bar,B1bar,C1bar,P1,k1] = obsvf(A1,B,C)
23 K1_1=place(A1bar(2,2)',C1bar(1,2)',[-10])
24 K1=P1^-1*[0' K1_1']
25 F1=A1-K1*C
26 KK=K1+F1*H
27 eig(A1-K1*C)
28 %%
29 H
30 K1
31 A-H*C*A-K1*C
32 inv(A-H*C*A-K1*C)
33 %% F*K1
34 inv(A-H*C*A-K1*C)*K1
35 %% F*H
36 aaa=inv(A-H*C*A-K1*C)*H
37 %%
38 [V,D]=eig(F1)
39 di=V
40 d=inv(V)
41 d(1,1)*di(1,1)*H(1,1) + d(1,2)*di(1,1)*H(2,1)+d(2,1)*di(1,2)*H(1,1)+d(2,2)*di(1,2)*H(2,1)
42 d(1,1)*di(2,1)*H(1,1) + d(1,2)*di(2,1)*H(2,1)+d(2,1)*di(2,2)*H(1,1)+d(2,2)*di(2,2)*H(2,1)
43
```

Magnetic_Levitation_NEW_VERSION_20160807.m

```
1
2  g=9.8;
3  xb0=0.0060;
4  Ic0=1.1000;
5
6  %% State Space Form
7  Ac = [0 1; 2*g/xb0 0]
8  Bc = [0; -2*xb0*g/Ic0/xb0]
9  Cc = [1 1; 1 1; 0 1]
10 Dc = 0
11 n = size(Ac,1);
12 m=size(Bc,2);
13 T = n;
14 EC = eye(n,n);
15 ED = zeros(n,1);
16 %%
17
18 LLL=place(Ac',Cc(2,1:2)',[-103, -104])'
19 LLL2=place(Ac',Cc',[-101, -102])'
```

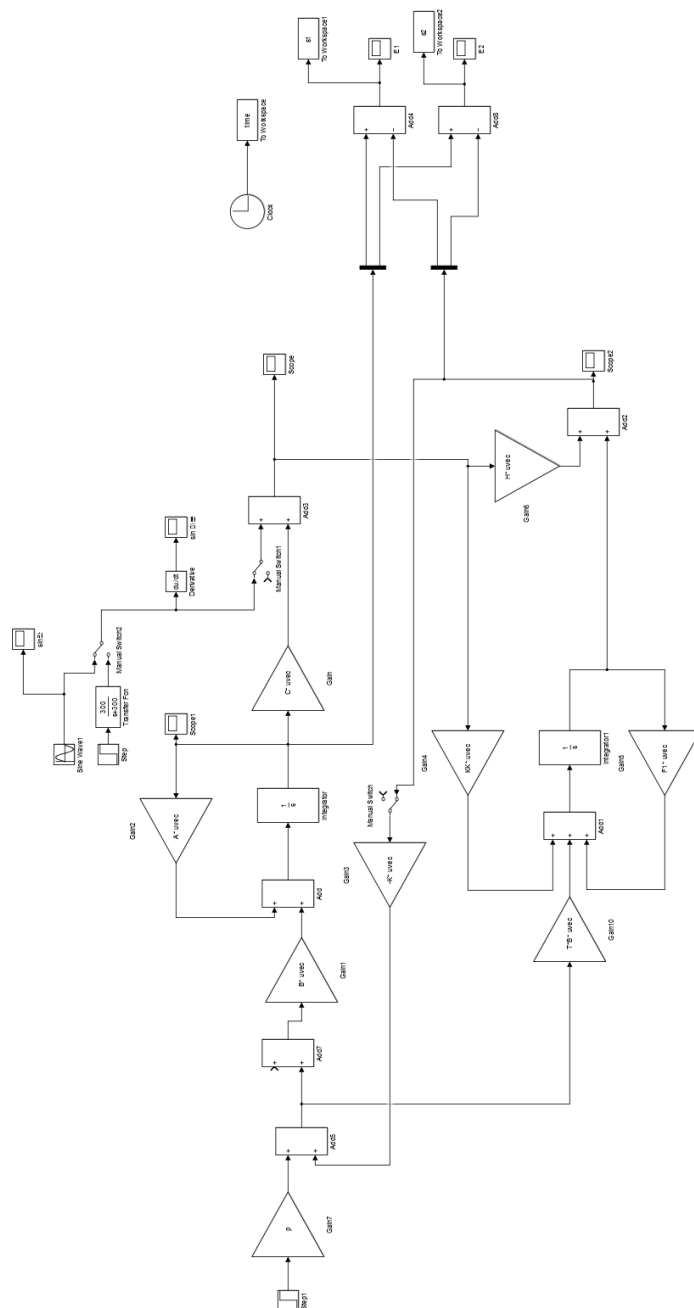


Figure A.1: Numerical_example.slx.


