SIAM J. CONTROL OPTIM.
Vol. 63, No. 5, pp. 3703–3727

RESILIENT STATE RECOVERY USING PRIOR MEASUREMENT SUPPORT INFORMATION*

YU ZHENG†, OLUGBENGA MOSES ANUBI‡, AND WARREN E. DIXON§

Abstract. Resilient state recovery of cyber-physical systems has attracted much research attention due to the unique challenges posed by the tight coupling between communication, computation, and the underlying physics of such systems. By modeling attacks as additive adversary signals to a sparse subset of measurements, this resilient recovery problem can be formulated as an error correction problem. To achieve exact state recovery, most existing results require less than 50% of the measurement nodes to be compromised, which limits the resiliency of the estimators. In this paper, we show that observer resiliency can be further improved by incorporating data-driven prior information. We provide an analytical bridge between the precision of prior information and the resiliency of the estimator. By quantifying the relationship between the estimation error of the weighted ℓ_1 observer and the precision of the support prior, this quantified relationship provides guidance for the estimator's weight design to achieve optimal resiliency. Several numerical simulations and an application case study are presented to validate the theoretical claims.

Key words. linear systems in control theory, observers, observability, optimality conditions

MSC codes. 93C05, 93B53, 93B07, 49K15

DOI. 10.1137/23M1611671

1. Notation and Preliminaries.

$\mathbb{R}, \mathbb{R}^n, \mathbb{R}^{n\times m}, \mathbb{Z}$ denote the space of real numbers, real vectors of length n, real matrices of n rows and m columns, and the space of integers, respectively. $\mathbb{R}_+$ denotes the space of positive real numbers. $\emptyset$ denotes the empty set. Normal-face lower-case letters (*e.g.* $x \in \mathbb{R}$) are used to represent real scalars, bold-face lower-case letters (*e.g.* $\mathbf{x} \in \mathbb{R}^n$) represent vectors, while normal-face upper-case letters (e.g., $X \in \mathbb{R}^{n\times m}$) represent matrices. $X^\top$ denotes the transpose of the matrix X. Let $\mathcal{T} \subseteq \{1, \cdots, n\}$, then $X_\mathcal{T} \in \mathbb{R}^{|\mathcal{T}|\times n}$ is the submatrix obtained by extracting the rows of $X \in \mathbb{R}^{m\times n}$ corresponding to the indices in $\mathcal{T}$. $\mathcal{T}^c$ denotes the complement of a set $\mathcal{T}$, and the universal set on which it is defined will be clear from

*Received by the editors October 25, 2023; accepted for publication (in revised form) July 3, 2025; published electronically October 14, 2025.

https://doi.org/10.1137/23M1611671

Funding: This work was funded by Florida State University (FSU) Council on Research and Creativity (CRC) under Award 33278 This material is based upon work supported by Florida State University (FSU) Council on Research Creativity (CRC) under Award 33278 and the Department of Energy under Award Number DE-CR0000028.

†Department of Electrical and Computer Engineering, Florida State University, Tallahassee, FL 32310 USA (yzheng6@fsu.edu).

‡Corresponding author. Department of Electrical and Computer Engineering, Florida State University, Tallahassee, FL 32310 USA (oanubi@fsu.edu).

§Department of Mechanical and Aerospace Engineering, University of Florida, Gainesville, FL 32611-6250 USA (wdixon@ufl.edu).

the context. Also, $\mathcal{T}_1 \backslash \mathcal{T}_2 \triangleq \mathcal{T}_1 \cap \mathcal{T}_2^c$ denotes set difference between the sets $\mathcal{T}_1$ and $\mathcal{T}_2$. For a matrix $X \in \mathbb{R}^{m\times n}$, $\mathbf{null}(X)$ and $\mathbf{range}(X)$ denote its null space and range space respectively.

For any $0 < p \leq \infty$, we use $\|\mathbf{x}\|_p \triangleq (\sum_{i=1}^n |\mathbf{x}_i|^p)^{\frac{1}{p}}$ to denote the p-norm of the vector $\mathbf{x} \in \mathbb{R}^n$. A weighted 1-norm of a vector $\mathbf{z} \in \mathbb{R}^n$ with the weight vector $\mathbf{w} \in \mathbb{R}^n$ is defined as

$$\|\mathbf{z}\|_{1,\mathbf{w}} \triangleq \sum_{i=1}^{n} \mathbf{w}_i |\mathbf{z}_i|. \tag{1.1}$$

We define a weight vector $\mathbf{w}(\mathcal{T}, \omega) \in \mathbb{R}^m$, based on a set $\mathcal{T} \subset \{1, 2, \cdots, m\}$, as

$$\mathbf{w}(\mathcal{T}, \omega)_i = \begin{cases} \omega & \text{if } i \in \mathcal{T} \\ 1 & \text{otherwise.} \end{cases} \tag{1.2}$$

where $0 < \omega < 1$ is the weight value.

The following mathematical preambles are used throughout the paper. The omitted proofs can be found in the standard references such as [14]. For any vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ and real numbers $p, q \in \mathbb{R}_+$, the following holds:

1. The topological equivalence of vector norms:

$$\|\mathbf{x}\|_q \leq \|\mathbf{x}\|_p \leq n^{\left(\frac{1}{p}-\frac{1}{q}\right)} \|\mathbf{x}\|_q, \text{ for } 0 < p \leq q \leq \infty. \tag{1.3}$$

For example, given a vector $\mathbf{x} \in \mathbb{R}^n$,

$$\|\mathbf{x}\|_\infty \leq \|\mathbf{x}\|_2 \leq \|\mathbf{x}\|_1 \leq \sqrt{n}\|\mathbf{x}\|_2 \leq n\|\mathbf{x}\|_\infty. \tag{1.4}$$

2. The triangle inequality:

$$\|\mathbf{x} + \mathbf{y}\|_p \leq \|\mathbf{x}\|_p + \|\mathbf{y}\|_p, \text{ for } 0 < p \leq \infty. \tag{1.5}$$

3. The reverse triangle inequality:

$$\|\mathbf{x} - \mathbf{y}\|_p \geq \Big| \|\mathbf{x}\|_p - \|\mathbf{y}\|_p \Big|, \text{ for } 0 < p \leq \infty. \tag{1.6}$$

The support of a vector $\mathbf{x} \in \mathbb{R}^n$ is a set of the indices of nonzero entries in $\mathbf{x}$, defined as

$$\mathsf{supp}(\mathbf{x}) \triangleq \{i \subseteq \{1, \ldots, n\} | \mathbf{x}_i \neq 0\}, \tag{1.7}$$

and $\|\mathbf{x}\|_0 = |\mathsf{supp}(\mathbf{x})|$. The vector $\mathbf{x} \in \mathbb{R}^n$ is said to be k-sparse if $\|\mathbf{x}\|_0 \leq k$, and Σ_k denotes the set of k-sparse vectors, given by

$$\Sigma_k \triangleq \left\{ \mathbf{x} \in \mathbf{R}^n \,\middle|\, |\mathsf{supp}(\mathbf{x})| \leq k \right\}. \tag{1.8}$$

Let $I_T \triangleq [i-T+1, i]$ denote a moving interval of fixed size T. When clear from context, the subscript T will be dropped for clarity. Accordingly, $I-1 \triangleq [i-T, i-1]$ denotes the $T(>1)$ time interval from $i-T$ to $i-1$. As a result, $\mathbf{x}_I = [\mathbf{x}_i^\top, \mathbf{x}_{i-1}^\top, \cdots, \mathbf{x}_{i-T+1}^\top]^\top \in \mathbb{R}^{Tn}$ is a flattened vector composed of vectors $\mathbf{x}_j$ in the descending order of $j \in I$. Given the supports $\mathcal{T}_j \subset \{1, 2, \cdots, m\}, \forall j \in I$, the support sequence for the entire time interval I is denoted by $\mathcal{T}_I = [\mathcal{T}_i^\top, \ m+\mathcal{T}_{i-1}^\top, \cdots, (T-1)m+\mathcal{T}_{i-T+1}^\top]^\top$, where $m+\mathcal{T}_{i-1}^\top$ denotes adding m to each element of $\mathcal{T}_{i-1}^\top$.

2. Introduction. The rapid development and wide application of cyber-physical systems (CPS) has benefited from the tight coupling and coordination among computation, communication, and physical components [19]. Digital coupling via communication networks or physical coupling via grid systems provides wider observability, stronger controllability, and faster response speed among physical components. However, the closed-loop interaction between the cyber world and the physical world exposes the physical plant to cyberattacks [25]. Small biases, injected through internet-of-thing sensors, could manipulate the physical processes maliciously [37, 41]. Thus, for guaranteed resilient operation, it is necessary that true signals are recovered under cyber-activities and fault-induced anomalies.

From a control system perspective, undesirable effects created by malicious intent could manifest as noise, disturbance, uncertainty, or any combination. However, attack signals are more challenging since they are possibly unbounded, or bounded with unknown bounds, and time-varying according to the attacker's policy [32]. These special features of attack signals result in the typical robust control and estimation laws [35], where bound information is required, being ineffective [36]. Assuming attackers don't have infinite resources, the attack vectors $\mathbf{e} \in \mathbb{R}^m$ are sparse with bounded support $\|\mathbf{e}\|_0 \leq s < m$ [10]. Based on this sparsity assumption on the set of attacked nodes, the majority of state recovery results are formulated as a sparse recovery problem closely related to the classical error correction problem [5, 10].

Consider a measurement model of the form

$$\mathbf{y} = H\mathbf{x} + \mathbf{e}, \tag{2.1}$$

where $H \in \mathbb{R}^{m\times n}$ $(n < m)$ is the measurement matrix, and $\mathbf{y}, \mathbf{e}, \mathbf{x}$ are the sensor measurements, attack injection, and internal state vectors, respectively. Given a coding matrix $F \in \mathbb{R}^{n\times m}$ satisfying $FH = 0$, the classical error correction problem is to recover a sparse vector $\mathbf{e}$ for which $\mathbf{y}_c \triangleq F\mathbf{y} = F\mathbf{e}$. This is usually solved by

$$\underset{\mathbf{e}}{\mathsf{Minimize}} : \|\mathbf{e}\|_0 \;\; \mathsf{Subject\ to} : \mathbf{y}_c = F\mathbf{e}. \tag{2.2}$$

Any sparse error $\|\mathbf{e}\| < s$ $(s < \frac{m}{2})$ could be recovered uniquely through the above optimization program if [34]

$$\mathsf{null}(F) \cap \Sigma_{2s} = \emptyset, \tag{2.3}$$

where $\Sigma_{2s} \subseteq \mathbb{R}^m$ denotes the set of all $2s$-sparse vectors which is a subset of the m-dimensional vector space. The minimization problem in (2.2) is an NP-hard problem but can be relaxed to its convex neighbor:

$$\underset{\mathbf{e}}{\mathsf{Minimize}} : \|\mathbf{e}\|_1 \;\; \mathsf{Subject\ to} : \mathbf{y}_c = F\mathbf{e}. \tag{2.4}$$

The solution of (2.4) is the unique solution of (2.2) if the coding matrix F satisfies the null space property (NSP) [4] or s-restricted isometric property (s-RIP) [5]. The authors in [24] also studied the robustness of ℓ_1 estimators while attacks and noise both exist. Alternative approaches employ ℓ_2 decoders as the convex relaxation of the program in (2.2). These methods utilize diverse sparse projectors, such as an event-trigger or switch mechanisms [1, 31] and constrained sensor fusion [7, 22, 30]. These studies have also been extended to networked control systems [21, 26, 27, 28]. However, both relaxed convex programs admit the uniqueness condition in (2.3), regardless of whether they are implemented in centralized or distributed systems. This condition can be cast as a $2s$-observerability assumption for linear systems,

requiring more than half of the sensors to be safe [10, 31]. In other words, 100% sensor redundancy is required. This assumption poses a major limitation on CPS's resiliency in practice.

The fundamental limitation in (2.3) can be relaxed by incorporating prior information. The authors in [11] studied a weighted ℓ_1 decoder with support prior for compressed sensing problems. The authors in [33] studied a modified compressed sensing program to recursively reduce the state estimation error along with convergence of the support prior estimation. In [17], the authors found the resilience of the state estimator can be improved by incorporating intermittent data authentication. The authors in [29] also found that utilizing the state prior could also increase the resilience of the state estimator. However, analysis is needed for why such methodology can improve resiliency and how much resiliency can be improved.

Contributions: In this paper, we studied an enhanced resilient estimation problem with reinforcement of data-driven prior information. Existing resilient estimation methods predominantly rely on the 2s-observability assumption [1, 7, 10, 13, 20, 21, 22, 31, 30]. Our work seeks to relax this assumption, thereby further improving the resiliency of CPS. To achieve this goal, we derive the column space property (CSP) and row-restricted isometry property (Row-RIP), which enables us to adjust the strictness of the observability conditions in relation to the estimation error bound. Our demonstrations indicate that resiliency can be significantly enhanced when the accuracy of the prior information exceeds that of a random coin flip. Furthermore, while previous studies have explored resilient estimation with additional prior information [16, 29], they do not fully explain why and how this information improves resiliency, nor do they identify the necessary conditions for its effectiveness. Our paper addresses this gap by establishing a connection between the precision of data-driven prior information and the resulting estimation error bound. These quantitative connections provide a systematic guide for the design of resilient estimators leveraging prior information, as illustrated by the design of the weighted ℓ_1 estimator presented in this paper.

