2015 European Control Conference (ECC)
July 15-17, 2015. Linz, Austria

# Secure and Robust State Estimation under Sensor Attacks, Measurement Noises, and Process Disturbances: Observer-Based Combinatorial Approach

Chanhwa Lee, Hyungbo Shim, and Yongsoon Eun

*Abstract*— **This paper presents a secure and robust state estimation scheme for continuous-time linear dynamical systems. The method is secure in that it correctly estimates the states under sensor attacks by exploiting sensing redundancy, and it is robust in that it guarantees a bounded estimation error despite measurement noises and process disturbances. In this method, an individual Luenberger observer (of possibly smaller size) is designed from each sensor. Then, the state estimates from each of the observers are combined through a scheme motivated by error correction techniques, which results in estimation resiliency against sensor attacks under a mild condition on the system observability. Moreover, in the state estimates combining stage, our method reduces the search space of a minimization problem to a finite set, which substantially reduces the required computational effort.**

## I. Introduction

Recent advances in computers and communications have enabled feedback control technology to address more sophisticated and complex problems of large-scale. For example, heterogeneous multi-agent systems are frequently encountered [1], decentralized and distributed control algorithms are developed [2], and large-scale traffic control is addressed using wireless sensor network [3]. As this trend prevails, the resulting systems that integrate computers, controls, and communication networks are now more exposed and can be vulnerable to malicious attacks. Indeed, attacks on systems that involve feedback controllers took place in reality [4], [5], [6], and may lead to catastrophic disruptions in critical infrastructure [6]. Therefore, resiliency of control systems under malicious attacks has become one of the critical system design considerations and is actively studied [7], [8], [9].

In this paper, we consider attacks on sensors of feedback control systems, and present a secure and robust state estimation scheme for continuous-time linear dynamical systems. The method is secure in that it correctly estimates the states under sensor attacks by exploiting sensing redundancy, and it is robust in that it guarantees a bounded estimation error despite measurement noises and process disturbances.

We consider linear dynamical systems with multiple outputs and design a Luenberger observer for each output. Then, we combine the state estimates from each of the observers through a scheme motivated by error correction techniques. We formulate the problem such that the error correcting method (like in [10] and [11]) is applicable to combine multiple state estimates from each of the observers. Specifically, the state estimates from a bank of observers are stacked to form a higher dimensional column vector, and an error correcting method, tailored to this specially structured vector, is used to achieve attack-resiliency. It is shown that the resiliency, or error correctability, arises from the redundancy of observability.

In the stage of combining state estimates, an $\ell_0$ minimization problem arises from error correction techniques. By adopting a combinatorial approach [12] and modifying it based on observers, our method substantially reduces the required computational effort to solve the minimization problem.

Additionally, the effect of bounded measurement noises and process disturbances on state estimation is analyzed. A method of calculating the bound on state estimation errors is provided, and the error bound turns out to be proportional to the bounds on noises and disturbances.

It should be pointed out that fault tolerant control [13] can be viewed as closely related to resiliency. However, the fault tolerant control mainly focuses on reliability from internal non-colluding faults while the attack resilient control deals with external malicious attacks which act in a coordinated way and is sometimes stealthy [14]. Physical redundancy approach has been used where redundant components are introduced along with majority voting logic [15], [16]. Functional redundancy approach has also been exploited, which includes state observer [17], Kalman filter [18], parameter estimation [19], threshold logic [20], and statistical decision theory [18]. The idea of employing a bank of observers is motivated by [21] and [22], in which it is used for detecting mode-switching and estimating state variables in switched dynamical systems.

The error correcting problem, which we use to combine estimates from a bank of observers, can be transformed to a problem of reconstructing sparse vectors [23]. Sparse signal recovery technique is one of the main concerns in compressed sensing (CS) literature [24], [25]. There are three main algorithmic approaches to sparse signal recovery: geometric, greedy, and combinatorial. The geometric algorithm uses linear programming techniques by recasting the $\ell_0$ minimization problem into a convex optimization

This work was supported by ICT R&D program of MSIP/IITP Grant number 14-824-09-013, Resilient Cyber-Physical Systems Research, and in part by the Brain Korea 21 Plus Project in 2015.

C. Lee and H. Shim are with ASRI, Department of Electrical and Computer Engineering, Seoul National University, Korea. chlee@cdsl.kr, hshim@snu.ac.kr

Y. Eun is with Department of Information & Communication Engineering, Daegu Gyeongbuk Institute of Science & Technology, Korea. yeun@dgist.ac.kr

978-3-9524269-3-7 ©2015 EUCA

problem [23]. Greedy algorithm iteratively approximates the signal coefficients [26]. Combinatorial approach identifies a subset of anomalous elements by investigating all possible combinations [12].

Motivated by the considerable work in CS, fundamental studies on state recovery of discrete-time linear time invariant (LTI) systems under attacks, have been carried out recently [27], [28], [29]. Basic concepts regarding this problem are introduced and characterized in [27] and the geometric approach is adopted to solve the problem, however, it can not guarantee real time estimation. Bounded noises, disturbances, and modeling errors are considered in [28] and the state estimation error is analyzed, but an explicit error bound is not given. Reference [29] proposes an event-triggered projected gradient descent algorithm which is a kind of iterative greedy algorithm with additional restrictive conditions.

Compared to [27]–[29], we take an observer-based combinatorial approach, and computational burden is much lessened by reducing the search space of an optimization problem to a finite set. Moreover, a bound on estimation error is explicitly derived from system parameters. We formulate the problem for continuous-time dynamics in this paper for convenience.

The rest of the paper is organized as follows. Section II introduces the notation used throughout the paper and the problem formulation. In Section III, the static error correcting problem for both noiseless and noisy situations, is considered. We then design individual observers using the Kalman observability decomposition, and the overall estimation scheme is presented in Section IV. Finally, simulation results are given in Section V and we provide concluding remarks in Section VI.

## II. Preliminaries

### A. Notation

In this subsection, we summarize the notation used throughout the paper. The subset of natural numbers, $\{1, 2, \cdots, \mathsf{p}\} \subset \mathbb{N}$, is denoted by $[\mathsf{p}]$. The cardinality of a set $S$ is denoted by $|S|$ and the support of a vector $v \in \mathbb{R}^{\mathsf{p}}$ is defined as $\mathsf{supp}(v) := \{\mathsf{i} \in [\mathsf{p}] : v_{\mathsf{i}} \neq 0\}$ where $v_{\mathsf{i}}$ is the i-th element of $v$. The cardinality of $\mathsf{supp}(v)$ defines the $\ell_0$ norm[1] of a vector $v$, i.e., $\|v\|_0 := |\mathsf{supp}(v)|$. A vector $v$ is said to be q-sparse when it holds that $\|v\|_0 \leq \mathsf{q}$, and a set $\Sigma_{\mathsf{q}} := \{v \in \mathbb{R}^{\mathsf{p}} : \|v\|_0 \leq \mathsf{q}\}$ denotes the set of all q-sparse vectors.

Assume that a vector $v \in \mathbb{R}^{\mathsf{p}}$ and a subset $\Lambda \subset [\mathsf{p}]$ of indices are given. By $v_\Lambda \in \mathbb{R}^{\mathsf{p}}$, it is meant that $v_\Lambda$ is obtained by setting the elements of $v$ indexed by $\Lambda^c := \{\mathsf{i} \in [\mathsf{p}] : \mathsf{i} \notin \Lambda\}$ to zero. Similar notation is used for a matrix $M \in \mathbb{R}^{\mathsf{p}\times\mathsf{n}}$. The matrix obtained by setting the rows of $M$ indexed by $\Lambda^c$ to zero, is denoted as $M_\Lambda \in \mathbb{R}^{\mathsf{p}\times\mathsf{n}}$. Sometimes the notation will be abused to imply $v_\Lambda \in \mathbb{R}^{|\Lambda|}$ (or $M_\Lambda \in \mathbb{R}^{|\Lambda|\times\mathsf{n}}$) which is the vector $v$ (or the matrix $M$) whose elements (or rows) not corresponding to the index set $\Lambda$ are actually eliminated.

