Reach Set-based Attack Resilient State Estimation against Omniscient Adversaries

Takumi Shinohara and Toru Namerikawa

Abstract—We consider the problem of secure state estimation in an adversarial environment with the presence of bounded noises. We assume the adversary has the knowledge of the healthy measurements and system parameters. To counteract the dangerous attacker, the problem is given as a min-max optimization, that is, the system operator seeks an estimator which minimizes the worst-case estimation error due to the manipulation by the attacker. On the proposed estimator, the estimation error is bounded at all times even if the system removal of an arbitrary set of $2l$ sensors is not observable, where $l$ is the number of the compromised sensors. To this end, taking the reach set of the system into account, we first show 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. Additionally, the upper bound of the worst-case estimation error is derived theoretically, and we also show a rigorous analytical bound under a certain condition. The attacked sensor identification algorithm is further provided. A simple numerical example finally shows to illustrate the effectiveness of the proposed estimator.

I. 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 are considered as CPS such as transportation, manufacturing, medical devices, and energy systems [1], [2], and each includes networked systems with embedded sensors, actuation, control, 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] and the Maroochy water breach [4]. CPS are particularly difficult to be secure due to a number of factors, e.g., the ability of a malicious third party to operate from anywhere in the world, the linkages between the cyberspace and physical systems, and the difficulty of reducing vulnerabilities in complex networks. 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 [5]–[9]. To be honest, while IoT (Internet of Things) devices have increased, cyber incidents are also increasing, and it is generally difficult to ensure the security for all sensors or devices. Additionally, in safety-critical systems as we mentioned above, it is also difficult to stop the operation immediately even if they subject to malicious attacks. Thus, one another challenge is to operate securely even if in the presence of malicious attacks.

In [10], [11], the authors dealt with the problem of secure state estimation against malicious sensor attacks in linear dynamical systems based on $l_0$ optimization. However, they only considered the case where the system is assumed to be noiseless, which greatly favors for system supervisors since the evolution of the system is deterministic. In [12]–[14], the authors extended the problem into a more realistic case where the system contains noises. They proved that the state can be reconstructed using a finite history of the sensor measurements if the system is observable after the removal of an arbitrary set of $2l$ 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 $2l$ sensors, then the state can be constructed by using all sensory data from time 0 [15]. Also for the static state estimation problem, the paper [16] showed the estimation error is bounded if the system is observable after removing $2l$ sensors.

In this paper, we focus on the secure estimation problem for linear systems with the bounded process and measurement noises. The malicious adversary is assumed to be omniscient, i.e., he/she has the knowledge about the benign measurements and system parameters. Our goal is to construct a resilient estimator where the 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 reach set is computed by the compromised measurement. In essence, the feasible set is given as a union of polytopes and the state estimate minimizing the worst-case error is equivalent to the Chebyshev center (i.e., the center of the minimum volume circumscribing ball) of the union. Then, we show the bound of the worst-case estimation error. In conventional papers [12]–[15], as we mentioned above, the estimation error possibly be unbounded unless the system is observable or detectable after removing an arbitrary set of $2l$ 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. Also, we give an algorithm to identify the compromised sensors.

The rest of this paper is organized as follows: In Section II, we formulate the secure state estimation problem and the resilient estimator. Section III is devoted to designing the estimator, and in Section IV, we provide the upper bound of the worst-case error. The attack identification problem is discussed in Section V. Via a numerical example using an unmanned ground vehicle control in Section VI, we verify the effectiveness of the proposed estimator, and finally in Section VII, we conclude this work.

Notation and Terminology

Let us define $\mathbb{R}$, $\mathbb{R}^+$, and $\mathbb{N}_0$ as the real numbers, positive real numbers, and nonnegative integers, respectively. We use $1_n$ to indicate the $n$-dimensional column vector whose entries are 1. For a vector $x$ and a matrix $A$, let $||x||$, $||x||_\infty$, $\rho(A)$, and $||A||_2$ be the Euclidean norm, infinity norm of the vector, spectral radius, and spectrum norm of the matrix, respectively.