```
20 %%
21
22 rank_of_observability_matrix1=rank(observ(Ac,Cc(1,1:2)))
23 rank_of_observability_matrix1=rank(observ(Ac,Cc(2,1:2)))
24 rank_of_observability_matrix1=rank(observ(Ac,Cc(3,1:2)))
25
26 %% Discrete Time
27 sys_v = ss(Ac,Bc,Cc,Dc);
28 sys_vd = c2d(sys_v,Ts);
29 A = sys_vd.A
30 B = sys_vd.B
31 C = sys_vd.C
32 D = Dc
33 %% Observer Gain
34 Ob_poles1 = [-1.5, -370];
35 L1 = place(Ac',Cc(1,1:2)',Ob_poles1)'
36 Ob_poles2 = [-1.5, -370];
37 L2 = place(Ac',Cc(2,1:2)',Ob_poles2)'
38 Ob_poles3 = [-1.5,-370];
39 L3 = place(Ac',Cc(3,1:2)',Ob_poles3)'
40
41 LLLL=[L1'; L2'; L3']'
42
43 Ac_L1C1=Ac-L1*[1 1]
44 Ac_L1C1_inv=inv(Ac_L1C1)
45
46 eig(Ac-L1*[1 1])
47
48 [V,D]=eig(Ac-L1*[1 1])
49 V_inv=inv(V)
50
51 %%
52
53 New_C=Cc
54
55 E=Bc
56 C11=New_C(1,1:2)
57 C22=New_C(2,1:2)
58 C33=New_C(3,1:2)
59
60 % step 1
61 % check the possibility of using the UIO
62 % rank should be equal on the rank(E and CE)
63
64 rank(E)
65 rank(New_C*E)
66 %%
67 % step 2
68
69 HH11=E*inv((C11*E)'*(C11*E))*(C11*E)'
70
71 TT11=eye(2)-HH11*C11
72
73 AA11=TT11*Ac
74
75 rank(observ(AA11,C11))
76
77 [A11bar,B11bar,C11bar,P11,k11] = obsvf(AA11,Bc,C11)
78
79 KK11_1=place(A11bar(2,2)',C11bar(1,2)',[-1000])
80
81 KK11=P11^-1*[0' KK11_1']'
82
83 eig(AA11-KK11*C11)
84
85 %KK11=place(A11',C11',[-500,-501])