Several special notations are also used for a stacked vector $x \in \mathbb{R}^{\mathsf{np}}$. For a given index $\mathsf{i} \in [\mathsf{p}]$, the index set $\{\mathsf{n}(\mathsf{i}-1)+1, \mathsf{n}(\mathsf{i}-1)+2, \cdots, \mathsf{ni}\}$ is denoted as $\Gamma_{\mathsf{i}}^{\mathsf{n}}$. Similarly to an index set $\Lambda \subset [\mathsf{p}]$, the index set $\bigcup_{\mathsf{i}\in\Lambda} \Gamma_{\mathsf{i}}^{\mathsf{n}} \subset [\mathsf{np}]$ is denoted as $\Lambda^{\mathsf{n}}$. A stacked vector $x \in \mathbb{R}^{\mathsf{np}}$ of length np can be split into p column vectors of length n, i.e., $x = \begin{bmatrix} x_1^{\mathsf{n}\top} & x_2^{\mathsf{n}\top} & \cdots & x_{\mathsf{p}}^{\mathsf{n}\top}\end{bmatrix}^\top \in \mathbb{R}^{\mathsf{np}}$, where $x_{\mathsf{i}}^{\mathsf{n}} \in \mathbb{R}^{\mathsf{n}}$ represent the i-th split column vector of length n in $x$. With the index set $\Gamma_{\mathsf{i}}^{\mathsf{n}}$ defined above, it follows that $x_{\mathsf{i}}^{\mathsf{n}} = x_{\Gamma_{\mathsf{i}}^{\mathsf{n}}} \in \mathbb{R}^{\mathsf{n}}$. The (n-stacked) support of $x \in \mathbb{R}^{\mathsf{np}}$ is defined as $\mathsf{supp}^{\mathsf{n}}(x) := \{\mathsf{i} \in [\mathsf{p}] : x_{\mathsf{i}}^{\mathsf{n}} \neq 0_{\mathsf{n}\times 1}\}$ and its cardinality defines the (n-stacked) $\ell_0$ norm of $x$, i.e., $\|x\|_{0^{\mathsf{n}}} := |\mathsf{supp}^{\mathsf{n}}(x)|$. Similarly to the usual vector case, a stacked vector $x$ is said to be (n-stacked) q-sparse when it holds that $\|x\|_{0^{\mathsf{n}}} \leq \mathsf{q}$, and a set $\Sigma_{\mathsf{q}}^{\mathsf{n}} := \{x \in \mathbb{R}^{\mathsf{np}} : \|x\|_{0^{\mathsf{n}}} \leq \mathsf{q}\}$ denotes the set of all (n-stacked) q-sparse vectors. If it is clear from the context that the vector taken into consideration is a stacked vector, we omit the term "n-stacked".

### B. Problem Formulation

Among various attack scenarios [14], we consider false data injection attacks on sensors and the plant is given by

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

where $x(t) \in \mathbb{R}^{\mathsf{n}}$ is the states, $u(t) \in \mathbb{R}^{\mathsf{m}}$ is the inputs, and $y(t) \in \mathbb{R}^{\mathsf{p}}$ is the measured outputs. In addition, $d(t) \in \mathbb{R}^{\mathsf{n}}$ is the process disturbances, $n(t) \in \mathbb{R}^{\mathsf{p}}$ is the measurement noises, and $a(t) \in \mathbb{R}^{\mathsf{p}}$ is the errors injected by adversarial attacks. The measurement of the i-th sensor at time $t$, denoted by $y_{\mathsf{i}}(t)$, is corrupted by both the noise $n_{\mathsf{i}}(t)$ and the attack $a_{\mathsf{i}}(t)$. We pose conditions on noises, disturbances, and attacks given as follows.

**Assumption 1:** The process disturbance $d$ and each measurement noise $n_{\mathsf{i}}$ for $\mathsf{i} \in [\mathsf{p}]$ are uniformly bounded, i.e.,

$$\|d(t)\|_2 \leq d_{\max}, \quad \|n_{\mathsf{i}}(t)\|_2 \leq n_{\max}, \quad {}^\forall t \geq 0. \qquad \Diamond$$

**Assumption 2:** The attack vector $a(t)$ is q-sparse, i.e., $a(t) \in \Sigma_{\mathsf{q}}$ for all $t$. More precisely, there exists an index set $\Omega \subset [\mathsf{p}]$ such that $\mathsf{supp}(a(t)) \subset \Omega$ for $t \geq 0$ and $|\Omega| \leq \mathsf{q}$. $\Diamond$

Assumption 2 implies that the adversary can compromise only a subset of sensors possibly with arbitrary attack values.

The objective of this paper is to estimate the state $x(t)$ of the given system (1) under Assumptions 1 and 2.

## III. Static Error Correction over Reals

This section considers an error correcting problem over real numbers when the signals are constant. Throughout this section, we will consider an (n-stacked) vector $\hat{z} \in \mathbb{R}^{\mathsf{np}}$ unless otherwise mentioned. Given a matrix $\Phi \in \mathbb{R}^{\mathsf{np}\times\mathsf{n}}$, we want to recover a vector $x \in \mathbb{R}^{\mathsf{n}}$ from measurements

$$\hat{z} = \Phi x + v + e \in \mathbb{R}^{\mathsf{np}} \tag{2}$$

which are corrupted by noise $v$ and error $e$. The matrix $\Phi$ is called a *coding matrix*, $v \in \mathbb{R}^{\mathsf{np}}$ is a vector of bounded

[1]Strictly speaking, $\ell_0$ "norm" is not a norm in the mathematical sense because it does not satisfy the absolute homogeneity of norm properties. However, it is conventionally called "norm" abusing terminology.

noises, and $e \in \mathbb{R}^{\mathsf{np}}$ denotes an arbitrary and unknown vector of sparse errors.

### *A. Noise-Free Signal Recovery*

In this subsection, let us assume that $v = 0_{\mathsf{np}\times 1}$ in (2). The following notion of correctability can now be introduced.

**Definition 1:** A coding matrix $\Phi \in \mathbb{R}^{\mathsf{np}\times\mathsf{n}}$ is said to be *(*$\mathsf{n}$*-stacked)* $\mathsf{q}$*-error correctable* if for all $x_1, x_2 \in \mathbb{R}^{\mathsf{n}}$ and $e_1, e_2 \in \Sigma^{\mathsf{n}}_{\mathsf{q}}$, $\Phi x_1 + e_1 = \Phi x_2 + e_2$ implies $x_1 = x_2$. $\Diamond$

We now give an equivalent condition which characterizes the error correctability of the matrix $\Phi$.

