Reach Set-Based Secure State Estimation against Sensor Attacks with Interval Hull Approximation

Takumi SHINOHARA * and Toru NAMERIKAWA **

Abstract: This paper deals with the problem of secure state estimation in an adversarial environment with the presence of bounded noises. The problem is given as min-max optimization, that is, the system operator seeks an optimal estimate which minimizes the worst-case estimation error due to the manipulation by the attacker. To derive the optimal estimate, taking the reach set of the system into account, we first show that the feasible set of the state can be represented as a union of polytopes, and the optimal estimate is given as the Chebyshev center of the union. Then, for calculating the optimal state estimate, we provide a convex optimization problem that utilizes the vertices of the union. On the proposed estimator, the estimation error is bounded even if the adversary corrupts any subset of sensors. For the sake of reducing the calculation complexity, we further provide another estimator which resorts to the interval hull approximation of the reach set and properties of zonotopes. This approximated estimator is able to reduce the complexity without degrading the estimation accuracy sorely. Numerical comparisons and examples finally illustrate the effectiveness of the proposed estimators.

Key Words: cyber-physical systems, system security, attack-resilient control, polytopes.

1. Introduction

From the viewpoints of increasing the efficiency of social systems, creating new industries, and improving productivity, cyber-physical systems (CPS) have attracted much attention in recent years. Many systems such as transportation, manufacturing, medical devices, and energy systems are considered as CPS [1], [2], and each includes networked systems embedded sensors, actuators, and computation that sense and interact with the physical world. Most of these systems are safety-critical, and thus if these are attacked and malfunctioning, serious harms can be caused to the physical entities. In fact, there exist several reports on cyber attacks targeting control systems, which carried significant damage to the physical plants, for instance, the Stuxnet incident [3], the Maroochy water breach [4], and recently, Ukrainian CyberAttacks [5]. CPS are particularly difficult to secure due to a number of factors, e.g., the ability of a malicious third party to operate from anywhere in the world, the tight linkages between the cyber space and physical systems, and the difficulty of reducing vulnerabilities in complex networks. From a cyber security perspective, the attacks may be avoided with the use of standard cryptographic techniques that guarantee data integrity and authentication. From a cyber-physical security perspective, however, the encryption of networks does not always guarantee the secure control of CPS as reported in [6], [7]. Accordingly, considering the cyber threat scenarios and strengthening security and resilience of CPS are a critical issue for the secure operations.

One challenge to a secure operation of CPS is identifying the vulnerabilities due to malicious attacks and developing countermeasures against them [8]–[12]. To be honest, however, while IoT (Internet of Things) devices have increased, cyber incidents are also increasing, and it is generally difficult to ensure the security of all sensors or devices. Additionally, in safety-critical systems, it is also difficult to immediately stop the operation even if they are subject to malicious attacks. Thus, one another challenge is to operate CPS securely even if in the presence of malicious attacks.

To this end, it is necessary to estimate the system state from the corrupted sensor measurement, and this problem is referred as a secure state estimation problem. The paper [13] is pioneering work of this problem, and the authors derived necessary and sufficient conditions for the feasible estimation and control and also provided an efficient state reconstruction algorithm based on $l_0$ optimization. Same research group further refined this work adopting an event-triggered approach [14]. Chong et al. derived a new concept of the observability in the presence of malicious attacks [15]. However, they only considered the case where the system is assumed to be noiseless, which greatly favors system supervisors since the evolution of the system is deterministic. In [16]–[18], the authors, therefore, extended the problem into a more realistic case where the system contains noises. They proved that the state can be estimated using a finite history of the sensor measurements if the system is observable after the removal of an arbitrary set of $l$ sensors, where $l$ is the number of the compromised sensors. Nakahira and Mo relaxed the condition, namely they showed that if the system is detectable after removing an arbitrary set of $l$ sensors, then the system can be inferred by using all sensor data from time $0$ [19].

In this paper, we focus on the secure estimation problem for linear systems in noisy environments. Our goal is to construct a resilient estimator whose estimation error is always bounded, whatever the adversary compromises any subset of sensors. To this end, we consider an estimator which minimizes the worst-
case error due to malicious injections. Taking the reach set of the system into account, the feasible set of the state contained in the set is computed by the compromised measurement. In essence, the feasible set is given as a union of polytopes and the state estimate which minimize the worst-case error is equal to the Chebyshev center (i.e., the center of the minimum volume circumscribing ball) of the set. Then, we show the bound of the worst-case estimation error. In conventional studies [16]–[19], as aforementioned, the estimation error is possibly unbounded unless the system is observable or detectable after removing any subset of $2^7$ sensors. In contrast, the proposed estimator can construct the state estimate and its estimation error is always bounded even if the system does not satisfy the above condition. We further provide a computational complexity-aware estimator utilizing the interval hull approximation of the reach set. We show that this approximated algorithm is able to harness the computational complexity and, under a certain condition, the worst-case error does not affect even using this approximation.

The rest of this paper is organized as follows: Section 2 gives some important definitions and properties of polytopes and zonotopes which are necessary for the subsequent analysis. In Section 3, we formulate the secure state estimation problem and the resilient estimator minimizing the worst-case error due to malicious injections. Section 4 is devoted to designing the estimator, and the estimation bound of the estimator is derived as well. For reducing the computational cost, an estimator leveraging the interval hull of the reach set is further provided. For reducing the computational cost, an estimator utilizing the interval hull approximation of the reach set. We further provide a computational complexity-aware estimator, and the estimation bound of the estimator is derived. Even using this approximation.

2. Preliminaries for Polytopes and Zonotopes

A convex polyhedron in $\mathcal{R}^n$ is defined as $P = \{x \in \mathcal{R}^n : Ax \leq b\}$ for some matrix $A \in \mathcal{R}^{m \times n}$ and vector $b \in \mathcal{R}^m$, while a bounded convex polyhedron is defined as $P$. A polytope can be interpreted as an intersection of a finite number of hyperplanes, and such definition is called an $\mathcal{H}$-polytope or $\mathcal{H}$-representation. By contrast, a polytope may also be defined as a convex hull of a finite set of points, and such definition is called an $\mathcal{V}$-polytope or $\mathcal{V}$-representation. The mathematical equivalence between each represented polytope can be proved by the Minkowski-Weyl theorem. For details, please refer to [20]. Figure 1 shows examples of an $\mathcal{H}$-polytope and a $\mathcal{V}$-polytope.

Zonotopes are a special class of convex polytopes. In tradition, a zonotope is defined as the image of a cube under an affine projection, or equivalently, the Minkowski sum of finite hyperplanes, and such definition is called an $\mathcal{H}$-polytope or $\mathcal{H}$-representation. The mathematical equivalence between each represented polytope can be proved by the Minkowski-Weyl theorem. For details, please refer to [20]. Figure 1 shows examples of an $\mathcal{H}$-polytope and a $\mathcal{V}$-polytope.

![Fig. 1 Pictorial examples illustrating an $\mathcal{H}$-polytope and a $\mathcal{V}$-polytope.](image1)

$Z = \{x \in \mathcal{R}^n : x = c + \sum_{j=1}^{p} \alpha_j g_j, -1 \leq \alpha_j \leq 1\}$.

(2)

where $c \in \mathcal{R}^n$ is the Chebyshev center (which is defined later) and $\{g_1, \ldots, g_p\} \subset \mathcal{R}^n$ is called a set of generators of the zonotope. For a zonotope with $p$ generators in $\mathcal{R}^n$, the value of $p/n$ is called the order of the zonotope. Setting a matrix $G \triangleq \{g_1, \ldots, g_p\}$ which collects all generators, a zonotope has another definition as follows:

$Z = \{x \in \mathcal{R}^n : x = c + GB, \|B\|_{\infty} \leq 1\}$.