A convex polyhedron in $\mathbb{R}^n$ is defined as $P = \{x \in \mathbb{R}^n : Ax \leq b\}$ for some matrix $A \in \mathbb{R}^{m \times n}$ and vector $b \in \mathbb{R}^m$, while a bounded convex polyhedron is called a polytope. Let $B(c, r) \triangleq \{x \in \mathbb{R}^n : ||x - c|| \leq r\} \subset \mathbb{R}^n$ be a closed ball whose center and radius are, respectively, $c$ and $r$. Setting $c = -b/\gamma$ and $r = 1/\gamma$ for $b \in \mathbb{R}^n$ and $\gamma \in \mathbb{R}^+$, another common representation of the ball is given by

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

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

$$\text{supp}(x) \triangleq \{i : x_i \neq 0\} \subseteq \{1, \ldots, n\},$$

while $\ell_0$ “norm” of a vector $x$ is the cardinality of supp$(x)$, that is, $||x||_0 \triangleq |\text{supp}(x)|$.

II. Problem Formulation

We consider the state estimation problem for the following linear time invariant system subjected to integrity attacks:

$$x(k+1) = Ax(k) + Bu(k) + w(k), \quad x(0) \in \mathcal{X}_0, \tag{2}$$
$$y(k) = Cx(k) + v(k) + y^a(k), \tag{3}$$

where $x(k) \in \mathbb{R}^n$ is the system state, $u(k) \in \mathbb{R}^q$ is the control input, and $y(k) \triangleq [y_1(k), \ldots, y_m(k)]^\top \in \mathbb{R}^m$ 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 $\mathcal{X}_0$ is given as a polytope. Let us define the sensor index set as $\mathcal{S} \triangleq \{1, \ldots, m\}$. 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 $\ell_\infty$ 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,

$$\mathcal{W} \triangleq \{w \in \mathbb{R}^n : ||w||_\infty \leq \delta^w\} \subset \mathbb{R}^n,$$
$$\mathcal{V} \triangleq \{v \in \mathbb{R}^m : ||v||_\infty \leq \delta^v\} \subset \mathbb{R}^m.$$

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, namely $k \in \mathbb{N}_0 \setminus \{\infty\}$. As is the case with the recent work, we assume that the input $u(k)$ is 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 assumptions regarding the malicious attacker.

Assumption 1: The malicious adversary has the knowledge of the system parameters, namely $A, B, C, \delta^w, \delta^v$.

Assumption 2: The benign measurement $Cx(k) + v(k)$ is known to the adversary.

Assumption 3: The adversary can manipulate at most $l$ of the $m$ sensors, i.e., $||y^a(k)||_0 \leq l$, $\forall k \in \mathbb{N}_0$.

We assume that the system supervisor knows how many sensors $l$ are possibly attacked, but cannot identify them. However, it is worth remarking that, whereas some existing results have assumed that the compromised sensor set is fixed, we make no such assumption.

A. Optimal Estimator

Our challenge is to construct a resilient estimator even if the adversary has the knowledge of the system and healthy measurement. Hence, the problem to be discussed is given as follows.

Problem 1: Suppose that Assumptions 1–3 hold, namely assume that the attacker has the knowledge of the system and benign measurement. Under the condition, construct a resilient estimator $f : \mathbb{R}^m \to \mathbb{R}^n$ which satisfies the following:

$$e(k) \triangleq ||x(k) - f(y(k))|| < \infty, \quad \forall k \in \mathbb{N}_0 \setminus \{\infty\}, \tag{4}$$

where $e(k)$ is the estimation error and $\hat{x}(k) \triangleq f(y(k))$ 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 $f^*(k)$ are respectively obtained by

$$e^*(k) = \max_{x(k) \in \mathbb{R}^n} e(k) = \max_{x(k) \in \mathbb{R}^n} ||x(k) - \hat{x}(k)||, \tag{5}$$
$$f^*(k) = \arg \min_{\hat{x}(k)} e^*(k) = \arg \min_{\hat{x}(k)} \max_{x(k) \in \mathbb{R}^n} ||x(k) - \hat{x}(k)||. \tag{6}$$

For deriving the state estimate, we first have the following set [17], [18].