The rest of the paper is organized as follows. Notations and preliminary results are provided in section 1. In section 3, we introduce CPS and Row-RIP, motivated by the uniqueness condition of state recovery. In section 4, we conduct a rigorous vulnerability analysis and show that violating the CSP implies the existence of a successful attack design against a resilient ℓ_1 estimator. We derive the estimation errors bound for the ℓ_1 decoder without prior and weighted ℓ_1 decoder with prior in section 5 and show that inclusion of prior information significantly lowers the resulting error bound. In section 6, a numerical simulation quantifies the influence of the precision of the prior information on system resilience. Concluding remarks are in section 8.

3. Model Development and Resilience Properties.

In this section, we present the model and relevant properties of a CPS. Moreover, instead of assuming a $2s$-observability as done in results such as [10, 31], we introduce CSP and Row-RIP to guarantee the uniqueness of state recovery under sparse attacks.

3.1. System Model.

Since the physical processes interact with the cyber components that operate in a discrete-time sequence, we consider the following discrete model of a CPS under attack and bounded noise:

$$\begin{aligned} \mathbf{x}_{i+1} &= A\mathbf{x}_i \\ \mathbf{y}_i &= C\mathbf{x}_i + \mathbf{e}_i, \end{aligned} \tag{3.1}$$

where $\mathbf{x}_i \in \mathbb{R}^n, \mathbf{y}_i \in \mathbb{R}^m$ are the state and measurement vector at the time instance i, respectively, $\mathbf{e}_i \in \mathbb{R}^m$ is a vector containing both noise and attack with attack support $\mathcal{T} \subset \{1, 2, \cdots, m\}$ ($|\mathcal{T}| < k$). The noise portion of $\mathbf{e}$ is assumed to be bounded

$$\sum_{i \in \mathcal{T}^c} |\mathbf{e}_i| < \varepsilon, \tag{3.2}$$

where $\varepsilon \in \mathbb{R}_+$ is the noise level. The known control inputs are neglected in (3.1) since they are irrelevant to state estimation problem [10, 39] or the reader could view (3.1) as a stable closed-loop dynamical model. By iterating (3.1) T steps backwards, the measurement model in T-length observation interval is given by

$$\mathbf{y}_I = H\mathbf{x}_{i-T+1} + \mathbf{e}_I, \tag{3.3}$$

where $\mathbf{y}_I, \mathbf{e}_I \in \mathbb{R}^{Tm}$ are the sequence of measurements and attacks in the interval I, respectively, $\mathbf{x}_{i-T+1} \in \mathbb{R}^n$ is the state vector at time $i - T + 1$, and $H = \begin{bmatrix}(CA^{T-1})^\top & \cdots & (CA)^\top & C^\top\end{bmatrix}^\top$ is assumed to have full column rank.

Due to the sparsity of the attack portion in $\mathbf{e}_I$, an ℓ_1 decoder is typically used to reconstruct the state from the corrupted measurements [2, 5, 10].

DEFINITION 3.1 (**Decoder of Horizon** T). *Given an observation matrix H, the decoder $\mathcal{D}$ maps the observation sequence $\mathbf{y}_I$ to a state estimate $\hat{\mathbf{x}}_{i-T+1}$. The state estimate is*

$$\begin{aligned}\hat{\mathbf{x}}_{i-T+1} &= \mathcal{D}(\mathbf{y}_I|H) \\ &\triangleq \arg\min_{\mathbf{x}\in\mathbb{R}^n} \|\mathbf{y}_I - H\mathbf{x}\|_1,\end{aligned} \tag{3.4}$$

where $\mathbf{y}_I$ is the observation history on I and $\hat{\mathbf{x}}_{i-T+1} \in \mathbb{R}^n$ is the resulting estimated initial state vector.

The ℓ_1 decoder defined in (3.4) can be efficiently solved by linear programming [4, 5], in a recursive manner [23], or through distributed solvers [20].

DEFINITION 3.2 (**Resilient Recovery**). *The decoder $\hat{\mathbf{x}}_{i-T+1} = \mathcal{D}(\mathbf{y}_I|H)$ in Definition* 3.1 *is said to resiliently recover the true state $\mathbf{x}_{i-T+1}$ if, given an error tolerance ϵ,*

$$\|\hat{\mathbf{x}}_{i-T+1} - \mathbf{x}_{i-T+1}\| \leq \epsilon. \tag{3.5}$$

If (3.5) *holds, then the decoder $\mathcal{D}$ is a resilient decoder with error tolerance ϵ.*

To achieve resilient recovery through the estimator in (3.4), the literature commonly assumes a condition, known as 2s-observability [10, 18], to ensure the unique existence of a state despite the presence of attack signals. However, this assumption imposes a significant constraint on system resiliency because it requires 100% sensor redundancy relative to the attacker's capabilities. In the remainder of this work, we examine the original conditions that are sufficient for resilient recovery and explore the potential to relax the 2s-observability assumption, thereby enhancing the resiliency of CPS.

3.2. CSP and Row-RIP. We begin with the result that guarantees unique state recovery from attacked measurements. Without loss of generality, the attack portion and noise portion in the error term $\mathbf{e}$ can be seen as orthogonal to each other since the noise on the attack portion indexed by $\mathcal{T}$ can be absorbed into the attack itself.

In addition, uniqueness in state recovery is a hallmark of sparse recovery problems when countering the effects of these attacks, as demonstrated in [3, 5]. Consequently, we focus our discussion on unique state recovery using the noise-free version of the measurement model in (3.3).

THEOREM 3.3 (**Uniqueness of State Recovery**). *Given an observation matrix $H \in \mathbb{R}^{Tm\times n}$ subject to k-sparse attacks on T-length time interval I (i.e. $|\mathcal{T}_j| \leq k$ for all $j \in I$). If, for any nonzero $\mathbf{h} \in \mathsf{range}(H)$, it is true that*

$$\|\mathbf{h}_{\mathcal{S}}\|_1 < \|\mathbf{h}_{\mathcal{S}^c}\|_1, \text{ for all } \mathcal{S} \subset \{1, 2, \cdots, Tm\} \text{ with } |\mathcal{S}| \leq Tk, \tag{3.6}$$

then for each attacked measurement $\mathbf{y}_I \in \mathbb{R}^{Tm}$, there exists a unique state vector $\hat{\mathbf{x}} \in \mathbb{R}^n$ and an attack vector $\hat{\mathbf{e}}_I$ satisfying (3.3).

Proof. Let $(\mathbf{z}_1, \mathbf{e}_1), (\mathbf{z}_2, \mathbf{e}_2) \in \mathbb{R}^n \times \Sigma_{Tk}$ be two different candidates satisfying (3.3) for a given $\mathbf{y}_I$. That is: $\mathbf{y}_I = H\mathbf{z}_1 + \mathbf{e}_1 = H\mathbf{z}_2 + \mathbf{e}_2$. Then $H(\mathbf{z}_1 - \mathbf{z}_2) = \mathbf{e}_2 - \mathbf{e}_1$. This is equivalent to $H(\mathbf{z}_1 - \mathbf{z}_2) \in \Sigma_{2Tk}$ for some $\mathbf{z}_1, \mathbf{z}_2 \in \mathbb{R}^n$. Thus, since H is full-ranked, the uniqueness condition $\mathbf{z}_1 = \mathbf{z}_2$ holds if and only if $\mathsf{range}(H) \cap \Sigma_{2Tk} = \{\mathbf{0}\}$. Given a nonzero $\mathbf{h} \in \mathsf{range}(H)$, this condition is equivalent to $\|\mathbf{h}\|_0 > 2Tk$.

To prove $\|\mathbf{h}\|_0 > 2Tk$ can be implied by the condition in (3.6), we suppose, for the sake of contradiction, that $\|\mathbf{h}\|_0 \leq 2Tk$. Choose $\overline{\mathcal{S}} \subseteq \{1, 2, \cdots, Tm\}$, with $|\overline{\mathcal{S}}| = Tk$, to be the indices of the largest components of $\mathbf{h}$ in absolute value. Then, it must be that $\|\mathbf{h}_{\overline{\mathcal{S}}}\|_1 \geq \|\mathbf{h}_{\overline{\mathcal{S}}^c}\|_1$, which is a contradiction. Thus, (3.6) implies that $\|\mathbf{h}\|_0 > 2Tk$. ∎

Remark 3.4. According to the proof of Theorem 3.3, the inequality in (3.6) implies $\|\mathbf{h}\|_0 > 2Tk$. This result is equivalent to $m > 2k$ which is well-known and used in related work (cf. [10, 31]).

Remark 3.5. Using the compactness of the intersection of $\mathsf{range}(H)$ and the unit norm ball, the inequality in (3.6) is equivalent to the existence of $\beta \in (0, 1)$ such that $\|\mathbf{h}_{\mathcal{S}}\|_1 \leq \beta\|\mathbf{h}_{\mathcal{S}^c}\|_1$ holds for all $\mathbf{h} \in \mathsf{range}(H)$, $\mathcal{S} \subset \{1, 2, \cdots, Tm\}, |\mathcal{S}| \leq Tk$.

DEFINITION 3.6 (**Column space property (CSP)**). *A matrix $H \in \mathbb{R}^{m\times n}$ is said to have a CSP of order $s < m$ (denoted as $H \triangleright \mathsf{CSP}(s)$) with a parameter β if, for every $\mathbf{h} \in \mathsf{range}(H)$,*

$$\|\mathbf{h}_{\mathcal{S}}\|_1 \leq \beta\|\mathbf{h}_{\mathcal{S}^c}\|_1, \text{ for all } \mathcal{S} \subset \{1, 2, \cdots, m\} \text{ with } |\mathcal{S}| \leq s. \tag{3.7}$$

Definition 3.6 is similar to the well-known null space property (NSP) [4] but is defined on the range space instead. The name CSP is used to avoid confusion with a recently defined range space property (RSP) [38]. Next, we consider a restricted isometry property on the row space of a matrix and establish a relationship with CSP.

DEFINITION 3.7 (**Row-Restricted Isometry Property (Row-RIP)**). *A matrix $H \in \mathbb{R}^{m\times n}$ is said to have a Row-RIP of order k (denoted as $H \triangleright \mathsf{rRIP}(k)$) if there exists a constant $\delta \in (0, 1)$ such that*

$$(1 - \delta)\|\mathbf{x}\|_2^2 \leq \|H_{\mathcal{T}}\mathbf{x}\|_2^2 \leq (1 + \delta)\|\mathbf{x}\|_2^2, \tag{3.8}$$

for all $\mathbf{x} \in \mathbb{R}^n$ and $\mathcal{T} \subset \{1, 2, \cdots, m\}$ with $|\mathcal{T}| \leq k$. Furthermore, the row-RIP constant of order k is defined as

$$\delta_k \triangleq \inf_{\delta} \{\delta \mid (3.8) \quad \textit{holds}\}. \tag{3.9}$$

LEMMA 3.8 (**Relating CSP and Row-RIP**). *Given* $H \in \mathbb{R}^{m\times n}$, *with* $H \triangleright \mathit{rRIP}(ak)$ *for some* $a > 1$ *and* $k \le \frac{m}{2a+1}$. *If*

$$\delta_k + a\delta_{ak} < a - 1, \tag{3.10}$$

then $H \triangleright \mathit{CSP}(k)$.

Proof. Choose an arbitrary set $\mathcal{T} \in \{1, 2, \cdots, m\}$ with $|\mathcal{T}| \le k \le m/(2a+1)$, and an arbitrary vector $\mathbf{h} \in \mathsf{range}(H)$. Then using the topology equivalence of norms in (1.4) and the inequality in (3.8), it follows that

$$\|\mathbf{h}_{\mathcal{T}}\|_1 \le \sqrt{|\mathcal{T}|}\|\mathbf{h}_{\mathcal{T}}\|_2 \le \sqrt{k(1+\delta_k)}\|\mathbf{x}\|_2, \tag{3.11}$$

with $\mathbf{h} = H\mathbf{x}$. Also, let $\mathcal{S} \subset \mathcal{T}^c$, with $|\mathcal{S}| = ak$, be a subset of $\mathcal{T}^c$ containing the smallest entries, in absolute values, of $\mathbf{h}_{\mathcal{T}^c}$. Such set $\mathcal{S}$ exists because $|\mathcal{S}| + |\mathcal{T}| \le ak + k \le m$. Then, the largest element in $\mathbf{h}_{\mathcal{S}}$ satisfies

$$|\mathcal{T}^c \backslash \mathcal{S}| \max_{i\in\mathcal{S}} |\mathbf{h}_i| \le \sum_{i\in\mathcal{T}^c\backslash\mathcal{S}} |\mathbf{h}_i| \le \sum_{i\in\mathcal{T}^c} |\mathbf{h}_i|,$$

which implies that

$$(m - |\mathcal{T}| - |\mathcal{S}|) \max_{i\in\mathcal{S}} |\mathbf{h}_i| \le \|\mathbf{h}_{\mathcal{T}^c}\|_1. \tag{3.12}$$

The inequality in (3.12) follows from the topological equivalence of norms in (1.4). Besides, since $k \le \frac{m}{2a+1}$ and $|\mathcal{S}| = ak$, it follows that $(2a+1)k \le m \Rightarrow (2a+1)k - k - ak \le m - |\mathcal{T}| - |\mathcal{S}| \Rightarrow m - |\mathcal{T}| - |\mathcal{S}| \ge ak$. Thus, it follows from (3.12) that

$$\max_{i\in\mathcal{S}} |\mathbf{h}_i| \le \frac{\|\mathbf{h}_{\mathcal{T}^c}\|_1}{ak} \Rightarrow \|\mathbf{h}_{\mathcal{S}}\|_\infty \le \frac{\|\mathbf{h}_{\mathcal{T}^c}\|_1}{ak}. \tag{3.13}$$

By considering the topological equivalence of the ∞-norm and 2-norm in (1.4), (3.13) implies

$$\sqrt{ak}\|\mathbf{h}_{\mathcal{S}}\|_2 \le \|\mathbf{h}_{\mathcal{T}^c}\|_1. \tag{3.14}$$

Since $H \triangleright \mathsf{rRIP}(ak)$, it follows that

$$\|\mathbf{h}_{\mathcal{T}^c}\|_1 \ge \sqrt{ak}\|\mathbf{h}_{\mathcal{S}}\|_2 \ge \sqrt{ak(1-\delta_{ak})}\|\mathbf{x}\|_2,$$

which implies

$$\|\mathbf{x}\|_2 \le \frac{1}{\sqrt{ak(1-\delta_{ak})}}\|\mathbf{h}_{\mathcal{T}^c}\|_1. \tag{3.15}$$

Combining (3.11) and (3.15) yields

$$\|\mathbf{h}_{\mathcal{T}}\|_1 \le \sqrt{\frac{1+\delta_k}{a(1-\delta_{ak})}}\|\mathbf{h}_{\mathcal{T}^c}\|_1.$$

From (3.10), it follows that $0 < \sqrt{\frac{1+\delta_k}{a(1-\delta_{ak})}} < 1$. Thus, $H \triangleright \mathsf{CSP}(k)$. ∎

4. Vulnerability Analysis. In this section, we discuss under what conditions the system is vulnerable to attacks in a conservative scenario. We make the following assumptions about the attackers' capability which are widely admitted in literature (cf. [15, 25] and references within):

1. The attacker has full model knowledge of (3.1);
2. The attacker can inject arbitrary bias at the compromised sensors $\mathcal{T}_i \subset \{1, \cdots, m\}$;
3. The resource of the attacker is limited, so the number of simultaneously attacked sensors is bounded such that $|\mathcal{T}_i| \leq k$ (equivalently, $\mathbf{e}_i \in \Sigma_k$).