(3)

In what follows, we use notations $[c; \{g_1, \ldots, g_p\}]_Z$ and $[c; G]_Z$ to indicate zonotopes which are defined as (2) and (3), respectively. Figure 2 shows examples of a polyhedron, a polytope, and a zonotope.

It is well known that zonotopes have several properties [20]–[22]:

![Fig. 2 Pictorial examples illustrating a polyhedron, a polytope, and a zonotope.](image2)

In this paper, we slightly abuse the notation and use $x \oplus W$ instead of $\{x\} \oplus W$ for the Minkowski sum of a vector $x$ and a set $W$.

1 In this paper, we slightly abuse the notation and use $x \oplus W$ instead of $\{x\} \oplus W$ for the Minkowski sum of a vector $x$ and a set $W$. 

Notation and Terminology

Let us define $\mathcal{R}, \mathcal{R}^n$, and $\mathcal{N}_0$ as the sets of real numbers, positive real numbers, and nonnegative integers, respectively. We use $\mathbf{1}_n$ to indicate the $n$-dimensional column vector whose entries are 1. For a vector $x \in \mathcal{R}^n$, let $\|x\|$ and $\|x\|_\infty$ be the Euclidean norm and the infinity norm of the vector, respectively. For a matrix $A \in \mathcal{R}^{m \times n}$, the spectral radius and spectrum norm of the matrix are, respectively, denoted by $\rho(A)$ and $\|A\|$. Moreover, we denote by $A_{i,\cdot}$ the $i$th row of $A$, for $i \in \{1, \ldots, m\}$. Again, for a vector $x \in \mathcal{R}^n$ and a matrix $A \in \mathcal{R}^{m \times n}$, we denote by $\|x\|_A$ and $\|A\|_\infty$ the vector and matrix whose elements are absolute values of $x$ and $A$, respectively. For two vectors $x$ and $y$ with the same dimension, by $x \leq y$, we specify that $x$ is element-wise less than or equal to $y$.

Let $B(c, r) \equiv \{x \in \mathcal{R}^n : \|x - c\| \leq r\} \subset \mathcal{R}^n$ be a closed ball whose center and radius are, respectively, $c \in \mathcal{R}^n$ and $r \in \mathcal{R}^n$. Setting $c = -b/y$ and $r = 1/y$ for $b \in \mathcal{R}^n$ and $y \in \mathcal{R}^+$, another common representation of the ball is given by

$B(-b/y, 1/y) = \{x \in \mathcal{R}^n : \|yx + b\| \leq 1\} \subset \mathcal{R}^n$.

(1)

For a set $\mathcal{S}$, $|\mathcal{S}|$ denotes the cardinality of the set. Given two sets $\mathcal{V}$ and $W$ such that $\mathcal{V} \subset \mathcal{R}^n$ and $W \subset \mathcal{R}^n$, the Minkowski sum is defined by $\mathcal{V} \oplus W \triangleq \{v + w : v \in \mathcal{V}, w \in W\}$. Finally, for a vector $x \in \mathcal{R}^n$, the support of the vector is

$\text{supp}(x) = \{i : x_i \neq 0\} \subseteq \{1, \ldots, n\}$.
Property 1 Any zonotope is a centrally symmetric set.

Property 2 A zonotope in $\mathbb{R}^n$ whose order is $m$ has more than $(2m)^{n-1}/\sqrt{n}$ vertices.

Property 3 Let $v$ be a vertex of a zonotope $Z = \{c, G\}$. Then, the vertex $v$ satisfies

$$v = c + G e_i \in [e_1, \ldots, e_p]^T, \ e_i = 1 \ or \ -1,$$

but, in general, not vice versa, i.e., not all points of this form are vertices of the zonotope $Z$.

Property 4 Zonotopes are closed under linear transformation. Let $L$ be a linear map. An image of a zonotope by the linear map can be computed as

$$LZ = \left[ Lc, [Lg_1, \ldots, Lg_p]\right]_Z,$$

which indicates that it can be computed in linear time with regard to the order of the zonotope.

Property 5 Zonotopes are closed under Minkowski sum. Consider two zonotopes $Z_1 = \{c_1, g_1, \ldots, g_p\}_Z$ and $Z_2 = \{c_2, h_1, \ldots, h_q\}_Z$. The Minkowski sum of these zonotopes can be computed as

$$Z_1 \oplus Z_2 = \{c_1 + c_2, g_1, \ldots, g_p, h_1, \ldots, h_q\}_Z,$$

which indicates that it can be computed by the concatenation of two lists.

According to Properties 4 and 5, thus, zonotopes can harness their computational complexity than usual polytopes.

3. Problem Formulation

Consider the state estimation problem for the following linear time-invariant system subjected to integrity attacks [16]–[19]:

$$x(k+1) = Ax(k) + Bu(k) + w(k), \quad x(0) \in X_0, \quad (4)$$

$$y(k) = Cx(k) + u(k) + y^a(k), \quad (5)$$

where $x(k) \in \mathbb{R}^n$ is the state system, $u(k) \in \mathbb{R}^d$ is the control input, and $y(k) \in \mathbb{R}^m$ is the compromised sensor measurement at time $k$, where $y_i(k)$ indicates the measurement from $i$th sensor. Assume that the initial state set $X_0$ is given as a zonotope. Without loss of generality, assume that its Chebyshev center is $0$, and denote its generators matrix by $G_0 \in \mathbb{R}^{m \times p}$. Let us define the sensor index set as $S \subseteq \{1, \ldots, m\}$. The vectors $w(k) \in \mathbb{R}^n$ and $v(k) \in \mathbb{R}^m$ represent the process and measurement noise, respectively. We assume that the noises are bounded, i.e., $\|w(k)\|_\infty \leq \delta_w \forall k \in \mathbb{N}_0$ and $\|v(k)\|_\infty \leq \delta_v \forall k \in \mathbb{N}_0$. Let us define $\mathcal{W}$ and $\mathcal{V}$ as the feasible sets of each noise, that is,

$$\mathcal{W} = \{w \in \mathbb{R}^n : \|w\|_\infty \leq \delta_w\} \subset \mathbb{R}^n,$$

$$\mathcal{V} = \{v \in \mathbb{R}^m : \|v\|_\infty \leq \delta_v\} \subset \mathbb{R}^m.$$

Note that each region is a zonotope, where each zonotope representation is, respectively, given as $\mathcal{W} = [0, \delta_w]_Z$ and $\mathcal{V} = [0, \delta_v]_Z$. The vector $y^a(k) \in \mathbb{R}^m$ indicates the attack injection designed by a malicious adversary. We consider the estimation problem in finite time. As is the case with the related work, the input $u(k)$ is assumed to be known at all times. We further make the standing assumptions that $(A, B)$ is controllable and $(A, C)$ is observable.

In this paper, we make the following assumption regarding the malicious attacker.

Assumption 1 The adversary can manipulate at most $l$ of the $m$ sensors, i.e., $\|y^a(k)\|_\infty \leq l \forall k \in \mathbb{N}_0$.

With the exception of Assumption 1, there are no assumptions on the attack vector $y^a(k)$, namely, the adversary can construct the attack sequence arbitrary in terms of stochastic properties, bounds of magnitude, time correlations, and so on, under the sparsity condition. As is the case with the conventional work, we assume that the system supervisor knows how many sensors $l$ are possibly attacked, but cannot identify them. However, we note that, whereas some existing results [16], [17] have assumed that the compromised sensor set is fixed for all time, we make no such assumption.

Remark 1 As indicated in [19], the parameter $l$ can be interpreted as a design parameter for the system manager. If he/she chooses a large $l$, the system resilience against sensor attacks will increase. However, a large $l$ can cause a performance degradation under the healthy operation, i.e., $y^a(k) \equiv 0$. Thus, there exists a trade-off between resilience and control performance during normal operation, which relies on $l$, and the defender should design a suitable $l$ with considering the trade-off.

