Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2016, Article ID 3750264, 9 pages
http://dx.doi.org/10.1155/2016/3750264

Research Article

Resilient State Estimation for Control Systems Using Multiple Observers and Median Operation

Heegyun Jeon,[1] Sungmin Aum,[1] Hyungbo Shim,[2] and Yongsoon Eun[1]

[1]*Department of Information and Communication Engineering, DGIST, Daegu 42988, Republic of Korea*
[2]*Department of Electrical and Computer Engineering, Seoul National University, Seoul 08826, Republic of Korea*

Correspondence should be addressed to Yongsoon Eun; yeun@dgist.ac.kr

Received 23 November 2015; Revised 22 January 2016; Accepted 27 January 2016

Academic Editor: Yan-Jun Liu

This paper addresses the problem of state estimation for linear dynamic systems that is resilient against malicious attacks on sensors. By "resiliency" we mean the capability of correctly estimating the state despite external attacks. We propose a state estimation with a bank of observers combined through median operations and show that the proposed method is resilient in the sense that estimated states asymptotically converge to the true state despite attacks on sensors. In addition, the effect of sensor noise and process disturbance is also considered. For bounded sensor noise and process disturbance, the proposed method eliminates the effect of attack and achieves state estimation error within a bound proportional to those of sensor noise and disturbance. While existing methods are computationally heavy because online solution of nonconvex optimization is needed, the proposed approach is computationally efficient by using median operation in the place of the optimization. It should be pointed out that the proposed method requires the system states being observable with every sensor, which is not a necessary condition for the existing methods. From resilient system design point of view, however, this fact may not be critical because sensors can be chosen for resiliency in the design stage. The gained computational efficiency helps real-time implementation in practice.

1. Introduction

Feedback control systems resilient against malicious attacks have received increasing attention in recent years [1–4]. This is because, combined with advances in computing and communications, feedback control systems now operate in a more connected manner with remotely located sensors, actuators, and other subsystems, which increase vulnerability of the systems compared to isolated ones in the past. The same trend is clearly seen in networked control systems [5, 6] and Cyber-Physical Systems [7, 8]. In particular, for applications to critical infrastructures of our society [9], such as power grid [10], public transportation, and nuclear facility, the consequence of malfunction due to attacks may be disastrous. Malicious attacks on control systems of trams, power grids, water distribution systems, and sewage plant have occurred in reality as reported in [11–13]. More potential attacks have been illustrated (see [1–4] and references therein for details).

In this paper, we develop a state estimation method for feedback control systems that is resilient against malicious attacks on sensors. Resilient state estimation is a method that can correctly estimate the true state of the system despite attacks on sensors. Such a method is sometimes referred to as secure state estimation.

The scenario considered here is the situation in which malicious attacks corrupt sensor outputs with the aim to degrade the control performance or fail the control systems. Such attacks, referred to as integrity attack [1], include the case where the sensors are physically destroyed and yielding false values or the case where the communication channels between sensors and controllers are compromised so that measurement values are intentionally altered. Altered sensor values can be arbitrary and no assumptions are made on their values or statistical properties.

Feedback systems under consideration are those with multiple sensors. First we consider the case where multiple sensors measure the same physical quantity redundantly and then we consider the case of multiple sensors measuring different physical quantities. The rationale is that the systems with multiple sensors can retain its functionality with a

properly designed state estimation mechanism, despite the fact that some sensors, not all, are compromised. We assume that compromising more sensors at once requires more effort and resource for the adversaries.

Our approach is based on Luenberger state observers. Specifically, for redundant sensors that measure the same physical quantity, sensor outputs are combined through a median operation, which then feed to a state observer to estimate the state. For multiple sensors that measure different physical quantities, multiple observers are constructed first, and states estimates are combined through element-wise median operations. Analyses are provided for conditions under which resilient state estimation is guaranteed. Additionally, experimental results on a magnetic levitation system are also given to illustrate the efficacy of the proposed approach.

State observers have been used previously to detect faults in the systems [14]. Most existing work designs an observer based scheme to generate residual signals that are used to detect faults. However, combining multiple state estimates using median operation in order to ensure resiliency has not been exploited to date.

Median operation has been used previously to ensure system tolerance to faults. For example, [15] designs a Guidance Navigation and Control (GNC) system where outputs from encoders, decoders, and data process units are combined through median operation to detect faults in the Data Processing Unit (DPU). Tripple Modular Redundancy (TMR) used in airline industry [16] executes voting based on AND-OR operation at logic level, which could be interpreted at selecting the median of the values from three computing units. However, it has not been used in the context of resilient state estimation where integrity attacks on the sensors are of the main concerns.

It should be acknowledged that seminal work of resilient state estimation is [17]. Formulated in discrete time linear systems setting, the method in [17] accumulates sensor outputs for multiple sampling periods, and process state estimation using techniques developed in compressed sensing literature [18, 19]. This work has been extended to systems with uncertainty, noise, and disturbance [20]. In [17], conditions for the correct estimation are given and an l_0 optimization problem is formulated. Since solving l_0 optimization online is computationally heavy (NP-hard), a relaxation condition on system parameters is given under which the solution of l_0 optimization is identical to a relaxed l_1 optimization. However, the relaxation condition narrows the class of the systems to which the method is applicable.

In an attempt to reduce computational effort, [21] approaches the problem of resilient state estimation using multiple observers. Contrast to the setting of [17, 20], [21] formulates the problem in continuous time linear dynamic systems setting and combines the estimates from multiple observers using the technique from compressed sensing. This method reduces l_0 optimization search space to a finite set leading to substantial reduction of computational effort from NP-hard to polynomial time. In addition, it is applicable to a large class of systems, compared to l_1 optimization method in [17], whose states are observable from the sensors.

Adaptive parameter estimation methods with various nonlinear elements [22, 23] may be used to solve resilient state estimation problem. When combining multiple observer outputs, especially, when each observes different number of states, adaptive fuzzy technique [24–29] can be utilized. These venues, however, have not yet been actively pursued.

The approach of current paper follows the setting of [21] and achieves computational complexity in the order of $\mathcal{O}(np)$ with n being the number of states and p being the number of sensors, under the assumption that the system states are observable from each sensor.

It should be pointed out that the proposed method requires the system states being observable with every sensor, which is not a necessary condition for the existing methods. From resilient system design point of view, however, this fact may not be critical because sensors can be chosen for resiliency in the design stage. On the other hand, the gained computational efficiency helps real-time implementation in practice.