These assumptions highlight the insufficiency of conventional bounded-disturbance-based robust estimation approaches since the attacks may not be bounded. Furthermore, it is more pragmatic to assume that attackers aim to maximize the perturbation of estimated states without triggering an alarm from the monitoring system.

DEFINITION 4.1 (**Successful attack** [6, 15]). *Consider the CPS in* (3.1) *and the corresponding measurement model in* (3.3) *with a state estimator* $\mathcal{D} : \mathbb{R}^{Tm} \to \mathbb{R}^n$. *Given an attack support* $\mathcal{T}$ *with* $|\mathcal{T}_j| \leq k$ *for all* $j \in I$ *and a positive integer* $k < m$, *the attack sequence* $\mathbf{e}_I \in \mathbb{R}^{Tm}$ *is said to be* (ϵ, α)*-successful if*

$$\|\mathbf{x}^\star - \mathcal{D}(\mathbf{y}_I)\|_2 \geq \alpha \ \text{ and } \ \|\mathbf{y}_I - H\mathcal{D}(\mathbf{y}_I)\|_2 \leq \epsilon, \tag{4.1}$$

where $\mathbf{y}_I = \mathbf{y}_I^\star + \mathbf{e}_I$ *with* $\mathbf{y}_I^\star \in \mathbb{R}^{Tm}$ *being the true measurement vector, and* $\mathbf{x}^\star = \mathcal{D}(\mathbf{y}_I^\star)$ *is the observed state vector without attacks.*

The first inequality in (4.1) quantifies the attack effectiveness using a threshold value of α while the second inequality quantifies the stealthiness using a threshold value of ϵ. Given a support sequence $\mathcal{T}$ with $|\mathcal{T}_i| \leq k$ for all $j \in I$. Let $\mathbf{x}_e$ be an optimal solution of

$$\begin{aligned} &\mathsf{Maxmize} : \|H_{\mathcal{T}}\mathbf{x}\|_1, \\ &\mathsf{Subject\ to} : \|H_{\mathcal{T}^c}\mathbf{x}\|_1 \leq \epsilon. \end{aligned} \tag{4.2}$$

Consider the attack defined accordingly as

$$\mathbf{e}_{I_{\mathcal{T}}} = H_{\mathcal{T}}\mathbf{x}_e, \ \ \mathbf{e}_{I_{\mathcal{T}^c}} = \mathbf{0}. \tag{4.3}$$

The next result gives the conditions under which the attack defined above is (ϵ, α)-successful for the given attack support $\mathcal{T}$.

Remark 4.2. It is implicitly assumed in (4.3) that $H_{\mathcal{T}^c}$ is full ranked. Otherwise, the constraint $\|H_{\mathcal{T}^c}\mathbf{x}\|_1 \leq \epsilon$ would be satisfied by any $\mathbf{x}_e$ in the null space of $H_{\mathcal{T}^c}$, thereby making the program in (4.2) ill-defined.

THEOREM 4.3 (**(ϵ, α)-successful attack**). *Given an attack support* $\mathcal{T}$, *with* $|\mathcal{T}| > \frac{\sigma_{\mathcal{T}^c}^2}{\sigma_{\mathcal{T}}^2}$, *such that* $H_{\mathcal{T}^c}$ *has full rank. If the subset*

$$\mathcal{S}_H(\mathcal{T}) \triangleq \{\mathbf{w} \in \mathsf{range}(H) \big| \|\mathbf{w}_{\mathcal{T}}\|_1 > \|\mathbf{w}_{\mathcal{T}^c}\|_1\}, \tag{4.4}$$

is nonempty, then the attack in (4.3) *is* (ϵ, α)*-successful for all*

$$\alpha \leq \frac{\sigma_1 - 1}{\sqrt{|\mathcal{T}|}\overline{\sigma}_{\mathcal{T}} - \underline{\sigma}_{\mathcal{T}^c}}\epsilon, \tag{4.5}$$

where $\overline{\sigma}_{\mathcal{T}}$ *and* $\underline{\sigma}_{\mathcal{T}^c}$ *are the largest and the smallest nonzero singular values of* $H_{\mathcal{T}}$ *and* $H_{\mathcal{T}^c}$ *respectively, and* $\sigma_1 = \max_{\mathbf{v} \in \mathbb{R}^n \setminus \{\mathbf{0}\}} \frac{\|H_{\mathcal{T}}\mathbf{v}\|_1}{\|H_{\mathcal{T}^c}\mathbf{v}\|_1}$.

Proof. First, we show that $\|\mathbf{x}^\star - \mathcal{D}(\mathbf{y}_I)\|_2 \geq \alpha$. For the optimization problem in (4.2), let $\mathbf{x} = \alpha\mathbf{v}$, where $\mathbf{v} \in \mathbb{R}^n$ is an arbitrary vector, then

$$\begin{aligned} \|H_{\mathcal{T}}\mathbf{x}_e\|_1 &\geq \max_{|\alpha|\|H_{\mathcal{T}^c}\mathbf{v}\|_1 \leq \epsilon} (|\alpha|\|H_{\mathcal{T}}\mathbf{v}\|_1) \\ &\geq \max_{\mathbf{v}\in\mathbb{R}^n\setminus\{\mathbf{0}\}} \frac{\|H_{\mathcal{T}}\mathbf{v}\|_1}{\|H_{\mathcal{T}^c}\mathbf{v}\|_1}\epsilon = \sigma_1\epsilon \end{aligned} \tag{4.6}$$

Let P be an appropriate permutation matrix satisfying $H = P\left[\begin{smallmatrix} H_{\mathcal{T}} \\ H_{\mathcal{T}^c}\end{smallmatrix}\right]$. Then, according to (4.3), $\mathbf{e}_I = P\left[\begin{smallmatrix} H_{\mathcal{T}} \\ 0\end{smallmatrix}\right]\mathbf{x}_e$. Consider a projection,

$$\mathbf{x}_e^\perp \triangleq \arg\min_{\mathbf{z}} \left\| H\mathbf{z} - P\begin{bmatrix} H_{\mathcal{T}} \\ 0\end{bmatrix}\mathbf{x}_e\right\|_1, \tag{4.7}$$

it follows that

$$\begin{aligned} \left\|H\mathbf{x}_e^\perp - P\begin{bmatrix} H_{\mathcal{T}} \\ 0\end{bmatrix}\mathbf{x}_e\right\|_1 &\leq \left\|H\mathbf{x}_e - P\begin{bmatrix} H_{\mathcal{T}} \\ 0\end{bmatrix}\mathbf{x}_e\right\|_1 \\ &\leq \|H_{\mathcal{T}^c}\mathbf{x}_e\|_1 \leq \epsilon. \end{aligned}$$

Then, by decomposing 1-norm on the disjoint sets $\mathcal{T}$ and $\mathcal{T}^c$, we have that

$$\begin{aligned} \left\|H\mathbf{x}_e^\perp - P\begin{bmatrix} H_{\mathcal{T}} \\ 0\end{bmatrix}\mathbf{x}_e\right\|_1 &= \left\|P\begin{bmatrix} H_{\mathcal{T}}(\mathbf{x}_e^\perp - \mathbf{x}_e) \\ H_{\mathcal{T}^c}\mathbf{x}_e^\perp\end{bmatrix}\right\|_1 \\ &= \left\|H_{\mathcal{T}}(\mathbf{x}_e^\perp - \mathbf{x}_e)\right\|_1 + \left\|H_{\mathcal{T}^c}\mathbf{x}_e^\perp\right\|_1. \end{aligned}$$

Thus, it follows that

$$\left\|H_{\mathcal{T}}(\mathbf{x}_e^\perp - \mathbf{x}_e)\right\|_1 + \left\|H_{\mathcal{T}^c}\mathbf{x}_e^\perp\right\|_1 \leq \epsilon. \tag{4.8}$$

Using the reverse triangle inequality $\|H_{\mathcal{T}}(\mathbf{x}_e^\perp - \mathbf{x}_e)\|_1 \geq |\|H_{\mathcal{T}}\mathbf{x}_e\|_1 - \|H_{\mathcal{T}}\mathbf{x}_e^\perp\|_1| \geq \|H_{\mathcal{T}}\mathbf{x}_e\|_1 - \|H_{\mathcal{T}}\mathbf{x}_e^\perp\|_1$, then (4.8) implies

$$\|H_{\mathcal{T}}\mathbf{x}_e\|_1 - \|H_{\mathcal{T}}\mathbf{x}_e^\perp\|_1 + \|H_{\mathcal{T}^c}\mathbf{x}_e^\perp\|_1 \leq \epsilon. \tag{4.9}$$

Notice $\sigma_1 = \max_{\mathbf{v}\in\mathbb{R}^n\setminus\{\mathbf{0}\}} \frac{\|H_{\mathcal{T}}\mathbf{v}\|_1}{\|H_{\mathcal{T}^c}\mathbf{v}\|_1}$, combining (4.6) and (4.9) yields

$$\|H_{\mathcal{T}}\mathbf{x}_e^\perp\|_1 - \|H_{\mathcal{T}^c}\mathbf{x}_e^\perp\|_1 \geq (\sigma_1 - 1)\epsilon.$$

Using the topological equivalence between 1-norm and 2-norm yields

$$\begin{aligned} \sqrt{|\mathcal{T}|}\|H_{\mathcal{T}}\mathbf{x}_e^\perp\|_2 - \|H_{\mathcal{T}^c}\mathbf{x}_e^\perp\|_2 &\geq (\sigma_1 - 1)\epsilon, \\ (\sqrt{|\mathcal{T}|}\overline{\sigma}_{\mathcal{T}} - \underline{\sigma}_{\mathcal{T}^c})\|\mathbf{x}_e^\perp\|_2 &\geq (\sigma_1 - 1)\epsilon, \\ \|\mathbf{x}_e^\perp\|_2 &\geq \frac{(\sigma_1 - 1)\epsilon}{\sqrt{|\mathcal{T}|}\overline{\sigma}_{\mathcal{T}} - \underline{\sigma}_{\mathcal{T}^c}}. \end{aligned} \tag{4.10}$$

Since $|\mathcal{T}| > \frac{\sigma_{\mathcal{T}^c}^2}{\overline{\sigma}_{\mathcal{T}}^2}$, the denominator of the right-hand side of (4.10) is positive. Moreover, we can choose a $\mathbf{v}_w \in \mathbb{R}^n$ satisfying $H\mathbf{v}_w = \mathbf{w}$, where $\mathbf{w}$ satisfies the condition in (4.4). Therefore there exists an $\mathbf{v}_w \in \mathbb{R}^n$ such that $\sigma_1 \geq \frac{\|H_{\mathcal{T}}\mathbf{v}_w\|_1}{\|H_{\mathcal{T}^c}\mathbf{v}_w\|_1} > 1$. Thus, the upper bound of $\|\mathbf{x}_e^\perp\|_2$ in (4.10) is always positive. Furthermore, according to (3.4) and (4.3),

$$\begin{aligned} D(\mathbf{y}_I) &= \arg\min_{\mathbf{z}} \|\mathbf{y}_I^\star + \mathbf{e}_I - H\mathbf{z}\|_1 \\ &= \arg\min_{\mathbf{z}} \left\|H\mathbf{x}^\star + P\begin{bmatrix} H_{\mathcal{T}} \\ 0\end{bmatrix}\mathbf{x}_e - H\mathbf{z}\right\|_1 \\ &= \mathbf{x}^\star + \arg\min_{\mathbf{z}} \left\|P\begin{bmatrix} H_{\mathcal{T}} \\ 0\end{bmatrix}\mathbf{x}_e - H\mathbf{z}\right\|_1. \end{aligned}$$

From (4.7), we have $\mathbf{x}^\star - \mathcal{D}(\mathbf{y}_I) = -\mathbf{x}_e^\perp$. Then

$$\|\mathbf{x}^\star - \mathcal{D}(\mathbf{y}_I)\|_2 = \left\|\mathbf{x}_e^\perp\right\|_2 \geq \frac{(\sigma_1 - 1)\epsilon}{\sqrt{|\mathcal{T}|}\overline{\sigma}_{\mathcal{T}} - \underline{\sigma}_{\mathcal{T}^c}},$$

which implies the upper bound of α in (4.5).