Remark 2 The vulnerabilities of actuation networks are, unfortunately, pointed out by the existing work [10]. In this paper, however, we only deal with sensor attacks since if there were attacks on the actuators, then there exists no stabilizing control law and it is impossible to estimate the true state system. In general, the system resilience against sensor attacks is improved by employing some redundant sensors, whereas it is difficult to reinforce the resilience against actuator attacks. Therefore, it should be noted that the security of actuation networks is much more important than the one of sensors networks.

3.1 Optimistic Estimator

Our challenge is to construct a resilient estimator, where the worst-case estimation performance is bounded for all times. Hence, the problem to be discussed is given as follows.

Problem 1 Suppose that Assumption 1 holds. Under the condition, construct a resilient estimator $f : \mathbb{R}^m \rightarrow \mathbb{R}^n$ which satisfies

$$e(k) = \|x(k) - f(y(k))\|_\infty < \infty \ \forall k \in \mathbb{N}_0, \quad (6)$$

where $e(k)$ is the estimation error and $\hat{x}(k)$ is the state estimate.

In this paper, we consider an estimator which minimizes the magnitude of the worst-case estimation error due to malicious injection $y^a(k)$ to construct a resilient one. The worst-case error $e^*(k)$ and optimal state estimate $\hat{x}^*(k)$ which minimizes the error are, respectively, obtained by

$$e^*(k) = \min_{\hat{x}(k)} \max_{y^a(k)} \|x(k) - \hat{x}(k) - f(y^a(k))\|_\infty$$

$$\hat{x}^*(k) = \min_{\hat{x}(k)} \max_{y^a(k)} \|x(k) - \hat{x}(k) - f(y^a(k))\|_\infty.$$

Though we should denote $e^*(k)$ and $f^*(k)$ as, respectively, $e^*(k)$ and $f^*(k)$ since they are functions of the state estimate $\hat{x}(k)$ and measurement $y(k)$, we simply denote them with using the time index $k$. 


\[ e^*(k) = \max_{x(k) \in \mathbb{R}^n} |x(k) - \hat{\chi}(k)|, \quad (7) \]

\[ f^*(k) = \arg \min_{\delta(k)} \max_{x(k) \in \mathbb{R}^n} |x(k) - \hat{\chi}(k)|, \quad (8) \]

For deriving the state estimate, we first have the following set \([23],[24]\).

**Definition 1** The reach set \(\mathcal{R}(k)\) is the set of states in \(\mathbb{R}^n\) to which the system will evolve at the next step given any \(x(k-1) \in \mathcal{R}(k-1)\), admissible control input, and allowable noise, i.e.,

\[ \mathcal{R}(k) = \{ x \in \mathbb{R}^n : \exists x(k-1) \in \mathcal{R}(k-1), u(k-1), w(k-1) \in \mathcal{W}, \] such that \( x = Ax(k-1) + Bu(k-1) + w(k-1) \}, \]
or,

\[ \mathcal{R}(k) = \mathcal{A}^k \mathcal{X}_0 \oplus \sum_{j=0}^{k-1} \mathcal{A}^{k-1-j} Bu(j) \oplus \bigoplus_{j=0}^{k-1} \mathcal{A}^{k-1-j} \mathcal{W}. \quad (9) \]

For subsequent analysis, we use a matrix \(H(k)\) and a vector \(c(k)\) configuring the reach set \(\mathcal{R}(k)\) in \(\mathcal{H}\)-representation:

\[ \mathcal{R}(k) = \{ x \in \mathbb{R}^n : H(k)x \leq c(k) \}. \quad (10) \]

Actually, the reach set is a zonotope since the feasible set of the process noise \(\mathcal{W}\) and the initial state \(\mathcal{X}_0\) are zonotopes. Hence, by (9), the reach set is also formulated as a zonotope:

\[ \mathcal{R}(k) = \left\{ \sum_{j=0}^{k-1} \mathcal{A}^{k-1-j} Bu(j), [\mathcal{A}^k \mathcal{G}_0, \delta^y \mathcal{A}^{k-1}, \ldots, \delta^y] \right\} \subseteq \mathbb{R}^n. \quad (11) \]

Let \(c(\mathcal{R}(k))\) and \(G(\mathcal{R}(k))\) be the Chebyshev center and the generators matrix of the reach set \(\mathcal{R}(k)\), respectively. Then, by Properties 4 and 5, one can obtain the reach set recursively:

\[ \mathcal{R}(k) = [\mathcal{A}c(\mathcal{R}(k-1)) + Bu(k-1), [\mathcal{A}G(\mathcal{R}(k-1)), \delta^y]] \subseteq \mathbb{R}^n. \]

Taking into account that the state at time \(k\) belongs to the reach set \(\mathcal{R}(k)\), the set of feasible state that can generate the compromised measurement \(y(k)\) is given as

\[ \mathcal{X}(k) = \{ x \in \mathcal{R}(k) : \exists v(k) \in \mathcal{V}, y^*(k) \text{ such that } ||y^*(k)||_0 \leq l \} \]

\[ \text{and } y(k) = Cx + v(k) + y^*(k). \]

Revisiting the worst-case error \(e^*(k)\) and optimal estimate \(f^*(k)\), then, they can be rewritten as follows by using \(\mathcal{X}(k)\):

\[ e^*(k) = \max_{x(k) \in \mathcal{X}(k)} |x(k) - \hat{\chi}(k)|, \quad (13) \]

\[ f^*(k) = \arg \min_{\delta(k)} \max_{x(k) \in \mathcal{X}(k)} |x(k) - \hat{\chi}(k)|, \quad (14) \]

which implies that the worst-case error is equal to the Chebyshev radius of the set \(\mathcal{X}(k)\) and the optimal estimate is equal to the Chebyshev center of the set. Here, for a bounded set \(S\), the Chebyshev radius \(r(S)\) and the Chebyshev center \(c(S)\) of the set are, respectively, defined as follows \([25]\):

\[ \rho(x, S) = \min_{r \in \mathbb{R}^+} \| r \mathcal{S} \subseteq \mathcal{B}(x, r) \],

\[ r(S) = \min_{x \in \mathcal{X}} \rho(x, S), \quad (15) \]

\[ c(S) = \arg \min_{x \in \mathcal{X}} \rho(x, S). \quad (16) \]

Geometrically speaking, the Chebyshev radius of a set is the radius of the minimum volume circumscribing ball which covers the set while the Chebyshev center of the set is the center of the ball. Accordingly, we have

\[ e^*(k) = r(\mathcal{X}(k)), \quad f^*(k) = c(\mathcal{X}(k)). \quad (17) \]

Hence, in order to obtain the optimal state estimate \(f^*(k)\), we need to get the feasible set \(\mathcal{X}(k)\) and calculate the Chebyshev center of the set. In the next section, we provide a concrete design procedure of the estimator.

4. Estimator Design

For an index set \(I \subseteq \{i_1, \ldots, i_L\} \subseteq S\) with \(|I| = j\), let us define the complement set \(I^C = \mathbb{U} - I\). Moreover, we define a subspace \(\mathcal{L}_I = \mathcal{S} \oplus \mathcal{L}_J\), where \(e_i \in \mathbb{R}^n\) is the \(i\)th vector of the canonical basis of \(\mathbb{R}^n\) and \(\mathcal{S} = \mathcal{S} \oplus \mathcal{L}_J\).