The contributions of this paper are to propose multiple observers combined by median operation as a means to solve resilient state estimation problem and achive higher computational efficiency compared to existing methods for a class of systems.

The outline of this paper is as follows. The problem formulation is given in Section 2. Section 3 presents the main designs and analyses, and Section 4 provides experimental results. Comparison to existing methods is given in Section 4 as well in terms of applicability and computational effort. The conclusions are formulated in Section 5.

2. Problem Formulation

Consider a linear time invariant system given by

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + d(t), \\ y(t) &= Cx(t), \\ w(t) &= y(t) + a(t) + \xi(t), \end{aligned} \tag{1}$$

where $x \in R^n$ is the plant state, $u \in R^m$ is control, $y \in R^p$ is the plant output, $w \in R^p$ is the measurement for feedback control, $d \in R^n$ is process disturbance, $\xi \in R^p$ is sensor noise, and $a \in R^p$ is a vector that represents the altered output value by external malicious attack. The matrices A, B, and C are in appropriate dimensions. Let the matrix C be written by

$$C = \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_p \end{bmatrix}, \tag{2}$$

where each C_i for $i = 1, 2, \ldots, p$ is a row vector that corresponds to the ith output y_i of the output vector y. The ith sensor being under attack is described by ith element of the vector $a(t)$, denoted by $a_i(t)$, being nonzero, and the value

of $a_i(t)$ represents the amount of measurement altered by the external attack.

In order to denote the set of sensors under attack, we introduce the following notation. The support of the vector $a(t)$ is defined as

$$\text{supp}\,(a\,(t)) = \{i \mid a_i\,(t) \neq 0\}, \tag{3}$$

and the cardinality of the set $\text{supp}(a(t))$ is denoted by $|\text{supp}(a(t))|$. The elements in the set $\text{supp}(a(t))$ are the indices of the attacked sensors.

We now introduce assumptions for the system of (1).

Assumption 1. The set $\text{supp}(a(t))$ satisfies $2|\text{supp}(a(t))| < p$ for all t.

Assumption 1 states that strictly less than half of all the sensors in the system may be under integrity attack. This is a standard assumption for resilient state estimation [17, 21] and in fact a necessary and sufficient condition for resilient state estimation problem to be solvable. The rationale is that the adversaries who attack the sensors have limited resource only enough to compromise a subset of the sensors.

Assumption 2. The pair (C_i, A) is observable for $i = 1, 2, \ldots, p$.

This assumption ensures that a bank of p observers can be constructed. This assumption can be viewed as restrictive. However, from system design point of view, one can select sensors that satisfy Assumption 2.

Assumption 3. The vectors $d(t)$ and $\xi(t)$ satisfy $|d_i(t)| \leq d_{\max}$ for $i = 1, 2, \ldots, n$ and $|\xi_i(t)| \leq \xi_{\max}$ for $i = 1, 2, \ldots, p$.

Assumption 3 states that the process disturbance and measurement noise are bounded.

We now formulate the following design problems.

Problem 4. Let Assumptions 1 and 2 hold. Assume further that no process disturbance and measurement noise exist in the system; that is, $d(t) = 0$ and $\xi(t) = 0$. Furthermore, let $C_i = C_0$ for $i = 1, 2, \ldots, p$. Construct a state estimator for the system of (1) such that the estimated state denoted by $\widehat{x}(t)$ asymptotically converges to $x(t)$ despite $a(t) \neq 0$.

Problem 5. Let Assumptions 1 and 2 hold. Assume further that $d(t) = 0$ and $\xi(t) = 0$. Construct a state estimator for the system of (1) such that the estimated state denoted by $\widehat{x}(t)$ asymptotically converges to $x(t)$ despite $a(t) \neq 0$.

It should be pointed out that unknown input observers (see, e.g., [30]), which address the problem of estimating states correctly despite unknown disturbances, may appear similar to Problems 4 and 5. However, the framework deals with unknown input entering the state dynamics instead of output equation, which differentiates Problems 4 and 5 from the problem of unknown input observers.

Another aspect that differentiates Problems 4 and 5 from existing work is that we seek a method of asymptotic estimation formulated in continuous dynamics, while [17, 20] seek instantaneous estimation formulated in discrete dynamics.

The above formulated problems aim to achieve asymptotic state estimation and do not consider the effect of process disturbance and measurement noise. In practice, modeling errors, external process disturbance, and measurement noise exist. Hence, we formulate the following analysis problems.

Problem 6. Let Assumptions 1, 2, and 3 hold. Analyze the effect of disturbance and measurement noise on the system of (1) and the state estimator of Problem 4.

Problem 7. Let Assumptions 1, 2, and 3 hold. Analyze the effect of disturbance and measurement noise on the system of (1) and the state estimator of Problem 5.

Solutions to Problems 4–7 are given in Section 3.

3. Resilient State Estimation

3.1. Median Operation. First we define sample median operation. The sample median of p many values $w_1, w_2, \ldots, w_p$, denoted by $\text{med}(w_1, \ldots, w_p)$, is defined by the $((p+1)/2)$th largest value of $w_1, w_2, \ldots, w_p$ if p is odd and defined by the average of the $(p/2)$th and the $(p/2+1)$th largest values of $w_1, w_2, \ldots, w_p$ if p is even.

We now examine the property of median operation in the context of the system of (1). Suppose there are p measurements denoted by w_i with $i = 1, 2, \ldots, p$, each measuring the same value denoted by y_0. Let $w_i = y_0 + a_i$ and $a_i \neq 0$ for $i \in J$. We denote the cardinality of J by q; that is, $q = |J|$. Then, it is straightforward to notice that, as long as the number of measurements p is greater than twice the number of elements in J, or equivalent to say $2q < p$, the median value is equal to y_0; that is,

$$\text{med}\left(w_1, \ldots, w_p\right) = y_0. \tag{4}$$

Notice that the fact above holds regardless of the values of $a_i(t)$ as long as $2q < p$ at any given time. Note also that (4) holds even if the elements of J change in time. As an illustration, an example is given.