Next, we show that $\|\mathbf{y}_I - H\mathcal{D}(\mathbf{y}_I)\|_2 \leq \epsilon$. Since $\mathbf{x}^\star - \mathcal{D}(\mathbf{y}_I) = -\mathbf{x}_e^\perp$ and $\mathbf{y}_I = \mathbf{y}_I^\star + \mathbf{e}_I$, the residual is

$$\begin{aligned}
\|\mathbf{y}_I - H\mathcal{D}(\mathbf{y}_I)\|_2 &= \|\mathbf{y}_I^\star + \mathbf{e}_I - H(\mathbf{x}^\star + \mathbf{x}_e^\perp))\|_2 \\
&= \left\| H\mathbf{x}^\star + P\begin{bmatrix} H_{\mathcal{T}} \\ 0 \end{bmatrix}\mathbf{x}_e - H\mathbf{x}^\star - P\begin{bmatrix} H_{\mathcal{T}} \\ H_{\mathcal{T}^c} \end{bmatrix}\mathbf{x}_e^\perp \right\|_2 \\
&= \left\| P\left(\begin{bmatrix} H_{\mathcal{T}} \\ H_{\mathcal{T}^c} \end{bmatrix}\mathbf{x}_e^\perp - \begin{bmatrix} H_{\mathcal{T}} \\ 0 \end{bmatrix}\mathbf{x}_e \right) \right\|_2 \\
&\leq \left\| \begin{bmatrix} H_{\mathcal{T}} \\ H_{\mathcal{T}^c} \end{bmatrix}\mathbf{x}_e^\perp - \begin{bmatrix} H_{\mathcal{T}} \\ 0 \end{bmatrix}\mathbf{x}_e \right\|_1 \\
&\leq \|H_{\mathcal{T}}(\mathbf{x}_e^\perp - \mathbf{x}_e)\|_1 + \|H_{\mathcal{T}^c}\mathbf{x}_e^\perp\|_1.
\end{aligned} \tag{4.11}$$

Combining (4.8) and (4.11) yields $\|\mathbf{y}_I - H\mathcal{D}(\mathbf{y}_I)\|_2 \leq \epsilon$. ∎

Remark 4.4. If $\mathsf{null}(H_{\mathcal{T}^c})\backslash\mathsf{null}(H_{\mathcal{T}}) \neq \emptyset$, let $\mathbf{v}_n \in \mathsf{null}(H_{\mathcal{T}^c})\backslash\mathsf{null}(H_{\mathcal{T}})$, then we have $\|H_{\mathcal{T}^c}\mathbf{v}_n\|_1 = 0$ but $\|H_{\mathcal{T}}\mathbf{v}_n\|_1 > 0$. Thus, $\sigma_1 \geq \frac{\|H_{\mathcal{T}}\mathbf{v}\|_1}{\|H_{\mathcal{T}^c}\mathbf{v}\|_1}$ is infinite, which implies that the attack in (4.3) is (ϵ, α)-successful for all $\epsilon, \alpha \in \mathbb{R}_+$.

5. Resilient State Recovery.

In this section, we analyze the resilience of a weighted ℓ_1 estimator where the weights adaption law includes support prior. With CSP and Row-RIP, different estimation errors are derived. The quantified relationship between the learning prior precision and the estimation error is also clarified and analyzed.

5.1. Resilient Recovery without Support Prior.

In this subsection, the moving-horizon ℓ_1 estimator in (3.4) is considered. The following theorem gives the conditions for the resilient state recovery by the above decoder.

THEOREM 5.1 (**Resilient Recovery with CSP**). *Consider the measurement model in* (3.3)*, assume the attacks* $\mathbf{e}_i \in \Sigma_k$ *for all* $i \in I$*. If* $H \triangleright \mathit{CSP}(Tk)$ *with a parameter* $\beta \in (0, 1)$*, the estimation error due to the decoder in* (3.4) *can be upper bounded as*

$$\|\hat{\mathbf{x}} - \mathbf{x}\|_2 \leq \frac{2(1+\beta)}{\underline{\sigma}(1-\beta)}\varepsilon, \tag{5.1}$$

where $\underline{\sigma}$ *is the smallest singular value of* H*.*

Proof. Since $\hat{\mathbf{x}}$ is the optimal solution of (3.4),

$$\begin{aligned}
\|\mathbf{y} - H\hat{\mathbf{x}}\|_1 \leq \|\mathbf{y} - H\mathbf{x}^\star\|_1 = \|\mathbf{e}\|_1, \\
\|\mathbf{y} - H\mathbf{x}^\star + H(\mathbf{x}^\star - \hat{\mathbf{x}})\|_1 \leq \|\mathbf{e}\|_1, \\
\|\mathbf{e} + H\tilde{\mathbf{x}}\|_1 \leq \|\mathbf{e}\|_1,
\end{aligned} \tag{5.2}$$

then decomposing the 1-norm over $\mathcal{T}$ and $\mathcal{T}^c$ yields

$$\|\mathbf{e}_{\mathcal{T}} + H_{\mathcal{T}}\tilde{\mathbf{x}}\|_1 + \|\mathbf{e}_{\mathcal{T}^c} + H_{\mathcal{T}^c}\tilde{\mathbf{x}}\|_1 \leq \|\mathbf{e}_{\mathcal{T}}\|_1 + \|\mathbf{e}_{\mathcal{T}^c}\|_1. \tag{5.3}$$

Using the reverse triangle inequality yields

$$\|\mathbf{e}_{\mathcal{T}}\|_1 - \|H_{\mathcal{T}}\tilde{\mathbf{x}}\|_1 - \|\mathbf{e}_{\mathcal{T}^c}\|_1 + \|H_{\mathcal{T}^c}\tilde{\mathbf{x}}\|_1 \leq \|\mathbf{e}_{\mathcal{T}}\|_1 + \|\mathbf{e}_{\mathcal{T}^c}\|_1, \tag{5.4}$$

thus, it holds that

$$\|H_{\mathcal{T}^c}\tilde{\mathbf{x}}\|_1 \leq \|H_{\mathcal{T}}\tilde{\mathbf{x}}\|_1 + 2\|\mathbf{e}_{\mathcal{T}^c}\|_1.$$

Let $\mathbf{h} = H\tilde{\mathbf{x}}$, based on (3.2), it follows that

$$\|\mathbf{h}_{\mathcal{T}^c}\|_1 \leq \|\mathbf{h}_{\mathcal{T}}\|_1 + 2\varepsilon. \tag{5.5}$$

Since $H \triangleright \mathsf{CSP}(Tk)$, there exists $\beta \in (0,1)$ such that $\|\mathbf{h}_{\mathcal{T}}\|_1 \leq \beta\|\mathbf{h}_{\mathcal{T}^c}\|_1$. Thus,

$$\|\mathbf{h}_{\mathcal{T}}\|_1 \leq \frac{2\beta}{1-\beta}\varepsilon. \tag{5.6}$$

Then, using the triangle inequality and (5.5), (5.6) implies

$$\begin{aligned} \|\mathbf{h}\|_2 &\leq \|\mathbf{h}_{\mathcal{T}}\|_1 + \|\mathbf{h}_{\mathcal{T}^c}\|_1 \\ &\leq 2\|\mathbf{h}_{\mathcal{T}}\|_1 + 2\varepsilon \\ &\leq \frac{2(1+\beta)}{1-\beta}\varepsilon. \end{aligned} \tag{5.7}$$

Finally, combining (5.7) with $\underline{\sigma}\|\tilde{\mathbf{x}}\|_2 \leq \|\mathbf{h}\|_2$ yields the error bound in (5.9). ∎

The following corollary extends the results to a stable error bound based on the Row-RIP condition.

COROLLARY 5.2 (**Resilient Recovery with Row-RIP**). *Suppose* $H \triangleright \mathsf{rRIP}((a+1)Tk)$ *for some* $a > \max(1, \frac{1}{(\underline{\sigma}-1)^2})$, $a \in \frac{1}{Tk}\mathbb{Z}$. *If* $k \leq \frac{m}{2a+1}$ *and*

$$\delta_{(a+1)Tk} < \frac{a(\underline{\sigma}-\mu_1)^2}{(1+\sqrt{a})^2} - 1, \tag{5.8}$$

where $\mu_1 > 0$ *and* $\underline{\sigma}$ *denotes the smallest singular value of* H, *then the estimation error due to the decoder in* (3.4) *can be upper bounded as*

$$\|\hat{\mathbf{x}} - \mathbf{x}\|_2 \leq \frac{2\varepsilon}{\mu_1\sqrt{aTk}}. \tag{5.9}$$

Proof. For the sake of clean presentation, we use both $\mathcal{T}_0$ and $\mathcal{T}$ to represent the actual attack support in the proof. We sort the coefficients of $\mathbf{h}_{\mathcal{T}_0^c}$ in descending order and let $\mathcal{T}_j, j \in \{1,2,\cdots\}$[1] denote jth support in $\mathbf{h}_{\mathcal{T}_0^c}$ with size $aTk \in \mathbb{Z}$, where $a > 1$. Then,

$$\|\mathbf{h}_{\mathcal{T}_j}\|_2 \leq (aTk)^{-1/2}\|\mathbf{h}_{\mathcal{T}_j}\|_\infty \leq (aTk)^{-1/2}\|\mathbf{h}_{\mathcal{T}_{j-1}}\|_1. \tag{5.10}$$

Let $\mathcal{T}_{01} = \mathcal{T}_0 \cup \mathcal{T}_1$, we have

$$\|\mathbf{h}_{\mathcal{T}_{01}^c}\|_2 \leq \sum_{j\geq 2}\|\mathbf{h}_{\mathcal{T}_j}\|_2 \leq \frac{1}{\sqrt{aTk}}\sum_{j\geq 1}\|\mathbf{h}_{\mathcal{T}_j}\|_1 \leq \frac{1}{\sqrt{aTk}}\|\mathbf{h}_{\mathcal{T}_0^c}\|_1. \tag{5.11}$$

[1] $k \leq \frac{m}{2a+1}$ guarantees at least $\mathcal{T}_j, j \in \{1,2\}$ exist since $\sum_{j=0}^{3}|\mathcal{T}_j| = (2a+1)Tk \leq Tm$.

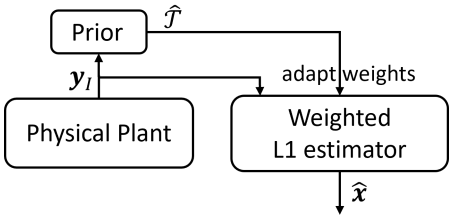

FIG. 1. *Schematic diagram of resilient estimation scheme with a data-driven prior.*

Following the same proof from (5.2) to (5.5) and substituting (5.11) into (5.5) yields

$$\begin{aligned}\sqrt{aTk}\|\mathbf{h}_{\mathcal{T}_{01}^c}\|_2 &\le \|\mathbf{h}_{\mathcal{T}_0}\|_1 + 2\varepsilon \\ &\le \sqrt{Tk}\|\mathbf{h}_{\mathcal{T}_0}\|_2 + 2\varepsilon \\ &\le \sqrt{Tk}\|\mathbf{h}_{\mathcal{T}_{01}}\|_2 + 2\varepsilon.\end{aligned} \tag{5.12}$$

According to the triangle inequality,

$$\|\mathbf{h}\|_2 \le \|\mathbf{h}_{\mathcal{T}_{01}^c}\|_2 + \|\mathbf{h}_{\mathcal{T}_{01}}\|_2 \le \left(\frac{1}{\sqrt{a}} + 1\right)\|\mathbf{h}_{\mathcal{T}_{01}}\|_2 + \frac{2\varepsilon}{\sqrt{aTk}}. \tag{5.13}$$

Since $H \triangleright \mathsf{rRIP}((a+1)Tk)$ and $\underline{\sigma}\|\tilde{\mathbf{x}}\|_2 \le \|\mathbf{h}\|_2$, we obtain

$$\underline{\sigma}\|\tilde{\mathbf{x}}\|_2 \le \left(\frac{1}{\sqrt{a}} + 1\right)\sqrt{1+\delta_{(a+1)Tk}}\|\tilde{\mathbf{x}}\|_2 + \frac{2\varepsilon}{\sqrt{aTk}}. \tag{5.14}$$

Since $\delta_{(a+1)Tk}$ satisfies the condition in (5.8),

$$\underline{\sigma} - \left(\frac{1}{\sqrt{a}} + 1\right)\sqrt{1+\delta_{(a+1)Tk}} > \mu_1. \tag{5.15}$$

Notice $a > \frac{1}{(\underline{\sigma}-1)^2}$ implies the existence of such $\mu_1 > 0$. Then (5.14) becomes

$$\mu_1\|\tilde{\mathbf{x}}\|_2 \le \frac{2\varepsilon}{\sqrt{aTk}} \tag{5.16}$$

which implies the estimation error bound in (5.9). ∎

5.2. Resilient Recovery with Support Prior. In this subsection, we present a resilient estimation scheme with an estimate of attack support, also known as the support prior. A weighted ℓ_1 estimator is utilized with weight adaption based on support prior. The scheme is illustrated in Figure 1. The prior information could be generated from any learning-based attack detector but estimates the attack support

$$\hat{\mathcal{T}} = \{\hat{\mathcal{T}}_i, \cdots, \hat{\mathcal{T}}_{i-T+1}\}.$$

The attack detector performs binary classification on each sensor channel. Let positive class (P) denote the node index that is in the support prior, while negative class (N) denotes the node index that is not in the support prior. Then a receiver operating characteristic (ROC) [12] table in Table 1 could be used to evaluate the prior.