Based on \(\mathcal{L}_I\), we define the following set:

\[ \mathcal{X}_I(k) = \{ x \in \mathcal{X}(k) : \exists v(k) \in \mathcal{V}, y^*(k) \in \mathcal{L}_J, 
\text{such that } y(k) = Cx + v(k) + y^*(k), \}

\[ \text{which represents all possible states which generates the measurement } y(k) \text{ when the sensors in the index set } I \text{ are benign and the sensors in } I^C \text{ are attacked. Thus, } \mathcal{X}(k) \text{ can be written as} \]

\[ \mathcal{X}(k) = \bigcup_{|I| = m} \mathcal{X}_I(k). \quad (20) \]

Again for an index set \(I \subseteq \{i_1, \ldots, i_L\} \subseteq S\), we define

\[ C_I \doteq \begin{bmatrix} C_{i_1} & \vdots & C_{i_L} \end{bmatrix} \in \mathbb{R}^{|I| \times n}, \quad v_I(k) \doteq \begin{bmatrix} v_{i_1}(k) \\ \vdots \\ v_{i_L}(k) \end{bmatrix} \in \mathbb{R}^{|I|}, \]

\[ y_I(k) \doteq \begin{bmatrix} y_{i_1}(k) \\ \vdots \\ y_{i_L}(k) \end{bmatrix} \in \mathbb{R}^{|I|}, \quad y_I^*(k) \doteq \begin{bmatrix} y_{i_1}^*(k) \\ \vdots \\ y_{i_L}^*(k) \end{bmatrix} \in \mathbb{R}^{|I|}, \]

which implies that the selecting rows of each matrix with indices in \(I\). By the definition of \(\mathcal{X}_I(k)\), since \(y^*(k) \in \mathcal{L}_J\), indicates \(y^*_I(k) = 0\) for an index set \(I\) with cardinality \(m - l, x(k) \in \mathcal{X}_I(k)\) is equivalent to that there exists \(v_I(k)\) such that \(y_I(k) = C_I x(k) + v_I(k)\) and \(||y_I^*(k)||_0 \leq \delta^v\). Thus, we must have

\[ ||v_I(k)||_0 = ||y_I^*(k) - C_I x(k)||_0 \leq \delta^v, \]

which implies that \(\mathcal{X}_I(k)\) is calculated by

\[ \mathcal{X}_I(k) = \{ x \in \mathcal{R}(k) : ||y_I(k) - C_I x(k)||_0 \leq \delta^v \}. \quad (22) \]

This can be written as the following using a matrix \(M_I \doteq \begin{bmatrix} I & -I \end{bmatrix} \in \mathbb{R}^{|I| \times |I|}: \)

1 Though we should denote \(\mathcal{X}(k)\) as \(\mathcal{X}(y(k))\) since it is a subspace depending on the compromised measurement \(y(k)\), we also abbreviate it as \(\mathcal{X}(k)\).
$X(k) = \{ x \in \mathbb{R}^n : M \gamma(k) - C x \leq \delta^t 1_{2n} \}$

which indicates that $X(k)$ is given as a polytope. Exploiting the matrix $H(k)$ and the vector $c(k)$, it is easy to see that the polytope can be reformulated as

$$X(k) = \{ x \in \mathbb{R}^n : \left[ -M C J H(k) \right] x \leq \left[ \delta^t 1_{2n} - M J \gamma(k) \right] c(k) \}.$$  

In order to calculate the optimal state estimate (i.e., the Chebyshev center of $X(k)$), we have to obtain the circumscribing ball covering $X(k)$. For a bounded set $S \subseteq \mathbb{R}^n$ which has nonempty interior, it is well known that the minimum volume ellipsoid that covers $S$ called the Löwner-John ellipsoid is computed by the following optimization problem [26]:

$$\min_{\Phi \in \mathbb{R}^{n \times n}, x \in \mathbb{R}^n} \log \det \Phi^{-1}$$

subject to $\sup_{x \in S} \| \Phi x + b \| \leq 1$,  

$$\min_{\gamma \in \mathbb{R}^n, J \in \mathbb{R}^{n \times n}} \gamma$$

subject to $\sup_{x \in X(k)} \| \gamma x + b \| \leq 1$.  

Evaluating the constraint function (28), however, involves solving a convex maximization problem, and is not tractable. As aforementioned, $X(k)$ is given as a polytope and the feasible set $X(k)$ is given as a union of polytopes. Recalling that every polytope is a convex hull of its vertices, therefore, we only have to consider the vertices of each polytope $X(k)$ to calculate the minimum volume circumscribing ball of $X(k)$. Thus, the above optimization problem is rewritten as

$$\min_{y(k) \in \mathbb{R}^n, J(k) \in \mathbb{R}^{n \times n}} \gamma(k)$$

subject to $\| y(k) v + b(k) \| \leq 1 \ \forall v \in V_X(k)$, where $V_X(k) = \bigcup_{j=1}^{m} V_{X,j}(k)$ and $V_{X,j}(k)$ is the vertex set of $X(j(k))$. Using the minimizers of (29), the optimal state estimate can be derived as $f^*(k) = -b(k)/\gamma(k)$. Note that $V_X(k)$ is, in general, not the vertex set of $X(k)$ since the union could eliminate some of the vertices or add new vertices. In this paper, however, we only have to get the vertex set which explain the Chebyshev ball of $X(k)$, and the vertex set is obviously a subset of $\bigcup_{j=1}^{m} V_{X,j}(k)$. In conclusion, the optimal state estimate can be computed by Algorithm 1.

All calculations regarding polytopes discussed in this section such as an affine mapping, Minkowski summation, and vertex enumeration can be implemented using existing computational geometry software packages. The reader is referred to [27]–[29] and the literature on computational geometry for details.

4.1 Bound for Estimation Error

This subsection is devoted to providing a bound on the estimation error of the proposed estimator. We start by introducing Jung’s theorem which states the relationship between the diameter and Chebyshev radius of a bounded set.

**Lemma 1 (Jung’s theorem [30, Theorem 2.6])** For a bounded set $S$ in $\mathbb{R}^n$, the following inequality holds:

$$d(S) \leq d(S) \sqrt{\frac{n}{2n+2}}.$$  

Then, the following theorem provides the bounds of the worst-case estimation error $e^*(k)$.

**Theorem 1** Define $V_{R(k)}$ as the vertex set of $R(k)$ and suppose that Assumption 1 holds. Regarding the worst-case estimation error $e^*(k)$, we have

$$e^*(k) \leq \frac{1}{\gamma_{R(k)}} \forall k \in N_0,$$

where $\gamma_{R(k)}$ is a solution of the following optimization problem:

$$\min_{\gamma \in \mathbb{R}^n, J \in \mathbb{R}^{n \times n}} \gamma(k)$$

subject to $\| y_{R(k)} v + b(k) \| \leq 1 \ \forall v \in V_{R(k)}$.

In particular, if for all index sets $K \subseteq S$ with $|K| = m - 2l$, $C_K$ has full column rank, then $e^*(k)$ has a rigorous bound as follows:

$$e^*(k) \leq \max_{|K|=m-2l} \delta^t \sqrt{\frac{2mnp}{n+1}} \forall k \in N_0,$$

where $F_K \cong C_K C_K^t$.

**Proof.** We first derive (35). Suppose that for all $K \subseteq S$ whose cardinality is $m - 2l$, $C_K$ has full column rank. Using a pair of index sets $I$ and $J$ whose cardinalities are $m - l$, $K$ is defined as

$$K = I \cap J = S \left( \{ I^C \} \cup \{ J^C \} \right).$$

Then, for any point $x_1(k) \in X(k)$ and $x_2(k) \in X_J(k)$, we have

$$y(k) = C x_1(k) + v_1(k) + y_1(k) = C x_2(k) + v_2(k) + y_2(k),$$

where $\| v_1(k) \|_{\infty} \leq \delta^t, \| v_2(k) \|_{\infty} \leq \delta^t, \gamma_1(k) \in L_{F_K}$, and $\gamma_2(k) \in L_{F_K}$. 