86 %KK11=KK11'
87
88 FF11=AA11-KK11*C11
89 KK_11=KK11+FF11*HH11
90
91 %%
92
```

```

93 HH22=E*inv((C22*E)')*(C22*E))*(C22*E)'
94
95 TT22=eye(2)-HH22*C22
96
97 AA22=TT22*Ac
98
99 rank(observ(AA22,C22));
100 [A22bar,B22bar,C22bar,P22,k22] = obsvf(AA22,Bc,C22)
101
102 KK22_1=place(A22bar(2,2)',C22bar(1,2)',[-1000])
103
104 KK22=P22^-1*[0' KK22_1']'
105
106 eig(AA22-KK22*C22)
107
108 %KK22=place(Ac',C22',[-500,-501])
109 %KK22=KK22'
110
111 FF22=AA22-KK22*C22
112 KK_22=KK22+FF22*HH22
113
114 %%
115 HH33=E*inv((C33*E)')*(C33*E))*(C33*E)'
116
117 TT33=eye(2)-HH33*C33
118
119 AA33=TT33*Ac
120
121 rank(observ(AA33,C33))
122
123 [A33bar,B33bar,C33bar,P33,k33] = obsvf(AA33,Bc,C33)
124
125 KK33_1=place(A33bar(2,2)',C33bar(1,2)',[-1000])
126
127 KK33=P33^-1*[0' KK33_1']'
128
129 eig(AA33-KK33*C33)
130
131 FF33=AA33-KK33*C33
132 KK_33=KK33+FF33*HH33
133
134
135

```

Block:Magnetic_Levitation_System/Median Operator

```

1
2 function State_X = fcn(Esti_Ob_x,A,C)
3
4 n = size(A,1);
5 p = size(C,1);
6
7 Expl_x = zeros(n,p);
8
9 for k=1:p
10     Expl_x(:,k) = Esti_Ob_x(n*(k-1)+1:n*k);
11 end
12 State_X = median(Expl_x');
13
14
15

```

Block:Magnetic_Levitation_System/Sensor Attack Diagnosis Method

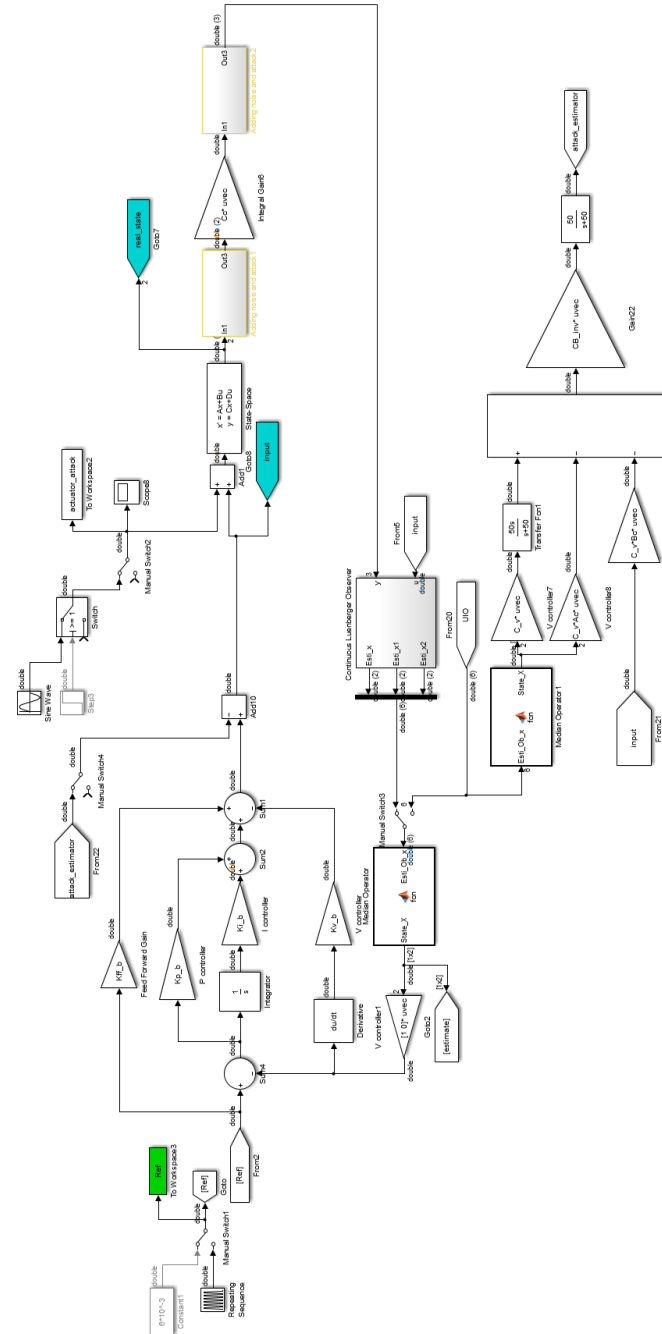


Figure A.2: Magnetic_Levitation_System.slx.