We use a deterministic metric, called the positive predictive value (PPV, also called precision), to evaluate the qualification of prior support. The metric is given by

$$\mathsf{PPV} \triangleq \frac{TP(\text{true positive})}{TP + FP(\text{false positive})} = \frac{|\mathcal{T} \cap \hat{\mathcal{T}}|}{|\hat{\mathcal{T}}|}. \tag{5.17}$$

TABLE 1
ROC of the prior (TP: true positive, TN: true negative, FP: false positive, FN: false negative).

$\mathcal{T}\backslash\hat{\mathcal{T}}$	P	N
P	TP	FN
N	FP	TN

PPV is chosen as the metric because the positive class is used for the support prior, where minimizing false cases typically enhances the contribution to the resilient estimation scheme. If $\mathsf{PPV} > 50\%$, we say the prior is better than the random flip of a fair coin or random guessing.

Next, the corresponding moving-horizon estimator is given as a weighted ℓ_1 minimization program:

$$\begin{aligned} &\mathsf{Minimize} \sum_{j=i-T+1}^{i} \|\mathbf{y}_j - C\mathbf{x}_j\|_{1,\mathbf{w}(\hat{\mathcal{T}}_j,\omega)} \\ &\mathsf{Subject\ to}\ \ \mathbf{x}_{j+1} - A\mathbf{x}_j = 0,\ \ j = I-1, \end{aligned} \tag{5.18}$$

where $\omega \in (0,1)$. The optimization problem in (5.18) is equivalent to

$$\underset{\mathbf{z}\in\mathbb{R}^n}{\mathsf{Minimize}}\ \|\mathbf{y}_I - H\mathbf{z}\|_{1,\mathbf{w}(\hat{\mathcal{T}},\omega)}, \tag{5.19}$$

where $\mathbf{w}(\hat{\mathcal{T}},\omega) = \begin{bmatrix} \mathbf{w}(\hat{\mathcal{T}}_i,\omega) \\ \vdots \\ \mathbf{w}(\hat{\mathcal{T}}_{i-T+1},\omega) \end{bmatrix} \in \mathbb{R}^{Tm}$.

Next, a theorem is given to build a quantitative bridge between the prior precision and the estimation error based on the same Row-RIP condition.

THEOREM 5.3 (**Resilient Recovery with support prior**). *Consider the measurement model in* (3.3)*, assume the attacks* $\mathbf{e}_i \in \Sigma_k$ *for all* $i \in I$ *with noise bounded as* $\sum_{i\in\mathcal{T}^c} |\mathbf{e}_i| < \varepsilon$*. Let* $\mathcal{T}$ *be the unknown support of attack vector* $\mathbf{e}_I$*, then assume an estimate* $\hat{\mathcal{T}}$ *satisfying*

$$|\hat{\mathcal{T}}| = \rho|\mathcal{T}| \ \text{ and } |\mathcal{T}\cap\hat{\mathcal{T}}| = \mathit{PPV}|\hat{\mathcal{T}}|, \tag{5.20}$$

where $\rho > 0$ *and* $\mathit{PPV} \in (0,\ 1)$ *is the precision of the estimate. If the following conditions are satisfied;*

1. $H \triangleright \mathit{rRIP}((a+1)Tk)$ *for some* $a > \max\left(1, \frac{1}{(\sqrt{\rho}-1)^2}, (1-\mathit{PPV})\rho\right), a \in \frac{1}{Tk}\mathbb{Z}$*, where* $k \le \frac{m}{2a+1}$,
2. *The Row-RIP constant satisfies condition in* (5.8) *with same* μ_1*,*

then the estimation error due to the program in (5.19) *can be upper bounded as*

$$\|\hat{\mathbf{x}} - \mathbf{x}\|_2 \le \frac{2\varepsilon}{\mu_2\sqrt{aTk}}, \tag{5.21}$$

where

$$\mu_2 = \mu_1 + \frac{(1-\omega)(1-\sqrt{\kappa})}{\sqrt{a}}\sqrt{1+\delta_{(a+1)Tk}}, \tag{5.22}$$

and $\kappa \triangleq 1 + \rho - 2\mathit{PPV}\rho$.

Proof. For a vector $\mathbf{z} \in \mathbb{R}^n$ and two sets $\mathcal{S}_1, \mathcal{S}_2 \subset \{1, 2, \ldots, n\}$, it holds that

$$\|\mathbf{z}_{\mathcal{S}_1 \cup \mathcal{S}_2}\|_1 = \|\mathbf{z}_{\mathcal{S}_1}\|_1 + \|\mathbf{z}_{\mathcal{S}_2}\|_1 - \|\mathbf{z}_{\mathcal{S}_1 \cap \mathcal{S}_2}\|_1.$$

If $\mathcal{S}_1$ and $\mathcal{S}_2$ are disjoint sets (i.e. $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$), then $\|\mathbf{z}_{\mathcal{S}_1 \cup \mathcal{S}_2}\|_1 = \|\mathbf{z}_{\mathcal{S}_1}\|_1 + \|\mathbf{z}_{\mathcal{S}_2}\|_1$. Additionally, we use $\mathcal{T}_0 = \mathcal{T}$ to represent the unknown support of attack vector $\mathbf{e}_I$, thus $|\mathcal{T}_0| \leq Tk$. We also use $\hat{\mathcal{T}}_0 = \hat{\mathcal{T}}$ to represent the estimated support of the attack support.

Let $\hat{\mathbf{x}}$ be the optimal solution of (5.19), $\tilde{\mathbf{x}} = \mathbf{x} - \hat{\mathbf{x}}$, and $\mathbf{h} = H\tilde{\mathbf{x}}$. Similar to (5.2), we have

$$\|\mathbf{e} + \mathbf{h}\|_{1,\mathbf{w}(\hat{\mathcal{T}}_0,\omega)} \leq \|\mathbf{e}\|_{1,\mathbf{w}(\hat{\mathcal{T}}_0,\omega)}. \tag{5.23}$$

By the definition of the weighted 1-norm, it follows that

$$\omega \left\|\mathbf{e}_{\hat{\mathcal{T}}_0} + \mathbf{h}_{\hat{\mathcal{T}}_0}\right\|_1 + \left\|\mathbf{e}_{\hat{\mathcal{T}}_0{}^c} + \mathbf{h}_{\hat{\mathcal{T}}_0{}^c}\right\|_1 \leq \omega \left\|\mathbf{e}_{\hat{\mathcal{T}}_0}\right\|_1 + \left\|\mathbf{e}_{\hat{\mathcal{T}}_0{}^c}\right\|_1. \tag{5.24}$$

Then decomposing the 1-norm over $\mathcal{T}_0$ and $\mathcal{T}_0^c$ on both sides yields

$$\begin{aligned} &\omega \left\|\mathbf{e}_{\hat{\mathcal{T}}_0 \cap \mathcal{T}_0} + \mathbf{h}_{\hat{\mathcal{T}}_0 \cap \mathcal{T}_0}\right\|_1 + \omega \left\|\mathbf{e}_{\hat{\mathcal{T}}_0 \cap \mathcal{T}_0^c} + \mathbf{h}_{\hat{\mathcal{T}}_0 \cap \mathcal{T}_0^c}\right\|_1 \\ &\quad + \left\|\mathbf{e}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0} + \mathbf{h}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0}\right\|_1 + \left\|\mathbf{e}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0^c} + \mathbf{h}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0^c}\right\|_1 \\ &\leq \omega \left\|\mathbf{e}_{\hat{\mathcal{T}}_0 \cap \mathcal{T}_0}\right\|_1 + \left\|\mathbf{e}_{\hat{\mathcal{T}}_0 \cap \mathcal{T}_0^c}\right\|_1 + \left\|\mathbf{e}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0}\right\|_1 + \left\|\mathbf{e}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0^c}\right\|_1. \end{aligned} \tag{5.25}$$

By using the reverse triangle inequality and arranging the inequality, we obtain

$$\begin{aligned} &\omega \left\|\mathbf{h}_{\hat{\mathcal{T}}_0 \cap \mathcal{T}_0^c}\right\|_1 + \left\|\mathbf{h}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0^c}\right\|_1 \\ &\quad \leq \left\|\mathbf{h}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0}\right\|_1 + \omega \left\|\mathbf{h}_{\hat{\mathcal{T}}_0 \cap \mathcal{T}_0}\right\|_1 + 2\left(\|\mathbf{e}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0^c}\|_1 + \|\mathbf{e}_{\hat{\mathcal{T}}_0 \cap \mathcal{T}_0^c}\|_1\right). \end{aligned} \tag{5.26}$$

Next, adding and subtracting $\omega\|\mathbf{h}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0^c}\|_1$ on the left side of (5.26), and $\omega\|\mathbf{h}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0}\|_1$ and $\omega\|\mathbf{e}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0^c}\|_1$ on the right yields

$$\begin{aligned} &\omega \left\|\mathbf{h}_{\mathcal{T}_0^c}\right\|_1 + (1-\omega)\left\|\mathbf{h}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0^c}\right\|_1 \\ &\quad \leq (1-\omega)\left\|\mathbf{h}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0}\right\|_1 + \omega\|\mathbf{h}_{\mathcal{T}_0}\|_1 + 2\left(\omega\|\mathbf{e}_{\mathcal{T}_0^c}\|_1 + (1-\omega)\left\|\mathbf{e}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0^c}\right\|_1\right). \end{aligned} \tag{5.27}$$

Again, adding and subtracting $(1-\omega)\|\mathbf{h}_{\hat{\mathcal{T}}_0 \cap \mathcal{T}_0^c}\|_1$ on the left side of (5.27) and substituting $\sum_{i \in \mathcal{T}_0^c} |\mathbf{e}_i| < \varepsilon$ yields

$$\|\mathbf{h}_{\mathcal{T}_0^c}\|_1 \leq \omega\|\mathbf{h}_{\mathcal{T}_0}\|_1 + (1-\omega)\left(\left\|\mathbf{h}_{\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0}\right\|_1 + \left\|\mathbf{h}_{\hat{\mathcal{T}}_0 \cap \mathcal{T}_0^c}\right\|_1\right) + 2\varepsilon. \tag{5.28}$$

Since $\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0$ and $\hat{\mathcal{T}}_0 \cap \mathcal{T}_0^c$ are disjoint and $(\hat{\mathcal{T}}_0{}^c \cap \mathcal{T}_0) \cup (\hat{\mathcal{T}}_0 \cap \mathcal{T}_0^c) = \mathcal{T}_0 \cup \hat{\mathcal{T}}_0 \setminus \hat{\mathcal{T}}_0 \cap \mathcal{T}_0$, we rewrite (5.28) as

$$\|\mathbf{h}_{\mathcal{T}_0^c}\|_1 \leq \omega\|\mathbf{h}_{\mathcal{T}_0}\|_1 + (1-\omega)\left\|\mathbf{h}_{\mathcal{T}_0 \cup \hat{\mathcal{T}}_0 \setminus \hat{\mathcal{T}}_0 \cap \mathcal{T}_0}\right\|_1 + 2\varepsilon. \tag{5.29}$$

We sort the coefficients of $\mathbf{h}_{\mathcal{T}_0^c}$ in descending order, and let $\mathcal{T}_j, j \in \{1, 2, \cdots\}$ denote jth support in $\mathbf{h}_{\mathcal{T}_0^c}$ with size $aTk \in \mathbb{Z}$, where $a > 1$. Since $\mathbf{h}_{\mathcal{T}_1}$ corresponds to the biggest coefficients in $\mathbf{h}_{\mathcal{T}_0^c}$, and $|\hat{\mathcal{T}}_0 \setminus \hat{\mathcal{T}}_0 \cap \mathcal{T}_0| = (1 - \mathsf{PPV})\rho Tk \leq aTk = |\mathcal{T}_1|$, we have

$\|\mathbf{h}_{\hat{\mathcal{T}}_0\setminus\hat{\mathcal{T}}_0\cap\mathcal{T}_0}\|_2 \le \|\mathbf{h}_{\mathcal{T}_1}\|_2$, then $\|\mathbf{h}_{\mathcal{T}_0\cup\hat{\mathcal{T}}_0\setminus\hat{\mathcal{T}}_0\cap\mathcal{T}_0}\|_2 \le \|\mathbf{h}_{\mathcal{T}_{01}}\|_2$. Additionally, according to the topological equivalence of vector norm in (1.4), since $|\mathcal{T}_0\cup\hat{\mathcal{T}}_0\setminus\hat{\mathcal{T}}_0\cap\mathcal{T}_0| = \kappa Tk$, it follows that

$$\left\|\mathbf{h}_{\mathcal{T}_0\cup\hat{\mathcal{T}}_0\setminus\hat{\mathcal{T}}_0\cap\mathcal{T}_0}\right\|_1 \le \sqrt{\kappa Tk}\left\|\mathbf{h}_{\mathcal{T}_0\cup\hat{\mathcal{T}}_0\setminus\hat{\mathcal{T}}_0\cap\mathcal{T}_0}\right\|_2 \le \sqrt{\kappa Tk}\,\|\mathbf{h}_{\mathcal{T}_{01}}\|_2\,. \tag{5.30}$$

Similarly,

$$\|\mathbf{h}_{\mathcal{T}_0}\|_1 \le \sqrt{Tk}\|\mathbf{h}_{\mathcal{T}_0}\|_2 \le \sqrt{Tk}\|\mathbf{h}_{\mathcal{T}_{01}}\|_2. \tag{5.31}$$