Algorithm 1 Calculate a state estimate minimizing worst-case error

**Require:** $y(k), I, A, C, H(k), c(k), M, \delta$

**Ensure:** $f^*(k)$

1. Compute $C_I$ and $y_I(k)$ for all $|I| = m - l$.
2. Compute the feasible set $X(k)$ for all $|I| = m - l$ as (23) and enumerate its vertices $V_{X_I}(k)$.
3. Obtain the vertex set $V_{X}(k)$ as $V_{X}(k) = \cup_{I=1}^{m} V_{X_I}(k)$.
4. Compute the optimization problem (29) and obtain $y(k)$ and $b(k)$.
5. return $f^*(k) = -b(k)/\gamma(k)$.
of $\mathcal{L}_{C_i}$. Since both $y_i^{(1)}(k)$ and $y_i^{(2)}(k)$ have zero entries, where $i \in \mathcal{K}$, we have

\begin{align*}
C_{x}(x^1(k) + v^1_{C}(k) & = C_{x}x^2(k) + v^2_{C}(k) \\
\Rightarrow C_{x}(x^1(k) - x^2(k)) & = v^1_{C}(k) - v^1_{C}(k) \\
\Rightarrow x^1(k) - x^2(k) & = F^{-\top}_{C_x}C_x(v^1_{C}(k) - v^1_{C}(k)).
\end{align*}

(37)

By the fact that $\max\|v^1_{C}(k) - v^1_{C}(k)\| = 2\delta^\top \sqrt{m}$, we obtain

\begin{align*}
\|x^1(k) - x^2(k)\| & \leq \|F^{-\top}_{C_x}C_x\|\|v^1_{C}(k) - v^1_{C}(k)\| \\
& \leq 2\delta^\top \sqrt{m}\|F^{-\top}_{C_x}C_x\| = 2\delta^\top \sqrt{m}\|F^{-\top}_{C_x}C_x\|.
\end{align*}

(38)

Hence, the upper bound of $\|x^1(k) - x^2(k)\|$ follows

\begin{equation}
\max_{x^1(k) \in \mathcal{L}_{C_1}(k), x^1(k) \in \mathcal{L}_{C_2}(k)} \|x^1(k) - x^2(k)\| = 2\delta^\top \sqrt{m}\|F^{-\top}_{C_x}C_x\|.
\end{equation}

(39)

Exploiting Lemma 1, the following inequality is finally derived:

\begin{equation}
e^*(k) = r(\mathcal{Z}(k)) \leq d(\mathcal{Z}(k)) \leq \sqrt{\frac{n}{2n + 2}} \leq \max_{|\mathcal{K}| = m-2l} \delta^\top \sqrt{\frac{2mnp(F^{-\top}_{C_x})}{n + 1}}.
\end{equation}

(40)

So far, we analyzed the case when $C_{x}$ has full column rank for all $|\mathcal{K}| = m-2l$. From now on, we suppose that there exist an index set $\mathcal{K}$ with cardinality $m-2l$ such that $C_{x}$ is not full column rank. As well as above, consider a pair of index sets $I$ and $J$ whose cardinalities are $m - l$ such that $\mathcal{K} = I \cap J$. If $C_{x}$ is not full column rank, then $C_{x}$ is not injective and $\ker C_{x} \neq \{0\}$, i.e., there exists a nonzero vector $x$ which satisfies $C_{x}x = 0$. Recalling (37), for any $y^{(1)}(k) \in \mathcal{L}_{C_1}, y^{(2)}(k) \in \mathcal{L}_{C_2}$, and $v^1 = v^2 = 0 \in \mathcal{V}$, we can assert that

\begin{equation}
C_{x}(x^1(k) - x^2(k)) = v^1_{C}(k) - v^1_{C}(k) = 0.
\end{equation}

(41)

Thus, if the reach set of $(x^1(k))$ and $(x^2(k))$ are unbounded, then there exist unbounded states satisfying (41) with $(x^1(k) - x^2(k)) \in \ker C_{x}$, and the upper bound of the diameter of $\mathcal{Z}(k)$ is also unbounded. In this paper, we consider the reach set of the state, and hence the upper bound of the diameter of $\mathcal{Z}(k)$ is equal to the diameter of $\mathcal{R}(k)$. Therefore, $e^*(k)$ satisfies

\begin{equation}
e^*(k) \leq r(\mathcal{R}(k)),
\end{equation}

(42)

where we utilize the symmetric property of $\mathcal{R}(k)$.

Since $\mathcal{R}(k)$ is a zonotope, $\mathcal{R}(k)$ is presented by the convex hull of its vertices. Defining the vertex set of $\mathcal{R}(k)$ as $\forall \mathcal{R}(k)$, $r(\mathcal{R}(k))$ is given as the Chebyshev radius of the set $\forall \mathcal{R}(k)$. Thus, the following optimization problem provides the minimum circumscribing ball covering the set:

\begin{equation}
\min_{y_{\forall \mathcal{R}(k)} \in \mathbb{R}^d} \gamma(\mathcal{R}(k))
\end{equation}

subject to \(\|y_{\forall \mathcal{R}(k)} + b\| \leq 1 \) \(\forall v \in \forall \mathcal{R}(k)\),

(44)

and we have $r(\mathcal{R}(k)) = 1/\gamma(\mathcal{R}(k))$. Therefore, if there exists an index set $\mathcal{K}$ with cardinality $m - 2l$ such that $C_{x}$ is not full column rank, the worst-case error follows (32).

According to this theorem, we find that the proposed estimator satisfies (6), namely it is a resilient one. It is worth remarking that the estimation error of the proposed estimator is always bounded. Even if the adversaries manipulate more than $m - 2l$ sensors or the system is not observable after removing any subset, the worst-case estimation error satisfies the relation of (32). This is the main contribution by considering the reach set of the system state. Nevertheless, notice that the reach set expands infinitely if the system is not strictly stable, i.e., $\rho(A) \geq 1$. Hence, unless the system is strictly stable, the right-hand side of (32) goes to infinity with $k \to \infty$.

5. Computational Complexity-Aware Estimator Design with Interval Hull Approximation

In the previous section, we derived that an optimal estimate which minimizes the worst-case error is obtained as the Chebyshev center of $\mathcal{Z}(k)$, and the worst-case error of the proposed estimator is bounded for all times. Here, for the sake of computing the optimal estimate, we need to enumerate all vertices of $\mathcal{Z}(k)$. However, the cost of this computation may increase depending on the time step $k$. More precisely, we see that the order of the zonotope $\mathcal{R}(k)$ is equal to $k + p/n$, and thus by Property 2, $\mathcal{R}(k)$ has at least $(2k + 2p/n)\sqrt{n}/\sqrt{n}$ vertices. By (23), therefore, the number of vertices of the feasible set $\mathcal{F}(k)$ may increase depending on the time step. Additionally, in Algorithm 1, we need to obtain $H(k)$ and $e^*(k)$ to characterize $\mathcal{F}(k)$, which is referred as the facet enumeration problem and is, in general, not easy to calculate. Hence, toward practical operations, we need to harness the computational complexity for the estimation. To achieve this, we propose a state estimator by resorting to an interval hull of the reach set.

Let $\text{Box}(\mathcal{S})$ be a function that maps a set $\mathcal{S} \subseteq \mathbb{R}^n$ to its interval hull, that is, the smallest Cartesian product of intervals containing the set $\mathcal{S}$ [33]. Note that, for every two sets $S_1, S_2 \subseteq \mathbb{R}^n$, we have

\begin{equation}
\text{Box}(S_1 \oplus S_2) = \text{Box}(S_1) \oplus \text{Box}(S_2).
\end{equation}

The following property provides the relation between Chebyshev centers of the reach set $\mathcal{R}(k)$ and its interval hull $\text{Box}(\mathcal{R}(k))$.