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.,
\[
\mathcal{R}(k) \triangleq \{x \in \mathbb{R}^n : \exists x' \in \mathcal{R}(k-1), u(k-1), w(k-1) \in \mathcal{W}, \text{ such that } x = Ax' + Bu(k-1) + w(k-1)\},
\]
or,
\[
\mathcal{R}(k) \triangleq A\mathcal{R}(k-1) + Bu(k-1) + \mathcal{W},
\]
\[
= A^k \mathcal{X}_0 \oplus \sum_{j=0}^{k-1} A^{k-1-j} Bu(j) \oplus \bigoplus_{j=0}^{k-1} A^{k-1-j} \mathcal{W}. \quad (7)
\]

We note that the reach set is given as a polytope since \(\mathcal{X}_0\) and \(\mathcal{W}\) are polytopes. For the subsequent analysis, we use a matrix \(H(k)\) and a vector \(c(k)\) configuring the reach set \(\mathcal{R}(k)\):
\[
\mathcal{R}(k) = \{x \in \mathbb{R}^n : H(k)x \leq c(k)\}. \quad (8)
\]
Taking into account that the state at time \(k\) belongs the reach set \(\mathcal{R}(k)\), the set of feasible state that can generate the compromised measurement \(y(k)\) is given as
\[
\mathcal{X}(k) \triangleq \{x \in \mathcal{R}(k) : \exists v(k) \in \mathcal{V} \text{ such that } \|y^m(k)\|_0 \leq l \text{ and } y(k) = Cx + v(k) + y^a(k)\}. \quad (9)
\]
Revisiting the worst-case error and optimal estimate, they can be rewritten as follows by using the feasible set \(\mathcal{X}(k)\):
\[
e^*(k) = \max_{x(k) \in \mathcal{X}(k)} e(k) = \max_{x(k) \in \mathcal{X}(k)} \|x(k) - \hat{x}(k)\|, \quad (10)
\]
\[
f^*(k) = \arg \min_{\hat{x}(k)} e^*(k) = \arg \min_{\hat{x}(k)} \max_{x(k) \in \mathcal{X}(k)} \|x(k) - \hat{x}(k)\|. \quad (11)
\]
which implies the optimal estimate is equivalent to the Chebyshev center (i.e., the center of the minimum volume circumscribing ball) of the set \(\mathcal{X}(k)\) and the worst-case error is the Chebyshev radius (i.e., the radius of the ball). Here, the Chebyshev center and radius of a bounded set \(\mathcal{X}\) are defined as follows as \(c(\mathcal{X})\) and \(r(\mathcal{X})\), respectively [19]:
\[
\rho(x, \mathcal{X}) \triangleq \min_{r \in \mathbb{R}^+: r \geq B(x, r)}, \quad (12)
\]
\[
c(\mathcal{X}) \triangleq \arg \min_{x \in \mathbb{R}^n} \rho(x, \mathcal{X}), \quad (13)
\]
\[
r(\mathcal{X}) \triangleq \min_{x \in \mathbb{R}^n} \rho(x, \mathcal{X}). \quad (14)
\]

Accordingly, we have \(f^*(k) = c(\mathcal{X}(k))\) and \(e^*(k) = r(\mathcal{X}(k))\). Hence, in order to obtain the optimal feasible state \(f^*(k)\), 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.

**III. Estimator Design**

For an index set \(\mathcal{I} \triangleq \{i_1, \ldots, i_j\} \subseteq \mathcal{S}\), let us define the complement set \(\mathcal{I}^c\) as \(\mathcal{I}^c \triangleq \mathcal{S} \setminus \mathcal{I}\). Moreover, define a subspace \(\mathcal{L}_I\) as \(\mathcal{L}_I \triangleq \text{span}(e_{i_1}, \ldots, e_{i_j})\), where \(e_i \in \mathbb{R}^m\) is the \(i\)th vector of the canonical basis of \(\mathbb{R}^m\) and \(\text{span}(e_{i_1}, \ldots, e_{i_j}) \triangleq \{a_1 e_{i_1} + \cdots + a_j e_{i_j} : a_1, \ldots, a_j \in \mathbb{R}\} \).