Example 8. Consider the case of $p = 5$. Assume that $y_0 = 2$, and $J = \{1, 3\}$. Accordingly, let $a(t)$ be $[3\ 0\ 5\ 0\ 0]^T$. Notice that $q = 2$ in this case and $2q < p$ is satisfied. Then, $w = [5\ 2\ 7\ 2\ 2]^T$ and $\text{med}(w_1, \ldots, w_5)$ is given by 2, which is equal to y_0. If $a(t) = [3\ 0\ 5\ 0\ 3]^T$, then, $q = 3$, and $2q > p$. This yields $w = [5\ 2\ 7\ 2\ 5]^T$ and $\text{med}(w_1, \ldots, w_5)$ is given by 5, which is not equal to y_0.

For the case when measurement noise exists, we have the following property for the median. Let w, y, ξ, and a be p-dimensional vectors. The vector y is of the form $y = y_0[1\ 1 \cdots 1]^T$ with $y_0 \in R$, the vector ξ represents noise, and as in Assumption 3, each element of the vector ξ is bounded by a constant $\xi_{\max}$; that is, $|\xi_i| \leq \xi_{\max}$, the vector $a(t)$ satisfies $|\text{supp}(a(t))| = q$ with $2q < p$, and let the vector w be given

by $w = y + \xi + a$. Then, we have the following for the sample median operation:

$$\left|\text{med}\left(w_1, \ldots, w_p\right) - y_0\right| \leq \xi_{\max}. \quad (5)$$

In words, this means when all the measurement is subject to bounded noise, sample median is also subject to noise, with the same bound as that for each element of the vector representing measurement noise. The derivation of (5) is in the appendix.

3.2. Design of Resilient State Observer. Now we propose a solution to Problem 4. Since all p sensors are measuring the same physical quantity, that is, $C_i = C_0$, for $1 \leq i \leq p$, we construct a Luenberger state observer in the following manner:

$$\dot{\widehat{x}} = A\widehat{x} + Bu + L\left(\text{med}\left(w_1, w_2, \ldots, w_p\right) - C_0\widehat{x}\right), \quad (6)$$

where the gain matrix L is chosen such that $A - LC_0$ is Hurwitz. Then it can be shown that, for the system of (1) with $d(t) = 0$ and $\xi(t) = 0$, the state observer (6) satisfies $\widehat{x}(t) \to x(t)$ as $t \to \infty$. In words, asymptotic state estimation is obtained by using (6). Specifically, since all the sensors measure the same output, we can denote this output by y_0 where $y_0 = C_0 x$. As explained earlier, under Assumption 1, $\text{med}(w_1, \ldots, w_p) = y_0$ is obtained. Also, due to Assumption 2, the matrix L can always be chosen to render $A - LC_0$ Hurwitz. This ensures the state estimate $\widehat{x}$ asymptotically converges to x.

Therefore, the state observer of (6) is a solution to Problem 4. It ensures asymptotic state estimation despite external attack $a(t)$ as long as the number of attacked sensors is less than half of all the sensors (Assumption 1). We emphasize that this solution is computationally very efficient as the computational complexity of median operation of p variables is given by $\mathcal{O}(p)$.

Next we consider the case where not all p sensors measure the same physical quantities. As given in Assumption 2, the system states are observable from each sensor. For each sensor output y_i, one can design a Luenberger type observer that estimates the state x asymptotically. The state estimate from ith sensor is denoted by $z^i \in R^n$ with a superscript i. Then, Assumption 2 allows design of the observer,

$$\dot{z}^i = Az^i + Bu + L_i\left(w_i - C_i z^i\right), \quad i = 1, 2, \ldots, p, \quad (7)$$

where L_i can be selected such that $(A - L_i C_i)$ is Hurwitz. By combining p state estimates $z^1, z^2, \ldots, z^p$ through median operation, we can obtain a state estimate

$$\widehat{x} = \left[\widehat{x}_1, \ldots, \widehat{x}_n\right]^T, \quad (8)$$

where

$$\widehat{x}_j = \text{med}\left(z_j^1, z_j^2, \ldots, z_j^p\right), \quad j = 1, 2, \ldots, n. \quad (9)$$

For the method in (7)–(9) to work, an additional assumption is needed.

Assumption 9. The set $\text{supp}(a(t))$ does not change over time.

The additional assumption is needed to avoid the case that attacks excite the transients response of each observer in (7) in a manner that prevents $\widehat{x}(t)$ from converging to $x(t)$. With Assumption 9, it can be shown that, for the system of (1) with $d(t) = 0$ and $\xi(t) = 0$, the state estimation method given by (7)–(9) achieves $\widehat{x}(t) \to x(t)$ as $t \to \infty$. This is possible because, under Assumption 1, more than half of p observers yield correct state estimates. Combining them through median would remove the effect of nonzero attack vector $a(t)$ and ensure asymptotic state estimate. Detailed derivation is given in the appendix. Therefore, the state estimation method of (7)–(9) for the system (1) provides a solution to Problem 5. Note that the additional computational effort for resiliency in this case is $\mathcal{O}(np)$, which is more scalable than NP-hard [17, 20], or polynomial time of [21].

3.3. Effect of Measurement Noise and Process Disturbance. Now we analyse the proposed state estimation method when measurement noise and process disturbances exist. In the presence of measurement noise and disturbance, asymptotic state estimation is generally not possible even without external attack. Hence, we focus on finding a bound on the estimation error. From a practical point of view, we deal with measurement noise and process disturbance that are bounded. Hence, Assumption 3 applies throughout this subsection.

First we consider the system of (1) with multiple sensors that measure the same physical quantity; that is, $C_i = C_0$ for $i = 1, 2, \ldots, p$. Then, it can be shown that there exist some positive constants μ and λ such that the state estimation given by (6) yields

$$\left\|\widehat{x}(t) - x(t)\right\|_2 \leq \mu\left\|\widehat{x}(0) - x(0)\right\|_2 e^{-\lambda t} + \frac{\mu\left(\|L\|_2\,\xi_{\max} + d_{\max}\right)}{\lambda}. \quad (10)$$

Note that inequality (10) implies that the estimation error is bounded when bounded noise as well as process disturbance is present. Note moreover that the first term in (10) diminishes as time goes and the bound on the remaining term in the error is proportional to the bounds of the measurement noise $\xi_{\max}$ and $d_{\max}$. This solves Problem 6 given in Section 2. The derivation of (10) is given in the appendix.

For the case with the sensors measuring different physical quantities, resilient state estimation is achieved by the method given in (7)–(9). When measurement noise and process disturbance exist, the method of (7)–(9) does not achieve asymptotic estimation. It turns out, however, that (10) holds for this case as well although the derivation now is more involved using p observers and element-wise median operation. Hence (10) solves Problem 7. The detailed derivation for this case is given in the appendix.