Property 6 The Chebyshev center of the interval hull of the reach set $\text{Box}(\mathcal{R}(k))$ is equal to the one of $\mathcal{R}(k)$, that is,

\begin{equation}
c(\text{Box}(\mathcal{R}(k))) = c(\mathcal{R}(k)) \ \forall k \in \mathbb{N}_0.
\end{equation}

(45)

Proof. By (9), it follows that

\begin{equation}
\text{Box}(\mathcal{R}(k)) = \text{Box}\left(A^{k-l}_j \oplus \sum_{j=0}^{k-l} A^{k-l-j}Bu(j) \oplus \bigoplus_{j=0}^{k-l} A^{k-l-j}W\right)
\end{equation}

\begin{equation}
= \text{Box}\left(A^{k-l}_j \frac{k-l}{j=0} \sum A^{k-l-j}Bu(j) \oplus \bigoplus_{j=0}^{k-l} A^{k-l-j}W\right).
\end{equation}

Here, according to Properties 4 and 5, one can formulate

\footnote{Note that there is beautiful literature about the problem such as [31], [32] which achieves to obtain $H(k)$ and $e^*(k)$ in polynomial time. In practice, moreover, it is worth mentioning that one can obtain the matrix and vector by implementing MPT 3.0 [29].}
\[
\bigoplus_{j=0}^{k-1} A^{k-1-j}W = [0, [\delta^n A^{k-1}, \ldots, \delta^n I]]_\mathbb{Z},
\]
which indicates that the Chebyshev center of Box(\bigoplus_{j=0}^{k-1} A^{k-1-j}W) is 0. The Chebyshev center of \(X_0\) is also 0, and therefore, we obtain
\[
c(\text{Box}(\mathcal{R}(k))) = \sum_{j=0}^{k-1} A^{k-1-j}Bu(j),
\]
which indicates that, due to (11), \(c(\text{Box}(\mathcal{R}(k))) = c(\mathcal{R}(k))\).

Regarding the reach set \(\mathcal{R}(k)\), let us define the following vector:
\[
\xi(k) \triangleq \left[ \begin{array}{c} \xi(G(\mathcal{R}(k)))_l \\ \vdots \\ \xi(G(\mathcal{R}(k)))_n \end{array} \right] \in \mathbb{R}^n, \quad (46)
\]
where, for a vector \(a = [a_1, \ldots, a_n] \), \(\Sigma(a^T)\) indicates the summation of all entries of \(a\), i.e., \(\Sigma(a^T) = \sum_{i=1}^{n} a_i.\) Since the vector \(\xi(k)\) indicates the summation of the absolute generators of the zonotope \(\mathcal{R}(k)\), each element of \(\xi(k)\) implies the absolute maximum value of the corresponding dimension of \(\mathcal{R}(k)\). By (11), this vector can be obtained by
\[
\xi(k) = \left[ \begin{array}{c} \Sigma(A^1G(\mathcal{R}(k)))_1 \\ \vdots \\ \Sigma(A^1G(\mathcal{R}(k)))_n \end{array} \right] + \tilde{\xi}(k), \quad (47)
\]
\[
\tilde{\xi}(k) = \tilde{\xi}(k-1) + \delta^w, \quad (48)
\]
Since Box(\(\mathcal{R}(k)\)) is symmetric for each axis and, according to Property 6, its Chebyshev center coincides with the one of \(\mathcal{R}(k)\), the \(\mathcal{H}\)-representation of Box(\(\mathcal{R}(k)\)) is given as
\[
\text{Box}(\mathcal{R}(k)) = \left\{ x \in \mathbb{R}^n : \left[ \begin{array}{c} I \\ -I \end{array} \right] x \leq \left[ \begin{array}{c} \xi(k) + c(\mathcal{R}(k)) \\ \xi(k) - c(\mathcal{R}(k)) \end{array} \right] \right\}.
\]
Therefore, one can easily derive that its vertex set is given as
\[
V_{\text{Box}(\mathcal{R}(k))} = \{ [\pm \xi_1(k), \ldots, \pm \xi_n(k)] + c(\mathcal{R}(k)) \} \quad (49)
\]
for any double-sign, and thus the number of the vertex \(V_{\text{Box}(\mathcal{R}(k))}\) is \(2^n\). In analogy with \(\mathcal{X}_f(k)\), for an index set \(I = \{i_1, \ldots, i_j\} \subset \mathcal{S}\), let us define the following set which is outer-approximated by the interval hull Box(\(\mathcal{R}(k)\)):
\[
\mathcal{Z}_f(k) \triangleq \left\{ x \in \text{Box}(\mathcal{R}(k)) : 3v(k) + \mathcal{V}y^d(k) \in \mathcal{L}_{f}, \text{ such that } y(k) = Cx + v(k) + y^d(k) \right\}
\]
\[
= \left\{ x \in \mathbb{R}^n : \left[ \begin{array}{c} -M_f C_f \\ I \\ -I \end{array} \right] x \leq \left[ \begin{array}{c} \delta^1 2\mathcal{Z}_f(k) - M_f y_f(k) \\ \xi(k) + c(\mathcal{R}(k)) \\ \xi(k) - c(\mathcal{R}(k)) \end{array} \right] \right\},
\]
\[
(50)
\]
Since the number of the hyperplanes configuring \(\mathcal{Z}_f(k)\) is fixed by \(2|I| + 2n\), the upper bound of the number of the vertices of \(\mathcal{Z}_f(k)\) is also constant for all time. Therefore, we obviously see that the computational complexity of vertex enumeration of the approximated set \(\mathcal{Z}_f(k)\) can be reduced than the case of \(\mathcal{X}_f(k)\). As with (20), the outer-approximated feasible region of the state is given as \(\mathcal{Z}(k) \triangleq \bigcup_{k \in \text{Box}(\mathcal{R}(k))} \mathcal{Z}_f(k)\). The modified secure state estimation algorithm utilizing the interval hull approximation is given as Algorithm 2, where \(\hat{f}^*(k)\) indicates the optimal estimate based on the outer-approximated feasible region defined as
\[
\hat{f}^*(k) \triangleq \arg \min_{\hat{f}(k) \in \hat{f}(k)} \max_{u(k) \in \text{Box}(\mathcal{R}(k))} \| x(k) - \hat{x}(k) \|. \quad (51)
\]
As well, let us define \(\hat{e}^*(k)\) to indicate the worst-case error under the approximated feasible region:
\[
\hat{e}^*(k) \triangleq \max_{u(k) \in \text{Box}(\mathcal{R}(k))} \| x(k) - \hat{x}(k) \|. \quad (52)
\]
Using nomenclatures of the Chebyshev radius and center, hence, the approximated worst-case error \(\hat{e}^*(k)\) and the approximated optimal estimate \(\hat{f}^*(k)\) are, respectively, given as
\[
\hat{e}^*(k) = r(\mathcal{Z}(k)), \quad \hat{f}^*(k) = c(\mathcal{Z}(k)). \quad (53)
\]

5.1 Bound for Estimation Error
We have shown that Algorithm 2 that utilizes the interval hull approximation of the reach set is able to reduce the computational complexity for the estimation. However, the worst-case estimation error possibly deteriorates by using this approximation. In this subsection, hence, we provide the error bound in Algorithm 2, and we further show that its bound is equal to the one of Algorithm 1 under a certain condition. Before continuing on, we obtain the following property regarding the Chebyshev radius of the interval hull of the reach set.

Property 7
\[
r(\text{Box}(\mathcal{R}(k))) = \| \xi(k) \| \quad \forall k \in \mathbb{N}_0.
\]

**Proof.** By the definition of the interval hull and (46), the diameter of Box(\(\mathcal{R}(k)\)) is given as \(d(\text{Box}(\mathcal{R}(k))) = 2\| \xi(k) \|\). According to Property 1, any zonotope is centrally symmetric, and thus, for a zonotope \(\mathcal{Z}\), we see that \(2r(\mathcal{Z}) = d(\mathcal{Z})\), which directly derives (54).