\(^2\)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 abbreviate it as \(\mathcal{X}(k)\).

Based on \(\mathcal{L}_I\), we define the following set:
\[
\mathcal{X}_I(k) \triangleq \{x \in \mathcal{R}(k) : \exists v(k) \in \mathcal{V}, y^m(k) \in \mathcal{L}_{I^c}, \text{ such that } y(k) = Cx + v(k) + y^a(k)\}, \quad (15)
\]
which represents all possible states which generates the measurement \(y(k)\) when the sensors in the index set \(\mathcal{I}\) are benign and the sensors in \(\mathcal{I}^c\) are attacked. Thus, one can derive that
\[
\mathcal{X}(k) = \bigcup_{|\mathcal{I}|=m-l} \mathcal{X}_I(k). \quad (16)
\]

For an index set \(\mathcal{I} \triangleq \{i_1, \ldots, i_j\} \subseteq \mathcal{S}\), we define
\[
\mathcal{C}_I \triangleq \begin{bmatrix} C_{i_1} \\ \vdots \\ C_{i_j} \end{bmatrix} \in \mathbb{R}^{l \times n}, \quad \mathcal{V}_I(k) \triangleq \begin{bmatrix} v_{i_1}(k) \\ \vdots \\ v_{i_j}(k) \end{bmatrix} \in \mathbb{R}^l, \quad (17)
\]
\[
y_I(k) \triangleq \begin{bmatrix} y_{i_1}(k) \\ \vdots \\ y_{i_j}(k) \end{bmatrix} \in \mathbb{R}^l, \quad \mathcal{Y}_I(k) \triangleq \begin{bmatrix} y_{i_1}^a(k) \\ \vdots \\ y_{i_j}^a(k) \end{bmatrix} \in \mathbb{R}^l, \quad (18)
\]
which implies that the selecting rows of each matrix with indices in \(\mathcal{I}\). By the definition of \(\mathcal{X}_I(k)\), since \(y^m(k) \in \mathcal{L}_{I^c}\) indicates \(y_I^m(k) = 0\), \(x(k) \in \mathcal{X}_I(k)\) is equivalent to that there exists \(v_I(k)\) such that \(y_I(k) = C_I x(k) + v_I(k)\) and \(\|v_I(k)\|_\infty \leq \delta^v\). Thus, we must have
\[
\|v_I(k)\|_\infty = \|y_I(k) - C_I x(k)\|_\infty \leq \delta^v, \quad (19)
\]
which implies that \(\mathcal{X}_I(k)\) is calculated by
\[
\mathcal{X}_I(k) = \{x \in \mathcal{R}(k) : \|y_I(k) - C_I x\|_\infty \leq \delta^v\}. \quad (20)
\]

This can be written as the following using a matrix \(M_I \triangleq [I - I^T] \in \mathbb{R}^{2|\mathcal{I}| \times |\mathcal{I}|}\):
\[
\mathcal{X}_I(k) = \{x \in \mathcal{R}(k) : M_I (y_I(k) - C_I x) \leq \delta^v \mathbf{1}_{|\mathcal{I}|}\} = \{x \in \mathcal{R}(k) : -M_IC_I x \leq \delta^v \mathbf{1}_{|\mathcal{I}|} - M_I y_I(k)\}, \quad (21)
\]
which indicates that \(\mathcal{X}_I(k)\) is given as a polytope. Exploiting the matrix \(H(k)\) and the vector \(c(k)\), we can rewrite the polytope as
\[
\mathcal{X}_I(k) = \{x \in \mathbb{R}^n : \begin{bmatrix} -M_IC_I \\ H(k) \end{bmatrix} x \leq \begin{bmatrix} \delta^v \mathbf{1}_{|\mathcal{I}|} - M_I y_I(k) \\ c(k) \end{bmatrix}\}. \quad (22)
\]