We would like to emphasize that the bound on estimation error does not depend on attack vector $a(t)$. Attack can be arbitrarily large, but the effect is eliminated by resilient state estimator construction, and the bound on error only depends

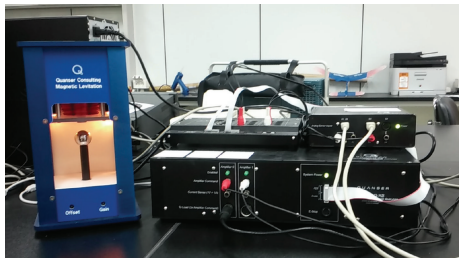

Figure 1: Magnetic levitation system.

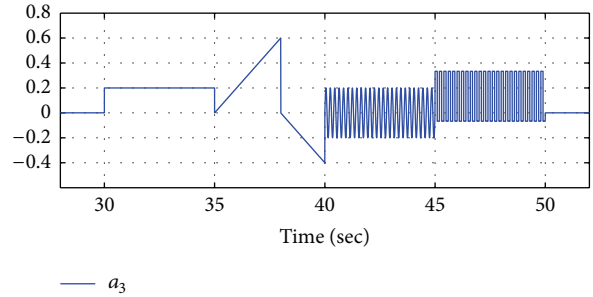

Figure 2: Attack signal on the third sensor.

on the initial error, the bound $d_{\max}$ of process disturbance, and the bound $\xi_{\max}$ for the measurement noise.

4. Experiment

4.1. Modeling. The proposed methods of resilient state estimation are experimentally validated using a magnetic leviation control system. Figure 1 shows the magnetic levitation system developed by Quanser for control education purpose. It consists of electromagnet, infrared ray position sensor, a steel ball, voltage amplifier, ADC converter, and data acquisition system connected to a PC using USB cable. A control algorithm is implemented using real-time workshop in Matlab/Simulink.

The system model is given by [31]

$$\begin{aligned} \dot{x}_1 &= x_2, \\ \dot{x}_2 &= g - \frac{K_m I^2}{M_b \left(x_1\right)^2}, \\ y &= x_1, \end{aligned} \tag{11}$$

where x_1 is the position of the ball, x_2 is the velocity of the ball, g is the gravitational constant, I is the current applied to the electromagnet, K_m is the electromagnet force constant, and M_b is the metal ball mass. Values for parameters K_m and M_b are specified in [31]. By linearizing the dynamics of (11) at the equilibrium point of $x_{\text{eq}} = [0.006\ 0]^T$ and $I_{\text{eq}} = 1$, the following linear model is obtained:

$$\begin{aligned} \Delta\dot{x} &= A\Delta x + B\Delta I \\ &= \begin{bmatrix} 0 & 1 \\ 3270 & 0 \end{bmatrix} \begin{bmatrix} \Delta x_1 \\ \Delta x_2 \end{bmatrix} + \begin{bmatrix} 0 \\ -26.67 \end{bmatrix} \Delta I, \end{aligned} \tag{12}$$

where Δ is used to indicate deviations from the equilibrium state x_{eq} and input I_{eq}.

Quanser magnetic levitation system has only one sensor that measures the position of the steel ball. In order to apply the proposed state estimation method, we virtually create in Matlab an additional position sensor and a velocity sensor. Then, the system output equation including attack can be written as

$$\begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix} = \begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} \begin{bmatrix} \Delta x_1 \\ \Delta x_2 \end{bmatrix} + \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}, \tag{13}$$

where $C_1 = [1\ 0]$, $C_2 = [1\ 0]$, and $C_3 = [0\ 1]$. It can be easily verified that the system of (12) and (13) satisfies Assumption 2.

4.2. Attack Scenario and State Estimation Results. We construct resilient state estimator given in (7)–(9). In the case of the magnetic levitation plant, the method yields three Luenberger observers as we have three sensors. Each observer dynamics is given by

$$\dot{z}^i = Az^i + B\Delta I + L_i \left(w_i - C_i z^i\right), \tag{14}$$

where $i = 1, 2, 3$ is the index for the ith sensor, z^i is the ith observer state, and w_i is the output of the ith sensor. The observer gain matrix L_i is selected such that $(A - L_i C_i)$ is Hurwitz for all $i = 1, 2, 3$. Specifically, the gains are $L_1 = [200\ 13271]^T$, $L_2 = [210\ 14299]^T$, and $L_3 = [4.0584\ 200]^T$, respectively. Then, $\Delta\widehat{x}$ is computed by

$$\begin{aligned} \Delta\widehat{x}_1 &= \text{med}\left(z_1^1, z_1^2, z_1^3\right), \\ \Delta\widehat{x}_2 &= \text{med}\left(z_2^1, z_2^2, z_2^3\right). \end{aligned} \tag{15}$$

Finally, the state estimate around the equilibrium is obtained by $\widehat{x} = \Delta\widehat{x} + x_{\text{eq}}$.

We consider the scenario where the velocity sensor, which provides the third measurement, is compromised by adversaries. The attack on the sensor, $a_3(t)$, consists of constant, ramp, sinusoid, and square waves as shown in Figure 2.

The estimated state $\widehat{x}$ and true state x are shown in Figure 3. As expected, $\widehat{x}$ is practically identical with x despite the attack on the velocity sensor. Slight mismatches between the two are due to modeling uncertainty which act as if they were disturbance.

For further investigation, Figure 4 shows state estimates z^1, z^2, and z^3 from the three observers. The effect of attack is clearly present in z^3. As shown by the analysis in Section 3,

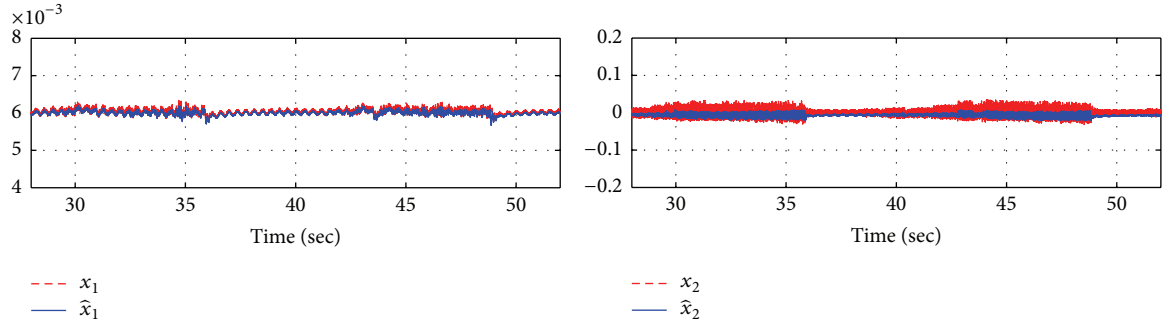

Figure 3: The estimated state and the true state.