Now, we provide the bound of the approximated worst-case estimation error in Algorithm 2.
Property 8 Suppose that Assumption 1 holds. The approximated worst-case error in Algorithm 2 satisfies
\[ \hat{e}^*(k) \leq \|\xi(k)\| \quad \forall k \in \mathbb{N}_0. \] (55)

Moreover, if there exists a vector \( \varepsilon = [\varepsilon_1, \ldots, \varepsilon_{p+x}]^\top \), \( \varepsilon_i = 1 \) or \(-1\) satisfying
\[ G(R(k))\varepsilon = \left[ \pm \xi_1(k) \quad \cdots \quad \pm \xi_n(k) \right]^\top \quad \forall k \leq n, \] (56)

then this error is bounded by (32), which indicates that the worst-case error does not deteriorate by using Algorithm 2.

Proof. Recalling that the approximated feasible region \( \hat{R}(k) \) is a subset of \( \text{Box}(R(k)) \), we see that the approximated worst-case error satisfies \( \hat{e}^*(k) \leq r(\text{Box}(R(k))) \forall k \in \mathbb{N}_0 \). Thus, by Property 7, we obtain the relation (55).

Next, we focus on deriving the condition such that this error is bounded by (32). By the definitions of the Chebyshev radius and interval hull, this condition is equivalent to \( r(\text{Box}(R(k))) = r(\text{Box}(R(k))) \forall k \in \mathbb{N}_0 \). Thus, by Property 7, we obtain the relation (55).

Without loss of generality, we here ignore the system input \( u(k) \), which implies \( r(R(k)) = 0 \forall k \in \mathbb{N}_0 \). Then, according to Property 3 and (49), if there exist a vector \( \varepsilon = [\varepsilon_1, \ldots, \varepsilon_{p+x}]^\top \), \( \varepsilon_i = 1 \) or \(-1\) satisfying the following, then \( R(k) \) and \( \text{Box}(R(k)) \) share at least one vertex:
\[ G(R(k))\varepsilon = \left[ \pm \xi_1(k) \quad \cdots \quad \pm \xi_n(k) \right]^\top . \]

Thus, by the Cayley-Hamilton theorem, we finally derive that if there exists the vector \( \varepsilon \) which satisfies (56), then the approximated worst-case error is bounded by (32).

According to this property, we find that the approximated estimator is also a resilient one and, under a certain condition, the worst-case error does not get worse than the one of Algorithm 1. For the sake of the calculation that whether there exists a vector \( \varepsilon \) satisfying (56), one needs to solve a combinatorial optimization problem, which is, in general, not tractable. However, it is worth remarking that this can be computed in advance, not real-time.

6. Numerical Example

6.1 Computational Performance

We first compare the computational performance of the proposed Algorithms 1 and 2. To perform this comparison, we randomly generated 30 systems with \( n = 4, m = 6 \), and we assume that two sensors are randomly compromised, i.e., \( l = 2 \). Each simulation is tested in 10 to 350 steps and each execution time is measured. The simulations are performed on a desktop equipped with an Intel Core i5-4460 3.20 GHz and an 8 GB memory chip and each algorithm is implemented by using CVX [27], [28] and MPT 3.0 [29].

Figure 3 shows the averaged results of simulation times in Algorithms 1 and 2. Obviously, Algorithm 2 outperforms Algorithm 1 in terms of the computational cost. Hence, we confirm that the computational complexity is reduced by utilizing the interval hull approximation of the reach set.

Figures 4 shows the bias injected by the malicious attacker, where he/she first corrupts the second sensor with a random noise, and then he/she asserts a replay attack to the first sensor. The attacker finally adds a monotonically increasing signal to the first sensor again. Note that the number of the compromised sensor is always 1, namely \( l = 1 \), and is known to the defender.

In this example, we demonstrate various attack scenarios. Figure 4 shows the estimation results regarding the UGV position and its velocity, respectively. For the purpose of comparison, we use the \( H_\infty \) filter and the robust Kalman filter (robust KF), which is described in [34]. For the precise algorithm of the robust KF, please see Appendix. As in both figures, the proposed algorithms achieve estimating the state in the presence of attacks. In particular, it is worth remarking that the proposed estimators achieve more accurate estimation.
than the $H_\infty$ filter and robust KF in the condition that the first sensor is compromised (the second and the third attack scenarios) where the removed system is not observable. Also, we can confirm the estimation errors in the proposed algorithms, which are depicted in Fig. 7, are low enough. Finally, for the readers’ reference, Fig. 8 shows the estimation result in $k = 30$, where the second sensor is compromised. This also illustrates that the proposed estimators outperform conventional ones. To summarize, Algorithm 2 estimates the state more efficiently in terms of the computational cost than Algorithm 1 without sacrificing the estimation performance.

7. Conclusion

In this paper, we have discussed the secure estimation problem in the presence of sensor attacks. We tackled to construct a resilient estimator which minimizes worst-case error due to the malicious injections. To this end, taking the reach set of the state into account, the feasible region of the state was given as a union of polytopes, and the optimal estimate which minimizes the worst-case error was obtained as the Chebyshev center of the set. On the proposed estimator, it was derived that the worst-case error is bounded for all times. It is worth noticing that the proposed method is able to estimate the state even if the adversary manipulates more than half of all sensors or the system is not observable after removing any subset of sensors. Further, for the sake of reducing the computational complexity, we have also provided another secure state algorithm resorting to the interval hull approximation of the reach set. Under a certain condition, the computational complexity can be reduced without affecting the worst-case error using this approximation. We finally confirmed that the effectiveness of the proposed estimators, and especially, the approximated algorithm achieves to reduce the computational cost without sacrificing the estimation performance.

Acknowledgments

The authors would like to thank Dr. Kazumune Hashimoto for fruitful discussion and his valuable comments. This work was supported by JST CREST Grant Number JPMJCR15K2, Japan.

References

[1] K.D. Kim and P.R. Kumar: Cyber-physical systems: A perspective at the centennial, Proc. IEEE, Vol. 100, no. Special Centennial Issue, pp. 1287–1308, 2012.
[2] J. Sztipanovits, X. Koutsoukos, G. Karsai, N. Kottenstette, P. Antsaklis, V. Gupta, B. Goodwine, J. Baras, and S. Wang: Toward a science of cyber-physical system integration, Proc. IEEE, Vol. 100, No. 1, pp. 29–44, 2012.
[3] R. Langner: Stuxnet: Dissecting a cyberwarfare weapon, IEEE Secur. Privacy, Vol. 9, No. 3, pp. 49–51, 2011.
[4] J. Slay and M. Miller: Lesson learned from the Maroochy water branch, Critical Infrastructure Protection, Vol. 253, pp. 73–82, 2007.
[5] ESET spol. s.r.o: Industroyer: Biggest malware threat to critical infrastructure since Stuxnet, [online] https://www.eset.com/int/industroyer, 2017.
[6] N.O. Tippenhauer, C. Pöpper, K.B. Rasmussen, and S. Čapkun: On the requirements for successful GPS spoofing attacks, Proc. 18th ACM Conf. Comput. Commun. Security, New York, NY, pp. 75–86, 2011.
[7] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava: Non-invasive spoofing attacks for anti-lock braking systems, Proc. 15th Int. Conf. Cryptographic Hardware and Embedded Syst., Santa Barbara, CA, pp. 55–72, 2013.
[8] Y. Mo, R. Chabukswar, and B. Sinopoli: Detecting integrity attacks on SCADA systems, IEEE Trans. Control Syst. Technol., Vol. 22, No. 4, pp. 1396–1407, 2014.
[9] T. Irita and T. Namerikawa: Detection of replay attack on smart grid with code signal and bargaining game, Proc. 2017 Amer. Control Conf., Seattle, WA, pp. 2112–2117, 2017.
[10] 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.
[11] Y. Mo and B. Sinopoli: On the performance degradation of cyber-physical systems under stealthy integrity attacks, IEEE Trans. Autom. Control, Vol. 61, No. 9, pp. 2618–2624, 2016.
[12] T. Shinohara and T. Namerikawa: On the vulnerabilities due to manipulative zero-stealthy attacks in Cyber-physical systems, SICE J. of Control, Measurement, and System Integration, Vol. 10, No. 6, pp. 563–570, 2017.
[13] H. Fawzi, P. Tabuada, and S. Diggavi: Secure estimation and
control for cyber-physical systems under adversarial attacks, *IEEE Trans. Autom. Control*, Vol. 59, No. 6, pp. 1454–1467, 2014.