In order to calculate the optimal state estimate (i.e., the Chebyshev center of \(\mathcal{X}_I(k)\)), we have to obtain the circumscribing ball of the set \(\mathcal{X}(k)\). For a bounded set \(\mathcal{X} \subset \mathbb{R}^n\) which has nonempty interior, it is well known that the minimum volume ellipsoid that covers \(\mathcal{X}\) called Löwner-John ellipsoid is computed by the following optimization problem [20]:
\[
\min_{\Phi \in \mathbb{R}^{n \times n}, b \in \mathbb{R}^n} \log \det \Phi^{-1} \quad \text{subject to } \sup_{x \in \mathcal{X}} \|\Phi x + b\| \leq 1, \quad (23)
\]
where there is an implicit constraint $\Phi > 0$. Consequently, the Löwner-John ellipsoid of the set $\mathcal{X}$ is given, using the minimizers of above optimization problem, by the following:

$$\mathcal{E}_{LJ} \triangleq \{ x \in \mathbb{R}^n : \| \Phi x + b \| \leq 1 \}. \quad (21)$$

Since we now want to calculate a minimum volume ball that covers $\mathcal{X}$, the matrix $\Phi$ in above equation is interpreted as an identity matrix $I$. Remembering equation (1), hence, the minimum volume ball $B(-b/\gamma, 1/\gamma)$ that covers $\mathcal{X}$ is computed by

$$\min_{\gamma \in \mathbb{R}^+, b \in \mathbb{R}^n} \gamma \quad \text{subject to} \quad \sup_{x \in \mathcal{X}} \| \gamma x + b \| \leq 1. \quad (22)$$

Evaluating the constraint function (22), however, involves solving a convex maximization problem, and is not tractable. As aforementioned before, $\mathcal{X}_2(k)$ is given as a polytope and the feasible set $\mathcal{X}(k)$ is given as a union of polytopes. Taking the fact that every polytope is the convex hull of its vertices [21] into account, therefore, we only have to consider the vertices of each polytope $\mathcal{X}_2(k)$ to calculate the minimum volume circumscribing ball of $\mathcal{X}(k)$. Thus, one can calculate the optimal state estimate as

$$\min_{\gamma(k) \in \mathbb{R}^+, b(k) \in \mathbb{R}^n} \gamma(k) \quad \text{subject to} \quad \| \gamma(k) v + b(k) \| \leq 1, \forall v \in \mathcal{V}(k), \quad (23)$$

where $\mathcal{V}(k) \triangleq \bigcup_{|I| = m-l} \mathcal{V}_{X_2}(k)$ and $\mathcal{V}_{X_2}(k)$ is the vertex set of $\mathcal{X}_2(k)$. Using the minimizers of (23), the optimal state estimate can be derived as $f^*(k) = -b(k)/\gamma(k)$. Note that $\mathcal{V}(k)$ is not always the vertex set of $\mathcal{X}(k)$ 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 explains the Chebyshev ball of $\mathcal{X}(k)$, and the vertex set is obviously a subset of $\bigcup_{|I| = m-l} \mathcal{V}_{X_2}(k)$. Consequently, the optimal state estimate can be computed as Algorithm 1.

All the calculation regarding polytopes discussed in this section such as affine map, Minkowski sum, and vertex enumeration are easily implemented using existing computational geometry software packages. The reader is referred to [22]–[24] and the literature on computational geometry for details.

**Algorithm 1** Calculate a state estimate minimizing worst-case error

**Require:** $y(k), l, A, C, H(k), c(k), M_I, \delta^w$

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

1. Compute $C_I$ and $y_I$ for all $|I| = m-l$.
2. Compute the feasible set $\mathcal{X}_2(k)$ for all $|I| = m-l$ as (19) and enumerate its vertices $\mathcal{V}_{X_2}(k)$.
3. Obtain the vertex set $\mathcal{V}(k)$ as $\mathcal{V}(k) = \bigcup_{|I| = m-l} \mathcal{V}_{X_2}(k)$.
4. Compute the optimization problem (23) and obtain $\gamma(k)$ and $b(k)$.
5. **return** $f^*(k) = -b(k)/\gamma(k)$.