Substituting (5.31) and (5.30) into (5.29) yields

$$\left\|\mathbf{h}_{\mathcal{T}_0^c}\right\|_1 \le \left[\omega\sqrt{Tk} + (1-\omega)\sqrt{\kappa Tk}\right]\|\mathbf{h}_{\mathcal{T}_{01}}\|_2 + 2\varepsilon. \tag{5.32}$$

Substituting (5.11) into (5.32) yields

$$\sqrt{aTk}\|\mathbf{h}_{\mathcal{T}_{01}^c}\|_2 \le \left[\omega\sqrt{Tk} + (1-\omega)\sqrt{\kappa Tk}\right]\|\mathbf{h}_{\mathcal{T}_{01}}\|_2 + 2\varepsilon. \tag{5.33}$$

By applying the triangle inequality, we obtain

$$\|\mathbf{h}\|_2 \le \left(\frac{\omega + (1-\omega)\sqrt{\kappa}}{\sqrt{a}} + 1\right)\|\mathbf{h}_{\mathcal{T}_{01}}\|_2 + \frac{2\varepsilon}{\sqrt{aTk}}. \tag{5.34}$$

Since $H \triangleright \mathsf{rRIP}((a+1)Tk)$ and $\underline{\sigma}\|\tilde{\mathbf{x}}\|_2 \le \|\mathbf{h}\|_2$, we obtain

$$\underline{\sigma}\|\tilde{\mathbf{x}}\|_2 \le \left(\frac{\omega + (1-\omega)\sqrt{\kappa}}{\sqrt{a}} + 1\right)\sqrt{1+\delta_{(a+1)Tk}}\|\tilde{\mathbf{x}}\|_2 + \frac{2\varepsilon}{\sqrt{aTk}}. \tag{5.35}$$

Subtracting $(\frac{1}{\sqrt{a}}+1)\sqrt{1+\delta_{(a+1)Tk}}\|\tilde{\mathbf{x}}\|_2$ on both sides yields

$$\left[\underline{\sigma} - \left(\frac{1}{\sqrt{a}}+1\right)\sqrt{1+\delta_{(a+1)Tk}}\right]\|\tilde{\mathbf{x}}\|_2 \le \frac{\omega + (1-\omega)\sqrt{\kappa} - 1}{\sqrt{a}}\sqrt{1+\delta_{(a+1)Tk}}\|\tilde{\mathbf{x}}\|_2 + \frac{2\varepsilon}{\sqrt{aTk}}.$$

Since $\delta_{(a+1)Tk}$ satisfies the condition in (5.8), the inequality in (5.15) holds. Then

$$\mu_1\|\tilde{\mathbf{x}}\|_2 \le \frac{\omega + (1-\omega)\sqrt{\kappa} - 1}{\sqrt{a}}\sqrt{1+\delta_{(a+1)Tk}}\|\tilde{\mathbf{x}}\|_2 + \frac{2\varepsilon}{\sqrt{aTk}}.$$

Let μ_2 be given as in (5.22), then

$$\mu_2\|\tilde{\mathbf{x}}\|_2 \le \frac{2\varepsilon}{\sqrt{aTk}}$$

which implies the estimation error bound in (5.21). ∎

Remark 5.4. By comparing the estimation error bound in (5.9) and (5.21), resilient recovery has a smaller estimation error by adding the measurement prior if $\mu_2 > \mu_1$, which is guaranteed by $\kappa = \rho + 1 - 2\mathsf{PPV}\rho < 1$. This condition is equivalent to $\mathsf{PPV} > 50\%$. In other words, if the prior is at least better than the random flip of a fair coin, then the resilient recovery with prior outperforms the resilient recovery without prior.

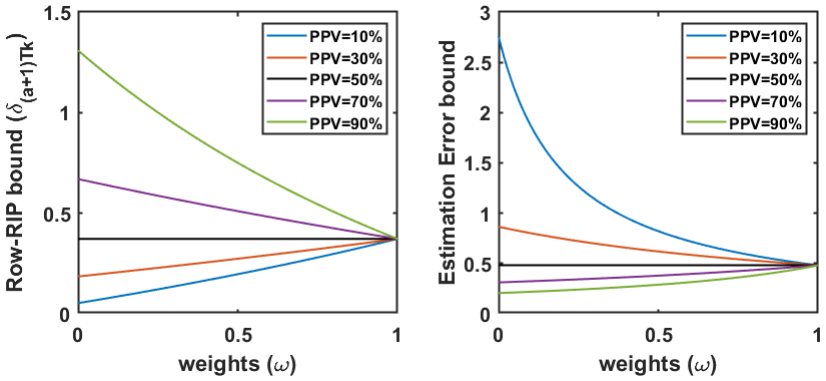

FIG. 2. *The effects of weight setting ω of the weighted ℓ_1 decoder in* (5.19) *and the precision* PPV *of the prior on the performance of resilient state recovery. (Other variables are set as $\rho = 1$, $\underline{\sigma} = 2$, $a = 2$, $Tk = 50$).*

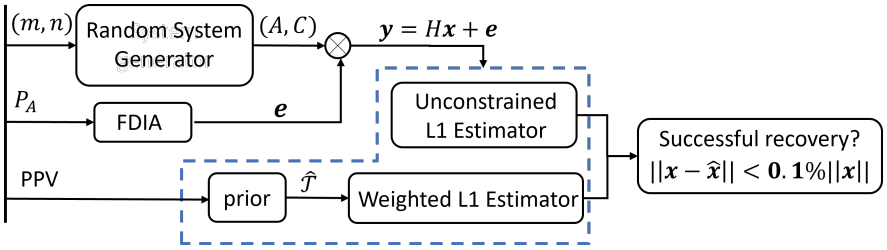

FIG. 3. *Block diagram depiction of the Monte Carlo test scenario. ($(m,n)$is the system dimension pair, m is the dimension of measurements, n is the dimension of states, P_A is the attack-to-normal-signal ratio, (A,C) is system dynamic pair,* PPV *is the precision of the prior).*

To visualize the effect of the weight ω of the weighted ℓ_1 decoder in (5.19) and the precision PPV of the prior on the performance of the state recovery, a plot of the estimation error bound in (5.21) and the Row-RIP constant's upper bound in (5.8) is shown in Figure 2. $\mathsf{PPV} = 50\%$ is a boundary where the weight setting does not improve or reduce the performance of the state recovery. Higher precision of the prior leads to better performance of the state recovery (less strict Row-RIP condition and smaller estimation error). Moreover, if the prior is better than the random flip of a fair coin, smaller weights correspond to better resilient recovery performance. If the prior is worse than the random flip of a fair coin, it is best to choose $\omega = 1$ which reduces the weighted ℓ_1 estimation to ℓ_1 estimation.

6. Numerical Simulation. In this section, we present Monte Carlo tests for the developed resilient state recovery schemes: weighted ℓ_1 estimator with prior, and ℓ_1 estimator without prior, as shown in Figure 3. The resilient estimation scheme is tested on random linear systems with different attack-to-normal-signal ratios and different prior precision.

The simulations are processed using the following procedure:

1. Select system dimension pair (m,n), where m is the size of measurements, n is the size of states, and $m > n$. Then generate an observable LTI model $\mathbf{x}_{i+1} = A\mathbf{x}_i$, $\mathbf{y}_i = C\mathbf{x}_i$, represented by pair (A,C), where $A \in \mathbb{R}^{n\times n}$ and $C \in \mathbb{R}^{m\times n}$ are sampled with independent Gaussian entries [5]. Although

the RIP conditions in the previous sections are NP-hard to verify, it has been shown that Gaussian matrices with independent identically distributed entries satisfy the RIP condition with overwhelming probabilities [5, 9].

2. Select an attack-to-normal-signal ratio P_A, and find attack location indexed in $\mathcal{T}$ randomly, where $|\mathcal{T}| \leq mP_A$. Then generate attack vectors by (4.2), and inject it into the selected attack location.
3. For the unconstrained ℓ_1 estimator, use linear programming to solve the ℓ_1 minimization problem (3.4), such that

$$\min_{t,\mathbf{x}} \mathbf{1}^\top t, \text{ subject to}: -t \leq \mathbf{y}_I - H\mathbf{x} \leq t. \tag{6.1}$$

4. For the weighted ℓ_1 estimator, simulate the prior information with a particular PPV by using a Bernoulli distributed agreement model:

$$\mathbf{q}_i = \epsilon_i \hat{\mathbf{q}}_i + (1-\epsilon_i)(1-\hat{\mathbf{q}}_i), \tag{6.2}$$

where $\epsilon_i \sim \mathcal{B}(1, \mathbf{p}_i)$ models the agreement between the estimate support prior $\hat{\mathcal{T}}$ and the actual attack support $\mathcal{T}$, its probability $\mathbf{p}_i = E[\epsilon_i] = \mathsf{Pr}\{\epsilon_i = 1\}$ approximates the given precision of the support prior PPV. Additionally, $\mathbf{q} \in \{0,1\}^n$ is an indicator vector of $\mathcal{T} \subseteq \{1, \ldots, n\}$ defined element-wise as

$$\mathbf{q}_i = \begin{cases} 0 & \text{if } i \in \mathcal{T} \\ 1 & \text{otherwise.} \end{cases} \tag{6.3}$$

Then the weighted ℓ_1 minimization problem in (5.18) is solved by

$$\min_{t,\mathbf{x}} \mathbf{w}(\hat{\mathcal{T}}, \omega)^\top t, \text{ subject to}: -t \leq \mathbf{y}_I - H\mathbf{x} \leq t, \tag{6.4}$$

where $\mathbf{w}(\hat{\mathcal{T}}, \omega)$ is the weight vector defined as (1.2) with the support prior $\hat{\mathcal{T}}^c$. According to Figure 2, we set $\omega = 0.01$ when the precision is above 50%, and $\omega = 0.99$ when the precision is lower than 50%.

5. Establish a performance evaluation criteria: we determined successful state recovery if the absolute estimation error is less than 0.1% of the nominal absolute value of states. To calculate the success percentage, 10000 trials of simulation are performed for different resilient estimation schemes.
6. Repeat the described simulation procedure for various settings of the system dimension (m, n), the attack-to-normal signal ratio P_A, and the precision PPV.

The results in Figure 4 and Figure 5 show the impact of system dimension (m, n) (especially the relationship between m and n), the prior precision PPV and the attack-to-normal-signal ratio P_A on the performance of resilient recovery using the unconstrained ℓ_1 estimator and the weighted ℓ_1 estimator. The x-axis represents the size of measurements $m \in [10, 86]$, while the y-axis represents the dimension of states $n \in [5, 43]$. Each small rectangular block in the subplots represents one of 400 different systems, each with a different dimension (m_{new}, n), where $m_{\text{new}} = \max(m, n)$.[2] Thus, the lower left corner of each subplot corresponds to the smallest measurement redundancy, while the upper right corner represents the largest measurement redundancy. We define successful recovery as the case where the absolute estimation error is less than 0.1% of the magnitude of the nominal state. By running 10000 trials

[2] $m_{\text{new}} \geq n$ must be guaranteed otherwise state recovery could not be accomplished.

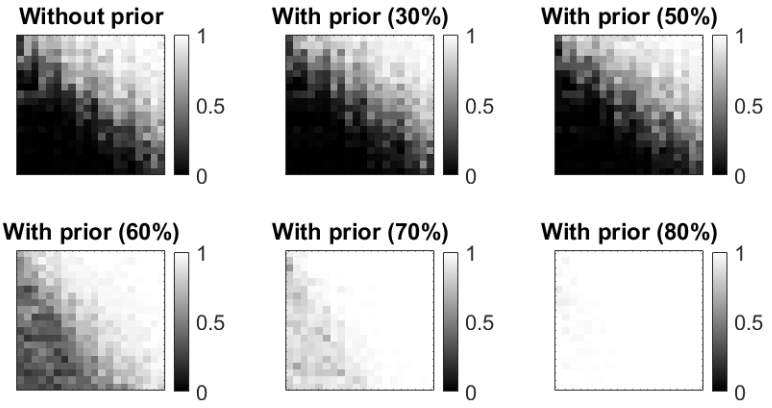

FIG. 4. *The success ratio of resilient recovery (from black* 0% *to white* 100%*) of unconstrained* ℓ_1 *estimator (without prior) and weighed* ℓ_1 *estimator with the prior (with prior) on* 400 *different dimensional LTI systems (x-axis: measurement dimension* $m_{new} \in [10, 86]$*, y-axis: state dimension* $n \in [5, 43]$*) with the attack-to-normal-signal ratio* $P_A = 40\%$*. Different precision, from* 30% *to* 80%*, of the prior are simulated.*

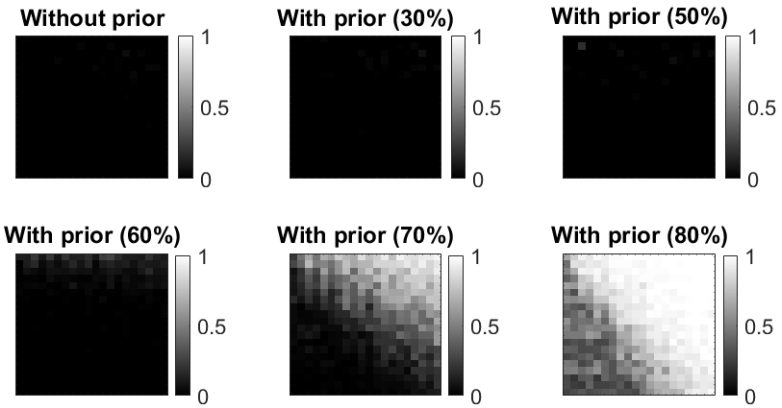

FIG. 5. *The success ratio of resilient recovery (from black* 0% *to white* 100%*) of unconstrained* ℓ_1 *estimator (without prior) and weighed* ℓ_1 *estimator with the prior (with prior) on* 400 *different dimensional LTI systems (x-axis: measurement dimension* $m_{new} \in [10, 86]$*, y-axis: state dimension* $n \in [5, 43]$*) with the attack-to-normal-signal ratio* $P_A = 60\%$*. From left to right, the mean value of agreement probability (positively correlated to the precision of the prior) is* 60%*,* 70%*, and* 80% *respectively.*

of simulation for each system with different dimensions, the grey level in the plots indicates the ratio of the number of successful estimations to 10000. The black color indicates 0% successful cases, while the white color indicates 100% successful cases.