[14] Y. Shoukry and P. Tabuada: Event-triggered state observers for sparse sensor noise/attacks, *IEEE Trans. Autom. Control*, Vol. 60, No. 8, pp. 2079–2091, 2016.

[15] M.S. Chong, M. Wakaiki, and J.P. Hespanha: Observability of linear systems under adversarial attacks, *Proc. 2015 Amer. Control Conf.*, Chicago, IL, pp. 2439–2444, 2015.

[16] M. Pajic, I. Lee, and G.J. Pappas: Attack-resilient state estimation for noisy dynamical systems, *IEEE Trans. Control Netw. Syst.*, Vol. 4, No. 1, pp. 82–92, 2017.

[17] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G.J. Pappas, and I. Lee: Design and implementation of attack-resilient cyber-physical systems, *IEEE Control Syst. Mag.*, Vol. 37, No. 2, pp. 66–81, 2017.

[18] Y. Shoukry, P. Nuzzo, A. Puggelli, A.L. Sangiovanni-Vincentelli, S.A. Seshia, and P. Tabuada: Secure estimation for cyber physical systems under sensor attacks: A satisfiability modulo theory approach, *IEEE Trans. Autom. Control*, Vol. 62, No. 10, pp. 4917–4932, 2017.

[19] Y. Nakahira and Y. Mo: Dynamic state estimation in the presence of compromised sensory data, *Proc. IEEE 54th Conf. Decision and Control*, Osaka, Japan, pp. 5808–5813, 2015.

[20] G.M. Ziegler: *Lectures on Polytopes*, Graduate Texts in Mathematics, Springer, 1995.

[21] P. McMullen: On zonotopes, *Trans. Amer. Math. Soc.*, Vol. 159, pp. 91–109, 1971.

[22] T. Zaslavski: Facing up to arrangements: Face-count formulas for partitions of space by hyperplanes, Memoirs of the AMS no. 154, Amer. Math. Soc., 1975.

[23] E.C. Kerrigan: Robust Constraint Satisfaction: Invariant Sets and Predictive Control, Ph.D. dissertation, Univ. Cambridge, Cambridge, U.K., 2000.

[24] P. Blanchini: Set invariance in control, *Automatica*, Vol. 35, pp. 1747–1767, 1999.

[25] D. Amir: Chebyshev centers and uniform convexity, *Pacific J. Math.*, Vol. 77, No. 1, pp. 1–6, 1978.

[26] S. Boyd and L. Vandenberghe: *Convex Optimization*, Cambridge University Press, 2004.

[27] M. Grant and S. Boyd: CVX: Matlab software for disciplined convex programming, version 2.1, [online] http://cvxr.com/cvx, 2017.

[28] M. Grant and S. Boyd: Graph implementations for nonsmooth convex programs, *Recent Advances in Learning and Control*, V. Blondel, S. Boyd, and H. Kimura, Eds., Lecture Notes in Control and Information Sciences, Springer, 2008.

[29] M. Herceg, M. Kvasnica, C.N. Jones, and M. Morari: Multi-parametric toolbox 3.0, *Proc. European Control Conf.*, Zürich, Switzerland, pp. 502–510, 2013.

[30] L. Danzer, B. Grünbaum, and V. Klee: Helly’s theorem and its relatives, *Proc. of Symp. in Pure Math.: Convexity*, Vol. 7, pp. 101–179, Amer. Math. Society, 1963.

[31] K. Fukuda and V. Rost: Combinatorial face enumeration in convex polytopes, *Comput. Geometry*, Vol. 4, No. 4, pp. 191–198, 1994.

[32] K. Fukuda, T.M. Liebling, and F.Margot: Analysis of backtrack algorithms for listing all vertices and all faces of a convex polyhedron, *Comput. Geometry*, Vol. 8, No. 1, pp. 1–12, 1997.

[33] A. Girard, C.L. Guernic, and O. Male: Efficient computation of reachable sets of linear time-invariant systems with inputs, *Hybrid Systems: Computation and Control*, LNCS, Vol. 3927, pp. 257–271, Springer, 2006.

[34] J. Mattingley and S. Boyd: Real-time convex optimization in signal processing, *IEEE Signal Processing Mag.*, Vol. 27, No. 3, pp. 50–61, 2010.

---

### Appendix A Robust Kalman Filter

The robust Kalman filter (robustKF), which is proposed in [34], is robust to sensor failures, measurement outliers, or intentional jamming than the traditional Kalman filter. Consider the following LTI system:

\[
\begin{align*}
  x(k+1) &= Ax(k) + w(k), \\
  y(k) &= Cx(k) + v(k) + d(k),
\end{align*}
\]

where \(x(k) \in \mathbb{R}^n\) is the state and \(y(k) \in \mathbb{R}^m\) is the sensor measurement. As is the case with the traditional Kalman filtering setup, it is assumed that the process noise \(w(k)\) is IID Gaussian variable whose mean is 0 and covariance is \(W\) and the measurement noise \(v(k)\) is also IID Gaussian variable whose mean is 0 and covariance is \(V\). The vector \(d(k)\) indicates an additional disturbance, which is assumed to be sparse. The main difference from the traditional Kalman filter is to obtain the *a posteriori* state estimate \(\hat{x}(k|k)\) using a convex \(\ell_1\) optimization problem. In the robustKF, the state estimate \(\hat{x}(k|k)\) to be the solution of the following convex optimization problem:

\[
\begin{align*}
  \min_{x \in \mathbb{R}_v, v \in \mathbb{R}^m, d \in \mathbb{R}^m} & \quad v^T \Sigma_1^{-1} v + (x - \hat{x}(k|k-1))^T \Sigma^{-1} (x - \hat{x}(k|k-1)) \\
  \text{subject to} & \quad y(k) = Cx + v + d,
\end{align*}
\]

where \(\hat{x}(k|k-1)\) is the *a priori* state estimate which is obtained by \(\hat{x}(k|k-1) = A\hat{x}(k-1|k-1), \lambda > 0\) is a design parameter, and \(\Sigma\) denotes the steady-state error covariance associated with predicting the next step. Thus, we see that the robustKF replaces the standard measurement update as a quadratic minimization problem that includes an \(\ell_1\) terms to take the additional disturbances into account.

---

*Takumi Shinohara*

He received the B.E. and M.E. degrees from Keio University, Tokyo, Japan, in 2016 and 2018, respectively. His research interests include system security and secure state estimation.

*Tofu Namemikawa (Member)*

He received the B.E., M.E., and Ph.D. in electrical and computer engineering from Kanazawa University, Japan, in 1991, 1993, and 1997, respectively. From 1994 until 2002, he was with Kanazawa University as an Assistant Professor. From 2002 until 2005, he was with the Nagaoka University of Technology as an Associate Professor, Niigata, Japan. From 2006 until 2009, he was with Kanazawa University again. In April 2009, he joined Keio University, where he is currently a Professor at Department of System Design Engineering, Keio University, Yokohama, Japan. He held visiting positions at Swiss Federal Institute of Technology in Zurich in 1998, University of California, Santa Barbara in 2001, University of Stuttgart in 2008 and Lund University in 2010. His main research interests are robust control, distributed and cooperative control and their application to power network systems. He is a member of ISIE and IEEE.