**IV. Estimation Bound**

This section is devoted to providing a bound on the estimation error of the estimator proposed in the previous section. The following theorem provides the bounds of the worst-case estimation error $e^*(k)$.

**Theorem 1:** Define $\mathcal{V}(\mathcal{R}(k))$ as the vertex set of $\mathcal{R}(k)$ and suppose that Assumptions 1–3 hold. Regarding the worst-case estimation error $e^*(k)$, we have

$$e^*(k) \leq \frac{1}{\gamma(\mathcal{R}(k))}, \quad \forall k \in \mathbb{N}_0 \setminus \{\infty\}, \quad (24)$$

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

$$\min_{\gamma(\mathcal{R}(k)) \in \mathbb{R}^+, b(\mathcal{R}(k)) \in \mathbb{R}^n} \gamma(\mathcal{R}(k)) \quad \text{subject to} \quad \| \gamma(\mathcal{R}(k)) v + b(\mathcal{R}(k)) \| \leq 1, \forall v \in \mathcal{V}(\mathcal{R}(k)). \quad (25)$$

If for all index sets $\mathcal{K} \subset \mathcal{S}$ with cardinality $m-2l$, $C_{\mathcal{K}}$ has full column rank, then $e^*(k)$ has a rigorous bound as follows:

$$e^*(k) \leq \max_{|\mathcal{K}| = m-2l} \frac{\delta^w}{\sqrt{2 m n p (F_{\mathcal{K}}^{-1})}}, \quad \forall k \in \mathbb{N}_0 \setminus \{\infty\}, \quad (26)$$

where $F_{\mathcal{K}} \triangleq C_{\mathcal{K}}^T C_{\mathcal{K}}$.

**Proof:** One can derive (26) using the same line of argument of [16, Theorem 2]. Due to space limitation, details are omitted.

Then, we tackle to obtain (24). Suppose here that there exists an index set $\mathcal{K}$ with cardinality $m-2l$ such that $C_{\mathcal{K}}$ is not full column rank. Using a pair of index sets $\mathcal{I}$ and $\mathcal{J}$ whose cardinalities are $m-l$, $\mathcal{K}$ is defined as

$$\mathcal{K} = \mathcal{I} \cap \mathcal{J} = \mathcal{S} \setminus \left( \mathcal{I}^c \cup \mathcal{J}^c \right). \quad (27)$$

Then, for any point $x^1(k) \in \mathcal{X}_I(k)$ and $x^2(k) \in \mathcal{X}_J(k)$, we have

$$C_{\mathcal{K}} x^1(k) + v^1(k) + y^{a1}(k) = C_{\mathcal{K}} x^2(k) + v^2(k) + y^{a2}(k),$$

where $\| v^1(k) \|_\infty \leq \delta^w$, $\| v^2(k) \|_\infty \leq \delta^w$, $y^{a1}(k) \in \mathcal{L}_{\mathcal{I}^c}$, and $y^{a2}(k) \in \mathcal{L}_{\mathcal{J}^c}$. Since both $y^{a1}(k)$ and $y^{a2}(k)$ have zero entries on the $i$th entry, where $i \in \mathcal{K}$, we have

$$C_{\mathcal{K}} (x^1(k) - x^2(k)) = v^1_{\mathcal{K}}(k) - v^2_{\mathcal{K}}(k). \quad (28)$$

If $C_{\mathcal{K}}$ is not full column rank, then we know that $C_{\mathcal{K}}$ is not injective and $\ker C_{\mathcal{K}} \neq \{0\}$, i.e., there exists a nonzero vector $x$ which satisfies $C_{\mathcal{K}} x = 0$. By (28), for any $y^{a1}(k) \in \mathcal{L}_{\mathcal{I}^c}$, $y^{a2}(k) \in \mathcal{L}_{\mathcal{J}^c}$ and $v^1 = v^2 = 0 \in \mathcal{V}$, we have

$$C_{\mathcal{K}} (x^1(k) - x^2(k)) = v^2_{\mathcal{K}}(k) - v^1_{\mathcal{K}}(k) = 0. \quad (29)$$

Thus, if the reach set of $x^1(k), x^2(k)$ is unbounded, then there exist unbounded states satisfying (29) and the diameter of $\mathcal{X}(k)$ is also unbounded. In this paper, we consider the reach set of the state, and hence the diameter of $\mathcal{X}(k)$ is equivalent to one of $\mathcal{R}(k)$, and we have $e^*(k) \leq r(\mathcal{R}(k))$.