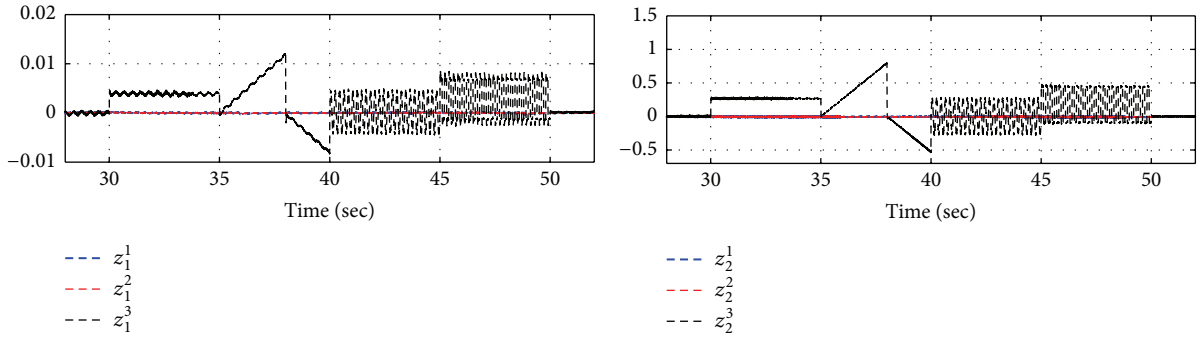

Figure 4: The states estimates from each Luenberger observer.

the element-wise median operation removes the effect of z^3 on $\widehat{x}$.

As illustrated by the above experiments, the proposed state estimation method is resilient against external attacks on the measurement.

4.3. Comparison with Existing Methods. Here we consider the method of [17] with the magnetic levitation system. It is difficult to apply the method of [17] on the magnetic levitation system for two reasons. First, the exact optimization using l_0 norm is computationally expensive (NP-hard) and no efficient method is known for l_0 optimization. Second, the relaxation condition in [17] for enabling l_1 convex optimization is *not satisfied* for the magnetic levitation system. Hence we do not implement and compare the method of [17] in the context of experiment with magnetic levitation.

The proposed method and that of [21] are compared in the following manner. From the above experiment, data from the sensors are stored. Then, two state estimation algorithms coded in Matlab m-file are executed on the stored sensor data, respectively. In this way, the execution times for the two algorithms alone (separated from the computation needed for control and communications) can be measured and compared.

We compared the two for the cases of 3, 5, 7, and 9 sensors. The cases of 5, 7, and 9 sensors use duplicated data from the first sensor for the sake of simplicity. The sensor data is collected over 58001 samples, and the time for 58001 executions of each algorithm is measured to obtain average value. Each Matlab code is executed on a computer with Intel i7-4790 CPU, 3.60 GHz clock speed, 32 GB RAM, and 64-bit Windows operating system. Both algorithms correctly estimate the true states despite attacks, although no plots are shown as our main interest here is the computational efficiency. Average execution time for the two algorithms is listed in Table 1.

Table 1: Computation time comparison between the proposed method and the method in [21].

Number of sensors	Proposed method	Method in [21]
3	0.06259 (msec)	0.1547 (msec)
5	0.08098 (msec)	0.5258 (msec)
7	0.01017 (msec)	2.115 (msec)
9	0.1196 (msec)	9.293 (msec)

Clearly, the proposed method is superior to the method in [21] in terms of computational effort, showing smaller computation time by orders of magnitude. We point out that method of [21] is superior to the proposed method in terms of applicability: the condition of systems states being observable from every sensor is not necessary for [21].

5. Conclusion

This paper addresses the problem of resilient state estimation against malicious attacks on the sensors. We propose a state estimation with a bank of observers combined through median operations. Then, we show that this method is resilient in the sense that state estimation converges to

the true state despite existence of attacks on sensors. For practical considerations, the effect of sensor noise and process disturbance on the proposed state estimation is analyzed.

We point out that the proposed method requires the system states being observable with every sensor, which is not required for the existing methods. This may not be a critical limitation because sensors can be chosen in the system design stage in applications where resiliency is of importance.

We emphasize that the proposed method is computationally efficient compared to existing methods in the literature, yielding the complexity of $\mathcal{O}(np)$ with n being the number of system states and p being the number of sensors. The gained computational efficiency helps real-time implementation for feedback systems in practice. Due to the simplicity of the state estimator structure and computational advantage over the existing method, the proposed method will benefit the design of resilient control systems.

Developing resilient state estimation methods using adaptive parameter estimation techniques is a future work.

Appendix

Derivation of Asymptotic State Estimate by (7)–(9). Denote the estimation error for each state observer corresponding to ith sensor by $\tilde{z}^i = z^i - x$. Then the estimation error dynamics for each observer can be written as

$$\dot{\tilde{z}}^i = \left(A - L_i C_i\right)\tilde{z}^i - L_i a_i, \tag{A.1}$$

the solution of which is given by

$$\tilde{z}^i(t) = e^{(A-L_iC_i)t}\tilde{z}^i(0) - \int_0^t e^{(A-L_iC_i)(t-\tau)} L_i a_i(\tau)\, d\tau. \tag{A.2}$$

Denote the two quantities in the right-hand side of (A.2) by $\bar{e}^i \in R^n$ and $\bar{a}^i \in R^n$, respectively:

$$\bar{e}^i(t) = e^{(A-L_iC_i)t}\tilde{z}^i(0), \tag{A.3}$$

$$\bar{a}^i(t) = -\int_0^t e^{(A-L_iC_i)(t-\tau)} L a_i(\tau)\, d\tau. \tag{A.4}$$

The vector $\bar{a}^i$ is nonzero only for $i \in \mathrm{supp}(a)$. Then, (9) is written as

$$\begin{aligned}\hat{x}_j = \mathrm{med}\Big(&x_j + \bar{e}_j^1 + \bar{a}_j^1, x_j + \bar{e}_j^2 + \bar{a}_j^2, \ldots, x_j + \bar{e}_j^p \\ &+ \bar{a}_j^p\Big), \quad j = 1, 2, \ldots, n.\end{aligned} \tag{A.5}$$

Now, Assumption 1 ensures less than half of $\bar{a}_j^1, \bar{a}_j^2, \bar{a}_j^3, \ldots, \bar{a}_j^p$ are nonzero in (A.5) for each $j = 1, 2, \ldots, n$. In addition, due to Assumption 2, $\bar{e}^i$ vanishes over time for all $j = 1, 2, \ldots, n$. This gives $\hat{x}_j \to x_j$ asymptotically for each $j = 1, 2, \ldots, n$, and as a whole $\hat{x} \to x$ is achieved.