```
1 function [y1,y2,y3,result]= fcn(e1,e2,e3,residual)
2
3
4 ee1=sqrt(e1(1,1)^2+e1(2,1)^2);
5
6 ee2=sqrt(e2(1,1)^2+e2(2,1)^2);
7
8 ee3=sqrt(e3(1,1)^2+e3(2,1)^2);
9
10 if (ee1>residual)
11     count1=1;
12 else
13     count1=0;
14 end
15
16 if (ee2>residual)
17     count2=2;
18 else
19     count2=0;
20 end
21
22 if (ee3>residual)
23     count3=3;
24 else
25     count3=0;
26 end
27
28
29
30 y1 = ee1;
31 y2=ee2;
32 y3=ee3;
33
34 result=count1+count2+count3;
35
36
```

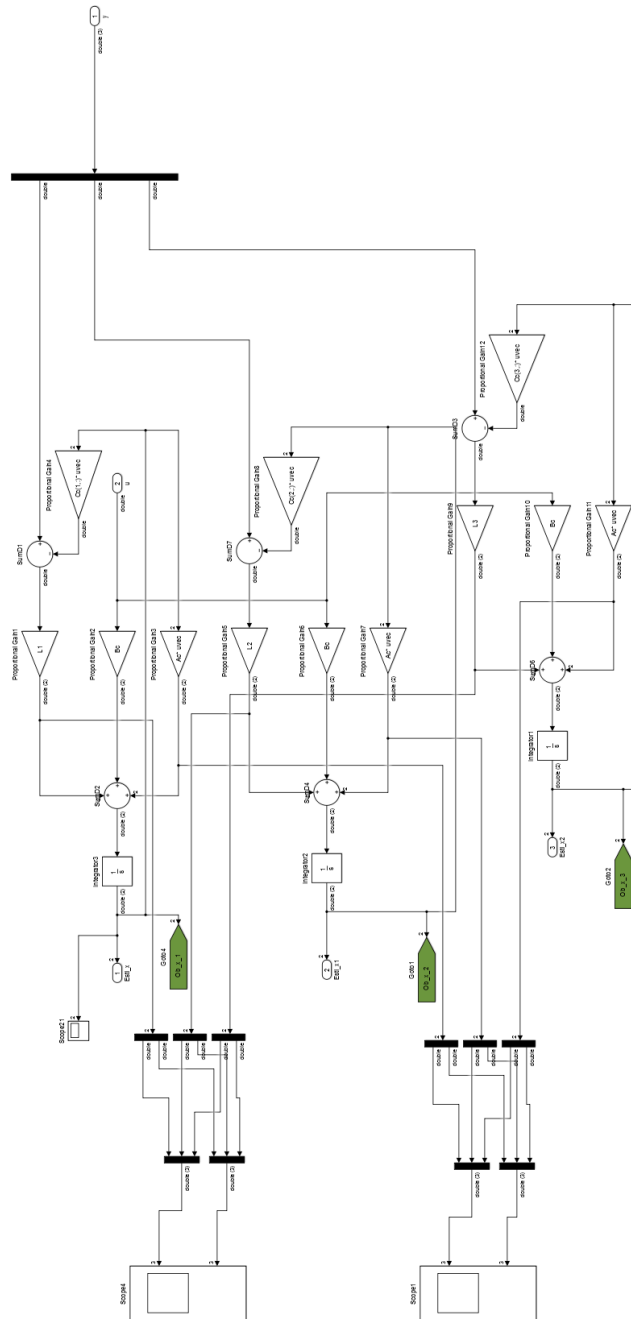


Figure A.3: Luenberger Observer.