**Lemma 1:** The matrix $\Phi \in \mathbb{R}^{\mathsf{np}\times\mathsf{n}}$ is ($\mathsf{n}$-stacked) $\mathsf{q}$-error correctable if and only if $\Phi_{\Lambda^{\mathsf{n}}}$ has full column rank for every set $\Lambda \subset [\mathsf{p}]$ satisfying $|\Lambda| \geq \mathsf{p} - 2\mathsf{q}$. $\Diamond$

*Proof:* (if): Suppose that $\Phi$ is not $\mathsf{q}$-error correctable. That is, there exist $x_1, x_2 \in \mathbb{R}^{\mathsf{n}}$ satisfying $x_1 \neq x_2$, and $e_1, e_2 \in \Sigma^{\mathsf{n}}_{\mathsf{q}}$ such that $\Phi x_1 + e_1 = \Phi x_2 + e_2$. Let $x := x_1 - x_2$ and $e := -e_1 + e_2$, then it follows that $\Phi x = e$ where $x \neq 0_{\mathsf{n}\times 1}$ and $e \in \Sigma^{\mathsf{n}}_{2\mathsf{q}}$. With an index set $\Lambda := (\mathsf{supp}^{\mathsf{n}}(e))^c$, it is obvious that $|\Lambda| \geq \mathsf{p} - 2\mathsf{q}$ and $\Phi_{\Lambda^{\mathsf{n}}} x = 0_{\mathsf{np}\times 1}$. Therefore, the null space of $\Phi_{\Lambda^{\mathsf{n}}}$ is not trivial, i.e., $\mathcal{N}(\Phi_{\Lambda^{\mathsf{n}}}) \neq \{0_{\mathsf{n}\times 1}\}$, which contradicts the full column rank condition of $\Phi_{\Lambda^{\mathsf{n}}}$.
(only if): Suppose, for the sake of contradiction, that there exists an index set $\Lambda \subset [\mathsf{p}]$ with $|\Lambda| \geq \mathsf{p} - 2\mathsf{q}$ and $x \neq 0_{\mathsf{n}\times 1}$ such that $\Phi_{\Lambda^{\mathsf{n}}} x = 0_{\mathsf{np}\times 1}$. Then it follows that $\|e\|_{0^{\mathsf{n}}} \leq 2\mathsf{q}$ where $e := \Phi x$. Let $e_1$ and $e_2$ be such that $e = -e_1 + e_2$ where $\|e_1\|_{0^{\mathsf{n}}} \leq \mathsf{q}$ and $\|e_2\|_{0^{\mathsf{n}}} \leq \mathsf{q}$. Thus, there exist $x \in \mathbb{R}^{\mathsf{n}}$ satisfying $x \neq 0_{\mathsf{n}\times 1}$, and $e_1, e_2 \in \Sigma^{\mathsf{n}}_{\mathsf{q}}$, such that $\Phi x + e_1 = \Phi 0_{\mathsf{n}\times 1} + e_2$, which implies $\Phi$ is not $\mathsf{q}$-error correctable. ■

Directly from Definition 1, $\Phi \in \mathbb{R}^{\mathsf{np}\times\mathsf{n}}$ is ($\mathsf{n}$-stacked) $\mathsf{q}$-error correctable if and only if there exists a decoding map $\mathcal{D} : \mathbb{R}^{\mathsf{np}} \to \mathbb{R}^{\mathsf{n}}$ such that $\mathcal{D}(\hat{z}) = x$ where $\hat{z} = \Phi x + e \in \mathbb{R}^{\mathsf{np}}$ and $e \in \Sigma^{\mathsf{n}}_{\mathsf{q}}$. From now on, we will discuss the problem of constructing a decoder that can actually correct ($\mathsf{n}$-stacked) $\mathsf{q}$ errors when $\Phi$ is ($\mathsf{n}$-stacked) $\mathsf{q}$-error correctable. Recall that, with a usual vector $\bar{z} = \Psi x + \bar{e} \in \mathbb{R}^{\mathsf{p}}$ where $\bar{e} \in \Sigma_{\mathsf{q}}$, the input $x$ is uniquely recovered by the well-known $\ell_0$ minimization decoder $\mathcal{D}_0 : \bar{z} \mapsto \arg\min_{\chi\in\mathbb{R}^{\mathsf{n}}} \|\bar{z} - \Psi\chi\|_0$ for $\Psi \in \mathbb{R}^{\mathsf{p}\times\mathsf{n}}$ with $\mathsf{p} > \mathsf{n}$ [10, Section 3], [27, Proposition 5]. Then, it is not difficult to see that the $\ell_0$ minimization also works for the stacked vector $\hat{z} = \Phi x + e \in \mathbb{R}^{\mathsf{np}}$. Indeed, we can reconstruct the input $x$ from the solution of the $\ell_0$ minimization problem

$$\min_{\chi\in\mathbb{R}^{\mathsf{n}},\ \varepsilon\in\mathbb{R}^{\mathsf{np}}} \|\varepsilon\|_{0^{\mathsf{n}}} \quad \text{subject to} \quad \varepsilon = \hat{z} - \Phi\chi, \tag{3}$$

or equivalently,

$$\min_{\chi\in\mathbb{R}^{\mathsf{n}}} \|\hat{z} - \Phi\chi\|_{0^{\mathsf{n}}}, \tag{3$'$}$$

as asserted in the following lemma.

**Lemma 2:** Assume that $\Phi \in \mathbb{R}^{\mathsf{np}\times\mathsf{n}}$ is $\mathsf{q}$-error correctable. For any $x \in \mathbb{R}^{\mathsf{n}}$ and $e \in \Sigma^{\mathsf{n}}_{\mathsf{q}}$, suppose that we obtain measurements of the form $\hat{z} = \Phi x + e \in \mathbb{R}^{\mathsf{np}}$. Then $x = \arg\min_{\chi\in\mathbb{R}^{\mathsf{n}}} \|\hat{z} - \Phi\chi\|_{0^{\mathsf{n}}}$, i.e., the decoder $\mathcal{D}_{0^{\mathsf{n}}} : \hat{z} \mapsto \arg\min_{\chi\in\mathbb{R}^{\mathsf{n}}} \|\hat{z} - \Phi\chi\|_{0^{\mathsf{n}}}$ corrects $\mathsf{q}$ errors. $\Diamond$

*Proof:* Suppose that there exist a solution $x' \in \mathbb{R}^{\mathsf{n}}$ of $\min_{\chi\in\mathbb{R}^{\mathsf{n}}} \|\hat{z} - \Phi\chi\|_{0^{\mathsf{n}}}$ satisfying $x' \neq x$ and $e' := \hat{z} - \Phi x' \in \Sigma^{\mathsf{n}}_{\mathsf{q}}$. Then, it follows that $\hat{z} = \Phi x' + e' = \Phi x + e$, and $\|e'\|_{0^{\mathsf{n}}} \leq \|e\|_{0^{\mathsf{n}}} \leq \mathsf{q}$ because $e'$ is the minimal solution. This implies that $\Phi$ is not $\mathsf{q}$-error correctable and thus completes the proof by contradiction. ■

So far, in order to solve (3) or (3$'$), we should have searched the whole space $\mathbb{R}^{\mathsf{n}}$. However, this can be drastically reduced to a finite set

$$\mathcal{F}_{\mathsf{p}-\mathsf{q}}(\hat{z}) := \big\{\chi \in \mathbb{R}^{\mathsf{n}} : \chi = (\Phi_{\Lambda^{\mathsf{n}}})^{\dagger}\, \hat{z}_{\Lambda^{\mathsf{n}}} \text{ where } \Lambda \subset [\mathsf{p}] \text{ and } |\Lambda| = \mathsf{p} - \mathsf{q}\big\}$$

where $(\Phi_{\Lambda^{\mathsf{n}}})^{\dagger}$ is the pseudoinverse of $\Phi_{\Lambda^{\mathsf{n}}}$. Note that $|\mathcal{F}_{\mathsf{p}-\mathsf{q}}(\hat{z})| \leq \binom{\mathsf{p}}{\mathsf{p}-\mathsf{q}} = \binom{\mathsf{p}}{\mathsf{q}}$. When it comes to solving (3) or (3$'$), the following theorem claims that it is enough to search the finite set $\mathcal{F}_{\mathsf{p}-\mathsf{q}}(\hat{z})$, not $\mathbb{R}^{\mathsf{n}}$.