In Figure 4, 40% measurements are attacked and the precision of the prior is simulated from 30% to 80%. The grey level becomes lighter from the lower left corner to the upper right corner in all subplots. This change indicates that larger measurement redundancy enables better resiliency of the system. There is an approximate boundary between the dark grey portion and the light grey portion. For the unconstrained ℓ_1 estimator, the boundary is around $m = 2n$, which is consistent with literature [10, 31]. As shown in the first row, when the precision of the prior is less than or equal to 50%, the estimation performance of the weighted ℓ_1 estimator (with prior)

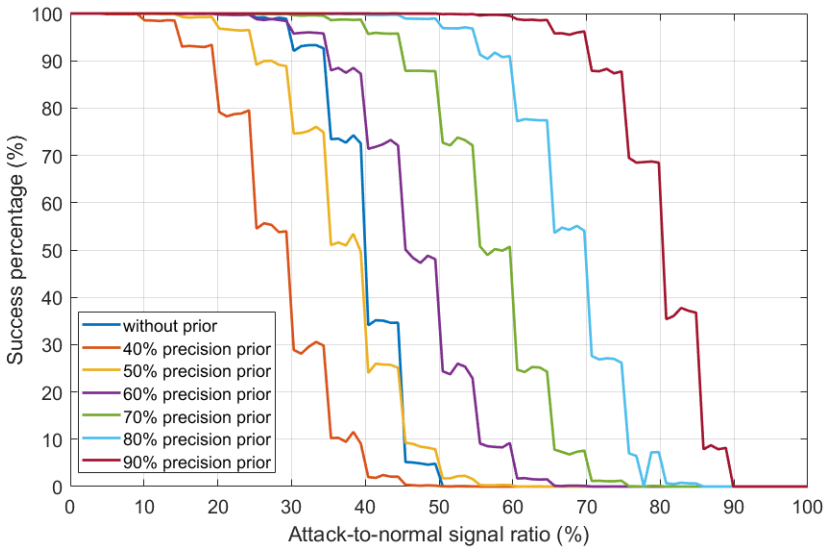

FIG. 6. *A comparison of estimation performance with different attack-to-normal-signal ratio* $P_A \in [0,1]$ *between unconstrained* ℓ_1 *estimator (without prior) and weighted* ℓ_1 *estimator with the prior (with different precision of prior). The precision of the prior is ranging from* 40% *to* 90%*, and the system dimension is* $m = 2n, n = 10$.

is similar to the unconstrained ℓ_1 estimator (without prior). As shown in the second row, the boundary moves to the lower left corner more when we use the weighted ℓ_1 estimation with the prior of higher precision. This shift indicates that if the prior is better than the random flip of a fair coin, less measurement redundancy is required for successful state recovery. By comparing all weighted ℓ_1 estimators with the prior of different precision, a positive correlation between the precision of the prior and the resilient estimation performance is observed as discussed in Theorem 5.3.

In Figure 5, we increase the attck-to-normal signal ratio to 60%. As proved in literature [10, 31] and in Theorem 5.2, the 2s-observability assumption is violated so that the unconstrained ℓ_1 estimator fails. When the prior's precision is less than 50%, the estimation performance cannot be improved by including the support prior $\hat{\mathcal{T}}$. Thus, the subplots in the first row are all black. But the second row immediately shows the improvement of the estimation performance by including the support prior $\hat{\mathcal{T}}$ with higher precision than 50%.

Furthermore, we plot the success ratio of the resilient recovery of both the unconstrained ℓ_1 estimator and the weighted ℓ_1 estimator with the prior for recovering states from attacked measurements as a function of the attack-to-normal-signal ratio in Figure 6. The S-shape curve between the success ratio of state recovery and the attack percentage indicates that the resilient recovery will maintain a high success ratio when a particular percentage of sensors remain safe. Beyond that point, the success ratio of state recovery rapidly declines. Flat portions of the curves in Figure 6 indicate that the success ratio of state recovery remains largely unchanged when there are only minor differences in the number of attacked channels.

Conversely, the dark blue line, representing the unconstrained ℓ_1 estimator without prior, shows the exact limitation proven in [10, 31]: more than 50% sensors are required to be safe. However, this limitation is relaxed by using a weighted ℓ_1 esti-

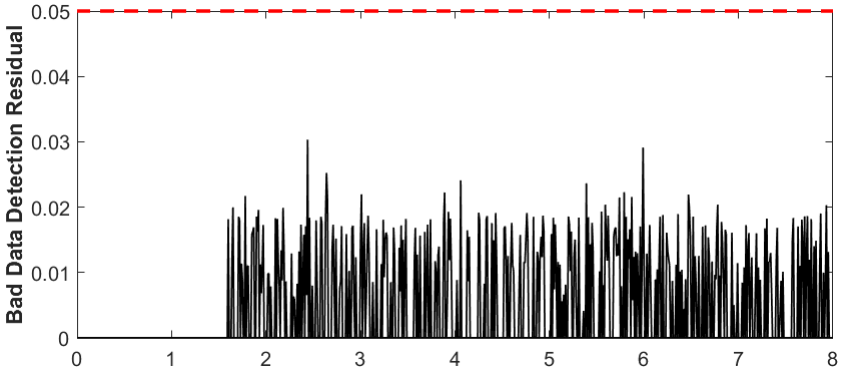

FIG. 7. *Bad data detection result (the residual threshold is set as* 0.05*).*

mator with prior as long as the precision of the prior is greater than 50%, as proved in Theorem 5.3. If the precision of prior is less than 50% (orange line) or lies on the boundary (yellow line), the resilient recovery performance may not be better than the unconstrained ℓ_1 estimator without prior. This Monte Carlo simulation confirms the proven limitation of the unconstrained ℓ_1 estimator in literature and validates the quantitative correlation between the precision of the prior and the resilient recovery performance outlined in this paper.

7. Application Simulation. In this section, we use a linear control system on the IEEE 14-bus system[3] to validate our theoretical claims. The bus system has 14 buses and 5 generators, and each bus in the network is assumed to be equipped with IIoT measurement devices with the capability of measuring active power injections and flow measurements. The detailed physical system construction can be found in [2], which includes the plant model, proportional and integral (PI) regulator, and measurement model. The goal of the resilient observer is to estimate 10 states, including 5 generator rotor angles and 5 generator frequencies, correctly from 19 measurements including 5 generator frequencies and net powers at 14 buses.

We implement the attacks designed in (4.3), 20% of the measurements are compromised, so $|\mathcal{T}| = 19 \times 0.2 \approx 4$ sensors are randomly selected to be attacked. Figure 7 indicates the attack designed in (4.3) is capable of bypassing the residual-based bad data detector. As shown in Figure 10, an observer without resilient design, such as a Luenberger observer, is unstable under such attacks. Although such attacks are too strong to be implemented in practice due to the assumption of knowing the system's model, it is sufficient for the comparison of the resiliency of resilient observers in this application example since resilient estimators are mainly affected by the number of attacked sensors instead of the design of attacks.

We used a Gaussian process regression (GPR)-based attack localization algorithm, from [40], to generate the support prior. The prior generator is to use GPR models to learn the nominal maps from hidden auxiliary states to the measurements. Attacked measurements are revealed if they cannot be explained by the trained GPR models with high likelihood. As discussed in Remark 5.4 and shown in the numerical simulation section, better resiliency through the proposed weighted ℓ_1 estimator is due to the precision guarantee of prior over 50%. However, given the probabilistic

[3]https://labs.ece.uw.edu/pstca/pf14/pg_tca14bus.htm

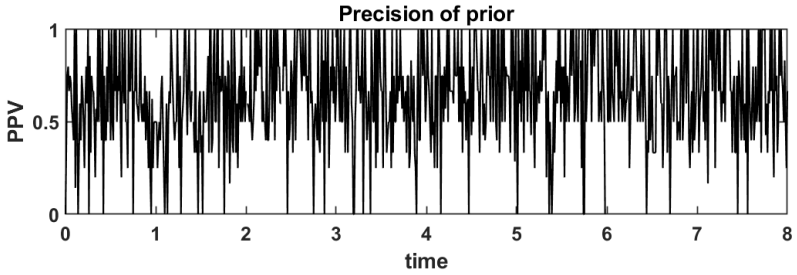

FIG. 8. *The precision of support prior generated by the GPR-based attack localizer for the power grid (The mean of precision is* 65.5%*).*

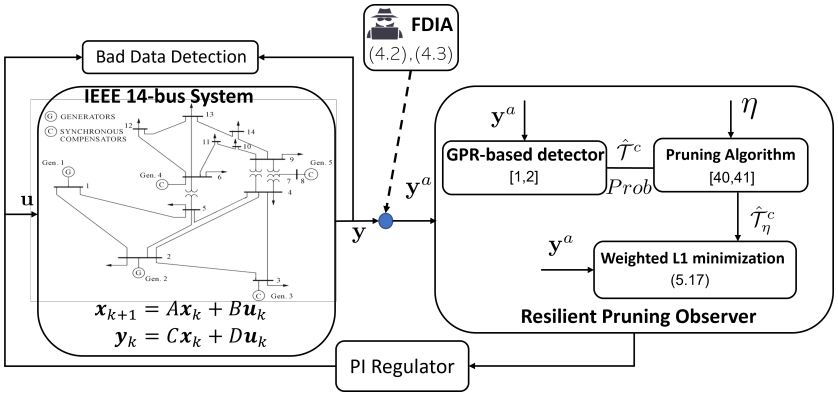

FIG. 9. *Block diagram depiction of the implementation of the resilient pruning observer (RPO) on IEEE* 14 *bus system (FDIA: false data injection attack).*

nature of data-driven approaches, relying solely on the prior derived from data-driven attack detectors may not rigorously ensure performance consistently. Therefore, we adopted a robustness mechanism, called pruning algorithm [39], to reinforce the prior. In this simulation, the mean of localization precision achieved $E(\mathsf{PPV}) = 65.5\%$, as shown in Figure 8. So the generated prior information is better than the random flip of a fair coin. As shown in Figure 9, we call the observer design, composed of the GPR-based localization algorithm, the pruning algorithm, and the weighted ℓ_1 estimator, the resilient pruning observer (RPO).

In this simulation, we compared RPO with other typical resilient observer designs, such as an event-triggered Luenberger observer (ETLO) [31], an unconstrained ℓ_1 observer (UL1O) [10], and a multimodel observer (MMO) [2]. UL1O utilized the ℓ_1 minimization program to recover the sparse attack signal [10]. ETLO is a resilient moving-horizon Luenberger-like observer solved by a projected gradient descent technique [31]. MMO is a constrained ℓ_1 estimator whose constraints include the system update law and the GPR attack detector [2]. UL1O, ETLO, and MMO assume $2Tk$-observability which is rephrased in Corollary 5.2 as a Row-RIP condition of order $(a+1)Tk$. This condition is satisfied when half of the sensors are safe [10, 8]. In this application example, 4 of 19 sensors are attacked. As further indicated in Theorem 5.3, the same-level Row-RIP condition, as the one in Corollary 5.2, is designed for our proposed weighted ℓ_1 estimator. Thus, the condition of the proposed RPO is also satisfied.

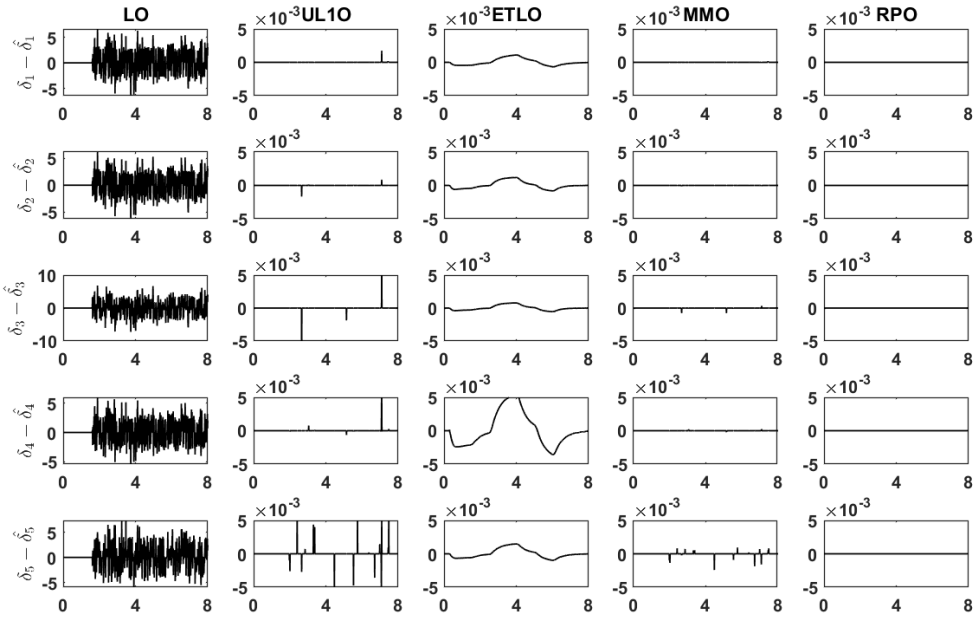

FIG. 10. *A comparison of the estimation errors of generator rotor angles by 5 observers (LO: Luenberger observer, UL1O: unconstrained ℓ_1 observer, MMO: multimodel observer, ETLO: event-triggered Luenberger observer, RPO: the proposed resilient pruning observer).*

TABLE 2
Error Metric Values.