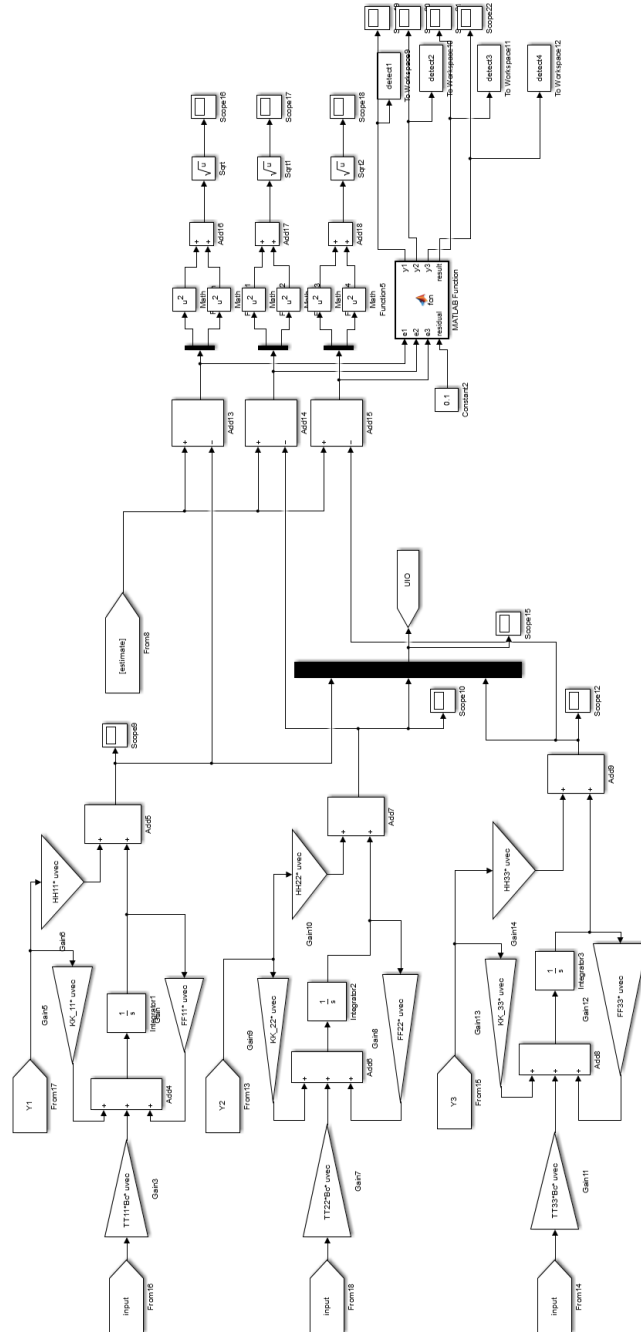


Figure A.4: Unknown Input Observer and Sensor Attack Diagnosis Method.

Bibliography

- [1] *Magnetic Levitation (MAGLEV) Manual*, Quanser Consulting, Markham, Canada, 1989.
- [2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, “Comprehensive experimental analyses of automotive attack surfaces,” *USENIX Security Symposium*, 2011.
- [3] J. Chen and R. J. Patton, *Robust model-based fault diagnosis for dynamic systems*. Springer Science & Business Media, 2012.
- [4] J. P. Farwell and R. Rohozinski, “Stuxnet and the future of cyber war,” *Survival*, no. 1, pp. 23–40, 2011.
- [5] H. Fawzi, P. Tabuada, and S. Diggavi, “Security for control systems under sensor and actuator attacks,” *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*, pp. 3412–3417, 2012.
- [6] —, “Secure estimation and control for cyber-physical systems under adversarial attacks,” *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014.
- [7] H. Jeon, S. Aum, H. Shim, and Y. Eun, “Resilient state estimation for control systems using multiple observers and median operation,” *Mathematical Problems in Engineering*, vol. 2016, 2016.
- [8] S. Karnouskos, “Stuxnet worm impact on industrial cyber-physical system security,” *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*, pp. 4490–4494, 2011.

-
- [9] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, “Experimental security analysis of a modern automobile,” *2010 IEEE Symposium on Security and Privacy*, pp. 447–462, 2010.
 - [10] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.
 - [11] C. Lee, H. Shim, and Y. Eun, “Secure and robust state estimation under sensor attacks, measurement noises, and process disturbances: observer-based combinatorial approach,” *Control Conference (ECC), 2015 European*, pp. 1872–1877, 2015.