**Theorem 1:** Assume that $\Phi \in \mathbb{R}^{\mathsf{np}\times\mathsf{n}}$ is $\mathsf{q}$-error correctable. Suppose that we obtain measurements of the form $\hat{z} = \Phi x + e \in \mathbb{R}^{\mathsf{np}}$ where $x \in \mathbb{R}^{\mathsf{n}}$ and $e \in \Sigma^{\mathsf{n}}_{\mathsf{q}}$. Then $x = \arg\min_{\chi\in\mathcal{F}_{\mathsf{p}-\mathsf{q}}(\hat{z})} \|\hat{z} - \Phi\chi\|_{0^{\mathsf{n}}}$. $\Diamond$

*Proof:* It is easily proved by the fact $x \in \mathcal{F}_{\mathsf{p}-\mathsf{q}}(\hat{z})$. ■

**Remark 1:** Since the $\ell_0$ minimization problem (3) is NP-hard [30] in terms of computational complexity, many researchers have pursued a relaxation of (3) while imposing additional conditions. It is emphasized that the algorithm proposed in Theorem 1 actually relieves the computational complexity, not by imposing additional conditions, but by reducing the search space to a finite set. Indeed, the algorithm is a kind of combinatorial approach which tests only $\binom{\mathsf{p}}{\mathsf{q}} \leq \mathsf{p}^{\mathsf{q}}$ candidates, while the conventional error correction algorithm often tests all $\binom{\mathsf{p}}{1} + \binom{\mathsf{p}}{2} + \cdots + \binom{\mathsf{p}}{\mathsf{p}} \approx 2^{\mathsf{p}}$ combinations. $\Diamond$

### *B. Robustness with Bounded Noises*

The measurements are prone to be contaminated by noises in most practical situations, e.g, imperfect sensors, quantization errors, modeling errors, or external disturbances. A signal recovery algorithm which is robust to bounded noises, is proposed in this subsection. By robustness, we mean that the error bound is guaranteed to be proportional to the noise level. Therefore, stable signal recovery is possible in the presence of noises.

Under bounded noise $v \in \mathbb{R}^{\mathsf{np}}$ satisfying $\|v^{\mathsf{n}}_{\mathsf{i}}\|_2 \leq v_{\max}$ for all $\mathsf{i} \in [\mathsf{p}]$ in (2), it will be shown that any solution of the following relaxed $\ell_0$ minimization problem

$$\begin{aligned}&\min_{\chi\in\mathcal{F}_{\mathsf{p}-\mathsf{q}}(\hat{z}),\ \varepsilon\in\mathbb{R}^{\mathsf{np}}} \|\varepsilon\|_{0^{\mathsf{n}}}\\ &\text{subject to } \|\hat{z}^{\mathsf{n}}_{\mathsf{i}} - \Phi_{\Gamma^{\mathsf{n}}_{\mathsf{i}}}\chi - \varepsilon^{\mathsf{n}}_{\mathsf{i}}\|_2 \leq v'_{\max}, \quad {}^{\forall}\mathsf{i} \in [\mathsf{p}]\end{aligned} \tag{4}$$

yields an approximation of the original input $x$ where $v'_{\max} := \sqrt{\mathsf{p} - \mathsf{q}}\, v_{\max}$. From an implementation point of view, (4) is transformed to the following minimization problem which is in more accessible form:

$$\min_{\chi\in\mathcal{F}_{\mathsf{p}-\mathsf{q}}(\hat{z})} \left|\left\{\mathsf{i} \in [\mathsf{p}] : \|\hat{z}^{\mathsf{n}}_{\mathsf{i}} - \Phi_{\Gamma^{\mathsf{n}}_{\mathsf{i}}}\chi\|_2 > v'_{\max}\right\}\right|. \tag{4$'$}$$

Note that (4$'$) has only one optimization variable $\chi$, while (4) has two optimization variables $\chi$ and $\varepsilon$. Consequently, when we implement the algorithm, the unconstrained problem (4$'$) is preferable to (4). However, when robustness of the given signal reconstruction scheme is analyzed, the problem (4) is more useful than (4′) because the corresponding error vector $\hat{e}$ and the noise vector $\hat{v}$ can be directly determined from the solution $\hat{x}$. Actually, (4′) can be interpreted as a relaxation of the problem (3′). The following proposition shows the equivalence of (4) and (4′).

**Proposition 1:** For any $x \in \mathbb{R}^{\mathsf{n}}$, $e \in \Sigma_{\mathsf{q}}^{\mathsf{n}}$, and $v \in \mathbb{R}^{\mathsf{np}}$ satisfying $\|v_{\mathsf{i}}^{\mathsf{n}}\|_2 \leq v_{\max}$ for all $\mathsf{i} \in [\mathsf{p}]$, suppose that the measurements are given by $\hat{z} = \Phi x + v + e \in \mathbb{R}^{\mathsf{np}}$. The $\ell_0$ minimization problem (4) is equivalent to the optimization problem (4′). ♢

*Proof:* It is omitted due to space limitation. ∎

As in the noiseless case of Theorem 1, a robust estimation scheme which utilizes an optimization over a finite set, is presented in the following theorem, with new notation of

$$\begin{aligned}\rho_{\mathsf{p-q}}(\Phi) &:= \min\left\{\sigma_{\min}\left(\Phi_{\Lambda^{\mathsf{n}}}\right) : \Lambda \subset [\mathsf{p}],\ |\Lambda| = \mathsf{p}-\mathsf{q}\right\} \\ &= 1\Big/\max\left\{\left\|(\Phi_{\Lambda^{\mathsf{n}}})^{\dagger}\right\|_2 : \Lambda \subset [\mathsf{p}],\ |\Lambda| = \mathsf{p}-\mathsf{q}\right\}, \\ k &:= (\sqrt{\mathsf{p}-\mathsf{q}}+1)\sqrt{\mathsf{p}-2\mathsf{q}}/\rho_{\mathsf{p}-2\mathsf{q}}(\Phi),\end{aligned}$$

where $\Phi \in \mathbb{R}^{\mathsf{np}\times\mathsf{n}}$ and $\sigma_{\min}\left(\Phi_{\Lambda^{\mathsf{n}}}\right)$ denotes the minimum singular value of $\Phi_{\Lambda^{\mathsf{n}}}$.

**Theorem 2:** Assume that $\Phi \in \mathbb{R}^{\mathsf{np}\times\mathsf{n}}$ is $\mathsf{q}$-error correctable. For any $x \in \mathbb{R}^{\mathsf{n}}$, $e \in \Sigma_{\mathsf{q}}^{\mathsf{n}}$, and $v \in \mathbb{R}^{\mathsf{np}}$ satisfying $\|v_{\mathsf{i}}^{\mathsf{n}}\|_2 \leq v_{\max}$ for all $\mathsf{i} \in [\mathsf{p}]$, suppose that the noisy observation $\hat{z} \in \mathbb{R}^{\mathsf{np}}$ is given by $\hat{z} = \Phi x + v + e$. Then