	RMS Metric				
	LO	**UL1O**	**MMO**	**ETLO**	**RPO**
δ_1	2.953	$6.2e-5$	$8.28e-6$	$5.61e-4$	$1.13e-15$
δ_2	2.881	$6.66e-5$	$7.89e-6$	$8.24e-4$	$2.55e-16$
δ_3	3.090	$5.45e-4$	$4.65e-5$	$6.06e-4$	$8.98e-16$
δ_4	3.195	$2.55e-4$	$2.01e-5$	$3.6e-3$	$9.44e-16$
δ_5	3.412	$6.41e-4$	$1.95e-4$	$9.66e-4$	$6.62e-16$
	Max. Ans. Metric				
	LO	**UL1O**	**MMO**	**ETLO**	**RPO**
δ_1	9.729	0.0017	$1.82e-4$	0.0012	$3.1e-14$
δ_2	9.482	0.0017	$1.53e-4$	0.0017	$5.94e-15$
δ_3	13.423	0.0116	$8.37e-4$	0.0013	$2.45e-14$
δ_4	12.834	0.0058	$3.55e-4$	0.0079	$2.42e-14$
δ_5	12.592	0.0078	0.0027	0.0021	$1.28e-14$

Figure 10 and Table 2 show the estimation errors of generator rotor angles by 4 resilient observers. LO becomes unstable in the presence of attacks. UTLO, ETLO, and MMO have non-negligible errors in terms of the magnitude of nominal states ($|\delta| < 0.005$). ETLO has smooth estimation errors since it is a dynamic observer design. MMO is an observer design that incorporates a prior measurement, so it works better than UL1O. However, the prior performance is not stable due to the uncertainty of the data-driven detector. By adding the pruning algorithm, the precision of prior

information ($E(\mathsf{PPV}) = 65.5\%$) is guaranteed to be better than a random flip of a fair coin. Therefore, RPO produces better estimation performance, which validates the statements in Remark 5.4.

8. Conclusion. An enhanced resilient state estimation scheme is developed that uses prior information to improve the resilience of the weighted ℓ_1 estimator. CSP and Row-RIP are properties introduced to measure the system's resilience under attacks. The traditional 2s-observability has also been shown to be one case of the proposed CSP. An optimization-based program is developed to generate a feasible attack against an ℓ_1 estimator while the system's CSP is violated. The improvement of the weighted ℓ_1 estimator's resilience is quantified with respect to the precision of the prior. The quantified relationship provides a theoretical guarantee of weight design for the weighted ℓ_1 estimator.

Through the analysis in this paper, we conclude that the precision of the prior is positively correlated to the resilience of the weighted ℓ_1 estimator. The enhanced resilient estimation scheme is capable of maintaining resilient state recovery even when more than half of the sensors are attacked. The fundamental limitation of resilient recovery is obviated by incorporating data-driven prior into the physics-driven estimation design.

This paper has established a quantitative bridge that provides an in-road to many avenues for future research. For instance, given a target estimation performance and detection precision, how many sensors should be deployed in the system? The precision of a learning-based attack detector depends on the representative quality of the training dataset, so what is the quantitative relationship between the generalization of the generative attack dataset and the system's resiliency? Additionally, a recursive algorithm is expected for the weighted ℓ_1 estimation scheme. For nonlinear systems, a similar quantitative bridge should be built for different linearization operators. While data-driven model predictive control (MPC) and moving-horizon estimation (MHE) have attracted much attention due to the difficulty of obtaining high-fidelity models, the resiliency of runtime data used for the data-driven models is not guaranteed. Therefore, a resilient data-driven MHE is expected, and the work presented in this paper could be utilized to achieve this goal.

Acknowledgments. The authors acknowledge Professor Rodney Roberts at Florida State University for insightful discussions on the topic.

REFERENCES

[1] L. An and G.-H. Yang, *Secure state estimation against sparse sensor attacks with adaptive switching mechanism*, IEEE Trans. Automat. Control, 63 (2017), pp. 2596–2603, https://doi.org/10.1109/TAC.2017.2766759.

[2] O. M. Anubi and C. Konstantinou, *Enhanced resilient state estimation using data-driven auxiliary models*, IEEE Trans. Ind. Inform., 16 (2019), pp. 639–647, https://doi.org/10.1109/TII.2019.2924246.

[3] E. J. Candes, *The restricted isometry property and its implications for compressed sensing*, C. R. Math., 346 (2008), pp. 589–592, https://doi.org/10.1016/j.crma.2008.03.014.

[4] E. J. Candès, J. Romberg, and T. Tao, *Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information*, IEEE Trans. Inform. Theory, 52 (2006), pp. 489–509, https://doi.org/10.1109/TIT.2005.862083.

[5] E. J. Candes and T. Tao, *Decoding by linear programming*, IEEE Trans. Inform. Theory, 51 (2005), pp. 4203–4215, https://doi.org/10.1109/TIT.2005.858979.

[6] J. Chen, J. Wei, W. Chen, H. Sandberg, K. H. Johansson, and J. Chen, *Geometrical characterization of sensor placement for cone-invariant and multi-agent systems against undetectable zero-dynamics attacks*, SIAM J. Control Optim., 60 (2022), pp. 890–916, https://doi.org/10.1137/21M1403618.

[7] Y. Chen, S. Kar, and J. M. Moura, *Resilient distributed estimation: Sensor attacks*, IEEE Trans. Automat. Control, 64 (2018), pp. 3772–3779, https://doi.org/10.1109/TAC.2018.2882168.

[8] M. S. Chong, M. Wakaiki, and J. P. Hespanha, *Observability of linear systems under adversarial attacks*, in American Control Conference, 2015, pp. 2439–2444.

[9] D. L. Donoho, *For most large underdetermined systems of linear equations the minimal 1-norm solution is also the sparsest solution*, Comm. Pure Appl. Math., 59 (2006), pp. 797–829, https://doi.org/10.1002/cpa.20132.

[10] H. Fawzi, P. Tabuada, and S. Diggavi, *Secure estimation and control for cyber-physical systems under adversarial attacks*, IEEE Trans. Automat. Control, 59 (2014), pp. 1454–1467, https://doi.org/10.1109/TAC.2014.2303233.

[11] M. P. Friedlander, H. Mansour, R. Saab, and O. Yilmaz, *Recovering compressively sampled signals using partial support information*, IEEE Trans. Inform. Theory, 58 (2011), pp. 1122–1134, https://doi.org/10.1109/TIT.2011.2167214.

[12] D. M. Green, J. A. Swets, et al., *Signal Detection Theory and Psychophysics*, Vol. 1, Wiley New York, 1966, http://andrei.gorea.free.fr/Teaching_fichiers/SDT%20and%20Psytchophysics.pdf.

[13] X. He, E. Hashemi, and K. H. Johansson, *Distributed control under compromised measurements: Resilient estimation, attack detection, and vehicle platooning*, Automatica, 134 (2021), 109953, https://doi.org/10.1016/j.automatica.2021.109953.

[14] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, 2012.

[15] L. Hu, Z. Wang, Q.-L. Han, and X. Liu, *State estimation under false data injection attacks: Security analysis and system protection*, Automatica, 87 (2018), pp. 176–183, https://doi.org/10.1016/j.automatica.2017.09.028.

[16] A. Khazraei, S. Hallyburton, Q. Gao, Y. Wang, and M. Pajic, *Learning-based vulnerability analysis of cyber-physical systems*, in 2022 ACM/IEEE 13th International Conference on Cyber-Physical Systems (ICCPS), IEEE, 2022, pp. 259–269.

[17] A. Khazraei and M. Pajic, *Attack-resilient state estimation with intermittent data authentication*, Automatica, 138 (2022), 110035, https://doi.org/10.1016/j.automatica.2021.110035.

[18] C. Lee, H. Shim, and Y. Eun, *Secure and robust state estimation under sensor attacks, measurement noises, and process disturbances: Observer-based combinatorial approach*, in IEEE European Control Conference, 2015, pp. 1872–1877.

[19] E. A. Lee and S. A. Seshia, *Introduction to Embedded Systems: A Cyber-physical Systems Approach*, MIT Press, 2016.

[20] J. G. Lee, J. Kim, and H. Shim, *Fully distributed resilient state estimation based on distributed median solver*, IEEE Trans. Automat. Control, 65 (2020), pp. 3935–3942, https://doi.org/10.1109/TAC.2020.2989275.

[21] A. Mitra and S. Sundaram, *Byzantine-resilient distributed observers for lti systems*, Automatica, 108 (2019), 108487, https://doi.org/10.1016/j.automatica.2019.06.039.

[22] Y. Nakahira and Y. Mo, *Attack-resilient h_2, h_∞, and l_1 state estimator*, IEEE Trans. Automat. Control, 63 (2018), pp. 4353–4360, https://ieeexplore.ieee.org/abstract/document/8325450.

[23] D. Needell, *Noisy signal recovery via iterative reweighted l1-minimization*, in 2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers, IEEE, 2009, pp. 113–117.

[24] M. Pajic, I. Lee, and G. J. Pappas, *Attack-resilient state estimation for noisy dynamical systems*, IEEE Trans. Control Netw. Syst., 4 (2016), pp. 82–92, https://doi.org/10.1109/TCNS.2016.2607420.

[25] F. Pasqualetti, F. Dorfler, and F. Bullo, *Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems*, IEEE Contr. Syst. Mag., 35 (2015), pp. 110–127, https://doi.org/10.1109/MCS.2014.2364725.

[26] A. Sargolzaei, B. C. Allen, C. D. Crane, and W. E. Dixon, *Lyapunov-based control of a nonlinear multiagent system with a time-varying input delay under false-data-injection attacks*, IEEE Trans. Ind. Inform., 18 (2021), pp. 2693–2703, https://doi.org/10.1109/TII.2021.3106009.

[27] A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane III, and W. E. Dixon, *Detection and mitigation of false data injection attacks in networked control systems*, IEEE Trans. Ind. Inform., 16 (2019), pp. 4281–4292, https://doi.org/10.1109/TII.2019.2952067.

[28] A. Sargolzaei, F. M. Zegers, A. Abbaspour, C. D. Crane, and W. E. Dixon, *Secure control design for networked control systems with nonlinear dynamics under time-delay-switch attacks*, IEEE Trans. Automat. Control, 68 (2022), pp. 798–811, https://doi.org/10.1109/TAC.2022.3154354.

[29] T. Shinohara, T. Namerikawa, and Z. Qu, *Resilient reinforcement in secure state estimation against sensor attacks with a priori information*, IEEE Trans. Automat. Control, 64 (2019), pp. 5024–5038, https://doi.org/10.1109/TAC.2019.2904438.

[30] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, *Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach*, IEEE Trans. Automat. Control, 62 (2017), pp. 4917–4932, https://doi.org/10.1109/TAC.2017.2676679.

[31] Y. Shoukry and P. Tabuada, *Event-triggered state observers for sparse sensor noise/attacks*, IEEE Trans. Automat. Control, 61 (2015), pp. 2079–2091, https://doi.org/10.1109/TAC.2015.2492159.

[32] T. Sui, Y. Mo, D. Marelli, X. Sun, and M. Fu, *The vulnerability of cyber-physical system under stealthy attacks*, IEEE Trans. Automat. Control, 66 (2020), pp. 637–650, https://doi.org/10.1109/TAC.2020.2987307.

[33] N. Vaswani and W. Lu, *Modified-cs: Modifying compressive sensing for problems with partially known support*, IEEE Trans. Signal Process., 58 (2010), pp. 4595–4607, https://doi.org/10.1109/TSP.2010.2051150.

[34] M. Vidyasagar, *An Introduction to Compressed Sensing*, SIAM, 2019.

[35] X. Wang, H. Su, F. Zhang, and G. Chen, *A robust distributed interval observer for lti systems*, IEEE Trans. Automat. Control, 68 (2022), pp. 1337–1352, https://doi.org/10.1109/TAC.2022.3151586.

[36] S. Weerakkody, O. Ozel, Y. Mo, and B. Sinopoli, et al., *Resilient control in cyber-physical systems: Countering uncertainty, constraints, and adversarial behavior*, Found. Trends Syst. Control, 7 (2019), pp. 1–252, https://doi.org/10.1561/2600000018.

[37] T.-Y. Zhang and D. Ye, *False data injection attacks with complete stealthiness in cyber–physical systems: A self-generated approach*, Automatica, 120 (2020), 109117, https://doi.org/10.1016/j.automatica.2020.109117.

[38] Y.-B. Zhao, *Equivalence and strong equivalence between the sparsest and least l1-norm nonnegative solutions of linear systems and their applications*, J. Oper. Res. Soc. China, 2 (2014), pp. 171–193, https://doi.org/10.1007/s40305-014-0043-1.

[39] Y. Zheng and O. M. Anubi, *Attack-resilient weighted ℓ_1 observer with prior pruning*, in American Control Conference, 2021, pp. 340–345.

[40] Y. Zheng and O. M. Anubi, *Resilient Observer Design for Cyber-Physical Systems with Data-Driven Measurement Pruning*, Springer International Publishing, Cham, 2022, pp. 85–117, https://doi.org/10.1007/978-3-030-97166-3_5.

[41] M. Zhu and S. Martínez, *On attack-resilient distributed formation control in operator-vehicle networks*, SIAM J. Control Optim., 52 (2014), pp. 3176–3202, https://doi.org/10.1137/110843332.