Derivation of Inequality (5). We can write

$$\begin{aligned}&\mathrm{med}\left(w_1, \ldots, w_p\right) \\ &\quad = y_0 + \mathrm{med}\left(\xi_1 + a_1, \xi_2 + a_2, \ldots, \xi_p + a_p\right).\end{aligned} \tag{A.6}$$

Notice that there are at least $\lceil p/2 \rceil$ many measurements w_i's that are greater than or equal to the $\mathrm{med}(w_1, \ldots, w_p)$, and there are also at least $\lceil p/2 \rceil$ many measurements that are less than or equal to the $\mathrm{med}(w_1, \ldots, w_p)$.

Suppose p is even and $\mathrm{med}(w_1, \ldots, w_p) > y_0 + \xi_{\max}$. Assuming $|\xi_i| \le \xi_{\max}$, there are at most q measurements greater than or equal to $\mathrm{med}(w_1, \ldots, w_p)$. Since $\lceil p/2 \rceil > q$, this is a contradiction. Now suppose $\mathrm{med}(w_1, \ldots, w_p) < y_0 - \xi_{\max}$, there are also at most q elements less than or equal to $\mathrm{med}(w_1, \ldots, w_p)$, and this is also a contradiction for the same reason.

When p is odd, contradictions can be shown in a similar manner using $(p+1)/2 \ge \lceil p/2 \rceil$.

Derivation of Inequality (10). The state estimate is written as

$$\dot{\hat{x}} = A\hat{x} + Bu + L\left(\mathrm{med}\left(w_1, w_2, \ldots, w_p\right) - C_0\hat{x}\right), \tag{A.7}$$

which is equivalent to

$$\dot{\hat{x}} = A\hat{x} + Bu + L\left(y_0 + \eta - C_0\hat{x}\right), \tag{A.8}$$

where $\eta = \mathrm{med}(w_1, w_2, \ldots, w_p) - y_0$ and $|\eta| \le \xi_{\max}$ by Assumption 1 and (5). Denote $x(t) - \hat{x}(t)$ by $\tilde{x}(t)$; then the state estimation error dynamics could be written as

$$\dot{\tilde{x}}(t) = \left(A - LC_0\right)\tilde{x}(t) + d(t) - L\eta(t), \tag{A.9}$$

and the solution of which is

$$\begin{aligned}\tilde{x}(t) = &\, e^{(A-LC_0)t}\tilde{x}_0 \\ &+ \int_0^t e^{(A-LC_0)(t-\tau)}\left(d(\tau) - L\eta(\tau)\right) d\tau.\end{aligned} \tag{A.10}$$

Taking the norms on both sides of (A.10),

$$\begin{aligned}\|\tilde{x}(t)\|_2 &= \left\| e^{(A-LC_0)t}\tilde{x}_0 \right. \\ &\quad \left. + \int_0^t e^{(A-LC_0)(t-\tau)}\left(d(\tau) - L\eta(\tau)\right) d\tau \right\|_2 \\ &\le \left\| e^{(A-LC_0)t}\tilde{x}_0 \right\|_2 \\ &\quad + \left\| \int_0^t e^{(A-LC_0)(t-\tau)}\left(d(\tau) - L\eta(\tau)\right) d\tau \right\|_2 \\ &\le \left\| e^{(A-LC_0)t}\tilde{x}_0 \right\|_2 \\ &\quad + \int_0^t \left\| e^{(A-LC_0)(t-\tau)} \right\|_2 \left\| \left(d(\tau) - L\eta(\tau)\right) \right\|_2 d\tau.\end{aligned} \tag{A.11}$$

By Assumption 3,

$$\begin{aligned}&\|\tilde{x}(t)\|_2 \\ &\le \left\| e^{(A-LC_0)t} \right\|_2 \|\tilde{x}_0\|_2 \\ &\quad + \left(\|L\|_2 \xi_{\max} + \xi^{1/2} d_{\max}\right) \int_0^t \left\| e^{(A-LC_0)(\tau)} \right\|_2 d\tau.\end{aligned} \tag{A.12}$$

Since $(A - LC_0)$ is Hurwitz, there exist positive constants ν and λ such that $\|e^{(A-LC)t}\|_2 \le \nu e^{-\lambda t}$ for all $t \ge 0$. Therefore,

$$\begin{aligned}\|\widetilde{x}(t)\|_2 &\le \nu e^{-\lambda t}\left\|\widetilde{x}_0\right\|_2 \\ &\quad + \left(\|L\|_2 \xi_{\max} + \xi^{1/2} d_{\max}\right)\int_0^t \nu e^{-\lambda(\tau)} d\tau.\end{aligned} \tag{A.13}$$

Let $\mu > \xi^{1/2}\nu$. Then (A.13) also satisfies

$$\begin{aligned}\|\widetilde{x}(t)\|_2 &\le \mu e^{-\lambda t}\left\|\widetilde{x}_0\right\|_2 \\ &\quad + \left(\|L\|_2 \xi_{\max} + d_{\max}\right)\mu\left(\frac{1}{\lambda}\right)\left(1 - e^{-\lambda t}\right) \\ &\le \mu e^{-\lambda t}\left\|\widetilde{x}_0\right\|_2 + \left(\|L\|_2 \xi_{\max} + d_{\max}\right)\mu\left(\frac{1}{\lambda}\right).\end{aligned} \tag{A.14}$$

This completes the proof.