$$\|\hat{x} - x\|_2 \leq k v_{\max}$$

where $\hat{x}$ is a solution of the minimization problem (4′). ♢

*Proof:* Since (4) and (4′) are equivalent by Proposition 1, $\hat{x}$ is also a solution of (4). Assuming that $\hat{e}$ is the error vector corresponding to $\hat{x}$ in (4), first, it is claimed that $\|\hat{e}\|_{0^{\mathsf{n}}} \leq \mathsf{q}$. Let $\bar{\Lambda}$ be any subset of $(\mathsf{supp}^{\mathsf{n}}(e))^c$ with $|\bar{\Lambda}| = \mathsf{p}-\mathsf{q}$. Then, with $\bar{x} := (\Phi_{\bar{\Lambda}^{\mathsf{n}}})^{\dagger}\,\hat{z}_{\bar{\Lambda}^{\mathsf{n}}} \in \mathcal{F}_{\mathsf{p-q}}(\hat{z})$, one has $\bar{x} = x + (\Phi_{\bar{\Lambda}^{\mathsf{n}}})^{\dagger}\, v_{\bar{\Lambda}^{\mathsf{n}}}$ because $\Phi_{\bar{\Lambda}^{\mathsf{n}}}$ has full column rank and thus $(\Phi_{\bar{\Lambda}^{\mathsf{n}}})^{\dagger}\,\Phi_{\bar{\Lambda}^{\mathsf{n}}} = I_{\mathsf{n}\times\mathsf{n}}$. Now, define $\bar{v} := \hat{z}_{\bar{\Lambda}^{\mathsf{n}}} - \Phi_{\bar{\Lambda}^{\mathsf{n}}}\bar{x} \in \mathbb{R}^{\mathsf{np}}$ and $\bar{e} := \hat{z} - \Phi\bar{x} - \bar{v}$. Then, it is obtained that

$$\begin{aligned}&\|\hat{z}_{\mathsf{i}}^{\mathsf{n}} - \Phi_{\Gamma_{\mathsf{i}}^{\mathsf{n}}}\bar{x} - \bar{e}_{\mathsf{i}}^{\mathsf{n}}\|_2 = \|\bar{v}_{\mathsf{i}}^{\mathsf{n}}\|_2 \leq \|\bar{v}\|_2 \\ &= \|(I_{\mathsf{np}\times\mathsf{np}} - \Phi_{\bar{\Lambda}^{\mathsf{n}}}(\Phi_{\bar{\Lambda}^{\mathsf{n}}})^{\dagger})v_{\bar{\Lambda}^{\mathsf{n}}}\|_2 \leq \sqrt{\mathsf{p}-\mathsf{q}}\,v_{\max} = v'_{\max},\end{aligned}$$

for all $\mathsf{i} \in [\mathsf{p}]$ where the last inequality comes from fact that $\|(I_{\mathsf{np}\times\mathsf{np}} - \Phi_{\bar{\Lambda}^{\mathsf{n}}}(\Phi_{\bar{\Lambda}^{\mathsf{n}}})^{\dagger})\|_2 \leq 1$ and $\|v_{\bar{\Lambda}^{\mathsf{n}}}\|_2 \leq \sqrt{\mathsf{p}-\mathsf{q}}\,v_{\max}$. By the construction of $\bar{e}$, it follows that $\|\bar{e}\|_{0^{\mathsf{n}}} \leq \mathsf{q}$ and $\|\hat{z}_{\mathsf{i}}^{\mathsf{n}} - \Phi_{\Gamma_{\mathsf{i}}^{\mathsf{n}}}\bar{x} - \bar{e}_{\mathsf{i}}^{\mathsf{n}}\|_2 \leq v'_{\max}$ for all $\mathsf{i} \in [\mathsf{p}]$. Thus, one can conclude that $\|\hat{e}\|_{0^{\mathsf{n}}} \leq \|\bar{e}\|_{0^{\mathsf{n}}} \leq \mathsf{q}$ because $\hat{e}$ is the minimal solution of (4). Now, the corresponding noise vector to $\hat{x}$ and $\hat{e}$ is defined by $\hat{v} := \hat{z} - \Phi\hat{x} - \hat{e}$, and thus $\|\hat{v}_{\mathsf{i}}^{\mathsf{n}}\|_2 \leq v'_{\max}$ for all $\mathsf{i} \in [\mathsf{p}]$ by the constraint in (4). Since $\hat{z} = \Phi x + v + e = \Phi\hat{x} + \hat{v} + \hat{e}$, it follows that $\Phi\tilde{x} + \tilde{e} = -\tilde{v}$ where $\tilde{x} := \hat{x} - x$, $\tilde{e} := \hat{e} - e$, and $\tilde{v} := \hat{v} - v$. Note that $\|\tilde{e}\|_{0^{\mathsf{n}}} \leq 2\mathsf{q}$ and $\|\tilde{v}_{\mathsf{i}}^{\mathsf{n}}\|_2 \leq v'_{\max} + v_{\max}$ for all $\mathsf{i} \in [\mathsf{p}]$. Let $\Lambda$ be any subset of $(\mathsf{supp}^{\mathsf{n}}(\tilde{e}))^c$ satisfying $|\Lambda| = \mathsf{p} - 2\mathsf{q}$. Then, $\Phi_{\Lambda^{\mathsf{n}}}\tilde{x} = -\tilde{v}_{\Lambda^{\mathsf{n}}}$. Since $\Phi_{\Lambda^{\mathsf{n}}}$ has full column rank by Lemma 1, it follows that $\tilde{x} = -\left(\Phi_{\Lambda^{\mathsf{n}}}\right)^{\dagger}\tilde{v}_{\Lambda^{\mathsf{n}}}$. Finally, one can calculate the bound of $\|\tilde{x}\|_2$ as $\|\tilde{x}\|_2 \leq \left\|\left(\Phi_{\Lambda^{\mathsf{n}}}\right)^{\dagger}\right\|_2 \|\tilde{v}_{\Lambda^{\mathsf{n}}}\|_2 \leq (\sqrt{\mathsf{p}-\mathsf{q}}+1)\sqrt{\mathsf{p}-2\mathsf{q}}\,v_{\max}/\rho_{\mathsf{p}-2\mathsf{q}}(\Phi) = k v_{\max}$. ∎

## IV. Dynamic Error Correction with Observers

In this section, a secure and robust dynamic observer design problem for the plant (1) is considered. The system is first transformed by the Kalman observability decomposition to design a Luenberger observer for each sensor. Then, the static error correcting methods discussed so far are applied to the information collected from each individual observer.

### A. Observability Decomposition and Observer Design

Assuming that only $\mathsf{i}$-th sensor is available in (1), the plant is reduced to the single-output system as follows:

$$\begin{aligned}\dot{x}(t) &= Ax(t) + Bu(t) + d(t) \\ y_{\mathsf{i}}(t) &= c_{\mathsf{i}}x(t) + n_{\mathsf{i}}(t) + a_{\mathsf{i}}(t)\end{aligned} \tag{5}$$

where $c_{\mathsf{i}}$ is the $\mathsf{i}$-th row of $C$. Denote the observability matrix of (5) by $G_{\mathsf{i}} := \left[c_{\mathsf{i}}^{\top}\ (c_{\mathsf{i}}A)^{\top}\ \cdots\ (c_{\mathsf{i}}A^{\mathsf{n}-1})^{\top}\right]^{\top}$, and let $\nu_{\mathsf{i}}$ be the observability index of $(A, c_{\mathsf{i}})$, i.e., $\nu_{\mathsf{i}} := \mathsf{rank}(G_{\mathsf{i}})$. Then the set of the first $\nu_{\mathsf{i}}$ rows of $G_{\mathsf{i}}$ is linearly independent. The null space of $G_{\mathsf{i}}$, $\mathcal{N}(G_{\mathsf{i}})$, which is $A$-invariant, is the unobservable subspace. Furthermore, the quotient space of $\mathcal{N}(G_{\mathsf{i}})$ is observable, and is sometimes called, with abuse of terminology, the observable subspace. The system (5) is now decomposed into two subspaces of $\mathbb{R}^{\mathsf{n}}$, i.e., $\mathcal{N}(G_{\mathsf{i}})$ and $\mathcal{N}(G_{\mathsf{i}})^{\perp}$. Recall that $\mathcal{N}(G_{\mathsf{i}})^{\perp} = \mathcal{R}(G_{\mathsf{i}}^{\top})$ where $\mathcal{R}(G_{\mathsf{i}}^{\top})$ is the range space of $G_{\mathsf{i}}^{\top}$. Choose matrices $Z_{\mathsf{i}} \in \mathbb{R}^{\mathsf{n}\times\nu_{\mathsf{i}}}$ and $W_{\mathsf{i}} \in \mathbb{R}^{\mathsf{n}\times(\mathsf{n}-\nu_{\mathsf{i}})}$ such that their columns are orthonormal bases of $\mathcal{R}(G_{\mathsf{i}}^{\top})$ and $\mathcal{N}(G_{\mathsf{i}})$, respectively. Furthermore, any two columns of them are orthonormal so that $[Z_{\mathsf{i}}\ W_{\mathsf{i}}]^{\top}[Z_{\mathsf{i}}\ W_{\mathsf{i}}] = I_{\mathsf{n}\times\mathsf{n}}$.