Defining the vertex set of $\mathcal{R}(k)$ as $\mathcal{V}(\mathcal{R}(k))$, $r(\mathcal{R}(k))$ is given as the Chebyshev radius of $\mathcal{V}(\mathcal{R}(k))$. Thus, the optimization
problem (25) provides the minimum circumscribing ball and we have \( r(R(k)) = 1 = R(k) \). Therefore, if there exists an index set \( \mathcal{K} \) with cardinality \( m - 2l \) such that \( C_\mathcal{K} \) is not full column rank (24) pertaining to the bound of estimation error is derived.

According to this theorem, we find that the proposed estimator satisfies (4) even if the adversary has the knowledge of the system parameters and the benign measurement, namely it is a resilient one.

**V. Attacked Sensor Identification**

One another challenge for the secure operation is to identify the compromised sensors. In this section, hence, we tackle the attacked sensor identification problem. Assume that the attacker injects a large bias \( y^a(k) \) to the system. Regarding the indices \( \{i_1, \ldots, i_l\} = \text{supp}(y^a(k)) \), then, the subset of the resulting measurements \( \{y_{i_1}(k), \ldots, y_{i_l}(k)\} \) is also a large one. Then, pertaining to a index set \( \mathcal{I} \) with cardinality \( m - l \) which contains the indices \( \{i_1, \ldots, i_l\} \), the following set of the feasible state which does not consider the reach set \( R(k) \) cannot be contained in the reach set since the obtained measurement is large:

\[
\mathcal{X}_\mathcal{I}(k) = \{ x \in \mathbb{R}^n : -M_TG_Tx \leq \delta^v \mathbf{1}_{2|\mathcal{I}|} - M_Ty_T(k) \}.
\]

If the set \( \mathcal{X}_\mathcal{I}(k) \) is not contained the reach set \( R(k) \), then the feasible set (19) will be \( \mathcal{X}_\mathcal{I}(k) = \emptyset \). In other words, the emptiness of the set \( \mathcal{X}_\mathcal{I}(k) \) indicates that some sensors in \( \mathcal{I} \) are compromised. Therefore, by checking the emptiness of the set \( \mathcal{X}_\mathcal{I}(k) \) for all \( |\mathcal{I}| = m - l \), we are able to identify the compromised sensors.

Before continuing on, we give Farkas’ lemma which states a solvability of a linear inequality.

**Lemma 1 (Farkas’ lemma [21, Proposition 1.7]):** Let \( H \in \mathbb{R}^{m \times n} \) and \( c \in \mathbb{R}^m \). A system \( Hx \leq c \) has no solution if and only if there exists a vector \( z \geq 0 \) such that \( z^\top H = 0 \) and \( z^\top c = -1 \).

According to Farkas’ lemma, regarding a given region \( P = \{ x \in \mathbb{R}^n : Hx \leq c \} \), if there exists a vector such that \( z^\top H = 0 \) and \( z^\top c = -1 \), then we know that \( P = \emptyset \). Thus, one can realize that the set \( \mathcal{X}_\mathcal{I}(k) \) is empty or not by calculating the following optimization problem:

\[
F = \min_z z^\top \left[ \delta^v \mathbf{1}_{2|\mathcal{I}|} - M_Ty_T(k) \right] c(k)
\]

subject to

\[
\begin{align*}
& z^\top \left[ -M_TG_T \right] = 0, \\
& z^\top \left[ \delta^v \mathbf{1}_{2|\mathcal{I}|} - M_Ty_T(k) \right] c(k) \geq -1, \\
& z \geq 0.
\end{align*}
\]