Derivation of Inequality (10) for the Case of $C_i \ne C_j$ for Some i and j. Let z^i be the state estimates from the ith sensor. Denote the estimation error dynamics for ith observer as $\widetilde{z}^i = x - z^i$; then

$$\dot{\widetilde{z}}^i = \left(A - L_i C_i\right)\widetilde{z}^i - L_i a_i - L_i \xi_i + d, \tag{A.15}$$

and the solution of which is given by

$$\begin{aligned}&\widetilde{z}^i(t) \\ &= e^{(A-L_iC_i)t}\widetilde{z}^i(0) \\ &\quad + \int_0^t e^{(A-L_iC_i)(t-\tau)}\left(-La_i(\tau) - L\xi_i(\tau) + d(\tau)\right)d\tau \\ &= e^{(A-L_iC_i)t}\widetilde{z}^i(0) - \int_0^t e^{(A-L_iC_i)(t-\tau)}\left(La_i(\tau)\right)d\tau \\ &\quad - \int_0^t e^{(A-L_iC_i)(t-\tau)}\left(L\xi_i(\tau)\right)d\tau \\ &\quad + \int_0^t e^{(A-L_iC_i)(t-\tau)} d(\tau)\, d\tau.\end{aligned} \tag{A.16}$$

Denote each quantity in the right-hand side of (A.16) by $\overline{e}^i \in R^n$, $\overline{a}^i \in R^n$, $\overline{\xi}^i \in R^n$, and $\overline{d}^i \in R^n$, respectively:

$$\overline{e}^i(t) = e^{(A-L_iC_i)t}\widetilde{z}^i(0), \tag{A.17}$$

$$\overline{a}^i(t) = -\int_0^t e^{(A-L_iC_i)(t-\tau)} La_i(\tau)\, d\tau, \tag{A.18}$$

$$\overline{\xi}^i(t) = -\int_0^t e^{(A-L_iC_i)(t-\tau)} L\xi_i(\tau)\, d\tau, \tag{A.19}$$

$$\overline{d}^i(t) = \int_0^t e^{(A-L_iC_i)(t-\tau)} d(\tau)\, d\tau. \tag{A.20}$$

Then (9) can be written as

$$\begin{aligned}\widehat{x}_j = \operatorname{med}\Big(&x_j + \overline{e}_j^1 + \overline{a}_j^1 + \overline{\xi}_j^1 + \overline{d}_j^1, \ldots, x_j + \overline{e}_j^p + \overline{a}_j^p \\ &+ \overline{\xi}_j^p + \overline{d}_j^p\Big), \quad j = 1, \ldots, n,\end{aligned} \tag{A.21}$$

where x_j, $\overline{e}_j^i$, $\overline{a}_j^i$, $\overline{\xi}_j^i$, and $\overline{d}_j^i$ are the jth components of x, $\overline{e}^i$, $\overline{a}^i$, $\overline{\xi}^i$, and $\overline{d}^i$.

Without the loss of generality, we may assume $z^i(0) = \widehat{x}(0)$, $i = 1, \ldots, p$. Since $(A - L_iC_i)$ is Hurwitz $\forall i = 1, \ldots, p$, under Assumptions 1, 2, 3, and 9, it can be seen from the derivation of (10) that $\|\overline{e}^i(t)\|_2$, $\|\overline{\xi}^i(t)\|_2$, and $\|\overline{d}^i(t)\|_2$, $i = 1, \ldots, p$, are bounded as

$$\begin{aligned}\left\|\overline{e}^i(t)\right\|_2 &\le \nu_e \|\widehat{x}(0) - x(0)\|_2 e^{-\lambda_e t}, \\ \left\|\overline{\xi}^i(t)\right\|_2 &\le \frac{\nu_n \|L\|_2 \xi_{\max}}{\lambda_n}, \\ \left\|\overline{d}^i(t)\right\|_2 &\le \frac{\nu_d \xi d_{\max}}{\lambda_d},\end{aligned} \tag{A.22}$$

for some constants $\nu_e, \nu_n, \nu_d > 0$ and $\lambda_e, \lambda_n, \lambda_d > 0$.

Since $\overline{e}_j^i$, $\overline{\xi}_j^i$, and $\overline{d}_j^i$ are components of $\overline{e}^i$, $\overline{\xi}^i$, and $\overline{d}^i$, $|\overline{e}_j^i| \le \|\overline{e}^i(t)\|_2$, $|\overline{\xi}_j^i| \le \|\overline{\xi}^i(t)\|_2$, and $|\overline{d}_j^i| \le \|\overline{d}^i(t)\|_2$. Let $\overline{\eta}_j^i = \overline{e}_j^i + \overline{\xi}_j^i + \overline{d}_j^i$ $i = 1, \ldots, p$, $j = 1, \ldots, n$. Then, (A.21) can be written as

$$\widehat{x}_j = \operatorname{med}\left(x_j + \overline{\eta}_j^1 + \overline{a}_j^1, \ldots, x_j + \overline{\eta}_j^p + \overline{a}_j^p\right), \tag{A.23}$$

and by (5), $|\widehat{x}_j - x_j| \le \max(|\eta_j^i|)$, $i = 1, \ldots, p$. Since $\max(|\overline{\eta}_j^i|)$ is bounded above as

$$\begin{aligned}\operatorname{med}\left(\left|\overline{u}_j^i\right|\right) &= \max\left|\overline{e}_j^i + \overline{\xi}_j^i + \overline{d}_j\right| \\ &\qquad i = 1, \ldots, p, \;\; j = 1, \ldots, n \\ &\le \max\left(\left|\overline{e}_j^i\right|\right) + \max\left(\left|\overline{\xi}_j^i\right|\right) \\ &\quad + \max\left(\left|\overline{d}_j\right|\right),\end{aligned} \tag{A.24}$$

we see that

$$\begin{aligned}\|\widehat{x}(t) - x(t)\|_2 &\le \xi^{1/2}\max\left(\left|\widehat{x}_j - x_j\right|,\;\; j = 1, \ldots, n\right) \\ &\le \xi^{1/2}\left(\max\left(\left|\overline{e}_j^i\right|\right) + \operatorname{med}\left(\left|\overline{\xi}_j^i\right|\right) + \max\left(\left|\overline{d}_j\right|\right)\right) \\ &\le \xi^{1/2}\left(\nu_e \|\widehat{x}(0) - x(0)\|_2 e^{-\lambda_e t} + \frac{\nu_n \|L\|_2 \xi_{\max}}{\lambda_n}\right. \\ &\quad \left. + \frac{\nu_d \xi d_{\max}}{\lambda_d}\right).\end{aligned} \tag{A.25}$$

Choose $\mu > \xi^{1/2}\max(\nu_e, \nu_n, \nu_d)$ and $0 < \lambda < \min(\lambda_e, \lambda_n, \lambda_d)$; we have

$$\begin{aligned}\|\widehat{x}(t) - x(t)\|_2 &\le \mu \|\widehat{x}(0) - x(0)\|_2 e^{-\lambda t} \\ &\quad + \frac{\mu\left(\|L\|_2 \xi_{\max} + d_{\max}\right)}{\lambda}.\end{aligned} \tag{A.26}$$

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was partially supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF-2013058304), funded by the Ministry of Education, and also supported by Institute for Information and Communications Technology Promotion grant funded by the Korea government (no. B0101-15-0557, Resilient Cyber-Physical Systems Research).