We make the change of state variables as defined by the transformation

$$\begin{bmatrix} z_{\mathsf{i}}^{\top} & w_{\mathsf{i}}^{\top}\end{bmatrix}^{\top} = \begin{bmatrix} Z_{\mathsf{i}} & W_{\mathsf{i}}\end{bmatrix}^{\top} x. \tag{6}$$

Now, in terms of this new state $\begin{bmatrix} z_{\mathsf{i}}^{\top} & w_{\mathsf{i}}^{\top}\end{bmatrix}^{\top}$, (5) becomes

$$\begin{aligned}\begin{bmatrix}\dot{z}_{\mathsf{i}}(t) \\ \dot{w}_{\mathsf{i}}(t)\end{bmatrix} &= \begin{bmatrix} S_{\mathsf{i}} & O \\ * & *\end{bmatrix}\begin{bmatrix} z_{\mathsf{i}}(t) \\ w_{\mathsf{i}}(t)\end{bmatrix} + \begin{bmatrix} Z_{\mathsf{i}}^{\top} \\ W_{\mathsf{i}}^{\top}\end{bmatrix}(Bu(t) + d(t)) \\ y_{\mathsf{i}}(t) &= \begin{bmatrix} r_{\mathsf{i}} & O\end{bmatrix}\begin{bmatrix} z_{\mathsf{i}}(t) \\ w_{\mathsf{i}}(t)\end{bmatrix} + n_{\mathsf{i}}(t) + a_{\mathsf{i}}(t)\end{aligned} \tag{7}$$

where $S_{\mathsf{i}} := Z_{\mathsf{i}}^{\top}AZ_{\mathsf{i}}$, $r_{\mathsf{i}} := c_{\mathsf{i}}Z_{\mathsf{i}}$, and $O$ represents the zero matrix of appropriate size. Finally, the observable subsystem of (7) is obtained as follows:

$$\begin{aligned}\dot{z}_{\mathsf{i}}(t) &= S_{\mathsf{i}}z_{\mathsf{i}}(t) + Z_{\mathsf{i}}^{\top}Bu(t) + Z_{\mathsf{i}}^{\top}d(t) \\ y_{\mathsf{i}}(t) &= r_{\mathsf{i}}z_{\mathsf{i}}(t) + n_{\mathsf{i}}(t) + a_{\mathsf{i}}(t).\end{aligned}$$

Here, the pair $(S_{\mathsf{i}}, r_{\mathsf{i}})$ is observable by the properties of the decomposition. Thus, we can design a standard Luengerger observer of the form

$$\dot{\hat{z}}_{\mathsf{i}}(t) = S_{\mathsf{i}}\hat{z}_{\mathsf{i}}(t) + Z_{\mathsf{i}}^{\top}Bu(t) + L_{\mathsf{i}}\left(y_{\mathsf{i}}(t) - r_{\mathsf{i}}\hat{z}_{\mathsf{i}}(t)\right) \tag{8}$$

where $L_{\mathsf{i}}$ is chosen so that $F_{\mathsf{i}} := S_{\mathsf{i}} - L_{\mathsf{i}}r_{\mathsf{i}}$ is Hurwitz. The error dynamics, with $\tilde{z}_{\mathsf{i}} := \hat{z}_{\mathsf{i}} - z_{\mathsf{i}}$, are governed by

$$\dot{\tilde{z}}_{\mathsf{i}}(t) = F_{\mathsf{i}}\tilde{z}_{\mathsf{i}}(t) + L_{\mathsf{i}}n_{\mathsf{i}}(t) - Z_{\mathsf{i}}^{\top}d(t) + L_{\mathsf{i}}a_{\mathsf{i}}(t). \tag{9}$$

The solution of (9) becomes

$$\tilde{z}_{\mathsf{i}}(t) = v_{\mathsf{i}}(t) + e_{\mathsf{i}}(t) \tag{10}$$

where $v_{\mathsf{i}}(t) := e^{F_{\mathsf{i}}t}\tilde{z}_{\mathsf{i}}(0) + \int_0^t e^{F_{\mathsf{i}}(t-\tau)}(L_{\mathsf{i}}n_{\mathsf{i}}(\tau) - Z_{\mathsf{i}}^\top d(\tau))d\tau$ and $e_{\mathsf{i}}(t) := \int_0^t e^{F_{\mathsf{i}}(t-\tau)}L_{\mathsf{i}}a_{\mathsf{i}}(\tau)d\tau$. Here, $e_{\mathsf{i}}(t)$ may have arbitrary values since it is affected by the attack signal $a_{\mathsf{i}}(t)$. For all $t \geq 0$ and $\mathsf{i} \in [\mathsf{p}]$, there exist $\mu_F \geq 1$ and $\lambda_F > 0$ such that $\|e^{F_{\mathsf{i}}t}\|_2 \leq \mu_F e^{-\lambda_F t}$ since all $F_{\mathsf{i}}$'s are Hurwitz. In addition, for some $\mu_L,\ \mu_Z \geq 1$, it holds that $\|e^{F_{\mathsf{i}}t}L_{\mathsf{i}}\|_2 \leq \mu_L e^{-\lambda_F t}$ and $\|e^{F_{\mathsf{i}}t}Z_{\mathsf{i}}^\top\|_2 \leq \mu_Z e^{-\lambda_F t}$. Then, one can easily show that

$$\|v_{\mathsf{i}}(t)\|_2 \leq \mu_F \|\tilde{z}_{\mathsf{i}}(0)\|_2 e^{-\lambda_F t} + v_{\max}$$

where $v_{\max} := \mu_L n_{\max}/\lambda_F + \mu_Z d_{\max}/\lambda_F$.

### *B. Observer-Based Combinatorial State Estimation in the Presence of Attacks, Noises, and Disturbances*

This subsection presents the main results of the paper. We apply the static error correcting methods studied so far into the observer design problem of the control system (1). From the similarity transformation (6), it trivially follows that $Z_{\mathsf{i}}^\top x = z_{\mathsf{i}}$ for all $\mathsf{i} \in [\mathsf{p}]$. By appending $\mathsf{n} - \nu_{\mathsf{i}}$ zero row vectors, $O_{(\mathsf{n}-\nu_{\mathsf{i}})\times\mathsf{n}}$, to each $Z_{\mathsf{i}}^\top$ and stacking them all, we finally have the following equation of the form

$$\begin{bmatrix} Z_1^{\mathsf{n}\top} \\ \vdots \\ Z_{\mathsf{p}}^{\mathsf{n}\top} \end{bmatrix} x(t) = \begin{bmatrix} z_1^{\mathsf{n}}(t) \\ \vdots \\ z_{\mathsf{p}}^{\mathsf{n}}(t) \end{bmatrix} = \begin{bmatrix} \hat{z}_1^{\mathsf{n}}(t) \\ \vdots \\ \hat{z}_{\mathsf{p}}^{\mathsf{n}}(t) \end{bmatrix} - \begin{bmatrix} \tilde{z}_1^{\mathsf{n}}(t) \\ \vdots \\ \tilde{z}_{\mathsf{p}}^{\mathsf{n}}(t) \end{bmatrix}, \tag{11}$$