(30)

If the calculated result satisfies \( F = -1 \), then \( \mathcal{X}_\mathcal{I}(k) = \emptyset \), which indicates that some sensors in the index set \( \mathcal{I} \) are compromised. For the convenience, defining index sets \( \mathcal{I}_1, \ldots, \mathcal{I}_r \) such that \( \mathcal{X}_{\mathcal{I}_1} = \cdots = \mathcal{X}_{\mathcal{I}_r} = \emptyset \), the attacked sensors set can be identified as \( \mathcal{I}_1 \cap \cdots \cap \mathcal{I}_r \). Thus, by calculating above optimization problem for all \( \mathcal{I} \) with cardinality \( m - l \), we are able to know which sensor subsets are compromised.

**Remark 1:** From the viewpoint of the attackers, they should not inject a large bias to the system since the attack is possibly identified/detected. The attack should be designed to be taken into account the noise bounds. In other words, the attack should be constructed to be regarded as part of noises. Needless to say, however, the attack designed as this does not degrade the system enough.

**VI. Numerical Example**

This section devotes to show the results of a numerical simulation to verify the effectiveness of the proposed estimator. Borrowing from [14], we use an unmanned ground vehicle (UGV) model for the example. We assume that the UGV moves along straight lines and completely stops in initial state. Under these assumptions, the system dynamics of the UGV is given as

\[
\begin{bmatrix}
\dot{p} \\
\dot{\mu}
\end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -B & 1 \end{bmatrix} \begin{bmatrix} p \\ \mu \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u + w,
\]

where \( p, \mu, \) and \( u \) are the UGV position, its velocity, and the force inputted to the UGV, respectively. The process noise is represented as \( w \). The parameters \( M \) and \( B \) are respectively the mechanical mass and the translational friction coefficient.

We assume that the output equation is given as

\[
y = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} p \\ \mu \end{bmatrix} + v + y^a,
\]

where \( v \) is the measurement noise and \( y^a \) is the attack vector. In this example, we set \( M = 0.8 \text{ kg}, B = 1 \), and \( \delta^v = \delta^v = 0.2 \) and discretize the model with 0.1 sec.

In this example, we demonstrate various attack scenarios. Fig. 1 shows the bias injected by the malicious attacker, where he/she first corrupts the 2nd sensor with a random noise, and then he/she asserts a replay attack to the 1st sensor. The attacker finally adds a monotonically increasing signal to the 1st sensor again. Note that the number of compromised sensor is always 1, namely \( l = 1 \), and is known to the defender.

Figs. 2 and 3 show the estimation results regarding the UGV position and its velocity, respectively. For the comparison, we use the \( H_\infty \) filter and robust Kalman filter (robust KF), which is robust to sensor failures, measurement outliers, or intentional sparse jamming proposed in [25]. As shown in both figures, the proposed algorithm outperforms than the \( H_\infty \) and robust KF, namely the proposed algorithm is able to estimate the system state in an adversarial environment more accurately. In particular, it is worth remarking that the proposed estimator achieves the accurate estimation in the condition that 1st sensor is compromised (2nd and 3rd attack scenarios), where the removed system is not observable. Also, we can confirm the estimation error in the proposed method, which is depicted in Fig. 4, is low enough compared with the \( H_\infty \) filter and robust KF.
Fig. 1. Attack signals on the sensors
Fig. 2. Estimated position
Fig. 3. Estimated velocity
Fig. 4. Estimation error

VII. CONCLUSION

In this paper, we discussed the secure estimation problem in the presence of the sensor attacks. The adversary is assumed to be an omniscient, that is, he/she has the knowledge of the system and the healthy measurement, and we have tackled to design a resilient state estimator against such attackers. 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 union. We also provided the bound of the worst-case error and attacked sensor identification algorithm. 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 sensor subsets.

ACKNOWLEDGMENT

The authors would like to thank Professor Zhihua Qu for fruitful discussion and his valuable comments.

REFERENCES