References

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

[2] A. A. Cardenas, T. Roosta, and S. Sastry, "Rethinking security properties, threat models, and the design space in sensor networks: a case study in SCADA systems," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1434–1447, 2009.

[3] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry, "Understanding the physical and economic consequences of attacks on control systems," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 3, pp. 73–83, 2009.

[4] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure control systems: a quantitative risk management approach," *IEEE Control Systems*, vol. 35, no. 1, pp. 24–45, 2015.

[5] K. Ji and D. Wei, "Resilient control for wireless networked control systems," *International Journal of Control, Automation, and Systems*, vol. 9, no. 2, pp. 285–293, 2011.

[6] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Distributed fault detection and isolation resilient to network model uncertainties," *IEEE Transactions on Cybernetics*, vol. 44, no. 11, pp. 2024–2037, 2014.

[7] T. Vollmer and M. Manic, "Cyber-physical system security with deceptive virtual hosts for industrial control networks," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1337–1347, 2014.

[8] Q. Chang, R. Gao, Y. Lei, L. Wang, and C. Wu, "Cyber-physical systems in manufacturing and service systems," *Mathematical Problems in Engineering*, vol. 2015, Article ID 704213, 2 pages, 2015.

[9] A. M. Grilo, J. Chen, M. Diaz, D. Garrido, and A. Casaca, "An Integrated WSAN and SCADA System for Monitoring a Critical Infrastructure," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 3, pp. 1755–1764, 2014.

[10] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proceedings of the 49th IEEE Conference on Decision and Control (CDC '10)*, pp. 5991–5998, IEEE, Atlanta, Ga, USA, December 2010.

[11] J. Slay and M. Miller, *Critical Infrastructure Protection*, Springer, Manhattan, NY, USA, 2008.

[12] Forbes, "Hackers Cut Cities' Power," 2008, http://www.forbes.com.

[13] The Register, *Polish Teen Derails Tram after Hacking Train Network*, 2008, http://www.theregister.co.uk.

[14] D. Henry and A. Zolghadri, "Design and analysis of robust residual generators for systems under feedback control," *Automatica*, vol. 41, no. 2, pp. 251–264, 2005.

[15] S. Fan, Y. Gao, Y. Lin, and L. Wan, "Formal analysis of a fault tolerant GNC system architecture," in *Proceedings of the 4th International Conference on Intelligent Control and Information Processing (ICICIP '13)*, pp. 736–743, Beijing, China, June 2013.

[16] J. H. Wensley, L. Lamport, J. Goldberg et al., "SIFT: design and analysis of a fault-tolerant computer for aircraft control," *Proceedings of the IEEE*, vol. 66, no. 10, pp. 1240–1255, 1978.

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

[18] D. L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[19] S. Li, L. D. Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and internet of things," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 4, pp. 2177–2186, 2013.

[20] M. Pajic, J. Weimer, N. Bezzo et al., "Robustness of attack-resilient state estimators," in *Proceedings of the 5th IEEE/ACM International Conference on Cyber-Physical Systems (ICCPS '14)*, pp. 163–174, Berlin, Germany, April 2014.

[21] C. Lee, H. Shim, and Y. Eun, "Secure and robust state estimation under sensor attacks, measurement noises, and process disturbances: observer-based combinatorial approach," in *Proceedings of the European Control Conference (ECC '15)*, pp. 1872–1877, Linz, Austria, July 2015.

[22] Y.-J. Liu and S. Tong, "Adaptive NN tracking control of uncertain nonlinear discrete-time systems with nonaffine dead-zone input," *IEEE Transactions on Cybernetics*, vol. 45, no. 3, pp. 497–505, 2015.

[23] Y.-J. Liu, L. Tang, S. Tong, and C. L. P. Chen, "Adaptive NN controller design for a class of nonlinear MIMO discrete-time systems," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 25, no. 5, pp. 1007–1018, 2015.

[24] Y.-J. Liu and S. Tong, "Adaptive fuzzy control for a class of nonlinear discrete-time systems with backlash," *IEEE Transactions on Fuzzy Systems*, vol. 22, no. 5, pp. 1359–1365, 2014.

[25] Y.-J. Liu and S. Tong, "Adaptive fuzzy control for a class of unknown nonlinear dynamical systems," *Fuzzy Sets and Systems*, vol. 263, pp. 49–70, 2015.

[26] Y. Liu and S. Tong, "Adaptive fuzzy identification and control for a class of nonlinear pure-feedback MIMO systems with unknown dead zones," *IEEE Transactions on Fuzzy Systems*, vol. 23, pp. 1387–1398, 2015.

[27] J. Wu, W. Chen, and J. Li, "Fuzzy-approximation-based global adaptive control for uncertain strict-feedback systems with a priori known tracking accuracy," *Fuzzy Sets and Systems*, vol. 273, pp. 1–25, 2015.

[28] J. Wu, W. Chen, F. Yang, J. Li, and Q. Zhu, "Global adaptive neural control for strict-feedback time-delay systems with predefined output accuracy," *Information Sciences*, vol. 301, pp. 27–43, 2015.

[29] Y. X. Li and G. H. Yang, "Fuzzy adaptive output feedback fault-tolerant tracking control of a class of uncertain nonlinear systems with non-affine nonlinear faults," *IEEE Transactions on Fuzzy Systems*, vol. 24, no. 1, pp. 223–234, 2015.

[30] J. Chen, R. J. Patton, and H.-Y. Zhang, "Design of unknown input observers and robust fault detection filters," *International Journal of Control*, vol. 63, no. 1, pp. 85–105, 1996.

[31] *Magnetic Levitation (MAGLEV) Manual*, Quanser Consulting, Markham, Canada, 1989.