where

$$\begin{aligned} Z_{\mathsf{i}}^{\mathsf{n}\top} &:= \begin{bmatrix} Z_{\mathsf{i}}^\top \\ O_{(\mathsf{n}-\nu_{\mathsf{i}})\times\mathsf{n}} \end{bmatrix}, & z_{\mathsf{i}}^{\mathsf{n}}(t) &:= \begin{bmatrix} z_{\mathsf{i}}(t) \\ 0_{(\mathsf{n}-\nu_{\mathsf{i}})\times 1} \end{bmatrix}, \\ \hat{z}_{\mathsf{i}}^{\mathsf{n}}(t) &:= \begin{bmatrix} \hat{z}_{\mathsf{i}}(t) \\ 0_{(\mathsf{n}-\nu_{\mathsf{i}})\times 1} \end{bmatrix}, & \tilde{z}_{\mathsf{i}}^{\mathsf{n}}(t) &:= \begin{bmatrix} \tilde{z}_{\mathsf{i}}(t) \\ 0_{(\mathsf{n}-\nu_{\mathsf{i}})\times 1} \end{bmatrix}. \end{aligned} \tag{12}$$

The equation (11) can be written in a compact form as

$$\hat{z}(t) = \Phi x(t) + \tilde{z}(t) = \Phi x(t) + v(t) + e(t) \in \mathbb{R}^{\mathsf{np}} \tag{13}$$

where $\Phi$ consists of $Z_{\mathsf{i}}^{\mathsf{n}\top}$'s and the last equality comes from (10). It is also assumed for $v(t)$ and $e(t)$ that additional zero elements are augmented as in (12). Note that (13) coincides with the static error correcting problem (2) except the time index $t$.

Before presenting the final theorem, new notions of $\mathsf{q}$-*redundant observability* and *observability under* $\mathsf{q}$-*sparse sensor attacks* are introduced.

**Definition 2:** The dynamical system (1) is said to be $\mathsf{q}$-*redundant observable*[2] if the pair $(A, C_\Lambda)$ is observable for any $\Lambda \subset [\mathsf{p}]$ with $|\Lambda| = \mathsf{p} - \mathsf{q}$. $\Diamond$

**Definition 3:** The dynamical system (1) is said to be *observable under* $\mathsf{q}$-*sparse sensor attacks* if the matrix $\Phi \in \mathbb{R}^{\mathsf{np}\times\mathsf{n}}$ in (13) is ($\mathsf{n}$-stacked) $\mathsf{q}$-error correctable. $\Diamond$

[2]The same concept was introduced in [29] with $\mathsf{q}$-sparse observability notion, but we used different terminology as $\mathsf{q}$-redundant observability because $\mathsf{q}$-sparse observability was formerly defined in [31] which concerns $\mathsf{q}$-sparse initial values.

A technical lemma revealing the equivalence between the above new notions is derived easily from Lemma 1.

**Lemma 3:** The system (1) is observable under $\mathsf{q}$-sparse sensor attacks if and only if it is $2\mathsf{q}$-redundant observable. $\Diamond$

*Proof:* Let $\Lambda \subset [\mathsf{p}]$ be any index set satisfying $|\Lambda| = \mathsf{p} - 2\mathsf{q}$. Denote the observability matrix of $(A, C_\Lambda)$ as $G_\Lambda := \left[C_\Lambda^\top\ (C_\Lambda A)^\top\ \cdots\ (C_\Lambda A^{\mathsf{n}-1})^\top\right]^\top$. By the construction of $\Phi$ and its elements $Z_{\mathsf{i}}^\top$'s, it follows that $\mathcal{R}(G_\Lambda^\top) = \mathcal{R}(\Phi_{\Lambda^{\mathsf{n}}}^\top)$. Thus, $\mathsf{rank}(G_\Lambda) = \mathsf{n}$ if and only if $\Phi_{\Lambda^{\mathsf{n}}}$ has full column rank. Finally, by Lemma 1, $\mathsf{rank}(G_\Lambda) = \mathsf{n}$ for any $\Lambda \subset [\mathsf{p}]$ satisfying $|\Lambda| = \mathsf{p} - 2\mathsf{q}$ if and only if $\Phi$ is $\mathsf{q}$-error correctable, which completes the proof. ■

Finally, we have the following theorem which suggests a secure and robust estimation algorithm for dynamical systems under sensor attacks in the presence of measurement noises and process disturbances.

**Theorem 3:** Under Assumptions 1 and 2, let the system (1) be $2\mathsf{q}$-redundant observable. In addition, suppose that observers are designed as (8). Then, for any $\delta > 0$, there exists a $T(\delta)$ such that

$$\|\hat{x}(t) - x(t)\|_2 \leq k v_{\max} + \delta, \quad {}^\forall t \geq T(\delta)$$

where, with $v''_{\max} := \sqrt{\mathsf{p} - \mathsf{q}}(v_{\max} + \delta/k)$,

$$\hat{x}(t) := \underset{\chi \in \mathcal{F}_{\mathsf{p}-\mathsf{q}}(\hat{z}(t))}{\arg\min} \left| \left\{ \mathsf{i} \in [\mathsf{p}] : \|\hat{z}_{\mathsf{i}}^{\mathsf{n}} - \Phi_{\Gamma_{\mathsf{i}}^{\mathsf{n}}}\chi\|_2 > v''_{\max} \right\} \right|. \ \Diamond$$

*Proof:* It easily follows from Theorem 2. ■

**Remark 2:** An anomaly detector which monitors the system to detect deviations from the nominal behavior [14], can be designed by the dedicated observer scheme [20]. Originated from the fault detection and isolation area, the dedicated observer scheme also utilizes a bank of observers like the proposed algorithm in Subsection IV-A. More precisely, the output error signal $\tilde{y}_{\mathsf{i}}$ of the following system

$$\begin{aligned} \dot{\tilde{z}}_{\mathsf{i}}(t) &= F_{\mathsf{i}}\tilde{z}_{\mathsf{i}}(t) + L_{\mathsf{i}}n_{\mathsf{i}}(t) - Z_{\mathsf{i}}^\top d(t) + L_{\mathsf{i}}a_{\mathsf{i}}(t), \\ \tilde{y}_{\mathsf{i}}(t) &= r_{\mathsf{i}}\tilde{z}(t) - n_{\mathsf{i}}(t) - a_{\mathsf{i}}(t). \end{aligned} \tag{9$'$}$$

where $\hat{y}_{\mathsf{i}} := r_{\mathsf{i}}\hat{z}_{\mathsf{i}}$ and $\tilde{y}_{\mathsf{i}} := \hat{y}_{\mathsf{i}} - y_{\mathsf{i}}$, can be used as a residual. Since (9$'$) is primarily designed to detect sensor (or instrument) faults, not malicious attacks, a decision logic, which announces possible anomalies in the $\mathsf{i}$-th sensor when the residual $\tilde{y}_{\mathsf{i}}$ exceeds a predefined threshold, can not identify stealthy attacks nor zero dynamics attacks [14]. On the other hand, the proposed error correcting algorithm in Theorem 3 can reveal those covert attacks because $e_{\mathsf{i}}$ in (10) becomes relatively large (i.e., $\|e_{\mathsf{i}}\|_2 \gg 0$) even when $\tilde{y}_{\mathsf{i}}$ is small enough. $\Diamond$