 - [12] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.
 - [13] M. Naghnaeian, N. Hirzallah, and P. G. Voulgaris, “Dual rate control for security in cyber-physical systems,” *2015 54th IEEE Conference on Decision and Control (CDC)*, pp. 1415–1420, 2015.
 - [14] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, “Robustness of attack-resilient state estimators,” *ICCPS’14: ACM/IEEE 5th International Conference on Cyber-Physical Systems (with CPS Week 2014)*, pp. 163–174, 2014.
 - [15] F. Pasqualetti, F. Dörfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.
 - [16] D. Seo and Y. Eun, “Design of control systems resilient against sensor and actuator attacks using disturbance observer mechanism,” 2016.
 - [17] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, “Non-invasive spoofing attacks for anti-lock braking systems,” *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 55–72, 2013.
-

-
- [18] Y. Shoukry, P. Nuzzo, N. Bezzo, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, “Secure state reconstruction in differentially flat systems under sensor attacks using satisfiability modulo theory solving,” *2015 54th IEEE Conference on Decision and Control (CDC)*, pp. 3804–3809, 2015.
 - [19] A. Teixeira, J. Araújo, H. Sandberg, and K. H. Johansson, “Distributed actuator reconfiguration in networked control systems,” *IFAC Proceedings Volumes*, vol. 46, no. 27, pp. 61–68, 2013.
 - [20] A. Teixeira, H. Sandberg, and K. H. Johansson, “Networked control systems under cyber attacks with applications to power networks,” *Proceedings of the 2010 American control conference*, pp. 3690–3696, 2010.
 - [21] Y. Won, K. Choi, H. Jeon, and Y. Eun, “Attack-resilient control system design using multiple controllers and experimental validation with quadrotors,” 2015.
-

요약문

미지의 입력 관측기 기반의 복원성이 있는 제어 시스템 설계

제어시스템의 복원성은 시스템에 악의적인 공격이 가해지는 경우에도 원활히 동작할 수 있도록 하는 특성이다. 본 논문에서 센서와 액추에이터가 동시에 공격이 가해지는 상황을 고려하였다. 악의적인 공격하에도 제어시스템의 복원성 (Resiliency of Control Systems)을 높일 수 있는 제어기법을 제안하였다. 센서공격과 액추에이터 공격에 대응하기 위해서는 각각의 공격에 대한 대응 기법이 필요하다.

본 논문에서는 센서 공격 대응기법으로 복원성을 확보한 상태추정기법 (Resilient State Estimation Method)을 사용하였다. 기존의 상태추정기법을 본 논문에서 제안하는 상황에서 사용하는 경우, 액추에이터 공격으로 인해 상태추정오차가 발생하게 된다. 이러한 단점을 보완하는 미지의 입력 관측기 (Unknown Input Observer) 기반의 상태추정기법을 제안하였다. 미지의 입력 관측기를 사용하는 경우, 외란 및 액추에이터 공격으로부터 발생하는 영향에 대해서 추정오차가 발생하지 않게 된다. 이 외에도 센서에 공격이 가해지거나 고장이 나는 경우, 공격의 유무를 판별하거나 공격받거나 고장 난 센서를 검출할 수 있는 알고리즘을 제안하였다.

액추에이터 공격 대응기법으로 미지의 입력 관측기 기반의 상태추정기법을 사용해서 외란 및 액추에이터 공격에 대한 영향을 추정하고 보상해주는 방법을 제안하였다. 이 방법은 외란 및 액추에이터 공격의 저주파 영역에 한해서 추정 및 보상이 가능하다.

시뮬레이션과 실험을 통해 본 논문에서 제안하는 상황을 구현하였고, 제안하는 제어기법을 설계하고 기존의 방법과 비교를 통해 성능을 검증하였다.

주요어휘: 제어시스템의 복원성, 센서 공격, 액추에이터 공격, 복원성을 확보한 상태추정, 미지의 입력 관측기