## V. Numerical Example

We consider a linear dynamical system (1) with

$$\begin{aligned} A &= -0.1 \times I_{2\times 2}, \qquad B = O_{2\times 1}, \\ C &= \begin{bmatrix} 1 & 0 & 1 & 1 & -1 & -2 \\ 0 & 1 & -1 & 1 & 2 & -1 \end{bmatrix}^\top, \end{aligned} \tag{14}$$

where $u(t) \equiv 0$ and, $d(t)$ and $n(t)$ are white noise signals that are saturated by $d_{\max} = 0.1$ and $n_{\max} = 0.1$, respectively. Note that (14) is 4-redundant observable. The

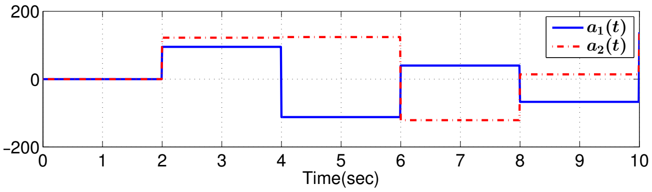


Fig. 1. Plot of attack $a_1(t)$ and $a_2(t)$

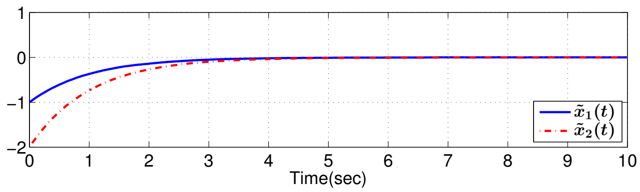


Fig. 2. Plot of state estimation error $\tilde{x}_1(t)$ and $\tilde{x}_2(t)$

2-sparse attack signal $a(t)$ is injected into the system. More precisely, $\mathsf{supp}(a(t)) = \{1,2\}$ for $t \geq 2$ and the attack signals are depicted in Fig. 1. The state estimation errors $\tilde{x}_{\mathsf{i}}(t) := \hat{x}_{\mathsf{i}}(t) - x_{\mathsf{i}}(t)$ are described in Fig. 2 which shows the attack-resilient property of our estimation algorithm.

## VI. Conclusion

In this paper, we have considered continuous-time LTI systems under sensor attacks in the presence of measurement noises and process disturbances. It is assumed that the adversarial attacks are q-sparse and noises/disturbances are bounded. By extending the classical error correction techniques to the stacked vector case, a secure and robust estimation algorithm based on a bank of Luenberger observers has been proposed under 2q-redundant observability condition of the given system. The contributions of this paper are as follows. First, without any additional restrictive conditions other than 2q-redundant observability, we could estimate the state values with relatively less computation. This advantage comes from the fact that we solve the $\ell_0$ minimization problem on a reduced finite set. Second, stable signal recovery is possible with a guaranteed error bound in the presence of noises/disturbances. Moreover, the maximum error bound is given in an explicit form of the bounds on noises/disturbances.

## References


[1] J. Kim, J. Yang, H. Shim, and J.-S. Kim, "Robustness of synchronization in heterogeneous multi-agent systems," in *Proc. of 12th European Control Conf.,* 2013, pp. 3821–3826.

[2] U. Ozguner, "Decentralized and distributed control approaches and algorithms," in *Proc. of 28th IEEE Conf. on Decision and Control,* 1989, pp. 1289–1294.

[3] W. Chen, L. Chen, Z. Chen and S. Tu, "A realtime dynamic traffic control system based on wireless sensor network," in *Proc. of International Conf. Workshops on Parallel Processing,* 2005, pp. 258–264.

[4] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy,* vol. 9, no. 3, pp. 49–51, 2011.

[5] A. Wright, "Hacking cars," *Communications of the ACM,* vol. 54, no. 11, pp. 18–19, 2011.

[6] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. on Power Systems,* vol. 23, no. 4, pp. 1836–1846, 2008.

[7] 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.

[8] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. on Information and System Security,* vol. 14, no. 1, pp. 13:1–13:33, 2011.

[9] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE,* vol. 100, no. 1, pp. 195–209, 2012.

[10] V. Guruswami, J. R. Lee, and A. Wigderson, "Euclidean sections of $\ell_1^N$ with sublinear randomness and error-correction over the reals," in *Proc. of 11th International Workshop on APPROX and 12th International Workshop on RANDOM,* vol. 5171 of *Lecture Notes in Computer Science*, Springer-Verlag, 2008, pp. 444–454.

[11] M. Rudelson and R. Vershynin, "Geometric approach to error-correcting codes and reconstruction of signals," *International mathematics research notices,* vol. 2005, no. 64, pp. 4019–4041, 2005.

[12] H. Q. Ngo and D.-Z. Du, "A survey on combinatorial group testing algorithms with applications to DNA library screening," *Discrete mathematical problems with medical applications,* vol. 55, pp. 171–182, 2000.

[13] P. M. Frank, "Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results," *Automatica*, vol. 26, no. 3, pp. 459–474, 1990.

[14] 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.

[15] R. E. Lyons and W. Vanderkulk, "The use of triple-modular redundancy to improve computer reliability," *IBM Journal of Research and Development,* vol. 6, no. 2, pp. 200–209, 1962.

[16] D. Dolev, N. A. Lynch, S. S. Pinter, E. W. Stark, and W. E. Weihl, "Reaching approximate agreement in the presence of faults," *Journal of the ACM,* vol. 33, no. 3, pp. 499–516, 1986.

[17] P. M. Frank and X. Ding, "Survey of robust residual generation and evaluation methods in observer-based fault detection systems," *Journal of process control*, vol. 7, no. 6, pp. 403–424, 1997.

[18] R. K. Mehra and J. Peschon, "An innovations approach to fault detection and diagnosis in dynamic systems," *Automatica,* vol. 7, no. 5, pp. 637–640, 1971.

[19] R. Isermann, "Fault diagnosis of machines via parameter estimation and knowledge processing–Tutorial paper," *Automatica*, vol. 29, no. 4, pp. 815–835, 1993.

[20] R. N. Clark, "Instrument fault detection," *IEEE Trans. on Aerospace Electronic Systems*, vol. 14, pp. 456–465, 1978.

[21] C. Lee, Z. Ping, and H. Shim, "On-line switching signal estimation of switched linear systems with measurement noise," in *Proc. of 12th European Control Conf.,* 2013, pp. 2180–2185.

[22] A. Tanwani, H. Shim, and D. Liberzon, "Observability for switched linear systems: Characterization and observer design," *IEEE Trans. on Automatic Control,* vol. 58, no. 4, pp. 891–904, 2013.

[23] E. J. Candès and T. Tao, "Decoding by linear programming," *IEEE Trans. on Information Theory,* vol. 51, no. 12, pp. 4203–4215, 2005.

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

[25] M. A. Davenport, M. F. Duarte, Y. C. Eldar, and G. Kutyniok, "Introduction to compressed sensing," in *Compressed Sensing: Theory and Applications,* Cambridge Univ. Press, 2012.

[26] J. A. Tropp, "Greed is good: Algorithmic results for sparse approximation," *IEEE Trans. on Information Theory,* vol. 50, no. 10, pp. 2231–2242, 2004.

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

[28] M. Pajic, J. Weimer, N. James, P. Tabuada, O. Sokolsky, I. Lee, and G. Pappas, "Robustness of attack-resilient state estimators," in *Proc. of 5th IEEE/ACM International Conf. on Cyber-Physical Systems,* 2014, pp. 163–174.

[29] Y. Shoukry and P. Tabuada, "Event-triggered projected Luenberger observer for linear systems under sparse sensor attacks," in *Proc. of 53rd IEEE Conf. on Decision and Control,* 2014, pp. 3548–3553.

[30] B. K. Natarajan, "Sparse approximate solutions to linear systems," *SIAM journal on computing*, vol. 24, no. 2, pp. 227–234, 1995.

[31] N. Tarfulea, "Observability for initial value problems with sparse initial data," *Applied and Computational Harmonic Analysis,* vol. 30, no. 3, pp. 423–427, 2011.